UNIT I

FOUNDATIONS OF COMPUTER NETWORKS

Introduction to Computer Networks

A **computer network** is a system that connects multiple computing devices so they can share data, resources, and services. Networks enable communication between users, applications, servers, and machines across small local areas or globally.

Types of Computer Networks

a. Personal Area Network (PAN)

- Very small range (a few meters).
- Examples: Bluetooth headphones, smartphone hotspot, smartwatches.

b. Local Area Network (LAN)

- Covers a building or small area.
- Wired (Ethernet) or wireless (Wi-Fi).
- Common in homes, offices, schools.

c. Metropolitan Area Network (MAN)

- Spans a city or large campus.
- Used by organizations connecting multiple branches.

d. Wide Area Network (WAN)

- Covers large geographic areas (countries, continents).
- The **Internet** is the largest WAN.
- Uses leased lines, satellite links, fiber optics.

e. Wireless Networks

- **Wi-Fi**, **cellular networks (4G/5G)**, **satellite networks**.
- Enable mobility and long-distance communication.

f. Virtual Private Network (VPN)

- Secure, encrypted connection over public networks.
- Used to access private networks remotely.

Network Topologies

Network topology is the **arrangement of devices (nodes) and connections (links) in a communication network**, determining how data flows between them. It can be a physical or logical layout and is crucial for network performance, reliability, and security.

Types of Network Topology

Common network topologies each have unique advantages and disadvantages, making them suitable for different use cases.

- **Bus:** All devices connect to a single central cable, or backbone.
    - **Pros:** Cost-effective and simple to implement in small networks with minimal cabling.
    - **Cons:** A single point of failure in the main cable can down the entire network, and performance decreases with heavy traffic due to data collisions.
- **Star:** All nodes connect to a central hub or switch. This is the most common topology in modern Local Area Networks (LANs), such as home and office setups.
    - **Pros:** Easy to manage, troubleshoot, and scale; the failure of one device does not affect the rest of the network.
    - **Cons:** The entire network depends on the central hub; if it fails, the whole system goes down
- **Ring:** Devices are connected in a closed loop, with each node linked to exactly two neighbors. Data typically flows in one direction, though dual-ring configurations offer redundancy.
    - **Pros:** Can span large distances with each node acting as a repeater; orderly data flow prevents collisions.
    - **Cons:** A single node or link failure can disrupt the entire network; difficult to troubleshoot.
- **Mesh:** Devices are extensively interconnected, providing multiple paths for data between any two nodes. Full mesh connects every device to every other device, while partial mesh connects only some nodes with multiple links.

  - **Pros:** Highly reliable, fault-tolerant, and secure due to redundancy and dedicated links.
  - **Cons:** Complex and expensive to install and maintain due to extensive cabling and configuration requirements.

- **Tree:** A hierarchical structure combining elements of bus and star topologies, with a root node connecting to groups of star-configured networks (branches).
  - **Pros:** Highly scalable, easy to manage in segments, and simple to isolate faults within a branch.
  - **Cons:** Dependent on the central root node, which is a single point of failure for all dependent branches.

- **Hybrid:** A combination of two or more different basic topologies (e.g., star-bus or star-ring).
  - **Pros:** Flexible, customizable to meet specific needs, and can combine the strengths of different layouts.
  - **Cons:** Complex architecture can be challenging to design, manage, and maintain.

Physical vs. Logical Topology

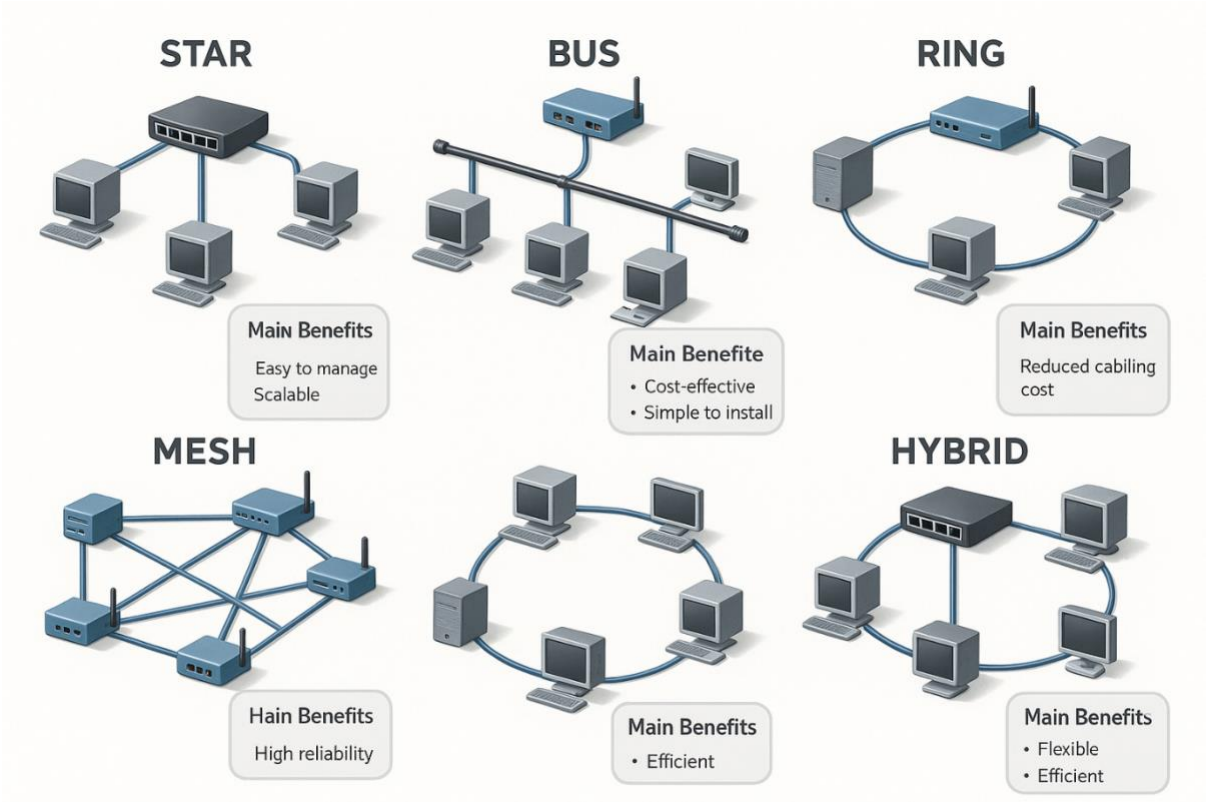
- **Physical Topology** describes the actual, tangible layout of cables, devices, and all physical interconnections.
- **Logical Topology** illustrates how data flows within the network, which may not match the physical layout. For example, a network might be wired as a physical star but function as a logical bus.

Key Considerations for Choosing a Topology

When selecting a network topology, administrators must balance several factors:

- **Cost:** The budget for hardware, cabling, and installation.
- **Scalability:** How easily the network can expand to accommodate future growth.
- **Reliability & Fault Tolerance:** The network's ability to remain operational despite component failures.

- **Security:** How easily security measures can be implemented and potential vulnerabilities managed.
- **Performance:** Required speed and efficiency of data transfer.



