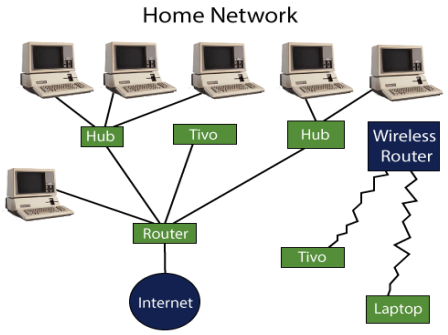
CN Tut 2 Activity

~(Group 4 Batch 1)

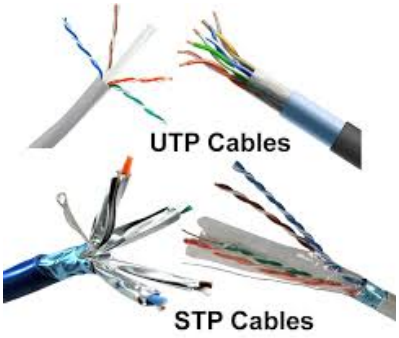
Q. Identification of various network components

1. Hardware Components

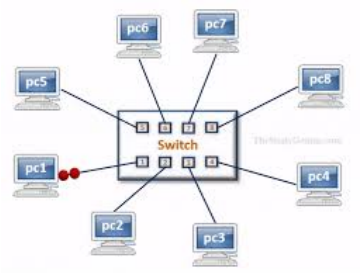
1) **Router** :
A device that connects two or more Networks or Computers.The main Goal of Router is to manage the traffic between these networks and to send their Data Packets to respected IP addresses.



2) **Cable**
It is a Physical connection that is used to transfer the data between networks.

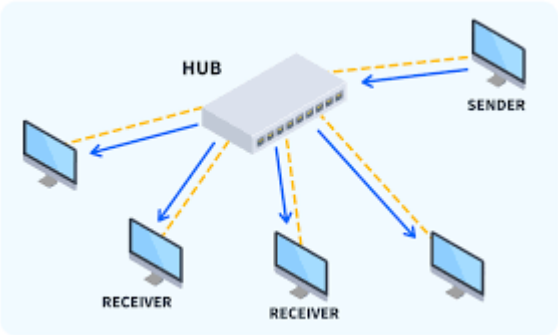


3) **Switch:**
Connects multiple devices in a single network and forwards data based on MAC addresses.



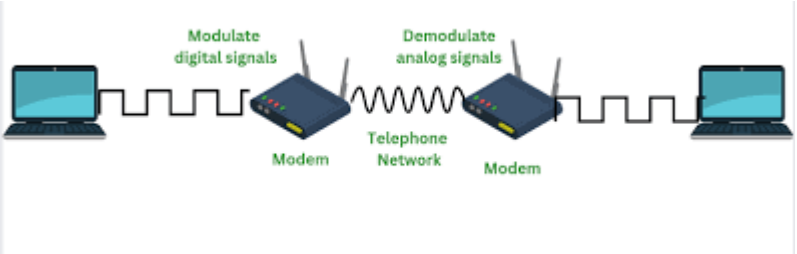
4) **Hub:**

A device that broadcasts data to all connected devices.primary function is to receive data signals from connected devices and broadcast them to all other connected devices, regardless of the intended recipient.



5) **Modem:**

Converts digital data to analog signals (and vice versa) for internet connectivity.



2. **Transmission Media:**

1) **Wired Media** :
Ethernet Cables , Fiber Optic cables , UTP-STP cables for sending Data through Physical connection.

2) **Wireless Media:**
Wi-Fi, Bluetooth, infrared, and radio frequency technologies for wireless communication.

3. Network Protocols

Protocols are the set of rules to establish communication between networks.

Ex.

1. **IP (Internet Protocol)**: Assigns unique addresses to devices and routes data packets across networks to their destination. It ensures the correct delivery of data but doesn't guarantee reliability.
2. **TCP (Transmission Control Protocol)**: Provides reliable data transmission by ensuring packets are delivered accurately and in order.
3. **UDP (User Datagram Protocol)**: Offers faster data transmission without reliability checks, often used for real-time applications like video streaming.

