LECTURE NOTES ON

ADVANCED COMPUTER NETWORKS

PREPARED BY :

Sri. Nalinikanta Mohapatra

Unit -1

Computer Network:

- A **computer network** is a collection of two or more interconnected computers and devices.
- It enables devices to communicate and exchange data.
- Networks allow users to share resources such as files, printers, software, and Internet connections.

Definition

A computer network is a group of interconnected computers and devices that communicate and share resources using communication links and networking protocols.

Need for Computer Networks

Computer networks are used to:

- Share files and data.
- Share hardware resources (printers, scanners).
- Share software applications.
- Access the Internet.
- Enable communication through email, messaging, and video conferencing.
- Reduce operational costs.
- Improve reliability and efficiency.

Characteristics of Computer Networks

- High-speed communication.
- Resource sharing.
- Scalability (easy to add new devices).
- Reliability.
- Security through authentication and encryption.
- Remote accessibility.

Components of a Computer Network

A computer network consists of the following components:

a) Sender

- Device that sends data.
- Example: Computer, Smartphone.

b) Receiver

- Device that receives data.

c) Transmission Medium

- Carries data between devices.
- Types:
    - Wired (UTP, Coaxial, Fiber Optic)
    - Wireless (Wi-Fi, Bluetooth)

d) Network Devices

- Hub
- Switch
- Router
- Gateway
- Modem

e) Protocols

- Rules that govern communication.
- Example:
    - TCP/IP
    - HTTP
    - FTP

Advantages of Computer Networks:

- Resource sharing
- Fast communication
- Centralized data management
- Easy backup
- Cost reduction
- Remote access
- Improved collaboration

Applications of Computer Networks:

- Online Banking
- E-Commerce
- Online Education
- Video Conferencing
- Cloud Computing
- Social Networking
- File Sharing
- Remote Working

Evolution of Computer Networks:

1960s – Mainframe Era

- Centralized computing.
- Large mainframe computers connected to terminals.
- Expensive and limited to large organizations.

1970s – ARPANET

- Developed by the U.S. Department of Defense.
- Introduced **Packet Switching**.
- First successful computer network.
- Foundation of today's Internet.

1980s – Local Area Networks (LAN)

- Ethernet technology introduced.
- Computers connected within offices and institutions.
- Resource sharing became easier.

1990s – Internet Era

- TCP/IP became the standard networking protocol.
- World Wide Web (WWW) became popular.
- Growth of email and web browsing.

2000s – Wireless Networking

- Introduction of Wi-Fi.
- Broadband Internet became common.
- Mobile communication expanded rapidly.

Present – Advanced Networking

Modern networks include:

- Cloud Computing
- Internet of Things (IoT)
- Software Defined Networking (SDN)
- 5G Networks
- Artificial Intelligence (AI)-based networking

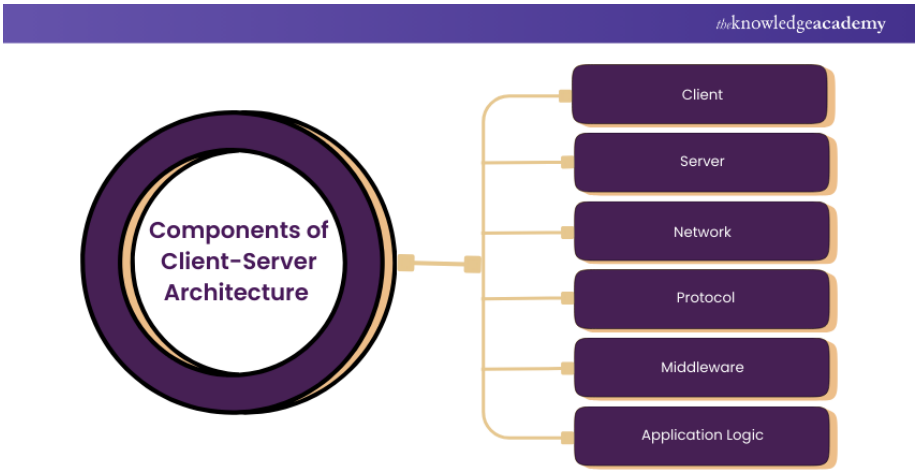
Network Architecture:

- **Network architecture** refers to the design and structure of a computer network.
- It defines how computers communicate, share resources, and exchange data.
- The two common network architectures are:
    - **Client-Server Architecture**
    - **Peer-to-Peer (P2P) Architecture**

Client Server Architecture:

Client-Server Architecture is a network model that allows communication and data exchange between different applications over a single or multiple servers.
This model divides the system into two parts: the client side and the server side.
a) Client: An application that requests services from the server, such as data retrieval, storage, calculations, or other functions.
b) Server: An application that processes client requests, sends responses, or performs specified actions.
The server and client may reside on the same machine or different devices across the network. Effective Communication occurs via predefined protocols like HTTP, FTP, or SMTP.
Client-Server Architecture is widely used in applications such as email, web browsing, online banking, and e-commerce.

Components of Client-Server Architecture:



Client-Server Architecture depends on three main components that need to work together for it to function. These components are:
a) Client: A client device or software that requests services from a server. Clients are consumer-facing and often include web browsers, mobile applications, or desktop applications that people can interact with. They communicate with the server to retrieve data, make transactions, or perform other tasks by delegating that responsibility to the server.
b) Server: A server is a computer or program that offers services or solutions to clients over a network. Servers handle processing of client requests, which includes tasks like file storage, database access, and application hosting, along with backend activities like computations, data management, and business logic, significantly reducing what clients need to handle.
c) Network: This serves as the channel through which clients and servers are connected for data transfer between them. Networks range from local area networks (LAN) within a single building to wide area networks (WAN) and the internet, which can span countries. It acts as the intermediary, facilitating the interchange of requests and responses between the clients and servers, which influences the speed and reliability of these interactions.
d) Protocol: Protocols are rules that define how data is exchanged between clients and servers, ensuring communication is orderly, secure, and understandable. Common protocols include HTTP or HTTPS for web services, FTP for file transfers, and SMTP for email. They help bridge communication between different systems, independent of their technology stack.

e) Middleware: Middleware acts as a bridge between client-side and server-side code, enabling them to communicate. It performs tasks such as authentication, load balancing, data translation, and message queuing, simplifying interactions within the Client-Server model by enhancing transaction speed, scalability, and integration.
f) Application Logic: Application logic is the code and processes that determine how a server responds to client requests, involving business rules, Big Data Processing, and workflows on the server side. It ensures the server correctly interprets client requests, performs necessary calculations or data manipulations, and delivers appropriate responses.

Characteristics of Client-Server Architecture

Client-Server architecture has distinct characteristics:
a) The client and server machines can differ greatly in hardware and software requirements and may come from different vendors.
b) The network can scale horizontally by adding more client machines or vertically by upgrading to more powerful servers or a multi-server configuration.
c) A single server can offer multiple services simultaneously, though each service must run its own server program.
d) Both client and server applications interact directly with a transport layer protocol, establishing communication to send and receive information.
e) Both client and server computers require a full stack of protocols, where the transport protocol utilises lower-layer protocols to send and receive individual messages.

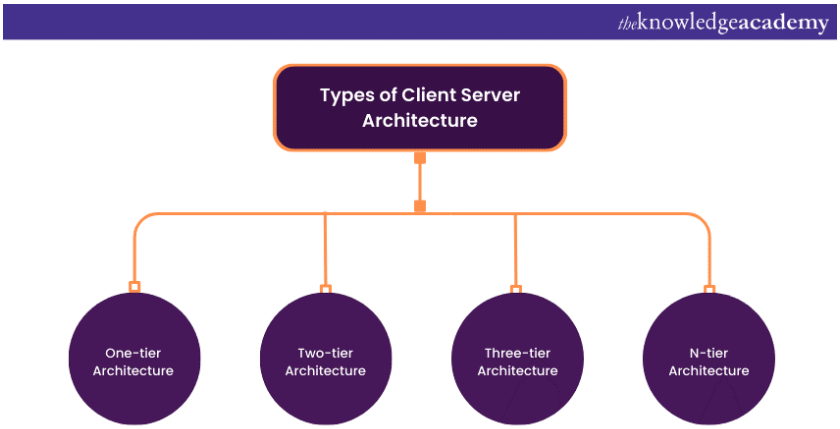
How Does Client-Server Architecture Work:

The basic steps of how Client-Server Architecture works are:
1) In the first step, the client sends a request to the server using the network medium. The request can be a query, a command, or a message.
2) In the second step, the server receives the request and processes it according to its logic and data. The server may access its own resources or other servers to fulfil the request.
3) In the third step, the server sends a response back to the client using the network medium. The response can be Data, an acknowledgement, or an error message.
4) Lastly, the client receives the response and displays it to the user or performs further actions based on it.

Examples of Client-Server Architecture

You might be surprised at how often you encounter Client-Server Architecture in everyday life. Here are three common examples:
1) Email Servers: Email has evolved into the primary communication method for businesses due to its speed and convenience. Various server components work together to deliver emails between users across different mail servers.
2) File Servers: When saving documents on services like Google Docs or Microsoft Office, you're interacting with file servers. These servers store data centrally and allow multiple clients to access it.
3) Web Servers: These high-powered servers host websites, which web clients access through DNS or an IP address. Here's a simplified process:
a) A user enters a URL in the browser.
b) The browser requests the IP address from the Domain Name System (DNS) .
c) The DNS server provides the IP address to the browser.
d) The browser sends an HTTPS or HTTP request to the web server.
e) The server sends back the requested files.
f) The user retrieves the files, and the process continues as needed.

Types of Client-Server Architecture



There are different types of Client-Server Architecture, depending on how many tiers or layers are involved in the communication process. Some of the common types are:

1) One-tier Architecture

A self-contained application on a single platform. In one-tier architecture, the client, server, and database are all on the same machine. The client handles user interaction and business logic, the server provides services like data storage and processing, and the database manages data. While simple and popular for small apps, this architecture is rarely used in production because it doesn't meet most system requirements.

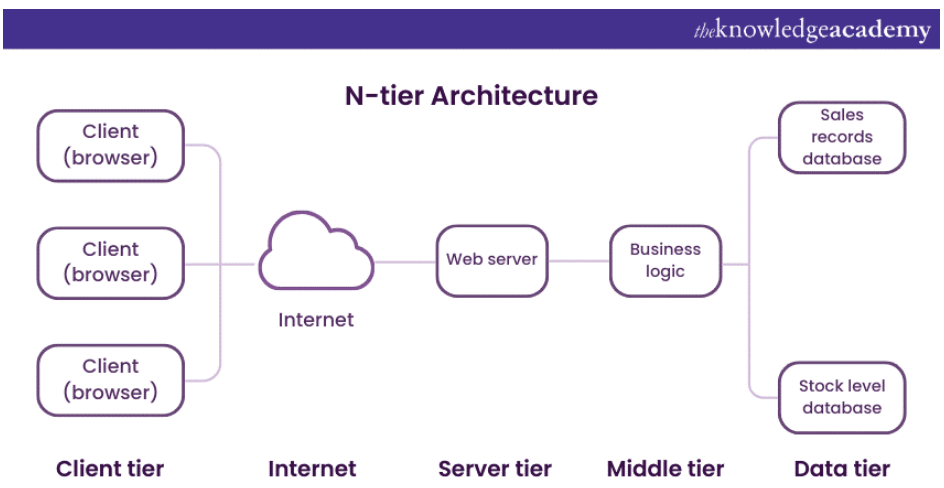
2) Two-tier Architecture

This basic Client-Server Architecture involves direct communication between the client and server without an intermediate layer. The client manages the User Interface (UI) and business logic, while the server handles data storage and processing. An example is a web browser requesting pages from a web server, which responds with HTML files. It's easy to implement but has drawbacks like low scalability, high network traffic, and security risks.

3) Three-tier Architecture

A more complex client-server setup with an intermediate layer (usually middleware or an application server) that handles business logic, acting as a bridge between the client and server. The client deals with the user interface (UI), while the server manages data storage. An example is an online banking system where the client is a web browser, the middleware checks transactions, and the server stores account data. This architecture improves scalability, performance, and security but increases complexity and cost.

4) N-tier Architecture:



A more flexible Client-Server Architecture with more than three tiers, allowing greater scalability, flexibility, and modularity. Each tier can be distributed across different machines or networks and updated independently. An example is an e-commerce system with a web browser displaying the product catalog, a web server handling HTTP requests, an application server processing business logic, and a database storing product information. While suitable for complex systems, it requires more resources and management.

Peer-to-Peer (P2P) architecture:

Peer-to-peer (P2P) architecture is a distributed computing model where nodes in the network behave as equals, communicating and sharing resources directly with each other. Unlike client-server architectures that rely on centralized servers to facilitate communication and resource sharing, P2P networks use the collective power of individual nodes to achieve scalability, fault tolerance, and resilience.

Characteristics of Peer-to-Peer (P2P) Networks:

- **Decentralization:** P2P networks operate without a central authority, allowing nodes to communicate and share resources directly.
- **Scalability**: P2P networks can be easily scaled to accommodate a large number of nodes without relying on a centralized infrastructure.
- **Fault tolerance:** P2P networks are resilient to node failure because the absence of a central server means that the network can continue to function even if some nodes become unavailable.
- **Resource sharing:** P2P network participants can share files, data, and computing resources directly with each other.
- **Autonomy:** Each node in a P2P network has autonomy over its own resources and decisions, which contributes to the overall resilience and flexibility of the network.

Types of Peer-to-Peer (P2P) Networks:

Below are the types of P2P Networks:

1. Pure P2P Networks

Also known as decentralized or true P2P networks, pure P2P networks operate without any central authority or dedicated infrastructure.

Peers in these networks have equal privileges and responsibilities, and they directly communicate and share resources with each other.

2. Hybrid P2P Networks

Hybrid P2P networks combine elements of both decentralized and centralized architectures.

They typically include some central servers or super peers that coordinate network activities, manage resources, or provide additional services.

Hybrid P2P networks aim to achieve a balance between decentralization and efficiency.

3. Overlay P2P Networks

Overlay P2P networks create a virtual network on top of an existing infrastructure, such as the internet.

Peers in these networks establish direct connections with each other, forming an overlay structure that facilitates resource sharing and communication.

Overlay P2P networks often employ distributed hash tables (DHTs) or other routing mechanisms to locate and retrieve resources efficiently.

4. Structured P2P Networks

Structured P2P networks organize peers into a specific topology or structure, such as a ring, tree, or mesh.

Peers maintain routing tables or other data structures to facilitate efficient resource lookup and data retrieval.

