TRAINING DAY 13 REPORT

Understand Computer Networking

Today, I learned some important concepts

Network Protocol

A **network protocol** is a set of rules and conventions that define how data is transmitted and communicated between devices on a network. It ensures that devices from computers and smartphones to routers and servers can understand each other and work together effectively, regardless of their internal design or manufacturer.

How Network Protocol Work

Network protocols work by providing a **structured way for devices to communicate** over a network, following specific rules to ensure data is properly **sent, received, and understood**.

Types of Network Protocol

1. TCP (Transmission Control Protocol)

- **Purpose:** Reliable, connection-based communication.
- **Use Case:** Web browsing, email, file transfer (where accuracy matters).
- **Key Feature:** Guarantees delivery, order, and error checking.

2. IP (Internet Protocol)

- **Purpose:** Handles addressing and routing of packets across networks.
- **Use Case:** Works with TCP/UDP to deliver data to the right device.
- **Key Feature:** Uses IP addresses to send packets to the correct destination.

3. UDP (User Datagram Protocol)

- **Purpose:** Fast, connectionless communication.
- **Use Case:** Video streaming, online gaming, voice calls (where speed > accuracy).
- **Key Feature:** No guarantee of delivery or order.

4. SMTP (Simple Mail Transfer Protocol)

- **Purpose:** Sends **outgoing email** from a client to a server or between servers.
- **Use Case:** Sending an email (used by Gmail, Outlook, etc.).
- **Key Feature:** Works with TCP to ensure email is sent reliably.

5. IMAP (Internet Message Access Protocol)

- **Purpose:** Accesses and manages **emails on a server**.
- **Use Case:** Reading your email on multiple devices.
- **Key Feature:** Keeps email on the server — syncs across devices.

6. HTTP (Hyper Text Transfer Protocol)

- **Purpose:** Transfers web content (HTML, images, etc.).
- **Use Case:** Loading websites in browsers.
- **Key Feature:** Stateless, but fast; usually used with TCP.

HTTPS is the secure version (uses encryption via SSL/TLS).

7. FTP (File Transfer Protocol)

- **Purpose:** Transfers files between computers over a network.
- **Use Case:** Uploading/downloading files from a web server.
- **Key Feature:** Can use usernames/passwords, or be anonymous.

Network Topology

Network topology refers to the **physical or logical layout** of a network — that is, **how devices (nodes) like computers, switches, and routers are connected** and how data flows between them.

Two Main Types:

1. **Physical Topology** – How devices are **physically connected** (e.g., cables, hardware).
2. **Logical Topology** – How data **logically moves** through the network, regardless of physical layout.

Common Types of Network Topologies:

1. Bus Topology

- **Structure**: All devices share a single backbone cable.
- **Pros**: Easy to set up, low cost.
- **Cons**: If the main cable fails, the whole network goes down. Data collisions are common.
- **Use case**: Small, temporary networks.

2. Star Topology

- **Structure**: All devices connect to a central hub or switch.
- **Pros**: Easy to manage; if one cable fails, others aren't affected.
- **Cons**: If the central device fails, the entire network goes down.
- **Use case**: Most home and office networks.

3. Ring Topology

- **Structure**: Devices are connected in a circle; data travels in one direction.
- **Pros**: Predictable data path.
- **Cons**: One failure can affect the entire ring unless it's a dual ring.
- **Use case**: Some fiber optic or token ring networks.

4. Mesh Topology

- **Structure**: Every device is connected to every other device.
- **Pros**: Highly reliable and fault-tolerant.
- **Cons**: Expensive and complex to set up.
- **Use case**: Military or mission-critical systems.

5. Tree Topology (Hierarchical)

- **Structure**: A combination of star and bus topologies; has a root node and branches.
- **Pros**: Scalable and easy to manage.
- **Cons**: If the root node fails, major parts of the network can be disrupted.
- **Use case**: Large enterprise networks.

6. Hybrid Topology

- **Structure**: Mix of two or more topologies.
- **Pros**: Flexible, scalable, and customizable.

- **Cons**: Can be complex and costly.
- **Use case**: Most modern networks (e.g., data centers, large businesses).

OSI Model

The **OSI model (Open Systems Interconnection model)** is a conceptual framework that standardizes how computers **communicate over a network**. It divides the network communication process into **7 layers**, each with a specific role. It helps:

- Design and troubleshoot networks
- Ensure interoperability between systems
- Understand how data moves from one device to another

Layers of OSI model

Layer 1 – Physical

- Sends raw bits over a medium (cables, air)
- Deals with voltage, light signals, radio waves
- Example: Network cables, switches, radio signals

Layer 2 – Data Link

- Packages data into frames
- Uses MAC addresses to move data between devices on the same network
- Example: Ethernet, Wi-Fi (MAC = Media Access Control)

Layer 3 – Network

- Handles logical addressing and routing
- Decides how data gets from sender to receiver
- Example: IP addressing and routing via routers

Layer 4 – Transport

- Breaks data into segments, ensures reliable delivery
- Adds port numbers
- Example: TCP (reliable), UDP (fast but unreliable)

Layer 5 – Session

- Opens, manages, and closes communication sessions
- Maintains sessions between two systems
- Example: Managing a login session on a website

Layer 6 – Presentation

- Translates, encrypts, compresses data
- Ensures data is readable by the receiving system
- Example: SSL/TLS encryption, converting data formats

Layer 7 – Application

- Closest to the user
- Provides network services to applications
- Example: Web browser using HTTP to load a website

Advantages of the OSI Model

Advantage	Description
1. Standardization	Provides a universal framework that helps vendors and developers build interoperable hardware and software.
2. Modularity	Each layer has a distinct function, making the model easier to understand, update, and troubleshoot.
3. Troubleshooting Aid	Helps network engineers isolate and fix problems by identifying which layer is failing.
4. Flexibility	Allows for new protocols and technologies to be added at any layer without changing the whole system.
5. Interoperability	Promotes communication between different systems and networks (multi-vendor compatibility).
6. Clear Layer Separation	Helps in teaching, learning, and designing networks by breaking down complex processes into manageable parts.

