RAAJDHANI ENGINEERING COLLEGE, BHUBANESWAR

LECTURE NOTE

Syllabus

Th.3b. COMPUTER NETWORKS

(3rd Sem),Diploma

Faculty Name-Sunita Dalei

Introduction:

- Introduction to computer networks
- Network Models
- OSI Reference Model, The layer architecture
- TCP/IP Model
- 4LayerofTCP/IP suite

Introduction to computer networks:

A **computer network** is a system of interconnected devices (such as computers, servers, printers, and other hardware) that communicate with each other to share resources, data, and services. The goal of a computer network is to enable devices to exchange information, whether for work, entertainment, or communication.

Key Concepts in Computer Networks:

- **Network Components**:
  - **Nodes**: Devices connected to the network, such as computers, routers, and printers.
  - **Links**: The physical or logical connections that allow communication between devices, such as cables or wireless signals.
  - **Switches/Routers**: These devices help direct the traffic in a network by determining the best path for data to travel.
- **Types of Networks**:
  - **LAN (Local Area Network)**: A network that covers a small geographical area like a home, office, or campus.
  - **WAN (Wide Area Network)**: A network that covers a large geographical area, like a country or even globally (e.g., the internet).
  - **MAN (Metropolitan Area Network)**: A network that covers a city or large campus area.
  - **PAN (Personal Area Network)**: A small-scale network typically for personal devices (e.g., connecting smartphones, laptops).
- **Communication Protocols**:
  - **TCP/IP (Transmission Control Protocol/Internet Protocol)**: The fundamental suite of protocols used for communication over the internet. It ensures reliable, error-free data transmission.
  - **HTTP (Hypertext Transfer Protocol)**: A protocol used to transfer web pages.
  - **FTP (File Transfer Protocol)**: A protocol for transferring files between computers.
  - **DNS (Domain Name System)**: A system that translates human-readable domain names (e.g., www.example.com) into IP addresses.
  - **SMTP (Simple Mail Transfer Protocol)**: A protocol used for sending emails.

- **Data Transmission**:
    - **Analog vs. Digital**: Analog signals are continuous, while digital signals are discrete and are typically used in modern computer networks.
    - **Bandwidth**: The amount of data that can be transferred over a network in a given period.
    - **Latency**: The delay before data transfer begins or is received. Lower latency improves the performance of applications like video calls or online gaming.

- **Topologies**:
    - **Bus**: All devices are connected to a single central cable.
    - **Star**: Devices are connected to a central hub or switch.
    - **Ring**: Devices are connected in a circular fashion.
    - **Mesh**: Every device is connected to every other device.

- **Types of Network Access**:
    - **Wired Networks**: Use cables to connect devices. Examples include Ethernet connections.
    - **Wireless Networks**: Use radio waves for communication. Examples include Wi-Fi, Bluetooth, and cellular networks.

- **Security in Networks**:
    - **Encryption**: The process of encoding data to protect it from unauthorized access.
    - **Firewalls**: Devices or software that monitor and control incoming and outgoing network traffic based on predetermined security rules.
    - **VPN (Virtual Private Network)**: A secure connection between two networks over the internet.

- **Internet**:
    - The **internet** is the largest WAN in the world, connecting millions of smaller networks globally. It uses a variety of protocols (most notably TCP/IP) and facilitates communication and resource sharing on a global scale.

Why Are Computer Networks Important?

- **Resource Sharing**: Computers and devices can share hardware (printers, scanners) and software (applications, databases) over a network.

- **Communication**: Facilitates communication via email, instant messaging, voice and video calls, and social media.

- **Access to Information**: The internet provides global access to a vast amount of information, databases, and resources.

Network Models

Network models provide a framework for understanding how different components of a network interact with each other. They define a set of rules or guidelines for how data is transferred across networks and how different network devices communicate. The two most commonly referenced network models are the **OSI (Open Systems Interconnection) Model** and the **TCP/IP Model**.

1. OSI Reference Model

The **OSI Model** is a conceptual framework used to understand network interactions in seven distinct layers. It was developed by the International Organization for Standardization (ISO) in the 1980s to standardize network protocols and improve interoperability between systems.

The 7 Layers of the OSI Model:

1. **Layer 1: Physical Layer**
    - **Function**: Deals with the physical connection between devices, such as cables, switches, and network interface cards (NICs).
    - **Examples**: Ethernet cables, fiber optics, wireless transmission.
    - **Data Units**: Bits (0s and 1s).
2. **Layer 2: Data Link Layer**
    - **Function**: Provides reliable data transfer by error detection and correction, and organizes bits into frames for transmission.
    - **Examples**: Ethernet, Wi-Fi (IEEE 802.11), PPP (Point-to-Point Protocol).
    - **Data Units**: Frames.
3. **Layer 3: Network Layer**
    - **Function**: Responsible for routing data packets between devices across different networks and subnetworks.
    - **Examples**: IP (Internet Protocol), Routers.
    - **Data Units**: Packets.
4. **Layer 4: Transport Layer**
    - **Function**: Ensures end-to-end communication and reliability, including flow control, error correction, and data segmentation.
    - **Examples**: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).
    - **Data Units**: Segments (TCP), Datagram (UDP).
5. **Layer 5: Session Layer**
    - **Function**: Manages sessions or connections between applications. It establishes, maintains, and terminates communication sessions.
    - **Examples**: NetBIOS, RPC (Remote Procedure Call).
    - **Data Units**: Data.
6. **Layer 6: Presentation Layer**
    - **Function**: Translates, encrypts, and compresses data. It ensures that data is in a readable format for the application layer.
    - **Examples**: SSL/TLS (encryption), JPEG, GIF (compression), ASCII.
    - **Data Units**: Data.
7. **Layer 7: Application Layer**
    - **Function**: Provides network services to end-user applications. It is the closest layer to the end-user.
    - **Examples**: HTTP, FTP, SMTP, DNS, POP3.
    - **Data Units**: Data (messages).

2. TCP/IP Model

The **TCP/IP Model** (Transmission Control Protocol/Internet Protocol) is a more simplified and practical model that was developed to standardize networking protocols for the internet. It consists of 4 layers, which correspond roughly to the OSI Model but are more focused on practical implementation.

The 4 Layers of the TCP/IP Model:

1. **Layer 1: Link Layer (Network Interface Layer)**:
    - **Function**: This layer is responsible for the physical connection to the network and for managing data frames between devices on the same local network.
    - **OSI Corresponding Layers**: Physical Layer & Data Link Layer.
    - **Examples**: Ethernet, Wi-Fi, ARP (Address Resolution Protocol).
2. **Layer 2: Internet Layer**:
    - **Function**: Responsible for logical addressing and routing of packets across networks. It ensures that data packets are delivered from the source to the destination across multiple networks.
    - **OSI Corresponding Layer**: Network Layer.
    - **Examples**: IP (Internet Protocol), ICMP (Internet Control Message Protocol), Routing Protocols (RIP, OSPF).
3. **Layer 3: Transport Layer**:
    - **Function**: Ensures reliable data transmission, error handling, and flow control between systems. It is responsible for establishing connections and ensuring that the data is sent correctly.
    - **OSI Corresponding Layer**: Transport Layer.
    - **Examples**: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).
4. **Layer 4: Application Layer**:
    - **Function**: Provides network services to end-user applications, similar to the OSI's Application, Presentation, and Session layers. It allows applications to interact with the network.
    - **OSI Corresponding Layers**: Application, Presentation, and Session Layers.
    - **Examples**: HTTP, FTP, DNS, SMTP, SSH.

3. 4 Layers of the TCP/IP Suite

The **TCP/IP Model** can also be understood as having 4 specific layers that facilitate the functioning of internet protocols:

1. **Network Interface Layer (Link Layer)**:
    - **Purpose**: Responsible for physical addressing and the methods for transferring data to and from the network hardware.
    - **Protocol Examples**: Ethernet, Wi-Fi, PPP, ARP.
2. **Internet Layer**:
    - **Purpose**: Handles the addressing, routing, and delivery of data packets across multiple networks. It defines how devices on different networks communicate with each other.
    - **Protocol Examples**: IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP.
3. **Transport Layer**:
    - **Purpose**: Manages the flow of data between two endpoints and ensures that data is reliably transmitted. This layer provides error detection, error correction, and flow control.
    - **Protocol Examples**: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).
4. **Application Layer**:
    - **Purpose**: Provides various network services to applications. It defines how applications interact with the network and how data is formatted for user-level applications.
    - **Protocol Examples**: HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System).

CHAPTER – 2: Physical Layer:

Physical Layer

The **Physical Layer** is the first layer of the OSI model and is responsible for the transmission and reception of raw data bits (0s and 1s) over a physical medium. This layer defines the hardware aspects of the network and includes the transmission media, electrical signals, and network interfaces.

Transmission Media - Principles and Issues

Transmission Media refers to the physical pathways through which data is transmitted between devices. There are two primary types:

- **Guided Media (Wired)**: Signals are directed along specific paths such as cables.
- **Unguided Media (Wireless)**: Signals are broadcast through the air, without the use of physical cables.

Key **issues** that affect transmission media include:

- **Bandwidth**: The amount of data that can be transmitted over the medium per unit of time (measured in Hz or bits per second).
- **Attenuation**: Loss of signal strength over distance.
- **Interference**: Disturbances that affect the quality of the signal, such as electromagnetic interference (EMI) or radio frequency interference (RFI).
- **Latency**: Delay in signal transmission from source to destination.
- **Security**: Unauthorized access or eavesdropping on the transmitted data.
- **Cost**: Installation and maintenance expenses related to different media.

Wired Media

1. **Coaxial Cable**
    - **Structure**: Consists of a central copper conductor, an insulating layer, a metallic shield, and an outer insulating layer.
    - **Bandwidth**: Offers moderate bandwidth.
    - **Advantages**: Provides good shielding from electromagnetic interference and is resistant to noise.
    - **Usage**: Used in cable TV, broadband internet, and legacy networking systems (e.g., 10BASE2 Ethernet).
2. **Unshielded Twisted Pair (UTP) Cable**
    - **Structure**: Made of pairs of wires twisted together. No additional shielding, so it is more susceptible to interference compared to other types.