Structured P2P networks offer predictable performance and scalability but may require additional overhead for maintenance. Examples include CAN (Content Addressable Network) and Pastry.

5. Unstructured P2P Networks

In contrast to structured P2P networks, unstructured P2P networks do not impose any specific topology or organization on peers.
Peers in these networks typically rely on flooding or random search algorithms to locate resources, resulting in lower efficiency but greater flexibility and simplicity.
Examples include early versions of Gnutella and Freenet.

Components of Peer-to-Peer (P2P) Systems

Below are the key components of Peer-to-Peer (P2P) Systems:

1. **Peer Nodes**: Individual participants in a P2P network, each acting as both a client and a server.
2. **Overlay Network:** A virtual network topology that connects peer nodes and facilitates communication and resource sharing.
3. **Indexing Mechanisms**: Systems for organizing and indexing shared resources, enabling efficient search and retrieval.
4. **Bootstrapping Mechanisms**: Processes for node discovery and network initialization that allow new nodes to join the network seamlessly.

Advantages:

Below are the advantages of Peer-to-Peer (P2P) Networks:

- **Decentralization**: P2P networks distribute control and resources among peers, eliminating the need for a central server. This decentralization increases resilience and reduces the risk of a single point of failure.
- **Load Distribution**: Workload is distributed across multiple peers in a P2P network, improving resource utilization and overall performance, particularly under heavy loads.
- **Cost Reduction**: P2P networks can significantly reduce costs associated with infrastructure, maintenance, and bandwidth, as they rely on resources contributed by peers rather than centralized servers.
- **Content Redundancy and Availability**: Content replication across multiple peers ensures redundancy and continuous availability, even if some peers go offline or experience failures.

Challenges of Peer-to-Peer (P2P) architecture:

Below are the challenges of Peer-to-Peer (P2P) Networks:

- **Scalability**: P2P networks face scalability challenges as they grow in size. Managing a large number of peers and ensuring efficient communication between them becomes increasingly complex.
- **Security**: Security is a significant concern in P2P networks due to the decentralized nature, making them susceptible to various threats such as malicious peers, data tampering, and unauthorized access. Protecting data integrity and ensuring secure communication among peers is essential.
- **Content Availability and Quality**: The availability and quality of content can vary widely in P2P networks due to factors like peer churn, network dynamics, and heterogeneous resources. Maintaining consistent access to high-quality content across the network poses a challenge.
- **Data Management and Consistency**: Managing distributed data in P2P networks involves storing, retrieving, replicating, and ensuring consistency across multiple peers. Achieving data consistency and coherence while dealing with peer dynamics and network partitions is a complex task.

Applications :

The P2P architecture has many applications in various domains, including:

- **File sharing:** Platforms like BitTorrent and eDonkey use P2P networks for efficient and decentralized file sharing.
- **Content Distribution:** P2P-based Content Delivery Networks (CDNs) distribute multimedia content and software updates to users around the world.
- **Collaboration and Communication:** P2P messaging and collaboration tools enable real-time communication and collaboration between users.

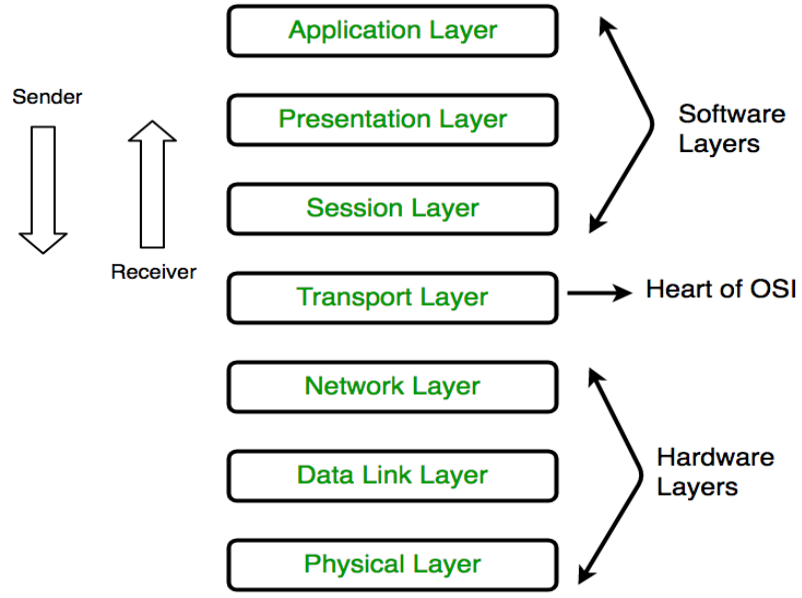
- **Distributed Computing:** P2P computing platforms use distributed resources for tasks such as scientific computing, data analysis, and cryptocurrency mining.

Peer-to-Peer Networks vs Client/Server Networks	
Peer-to-Peer Networks	**Client/Server Networks**
• Easy to set up	• More difficult to set up
• Less expensive to install	• More expensive to install
• Can be implemented on a wide range of operating systems	• A variety of operating systems can be supported on the client computers, but the server needs to run an operating system that supports networking
• More time consuming to maintain the software being used (as computers must be managed individually)	• Less time consuming to maintain the software being used (as most of the maintenance is managed from the server)
• Very low levels of security supported or none at all. These can be very cumbersome to set up, depending on the operating system being used	• High levels of security are supported, all of which are controlled from the server. Such measures prevent the deletion of essential system files or the changing of settings
• Ideal for networks with less than 10 computers	• No limit to the number of computers that can be supported by the network
• Does not require a server	• Requires a server running a server operating system
• Demands a moderate level of skill to administer the network	• Demands that the network administrator has a high level of IT skills with a good working knowledge of a server operating system

OSI Model:

The OSI Model is a conceptual framework created by the International Organization for Standardization (ISO) to describe how data is transmitted across a network using a structured seven-layer architecture.

- Divides network communication into seven functional layers.
- Assigns specific responsibilities to each layer.
- Promotes compatibility between different networking systems.
- Simplifies network design, implementation, and troubleshooting.



Layer 1: The Physical Layer

The **Physical Layer** is the foundation of the OSI model, acting as the bridge for actual physical connections between devices. Its primary mission is the transmission of raw, unstructured bitstreams over a physical medium from one node to the next.

- **Core Responsibility:** It manages the hardware-level transmission of individual bits. When receiving data, it translates incoming physical signals back into digital 0s and 1s to be processed by the Data Link layer.
- **Essential Hardware:** Common devices operating at this level include Hubs, Repeaters, Modems, and Cables.
- **Bit Synchronization:** It ensures the sender and receiver are "in sync" by providing a clock signal that controls the timing of bit transmission.
- **Bit Rate Control:** It dictates the transmission speed, defined as the number of bits sent per second.
- **Physical Topologies:** It defines the structural layout of the network, such as Bus, Star, or Mesh configurations.
- **Transmission Mode:** It determines the direction of data flow, utilizing modes like Simplex (one-way), Half-Duplex (two-way, one at a time), or Full-Duplex (simultaneous two-way).

Layer 2: The Data Link Layer (DLL)

The **Data Link Layer** serves as the bridge between the physical hardware and the logical network, ensuring reliable node-to-node delivery of data. Its primary goal is to ensure that data transfer is error-free across the physical medium.

1. Data Packaging (Framing): At this layer, data packets received from the Network layer are divided into manageable units called Frames. This is done by adding specific "start" and "stop" bits so the receiver can recognize where one unit of data ends and the next begins.

2. Addressing and Hardware: The DLL uses **MAC addresses** (Physical Addressing) to identify hosts. It encapsulates the sender's and receiver's MAC addresses into the frame header. Common devices operating here are **Switches and Bridges**.

3. Sublayers:

- **Logical Link Control (LLC):** Manages flow and error control while acting as an interface for upper-layer protocols.
- **Media Access Control (MAC):** Determines how devices physically access the transmission medium and handles hardware addressing.

4. Error Control: It detects and retransmits damaged or lost frames to maintain data integrity.

5. Flow Control: It synchronizes the data rate between a fast sender and a slower receiver to prevent data "bottlenecks" or loss.

6. Access Control: When multiple devices share the same communication channel, the MAC sublayer dictates which device has the right to transmit at any given time to avoid collisions.

Layer 3: The Network Layer

The **Network Layer** manages data transmission between hosts across different networks by handling logical addressing and path finding.

- **Data Unit:** Data segments are encapsulated into Packets.
- **Logical Addressing:** Assigns unique **IP addresses** (sender and receiver) to the packet header to identify devices globally.
- **Routing:** Determines the most efficient physical path from the source to the destination across interconnected networks.
- **Hardware:** Primarily implemented via **Routers and Switches**.
- **Inter-networking:** Facilitates communication between disparate networks by directing traffic to the correct destination.

Layer 4: The Transport Layer

The Transport Layer ensures the end-to-end delivery of entire messages. It acts as a liaison, providing services to the Application layer while utilizing the infrastructure of the Network layer to ensure data reaches the correct application on the destination host.

- **Data Unit:** Data is broken down into Segments.
- **Service Point Addressing:** Uses Port Numbers (e.g., Port 80 for web traffic) to ensure data is delivered to the specific process or application intended, not just the device.
- **Segmentation & Reassembly:** Splits large messages into smaller segments for transmission and reassembles them in the correct order at the destination.
- **Protocols:** Common protocols include **TCP** (reliable), **UDP** (fast).
- **Connection-Oriented (TCP):** Requires a "handshake" to establish a connection; ensures reliability via error checking and acknowledgements.
- **Connectionless (UDP):** Sends data immediately without a formal connection; faster but offers no guarantee of delivery.

Layer 5: The Session Layer

The **Session Layer** acts as the "dialogue manager," governing the opening, closing, and security of communication channels between two devices.

- **Session Lifecycle:** Manages the establishment, maintenance, and termination of connections between applications.
- **Authentication & Security:** Ensures that the communicating parties are verified and the connection is secure.
- **Synchronization:** Inserts checkpoints into the data stream. This allows a transfer to resume from the last saved point if a failure occurs, rather than restarting from the beginning.
- **Dialog Control:** Directs whether communication is half-duplex (alternating) or full-duplex (simultaneous).

Layer 6: The Presentation Layer

Often called the Translation Layer, the Presentation Layer ensures that data is formatted, secured, and compressed so that the receiving application can correctly interpret it.

- **Translation:** It extracts data from the Application Layer and converts it into a standardized format for network transmission, bridging differences in data representation between different systems.
- **Standards & Formats**: Handles the encoding of media using standards such as JPEG, MPEG, and GIF.
- **Encryption/Decryption**: Provides security by converting "plain text" into "ciphertext" (encryption) and back again (decryption) using key values. This process is typically handled by protocols like TLS/SSL.
- **Compression:** Reduces the total number of bits required for transmission, which increases network efficiency and speed.

Layer 7: The Application Layer

The Application Layer sits at the top of the OSI stack and serves as the direct interface between the software user and the network. It produces the data that will be sent and displays the information received from other layers.

- **User Interface**: Acts as a "window" for network-based applications (like web browsers or email clients) to access network services.
- **Core Protocols**: Utilizes high-level protocols such as HTTP/S (Web), SMTP (Email), FTP (File Transfer), and DNS (Domain Name Resolution).
- **Network Virtual Terminal (NVT):** Enables users to log into and interact with remote hosts as if they were physically present at the terminal.
- **File Transfer, Access, and Management (FTAM):** Provides the framework for users to retrieve, manage, and manipulate files stored on remote computers.

- **Directory Services**: Offers distributed database access to manage global information regarding various network objects and services.

Advantages of the OSI Model

- Provides a standard for network communication.
- Simplifies network design and development.
- Makes troubleshooting easier.
- Supports interoperability between different vendors.
- Allows independent development of each layer.

Limitations of the OSI Model

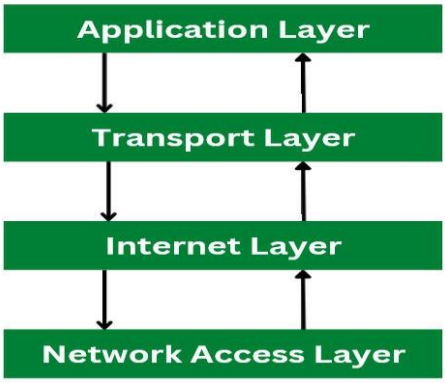
- It is a **reference model**, not an actual protocol.
- Some layers have overlapping functions.
- More complex than the TCP/IP model.

TCP/IP Model:

- The TCP/IP (Transmission Control Protocol/Internet Protocol) Model is the standard networking model used for communication over the Internet.
- It was developed by the U.S. Department of Defense (DoD).
- It defines how data is transmitted from one device to another through interconnected networks.
- Unlike the OSI model, the TCP/IP model consists of 4 layers.

Objectives of the TCP/IP Model:

1. Provides reliable communication between devices.
2. Enables data transmission over the Internet.
3. Supports communication between different types of networks.
4. Ensures interoperability among different hardware and software platforms.



Layers of TCP/IP Model:

1. Application Layer

This is the top layer of the TCP/IP model, where applications like web browsers, email clients, and file-sharing tools interact with the network.

- Acts as a bridge between user applications and lower network layers.
- Supports protocols such as HTTP, FTP, SMTP, and DNS.
- Handles data formatting so information is correctly understood by both sender and receiver.
- Provides encryption for secure communication.
- Manages sessions to track ongoing connections.

2. Transport Layer

Ensures reliable and efficient delivery of data between devices, managing segmentation, ordering, and retransmission as needed.

- Breaks large messages into packets and reassembles them at the destination.
- TCP checks for errors, resends lost data, and ensures correct order.
- UDP provides low-latency, connectionless delivery without error checking.
- Prevents the receiver from being overwhelmed by regulating data flow.
- Uses port numbers to allow multiple applications to share the network simultaneously.

TCP (Transmission Control Protocol): TCP is used when reliability and accuracy are important. It ensures that data is delivered exactly as sent.

- TCP detects errors in the data using checksums to ensure integrity.
- If any data is lost or corrupted during transmission, TCP automatically resends it.
- Data is broken into packets, and TCP ensures these packets arrive in the correct sequence.
- TCP establishes a connection between sender and receiver before sending data, maintaining a stable session throughout the communication.
- Loading web pages, downloading files, sending emails, or any application where data must be complete and accurate.

UDP (User Datagram Protocol): UDP is used when speed is more important than perfect accuracy. It is faster but does not guarantee reliable delivery.

- UDP detects errors via checksums but does not verify or recover from them.
- Lost or damaged data is not resent.
- Packets may arrive out of order, and the protocol does not fix it.
- Because it avoids extra checks and connections, UDP is faster and uses fewer resources.
- Live video streaming, online gaming, VoIP calls, or real-time applications where speed matters more than reliability.