Uses of Networks in Different Environments

a. Homes

- Sharing internet access between devices.
- Streaming video, gaming, video calls.
- Managing **smart home IoT devices** (lights, TVs, thermostats).
- Wi-Fi mesh systems for better coverage.

b. Offices and Enterprises

- File sharing, email, VoIP communication.
- Centralized data storage and backups.
- Access control, security systems, surveillance cameras.
- Collaboration platforms (Teams, Zoom, Slack).

c. Data Centers

- High-speed connections between servers.
- Rack-level networking, spine-leaf architecture.
- Redundancy and load balancing.
- Hosting cloud services, virtual machines, and big-data applications.

Network Use in Emerging and Advanced Applications

a. Internet of Things (IoT)

Computer networks enable IoT devices to communicate and exchange data.

- Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRaWAN.
- Smart home appliances, sensors, security devices.
- Smart city applications: traffic control, energy monitoring.

b. Cloud Services

Cloud computing relies heavily on high-speed networks.

- Accessing remote servers and storage (AWS, Azure, Google Cloud).
- Virtual networks (VPCs), load balancers, firewalls.
- Data synchronization and distributed computing.

c. Industrial Automation (Industry 4.0)

Used for machine-to-machine (M2M) communication.

- Ethernet/IP, PROFINET, Modbus, OPC-UA.
- Connecting robots, PLCs, sensors, SCADA systems.
- Real-time monitoring of production lines.
- Enhances efficiency, predictive maintenance, and automation.

OSI & TCP/IP Models – Layered Architecture

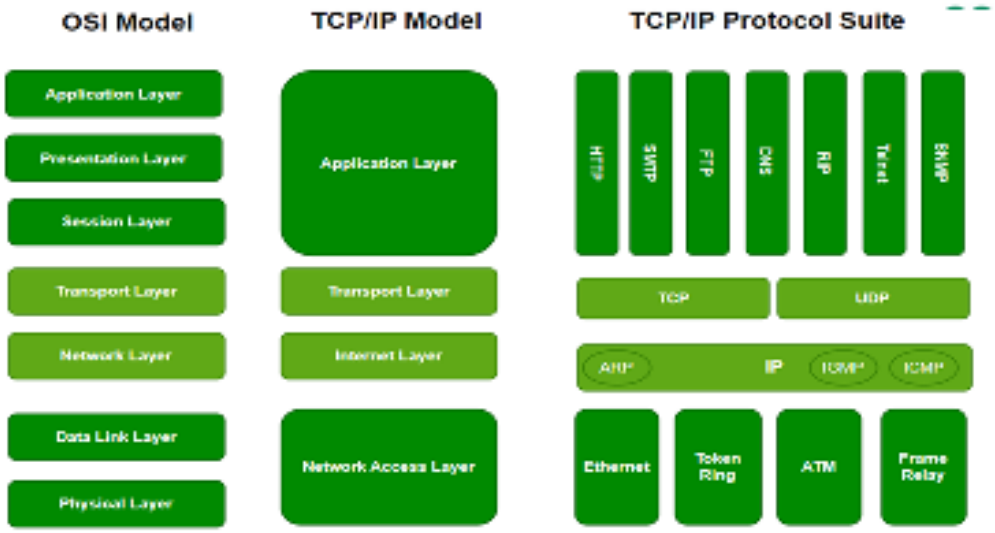
OSI and TCP/IP both are logical models. One of the main similarities between the OSI and TCP/IP models is that they both describe how information is transmitted between two devices across a network. Both models define a set of layers. Each layer performs a specific set of functions to enable the transmission of data.

- **OSI Model:** It has 7 layers Physical layer, Data Link layer, Network layer, Transport layer, Session layer, Presentation layer, and Application layer. Each layer performs its task independently.

- **TCP/IP Model:** It has 4 layers named as Physical layer, Network layer, Transport layer, and Application layer. It also can be used as a communications protocol in a private computer network.

OSI Model v/s TCP/IP Model

The OSI (Open Systems Interconnection) Model and the TCP/IP (Transmission Control Protocol/Internet Protocol) Model are two frameworks used to understand how data moves through networks. While they both help in organizing network communication, they have distinct structures and purposes. Understanding these differences is essential for anyone learning about or working with computer networks.



OSI vs TCP/IP

Parameter	OSI Model	TCP/IP Model
Full Form	Open Systems Interconnection	Transmission Control Protocol/Internet Protocol
Layers	7 layers (Application, Presentation, Session, Transport, Network, Data Link, Physical)	4 layers (Application, Transport, Internet, Network Access)
Usage	Works as a reference model for understanding and designing networks, but not implemented directly	A practical model used in real-world networking, forms the basis of the Internet
Approach	Strict layer-by-layer architecture, each layer has a defined function and communicates only with adjacent layers	Flexible architecture, layers are not as rigidly separated and can interact

Parameter	OSI Model	TCP/IP Model
Error Handling	Error handling is present at the Data Link (frame errors) and Transport layer (end-to-end reliability)	Error handling is mainly the job of TCP, while UDP provides no reliability
Development	Designed by ISO in the late 1970s to standardize communication across different systems	Developed by DARPA (U.S. Defense) in the 1970s for building the ARPANET (precursor to the Internet)

Transmission Media – Wired & Wireless

Transmission media refers to the physical or logical pathways used to transmit data from one device to another in a computer network.
It is broadly classified into:

1. **Wired (Guided) Media** – Signals travel through a physical medium.
2. **Wireless (Unguided) Media** – Signals are transmitted through air (radio, light).

1. Wired (Guided) Transmission Media

Wired media provide **high speed, reliability, and security**. Data signals are guided through cables.

A. Twisted Pair Cable

Used widely in LANs, telephones, and home networks.

Types:

- **UTP (Unshielded Twisted Pair)** – Common in Ethernet (Cat5e, Cat6, Cat7).
- **STP (Shielded Twisted Pair)** – Has shielding to reduce interference.

Features:

- Speed: Up to 1–10 Gbps (higher categories support more).
- Distance: Up to ~100 meters.
- Advantages: Low cost, easy installation.
- Disadvantages: Susceptible to electromagnetic interference (EMI).

B. Coaxial Cable

Used in cable TV networks, older LANs, and broadband.

Features:

- Better shielding than twisted pair.
- Speed: 10 Mbps to several Gbps depending on system.
- Distance: Hundreds of meters.
- Advantages: Good noise immunity.
- Disadvantages: Bulkier and more expensive than twisted pair.

C. Fiber Optic Cable

Transmits data using **light signals** through glass or plastic fibers.

Features:

- Extremely high speed (10 Gbps → 400 Gbps → 1 Tbps systems).
- Very long distance (kilometers without repeaters).
- Immune to EMI.
- Very secure.

Types:

- **Single-mode fiber (SMF):** Long distance, thin core, used in telecom.
- **Multi-mode fiber (MMF):** Shorter distance, thick core, used in LANs and data centers.

Advantages:

- Highest bandwidth.
- Ideal for backbone networks, data centers, ISPs.

Disadvantages:

- Higher cost.
- Requires skilled installation.