- **Categories**:
  - **Cat 5e**: Supports up to 1000 Mbps (Gigabit Ethernet).
  - **Cat 6**: Supports 10 Gbps for shorter distances.
  - **Cat 7**: Enhanced shielding for higher speeds.
- **Advantages**: Low cost, easy to install.
- **Disadvantages**: Prone to electromagnetic interference (EMI) and attenuation over long distances.
- **Usage**: Commonly used in Ethernet networks (e.g., 100BASE-T, 1000BASE-T).

3. **Shielded Twisted Pair (STP) Cable**
   - **Structure**: Similar to UTP, but with additional shielding around each pair of wires to reduce electromagnetic interference.
   - **Bandwidth**: Higher than UTP.
   - **Advantages**: Better resistance to noise and interference.
   - **Disadvantages**: More expensive and harder to install due to shielding.
   - **Usage**: Used in environments with high electromagnetic interference (e.g., industrial areas).
4. **Fiber Optic Cable**
   - **Structure**: Uses strands of glass or plastic fibers to transmit data as light signals. Consists of a core (where the light travels), a cladding (which reflects light back into the core), and a protective outer layer.
   - **Bandwidth**: Extremely high bandwidth, capable of transmitting large amounts of data over long distances with minimal attenuation and interference.
   - **Types**:
     - **Single-Mode Fiber (SMF)**: Designed for long-distance transmission, uses a single light path (mode). It can carry signals over hundreds of kilometers.
     - **Multimode Fiber (MMF)**: Designed for shorter distances, uses multiple light paths. It has higher attenuation compared to SMF.
   - **Advantages**: High speed, minimal signal degradation.
   - **Disadvantages**: Expensive, requires specialized equipment and installation.
   - **Usage**: Backbone connections, data centers, long-distance telecommunications.

Wireless Media

1. **High Frequency (HF)**
   - **Frequency Range**: 3–30 MHz.
   - **Range**: Can cover long distances, typically used for radio communications.
   - **Applications**: Amateur radio, military, and aviation communication.
2. **Very High Frequency (VHF)**
   - **Frequency Range**: 30–300 MHz.
   - **Range**: Good for medium-range communication; signals can travel 30-50 miles.
   - **Applications**: FM radio, TV broadcasts, two-way radios, and marine communications.
3. **Ultra High Frequency (UHF)**
   - **Frequency Range**: 300 MHz–3 GHz.
   - **Range**: Shorter range compared to VHF but higher capacity for data transmission.
   - **Applications**: TV broadcasts, mobile phones, satellite communications, GPS, and Wi-Fi.
4. **Microwave**
   - **Frequency Range**: 1 GHz–100 GHz.
   - **Range**: Used for high-capacity, line-of-sight communication. Can cover long distances with relay stations.
   - **Applications**: Point-to-point communication, satellite links, cellular communication.
5. **Ku Band**
   - **Frequency Range**: 12–18 GHz.
   - **Range**: Used for satellite communications, especially for television and internet services.

- **Applications**: Satellite communication systems, direct broadcast satellite (DBS) services.

6. **Wi-Fi (802.11 Standards)**
   - **Frequency Range**: Typically 2.4 GHz and 5 GHz (with newer versions supporting 6 GHz in Wi-Fi 6E).
   - **Standard Variants**:
     - **802.11a**: Operates at 5 GHz, supports speeds up to 54 Mbps.
     - **802.11b**: Operates at 2.4 GHz, supports speeds up to 11 Mbps.
     - **802.11g**: Operates at 2.4 GHz, supports speeds up to 54 Mbps.
     - **802.11n**: Operates at 2.4 GHz and 5 GHz, supports speeds up to 600 Mbps.
     - **802.11ac**: Operates at 5 GHz, supports speeds up to 1.3 Gbps.
   - **Applications**: Used in wireless local area networks (WLANs) for homes, businesses, and public areas.

Cellular Data Networks

1. **2G (Second Generation)**
   - **Technology**: Digital network for voice and limited data.
   - **Speed**: Up to 50-100 Kbps.
   - **Standard**: GSM (Global System for Mobile Communications), CDMA.
   - **Applications**: Voice calls, SMS (Short Message Service).
2. **3G (Third Generation)**
   - **Technology**: Improved digital network with higher speeds for data and voice.
   - **Speed**: 384 Kbps to several Mbps.
   - **Standard**: UMTS (Universal Mobile Telecommunications System), CDMA2000.
   - **Applications**: Internet browsing, video calls, multimedia.
3. **4G (Fourth Generation)**
   - **Technology**: IP-based broadband network for high-speed internet access.
   - **Speed**: 100 Mbps to 1 Gbps.
   - **Standard**: LTE (Long-Term Evolution), WiMAX.
   - **Applications**: HD video streaming, gaming, mobile hotspots.
4. **5G (Fifth Generation)**
   - **Technology**: Next-gen wireless network offering ultra-fast speeds, low latency, and greater device connectivity.
   - **Speed**: Up to 10 Gbps (theoretical max).
   - **Standard**: 5G NR (New Radio).
   - **Applications**: Autonomous vehicles, IoT (Internet of Things), smart cities, VR/AR (Virtual Reality/Augmented Reality), high-speed internet.

