LAB: Assignment 2

Objective: To understand the Networking Components (Hardware/Software)

Instructions: The instructor is required to discuss the following questions with the students. Students are required to make note on these questions.

Q1. Network Interface Cards - their use, types and working.

Q2. Hub Device and its' working.

Q3. Switch Device and its' working.

Q4. Router Device and its' working.

Q5. Bridge device and its' working.

Q6. Types of networking wires and connectors, shapes and specifications.

Q7. Wireless Access Points.

Q8. Proxy Servers and usages.

Q9. Firewall and working principle.

Q1. Network Interface Cards - their use, types and working.

A **Network Interface Card (NIC)** is a hardware component that connects a computer to a network. It acts as the translator between your computer's data and the signals on the network cable or wireless network.

- **Use**: The primary use of a NIC is to provide a dedicated, full-time connection to a network.
- **Types**:
    - **Wired NICs**: These use an Ethernet port and cable (typically with an RJ45 connector) to connect to the network.
    - **Wireless NICs**: These use an antenna to connect to a Wi-Fi network without physical cables. They are standard in laptops and smartphones.
- **Working**: Every NIC has a unique physical address called a **MAC (Media Access Control) address**. When sending data, the NIC formats it into packets and transmits them. When receiving data, it checks the packet's destination MAC address; if it matches its own, it processes the packet and sends it to the computer's CPU.

Q2. Hub Device and its' working.

A **Hub** is a basic, non-intelligent networking device that connects multiple devices in a Local Area Network (LAN). It operates at the **Physical Layer (Layer 1)** of the OSI model.

- **Working**: When a data packet arrives at one port of the hub, it is simply copied and broadcasted (repeated) to all other ports on the hub. It doesn't know which specific device the packet is intended for. This means all devices connected to the hub share the same bandwidth. If two devices try to send data at the same time, a "collision" occurs, slowing down the entire network. Hubs are now largely considered obsolete and have been replaced by switches.

Q3. Switch Device and its' working.

A **Switch** is an intelligent networking device that connects multiple devices in a LAN. It operates at the **Data Link Layer (Layer 2)** of the OSI model.

- **Working**: Unlike a hub, a switch is smart. It maintains a table of the MAC addresses of all the devices connected to its ports. When a data packet arrives, the switch reads the destination MAC address from the packet's header and forwards the packet only to the port connected to the intended recipient. This creates a dedicated connection between the sender and receiver, preventing data collisions and making the network much more efficient and faster than one using a hub.

Q4. Router Device and its' working.

A **Router** is a device that connects different networks together. Its main job is to forward data packets between these networks, such as connecting your home network (LAN) to the Internet (WAN). It operates at the **Network Layer (Layer 3)** of the OSI model.

- **Working**: Routers use **IP (Internet Protocol) addresses** to direct traffic. Each router maintains a **routing table**, which is a list of paths to various network destinations. When a packet arrives, the router examines the destination IP address and uses its routing table to determine the most efficient path to send the packet on its way to its final destination. They are the backbone of the internet, directing all traffic.

Q5. Bridge device and its' working.

A **Bridge** is a device used to connect two separate LAN segments, making them appear as a single network. It operates at the **Data Link Layer (Layer 2)** of the OSI model, just like a switch.

- **Working**: A bridge inspects incoming traffic and checks the destination MAC address. It keeps a table of which MAC addresses are on which side of the bridge. If the destination device is on the same segment as the source, the bridge blocks the traffic from crossing over, reducing unnecessary traffic. If the destination is on the other segment, it forwards the packet. Switches are essentially multi-port bridges and have largely replaced them.

Q6. Types of networking wires and connectors, shapes and specifications.

There are three main types of networking cables:

1. **Twisted Pair Cable**:
    - **Description**: The most common type of network cable, used for Ethernet. It consists of four pairs of thin, insulated copper wires twisted together to reduce electromagnetic interference.
    - **Connector**: **RJ45**, which looks like a wider version of a telephone jack.
    - **Specifications**: Comes in different categories like **Cat5e**, **Cat6**, and **Cat7**, which support progressively higher speeds and bandwidth.
2. **Fiber Optic Cable**:
    - **Description**: Transmits data using light pulses through thin strands of glass or plastic. It's extremely fast, can travel long distances, and is immune to electrical interference.
    - **Connectors**: Common connectors include **SC (Subscriber Connector)**, **ST (Straight Tip)**, and **LC (Lucent Connector)**.
    - **Specifications**: Categorized as **Single-Mode** (for long distances) and **Multi-Mode** (for shorter distances).
3. **Coaxial Cable**:
    - **Description**: Features a central copper conductor, insulation, a braided metal shield, and an outer jacket. Used for cable TV and older computer networks.

- **Connector**: **BNC (Bayonet-Neill-Concelman)** connector.

Q7. Wireless Access Points.

A **Wireless Access Point (WAP)** is a device that allows wireless-capable devices (like laptops, phones) to connect to a wired network. A WAP is not a router; its main job is to produce a Wi-Fi signal.

- **Working**: The WAP connects to a wired router or switch via an Ethernet cable. It then broadcasts a wireless signal (SSID) over a specific area. Wi-Fi-enabled devices can find this signal and connect to it, granting them access to the wired network and, by extension, the internet. In many home setups, the router and the wireless access point are combined into a single device, often called a "wireless router."

Q8. Proxy Servers and usages.

A **Proxy Server** is a server that acts as an intermediary for requests from clients seeking resources from other servers. When you use a proxy, your traffic flows through the proxy server on its way to the address you requested.

- **Usages**:
  - **Anonymity & Privacy**: It hides your original IP address, making your online actions harder to trace.
  - **Security**: Proxies can be configured to block access to malicious websites and can act as a buffer against cyberattacks.
  - **Content Filtering**: Schools and companies use proxies to restrict access to certain websites and content.
  - **Improved Performance**: Proxies can **cache** (store) copies of frequently visited websites. When another user requests the same page, the proxy can deliver it from its cache, which is much faster.
  - **Bypassing Geo-Restrictions**: It can make your traffic appear to be coming from a different geographic location, allowing you to access content that is restricted in your region.

Q9. Firewall and working principle.

A **Firewall** is a network security system that acts as a protective barrier between a trusted internal network (e.g., your home or office network) and an untrusted external network (e.g., the Internet). It can be implemented as hardware, software, or a combination of both.

- **Working Principle**: A firewall monitors and filters all incoming and outgoing network traffic based on a set of pre-defined security rules. It inspects each data packet and decides whether to **allow** it or **block** it. This decision is based on information like the source and destination IP addresses, port numbers, and protocols. By enforcing these rules, a firewall

helps prevent unauthorized access, viruses, malware, and other cyber threats from entering or leaving the protected network.