2. Wireless (Unguided) Transmission Media

Wireless media use **electromagnetic waves** for communication through air or vacuum.

A. Radio Waves

Used for Wi-Fi, Bluetooth, radio broadcasting, cellular networks.

Features:

- Frequency range: 3 kHz to 1 GHz.
- Penetrates walls; good for indoor use.
- Advantages: Mobility, wide coverage.

- Disadvantages: Interference, limited security.

B. Microwaves

Used in satellite communication, WiMAX, point-to-point links.

Types:

- **Terrestrial Microwave:** Line-of-sight towers.
- **Satellite Microwave:** Uses geostationary or low-earth satellites.

Features:

- High frequency (1–30 GHz).
- Requires clear line-of-sight.
- High bandwidth.

C. Infrared

Used in remote controls, short-range communication, some IoT devices.

Features:

- Very short range (a few meters).
- Requires line-of-sight.
- Not suitable for outdoor long-range due to sunlight interference.

D. Millimeter Waves (mmWave)

Used in 5G networks, radar systems.

Features:

- Extremely high frequency (30–300 GHz).
- High data rate but limited range.
- Easily absorbed by obstacles.

E. Visible Light Communication (VLC) / Li-Fi

Uses LED light signals for data transmission.

Features:

- Very high speeds (in research, up to 10 Gbps).
- Requires direct line-of-sight.
- Cannot penetrate walls, making it secure.

Switching Techniques

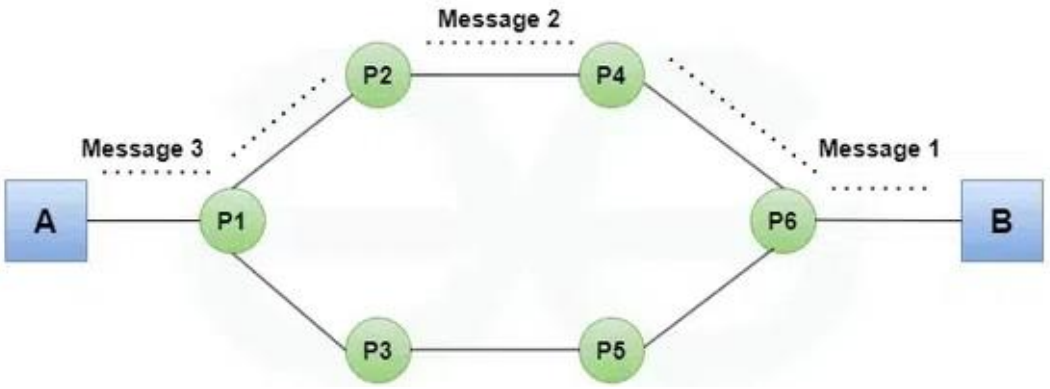
Switching is the method used to forward data from a sender to a receiver across a network. It determines **how data travels through intermediate network devices** (switches/routers).

There are **three main switching techniques**:

1. **Circuit Switching**
2. **Packet Switching**
3. **Message Switching**

1. Circuit Switching

Circuit switching creates a **dedicated communication path** between two devices before data transfer begins.



How it works

1. **Connection establishment** (dedicated path created).
2. **Data transfer** (continuous, guaranteed bandwidth).
3. **Connection release** (path freed).

Used in:

- Traditional telephone networks
- Some dedicated communication channels

Advantages:

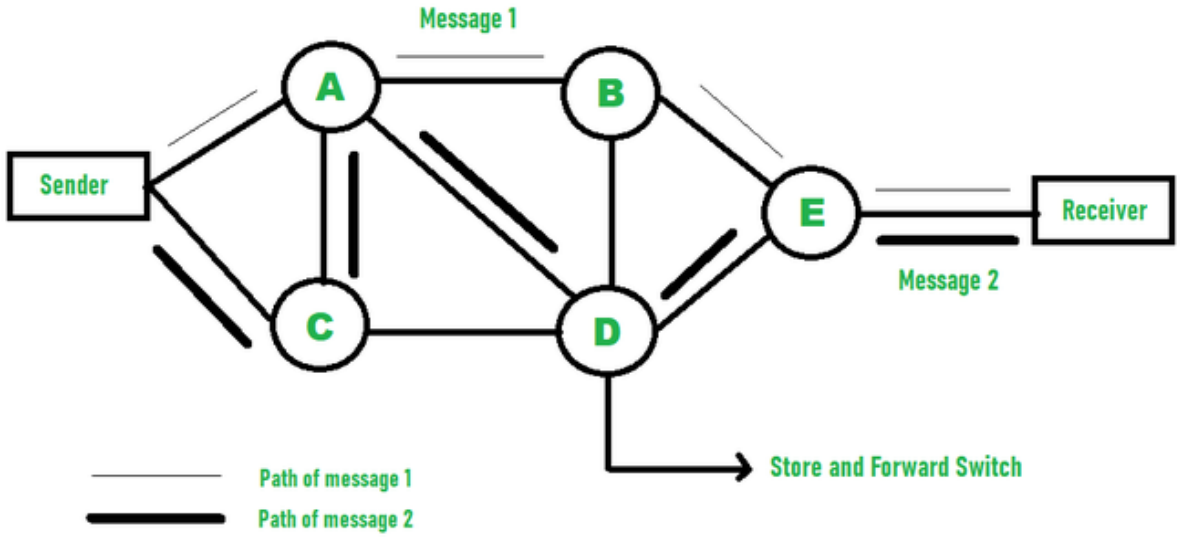
- Guaranteed bandwidth
- Consistent latency
- Reliable for real-time communication (voice calls)

Disadvantages:

- Inefficient: channel remains reserved even when idle
- Not suitable for bursty data like internet traffic

2. Packet Switching

Data is divided into **small packets**, each sent independently through the network. Packets may take **different paths** and are reassembled at the destination.