Network Topologies:

Network topology refers to the arrangement of various elements (links, nodes, devices) in a network. It defines how different network devices are connected and how data flows between them. Some common topologies are:

1. **Bus Topology**
   - **Structure**: All devices are connected to a single central cable (the "bus").
   - **Advantages**: Simple and inexpensive to implement.
   - **Disadvantages**: Difficult to troubleshoot; the entire network can go down if the bus fails.
2. **Star Topology**
   - **Structure**: All devices are connected to a central device (usually a switch or hub).
   - **Advantages**: Easy to install and manage, failure of one device doesn’t affect the rest of the network.

    - **Disadvantages**: Dependency on the central device; if the hub or switch fails, the entire network can be affected.
3. **Ring Topology**
    - **Structure**: Devices are connected in a circular fashion.
    - **Advantages**: Simple data transmission; each device gets an equal chance to send data.
    - **Disadvantages**: If one device or link fails, the entire network is affected.
4. **Mesh Topology**
    - **Structure**: Each device is connected to every other device.
    - **Advantages**: Highly reliable, fault-tolerant, and redundant paths.
    - **Disadvantages**: Expensive and complex to install due to the large number of connections.
5. **Tree Topology**
    - **Structure**: A hybrid of star and bus topologies; multiple star networks connected together.
    - **Advantages**: Scalable and flexible.
    - **Disadvantages**: More difficult to manage than simpler

CHAPTER –3: Data Link Layer:

Design Issues in the Data Link Layer (DLL) and Network Switching:

The **Data Link Layer (DLL)** is the second layer in the OSI model, directly above the Physical Layer. It plays a crucial role in providing reliable communication over a physical medium. It does this by handling error detection and correction, data framing, and flow control. The protocols and techniques used at this layer help to ensure that data is transmitted without errors and in a format that can be interpreted by the receiving device.

---

1. Data Link Layer Protocols

Ethernet

Ethernet is the most widely used Data Link Layer protocol in local area networks (LANs). It is defined in several standards, the most common being **IEEE 802.3**.

- **Frame Structure**: Ethernet uses frames to transmit data. The frame includes a destination and source MAC address, length/type field, data payload, and error-checking (CRC) field.
- **Media Access Control (MAC)**: Ethernet uses a method called **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)** to control access to the shared transmission medium.
    - **CSMA/CD** works by checking if the medium is idle. If it is, the device sends the data. If two devices send at the same time (a collision), they both stop transmitting, wait for a random backoff time, and then try again.
- **Speed**: Ethernet can operate at various speeds, such as **10 Mbps (legacy)**, **100 Mbps (Fast Ethernet)**, **1 Gbps (Gigabit Ethernet)**, **10 Gbps** and beyond.
- **Advantages**: High reliability, scalability, and low cost.
- **Disadvantages**: Limited to short distances; when multiple devices are connected to the same network, bandwidth contention and collisions can become issues, especially in traditional shared Ethernet networks.

WLAN (Wireless Local Area Network)

WLAN protocols, specifically the **IEEE 802.11** family, define how wireless communication takes place in a network. The most common WLAN protocols are **Wi-Fi**.

- **Frame Structure**: Similar to Ethernet, the WLAN frame includes destination/source MAC addresses, frame type, data payload, and a CRC for error detection.
- **Access Method**: WLANs use a variant of **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)** to avoid collisions, as wireless signals cannot detect collisions as effectively as wired ones.
    - In CSMA/CA, a station first checks if the channel is free. If it is, it sends a request to send (RTS) and waits for a clear-to-send (CTS) response from the receiving station.
- **Security**: Security protocols like **WPA2 (Wi-Fi Protected Access 2)** and **WPA3** are implemented to protect data confidentiality and prevent unauthorized access.
- **Speed**: Ranges from **802.11b** (11 Mbps) to **802.11ac** (1-3 Gbps), with the newer **802.11ax (Wi-Fi 6)** offering improved speed, range, and congestion management.
- **Advantages**: Mobility, no need for cabling, ease of setup.
- **Disadvantages**: Interference from other wireless devices, security concerns, lower range than wired networks, and potential congestion in crowded areas.

Bluetooth

Bluetooth is a short-range wireless communication protocol designed for personal area networks (PANs). It operates in the **2.4 GHz ISM (Industrial, Scientific, and Medical)** band.