3. Internet Layer

Responsible for addressing, packaging, and routing data packets so they can travel across networks and reach the correct destination device. It ensures that data can move between different networks efficiently.

- Assigns IP addresses to identify source and destination devices.
- Determines the best path for data to travel across networks.
- Breaks large packets into smaller ones for transmission and reassembles them at the destination.
- Primarily uses IP (Internet Protocol), along with supporting protocols like ICMP for error reporting and ARP for address resolution.

4. Network Access (Link Layer)

Responsible for physically transmitting data over network hardware, including cables, switches, and wireless connections. It handles how data is formatted for the network medium and ensures it reaches the next device on the path.

- Sends and receives raw bits over physical media like Ethernet cables, fiber optics, or Wi-Fi.
- Organizes data into frames for proper transmission and recognition by devices.
- Detects transmission errors using checksums or CRC.
- Uses hardware addresses to identify devices within the same network segment.
- Determines how multiple devices share the same physical medium, avoiding collisions.

Advantages:

- **Widely Used:** Forms the foundation of the Internet and most modern networks.
- **Platform Independent:** Works on different hardware and operating systems.
- **Reliable Communication:** TCP ensures error checking, delivery confirmation, and data integrity.
- **Scalable:** Can support small networks to global Internet-scale networks.
- **Open Standard:** Free to use and not controlled by a single organization.

Disadvantages:

- **Complexity for Beginners:** Can be difficult to fully understand all protocols.
- **No Strict Layer Enforcement:** Unlike OSI, layer boundaries are not rigid, which may cause implementation variations.
- **Overhead:** TCP's error checking and reliability features can add extra data overhead.
- **Security Limitations:** Basic TCP/IP was not designed with strong built-in security; additional protocols like TLS/SSL are needed.
- **Limited Multimedia Support:** Original design focused on data, not optimized for real-time audio/video (needs extra protocols).

Addressing Mechanisms:

Addressing mechanisms in computer networks are systems of rules used to uniquely identify devices, processes, or networks. They form a hierarchical, layered architecture to ensure data successfully travels across local connections and the global internet. The four primary levels of addressing are physical, logical, port, and specific. Here is a breakdown of the four main addressing mechanisms:

1. Physical Addresses (MAC Address)

Operating at the **Data Link Layer (Layer 2)**, physical or MAC (Media Access Control) addresses are hardware-burned, unique identifiers (e.g., 00:1A:2B:3C:4D:5E) assigned to a Network Interface Card (NIC).

- **Purpose:** They are used for direct, node-to-node delivery within the same local network (LAN or WAN).
- **Resolution Mechanism:** Protocols like ARP (Address Resolution Protocol) map dynamic logical addresses to static physical addresses so local data frames can reach their destination.

2. Logical Addresses (IP Address)

Operating at the **Network Layer (Layer 3)**, logical addresses are software-based addresses that identify a device globally across interconnected networks.

- **Purpose:** They are used to route data across different networks (e.g., the Internet).
- **Mechanisms:**
    - **IPv4:** A 32-bit numeric address represented in dot-decimal notation (e.g., 192.168.1.15).
    - **IPv6:** A 128-bit address in hexadecimal format (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334) to accommodate a massive number of devices.
    - **Subnetting & NAT:** Mechanisms like subnetting divide large blocks of IPs into smaller, manageable networks, while Network Address Translation (NAT) maps multiple private local IPs to a single public IP.

3. Port Addresses

Operating at the **Transport Layer (Layer 4)**, port addresses are 16-bit numbers assigned to specific software processes or applications on a host.

- **Purpose:** While IP addresses get data to the correct computer, port addresses ensure the data reaches the correct application (e.g., web traffic, email) running on that computer.

- **Mechanisms:** Examples include **Port 80** for unencrypted HTTP web traffic and **Port 443** for secure HTTPS traffic.

4. Specific Addresses (Domain Names)

Operating at the **Application Layer (Layer 7)**, these are user-friendly, symbolic addresses meant for human readability.

- **Purpose:** They allow users to connect to networks using easy-to-remember names instead of numeric IP addresses.
- **Resolution Mechanism:** DNS (Domain Name System) acts as a digital phonebook, translating symbolic names (e.g., google.com) into underlying IP addresses.

IPv4:

IPv4 (Internet Protocol version 4) is the foundational protocol used to identify devices and route traffic across packet-switched computer networks. It assigns a unique 32-bit logical address to every connected machine, limiting the address pool to 2^{32} (about 4.3 billion) total addresses.

Address Structure:

An IPv4 address is split into two parts: a **network ID** and a **host ID**. It is represented in dotted-decimal notation consisting of four 8-bit numbers (octets), ranging from 0 to 255.

Example: 192.168.0.1

Address Classes

Traditionally, the IPv4 address space was segmented into five classes to determine the proportion of network bits to host bits:

- **Class A:** 0.0.0.0 to 127.255.255.255 (For very large networks, such as those used by governments and major corporations)
- **Class B:** 128.0.0.0 to 191.255.255.255 (For mid-sized networks like large universities)
- **Class C:** 192.0.0.0 to 223.255.255.255 (For smaller local area networks)
- **Class D:** 224.0.0.0 to 239.255.255.255 (Reserved for multicasting)
- **Class E:** 240.0.0.0 to 255.255.255.255 (Reserved for experimental use)

Modern networks use **CIDR (Classless Inter-Domain Routing)** instead of these strict classes, allowing flexible subnetting to prevent wasting IP addresses.

Packet Structure:

At the network layer of the OSI model, data is transmitted in packets called datagrams. The IPv4 packet header contains essential routing information:

- **Source & Destination IP:** Identifies the packet's origin and final destination.
- **Time to Live (TTL):** Prevents infinite routing loops by decrementing at each router hop; packets with a TTL of 0 are dropped.
- **Flags & Fragment Offset:** Used when large packets are split up (fragmented) to traverse networks with smaller Maximum Transmission Units (MTUs).

Advantages of IPv4:

- **Universal Compatibility:** Supported by almost all network devices, legacy systems, and routers globally, ensuring maximum interoperability.
- **Simplicity:** Simpler packet headers allow network routers to process and route traffic very quickly.
- **Efficiency:** Requires less memory cache and processing power to read and store compared to newer protocols.
- **Broadcast Support:** Allows transmission of data to all devices on a specific local network simultaneously.
- **Proven Reliability:** The technology is highly established with decades of real-world use and troubleshooting documentation.

Disadvantages of IPv4:

- **Address Exhaustion:** The 32-bit pool provides 2^{32} (about 4.3 billion) addresses, which has been depleted by the massive growth of connected devices.
- **Dependency on NAT:** Because public IP addresses are scarce, networks rely heavily on NAT to share one public address among dozens of private local devices.
- **Security Vulnerabilities:** Built-in IPsec is not native to IPv4 and is largely optional, making it highly susceptible to IP spoofing, packet sniffing, and unauthorized interceptions.
- **Complex Configuration:** Demands either manual IP configuration or constant use of DHCP, which increases the likelihood of human error and management overhead.
- **Inefficient Routing:** The hierarchical structure and address expansion make routing less effective at a global scale compared to newer alternatives.
- **Limited Quality of Service (QoS):** Traffic prioritization is inconsistent, making it more challenging to seamlessly support real-time applications like video conferencing or online gaming.

IPv6:

IPv6 addressing is the next-generation internet protocol that uses a 128-bit address system, providing 340 undecillion unique addresses. This massive expansion resolves the address depletion problem of older IPv4 networks and supports direct, NAT-free device communication with built-in security.

Address Format and Representation:

Unlike IPv4, which uses decimal numbers and periods, an IPv6 address is written in **hexadecimal** and uses **colons**.

- **Structure:** An address is 128 bits long, divided into **8 groups (hextets)**, each containing 4 hexadecimal digits.
- **Example:** 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Address Structure:

An IPv6 address is split into two halves, each consisting of 64 bits: the **Network Prefix** and the **Interface ID**.

- **Network Prefix (First 64 bits):** This is analogous to the network and subnet mask in IPv4. It identifies the geographical region, the Internet Service Provider (ISP), and the local network.
- **Interface ID (Last 64 bits):** This functions like the host part of an IPv4 address, uniquely identifying the specific device interface on your network.

Address Types:

IPv6 eliminates the traditional IPv4 "broadcast" method and introduces new addressing paradigms:

- **Unicast:** Identifies a single interface. Packets sent here go directly to that specific device.
    - *Global Unicast Address (GUA):* The equivalent of a public IPv4 address, globally routable on the internet.
    - *Link-Local Address (LLA):* Automatically generated by devices on the local network. They cannot be routed to the internet and are primarily used for local communication and device discovery.
- **Multicast:** Identifies a group of interfaces. Packets sent to a multicast address are delivered to all members of that group simultaneously.
- **Anycast:** Multiple devices are assigned the same Anycast address. When traffic is sent here, routing protocols deliver the packet to the device that is topologically or physically closest to the sender.

Advantages Over IPv4:

- **Limitless IP space:** 2^{128} possible addresses—enough to assign unique addresses to every conceivable device or Internet of Things (IoT) sensor.
- **Built-in Security:** IPv6 natively enforces **IPSec** (Internet Protocol Security) for built-in encryption and packet authentication.
- **No NAT Required:** Network Address Translation (NAT) isn't needed, allowing true end-to-end connectivity.
- **Efficient Routing:** Simplifies and streamlines data processing by using a fixed 40-byte header, bypassing overhead and improving transmission speeds.

Subnetting:

Subnetting in computer networks is the process of dividing a larger IP network into smaller, more manageable networks called **subnets**. It helps improve network performance, security, and efficient use of IP addresses. **subnetting is used o** Reduces network congestion by limiting broadcast traffic, Improves security by separating different parts of a network, Makes network management easier, uses IP addresses more efficiently. Some terms used in subnetting are:

1. IP Address: A unique address assigned to each device on a network.
2. Subnet Mask: Determines which part of an IP address represents the network and which part represents the host.
3. Network ID: Identifies the subnet.
4. Host ID: Identifies a specific device within the subnet.

Advantages:

- Efficient use of IP addresses.
- Reduces broadcast traffic.
- Improves security.
- Easier network management.
- Better performance.
- Fault isolation.

Disadvantages:

- Complex to configure.
- Requires skilled administrators.
- Increased setup time.
- More routing complexity.
- May require additional networking hardware.
- Risk of configuration errors.

Supernetting:

Supernetting (also called route aggregation or CIDR – Classless Inter-Domain Routing) is the process of combining multiple smaller, contiguous networks into one larger network. It is the opposite of subnetting. **Supernetting is used** to reduces the size of routing tables, improves routing efficiency , simplifies network management, conserves router memory and processing resources.

Advantages

- Smaller routing tables.
- Faster routing decisions.
- Lower memory and CPU usage on routers.
- Easier network administration.

Disadvantages

- Can waste IP addresses if the aggregated block is not fully used.
- Requires contiguous address blocks.
- Misconfiguration can lead to incorrect routing.

UNIT-II

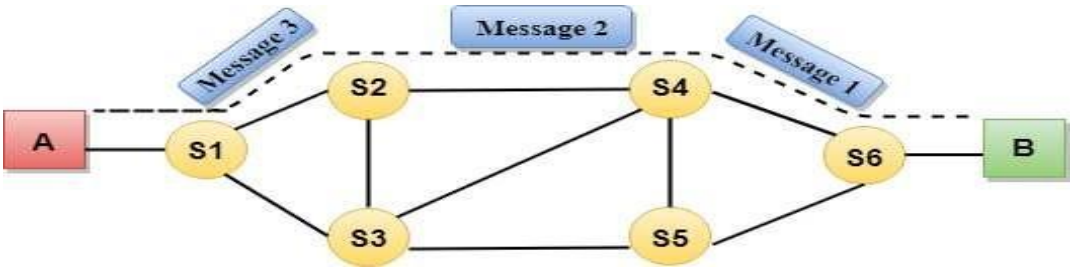
Switching Techniques:

Switching in computer networks is the process of forwarding data from a source to a destination through a series of intermediate nodes (switches or routers). Three main techniques are used: **Circuit Switching**, **Message Switching**, and **Packet Switching**.

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission. Switching technique is used to connect the systems for making one-to-one communication.

Circuit Switching

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.
- Communication through circuit switching has 3 phases: 1. Circuit establishment
  2. Data transfer
  3. Circuit Disconnect



Advantages of Circuit Switching:

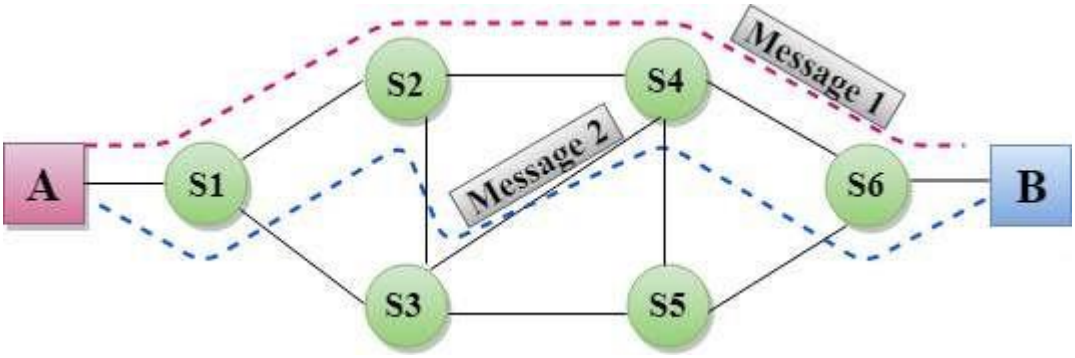
- In the case of Circuit Switching technique, the communication channel is dedicated.
- It has fixed bandwidth.

Disadvantages of Circuit Switching:

- Once the dedicated path is established, the only delay occurs in the speed of data transmission.
- It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
- It is more expensive than other switching techniques as a dedicated path is required for each connection.
- It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
- In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Message Switching:

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.



