UNIT - 1 | Network Overview

What is a computer network? A system connecting devices to share resources (data, hardware, software).

Benefits:

- Resource sharing: Files, printers, applications.
- Communication: Email, instant messaging, video conferencing.
- Collaboration: Shared workspaces, project management tools.
- Centralized management: Easier administration of software and security.

Evolution of Computer Networks

Early days (1950s-1960s):

- Mainframes: Large, centralized computers with limited user access.
- Terminals: Dumb devices used to interact with mainframes.

ARPANET (1960s): First packet-switching network, foundation of the internet.

- Packets: Data broken into smaller units for efficient transfer.

Client-server model (1970s-1980s): Separation of tasks.

- Clients: Request resources from servers.
- Servers: Provide resources and manage network access.

Local Area Networks (LANs) become widespread in businesses (1980s onwards).

- Ethernet: Dominant LAN technology for wired connections.
- Wi-Fi: Enables wireless LAN connectivity.

Internet explosion (1990s onwards): Global network connecting billions of devices.

- World Wide Web (WWW): Hypertext-based information system.

Network Architecture

Network architecture is essentially the blueprint for your computer network. It defines how all the devices and services are structured to work together.

1. **Physical Design:** This includes how devices are connected physically (cables, wireless) and the overall layout of the network (star, mesh, etc.).
2. **Logical Design:** This refers to the rules and protocols that govern how data flows through the network, including addressing schemes and security measures.

Some Network Architecture:

Layered approach: Open Systems Interconnection (OSI) model (7 layers).

- Each layer performs specific functions and communicates with its peer layer on other devices.

TCP/IP model: Dominant protocol suite used on the internet (subset of OSI model).

Configuring Network

- **Assigning IP addresses:** Unique identifier for each device (IPv4, IPv6).
- **Subnetting:** Dividing a network into smaller logical segments (subnets) for efficient routing.
- Configuring network devices:
    - **Routers:** Connect different networks and forward packets based on IP addresses.
    - **Switches:** Connect devices within a network and learn MAC addresses for efficient communication.
    - **Firewalls:** Security devices that filter incoming and outgoing traffic.
- **Security protocols:** Protecting data and access (encryption, authentication, authorization).

Network Strategies

- **Network design:** Defining network layout, topology, components based on needs (scalability, security, performance).
- **Scalability:** Ability to grow and adapt to changing needs (adding users, devices, applications).
- **Performance optimization:** Techniques to ensure efficient data transfer and low latency (bandwidth management, traffic shaping).
- **Security:** Protecting network from unauthorized access and threats (intrusion detection, vulnerability management).

Network Types

By Geographical Scope:

- **Local Area Network (LAN):** Covers a small area (building, office). High speed, low latency, private ownership.
- **Metropolitan Area Network (MAN):** Covers a city or town. Connects multiple LANs, moderate speed. May be private (company) or public (city network).
- **Wide Area Network (WAN):** Covers a large geographical area (country, globe). Long distances, lower speed, higher cost.

By Function:

- **Personal Area Network (PAN):** Connects personal devices (phones, wearables) within a short range (Bluetooth).
- **Storage Area Network (SAN):** High-speed network dedicated for storage devices (fibre channel).
- **Virtual Private Network (VPN):** Secure tunnel over a public network (internet) to connect remote users or sites.

Subtopics of Specific Network Types

LAN Technologies:

- **Ethernet:** Most common LAN technology, uses cables (Cat5, Cat6) for wired connections.
- **Wi-Fi:** Enables wireless LAN connectivity using radio waves (IEEE 802.11 standards - a/b/g/n/ac).

WAN Technologies:

- **Leased lines:** Dedicated, high-bandwidth connections between locations.
- **Public switched networks:** Shared infrastructure provided by service providers (e.g., PSTN).
- **Satellite networks:** Data transmission via satellites for remote locations.

- **Cellular networks:** Mobile data access using

Line Configuration

- **Point-to-point:** Direct connection between two devices using a cable (e.g., dedicated line).
- **Multipoint:** One device connects to multiple devices (e.g., star topology using switch).