- **Topology**: Bluetooth typically uses a **piconet** topology, where devices are either masters or slaves. A master device can communicate with up to seven active slave devices in a network.
- **Access Method**: Bluetooth uses a **Frequency-Hopping Spread Spectrum (FHSS)** to reduce interference. This technique involves rapidly switching the frequency over a range of 79 (or 1600 in the case of Bluetooth 5.0) different channels.
- **Security**: Bluetooth implements security through pairing, encryption, and authentication. It uses protocols such as **SSP (Secure Simple Pairing)** for secure connections.
- **Speed**: Bluetooth operates at speeds ranging from **1 Mbps (Bluetooth 1.x)** to **3 Mbps (Bluetooth 2.0)** and **24 Mbps (Bluetooth 3.0)** using high-speed channels, with **Bluetooth 5.0** offering much higher range and throughput.
- **Advantages**: Low power consumption, ideal for short-range communication, ease of use.
- **Disadvantages**: Limited range (up to 100 meters), low data transfer rates compared to Wi-Fi, interference from other devices operating on the same frequency band.

2. Switching Techniques

Switching refers to the method by which data is routed from one device to another in a network. There are various switching techniques used to handle data traffic in different types of networks.

Circuit Switching

- **Concept**: In circuit-switched networks, a dedicated communication path is established between two devices for the duration of the communication session. This path remains open and reserved, ensuring constant bandwidth.
- **Usage**: Traditionally used in telephone networks (e.g., landline phones).
- **Advantages**: Guaranteed bandwidth, no congestion.
- **Disadvantages**: Inefficient use of resources; unused capacity during idle times.

Packet Switching

- **Concept**: In packet-switched networks, data is divided into small packets that are routed independently to their destination. Each packet may take a different path, depending on network conditions.
- **Usage**: The **Internet** and most modern data networks use packet switching.
- **Advantages**: Efficient use of network resources, no need for a dedicated connection, supports multiplexing.
- **Disadvantages**: Overhead due to packet headers and reassembly; packets may arrive out of order or get lost.

Message Switching

- **Concept**: Data is sent as a whole message from the source to the destination. The entire message is stored and forwarded at each intermediate node.
- **Usage**: Rarely used in modern networks, but has applications in legacy systems like **telegraphy** and some email systems.
- **Advantages**: No need for a dedicated path.
- **Disadvantages**: High delay and storage requirements at each node, especially for large messages.

Store-and-Forward Switching

- **Concept**: A switch receives a complete data frame before forwarding it. This technique allows the switch to check for errors before transmitting the frame.
- **Usage**: Common in LAN switches.
- **Advantages**: Error detection and correction, better reliability.
- **Disadvantages**: Higher latency compared to cut-through switching.

Cut-Through Switching

- **Concept**: In cut-through switching, as soon as a switch receives the destination address, it starts forwarding the frame without waiting for the entire frame to be received.
- **Usage**: Primarily used in low-latency applications, such as gaming or high-speed data centers.
- **Advantages**: Lower latency, faster frame forwarding.
- **Disadvantages**: If a frame contains errors, it may be forwarded without checking for errors, leading to potential problems.

3. Virtual LAN (VLAN)

A **VLAN (Virtual Local Area Network)** is a logical grouping of network devices that appear to be on the same physical network, regardless of their physical location. VLANs are typically implemented in Layer 2 (Data Link Layer) switches and help organize networks more efficiently.

- **Purpose**:
  - To segment a network for improved performance, security, and management.
  - VLANs can help reduce broadcast traffic and improve traffic isolation.
  - They enable logical grouping based on functional or departmental needs, even if devices are physically scattered.
- **How it Works**: VLANs are configured on switches by tagging Ethernet frames with a VLAN ID (typically using IEEE 802.1Q tagging). This tag helps the switch determine which VLAN the frame belongs to and ensures proper forwarding.
- **Advantages**:

    - **Improved Security**: By isolating traffic between VLANs, sensitive data can be kept within certain network segments.
    - **Reduced Broadcast Traffic**: Broadcasts are limited to a VLAN, reducing network congestion.
    - **Simplified Network Management**: Easier to move devices between VLANs without changing physical connections.
    - **Cost Efficiency**: Reduces the need for additional hardware, as the network can be logically segmented instead of physically segmented.
- **Disadvantages**:
    - **Increased Complexity**: VLANs require careful management and configuration, especially with inter-VLAN routing.
    - **Performance Overhead**: The process of tagging frames and routing between VLANs can create some additional overhead.
- **Common VLAN Use Cases**:
    - **Departmental Isolation**: Isolating finance, HR, and marketing departments into separate VLANs.
    - **Guest Networks**: Creating a separate VLAN for guests to access the internet while keeping them isolated from the internal network.
    - **Security**: Segmenting sensitive data into a VLAN that only authorized personnel can access.

CHAPTER – 4: Network Layer:

Internet Protocols (IPv4 & IPv6):

Design Issues:

- **Addressing:**
    - IPv4 uses 32-bit addresses (limited to ~4.3 billion addresses).
    - IPv6 uses 128-bit addresses to solve the exhaustion issue and support future scalability.
- **Header Complexity:**
    - IPv4 headers are more complex and include fields like checksum, which increases processing overhead.
    - IPv6 simplifies the header structure, improving router performance and extensibility.
- **Compatibility & Transition:**
    - IPv4 and IPv6 are not inherently compatible.
    - Mechanisms like dual stack, tunneling (e.g., 6to4), and NAT64 are required for transition.
- **Security:**
    - IPv4 security is mostly optional and implemented through add-ons (e.g., IPsec).
    - IPv6 was designed with mandatory support for IPsec.
- **Broadcasting vs Multicasting:**
    - IPv4 supports broadcasting, which can lead to network congestion.
    - IPv6 replaces broadcasting with multicasting and anycasting for better efficiency.