Advantages of Message Switching:

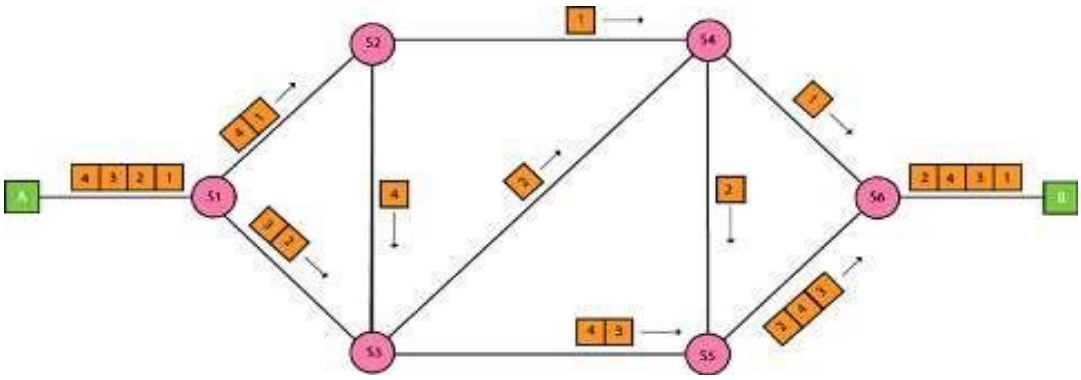
- Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
- Traffic congestion can be reduced because the message is temporarily stored in the nodes.
- Message priority can be used to manage the network.
- The size of the message which is sent over the network can be varied. Therefore, it supports the data of unlimited size.

Disadvantages of Message Switching:

- The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.
- The Long delay can occur due to the storing and forwarding facility provided by the message switching technique.

Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.



Advantages of Packet Switching:

- Cost-effective: In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.
- Reliable: If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- Efficient: Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages of Packet Switching:

- Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
- The protocols used in a packet switching technique are very complex and requires high implementation cost.
- If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered.

Virtual circuit switching

It is a connection-oriented packet-switching technique. Before transmitting data, the network establishes a logical path (virtual circuit) between the source and destination. All packets follow this predetermined route, ensuring in-order delivery and allowing the network to reserve resources and guarantee quality of service.

How It Works:

Virtual circuit switching operates on top of underlying packet-switched networks but mimics the behavior of traditional circuit-switched telephone networks. The communication occurs in three distinct phases:

1. **Setup Phase:** The source sends a "call request" packet through the network to the destination. As it traverses the network, intermediate switches create entries in their routing tables, effectively reserving the path and necessary bandwidth. The destination sends an acknowledgment packet back to the source, completing the circuit establishment.
2. **Data Transfer Phase:** The sender breaks its data into packets. Each packet is stamped with a Virtual Circuit Identifier (VCID) rather than a full destination address. Switches use this ID to instantly route the packet along the pre-established path.
3. **Teardown Phase:** Once all data is successfully transmitted, the source (or destination) sends a special teardown/termination packet. This instructs all intermediate switches to clear their routing tables and free up the reserved network resources.

Types of Virtual Circuits:

- **Switched Virtual Circuits (SVCs):** Dynamically established on-demand for a single communication session and torn down as soon as the session is complete (e.g., a phone call or a file download).
- **Permanent Virtual Circuits (PVCs):** Preconfigured by a service provider to provide a continuous, dedicated link between two endpoints. They eliminate the need for repeated call setups and are commonly used for repeated or continuous usage.

Advantages:

- **Guaranteed Delivery & QoS:** Because resources are reserved during setup, it supports Quality of Service (QoS) guarantees.
- **In-Order Delivery:** Since all packets follow the same path, they arrive at the destination in the exact order they were sent.
- **Faster Forwarding:** Routers do not need to calculate a new route for every single packet, and packet headers only contain a short VCID instead of a massive global IP address.

Disadvantages:

- **Setup Overhead:** Establishing and tearing down the circuit introduces latency before data transmission can actually begin.
- **Vulnerability:** If an intermediate node or router along the predetermined path fails, the entire virtual connection drops, unlike datagram networks which can dynamically route around failures.

Where It Is Used

While pure virtual circuit switching isn't commonly implemented for everyday internet traffic (which generally relies on connectionless datagram switching like IP), its concepts are fundamental to several foundational and modern networking technologies:

- **ATM (Asynchronous Transfer Mode):** Used virtual paths and virtual channels heavily in legacy telecommunication backbones.
- **MPLS (Multiprotocol Label Switching):** A modern evolution of virtual circuits, often called "tag switching," used by internet service providers to direct data across enterprise networks along predetermined paths.

Routing algorithms:

Distance vector, link state, and path vector are all dynamic routing algorithms used in the network layer to find the best path for data packets. Distance vector routers share their distance vectors with neighbors to calculate routes based on hop count, while link state routers flood a complete network map to all routers, allowing each to independently compute the shortest path using an algorithm like Dijkstra's.

Distance vector

Distance-vector routing is a type of dynamic routing protocol where each router maintains a routing table with the "distance" (cost) to reach other nodes and the next hop to use. Routers periodically exchange their routing tables with their immediate neighbors to learn about the network topology and update their own tables with the best-known routes. This is also known as the Bellman-Ford algorithm.

How it works:

- **Initialization**: When a router starts, it sets the distance to itself as 0 and the distance to all other routers as infinity.
- **Sharing information**: Routers share their routing tables with their direct neighbors. This exchange happens either periodically or when a change is detected in the network.
- **Calculating distance**: When a router receives an update from a neighbor, it uses the neighbor's information to recalculate its own routing table. The new distance to a destination is calculated by taking the minimum of the costs through all its neighbors.
- **Convergence**: Routers continue to exchange information until the tables stabilize, and all routers have learned the best paths to all destinations in the network.

Characteristics:

- **Metric**: Uses distance, often measured in hops (the number of routers a packet passes through), to determine the best path.
- **Information**: Each router only sends its distance and next-hop information to its neighbors, not the entire network map.
- **Advantages**: Simple to implement and has a lower processing overhead compared to other protocols.
- **Disadvantages**: Can lead to **counting-to-infinity problems** and has **slower convergence** compared to link-state routing protocols, making it less suitable for large or highly dynamic networks.

Link state:

Link-state routing is a dynamic routing algorithm where each router builds a complete map of the network's topology, not just its immediate neighbors. Routers achieve this by flooding their local link information to all other routers, and each router then independently uses an algorithm like Dijkstra's algorithm to calculate the shortest path to every other destination on the network. Common examples of link-state protocols include OSPF and IS-IS.

How it work :

Neighbor discovery: Each router initially learns about its direct neighbors by sending out "hello" packets.

- **Link-state packet (LSP) creation:** After discovering neighbors, each router creates an LSP containing information about its directly connected links and their cost or status.
- **Flooding:** The LSP is then flooded throughout the entire network, ensuring every router receives a

copy. Routers use a sequence number in the LSP to prevent loops and ensure they have the most recent information.

- **Topology map creation:** Each router stores all the LSPs it receives to build a complete, synchronized map of the entire network's topology.
- **Shortest-path calculation:** Independently, each router runs Dijkstra's algorithm on its topology map to compute the shortest path to every other router.
- **Routing table generation:** The results of the Dijkstra's algorithm are used to build the router's final routing table, which determines the best path for outgoing data packets.

Advantages:

- **Global network view:** Provides routers with a comprehensive understanding of the entire network.
- **Efficient routing:** Enables efficient routing by calculating the shortest path to all destinations.
- **Faster convergence:** Convergence, the process of all routers agreeing on the network topology, is typically faster than in other protocols.

Disadvantages:

- **Higher CPU and memory usage:** Requires more processing power and memory to run Dijkstra's algorithm on a large network.
- **Increased traffic:** Flooding LSPs can create a significant amount of network traffic, especially during network changes.

Routing Protocols:

The Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) are two fundamental routing protocols used in computer networks, but they operate on entirely different principles and are suited for different network environments.

RIP (Routing Information Protocol)

RIP stands for Routing Information Protocol in which distance vector routing protocol is used for data/packet transmission. In the Routing Information Protocol (RIP), the maximum number of Hop is 15, because it prevents routing loops from source to destination. Compared to other routing protocols, RIP (Routing Information Protocol) is poor and limited in size i.e. small network. The main advantage of using RIP is it uses the UDP (User Datagram Protocol).

Advantages of RIP

- **Simplicity:** RIP is very simple and can be used to configure and implement and is thus suitable for use in a network that has less nodes.
- **Low Resource Usage:** RIP also low on complexity, and thus makes an excellent protocol for environments with low processing power.
- **Compatibility:** RIP is supported by all most all the networking devices hence there is the ability to fine tune work on different hardware.

Disadvantages of RIP

- **Scalability Issues:** RIP is not suitable for large network as it has only 15 hops limit for routing the data within the network.

- **Slow Convergence:** RIP 'convergence time' can be long depending on the size of the network and as a result, they can lead to temporary routing loops or sub-optimal routing.
- **Limited Features:** However, basic services provided by RIP do not include such facilities as hierarchical routing or load sharing that complicates the service usage in the networks of a larger scale.

OSPF (Open Shortest Path First):

OSPF stands for Open Shortest Path First which uses a **link-state routing algorithm**. Using the link state information which is available in routers, it constructs the topology in which topology determines the routing table for routing decisions. It supports both variable-length subnet masking and classless inter-domain routing addressing models. Since it uses Dijkstra's algorithm, it computes the shortest path tree for each route. The main advantage of the OSPF (Open Shortest Path first) is that it handles the error detection by itself and it uses multicast addressing for routing in a broadcast domain.

OSPF is an Interior Gateway Protocol (IGP), where routers connect networks using the Internet Protocol (IP). It is a router protocol which is used to find the best path for packets when they are passing through the set of connected networks simultaneously. The main disadvantage of OSPF is that it is difficult than other protocols.

Advantages of OSPF:

- **Scalability:** OSPF is designed for the large network with no restrictions placed upon the hop count.
- **Fast Convergence:** The OSPF is faster to converge, meaning that it takes the least time to restore the network in cases of a breakdown, making the network performances to be even better.
- **Hierarchical Design:** OSPF supports the multi-area routing which assists in minimizing the routing overhead in the networks.
- **Load Balancing:** routing – OSPF has the capability of supporting equal cost multi-path or simply known as ECMP routing for load balancing.

Disadvantages of OSPF:

- **Complexity:** OSPF is much more difficult to configure and to administer as compared to RIP which may be time consuming and might even need the services of a professional.
- **Higher Resource Usage:** OSPF however requires a lot of processing power and memory which might be construed as limiting factors especially for small routers.
- **Initial Configuration Effort:** This is achieved at the cost of having greater initial configuration efforts in the large or hierarchical OSPF networks.

Difference Between RIP and OSPF:

RIP	OSPF
RIP Stands for Routing Information Protocol.	OSPF stands for Open Shortest Path First.

RIP	OSPF
RIP works on the Bellman-Ford algorithm.	OSPF works on Dijkstra algorithm.
It is a Distance Vector protocol and it uses the distance or hops count to determine the transmission path.	It is a link-state protocol and it analyzes different sources like the speed, cost and path congestion while identifying the shortest path.
It is used for smaller size organizations.	It is used for larger size organizations in the network.
It allows a maximum of 15 hops.	There is no such restriction on the hop count.
It is not a more intelligent dynamic routing protocol.	It is a more intelligent routing protocol than RIP.
The networks are classified as areas and tables here.	The networks are classified as areas, sub-areas, autonomous systems, and backbone areas here.
Its administrative distance is 120.	Its administrative distance is 110.
RIP uses UDP(User Datagram Protocol) Protocol.	OSPF works for IP(Internet Protocol) Protocol.
It calculates the metric in terms of Hop Count.	It calculates the metric in terms of bandwidth.
In RIP, the whole routing table is to be broadcasted to the neighbors every 30 seconds by the routers.	In OSPF, parts of the routing table are only sent when a change has been made to it.
RIP utilizes less memory compared to OSPF but is CPU intensive like OSPF.	OSPF device resource requirements are CPU intensive and memory.

RIP	OSPF
It consumes more bandwidth because of greater network resource requirements in sending the whole routing table.	It consumes less bandwidth as only part of the routing table is to send.
Its multicast address is 224.0.0.9.	OSPF's multicast addresses are 224.0.0.5 and 224.0.0.6.

UNIT-III

Wireless and Mobile Networks

Basics of Wireless Communication:

Wireless communication is the transfer of data between devices without using cables. It uses electromagnetic waves such as radio waves, microwaves, or infrared signals.

Components:

1. Sender (Transmitter): Sends data by converting it into wireless signals.
2. Receiver: Receives the wireless signals and converts them back into data.
3. Antenna: Helps transmit and receive wireless signals.
4. Wireless Medium: The free space (air) through which the signals travel.

Types of Wireless Communication:

1. Wi-Fi: Connects devices to the internet over short distances using wireless access points.
2. Bluetooth: Connects nearby devices such as headphones, keyboards, and smartphones.
3. Cellular Networks (3G, 4G, 5G): Provide mobile communication and internet services over large areas.
4. Satellite Communication: Uses satellites to enable communication across countries and remote locations.
5. Infrared (IR): Uses infrared light for very short-range communication, such as TV remote controls.

How Wireless Communication Works:

1. The sender converts digital data into wireless signals.
2. The antenna transmits these signals through the air.
3. The receiver's antenna captures the signals.
4. The receiver converts the signals back into digital data.

Advantages:

1. Mobility: Users can move freely while staying connected.
2. Easy Installation: No cables are required, making setup simple.
3. Cost-Effective: Reduces the cost of wiring and maintenance.
4. Flexibility: New devices can be added easily.
5. Accessibility: Provides internet and network access in many locations.

Disadvantages:

1. Security Risks: Wireless signals can be intercepted if not properly secured.
2. Interference: Other electronic devices and obstacles can affect signal quality.
3. Limited Range: Signal strength decreases with distance.
4. Variable Speed: Network speed may reduce due to congestion or weak signals.

Applications:

1. Wi-Fi Networks: Internet access in homes, schools, and offices.
2. Mobile Communication: Voice calls, messaging, and mobile internet.
3. Bluetooth Devices: Wireless headphones, speakers, keyboards, and mice.
4. Smart Homes (IoT): Connects smart lights, cameras, and home appliances.
5. GPS Navigation: Helps determine location and provide directions.
6. Wireless Printing & File Sharing: Allows devices to print and share files without cables.

Wi-Fi:

Wi-Fi is a wireless networking technology that enables devices (computers, phones, smart gadgets) to connect to a local network (WLAN) and the internet using radio waves instead of physical cables. It uses **radio waves** to transmit data. It is based on the IEEE 802.11 family of standards and is managed by the Wi-Fi Alliance.

Features of Wi-Fi:

1. Provides wireless internet access within a limited area.
2. Uses radio frequency bands such as 2.4 GHz, 5 GHz, and 6 GHz (Wi-Fi 6E/7).
3. Supports multiple devices at the same time.
4. Requires a wireless router or access point.

