Report of Day-2(07-06-25)

Today's Objectives:

Theory:

1) Getting the Overview of the OSI model.
2) Understand the difference between the MAC and IP address.
3) Understand the types of network-cables.

Practical:

1) Creating a small LAN.

2) Observe the MAC address using Ipconfig / all.

3) To know the correct cables for switch/PC, router/router connections.

Overview of the OSI Model:

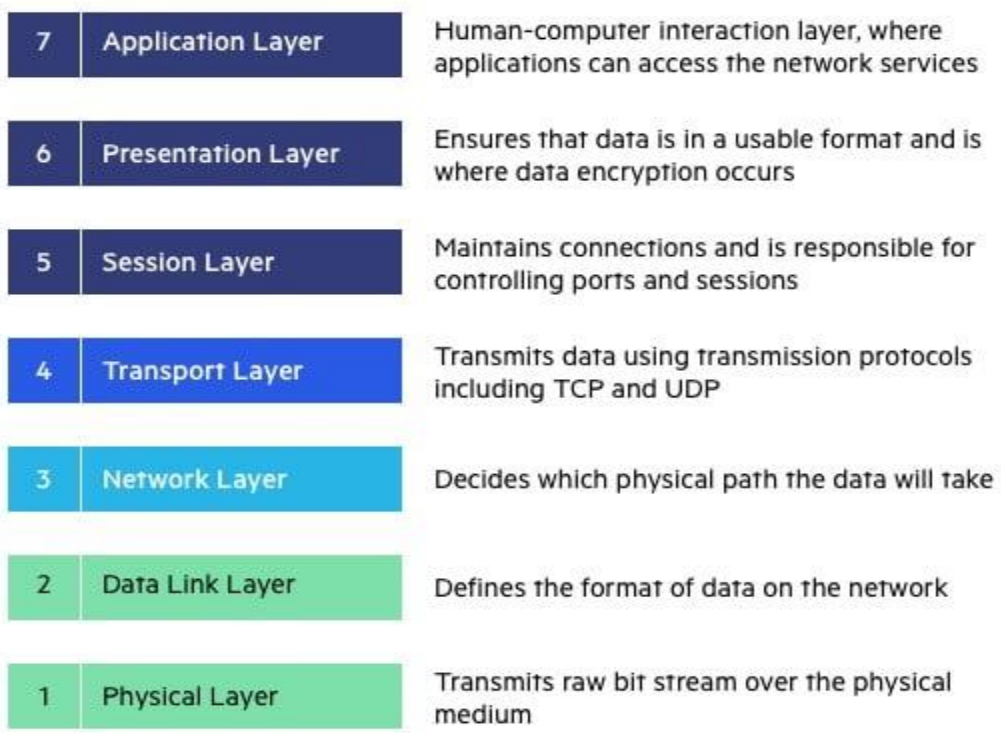
The OSI (Open Systems Interconnection) model outlines seven layers that enable computer systems to communicate over a network, from physical hardware to high-level applications. Each layer interacts with the ones above and below it, helping structure data transmission and making network troubleshooting easier.

Introduced in 1983 and adopted as an international standard by ISO in 1984, the OSI model became the first widely accepted framework for network communications. While the modern Internet relies on

the simpler TCP/IP model, the OSI model remains a valuable tool for understanding and explaining how networks function.

Advantages of the OSI Model:

- Shared understanding: It provides a universal language for networking, helping different devices and software communicate effectively. Its layered structure simplifies troubleshooting by isolating issues.
- Faster development: Developers can work on individual layers independently, accelerating innovation and allowing specialized teams to focus on specific functions.
- Flexible standardization: New technologies can be integrated at any layer without disrupting the overall network, ensuring compatibility, scalability, and long-term adaptability.



7. Application Layer

The Application Layer serves as the interface between the end-user applications and the underlying network services. This layer provides protocols and services that are directly utilized by end-user applications to communicate across the network. Key functionalities of the Application Layer include resource sharing, remote file access, and network management.

Examples of protocols operating at the Application Layer include Hypertext Transfer Protocol (HTTP) for web browsing, File Transfer Protocol (FTP) for file transfers, Simple Mail Transfer Protocol (SMTP) for email services, and Domain Name System (DNS) for resolving domain names to IP addresses. These protocols ensure that user applications can effectively communicate with each other and with servers over a network.

6. Presentation Layer

The Presentation Layer, also known as the syntax layer, is responsible for translating data between the application layer and the network format. It ensures that data sent from the application layer of one system is readable by the application layer of another system. This layer handles data formatting, encryption, and compression, facilitating interoperability between different systems.

One of the key roles of the Presentation Layer is data translation and code conversion. It transforms data into a format that the

application layer can understand. For example, it may convert data from ASCII to EBCDIC. It also includes encryption protocols to ensure data security during transmission and compression protocols to reduce the amount of data for efficient transmission.