2. Routing – Principles and Issues

Principles:

- Routing determines the best path for data to travel from source to destination.
- Routers use routing tables and algorithms to make forwarding decisions.

Design Issues:

- **Scalability:** Routing protocols must handle growing network sizes without performance degradation.
- **Convergence Time:** Time taken for all routers to learn a new route after a change (e.g., link failure).
- **Loop Prevention:** Mechanisms to avoid routing loops, which can lead to packet loss or congestion.
- **Load Balancing:** Efficient use of multiple paths to distribute traffic evenly.
- **Policy Control:** Ability to enforce policies (e.g., preferred paths, cost limitations).
- **Resource Utilization:** CPU and memory usage in routers to maintain and update routing tables.

3. Routing Algorithms

A. Distance-Vector Routing

- **Design Principles:**
  - Routers share their routing tables with neighbors.
  - Based on Bellman-Ford algorithm.
- **Issues:**
  - **Slow convergence** (e.g., after a link failure).
  - **Routing loops** and **count-to-infinity** problems.
  - **Limited scalability** in large networks.

B. Link-State Routing

- **Design Principles:**
  - Each router has a complete map of the network.
  - Uses Dijkstra's algorithm to compute shortest paths.
  - Routers flood the network with link-state advertisements (LSAs).
- **Issues:**
  - **Higher memory and processing requirements.**
  - **Flooding overhead** during topology changes.
  - **Complex implementation** compared to distance-vector.

4. Routing Protocols

A. RIP (Routing Information Protocol)

- **Based on Distance-Vector algorithm.**
- **Design Issues:**
  - Maximum hop count limit of 15 (restricts scalability).
  - Slow convergence and vulnerability to routing loops.
  - Uses periodic updates (every 30 seconds), increasing unnecessary traffic.

B. OSPF (Open Shortest Path First)

- **Based on Link-State algorithm.**
- **Design Issues:**

- More complex configuration and maintenance.
- Uses areas and hierarchical design to manage scalability.
- Requires more CPU and memory than RIP, especially in large networks.
- Fast convergence but susceptible to **LSA storms** during frequent topology changes.

CHAPTER –5: Transport Layer:

The **Transport Layer** is responsible for **end-to-end communication**, ensuring data is delivered reliably and in the correct order (if needed), across a network between applications running on different hosts.

Design Issues in the Transport Layer

Design Aspect	Explanation
Service Type	Should the transport layer provide **connection-oriented (TCP)** or **connectionless (UDP)** service?
Reliability	Ensuring data delivery without loss, duplication, or corruption (TCP handles this).
Data Ordering	Packets may arrive out of order; mechanisms may be needed to reorder them (TCP does this).
Error Control	Detecting and recovering from transmission errors using checksums, acknowledgments, etc.
Flow Control	Preventing a fast sender from overwhelming a slow receiver (TCP uses a window mechanism).
Congestion Control	Managing traffic load to prevent congestion in the network (TCP includes congestion control).
Multiplexing	Allowing multiple applications to use the transport layer concurrently (via port numbers).
Efficiency vs Overhead	Balancing between performance and features (UDP is faster but less reliable; TCP is feature-rich but heavier).
Security	Though not a core part of the transport layer, protocols like TLS can be built on top of it for secure communication.

User Datagram Protocol (UDP)

Features:

- **Connectionless:** No setup before data transfer.
- **Unreliable:** No guarantees on delivery, order, or duplication.
- **Lightweight:** Minimal header (8 bytes).
- **No congestion or flow control.**
- Suitable for real-time or broadcast/multicast applications.

Use Cases:

- Streaming media (VoIP, video, online gaming)
- DNS lookups
- Simple query-response systems

Design Pros & Cons:

Pros	Cons
Low latency, fast transmission	No guarantee of delivery
Low overhead	No order control or retransmission
Simple to implement	No congestion control (may cause network issues)

Transmission Control Protocol (TCP)

Features:

- **Connection-oriented:** Requires a 3-way handshake before communication.
- **Reliable:** Guarantees delivery, in order, and error-checked.
- **Flow Control:** Uses a sliding window mechanism.
- **Congestion Control:** Adapts to network conditions (e.g., slow start, congestion avoidance).
- **Byte stream abstraction:** Data sent as a continuous stream, not discrete packets.