How Wi-Fi Works:

1. The internet connection reaches a wireless router.
2. The router converts the internet data into radio signals.
3. These signals are transmitted through the air.
4. Wi-Fi-enabled devices receive the signals using their wireless adapters.
5. The devices send and receive data through the router.

Advantages of Wi-Fi:

1. No cables are required.
2. Easy to install and use.
3. Allows users to move freely within the coverage area.
4. Supports multiple devices simultaneously.
5. Cost-effective for homes, schools, and offices.

Disadvantages of Wi-Fi

1. Limited coverage range.
2. Signal interference from walls and other electronic devices.
3. Lower security than wired networks if not properly protected.
4. Speed may decrease when many devices are connected.

Applications of Wi-Fi

1. Home and office internet access.
2. Schools, colleges, and universities.
3. Public places such as airports, hotels, and cafés.
4. Smart home devices (IoT).
5. Video streaming, online gaming, and video conferencing.

Bluetooth:

Bluetooth is a short-range wireless technology that enables computers and devices to exchange data over the 2.4 GHz ISM frequency band. It is widely used to create temporary Wireless Personal Area Networks (WPANs) for connecting peripherals (mice, keyboards) and streaming audio over distances up to 10 meters.

Bluetooth Network Architectures:

Bluetooth networks are built using two primary ad-hoc structures:

- **Piconet:** The basic Bluetooth network unit consisting of one designated "Master" device and up to seven active "Slave" devices connected simultaneously. The master dictates the timing and frequency-hopping sequence for the network.
- **Scatternet:** Formed by linking multiple piconets together. A device can act as a slave in one piconet and a master (or slave) in another, enabling communication across a broader physical area.

Topologies & Operations:

1. **Point-to-Point:** Direct connection between two devices, such as a laptop and a wireless headset.
2. **Point-to-Multipoint:** One master device communicating with several slaves, such as a PC connected to a keyboard, mouse, and printer simultaneously

Bluetooth Versions & Implementations:

1. **Bluetooth Classic (BR/EDR):** Designed for high-reliability, continuous data and audio streaming. It provides speeds up to ~3 Mbps and is the standard for wireless speakers and legacy networking.
2. **Bluetooth Low Energy (BLE):** Optimized for low power consumption, making it ideal for Internet of Things (IoT) devices, health sensors, and smart home tags. It allows devices to operate on coin-cell batteries for months or years.
3. **Bluetooth Mesh:** Used extensively in smart home networks. It allows devices to relay data across multiple nodes (many-to-many topology), allowing a single command to control lighting or security systems across a large facility without needing a central router.

Features of Bluetooth:

- Provides wireless communication over short distances (typically up to **10 meters**, depending on the device class).
- Consumes low power, making it suitable for battery-powered devices.
- Supports secure communication through pairing and encryption.
- Can connect multiple compatible devices.

How Bluetooth Works:

1. Bluetooth-enabled devices search for nearby devices.
2. The devices are **paired** using a secure connection.
3. Once paired, they exchange data through radio waves.
4. Data transmission continues until the connection is disconnected.

Advantages :

1. No cables are required.
2. Easy to set up and use.
3. Low power consumption.
4. Secure communication through device pairing.
5. Widely supported by smartphones, laptops, and other devices.

Disadvantages :

1. Limited communication range.
2. Slower data transfer than Wi-Fi.
3. Can experience interference from other devices using the 2.4 GHz frequency.
4. Supports only a limited number of connected devices at one time.

Cellular Networks:

Cellular networks are wireless communication systems that provide voice calls, text messaging, and internet access through a network of **cell towers (base stations)**. The coverage area is divided into small regions called **cells**, allowing mobile devices to stay connected while moving.

How Cellular Networks Work:

1. A mobile device sends data to the nearest cell tower.
2. The cell tower forwards the data to the mobile network.
3. The network connects the user to the internet or another mobile device.
4. As the user moves, the connection is transferred from one cell tower to another (handover).

Types of Cellular Networks:

1. 2G (Second Generation): Introduced digital mobile communication, replacing analog systems.

Features:

- Supports voice calls and SMS.
- Provides basic internet services (GPRS/EDGE).
- Better call quality than 1G.
- More secure than analog networks.

Advantages:

- Reliable voice communication.
- Low power consumption.
- Affordable technology.

Disadvantages:

- Very slow internet speed.
- Not suitable for video streaming or modern applications.

2. 3G (Third Generation): Introduced faster mobile internet and multimedia services.

Features:

- Supports voice calls, video calls, and internet browsing.
- Higher data speeds than 2G.
- Better support for multimedia applications.

Advantages:

- Faster internet.
- Video calling support.
- Improved mobile browsing.

Disadvantages:

- Slower than 4G and 5G.
- Higher battery consumption than 2G.

3. 4G (Fourth Generation): Provides high-speed internet using LTE (Long-Term Evolution) technology.

Features:

- High-speed internet access.
- Supports HD video streaming and online gaming.
- Better voice quality with VoLTE.
- Lower network latency than 3G.

Advantages:

- Fast downloads and uploads.
- Smooth video streaming.
- Better performance for online applications.

Disadvantages:

- Higher battery usage.
- Requires good network coverage.

4. 5G (Fifth Generation): The latest generation of cellular technology, offering ultra-fast internet, very low latency, and support for millions of connected devices.

Features:

- Extremely high data speeds.
- Very low latency (fast response time).
- Supports IoT (Internet of Things) devices.
- Higher network capacity.

Advantages:

- Ultra-fast internet.
- Excellent for online gaming, AR/VR, and smart cities.
- Supports many connected devices simultaneously.
- Improved network efficiency.

Disadvantages:

- Limited availability in some areas.
- Requires new infrastructure and compatible devices.
- Higher deployment cost.

Wireless LANs:

A Wireless Local Area Network (WLAN) is a network that links devices using radio waves instead of physical cables to form a local area network. Primarily operating under the **IEEE 802.11** (Wi-Fi) standards, it provides high-speed, mobile connectivity for homes, offices, and public hotspots. WLANs typically operate in one of two ways:

- **Infrastructure Mode:** Devices connect through a centralized Access Point (AP), which acts as a bridge to a wired network and provides internet access (common in homes and offices).
- **Ad-Hoc Mode:** Devices communicate directly with one another in a peer-to-peer fashion without a centralized base station (used for temporary, quick file sharing).

Components:

- **Access Point (AP):** The central hub that connects wireless devices to the primary wired network or the internet.
- **Stations (STA):** The end-user devices (laptops, smartphones, IoT sensors) equipped with a wireless network adapter.
- **Distribution System (DS):** The system (often Ethernet cabling) that connects multiple APs together to form a larger coverage area.

Characteristics of Wireless LAN

- **Coverage:** Suitable for small to medium areas.
- **Speed:** Depends on the Wi-Fi standard and signal strength.
- **Mobility:** Users can move within the coverage area without losing connection.
- **Flexibility:** Devices can join or leave the network easily.

Advantages of Wireless LAN

- No network cables are required.
- Easy and quick to install.
- Users can move freely while staying connected.
- Easy to add new devices to the network.
- Reduces installation and maintenance costs.

Disadvantages of Wireless LAN

- Limited coverage area.
- Signal interference from walls and electronic devices.
- Lower security than wired networks if not properly protected.
- Speed may decrease when many devices are connected.

IEEE 802.11 Standards:

IEEE 802.11 is a family of standards developed by the **Institute of Electrical and Electronics Engineers (IEEE)** for **Wireless Local Area Networks (WLANs)**. It defines how devices communicate wirelessly using **Wi-Fi**.

1. IEEE 802.11 (Original): The first Wi-Fi standard, introduced in **1997**.

Features:

- Speed up to **2 Mbps**.
- Operates in the **2.4 GHz** band.
- Used for basic wireless communication.

Advantages:

- Introduced wireless networking.
- Simple and reliable for basic use.

Disadvantages:

- Very low speed.
- Obsolete in modern networks.

2. IEEE 802.11a: Introduced in **1999**, offering higher speed than the original standard.

Features:

- Speed up to **54 Mbps**.
- Uses the **5 GHz** frequency band.
- Less interference than 2.4 GHz.

Advantages:

- Faster data transfer.
- Reduced interference.

Disadvantages:

- Shorter coverage range.
- Less compatible with older devices.

3. IEEE 802.11b: A widely used Wi-Fi standard introduced in **1999** for homes and offices.

Features:

- Speed up to **11 Mbps**.
- Uses the **2.4 GHz** band.
- Better coverage than 802.11a.

Advantages:

- Longer range.
- Low cost.

Disadvantages:

- Slower speed.
- More interference from other 2.4 GHz devices.

4. IEEE 802.11g: An improved version of 802.11b introduced in **2003**.

Features:

- Speed up to **54 Mbps**.
- Uses the **2.4 GHz** band.
- Compatible with 802.11b devices.

Advantages:

- Higher speed.
- Good coverage.

Disadvantages:

- Can experience interference in the 2.4 GHz band.

5. IEEE 802.11n (Wi-Fi 4): Introduced in **2009**, providing faster speed and better coverage.

Features:

- Speed up to **600 Mbps**.
- Operates on **2.4 GHz and 5 GHz**.
- Uses **MIMO (Multiple Input Multiple Output)** technology.

Advantages:

- High speed.
- Better range.
- Supports multiple users.

Disadvantages:

- Performance depends on compatible devices.

6. IEEE 802.11ac (Wi-Fi 5): Introduced in **2013** to provide very high-speed wireless communication.

Features:

- Speed up to **6.9 Gbps**.
- Operates only on the **5 GHz** band.
- Supports wider channels and MU-MIMO.

Advantages:

- Very fast internet.
- Excellent for HD streaming and online gaming.

Disadvantages:

- Shorter range than 2.4 GHz.
- Requires compatible devices.

7. IEEE 802.11ax (Wi-Fi 6): The latest widely used Wi-Fi standard, introduced in **2019**, designed for faster and more efficient wireless communication.

Features:

- Speed up to **9.6 Gbps**.
- Operates on **2.4 GHz and 5 GHz** (6 GHz with Wi-Fi 6E).
- Better performance in crowded networks.

Advantages:

- Higher speed.
- Lower latency.
- Better battery efficiency.
- Supports many connected devices.

Disadvantages:

- Requires Wi-Fi 6 compatible devices.
- Higher installation cost.

Mobile IP :

Mobile IP is a communication protocol that allows a mobile device to move between different networks while maintaining its permanent IP address. It prevents dropped sessions or connection losses by routing data through the device's home network, enabling seamless internet transitions.

Components:

- **Mobile Node (MN):** The mobile device (e.g., smartphone, laptop) changing its point of attachment to the internet.
- **Home Agent (HA):** A router on the mobile node's home network that maintains the current location of the mobile device and intercepts packets addressed to it.
- **Foreign Agent (FA):** A router on the visited (foreign) network that provides routing services to the mobile node.

The 3-Phase Process:

1. **Agent Discovery:** The Home Agent and Foreign Agent broadcast periodic advertisements to announce their presence and services. The Mobile Node listens to these messages to determine if it is on its home network or a foreign network.
2. **Registration:** When visiting a foreign network, the Mobile Node obtains a temporary **Care-of Address (CoA)**. It then registers this new address with its Home Agent, ensuring the Home Agent knows exactly where to forward its traffic.
3. **Data Transfer:**
   - When a remote device sends data to the Mobile Node, the data first goes to the Home Agent.
   - The Home Agent encapsulates the packet (a process called **tunneling**) and forwards it to the Mobile Node's Care-of Address.
   - The Foreign Agent (or the Mobile Node directly) decapsulates the packet and delivers it.

Limitations & Challenges:

- **Triangle Routing:** Because all data must route through the Home Agent, it can result in inefficient, longer paths (e.g., from the sender → Home Agent → Foreign Agent).
- **Security:** Tunneling packets across networks makes the system vulnerable to redirection attacks and requires robust authentication to secure data packets.

Handoff Mechanisms:

A handoff (or handover) in computer networking is the process of transferring an ongoing data session or call from one base station, access point, or channel to another without losing connectivity. It ensures seamless mobility as a user moves between network coverage areas. The handoff process generally follows three main stages:

1. **Initiation:** The mobile device or network evaluates signal strength, interference, or traffic capacity to determine if a switch is necessary.
2. **Generation:** The network allocates resources and establishes a new connection.
3. **Execution:** The data flow is officially transferred from the old connection to the new path.

Common Handoff Types

- **Hard Handoff:** Uses a "break-before-make" policy, where the connection with the old base station is completely disconnected before the new one is established. It causes a brief interruption but is highly efficient.
- **Soft Handoff:** Uses a "make-before-break" policy. The mobile device temporarily maintains connections with both base stations simultaneously to guarantee continuous, high-quality service.

Advantages:

- **Seamless Connectivity:** Prevents dropped calls and interrupted data sessions while moving across large distances.
- **Load Balancing:** Allows the network to transfer users from congested cells to underutilized cells, maximizing overall capacity.
- **Power Optimization:** Helps mobile devices reduce power consumption, as they do not have to maintain a high-power link with a distant, fading base station.

Disadvantages:

- **Handoff Latency:** The switching process introduces a delay (latency), which can cause temporary lagging or degrade Real-Time Protocol (RTP) streaming.
- **Resource Overhead:** Increases signaling traffic and operational load on the core network due to continuous monitoring and coordination.
- **Complexity:** Soft handoffs require more hardware and consume multiple channels at once, making them significantly more expensive to deploy. Conversely, hard handoffs risk high call-drop rates if the transition is delayed.

UNIT-IV
NETWORK SECURITY AND CRYPTOGRAPHY

- Modern computer networks have become the backbone of communication, business, education, healthcare, banking, e-commerce, cloud computing, and industrial automation. With the rapid growth of the Internet, mobile computing, cloud services, 5G technology, and the Internet of Things (IoT), networks have become highly interconnected and increasingly complex. While these advancements improve efficiency and connectivity, they also expose networks to a wide range of security threats.
- Network security is the practice of protecting network infrastructure, devices, applications, and data from unauthorized access, misuse, modification, destruction, or disruption. The objective of network security is to ensure that information remains secure during storage, processing, and transmission.
- The fundamental goals of network security are represented by the **CIA Triad**:
  1. Confidentiality: Ensures that information is accessible only to authorized users.
  2.Integrity: Ensures that data remains accurate, complete, and unaltered.
  3.Availability: Ensures that network resources and services are available whenever required by authorized users.
- As cyber threats continue to evolve, organizations must implement robust security policies, cryptographic techniques, authentication mechanisms, firewalls, and continuous monitoring to protect modern networks.