Network Topology

Physical or logical layout of a network:

- **Star:** Central device (switch) connects all devices. Offers good scalability and fault tolerance (failure of one device doesn't affect others).
- **Bus:** All devices are connected to a single cable. Simple and inexpensive, but failure of one device or cable can disrupt entire network.
- **Mesh:** Devices connect to each other, creating multiple pathways for data transmission. Offers high redundancy but can be complex to manage.
- **Ring:** Devices are connected in a closed loop, data travels in one direction. Offers good security but can be slow and a single device failure can disrupt the entire network.

Transmission Mode

How data travels on the network:

- **Unicast:** One-to-one communication (sending a file to a specific device).
- **Broadcast:** One-to-many communication (sending a message to all devices on the network).
- **Multicast:** One-to-many communication for a specific group of devices (e.g., sending a video conference stream to participants).

Key Components of Network

Network devices:

- **Routers:** Connect different networks and forward packets based on IP addresses.
- **Switches:** Connect devices within a network and learn MAC addresses for efficient communication.
- **Firewalls:** Security devices that filter incoming and outgoing traffic.
- **Modems:** Modulate and demodulate signals for data transmission over different mediums (phone lines, cable).

Cables: Physical connections between devices:

- **Copper:** Traditional twisted-pair cables (Ethernet) for data transmission.
- **Fiber optic:** Uses light pulses for high-speed, long-distance data transmission.

Network protocols: Set of rules for communication:

- **TCP/IP:** Dominant protocol suite used on the internet.
    - **TCP (Transmission Control Protocol):** Guarantees reliable data delivery by breaking data into packets, acknowledging receipt, and retransmitting lost packets.
    - **IP (Internet Protocol):** Addresses packets for routing across the network.

Differentiating Between Networks

- **LAN vs. MAN vs. WAN:**
    - Geographical scope is the key differentiator.
    - LAN: Smallest (building), highest speed, private ownership.
    - MAN: Medium size (city), moderate speed, can be private or public.
    - WAN: Largest size (country/globe), lowest speed, highest cost.
- **LAN vs. Internet:**
    - Scope: LAN - private, Internet - public.
    - Control: LAN - owned by an organization, Internet - global network of interconnected networks.
    - Security: LAN - typically more secure, Internet - inherently more vulnerable.
- **Internet:** Global network of interconnected networks, uses TCP/IP protocol for communication. Offers services like email, web browsing, file transfer, and more.

UNIT - 2 | OSI Model

A conceptual framework for network communication divided into 7 layers:

1. Physical Layer: Deals with the physical transmission of data (cables, connectors, voltage levels, bit encoding)

2. Data Link Layer: Handles error-free transmission between devices on a network:

- **Framing:** Divides data into manageable units (frames) with headers containing addressing and control information, and trailers for error detection.
- **Error detection** and correction (as mentioned above).
- **Flow control:** Regulates data flow to prevent overwhelming the receiver (e.g., stop-and-wait, sliding window).
- **Media Access Control** (MAC) sublayer (discussed separately).

3. Network Layer: Routes data packets across networks:

- **Logical addressing:** Assigns unique logical addresses (IP addresses) to devices.
- **Routing protocols:** Determine the best path for data packets to reach their destination.

4. Transport Layer: Provides reliable data transfer between applications:

- **Port numbers:** Identify specific applications on a device.
- Connection establishment, termination, and flow control.
- Error detection and correction (ensures reliable delivery).

5. Session Layer: Establishes, manages, and terminates sessions between applications.

6. Presentation Layer: Deals with data format and encryption:

- Data compression and decompression.
- Encryption and decryption.

7. Application Layer: Provides network services to applications (e.g., web browsing, email, file transfer)

Signals and Transmission Media

Bandwidth-limited signals: Information signals with a limited frequency range, affecting the amount of data they can carry.