Use Cases:

- Web browsing (HTTP/HTTPS)
- Email (SMTP, IMAP)
- File transfers (FTP)

Design Pros & Cons:

Pros	Cons
Reliable and accurate delivery	Higher latency and overhead
Ordered and error-free data	More complex to implement
Adaptive to network conditions	Slower performance for real-time applications

Summary Table: UDP vs TCP

Feature	TCP	UDP
Connection Type	Connection-oriented	Connectionless
Reliability	Reliable (ACKs, retransmissions)	Unreliable
Ordering	Guarantees order	No ordering
Speed	Slower due to overhead	Faster
Header Size	20–60 bytes	8 bytes
Congestion Control	Yes	No
Flow Control	Yes	No
Use Case Examples	HTTP, FTP, SMTP	DNS, VoIP, online gaming

CHAPTER – 6: Application Layer:

1. **DNS (Domain Name System)**

Design Issues:

- **Scalability:** DNS must handle billions of domain names efficiently.
- **Distributed Architecture:** Data is spread across thousands of servers, which increases complexity.
- **Caching:** To reduce query load and latency, caching is used — but it must be managed carefully (e.g., TTL settings).
- **Security:** DNS is vulnerable to attacks like spoofing and cache poisoning. DNSSEC (DNS Security Extensions) helps address this.
- **Fault Tolerance:** DNS should provide continuous service even if some servers go down.
- **Consistency:** Propagation delays can cause inconsistencies during DNS updates.

2. DHCP (Dynamic Host Configuration Protocol)

Design Issues:

- **Address Pool Management:** Ensuring that IP addresses are properly allocated and not exhausted.
- **Lease Management:** Handling lease time, renewal, and expiration correctly.
- **Security:** DHCP lacks authentication, making it vulnerable to rogue DHCP servers.
- **Reliability:** The protocol must ensure clients always receive valid configuration even after reboot.
- **Mobility Support:** Mobile clients moving between networks need fast reconfiguration.
- **Scalability:** Large networks must manage thousands of leases efficiently.

3. SNMP (Simple Network Management Protocol)

Design Issues:

- **Scalability:** Managing large networks with thousands of devices.
- **Security:** SNMPv1 and v2 lack proper encryption/authentication; SNMPv3 adds secure communication.
- **Polling Overhead:** Continuous polling by SNMP managers can increase traffic load.
- **Data Representation:** SNMP uses a simple data model (MIB – Management Information Base), which may be limited for complex data.
- **Reliability:** Uses UDP, which may lead to lost management data.
- **Access Control:** Controlling who can read or write MIB data is critical.

4. FTP (File Transfer Protocol)

Design Issues:

- **Connection Complexity:** Uses two TCP connections (control and data), making firewall/NAT traversal difficult.
- **Security:** FTP transmits data, including usernames and passwords, in plaintext. FTPS/SFTP are alternatives.

- **Statefulness:** FTP is a stateful protocol, which complicates implementation and increases resource usage.
- **Performance:** May suffer from latency or overhead on slow or congested networks.

5. TFTP (Trivial File Transfer Protocol)

Design Issues:

- **Simplicity vs Features:** Designed to be minimal; lacks authentication, encryption, or directory navigation.
- **Reliability:** Uses UDP and includes its own basic error-checking and retransmission but is still less reliable than TCP-based FTP.
- **Security:** Extremely vulnerable due to lack of authentication/encryption — often restricted to LANs.
- **File Size Limitations:** Often limited in the size of files it can transfer.

6. SMTP (Simple Mail Transfer Protocol)

Design Issues:

- **Reliability:** Must ensure email delivery even when the recipient server is temporarily unavailable.
- **Security:** SMTP was designed without encryption. Modern email systems use STARTTLS, SPF, DKIM, and DMARC to address spam and spoofing.
- **Spam Control:** SMTP is vulnerable to abuse for sending spam.
- **Store and Forward:** Relies on relaying through intermediate servers, which may introduce delays or failures.
- **Size Limits:** SMTP has limits on attachment sizes.

7. WWW (World Wide Web – HTTP/HTTPS Protocol)

Design Issues:

- **Statelessness:** HTTP is stateless by default, requiring cookies, sessions, or tokens for continuity.
- **Security:** HTTP transmits data in plaintext; HTTPS (HTTP over TLS) is essential for secure communication.
- **Caching:** Managing efficient web content caching while ensuring freshness.
- **Latency and Performance:** Modern web apps are heavy; HTTP/2 and HTTP/3 aim to improve speed and reduce latency.
- **Scalability:** Web servers must handle high volumes of traffic and concurrent connections.
- **Interoperability:** Browsers and web servers must follow standards for compatibility.

8. Telnet

Design Issues:

- **Security:** Sends commands and credentials in plaintext; easily intercepted.

- **Lack of Encryption:** No built-in secure transmission.
- **Obsolete:** Largely replaced by SSH in secure environments.
- **Remote Access Control:** No access control mechanism beyond basic authentication.

9. SSH (Secure Shell)

Design Issues:

- **Key Management:** Public key infrastructure (PKI) must be properly managed to avoid unauthorized access.
- **Performance:** Encryption adds overhead, although modern implementations are efficient.
- **Complexity:** Configuration and key exchange mechanisms can be complex.
- **Authentication Methods:** Supports multiple methods (password, public key, certificates), each with its own security considerations.

