Government College of Engineering and Research, Avasari (Khurd)
Tal- Ambegaon, Dist-Pune.412405
(NBA and NAAC accredited)

Third Year of Computer Engineering (2019 Course)
310247 : Computer Networks and Security Laboratory
Group A (Unit I and II)
Assignment No.: 01

Title

Setup of a Wired LAN using a Layer 2 Switch and verification using Wireshark

Objectives

- To understand how to physically set up a LAN using a Layer 2 switch.
- To crimp and test Ethernet cables.
- To configure IP addresses on end devices.
- To test LAN connectivity using the `ping` utility.
- To analyze packet flow using `Wireshark`.

Problem Statement

Design and implement a simple wired LAN setup involving at least two computers and a Layer 2 switch. Validate the configuration by assigning IP addresses, using `ping` for testing connectivity, and analyzing packet transfers using `Wireshark`.

Software and Hardware Requirements

Hardware:

- 2 or more computers (PCs or laptops with Ethernet ports)
- Layer 2 Switch (e.g., Cisco, D-Link, Netgear)
- Cat5e/Cat6 Ethernet cables
- RJ-45 connectors
- Crimping Tool
- Cable tester (Line Tester)

Software:

- Windows/Linux OS with command-line access
- Wireshark Packet Analyzer

Theory

Local Area Network (LAN):
A Local Area Network (LAN) is a network that connects computers and other devices within a limited geographical area such as a home, school, or office building. LANs are typically high-speed and use Ethernet or Wi-Fi technology for communication. Devices in a LAN can share resources such as files, printers, and internet connections. Communication in LANs is often achieved using switches, routers, and network cables.

Switch:
A switch is a network device that operates at Layer 2 (Data Link Layer) of the OSI model. It connects multiple devices within a LAN and uses MAC (Media Access Control) addresses to forward data only to the intended recipient. Unlike hubs, which broadcast data to all connected devices, switches improve efficiency and reduce collisions by sending data only to the target port. Layer 2 switches do not perform routing (which is a Layer 3 operation) but are ideal for internal LAN communication.

Ping Utility:
`ping` is a network diagnostic command-line tool used to test the reachability of a host on an IP network. It sends Internet Control Message Protocol (ICMP) Echo Request packets to the destination host and listens for Echo Reply packets. The output shows whether the destination is reachable, the round-trip time, and packet loss statistics. `ping` is widely used to troubleshoot network connectivity issues.

Wireshark:
Wireshark is an open-source packet analyzer used for network troubleshooting, analysis, and education. It captures network packets in real-time and displays them in detail for examination. Users can filter packets by protocol, source/destination address, port number, and more. In this experiment, Wireshark helps verify and visualize the ICMP packets generated by the `ping` utility. It provides a deeper understanding of how data moves across a LAN.

Capturing Ping Packets using Wireshark
Wireshark can be used to capture and analyze `ping` packets (ICMP Echo Request and Reply) exchanged between devices on a network. Follow these steps to capture ping traffic:

1. **Open Wireshark:** Launch Wireshark on the computer where you want to capture packets.
2. **Select Network Interface:** Choose the active network interface (e.g., `Ethernet0`) that is connected to the LAN. Double-click to start capturing packets.
3. **Apply Filter:** In the display filter bar at the top, type `icmp` and press `Enter`. This ensures that only ICMP packets (used by `ping`) are displayed.
4. **Run Ping Command:** Open a command prompt or terminal and execute:

   ```
   ping <destination_IP_address>
   ```

   For example: `ping 192.168.1.11`

5. **Observe Captured Packets:** In Wireshark, you will see ICMP Echo Request and Echo Reply packets appear in real time. Each entry shows:
   - Timestamp
   - Source and Destination IP addresses
   - Protocol as ICMP
   - Type (Echo Request = 8, Echo Reply = 0)
6. **Stop Capture:** Click the red square button on the toolbar to stop capturing once the ping completes.
7. **Analyze Packet Details:** Click on any ICMP packet to expand its headers (Ethernet, IP, ICMP) and view details such as sequence number, checksum, TTL, and payload.