5. Session Layer:

The Session Layer manages and controls the connections between computers. It establishes, maintains, and terminates connections, ensuring that data exchanges occur efficiently and in an organized manner. The layer is responsible for session checkpointing and recovery, which allows sessions to resume after interruptions.

Protocols operating at the Session Layer include Remote Procedure Call (RPC), which enables a program to execute a procedure on a remote host as if it were local, and the session establishment phase in protocols like NetBIOS and SQL. These services enable reliable communication, especially in complex network environments.

4. Transport Layer:

The Transport Layer provides end-to-end communication services for applications. It ensures complete data transfer, error recovery, and flow control between hosts. This layer segments and reassembles data for efficient transmission and provides reliability with error detection and correction mechanisms.

Protocols at this layer include Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). TCP is connection-oriented and

ensures reliable data transfer with error checking and flow control, making it suitable for applications like web browsing and email. UDP is connectionless, offering faster, though less reliable, transmission, suitable for applications like video streaming and online gaming.

3. Network Layer:

The Network Layer is responsible for data routing, forwarding, and addressing. It determines the best physical path for data to reach its destination based on network conditions, the priority of service, and other factors. This layer manages logical addressing through IP addresses and handles packet forwarding.

Key protocols at this layer include the Internet Protocol (IP), which is important for routing and addressing, Internet Control Message Protocol (ICMP) for diagnostic and error-reporting purposes, and routing protocols like Routing Information Protocol (RIP) that manage the routing of data across networks.

2. Data Link Layer:

The Data Link Layer is responsible for node-to-node data transfer and error detection and correction. It ensures that data is transmitted to the correct device on a local network segment. This layer manages MAC (Media Access Control) addresses and is divided into two sublayers: Logical Link Control (LLC) and Media Access Control (MAC).

Protocols and technologies at this layer include Ethernet, which defines the rules for data transmission over local area networks (LANs), and Point-to-Point Protocol (PPP) for direct connections between two network nodes. It also includes mechanisms for detecting and possibly correcting errors that may occur in the Physical Layer.

1. Physical Layer:

The Physical Layer is responsible for the physical connection between devices. It defines the hardware elements involved in the network, including cables, switches, and other physical components. This layer also specifies the electrical, optical, and radio characteristics of the network.

Functions of the Physical Layer include the modulation, bit synchronization, and transmission of raw binary data over the physical medium. Technologies such as Fiber Optics and Wi-Fi operate at this layer, ensuring that the data physically moves from one device to another in the network.

What's the difference between MAC and IP addresses?

MAC addresses and IP addresses both identify a network device but in different ways. Some of the main differences between a MAC address and an IP address include the following:

- Local identification vs. global identification.
- Layer 2 vs. Layer 3 operation.

- Physical address vs. logical address.
- Number of bits.
- Address assignment and permanence.
- Address formatting.

A MAC address is responsible for local identification and an IP address for global identification. For example, the MAC address is only significant on the LAN to which a device is connected. It is not used or retained in the data stream once packets leave that network. This is the primary difference between a MAC address and IP address, affecting how the addresses differ in their number of bits, address assignment and interactions.

Another difference between a MAC address and IP address is the way the addresses are assigned. Manufacturers assign a unique MAC address to each device, and these addresses are typically regarded as permanent. But it is possible to alter or spoof a MAC address with command-line tools and software settings. An IP address is bound to a network device via software configurations. Network administrators can manually change the address at any time or use Dynamic Host Protocol Configuration (DHCP) to change it dynamically.

What is a MAC address?

Media access control refers to the piece of hardware that controls how data is pushed out onto a network. A MAC device operates on Layer 2 -- the data link layer -- of the OSI model for networking. Each

device has a MAC address that acts as a unique identifier for the network interface card (NIC) installed on the device. This address operates at Layer 2, letting devices talk to each other within the same broadcast domain.

A MAC address consists of 12 hexadecimal digits, usually grouped into six pairs separated by hyphens. MAC addresses are available from 00-00-00-00-00-00 through FF-FF-FF-FF-FF-FF. The first half of the number is typically used as a manufacturer ID, while the second half is a device identifier. In nearly all enterprise network devices today, this number is hardcoded into the device during the manufacturing process.

The number of device-identifying bits is limited, however, so manufacturers do reuse them. Each manufacturer has about 1.68 million available addresses, so when it burns a device with a MAC address ending in FF-FF-FF, it starts again at 00-00-00. This approach assumes it is highly unlikely two devices with the same address will end up in the same local network segment.

No two devices on a local network should ever have the same MAC address. If that does happen, both devices have communication problems because the local network gets confused about which device should receive the packet. When a switch broadcasts a packet to all ports to find the intended recipient, the device that responds first receives the packet stream. If the device reboots, is taken away or shuts down, the other node then receives the packets.