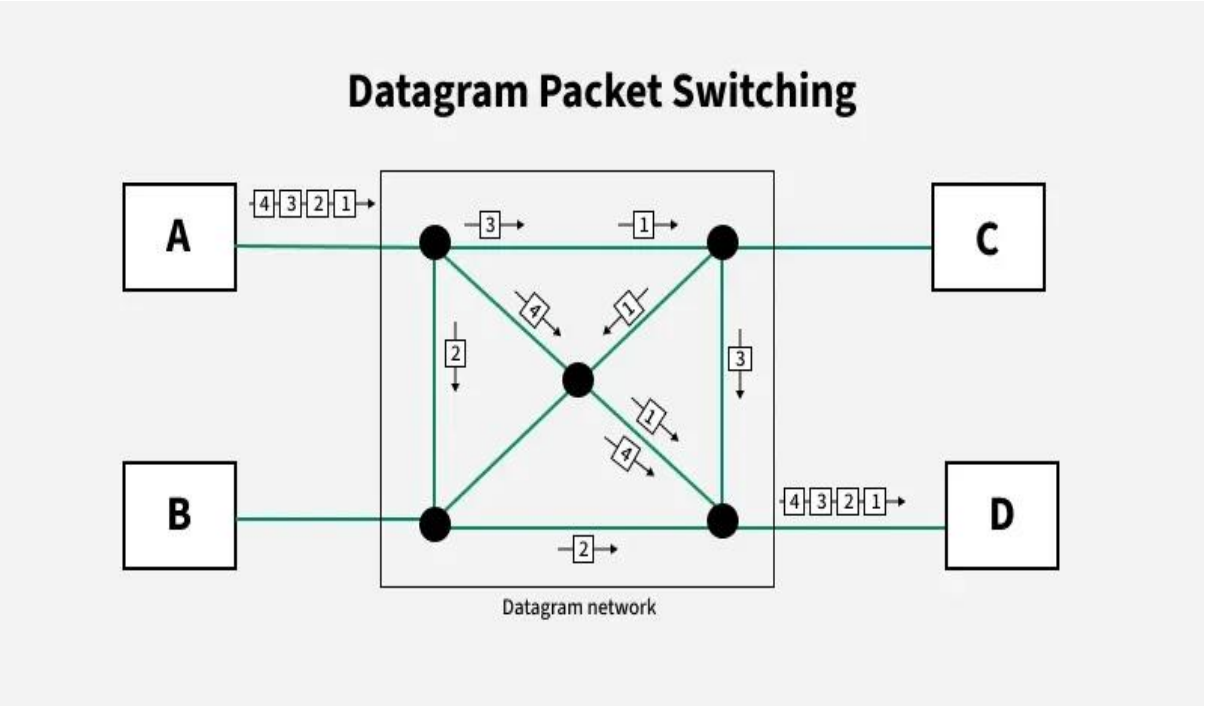
Two types:

- **Datagram Packet Switching**
- **Virtual Circuit Packet Switching**

A. Datagram Packet Switching

Each packet:

- Travels independently
- Takes any available path
- Has full destination address



Used in:

- **Internet** (IP, routers)
- Most modern data communication

Advantages:

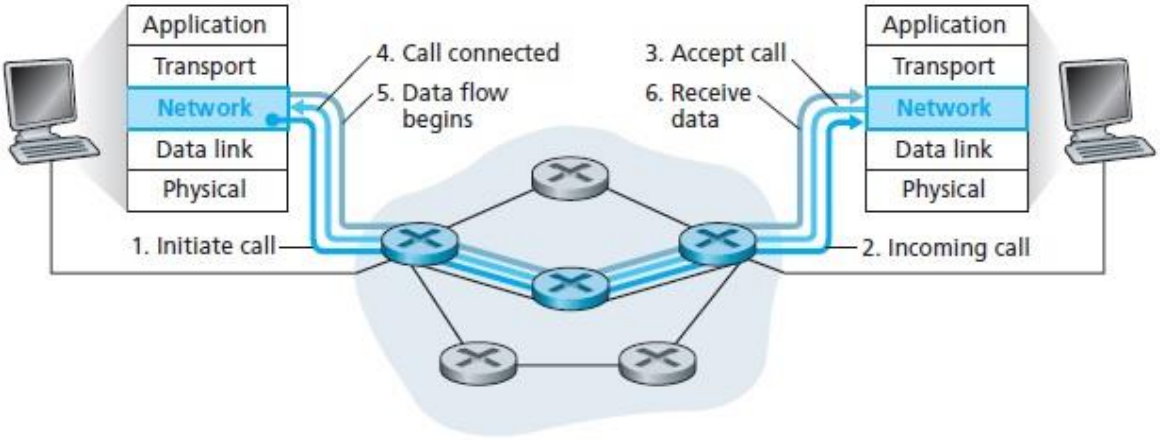
- Efficient use of network resources
- Highly fault-tolerant
- Good for bursty data

Disadvantages:

- Packets may arrive out of order
- Variable delays
- Requires reassembly logic

B. Virtual Circuit Packet Switching

Before sending packets, a **logical path (VC)** is established.
Packets follow the **same route**, but no dedicated physical circuit is created.



Used in:

- Frame Relay
- ATM networks

Advantages:

- More reliable than datagram
- Less overhead (smaller headers)
- Orderly delivery

Disadvantages:

- Setup delay (similar to circuit switching)
- Failure in the virtual circuit disrupts communication

3. Message Switching

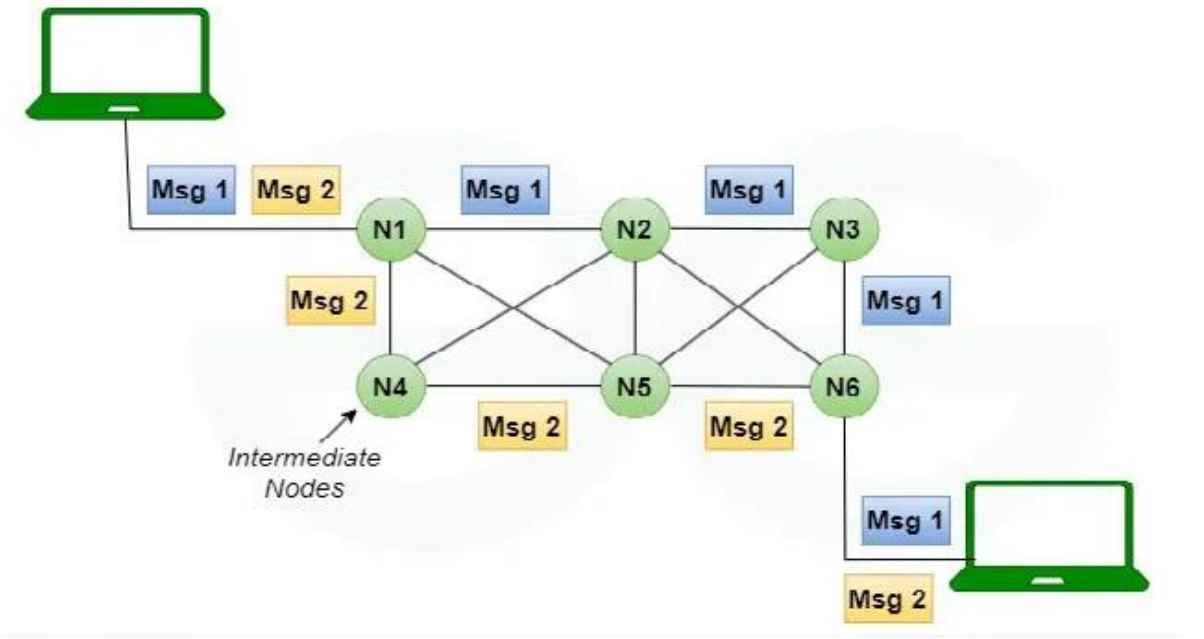
Entire message is treated as **one unit** and forwarded from switch to switch (store-and-forward).

Features:

- No need for a dedicated path
- Each intermediate node stores message, then forwards it

Used historically in:

- Telegraph networks
- Early communication systems



Advantages:

- No need for connection setup
- Efficient channel usage

Disadvantages:

- Large delays due to store-and-forward
- Requires large memory at nodes
- Not suitable for real-time communication

4. Comparison of Switching Techniques

Feature	Circuit Switching	Packet Switching	Message Switching
Path	Dedicated	Dynamic (or virtual)	Dynamic
Delay	Low	Variable	High
Real-time support	Excellent	Good (TCP/UDP)	Poor
Efficiency	Low	High	Moderate
Storage needed	Minimal	Some (buffering)	High
Examples	PSTN phone	Internet	Telegraph

5. Where They Are Used Today

Circuit Switching

- VoIP replaced most, but concept still used in some dedicated links.