Transmission media: Physical paths for carrying data signals, each with its own characteristics:

- Wired:
  - **Coaxial cable:** Offers high bandwidth and good noise resistance (used for cable TV).
  - **Twisted-pair cable:** Most common type, affordable and easy to install, but susceptible to interference (categories like Cat5e for Ethernet).
  - **Fiber optic cable:** Uses light pulses for high-speed, long-distance transmission with minimal interference.
- Wireless:
  - **Radio waves:** Used for cellular networks, Wi-Fi, Bluetooth, with varying ranges and susceptibility to interference.
  - **Microwaves:** Used for long-distance, high-bandwidth applications like satellite communication.
  - **Infrared:** Used for short-range applications like remote controls due to limited range and line-of-sight requirement.

Modulation

Process of converting digital data (0s and 1s) into a signal suitable for transmission over a physical medium:

- **Amplitude Modulation (AM):** Varies the amplitude (strength) of a carrier signal to represent data bits.
  - Double-sideband modulation (DSB) - Less efficient, wastes bandwidth.
  - Single-sideband modulation (SSB) - More efficient, utilizes less bandwidth.
- **Frequency Modulation (FM):** Varies the frequency of a carrier signal to represent data bits.
  - Wideband FM (WBFM) - Used for radio broadcasting, high fidelity but requires more bandwidth.
  - Narrowband FM (NBFM) - Used for voice communication, more efficient bandwidth usage.

Data Link Protocols

As mentioned earlier, data link protocols govern data exchange between network devices. Here are some key protocols and their subtopics:

Ethernet: Most common LAN protocol using Carrier Sense Multiple Access with Collision Detection (CSMA/CD) for MAC.

- Frame format: Defines the structure of Ethernet frames with headers (source and destination MAC addresses, frame type) and data payload.
- CSMA/CD: Ensures orderly data transmission by listening for collisions and retransmitting if necessary.

Point-to-Point Protocol (PPP): Used for dial-up and leased line connections.

- Encapsulation: Adds header information to data packets for transmission.
- Error detection and correction (uses techniques like CRC).

Medium Access Sublayer (MAC)

A sublayer of the data link layer with functionalities:

- **Carrier access control (MAC protocols):** Techniques to prevent collisions when multiple devices share a single medium:
    - CSMA/CD (mentioned in Ethernet)
    - Token Ring: Passes a special token sequentially between devices, allowing only the token holder to transmit.
    - Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA): Devices avoid collisions by sending request-to-send (RTS) and clear-to-send (CTS) signals before transmitting.

Channel Allocation Problem

The challenge of efficiently assigning channels or bandwidth to multiple users in a shared medium:

- **Static allocation:** Pre-assigning fixed channels to users.
    - Advantages: Simple to implement, predictable performance.
    - Disadvantages: Inefficient if traffic patterns change dynamically, can lead to wasted bandwidth.
- **Dynamic allocation:** Assigning channels on-demand based on user needs:
    - Advantages: More efficient utilization of bandwidth, accommodates changing traffic patterns.
    - Disadvantages: Requires more complex algorithms and management overhead.

Dynamic allocation techniques:

- **Frequency Hopping Spread Spectrum (FHSS):** Rapidly switches carrier frequencies to avoid interference. (Used in Bluetooth)
- **Direct Sequence Spread Spectrum (DSSS):** Spreads the data signal over a wider bandwidth to make it less susceptible to interference. (Used in Wi-Fi)
- **Code Division Multiple Access (CDMA):** Assigns unique codes to users, allowing them to share the same frequency channel without interference. (Used in cellular networks)

UNIT - 3 | IEEE Standard

Family of IEEE standards for Local Area Networks (LANs) and Metropolitan Area Networks.

Managed by the IEEE 802 LAN/MAN Standards Committee (LMSC)

IEEE 802.3 - Ethernet:

- Defines different speeds (10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps, etc.)
- Covers various media types (coaxial cable, twisted pair, fiber optic)
- Subcategories: 802.3u (Fast Ethernet), 802.3ab (Gigabit Ethernet)

IEEE 802.11 - Wireless LAN (Wi-Fi):

- Defines different frequency bands (2.4 GHz, 5 GHz) and protocols (802.11a, b, g, n, ac, ax)
- Focuses on security mechanisms (WEP, WPA, WPA2)

Network Devices

Switches: Layer 2 devices that learn MAC addresses and forward data frames to specific ports

- Managed vs. Unmanaged Switches: Managed switches offer more configuration options.
- Learning Switches: Learn and maintain a MAC address table to improve forwarding efficiency.