Security Challenges in Modern Networks:

Security challenges are vulnerabilities, threats, and risks that compromise the confidentiality, integrity, and availability of network resources. These challenges arise due to technological advancements, increasing network connectivity, software vulnerabilities, human errors, and sophisticated cyberattacks.
Modern networks face security challenges because they support:

- Cloud computing
- Internet of Things (IoT)
- Wireless communication
- Mobile devices
- Remote access
- Online transactions
- Artificial Intelligence (AI)
- Big Data applications

These technologies expand the attack surface and make securing networks more difficult.

Major Security Challenges in Modern Networks are:

1.Malware Attacks:

Malware (Malicious Software) is software intentionally designed to damage computer systems, steal confidential information, or disrupt network operations.

Types of Malware

(a) Virus

A virus attaches itself to executable files and spreads when the infected program is executed.

Characteristics

- Requires user interaction.
- Corrupts files.
- Slows system performance.

(b) Worm

A worm is a self-replicating malware that spreads automatically through computer networks without user intervention.

Characteristics

- Consumes network bandwidth.
- Spreads rapidly.

- Causes network congestion.

(c) Trojan Horse

A Trojan disguises itself as legitimate software but secretly provides unauthorized access to attackers.

(d) Spyware

Spyware secretly collects sensitive user information such as passwords, browsing history, and banking credentials.

(e) Ransomware

Ransomware encrypts files and demands payment from the victim to restore access.

Effects of Malware

- Data corruption
- Data theft
- System crashes
- Unauthorized access
- Financial losses
- Business interruption

Prevention

- Install antivirus software.
- Update operating systems regularly.
- Avoid downloading software from untrusted sources.
- Scan removable media before use.
- Educate users about cyber threats.

2. Phishing Attack:

Phishing is a cyberattack in which attackers impersonate trusted organizations to trick users into revealing sensitive information such as usernames, passwords, or banking details.

Types:

- Email Phishing
- Spear Phishing
- Whaling
- SMS Phishing (Smishing)
- Voice Phishing (Vishing)

Example

A fake email pretending to be from a bank requests the user to verify account details through a fraudulent website.

Effects

- Identity theft
- Financial fraud
- Data leakage

Prevention

- Verify sender information.
- Do not click suspicious links.
- Use Multi-Factor Authentication (MFA).
- Conduct user awareness training.

3.Distributed Denial of Service (DDoS) Attack:

A Distributed Denial of Service (DDoS) attack attempts to make a network or server unavailable by overwhelming it with massive traffic generated from multiple compromised devices (botnets).

Effects

- Website downtime
- Slow network performance
- Service disruption
- Financial loss

Prevention

- Firewalls
- Traffic filtering
- Content Delivery Networks (CDN)
- DDoS mitigation services

4.Data Breach:

A data breach occurs when confidential or sensitive information is accessed, copied, or disclosed without authorization.

Causes

- Weak passwords
- Software vulnerabilities
- Insider attacks
- Phishing
- Poor access control

Consequences

- Loss of customer trust
- Financial penalties
- Identity theft
- Legal consequences

Prevention

- Data encryption
- Strong authentication
- Regular security audits
- Access control mechanisms

5.Insider Threat:

An insider threat originates from trusted individuals such as employees, contractors, or business partners who intentionally or accidentally compromise network security.

Types:

1.Malicious Insider: Intentionally steals confidential information.

2.Negligent Insider: Accidentally exposes sensitive information through carelessness.

Prevention

- Principle of least privilege
- User activity monitoring
- Security awareness training
- Role-based access control

6.Cloud Security Challenges

Cloud computing stores applications and data on remote servers accessible via the Internet.

Challenges

- Data leakage
- Misconfigured cloud services
- Unauthorized access
- Insider threats
- Insecure APIs

Security Measures

- Encryption
- Identity and Access Management (IAM)
- Multi-Factor Authentication
- Regular backups

7.Internet of Things (IoT) Security

IoT devices include smart sensors, cameras, wearable devices, industrial controllers, and smart home appliances.

Challenges

- Weak authentication
- Default passwords
- Outdated firmware
- Limited computing resources
- Device hijacking

Solutions

- Firmware updates
- Secure authentication
- Encryption
- Network segmentation

8.Wireless Network Security

Wireless networks transmit data using radio waves, making them vulnerable to interception.

Common Threats

- Packet sniffing
- Rogue Access Point
- Evil Twin Attack
- Password cracking
- Session hijacking

Prevention

- WPA3 encryption
- Strong Wi-Fi passwords
- VPN
- Disable unused wireless services

Weak Authentication:

Weak authentication increases the risk of unauthorized access.

Causes

- Weak passwords
- Password reuse
- Shared accounts
- Lack of Multi-Factor Authentication

Prevention

- Strong password policy
- Multi-Factor Authentication
- Password managers
- Biometric authentication

9.Network Misconfiguration:

Improper configuration of routers, switches, firewalls, or servers creates security vulnerabilities.

Examples

- Open ports
- Weak firewall rules
- Default administrator passwords
- Unpatched systems

Prevention

- Regular configuration audits
- Patch management
- Security policies
- Automated configuration tools

10. Advanced Persistent Threats (APT):

An Advanced Persistent Threat (APT) is a sophisticated cyberattack in which attackers gain unauthorized access to a network and remain undetected for a long period.

Characteristics

- Highly targeted
- Long-term attack
- Difficult to detect
- Continuous data theft

Prevention

- Continuous monitoring
- Threat intelligence
- Endpoint Detection and Response (EDR)
- Intrusion Detection Systems (IDS)

Symmetric and Asymmetric Cryptography:

- **Cryptography** is the science of protecting information by converting readable data (**plaintext**) into an unreadable form (**ciphertext**) using mathematical algorithms. It ensures secure communication over computer networks by providing **confidentiality, integrity, authentication, and non-repudiation**.
- The two main types of cryptography are:
  1. **Symmetric Cryptography (Secret Key Cryptography)**
  2. **Asymmetric Cryptography (Public Key Cryptography)**

1.Symmetric Cryptography (Secret Key Cryptography) :

Symmetric cryptography is a method in which **the same secret key is used for both encryption and decryption**. The sender and receiver must possess the same key before communication begins.

Working Principle:

1. The sender converts plaintext into ciphertext using a secret key.
2. The ciphertext is transmitted through the network.
3. The receiver uses the same secret key to decrypt the ciphertext.
4. The original plaintext is recovered.

Characteristics:

- Uses only one secret key.
- Fast and efficient.
- Suitable for encrypting large amounts of data.
- Requires secure key distribution.

Advantages:

1. **High speed**: Symmetric algorithms perform encryption and decryption faster compared to asymmetric algorithms.
2. **Low Computational Requirement:** They require less memory and processing power.
3. **Efficient Data Encryption:** Suitable for encrypting large files and continuous data transmission.
4. **Simple Implementation:** The algorithms are easier to implement and manage.

Disadvantages:

1. **Key Distribution Problem:** Securely sharing the secret key between users is difficult.
2. **Poor Scalability:** A large number of users require many different keys.
3. **Key Compromise Risk:** If the secret key is exposed, the encrypted data becomes insecure.

Applications:

- Data storage encryption
- VPN communication
- Wireless network security
- Database security
- File encryption
- Secure communication systems

2.Asymmetric Cryptography:

Asymmetric cryptography is a cryptographic technique that uses two different but mathematically related keys for encryption and decryption. It is also known as Public Key Cryptography.

The two keys are:

1. **Public Key:** A key that is available publicly and can be shared with anyone.
2. **Private Key:** A secret key that is kept only by the owner.

Features:

- Uses a pair of keys.
- Public key can be openly distributed.
- Private key remains confidential.
- Provides authentication and digital signature support.
- More secure for key exchange.

Advantages:

1. **Secure Key Distribution:** No need to exchange a secret key before communication.
2. **Authentication:** Provides user authentication through digital signatures.
3. **Non-repudiation:** Ensures that the sender cannot deny sending a message.
4. **Improved Security:** The private key is never shared with other users.

Disadvantages:

1. **Slow Processing:** Encryption and decryption are slower compared to symmetric methods.
2. **High Computational Cost:** Requires more processing power and memory.
3. **Not Suitable for Large Data:** Mainly used for key exchange and authentication.

Applications:

- SSL/TLS security
- Digital signatures
- Secure email communication
- Online banking security
- Public Key Infrastructure (PKI)
- Secure authentication systems

Network Authentication Mechanisms:

Network Authentication is the process of verifying the identity of a user, device, or system before allowing access to network resources. It ensures that only authorized users can access confidential information and network services.

Authentication is one of the fundamental security services of a computer network. It protects networks from unauthorized access, identity theft, and malicious activities.

Objectives:

The main objectives of network authentication are:

1. **Identity Verification** :Confirms that the user or device is genuine.
2. **Access Control** :Allows only authorized users to access network resources.
3. **Data Protection** :Prevents unauthorized users from accessing sensitive information.
4. **Secure Communication** :Establishes trust between communicating entities.
5. **Prevention of Attacks** :Protects against impersonation, replay attacks, and unauthorized access.

Authentication Factors: Authentication mechanisms are generally based on one or more authentication factors.

1. Knowledge Factor: This method uses information known only by the user.

Examples: Password , PIN , Security questions

Advantages:

- Simple to implement.
- Low cost.

Limitations:

Passwords can be guessed, stolen, or compromised.

2. Possession Factor: This method uses a physical object owned by the user.

Examples: Smart card , Security token , Mobile authentication device ,One-Time Password (OTP generator)

Advantages:

- Provides stronger security than passwords.
- Difficult for attackers to duplicate.

Limitations:

- Device may be lost or stolen.

3. Inherence Factor: This method uses unique biological characteristics of a user.

Examples: Fingerprint recognition , Face recognition , Voice recognition

Advantages:

- Highly secure.
- Difficult to duplicate.

Limitations:

- Requires specialized hardware.
- Privacy concerns.

Types of Network Authentication Mechanisms:

The commonly used network authentication mechanisms are:

1. Password-Based Authentication
2. Multi-Factor Authentication (MFA)
3. Digital Certificate Authentication
4. Kerberos Authentication
5. Biometric Authentication
6. Token-Based Authentication
7. IEEE 802.1X Authentication

1.Password-Based Authentication:

Password-based authentication is the simplest authentication mechanism where a user proves identity by providing a username and password.

Working

1. User enters username and password.
2. The system compares the entered password with the stored password value.
3. If the credentials match, access is granted.

Advantages

- Easy to implement.
- Low cost.
- Widely supported.

Disadvantages

- Vulnerable to password guessing attacks.
- Passwords may be stolen through phishing.
- Users may choose weak passwords.

Applications

- Computer login systems
- Web applications
- Network access systems

2.Multi-Factor Authentication (MFA): Multi-Factor Authentication is a security mechanism that requires two or more independent authentication factors to verify a user's identity.

Factors Used

1. Something you know → Password/PIN
2. Something you have → OTP token/smart card
3. Something you are → Biometric information

Advantages

- Provides stronger security.
- Reduces risk of account compromise.
- Protects against stolen passwords.

Applications

- Online banking
- Cloud services
- Enterprise networks

3. Digital Certificate Authentication: Digital certificate authentication uses electronic certificates to verify the identity of users, devices, or servers.

A digital certificate contains:

- Owner's identity
- Public key
- Certificate authority information
- Digital signature

Working

1. A user or server presents a digital certificate.
2. Certificate Authority (CA) verifies the certificate.
3. The identity is authenticated.
4. Secure communication is established.

Components: 1.Certificate Authority (CA): An organization that issues and verifies digital certificates. **2.Public Key Infrastructure (PKI):** A framework used for managing digital certificates and encryption keys.

4.Kerberos Authentication: Kerberos is a **network authentication protocol** that uses secret-key cryptography to provide secure authentication over an insecure network. It was developed by MIT.

Main Components:

1. Authentication Server (AS)

- Verifies the user's identity.

2. Ticket Granting Server (TGS)

- Provides service tickets to users.

3. Client and Server

- Users and network services requesting authentication.

Working of Kerberos

1. User requests authentication from Authentication Server.
2. Authentication Server provides a Ticket Granting Ticket (TGT).
3. User presents TGT to Ticket Granting Server.
4. TGS provides a service ticket.
5. User accesses the requested network service.

Advantages

- Password is not transmitted over the network.
- Provides mutual authentication.
- Prevents replay attacks.

Applications

- Enterprise networks
- Windows Active Directory
- Distributed systems

5.Biometric Authentication: Biometric authentication verifies a user's identity based on unique physical or behavioral characteristics.

Types:

Physical Biometrics

- Fingerprint
- Iris
- Face recognition

Behavioral Biometrics

- Voice pattern
- Signature dynamics

Advantages

- High security.
- Difficult to forge.
- User-friendly.

Disadvantages

- Expensive implementation.
- Privacy concerns.
- Biometric data cannot be changed if compromised.

6.Token-Based Authentication: Token-based authentication uses a security token to verify user identity without repeatedly sending passwords.

Types of Tokens

1. Hardware Token : Physical security device.
2. Software Token : Mobile applications generating OTPs.
3. Access Token : Digital token used by applications and services.

Applications

- VPN authentication
- Cloud applications
- Remote access systems

7.IEEE 802.1X Authentication: IEEE 802.1X is a port-based network access control mechanism used to authenticate devices before allowing network access.

Components:

1. Supplicant: Client device requesting network access.

2. Authenticator: Network switch or wireless access point.

3. Authentication Server: Usually a RADIUS server.

Working

1. Device connects to network.
2. Authentication request is sent.
3. Authentication server verifies credentials.
4. Network access is granted or denied.

Applications

- Enterprise LAN security
- Wireless network security
- Campus networks

Firewalls:

A Firewall is a network security system, available as hardware or software, that monitors and controls incoming and outgoing traffic based on predefined rules. It acts like a security guard, filtering data packets to either:

- **Accept:** Allow the traffic.
- **Reject:** Block with an error response.
- **Drop:** Block silently without response.

Importance

- **Prevent Unauthorized Access:** Like a locked door with a guard, only trusted users and traffic are allowed through.
- **Block Malicious Traffic:** Harmful data such as viruses, phishing attempts, or denial-of-service (DoS) attacks are stopped before reaching the system.
- **Protect Sensitive Information:** Safeguards personal and business data from theft or accidental leaks.
- **Control Network Usage:** Enforces policies such as parental controls, workplace restrictions, or government filtering.
- **Mitigate Insider Risks:** Detects suspicious applications or data exfiltration attempts from within the network.

Working of Firewall

A firewall inspects all incoming and outgoing traffic and decide whether to allow or block it.

