Computer Networks-LAB-3

Physical Layer and Data Link Layer

Lab Objectives:

1. Explore different types of physical transmission media: Copper, Fiber, and Wireless.
2. Understand the functionalities of the Data Link Layer.
3. Configure and analyze Ethernet frames using network tool wireshark.

Section 1: Exploring Physical Transmission Media

1.1 Copper Media (Twisted Pair, Coaxial)

- Used for wired networks.
- Common types: UTP (Unshielded Twisted Pair), STP (Shielded Twisted Pair), and Coaxial cables.
- Pros: Cost-effective, easy to install.
- Cons: Susceptible to electromagnetic interference.

Practical Task:

1. Identify different copper cables (UTP, STP, Coaxial).
2. Use a cable tester to check continuity.

1.2 Fiber Optic Media

- Uses light for data transmission.
- Types: Single-mode, Multi-mode fiber.
- Pros: High bandwidth, long-distance communication, immune to EMI.
- Cons: Expensive, complex installation.

Practical Task:

1. Inspect fiber optic cables.
2. Test fiber optic connections using a fiber optic tester.

1.3 Wireless Transmission Media

- Uses radio waves, microwaves, or infrared for data transmission.
- Common types: Wi-Fi, Bluetooth, Satellite, Cellular networks.
- Pros: Mobility, easy deployment.
- Cons: Susceptible to interference, security risks.

Practical Task:

1. Analyze Wi-Fi signal strength using Windows **Netsh** command:

```
netsh wlan show interfaces
```

2. Capture wireless packets using **Wireshark**.

Section 2: Understanding Data Link Layer Functionalities

2.1 Role of Data Link Layer

- Provides reliable node-to-node communication.
- Handles framing, error detection, and MAC addressing.
- Works with Ethernet, Wi-Fi, PPP protocols.

2.2 MAC Addressing

- Unique identifier assigned to network interfaces.
- Format: 48-bit address (e.g., 00:1A:2B:3C:4D:5E).
- Used in Ethernet and wireless networking.

Practical Task:

1. Find the MAC address of a system using:

```
ipconfig /all
```

2. Change the MAC address (Windows example using Registry Editor):
    - Open **Regedit**.
    - Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}.
    - Locate your network adapter, edit NetworkAddress value.

- Restart the network adapter.

Section 3: Configuring and Analyzing Ethernet Frames

3.1 Ethernet Frame Structure

- **Preamble (7 bytes)**: Synchronization.
- **SFD (1 byte)**: Start of Frame Delimiter.
- **Destination MAC (6 bytes)**: Receiver address.
- **Source MAC (6 bytes)**: Sender address.
- **Type/Length (2 bytes)**: Identifies protocol.
- **Payload (46-1500 bytes)**: Actual data.
- **FCS (4 bytes)**: Error checking.

3.2 Capturing Ethernet Frames

Practical Task:

1. Open **Wireshark** and start capturing packets.
2. Filter Ethernet frames using:

eth.type == 0x0800

3. Analyze the captured frame structure.

3.3 Configuring Ethernet Interface

Practical Task:

1. Assign an IP address manually:

netsh interface ip set address name="Ethernet" static 192.168.1.100 255.255.255.0 192.168.1.1

2. Bring the interface up/down:
3. netsh interface set interface name="Ethernet" admin=enabled

netsh interface set interface name="Ethernet" admin=disabled

4. Verify connectivity using:

ping 192.168.1.1

Conclusion:

In this lab, we explored various transmission media, studied Data Link Layer functionalities, and analyzed Ethernet frames. Understanding these concepts is crucial for network configuration and troubleshooting in Windows environments.

Lab Submission:

- Screenshots of captured Ethernet frames in Wireshark.
- Commands executed for MAC address verification and Ethernet configuration.
- Summary of observations and results.

Additional Resources:

- Wireshark Official Documentation: https://www.wireshark.org/docs/
- Microsoft Networking Documentation: https://learn.microsoft.com/en-us/windows-server/networking/