What is an IP address?

Internet Protocol controls how devices on the internet communicate and defines the behavior of internet routers. It corresponds to Layer 3, the network layer, of the OSI reference model. The internet was initially built around IPv4 and is in transition to IPv6.

An IP address identifies a device on the global internet, acting as the device's logical address to identify its network connection. Typically, an ISP assigns the IP address to a customer's device. Network administrators use DHCP to assign and manage IP addresses within the local network.

An IPv4 address consists of 32 bits, usually written as four octets using decimal numbers, separated by periods. This format is also known as a dotted quad. Possible values range from 000.000.000.000 through 255.255.255.255, although many possible addresses are disallowed or reserved for specific purposes. One example is 192.0.2.127.

Types of Network Cables: An ethernet cable allows the user to connect their devices such as computers, mobile phones, routers, etc, to a Local Area Network (LAN) that will allow a user to have internet access, and able to communicate with each other through a wired connection. It also carries broadband signals between devices connected through it. In this article, we are going to discuss different types of ethernet cable used in local area networks for reliable internet connection.

Types of Ethernet Cables:

- Coaxial Cables
- Twisted Pair Cables
- Fiber optic Cables

Coaxial Cables:

A coaxial cable is used to carry high-frequency electrical signals with low losses. It has a copper conductor in the middle that is surrounded by a dielectric insulator. The dielectric insulator is surrounded by a plaited conducting metallic shield which reduces Electromagnetic Interference of the metal and outside interference and finally, the metallic shield is covered by a plastic covering called a sheath usually made of PVC or some other fire-resistant plastic material. Its maximum transmission speed is 10 Mbps. It is usually used in telephone systems, cable TV, etc.

Twisted Pair Cables:

A twisted pair is a copper wire cable in which two insulated copper wires are twisted around each other to reduce interference or crosstalk. It uses 10BASE-T, 100BASE-T, and some other newer ethernet variants. It uses RJ-45 connectors.

- **Shielded Twisted Pair (STP) Cable:** In STP the wires are covered by a copper braid covering or a foil shield, this foil shield adds a layer that protects it against interference leaking into and out of the cable. Hence, they are used for longer distances and higher transmission rates.
- **Unshielded Twisted Pair (UTP) Cable:** Unshielded twisted pair cable is one of the most used cables in computer

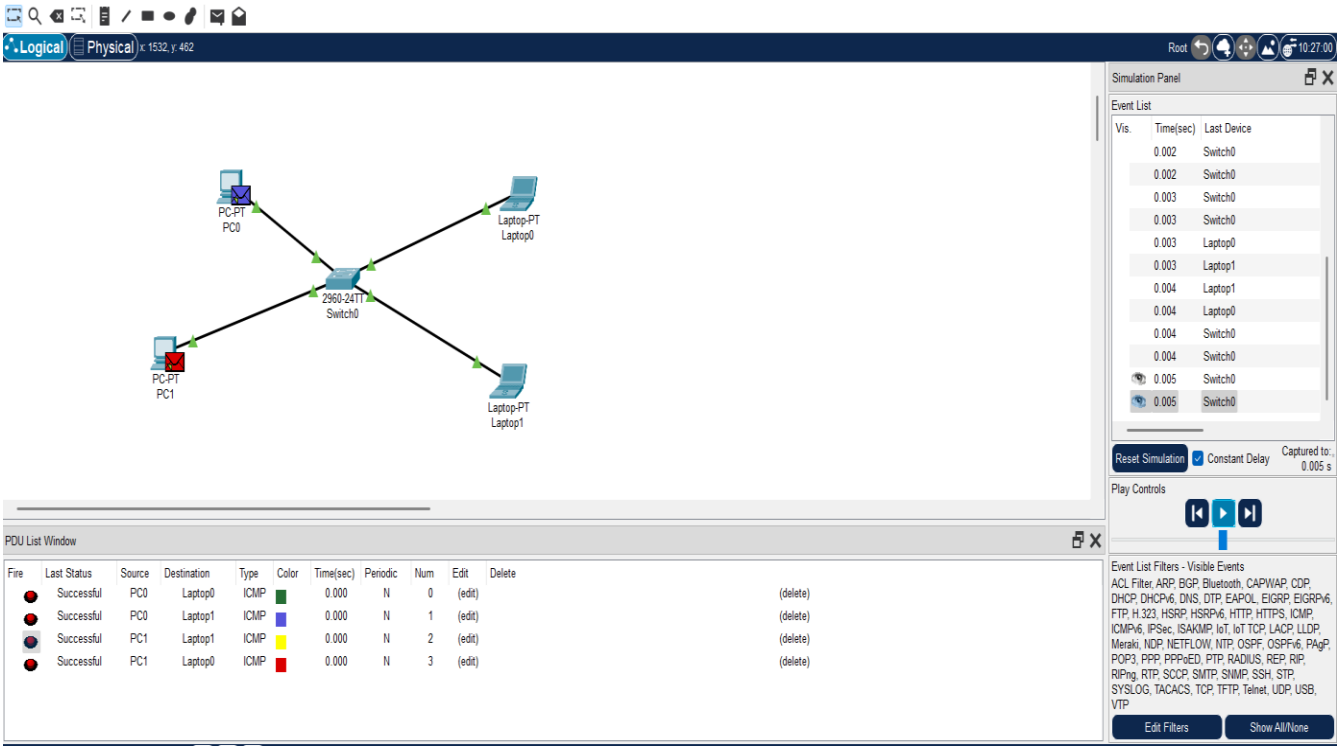
networks at present time. UTP consists of two insulated copper wires twisted around one another, the twisting of wires helps in controlling interference.