1. All data packets entering or leaving the network must first pass through the firewall.
2. The firewall examines each packet against predefined security rules set by the organization.
3. If the packet matches safe rules, it is allowed; if it is suspicious, blacklisted, or contains malicious content, it is blocked.
4. Blocked or unusual traffic is recorded in logs, and real-time alerts may be generated for serious threats.
5. Since it is not possible to define every rule, the firewall applies a default policy (accept, reject, or drop). Setting the default policy to drop or reject is considered best practice to prevent unauthorized access.

Types of Firewall:

Firewalls can be categorized based on their generation:

1. Network Placement

- Packet Filtering Firewall
- Stateful Inspection Firewall
- Proxy Firewall (Application Level)
- Circuit-Level Gateway
- Web Application Firewall (WAF)
- Next-Generation Firewall (NGFW)

2. Systems Protected

- Network Firewall
- Host-Based Firewall

3. Data Filtering Method

- Perimeter Firewall
- Internal Firewall
- Distributed Firewall

4. Form Factors

- Hardware Firewall
- Software Firewall

VPN:

A Virtual Private Network (VPN) is a security technology that creates an encrypted tunnel between your device and a VPN server over the internet, so your traffic travels privately and your real IP address is hidden.

- **Privacy protection:** Hides your IP and encrypts traffic, so ISPs, advertisers, and third parties can't easily monitor your browsing.
- **Security on public Wi-Fi:** Encryption protects logins and personal data on unsafe networks (airports, cafes).
- **Bypass geo-restrictions:** Changes your apparent location by routing through another region's server, unlocking region-limited sites or services.
- **Reduce ISP throttling:** Since traffic is encrypted, ISPs can't easily identify specific activities (streaming/gaming) to selectively slow them.
- **Secure remote access:** Let employees connect to internal company resources securely from outside the organization.

Working:

1. Connection establishment: When you turn on the VPN, the VPN client authenticates you and sets up a secure session with a VPN server.

2. Data encryption: Your outgoing traffic is encrypted using cryptographic algorithms, so intercepted packets look like unreadable ciphertext to hackers, ISPs, or attackers on public Wi-Fi.

3. Traffic redirection (tunnelling): The encrypted traffic is sent through the tunnel to the VPN server, and the VPN server replaces your real IP with its own public IP, hiding your identity/location from the destination site.

4. Decryption and forwarding: The VPN server decrypts the traffic and forwards it to the actual website/service; replies come back to the VPN server and then travel back to you through the same encrypted tunnel.

5. End-to-end protection: This tunnel provides privacy (confidentiality), helps maintain integrity against tampering during transit, and improves anonymity by masking your IP.

Types :

A) Types based on usage (deployment)

A deployment-based VPN type describes who is connecting and what network is being protected.

- **Remote Access VPN:** It allows an individual user to securely connect to a private network over the internet, and it is widely used by employees working remotely.
- **Site-to-Site VPN:** It securely connects two or more separate networks, such as a head office and branch offices, so internal communication remains protected across locations.
- **Mobile VPN:** It is designed for mobile users and keeps the VPN session stable even when the device switches between Wi-Fi and cellular networks.
- **MPLS VPN:** It is a provider-managed enterprise WAN solution that offers scalable connectivity and traffic prioritization, but it typically does not provide end-to-end encryption by default.

B) Types based on protocols (tunnelling technology)

Protocol-based VPN types describe how the tunnel is created and secured, and they affect speed, security, and compatibility.

- **PPTP:** It is an older protocol that can be fast, but it provides weak security, so it is mainly used only for legacy systems.
- **L2TP/IPsec:** It combines L2TP tunnelling with IPsec encryption, which improves security, but it can add performance overhead.
- **OpenVPN:** It is an open-source protocol that uses SSL/TLS for encryption, and it is widely adopted because it provides strong security and flexibility.
- **IKEv2/IPsec:** It is a secure and fast protocol that works very well on mobile devices because it reconnects quickly when network conditions change.

VPN Protocols:

1) OpenVPN: OpenVPN is an open-source VPN protocol that uses SSL/TLS to provide secure authentication and encryption.

- It can run on UDP for better speed and on TCP for higher reliability on unstable networks.
- It supports strong encryption such as AES-256 and ChaCha20 to protect confidentiality and integrity.
- It works on most operating systems and often passes through NAT and firewalls more easily than older protocols.
- It is commonly used for secure remote access, privacy, and bypassing network restrictions.

2) WireGuard: WireGuard is a modern VPN protocol designed to be lightweight, fast, and easier to secure due to a small codebase.

- It mainly uses UDP and modern cryptography like ChaCha20, Poly1305, and BLAKE2s.
- It delivers high speed and low latency, which makes it suitable for streaming and online gaming.
- It works very well on mobile devices because it reconnects quickly when the network changes.

3) IKEv2/IPsec: IKEv2/IPsec uses IKEv2 to set up secure tunnels and IPsec to provide encryption and integrity.

- It automatically re-establishes the VPN session when switching between Wi-Fi and mobile data.
- It supports strong encryption like AES-256 and can use Perfect Forward Secrecy for better long-term security.
- It is widely used in enterprise environments for secure remote access.

4) L2TP/IPsec: L2TP/IPsec combines L2TP tunnelling with IPsec encryption to secure traffic.

- It provides better security than PPTP, but it uses double encapsulation, which can reduce throughput.
- It is supported on many platforms, so it is useful for legacy and cross-platform setups.
- It is often chosen only when newer protocols are not available.

5) PPTP: PPTP is an older VPN protocol that is fast but not secure by modern standards.

- It has low overhead, which improves speed, but it uses weak encryption and is vulnerable to attacks.
- It is not recommended for sensitive data and should be used only for legacy compatibility.

6) SSTP: SSTP is a Microsoft VPN protocol that tunnels traffic over SSL/TLS using TCP port 443.

- It can pass through many firewalls because it looks similar to normal HTTPS traffic.
- It offers strong security, especially on Windows, but it has limited support on non-Windows platforms.
- It is a good choice when networks block common VPN protocols.

Drawbacks of Using VPN:

- **Reduced internet speed:** Encryption and routing traffic through remote servers can increase latency and lower connection speeds.
- **Inconsistent provider quality:** Some VPN providers may use weak encryption or maintain user logs, which can compromise privacy.
- **Blocking and restrictions:** Certain websites, streaming services, and countries actively detect and block VPN traffic, limiting access.
- **Configuration complexity:** Advanced setups and manual configurations may require technical expertise, particularly in enterprise environments.
- **Cost factors:** Free VPNs often impose limits on bandwidth and features, while reliable premium services require ongoing subscription fees.

Advantages of VPN:

- Secure communication over the Internet
- Strong encryption
- Supports remote work
- Protects confidential information
- Cost-effective alternative to leased lines
- Enables secure branch office connectivity
- Enhances privacy
- Supports cloud connectivity

IDS/IPS:

Intrusion Prevention System (IPS):

An Intrusion Prevention System (IPS) actively monitors network and system traffic to detect and block malicious activity in real time. It extends traditional IDS capabilities by not only identifying threats but also automatically preventing attacks before they cause damage.

- Detects and blocks attacks such as malware, DoS/DDoS, SQL injection, and brute-force attacks.
- Blocks malicious traffic by dropping packets, resetting connections, or blocking IP addresses.
- Provides real-time alerts, logs, and packet inspection to improve network security

Working:

An IPS works by analyzing network traffic in real-time and comparing it against known attack patterns and signatures. When the system detects suspicious traffic, it blocks it from entering the network.

1. Inline Deployment: An IPS is typically deployed in-line, meaning it is placed directly in the path of network traffic between internal networks and external sources (such as the internet).

2. Traffic Preprocessing: Before deep inspection begins, the IPS preprocesses incoming traffic to ensure it's correctly interpreted:

- **Traffic Normalization:** It standardizes traffic formats to prevent attackers from using encoding tricks to evade detection.

- **Packet Reassembly**: The IPS reassembles fragmented packets to ensure no data is missed and malicious content isn't hidden in fragments.

3. Layered Packet Inspection: An IPS performs deep packet inspection (DPI) to understand both the structure and intent behind the network traffic. This analysis occurs at multiple layers of the OSI model:

- **Network Layer:** Checks packet origins and destinations.
- Transport Layer: Examines the reliability and integrity of the connections.
- Application Layer: Inspects the type of data being transmitted (e.g., login credentials, file transfers).

4. Detection Mechanisms: The IPS uses various detection mechanisms to identify threats:

- **Signature-Based Detection**: Compares traffic against known attack patterns or signatures (like fingerprints of known malware or exploits).
- **Anomaly-Based Detection:** Flags any behavior that deviates from normal network activity, such as sudden spikes in traffic or unusual request patterns.
- **Behavior-Based Detection:** Monitors and tracks actions over time, identifying suspicious patterns like repeated failed login attempts or unauthorized access attempts.
- **Policy-Based Detection:** Enforces custom rules defined by administrators (e.g., blocking traffic from specific countries or blocking certain file types).

5. Automated Response Actions: Once a threat is detected, the IPS can immediately take action to mitigate it:

- **Drop Malicious Packets:** Discards harmful traffic before it reaches its target.
- **Block Source IP:** Prevents further connections from the attacker's IP address.
- Terminate Sessions: Ends suspicious or unauthorized sessions.
- **Trigger Alerts/Logs:** Generates alerts or logs for the administrator to review.
- **Update Firewall Rules:** Automatically adjusts firewall settings to block traffic from malicious sources.

6. Tuning and Maintenance: An IPS requires regular updates and fine-tuning to stay effective:

- **Update Signatures:** Regular updates are needed to add new attack signatures and detection patterns.
- **Reduce False Positives:** Fine-tuning helps minimize alerts for non-malicious traffic, ensuring the system only triggers legitimate threats.
- **Optimize Performance:** Adjust settings to ensure the IPS can handle high traffic loads without performance degradation.

Types:

IPS systems can be classified into the following types based on their monitoring focus and deployment:

- **Network-Based Intrusion Prevention System (NIPS)**: Monitors and inspects network traffic in real time to detect and block malicious packets before they reach target systems.
- **Host-Based Intrusion Prevention System (HIPS)**: Protects individual endpoints by monitoring system calls, processes, file integrity, and inbound/outbound host traffic.
- **Wireless Intrusion Prevention System (WIPS)**: Secures wireless networks by detecting and preventing rogue access points, unauthorized devices, and wireless protocol attacks.
- **Network Behavior Analysis (NBA)**: Analyzes network traffic patterns to identify abnormal behavior such as DDoS attacks, malware propagation, and unusual traffic flows.

Benefits:

An IPS is an essential tool for network security. Here are some reasons why:

- **Protection Against Known and Unknown Threats**: An IPS can block known threats and also detect and block unknown threats that haven't been seen before.
- **Real-Time Protection**: An IPS can detect and block malicious traffic in real-time, preventing attacks from doing any damage.
- **Compliance Requirements**: Many industries have regulations that require the use of an IPS to protect sensitive information and prevent data breaches.
- **Cost-Effective**: An IPS is a cost-effective way to protect your network compared to the cost of dealing with the aftermath of a security breach.

- **Increased Network Visibility**: An IPS provides increased network visibility, allowing you to see what's happening on your network and identify potential security risks.

Intrusion Detection System (IDS):

An Intrusion Detection System (IDS) is a security tool that monitors network traffic or system activities to detect unauthorized access or suspicious behavior. Think of it as a "watchdog" that looks for signs of cyber attacks or security breaches, helping administrators respond quickly before damage occurs.

- Detects threats such as malware, port scanning, DoS/DDoS attacks and brute-force attacks.
- Supports both Host-based IDS (HIDS) and Network-based IDS (NIDS).
- Uses signature-based, anomaly-based and behavior-based methods to detect threats.
- Generates alerts and logs that help security teams investigate and respond to incidents.

Common Methods of Intrusion:

- **Address Spoofing:** Hiding the source of an attack by using fake or unsecured proxy servers making it hard to identify the attacker.
- **Fragmentation**: Sending data in small pieces to slip past detection systems.
- **Pattern Evasion:** Changing attack methods to avoid detection by IDS systems that look for specific patterns.
- **Coordinated Attack:** Using multiple attackers or ports to scan a network, confusing the IDS and making it hard to see what is happening.

Working of IDS

An IDS operates by monitoring network traffic or system activities to detect suspicious or malicious actions. Here's how it works:

- **Traffic Monitoring:** The IDS captures and monitors data flowing through the network.
- **Pattern Matching:** It compares the incoming data against a set of predefined rules or patterns that could indicate potential attacks or intrusions.
- **Alerting:** If the system detects an activity that matches any of these patterns, it triggers an alert to notify the system administrator.
- **Administrator Action:** Upon receiving the alert, the administrator can investigate the source of the potential attack and take necessary actions to mitigate the risk.

Classification of IDS

There are several types of IDS, categorized based on where they operate or how they detect intrusions:

1. Network Intrusion Detection System (NIDS)

- **Function:** NIDS is deployed at strategic points within the network to monitor traffic from all devices.
- **Usage:** It examines passing traffic across subnets and compares it against known attack signatures. When an attack is detected, it alerts the administrator.

2.Host Intrusion Detection System (HIDS)

- **Function:** HIDS operates on individual devices (hosts) within the network.
- **Usage:** It monitors traffic and file integrity on that specific host, comparing current system files with previous snapshots to detect unauthorized changes.

3. Hybrid Intrusion Detection System

- **Function:** A hybrid IDS combines multiple IDS types to provide more comprehensive protection.
- **Usage:** It integrates host-based and network-based monitoring to give a complete view of network and system activity.

4. Application Protocol-Based IDS (APIDS)

- **Function:** APIDS monitors and analyzes application-specific protocols to detect potential attacks targeting specific applications.
- **Usage:** It tracks communication protocols like SQL to detect malicious activity during database interactions.

5. Protocol-Based IDS (PIDS)

- **Function:** PIDS monitors communication protocols between devices (like HTTPS or HTTP) to detect abnormal activity.
- **Usage:** It ensures that the communication follows expected patterns, identifying deviations that may signal an attack.

Detection Method of IDS:

Signature-Based Detection

This method relies on predefined patterns (signatures) of known attacks. It compares incoming data to a database of attack signatures.

- Easy to implement and effective for detecting known threats.
- Cannot detect new or unknown attacks unless their signature is added to the database.

Anomaly-Based Detection

Anomaly-based IDS uses machine learning or statistical models to define what normal behavior looks like. Any activity that deviates from this norm is flagged as suspicious.

- Can detect unknown attacks or behaviors.
- High rate of false positives if the model is not fine-tuned.