Packet Switching

- Foundation of the **Internet**
- LANs, WANs, cellular networks (4G/5G)

Message Switching

- Rare today; concepts remain in store-and-forward systems like email servers.

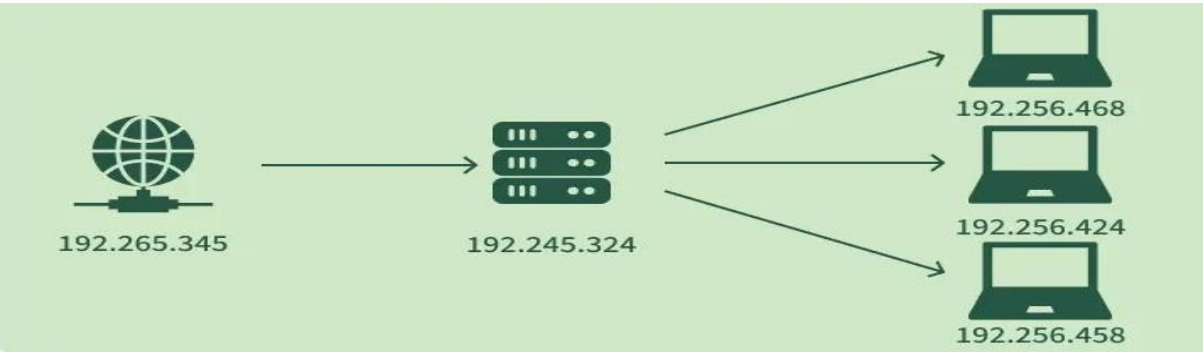
Core Network Protocols – IP, TCP, UDP, ICMP

A network protocol is a set of rules that govern data communication between different devices in the network. It determines what is being communicated, how it is being communicated, and when it is being communicated. It permits connected devices to communicate with each other, irrespective of internal and structural differences.

How do Network Protocols Work?
It is essential to understand how devices communicate over a network by recognizing network protocols. The Open Systems Interconnection (OSI), the most widely used model, illustrates how computer systems interact with one another over a network. The communication mechanism between two network devices is shown by seven different layers in the OSI model. Every layer in the OSI model works based on different network protocols. At every layer, one or more protocols are there for network communication. To enable network-to-network connections, the Internet Protocol (IP), for instance, routes data by controlling information like the source and destination addresses of data packets. It is known as a network layer protocol.

1. IP (Internet Protocol)

Internet Protocol (IP) is a set of rules that governs how data is transmitted across networks by breaking it into packets and using unique IP addresses to route them to the correct destination. Each device on a network is assigned an IP address, which acts as its unique identifier, similar to a postal address. The protocol works in conjunction with other protocols like TCP to ensure data arrives at its intended recipient.



How it works

- **Packetization:** Data is broken down into smaller pieces called packets.
- **Addressing:** Each packet is given a header that includes the source and destination IP addresses.
- **Routing:** Routers use the destination IP address to forward the packet along the most efficient path to its destination.
- **Assembly:** At the destination, the packets are reassembled into the original data.

Key versions

- IPv4**:** The older version, using a 32-bit address system, which has led to address exhaustion due to the internet's growth.
- IPv6**:** The newer version, using a 128-bit address system, which provides a vastly larger number of addresses to accommodate the increasing number of internet-connected devices.

Why it's important

- It is a fundamental component of the internet, enabling devices to communicate with each other across vast distances.
- It provides the addressing and routing mechanisms necessary for all internet-based communication, from web browsing to email and video streaming.
- Without IP, the modern internet as we know it would not exist.

2. TCP (Transmission Control Protocol)

TCP, or Transmission Control Protocol, is a core internet protocol that ensures reliable, ordered, and error-checked delivery of data between devices. It works with IP (Internet Protocol) to establish a connection-oriented, full-duplex communication, breaking data into packets, managing their flow with acknowledgments and retransmissions, and reassembling them in the correct order at the destination. TCP is essential for applications like web browsing, email, and file transfers where data accuracy is critical.

Key functions of TCP

- **Reliable data delivery:** TCP guarantees that data packets are delivered accurately and without loss. It achieves this through a system of acknowledgments, where the receiver confirms receipt of data, and retransmissions, where the sender resends packets that were not acknowledged.

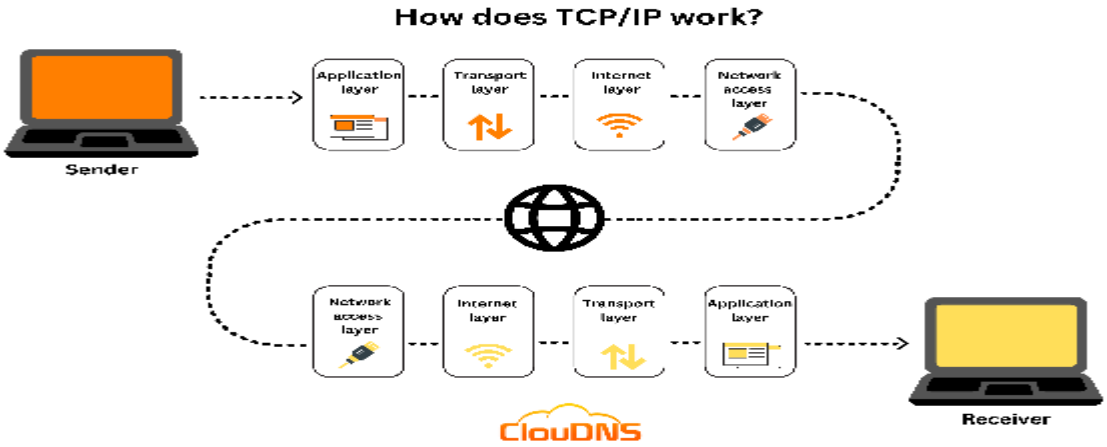
- **Ordered data transmission:** It ensures that data packets are delivered to the application in the same order they were sent, even if they arrive out of sequence.
- **Connection-oriented communication:** Before data is transferred, TCP establishes a connection between the sender and receiver through a process called a three-way handshake. This connection is maintained until all data has been exchanged and is then closed gracefully.
- **Error-checking and recovery:** TCP includes mechanisms for error-checking and recovery, identifying and correcting errors that may occur during transmission.
- **Flow and congestion control:** It manages the flow of data to prevent overwhelming the receiving device and implements congestion control to avoid network congestion.