Disadvantages of the OSI Model

Disadvantage	Description
1. Theoretical Model	It's more conceptual than practical — not all real-world systems follow the OSI model strictly.
2. Redundancy &	Some layers (like Session and Presentation) are often

Disadvantage	Description
Complexity	unnecessary or combined in actual implementations.
3. Inefficient for Real-time Use	The strict layering can cause performance issues in systems that prioritize speed over reliability (e.g., streaming).
4. Slower Adoption	The OSI model was developed after the TCP/IP model and didn’t gain widespread practical use in real-world networks.
5. Limited Practical Protocols	Some OSI layer protocols (especially at layers 5-6) are rarely used or completely replaced by simpler TCP/IP approaches.

TCP/IP Model

The **TCP/IP model** (Transmission Control Protocol/Internet Protocol) is the **real-world foundation of the internet** and modern networking. It defines **how data is sent, addressed, transmitted, routed, and received** between devices.It's simpler and more practical than the OSI model, and it's the standard for how devices communicate over networks.

Layers of TCP/IP Model

1. Application Layer

- Where applications access network services.
- Supports protocols like:
  - **HTTP/HTTPS** – Web pages
  - **FTP** – File transfer
  - **SMTP/IMAP** – Email
  - **DNS** – Domain name resolution

2. Transport Layer

- Ensures correct data transfer between devices.
- Key protocols:
  - **TCP** – Reliable, ordered data delivery with error checking.
  - **UDP** – Faster, connectionless, no guarantees (used in streaming, gaming).

3. Internet Layer

- Handles addressing and routing.
- Key protocols:
  - **IP (Internet Protocol)** – Assigns IP addresses, routes packets.
  - **ICMP** – Diagnostic tools (e.g., ping).
  - **ARP** – Resolves IP to MAC addresses (used in LANs).

4. Network Access Layer

- Responsible for how data is physically sent over cables, Wi-Fi, etc.
- Includes:
  - **Ethernet**
  - **Wi-Fi (802.11)**
  - **MAC addressing**
  - **Device drivers and physical media**

Difference between TCP/IP vs OSI Model

Feature	TCP/IP Model	OSI Model
Layers	4	7
Use in real networks	Widely used	Mostly theoretical
Developed by	DoD (U.S.)	ISO
Structure	Simpler	More detailed

MAC Address

A **MAC address** (**Media Access Control address**) is a **unique hardware identifier** assigned to a **network interface card (NIC)**. It's used to identify devices on a **local network (LAN)**.

Data Link Layer

The **Data Link Layer** is **Layer 2** of the **OSI model**, sitting just above the Physical Layer. Its main job is to **ensure reliable data transfer between two directly connected devices** on the same local network.

Key Responsibilities of the Data Link Layer

Framing	Breaks raw bits into **data frames** for easier transmission and error handling.

Framing	Breaks raw bits into **data frames** for easier transmission and error handling.
MAC Addressing	Uses **MAC addresses** to identify source and destination devices.
Error Detection	Detects (and sometimes corrects) errors that occur in the Physical Layer.
Flow Control	Manages the pace of data transfer to prevent buffer overflow.
Access Control	Controls which device can send data on a shared medium (like Wi-Fi).

IP Address

An **IP address** (**Internet Protocol address**) is a **unique identifier** assigned to every device connected to a **network**. It allows devices to **find and communicate** with each other on the internet or a local network.

Static vs Dynamic IP

Type	Description
Static IP	Manually set; stays the same every time
Dynamic IP	Automatically assigned by a DHCP server; can change

Public vs Private IP

Type	Description	Example Ranges
Public IP	Used on the internet, globally unique	Assigned by ISPs
Private IP	Used within private networks (LANs)	192.168.x.x, 10.x.x.x, 172.16.x.x

IPv4 (Internet Protocol version 4)

- Most common format
- **32-bit address**, shown as 4 numbers (0–255), separated by dots
- Example: 192.168.1.1

IPv6 (Internet Protocol version 6)

- Newer format, developed due to IPv4 address exhaustion
- **128-bit address**, shown in hexadecimal, separated by colons

- Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Classful IP Addressing

Classful IP addressing is an older method of dividing the IPv4 address space into fixed classes (A, B, C, D, E) based on the first few bits of the IP address. It was used to allocate IP addresses to networks before the introduction of CIDR (Classless Inter-Domain Routing).

IPv4 Address Structure

An IPv4 address is 32 bits, split into:

- **Network portion**: identifies the network
- **Host portion**: identifies the specific device (host) within the network

Classful addressing defines how many bits are used for network vs host based on the class.