4. **DNS (Domain Name System)**: Translates human-readable domain names (e.g., google.com) into IP addresses required for network communication.
5. **HTTP/HTTPS**: Protocols used for accessing websites, with HTTPS adding encryption for secure communication.

4. Software Components

1. **Operating Systems**: Network-enabled OS like Windows, macOS, or Linux manages network interactions.
2. **Networking Software**: Tools for configuring and monitoring networks (e.g., Cisco Packet Tracer, Wireshark).
3. **Protocols**: Software rules that define data communication (e.g., TCP/IP, HTTP, FTP).
4. **Virtualization Software**: Allows creation of virtual networks, such as VMware or Hyper-V.

Q. What component is required to share RAM over a configured network?

Sharing RAM in a network is a combination of software components, hardware components, and protocols. The structure goes like this:

1. Software Component

- *Remote Memory Software (RMS):* A program that allows memory resources to be shared across systems, such as Memcached or Distributed Shared Memory (DSM) systems.
- *Virtualization Software*: Hypervisors (like VMware or Hyper-V) or tools for the cloud that help share resources, specifically memory.
- *Operating System Support:* The OS must support memory sharing options or a network-attached memory configuration. Examples include NFS for Linux or Windows File Sharing for RAMDisk access.

2. Hardware Component

- *High-Performance Servers*: Systems with enough RAM to share and work upon.
- *High-Speed Network Interfaces (NICs)*: Make possible super-fast data transfer speeds required for real-time memory access (for instance, Gigabit Ethernet or 10GbE).
- *Switches or Routers*: Connects devices in the local area network with low-latency requirements to facilitate communication.

3. Network Protocol

- Remote Direct Memory Access (RDMA): Protocol allows for direct access of memory over the network, with low latency and high throughput.
- iSCSI or NFS are both protocols that allow memory or storage to be shared over a network for a distributed system.

TCP or UDP are core protocols for establishing reliable communication between devices for data transfer.

Q. What is a device driver?

Device Drivers

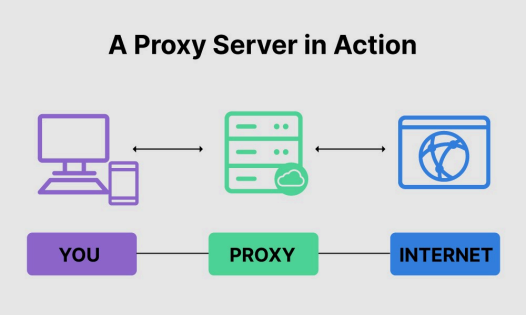
A device driver is a software that allows computers to communicate with hardware like network devices.We need to install the correct device driver to work hardware devices properly.

- **Universal Drivers** :
  These are drivers that work with many different types of network devices.
  For example, drivers for Intel, Realtek, and Broadcom network cards can work on many devices of the same brand.

- **Plug and Play :**
  Modern operating systems like Windows and Linux detect the device automatically and install the correct driver.
  For example, plug in an Ethernet cable, the system might automatically install the network driver.

Q. How can a proxy server enhance the utility of resources to be shared over the internet?

A proxy server is a system that functions as a gateway between the users and the internet therefore preventing cyber attackers from entering private networks.



Benefits Of A Proxy Server:

1. It enhances the security of the user by acting as a firewall between the user and the internet.
2. By using different proxies, it can help users to avoid unwanted ads or collection of IP-specific data.
3. We can access location-specific content by using a proxy on a server located in a different country. For example, the technology can allow you to open location-restricted websites by using local IP addresses of the location you want to appear to be in.

A proxy server can enhance the utility of resources shared over the internet by providing the following benefits:

1. **Bandwidth Optimization:** Proxy servers can be used to cache high-demand content so that requests to the origin server are minimized and thereby optimize bandwidth utilization.
2. **Load Balancing:** Proxy servers distribute the load of incoming requests onto several back-end servers to ensure maximum usage of server resources without overloading them.