How TCP works

- **Connection establishment:** A client initiates a connection with a server using a three-way handshake:

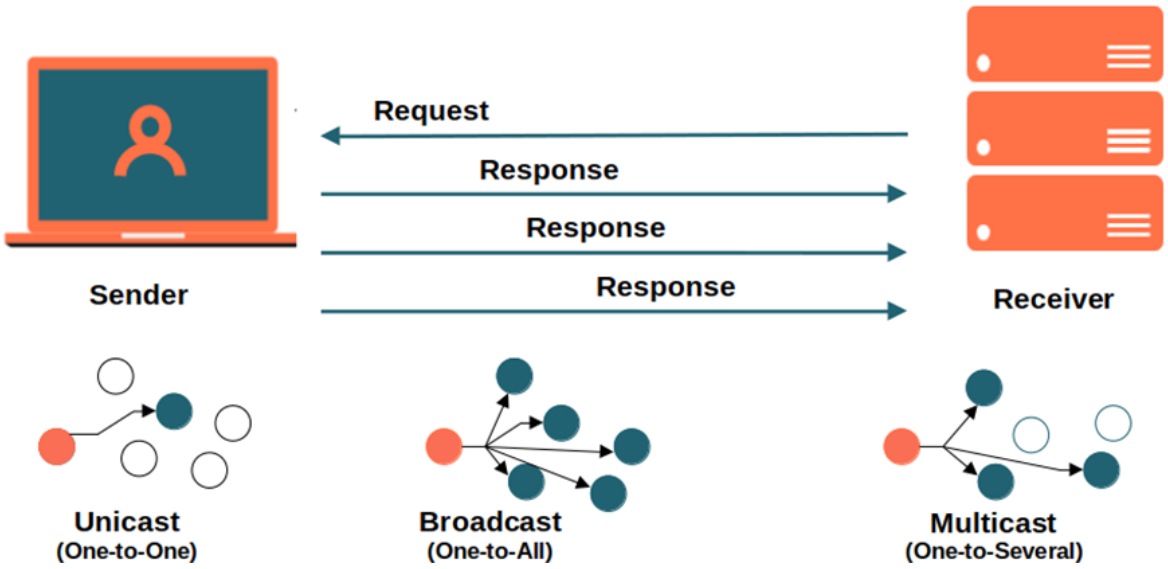
1. Client sends a SYN (synchronize) packet.
2. Server responds with a SYN-ACK (synchronize-acknowledge) packet.
3. Client sends an ACK (acknowledge) packet to finalize the connection.

- **Data transmission:** Once connected, TCP breaks down the data into smaller, manageable packets. It numbers each packet to ensure they are reassembled in the correct order at the receiving end.
- **Acknowledgment:** The receiver sends acknowledgments for packets it receives correctly.
- **Retransmission:** If the sender doesn't receive an acknowledgment for a packet within a certain time frame, it assumes the packet was lost and retransmits it.
- **Connection termination:** When data transfer is complete, the connection is closed gracefully using FIN (finish) flags.



3. UDP (User Datagram Protocol)

UDP, or User Datagram Protocol, is a simple, **connectionless** and **unreliable** transport layer protocol that prioritizes speed and efficiency over guaranteed delivery. It does not establish a connection, send acknowledgments, or perform error checking like its counterpart TCP, making it ideal for real-time applications like online gaming, video conferencing, and streaming, where occasional data loss is acceptable.



How it works

- **Connectionless**: UDP does not need to establish a connection before sending data, which makes it faster.

- **No acknowledgments**: The sender does not wait for an acknowledgment that the data was received, and the receiver does not send one.
- **Best-effort delivery**: It relies on the underlying IP to deliver datagrams, but it doesn't guarantee their arrival or order.
- **Low overhead**: Due to the lack of connection setup, acknowledgments, and flow control, UDP has a very small header and low overhead.
- **Port numbers**: UDP uses port numbers to send data to the correct process on a destination host.

Common applications

- **Real-time applications**: Online gaming, video and voice over IP (VoIP) calls.
- **Streaming media**: Audio and video streaming where speed is critical and minor packet loss is tolerable.
- **Query-response protocols**: Domain Name System (DNS) and Simple Network Management Protocol (SNMP) queries, where small amounts of data are exchanged quickly.
- **Multicasting and broadcasting**: Broadcasting data to multiple recipients without maintaining separate connections.
- **IoT and sensors**: Devices that need to send frequent, small data packets with minimal delay.

4. ICMP (Internet Control Message Protocol)

ICMP, or Internet Control Message Protocol, is a network protocol that network devices use to send error and operational information, playing a crucial role in diagnosing network communication problems. It helps determine if data is reaching its destination, with common tools like `ping` and `traceroute` relying on ICMP to provide information about reachability and latency. ICMP is a supporting protocol of the IP suite, meaning it's a core part of the internet's functionality for reporting issues like a destination being unreachable or a packet being too large.

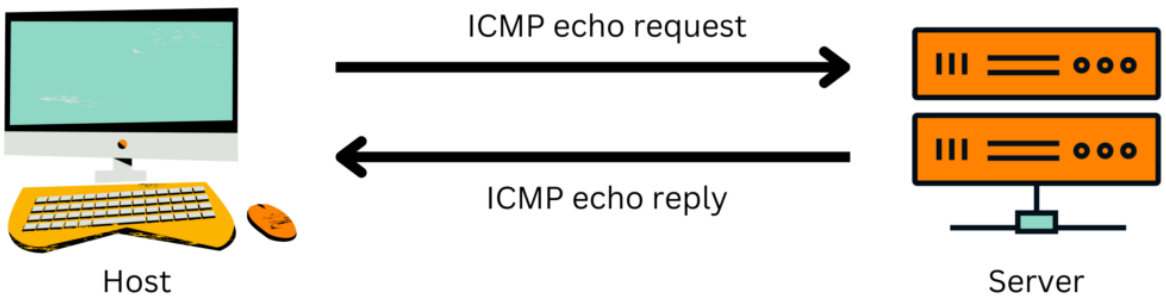
Key functions and uses

- **Error reporting**: When a problem occurs, such as a host being unreachable, a router will send an ICMP message back to the source device to report the issue.

- **Network diagnostics**: ICMP is used by diagnostic tools to test and understand network performance.
  - **ping**: Sends an "echo request" and waits for an "echo reply" from the destination to measure round-trip time (latency) and check if a host is alive.
  - **traceroute**: Uses ICMP "time exceeded" messages to identify the path and routers that a packet takes to reach its destination.
- **Operational information**: It can provide other operational data, such as a message to inform the source that a packet is too large for the network path.
- **Network layer protocol**: ICMP operates at the network layer (Layer 3), which is why it can be encapsulated directly in IP datagrams without needing a transport layer protocol like TCP or UDP.

Limitations and risks

- **No error correction**: ICMP is a protocol for reporting and controlling errors, not correcting them.
- **Can be exploited**: Due to its nature, ICMP can be used maliciously in denial-of-service attacks, such as ping floods, which is why some network administrators choose to disable it. However, blocking it can negatively impact network diagnostics and reliability.



IP Addressing – IPv4, IPv6, Sub netting, DNS, DHCP

IP addressing involves assigning unique numerical addresses to devices on a network for communication, using two main protocols: the older, 32-bit IPv4 and the newer, 128-bit IPv6. Subnetting divides a large network into smaller, manageable sub-networks using a subnet mask. DNS (Domain Name System) translates human-readable domain names into IP addresses, while DHCP (Dynamic Host Configuration Protocol) automatically assigns IP addresses and other network configurations to devices.