Summary Table

Protocol	Key Design Issues
DNS	Scalability, caching, security, consistency
DHCP	Address management, lease handling, security, scalability
SNMP	Security (v1/v2), polling overhead, scalability
FTP	Plaintext transmission, complex connection model, firewall issues
TFTP	Minimal features, security, UDP limitations
SMTP	Security, spam vulnerability, reliability
WWW (HTTP)	Statelessness, caching, performance, security
Telnet	Plaintext communication, obsolete, insecure
SSH	Secure communication, key management, authentication

CHAPTER –7: Network Devices:
NIC (Network Interface Card):

Role:

- Hardware component that connects a computer/device to a network.
- Converts data between the device's internal data format and signals on the network medium.

Design Considerations:

- **Speed Support:** e.g., 100 Mbps, 1 Gbps, 10 Gbps.
- **Full-Duplex vs Half-Duplex:** Most modern NICs support full-duplex.
- **MAC Address:** Unique hardware address for network identification.
- **Driver Support:** OS compatibility and features like interrupt moderation.
- **Offloading Capabilities:** e.g., checksum offloading, TCP segmentation offload to improve CPU efficiency.

2. Hub

Role:

- Basic Layer 1 (Physical Layer) device that connects multiple devices in a LAN.
- Broadcasts incoming signals to all ports.

Design Considerations:

- **No Intelligence:** Cannot filter traffic; leads to unnecessary traffic on the network.
- **Collision Domain:** All devices share the same domain → high risk of collisions.
- **Obsolete:** Rarely used today; replaced by switches.

3. Switches

Switches operate at **Layer 2 (Data Link Layer)** or **Layer 3 (Network Layer)** depending on functionality.

Types in Enterprise Networks:

A. Access Switch

- **Role:** Connects end-user devices (PCs, printers, IP phones) to the network.
- **Design Features:**
  - Typically Layer 2.
  - PoE (Power over Ethernet) support for IP phones and access points.
  - VLAN support.
  - Security features like port security and 802.1X authentication.

B. Distribution Switch

- **Role:** Aggregates traffic from multiple access switches; acts as a gateway between access and core layers.
- **Design Features:**
  - Usually Layer 3 capable.
  - Redundancy and load balancing.
  - Higher throughput than access switches.
  - ACLs (Access Control Lists) and routing support.

C. Core Switch

- **Role:** Backbone of the network; connects distribution switches and provides high-speed data transmission across the enterprise.
- **Design Features:**
  - High-speed Layer 3 switching.
  - Redundant power and network interfaces.
  - High reliability and throughput (10 Gbps+).
  - No user access devices connected directly.

4. Router

Role:

- Layer 3 (Network Layer) device that routes packets between different networks (LANs/WANs).
- Used for inter-network communication.

Design Considerations:

- **Routing Protocol Support:** RIP, OSPF, BGP, etc.
- **Performance:** Must handle high throughput, especially on WAN links.
- **Security Features:** NAT, firewall, VPN, ACLs.
- **Redundancy:** Dual power supplies, redundant interfaces.

5. WiFi Access Point (AP)

Role:

- Provides wireless connectivity (WiFi) to mobile or wireless devices.
- Acts as a bridge between the wired LAN and wireless clients.

Design Considerations:

- **Frequency Bands:** 2.4 GHz, 5 GHz, and newer 6 GHz (WiFi 6E).
- **Standards Support:** IEEE 802.11 a/b/g/n/ac/ax (WiFi 6).
- **Coverage and Capacity:** Number of clients supported, signal range.
- **Security:** WPA3, MAC filtering, 802.1X support.
- **PoE Support:** Often powered via Ethernet.

6. Wireless LAN Controller (WLC)

Role:

- Centralized device that manages multiple WiFi Access Points.
- Provides configuration, authentication, security, load balancing, and firmware updates.

Design Considerations:

- **Central Management:** Reduces administrative overhead.
- **Roaming Support:** Seamless handoff between APs (Layer 2/3 roaming).
- **Scalability:** Number of APs and clients it can support.
- **Redundancy:** HA (High Availability) for controller failure protection.
- **Integration:** With RADIUS, AAA servers, and monitoring tools.

Visual Hierarchy (Enterprise Network Topology)

```
less
CopyEdit
               [ Core Switches ]
                      ||
               [ Distribution Switches ]
                      ||
          +-----------+-----------+
          |                       |
[ Access Switch ]       [ Wireless Access Point ]
          |                           |
      [ End Devices ]       [ Mobile Clients ]
                      ||
                 [Router / Firewall]
                      ||
                [Internet / WAN]
```

Summary Table

Device	Layer	Main Role	Modern Use
NIC	Layer 1/2	Connects device to network	Yes
Hub	Layer 1	Broadcast traffic to all ports	Obsolete
Access Switch	Layer 2	Connects end devices	Yes
Distribution Switch	Layer 3	Aggregates access layer traffic	Yes
Core Switch	Layer 3	High-speed backbone switching	Yes
Router	Layer 3	Routes packets between networks	Yes
WiFi Access Point	Layer 2	Wireless access for end devices	Yes
Wireless LAN Controller	Layer 2/3	Centralized WiFi AP management	Yes