

## Assignment – 2

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

Ans1. A Network Interface Card is a hardware component which enables computers or other devices to connect to a network, handling both the physical and logical aspects of data communication.

Use:

- It provides a connection between a device and a wired (Ethernet, fiber optic) or wireless (Wi-Fi) network.
- It converts data signals between the computer's internal format and network format for transmission.
- Every NIC has a unique MAC address used for local network identification and data delivery.

Types:

1. Ethernet NICs: Connect using cables like Cat5 or Cat6 cables.
2. Wireless NICs: Use Wi-Fi to connect wirelessly.
3. Fiber Optic NICs: Used for high-speed fiber optic connections.
4. Bluetooth NICs: For short-range wireless communication.

Working:

- When data is sent from the computer, the NIC converts it into signals suitable for transmission (electrical signals for wired, radio waves for wireless).
- It attaches a MAC address to data frames for identification.
- On receiving data, the NIC checks for errors and passes the data to the computer's operating system.

Q2. Hub Device and its' working.

Ans2. A hub is a simple networking device that connects multiple Ethernet devices, making them act as a single network segment. It sends data to all ports regardless of which port has sent the data request.

Working:

- When a hub receives a data packet from one device, it broadcasts the packet to all other connected devices regardless of the destination.
- It operates at the physical layer (Layer 1) of the OSI model.
- Hubs do not filter data or know the destination MAC address.

**Q3. Switch Device and its' working.**

**Ans3.** A switch is a more intelligent device that connects devices on a network and manages data traffic efficiently. It sends data to only the port which has sent a request to the server.

**Working:**

- Switches operate at the data link layer (Layer 2).
- When a switch receives a packet, it reads the MAC address and forwards the packet only to the intended device.
- It maintains a MAC address table to track devices connected to each port.
- This reduces collisions and improves network efficiency.

**Q4. Router Device and its' working.**

**Ans4.** A router connects multiple networks together, such as a local network to the internet.

**Working:**

- Routers operate at the network layer (Layer 3).
- They examine the IP address of data packets to determine the best path for forwarding.
- Routers use routing tables and protocols (like OSPF, BGP) to direct packets.
- They also manage traffic, provide firewall capabilities, and can perform NAT (Network Address Translation).

**Q5. Bridge device and its' working.**

**Ans5.** A bridge connects two or more network segments, improving performance and managing traffic between them.

**Working:**

- Operates at the data link layer (Layer 2).
- It filters traffic by forwarding only data destined for the other segment.
- Bridges reduce collisions by dividing collision domains.
- It learns MAC addresses to decide whether to forward or filter frames.

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

**Ans6. Wires/Cables:**

**1. Twisted Pair Cables:**

- Unshielded Twisted Pair (UTP): Common for Ethernet (Cat5, Cat5e, Cat6).
- Shielded Twisted Pair (STP): Has shielding to reduce interference.

2. Coaxial Cable:

- Single copper conductor with shielding. Used in older networks and cable TV.

3. Fiber Optic Cable:

- Uses light signals. Types include single-mode and multi-mode fibers.

Connectors:

- RJ45: Used with twisted pair cables for Ethernet.
- BNC Connector: Used with coaxial cables.
- SC, ST, LC Connectors: Used with fiber optic cables.

Shapes and Specifications:

- RJ45 connector: 8 pins arranged in a rectangular shape.
- Fiber connectors vary in shape but are designed to align fiber cores precisely.

Q7. Wireless Access Points.

Ans7. A Wireless Access Point (WAP) is a networking device that allows wireless devices to connect to a wired network. They act as a bridge between wireless clients and the wired LAN. WAPs broadcast SSIDs and handle authentication, encryption and data transfer. Used in offices, public hospitals and homes to provide wireless coverage.

Q8. Proxy Servers and usages.

Ans8. Proxy Server:

- Acts as an intermediary between a client and the internet.
- Requests from clients go to the proxy first, which then forwards the request to the target server.

Usages:

- Improve security and privacy by hiding client IP addresses.
- Cache frequently accessed content to reduce bandwidth.
- Filter web traffic to block unwanted sites.
- Log user activity for monitoring.

Q9. Firewall and working principle.

Ans9. A security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Working Principle:

- Inspects packets at various layers (network, transport).

- Filters traffic based on IP addresses, ports, protocols, or content.
- Can be hardware-based or software-based.
- Types include packet-filtering firewalls, stateful inspection firewalls, and next-generation firewalls.
- Helps prevent unauthorized access, malware, and attacks.