3. **Access Control:** Proxies can restrict or permit access to certain resources depending on the user role, IP address, or authentication mechanism available.
4. **Enhanced Security:** Proxies anonymize user data, secure IP addresses, and provide a barrier against external threats like malware or cyberattacks.
5. **Content Filtering:** Proxy servers can filter unwanted or malicious content so that organizations can use the Internet for safe browsing.
6. **Geolocation Flexibility:** Proxies enable access to location-restricted resources by masking the user's real location with a different IP address.
7. **Efficient Resource Sharing:** Proxies simplify sharing within a network by centralizing access to resources, ensuring the safe and optimized use of shared files, applications, or services.
8. **Monitoring and Logging:** Proxy servers will log network activity, give system administrators a means to survey usage, find patterns, and optimize resource management.

Keywords Explanation

Wireshark

Wireshark is a widely used, open source network analyzer that can capture and display real time network traffic. It is particularly useful for troubleshooting network issues, analyzing network protocols and ensuring network security. Networks must be monitored to ensure smooth operations and security

Thin client

A thin client is a device with limited computing capacity. Your users can use it to perform more complicated, compute-intensive tasks by exchanging data with a centralized server. Traditionally, organizations had to purchase expensive desktop machines for employees to perform business-related tasks. Virtual desktop infrastructure (VDI) technology has replaced this with virtual desktops that your users can access using thin client terminals. Thin clients use fewer resources and are easier to manage and secure compared to traditional desktop devices. Some organizations may also choose to deploy their clients as applications that users can run on their personal smart devices.

ALOHA

ALOHA is a multiple access protocol for transmission of data via a shared network channel. It operates in the medium access control sublayer (MAC sublayer) of the open systems interconnection (OSI) model. Using this protocol, several data streams originating from multiple nodes are transferred through a multi-point transmission channel.

CSMA protocol

Carrier Sense Multiple Access (CSMA) is a method used in computer networks to manage how devices share a communication channel to transfer the data between two devices. In this protocol, each device first senses the channel before sending the data. If the channel is busy, the device waits until it is free. This helps reduce collisions, where two devices send data at the same time, ensuring smoother communication across the network. CSMA is commonly used in technologies like Ethernet and Wi-Fi.

Q. How to establish a LAN network?

Requirements to set up LAN Network:

- Workstation/Personal devices: laptop, computer, mobile phones, etc.
- Network devices: router, switch, modem (if not already present in the router)
- Sharing resources: printers, disk drives, etc.
- Cables: Ethernet cables, wires for connecting other devices (in case of wired LAN)
- Internet connection: Wi-Fi (in case of wireless LAN)
- Instructions to set up LAN Network:
- Following steps should be followed to set up a LAN network:

Steps:-

- **Identify services**: Identify the network services such as printers, disk drives, data, etc. that will be shared among workstations.
- **Identify devices**: Identify devices such as computers, mobile phones, laptops, etc. with a unique address that will be connected to the network.
- **Plan connections**: Design the network by laying out cable wires between network devices or by making wireless connections. Wired LAN is set up using Ethernet cables while wireless LAN is set up using Wi-Fi that connects network devices without making any physical connection. A wired LAN network is more secure than a wireless LAN network but it is difficult to relocate.
- **Select networking device**: Select switch or router with enough ports to connect all workstations within the network. The choice of networking device is based on the requirements of the network.
- **Configure ports**: Configure WAN ports according to the information provided by ISP (Internet Service Provider). Also, configure LAN ports of cable routers such that there are enough addresses available for all the workstations within the network. A cable router acts as DHCP (Dynamic Host Configuration Server) server that automatically allocates addresses to all the devices connected to the network.
- **Make connections**: Connect all the devices using wires to configure a LAN network. Standard Ethernet cables are used to connect workstations and servers while Ethernet crossover cable is used to connect the switch to cable routers by connecting the standard port of the switch with router's LAN port. For wireless LAN, connect all the devices to Wi-Fi with SSID (Service Set Identifier) provided by the router or switch to configure the LAN network.
- **Test the network**: Test each of the workstation connected to the network and ensure every workstation has access to network services.