Fiber Optic Cables:

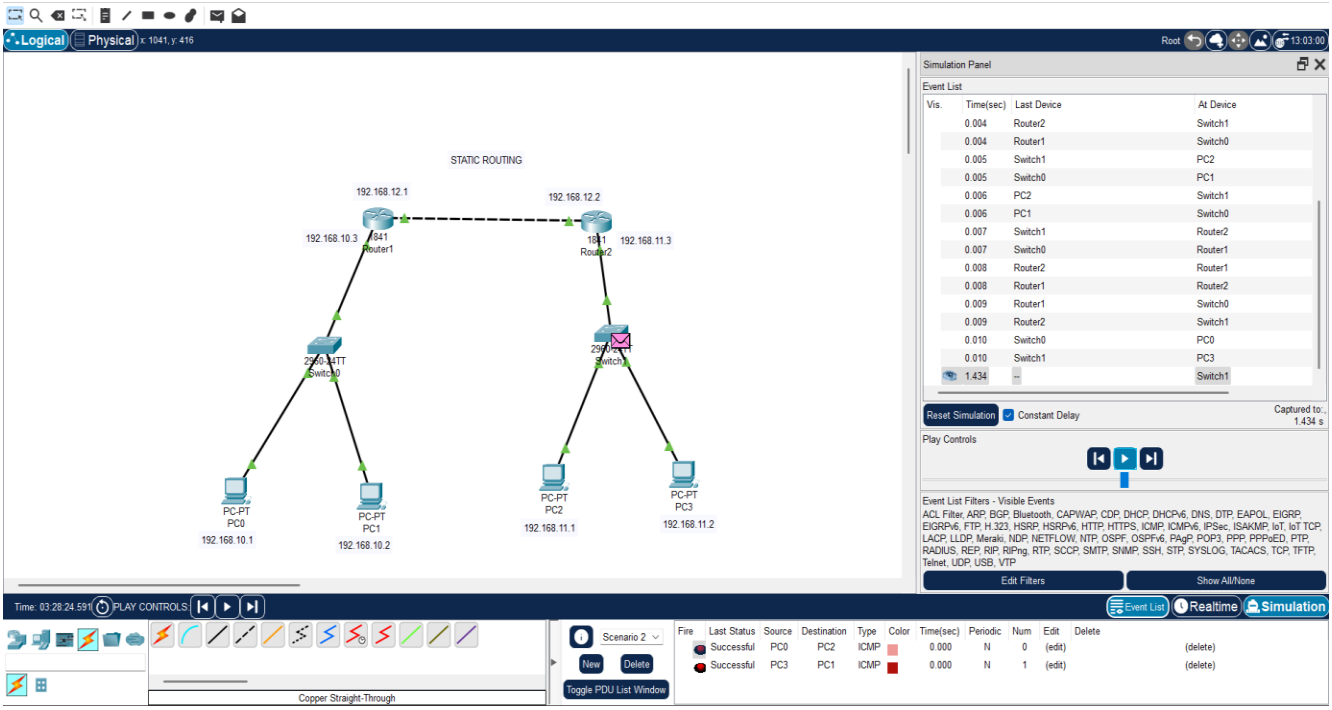
Fiber optic cables use optical fibers which are made of glass cores surrounded by several layers of covering material generally made of PVC or Teflon. It transmits data in the form of light signals due to which there are no interference issues in fiber optics. Fiber optics can transmit signals over a very long distance as compared to twisted pairs or coaxial cables. It uses 10BaseF, 100BaseFX, 100BaseBX, 100BaseSX, 1000BaseFx, 1000BaseSX, and 1000BaseBx ethernet variants. Hence, it can carry information at a great speed.

Creating a small network using LAN:

Creating a LAN using Switch:



Creating a LAN using the Switches and Routers with their appropriate cables:



Divyanshu Majhi