IP Addressing: IPv4 and IPv6

- **IPv4 (Internet Protocol version 4):** An older standard that uses a 32-bit address, providing approximately 4.3 billion unique addresses. The IPv4 address pool is nearly depleted due to the rapid growth of internet-connected devices.
- **IPv6 (Internet Protocol version 6):** A newer standard designed to address IPv4 exhaustion. It uses a 128-bit address, offering a virtually unlimited number of addresses.

Subnetting

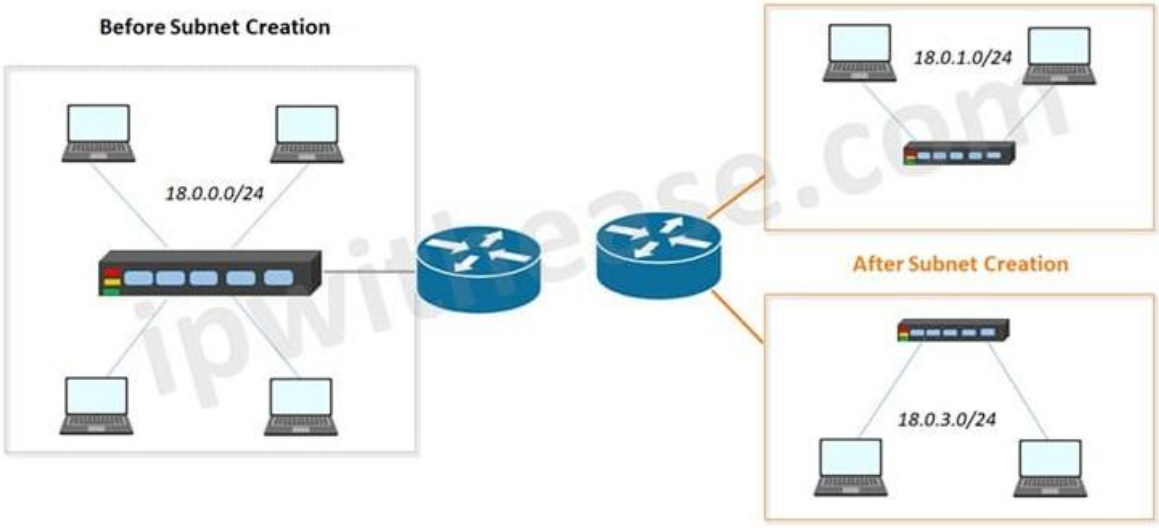
Subnetting is the process of dividing a larger IP network into smaller, more manageable sub-networks (subnets) to improve network performance, security, and efficiency. By creating subnets, administrators can better organize devices, control traffic flow, and optimize IP address usage, as communication within a subnet can happen directly, while communication between subnets requires a router.

How subnetting works

- **Logical subdivision:** A single IP network is logically split into multiple subnets. Each subnet is a smaller, independent network within the larger one.
- **Subnet masks:** A subnet mask is used to determine which part of an IP address identifies the network and which part identifies a specific device (host) within that network.
- **IP addresses:** Devices in the same subnet share identical "most-significant bits" in their IP addresses.
- **Communication:** Devices within the same subnet can communicate directly with each other. Communication between different subnets must pass through a router.

Benefits of subnetting

- **Improved performance:** Subnetting divides a large network into smaller broadcast domains, which reduces network congestion and improves overall speed.
- **Enhanced security:** Subnetting allows for the creation of more secure boundaries between different parts of a network, such as separating guest Wi-Fi from employee computers.
- **Efficient IP address management:** It enables a more efficient use of IP addresses by allowing for the creation of subnets with the specific number of addresses needed for each segment, rather than having large, unused blocks of IP addresses.



DHCP (Dynamic Host Configuration Protocol)

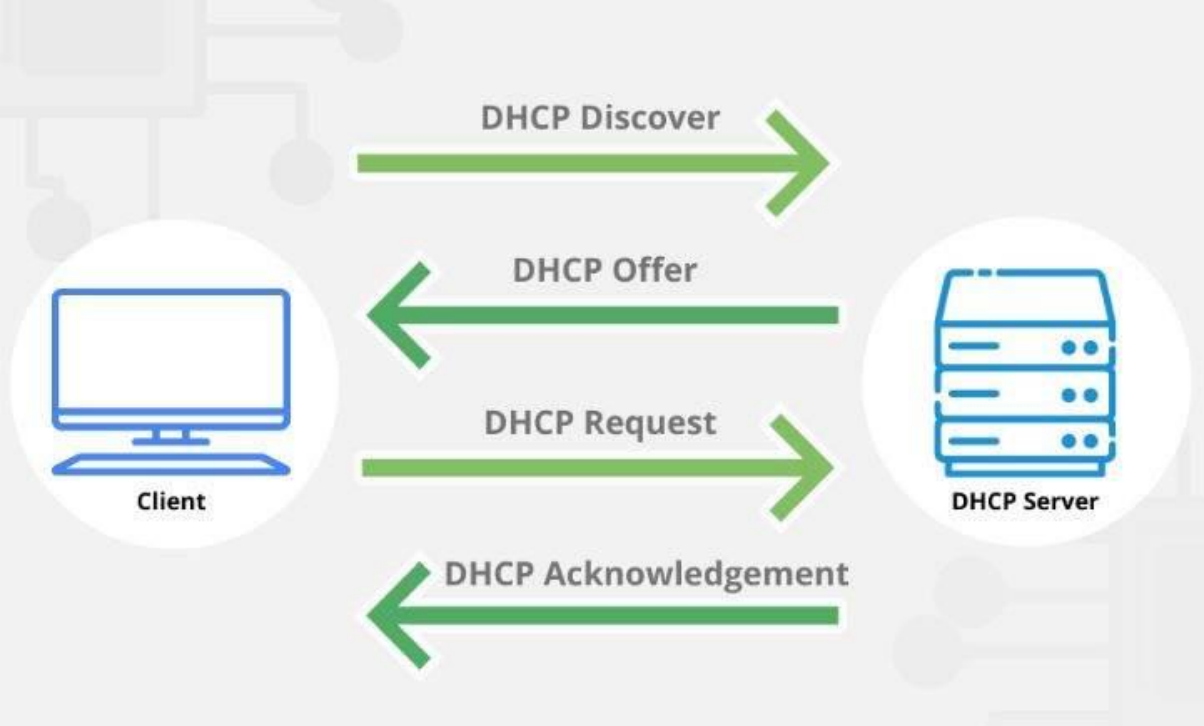
DHCP, or Dynamic Host Configuration Protocol, is a client/server network protocol that automatically assigns IP addresses and other network configuration information to devices on a network, eliminating the need for manual configuration. It reduces administrative effort, prevents IP address conflicts by assigning unique addresses, and provides flexibility for devices that move between networks by granting temporary IP address "leases".

How DHCP works

DHCP communication is a four-step process known as "DORA":

- **Discovery:** A client device, like a laptop, broadcasts a request to find an available DHCP server on the network.
- **Offer:** DHCP servers respond with an offer that includes a proposed IP address and other configuration details.