Preparing Ethernet Cables using T568B Wiring Standard

To connect devices in a wired LAN, we use Ethernet cables terminated with RJ-45 connectors. The T568B wiring standard specifies the color sequence for the eight wires inside a twisted-pair cable. Follow the steps below to prepare a *straight-through* Ethernet cable:

1. **Strip the Cable Jacket:** Use a cable stripper or crimping tool to remove about 1.5 inches (3-4 cm) of the outer PVC jacket of the Cat5e or Cat6 cable.
2. **Untwist and Arrange the Wires:** Gently untwist the 4 twisted pairs and straighten the individual wires. Arrange them in the T568B color sequence from left to right:

   ```
   White-Orange, Orange, White-Green, Blue, White-Blue, Green, White-Brown, Brown
   ```
3. **Trim Wires Evenly:** Use a cutter to trim the wires to the same length—around 1.3 cm (0.5 inch) from the jacket.
4. **Insert into RJ-45 Connector:** Holding the RJ-45 plug with the clip facing down, insert the wires carefully into the connector channels, ensuring each wire goes into the correct slot.
5. **Crimp the Connector:** Insert the RJ-45 plug into a crimping tool and squeeze firmly. This secures the wires and punctures their insulation for electrical contact.
6. **Repeat for Other End:** Prepare the other end of the cable similarly using the same T568B color pattern to create a straight-through cable.
7. **Test the Cable:** Use a cable tester (line tester) to verify proper connectivity and continuity for all 8 wires.

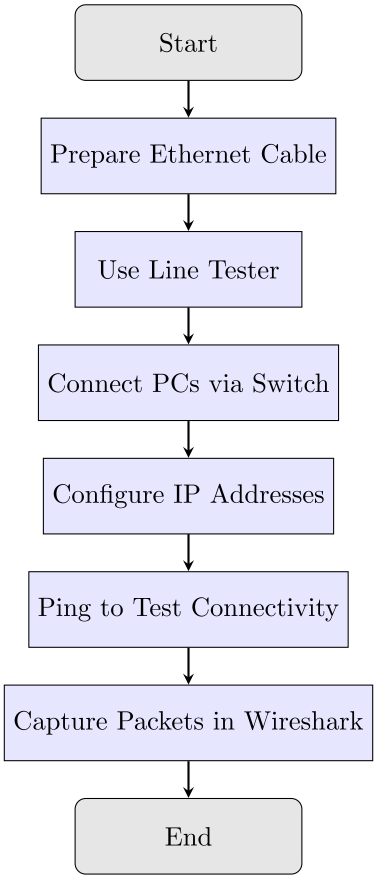
T568B Color Code Order:

Pin Number	Color (T568B)
1	White-Orange
2	Orange
3	White-Green
4	Blue
5	White-Blue
6	Green
7	White-Brown
8	Brown

Steps

1. Prepare Ethernet cables using T568B wiring standard.
2. Use line tester to verify cable functionality.
3. Connect the computers to the Layer 2 switch using the cables.
4. Assign static IP addresses to each system.
5. Verify connectivity using the `ping` command.
6. Use Wireshark to capture and analyze packets.

Flowchart



Test Cases

Test Case ID	Description	Expected Result	Actual Result	Status
TC1	Cable test with line tester	All lights glow in sequence		
TC2	IP configuration correctness	IPs in same subnet		
TC3	Ping between two PCs	Replies received		

TC4	Wireshark captures ICMP packets	ICMP Echo & Reply seen		

Test Data Set

Device	IP Address	Subnet Mask
PC1	192.168.1.10	255.255.255.0
PC2	192.168.1.11	255.255.255.0

Conclusion / Analysis

- A LAN was successfully established using a Layer 2 switch.
- Custom Ethernet cables were prepared and verified.
- IP addresses were configured, and `ping` was used to test connectivity.
- `Wireshark` analysis showed ICMP Echo Request and Echo Reply packets, validating communication.

Assessment Grade/Marks

__________ / 10

Assessor's Signature

Name: ______________________________

Sign: ______________________________

Date: __________ / __________ / 202_____