Bridges: Layer 2 devices that connect LAN segments, filtering traffic based on MAC addresses

- Transparent Bridges: Operate invisibly to the network, learning and forwarding traffic.
- Source Routing Bridges: Use source MAC addresses to determine forwarding paths.

Routers

- Layer 3 devices that connect networks and forward packets based on IP addresses

Subtopics:

- **Routing Protocols (e.g., RIP, OSPF, BGP):**
  - **Distance Vector Routing (RIP):** Uses hop count to determine best path, simple but can be inefficient for large networks.
  - **Link-State Routing (OSPF):** Routers share information about entire network topology, leading to more efficient routing.
  - **Border Gateway Protocol (BGP)**: Used for routing between different autonomous systems (AS) on the internet.
- **Routing Tables:** Maintain information about known networks and next hops for packet forwarding.

Layer Routing Algorithms

- Algorithms used by routers to determine the best path for forwarding packets across networks (already covered in Routers above)

Congestion Control Algorithms

Techniques used to prevent overloading networks and maintain efficient data flow

Subtopics:

- **Stop-and-Wait:** Sender transmits a packet and waits for an acknowledgment (ACK) before sending the next. Simple but inefficient for high latency networks.
- **Go-Back-N:** Sender transmits a window of packets and waits for ACKs. If a timeout occurs, all packets in the window are retransmitted. Less efficient than windowing.
- **Windowing (e.g., TCP):** Sender transmits a window of packets and monitors ACKs. Sender can adjust window size based on network conditions.

OSI Model Layers (Focus on highlighted layers)

Transport Layer (Layer 4): Provides reliable data transfer between applications

- Port numbers: Identify specific applications on a host. (e.g., Port 80 for HTTP)
- TCP (Transmission Control Protocol): Provides reliable, in-order delivery with error checking and congestion control.
- UDP (User Datagram Protocol): Offers connectionless, best-effort delivery suitable for real-time applications (e.g., video streaming).

Session Layer (Layer 5): Establishes, manages, and terminates sessions between applications

- Session establishment, negotiation, and termination.
- Dialog control (allowing half-duplex or full-duplex communication).

Presentation Layer (Layer 6): Handles data format conversion (encryption/decryption)

- Data compression and decompression.
- Encryption and decryption for secure data transmission.

Application Layer (Layer 7): Provides network services to applications (e.g., HTTP, FTP)

- Provides a variety of network protocols for different applications (e.g., HTTP for web browsing, FTP for file transfer).
- User interaction with network services.

UNIT - 4 | TCP/IP

A layered model for network communication (typically 4 layers, some consider 5)

Layers (Top-Down):

1. Application Layer: Provides services to applications for user interaction (protocols like):

- **HTTP (Hypertext Transfer Protocol):** Transfers web pages
- **FTP (File Transfer Protocol):** Transfers files between computers (has modes like binary, ASCII)
- **Telnet:** Remote terminal access (text-based)
- **SMTP (Simple Mail Transfer Protocol):** Sends email messages
- **POP3 (Post Office Protocol 3):** Retrieves email messages

2. Transport Layer: Ensures reliable data transfer:

- **TCP (Transmission Control Protocol):** Reliable, sequenced delivery (used for web browsing, file transfer)
- **UDP (User Datagram Protocol):** Fast, connectionless delivery (used for streaming media, VOIP)

3. Network Layer: Routes data packets across networks:

- **IP (Internet Protocol):** Assigns IP addresses for identification and routing
- **ICMP (Internet Control Message Protocol):** Error reporting and diagnostics (e.g., ping)

4. (Optional) Data Link Layer: Handles physical transmission on the network media (often combined with Physical layer):