Benefits:

- **Detects Malicious Activity:** IDS can detect any suspicious activities and alert the system administrator before any significant damage is done.
- **Improves Network Performance:** IDS can identify any performance issues on the network, which can be addressed to improve network performance.
- **Compliance Requirements:** IDS can help in meeting compliance requirements by monitoring network activity and generating reports.
- **Provides Insights:** IDS generates valuable insights into network traffic, which can be used to identify any weaknesses and improve network security.

Limitations:

- **False Alarms**: IDS can generate false positives, alerting on harmless activities and causing unnecessary concern.
- **Resource Intensive**: It can use a lot of system resources, potentially slowing down network performance.
- **Requires Maintenance**: Regular updates and tuning are needed to keep the IDS effective, which can be time-consuming.
- **Doesn't Prevent Attacks**: IDS detects and alerts but doesn’t stop attacks, so additional measures are still needed.
- **Complex to Manage**: Setting up and managing an IDS can be complex and may require specialized knowledge.

UNIT-5

-: Software-Defined Networking (SDN) and Cloud Networking:-

Introduction to SDN:

- Software-Defined Networking (SDN) is a modern networking approach that transforms the way computer networks are designed, managed, and operated. Unlike traditional networks, where each router or switch makes its own forwarding decisions, SDN separates the **control plane** (network intelligence) from the **data plane** (packet forwarding). This separation allows network administrators to manage the entire network through a centralized software controller.
- SDN provides a programmable and flexible networking environment that simplifies network configuration, improves resource utilization, and supports automation. It is widely used in data centers, cloud computing, enterprise networks, and 5G communication systems.

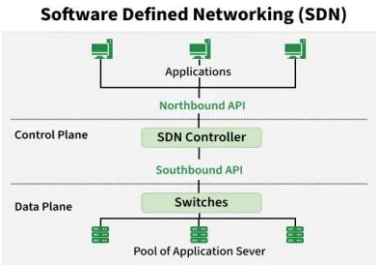
Concept of SDN:

The fundamental concept of SDN is the **separation of the control plane from the data plane**.

- **Control Plane:** Responsible for making decisions about where network traffic should be sent.
- **Data Plane:** Responsible for forwarding packets according to the rules provided by the control plane.

In SDN:

- The control plane is centralized in an **SDN Controller**.
- The data plane consists of network devices such as switches and routers.
- Network administrators configure and monitor the network through software applications.



Need for SDN

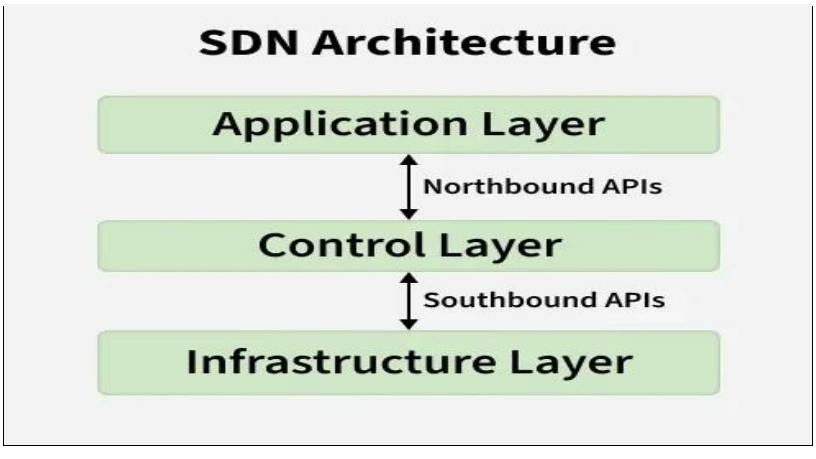
Traditional networks rely on individually configured devices, making management complex and inflexible. SDN is needed to simplify network control and efficiently handle modern, dynamic network requirements.

Centralized Control: SDN centralizes network intelligence in a controller, enabling consistent policy enforcement and easier network management.

Programmability: Network behavior can be programmed using software, allowing automated configuration, faster deployment, and reduced manual errors.

Flexibility and Agility: SDN enables quick adaptation to changing traffic patterns and application demands without reconfiguring individual devices.

SDN Architecture:



1. Application Layer:

Contains network applications such as traffic management, security, and monitoring tools.

Allows administrators to define network policies and requirements.

Communicates with the SDN controller through northbound APIs.

2. Control Layer:

Hosts the SDN controller, which acts as the brain of the network.

Translates application requirements into forwarding rules.

Maintains a global view of the network and makes routing decisions.

3. Infrastructure Layer (Data Plane):

Consists of physical or virtual switches and routers.

Forwards packets based on rules received from the controller.

Does not make independent decisions, ensuring simple and efficient forwarding.

4. Northbound and Southbound APIs

In Software Defined Networking, APIs act as communication interfaces between different layers of the SDN architecture. These interfaces enable programmability and centralized control of the network.

1. Northbound APIs:

Northbound APIs allow communication between the Application Layer and the SDN Controller. They enable network applications to define high-level policies, such as routing, load balancing, and security rules, without dealing with low-level network details. These APIs simplify network management and support automation by providing an abstract view of the network.

Example: REST APIs are commonly used as northbound interfaces to allow applications to interact with the SDN controller using standard web-based methods.

2. Southbound APIs:

Southbound APIs enable communication between the SDN Controller and the Infrastructure Layer (switches and routers). They allow the controller to install forwarding rules and manage packet flow in the data plane. Through southbound APIs, network devices follow instructions from the centralized controller instead of making independent decisions.

Example: OpenFlow is a widely used southbound protocol that allows the SDN controller to directly program flow tables in switches.

Advantages:

Centralized control: A controller manages the network from one place, making monitoring and policy enforcement easier.

Automation: Configuration, provisioning, and traffic control can be automated, reducing manual work and errors.

Programmability: Network behavior can be changed through software and APIs to match new requirements.

Flexibility: Policies and services can be updated quickly without replacing hardware.

Scalability: Central control helps manage large networks more efficiently.

Cost efficiency: SDN can run on commodity hardware, lowering dependency on expensive proprietary devices.

Better fault handling: The controller can detect failures and reroute traffic to keep services running.

Faster innovation: New features and services can be deployed rapidly through software updates.

Disadvantages:

Single point of failure: If a centralized controller goes down, network control can be disrupted unless redundancy is in place.

Scalability: In very large networks, the controller can become a bottleneck if it cannot manage all devices fast enough.

Resilience: SDN can reroute traffic, but real reliability depends on controller availability and good failover design.

Migration complexity: Mixing SDN with traditional networks takes careful planning and can be difficult to deploy smoothly.

Security risks: The controller is a high-value target, so strong authentication, access control, and monitoring are required.

Applications:

Data centers: SDN gives centralized control to automate provisioning and route traffic dynamically for better performance.

Cloud networking: SDN builds programmable virtual networks that support multi-tenancy, fast service rollout, and easy scaling.

Traffic management: SDN monitors traffic in real time and adjusts paths to improve load balancing and reduce congestion.

Network virtualization: SDN enables overlays and virtual network functions, improving resource usage and isolating tenants.

Security: SDN applies security policies centrally and can update rules quickly for threat detection and mitigation.

OpenFlow and SDN Controllers:

OpenFlow is the first standardized communication protocol designed specifically for Software-Defined Networking (SDN). It enables communication between the SDN controller and OpenFlow-enabled switches or routers.

In traditional networking, each switch contains both the control plane and data plane. However, in SDN, these functions are separated. The SDN controller makes forwarding decisions, while the switch simply follows those instructions. OpenFlow provides the communication mechanism that allows the controller to install, update, or remove forwarding rules in switches.

Need for OpenFlow:

1. Provides centralized control over network devices.
2. Simplifies network management.
3. Reduces manual configuration.
4. Enables network automation.
5. Supports programmable networks.
6. Improves traffic engineering.
7. Provides vendor-independent communication.
8. Enables quick implementation of new network policies.

OpenFlow architecture consists of three major components such as:

(a) SDN Controller

The SDN controller is responsible for making forwarding decisions.

Functions include:

Maintaining network topology.
Installing forwarding rules.
Monitoring traffic.
Managing bandwidth.
Applying security policies.

(b) OpenFlow Switch

An OpenFlow switch is responsible only for forwarding packets according to rules received from the controller.

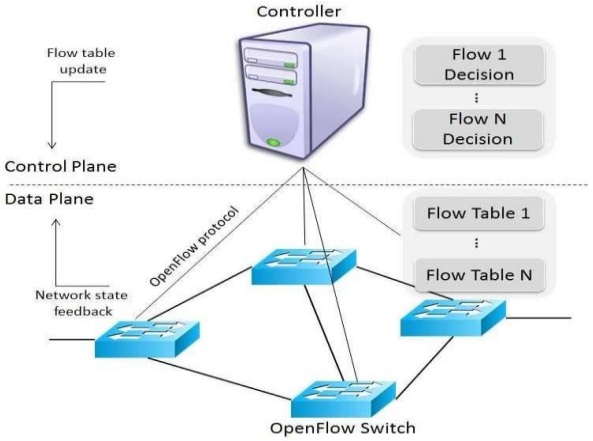
Functions include:

Receiving packets.
Searching the flow table.
Executing forwarding actions.
Reporting unknown packets to the controller.

(c) Secure Communication Channel

The controller communicates with switches through a secure communication channel using OpenFlow messages.

This communication is generally protected using TLS (Transport Layer Security) to prevent unauthorized access.



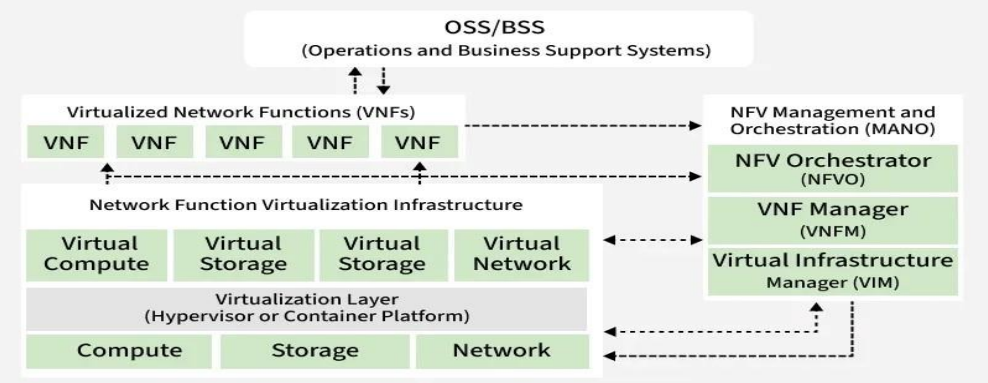
Virtualization in Networking (NFV):

Network Functions Virtualization (NFV) is a technology that virtualizes traditional network functions, like routing, load balancing, and firewalls, so they run as software on standard servers instead of dedicated hardware devices.

- Replaces dedicated network hardware with software-based Virtual Network Functions (VNFs)
- Enables faster deployment and easy scaling of network services on demand
- Reduces costs by using standard, commodity servers instead of specialized devices
- Simplifies network management through automation and centralized orchestration.

NFV Architecture

The architecture of NFV is divided into three key parts, each responsible for infrastructure, network functions, and management.



- **Virtualized Infrastructure:** Provides the compute, storage, and networking resources needed to host VNFs. This is abstracted using hypervisors for VMs or container platforms for cloud-native deployments.
- **Virtual Network Functions (VNFs):** Software implementations of network functions such as routing, switching, firewalls, load balancers, and VPNs. VNFs can be deployed, scaled, or updated independently.
- **Management and Orchestration (MANO):** The central framework responsible for lifecycle management of VNFs, resource allocation, automation, and overall coordination of the NFV environment. It includes NFV Orchestrator (NFVO), VNF Manager (VNFM), and Virtualized Infrastructure Manager (VIM).

Working of NFV:

The working of NFV can be understood in four main steps, each handling virtual network functions, automation, rapid deployment, and flexible management of network services.

- **Virtualized Network Functions (VNFs):** Software running on VMs or containers performs tasks traditionally handled by dedicated hardware, including routing, load balancing, firewalls, and VPN services.
- **Automation and Control:** Hypervisors, container platforms, or software-defined networking (SDN) controllers manage the provisioning, configuration, and orchestration of VNFs.

- **Rapid Deployment:** Network services can be deployed, updated, or scaled automatically without manual hardware setup.
- **Flexible Management:** Centralized orchestration ensures optimized resource usage, service chaining, and dynamic scaling of network functions.

Applications:

- **Telecommunication Networks:** NFV virtualizes core network functions such as IMS, EPC, and 5G core for faster and scalable service deployment.
- **Virtual Customer Premises Equipment (VCPE):** Customer network functions like routers and firewalls are delivered as software from the cloud instead of physical devices.
- **Security Services:** Firewalls, intrusion detection, and intrusion prevention systems are implemented as virtual network functions.
- **Load Balancing:** NFV enables software-based load balancers that dynamically distribute traffic without dedicated hardware.
- **Cloud Data Centers:** NFV supports efficient deployment and management of network services using shared cloud infrastructure.
- **Enterprise WAN and VPN Services:** NFV allows flexible and quick provisioning of virtual WAN and VPN connectivity for enterprises.

Advantages:

- **Cost Savings:** Runs on standard servers with a pay-as-you-go model, reducing both CapEx and OpEx.
- **Faster Deployment:** Virtualized functions can be deployed in hours, avoiding the delays of physical hardware setup.
- **Scalability:** Network resources can be scaled up or down dynamically without buying extra hardware.
- **Simplified Management:** Software-based functions are easier to configure, update, and maintain, lowering operational complexity.
- **Flexibility:** Multiple network services like routing, firewalls, and load balancing can be implemented via software for quick adaptation.

Disadvantages:

- **Weaker Physical Security:** Shared servers are more vulnerable than dedicated hardware, putting multiple VNFs at risk if the host is compromised.
- **Malware Spread:** Malware can propagate quickly between VNFs on the same server, requiring strong isolation measures.
- **Reduced Visibility:** East-west traffic between VNFs is harder to monitor with traditional tools, complicating threat detection.
- **Virtualization Dependency:** NFV depends on hypervisors and orchestration platforms; flaws here can impact multiple network functions.
- **Performance Overhead:** Shared resources may cause latency or contention, affecting VNF performance and service quality.
- **Complex Security Management:** Maintaining consistent security policies across virtualized environments increases operational complexity.

Cloud Computing and Network Virtualization:

Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (such as servers, storage, networks, applications, and services) that can be rapidly provisioned and released with minimal management effort.