- **MAC Addressing:** Assigns unique addresses to devices on the network
- **Error Detection and Correction:** Ensures data integrity during transmission

5. Physical Layer: Transmits raw data bits over a physical medium (cables, wireless):

- **Media Types:** Coaxial cables, twisted-pair cables, fiber optic cables, radio waves

TCP/IP vs OSI Model

OSI Model: A reference model with 7 layers for theoretical understanding

Key Differences:

- TCP/IP combines Session & Presentation layers into Application layer (focuses on practicality)
- TCP/IP is a working model used in the internet, OSI is a conceptual framework

Mobile Communication Network Model (Cellular Network)

- Uses base stations and cell towers for communication between mobile devices

Generations (G): Evolution of cellular network technology:

- **1G:** Analog voice communication (limited data)
- **2G:** Introduction of digital voice and SMS
- **3G:** Enabled internet access and faster data speeds
- **4G:** Increased data speeds and improved mobile broadband
- **5G:** Ultra-fast data speeds, low latency for new applications (still under development)

Sub-topics:

- **Mobile Switching Center (MSC):** Central office that routes calls between mobile devices and landlines
- **Base Transceiver Station (BTS):** Handles communication with mobile phones within a specific cell
- **Mobile Station (MS):** The mobile phone itself, communicates with the nearest BTS
- **Handoff:** Process of transferring a call from one BTS to another as the mobile user moves

Wi-Fi Network

- Wireless network using radio waves (IEEE 802.11 standards - like a/b/g/n/ac)
- Provides internet access to devices within range of a router or access point
- **Security Protocols:** WPA, WPA2 (protects Wi-Fi networks with encryption)

Network Topologies: Different ways Wi-Fi devices are arranged (e.g., Star, Mesh)

Wireless Access Point (WAP): Connects wired network to Wi-Fi devices

Wi-Fi Direct: Allows devices to connect directly without a router (useful for file sharing)

Bluetooth

- Short-range wireless technology for connecting devices (up to 10 meters)
- Used for data transfer (e.g., files, audio) and device communication (e.g., headphones, speakers)
- **Bluetooth versions:** Different versions offer varying speeds and features

Bluetooth Profiles: Define how devices communicate for specific purposes (e.g., HFP - hands-free calling, A2DP - stereo audio)

Bluetooth Low Energy (BLE): Lower power consumption for wearable devices and Internet of Things (IoT)

Broadband & Baseline Connections

Broadband: High-speed internet connection with fast data transfer rates (greater than 25 Mbps). How data travels in broadband connections:

- **Cable Internet:** Uses existing cable TV infrastructure
- **DSL (Digital Subscriber Line):** Uses existing telephone lines
- **Fiber Optic Internet:** Uses fiber optic cables for high-speed data transmission
    - **Examples:** Cable internet, DSL internet, Fiber optic internet

Baseline: Lower-speed internet connection with slower data transfer rates (less than 25 Mbps)

Example: Dial-up internet (uses phone lines)

Focus on Key Differences

Speed: Broadband offers significantly faster data transfer rates compared to baseline connections. (e.g., Broadband: > 25 Mbps, Baseline: < 25 Mbps)

Technology:

- **Broadband:** Utilizes advanced technologies like cable, DSL, or fiber optics.
- **Baseline:** Relies on older technologies like dial-up which uses phone lines.

Applications:

- **Broadband:** Supports demanding applications like streaming video, online gaming, and large file transfers.
- **Baseline:** Limited to basic tasks like email and web browsing (may experience delays).

Factors Affecting Connection Speed

- **Bandwidth:** Maximum amount of data transferable in a given time
- **Latency:** Delay in data transmission

Additional Network Concepts (for reference):

- **Domain Name System (DNS):** Translates domain names (like [invalid URL removed]) to IP addresses (numerical identifiers) for easier user access
- **Dynamic Host Configuration Protocol (DHCP):** Assigns IP addresses to devices automatically on a network
- **Simple Network Management Protocol (SNMP):** Manages and monitors network devices for troubleshooting