- **Request:** The client selects one of the offers and sends a request to the chosen server to confirm.
- **Acknowledgment:** The server sends an acknowledgment (ACK) to the client, finalizing the lease and configuration, which includes the assigned IP address.



Key functions and benefits

- **Automatic configuration:** Automatically assigns IP addresses, subnet masks, default gateways, and DNS server addresses to devices.
- **Reduced administrative burden:** Frees up network administrators from manually configuring each device, especially on large networks.
- **IP address management:** Manages IP addresses from a central point and prevents conflicts by ensuring unique assignments through a leasing system.
- **Flexibility:** Allows devices to move to different parts of the network and receive a new IP address automatically without manual intervention.
- **Efficient address use:** Reuses IP addresses when devices disconnect by returning the lease to the pool for assignment to other devices.

Network Communication Flow

Network communication flow is the process of data moving from a sender to a receiver, involving multiple layers that add and remove headers to format, route, and transmit the information. The sender creates data (Application), which is then formatted, encrypted, and compressed (Presentation). A session is established (Session), the data is broken into segments like TCP or datagrams (Transport), and then each packet gets IP addresses (Network). At the Data Link layer, packets are put into frames with MAC addresses for local networks, and finally, the Physical layer converts frames into bits for transmission via a medium like Wi-Fi or cables.

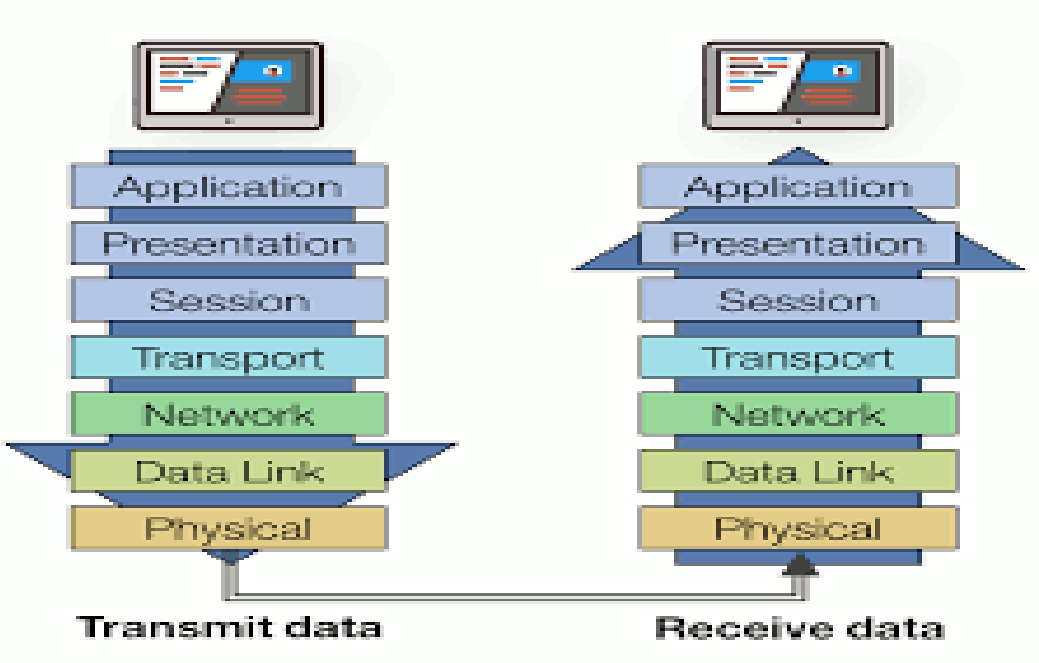
Sender side

1. **Application Layer:** A user or application generates data, like an email or a webpage request, using protocols like HTTP or SMTP.
2. **Presentation Layer:** The data is formatted, compressed, or encrypted for security.
3. **Session Layer:** A session is created between the sender and receiver to manage the communication.
4. **Transport Layer:** Data is divided into segments (TCP) or datagrams (UDP). TCP provides reliable, ordered delivery, while UDP is faster and connectionless.
5. **Network Layer:** Segments are placed into IP packets, each with a source and destination IP address, which routers use to send the packet across different networks.
6. **Data Link Layer:** Packets are encapsulated into frames, which include the source and destination MAC addresses for local network delivery. Switches use MAC addresses to forward frames within a local area network (LAN).
7. **Physical Layer:** Frames are converted into a stream of bits (0s and 1s) and transmitted over a physical medium such as a cable or radio waves.

Receiver side

1. **Physical Layer:** The receiver's physical layer receives the bitstream from the transmission medium.
2. **Data Link Layer:** The bits are reassembled into frames, and the MAC address is checked to ensure it's the intended recipient.
3. **Network Layer:** The IP address is checked, and the packet is passed to the transport layer.
4. **Transport Layer:** The layer reassembles the segments or datagrams into the original data, checking for any errors and reordering them if necessary.
5. **Session Layer:** The session layer ensures the communication session remains active until the process is complete.
6. **Presentation Layer:** The data is decrypted, uncompressed, and reformatted into a usable format.

7. **Application Layer:** The final, reconstructed data is delivered to the receiving application, such as a web browser displaying a webpage.



Applications: Smart homes, industrial IoT (e.g., SCADA), DNS in browser communications, IP addressing in 5G & cloud, DHCP in enterprise Wi-Fi networks.

Network applications are integral to modern connected environments, from automating homes to managing large-scale industrial systems.

Smart Homes

In smart homes, network applications enable the remote monitoring and control of various devices and systems, primarily through the Internet of Things (IoT).

- **Remote Access and Control:** Homeowners use smartphone applications or web interfaces to control lighting, thermostats, security cameras, and appliances from anywhere in the world.
- **Automation:** Devices communicate with each other over local networks (like Wi-Fi, Bluetooth, Zigbee, or Z-Wave) and a central hub to trigger actions automatically (e.g., lights turning on when motion is detected).

- **Energy Management:** Smart thermostats and lighting systems use sensors and network connectivity to learn usage patterns and optimize energy consumption, often providing users with feedback on their usage data.
- **Security and Safety:** Networked security cameras, smart locks, and sensors (smoke, water leak) provide real-time alerts to homeowners' devices and can even contact authorities in emergencies.

Industrial IoT (e.g., SCADA)

Supervisory Control and Data Acquisition (SCADA) systems, enhanced by Industrial IoT (IIoT), use network applications for large-scale industrial process monitoring and control.

- **Real-time Data Acquisition:** Sensors and Remote Terminal Units (RTUs)/Programmable Logic Controllers (PLCs) collect vast amounts of data from the field and transmit it over networks (including Ethernet, Wi-Fi, and 5G) to a central supervisory system.
- **Supervisory Control and HMI:** Operators interact with the system via Human-Machine Interfaces (HMI), which are network-based graphical dashboards, to monitor processes, analyze data, and issue control commands (e.g., adjusting a flow rate or stopping a machine).
- **Predictive Maintenance:** Data analysis applications use the gathered data to predict equipment failures, allowing for proactive maintenance and reduced downtime, a significant improvement over traditional systems.
- **Cloud Integration:** The integration of cloud computing allows for enhanced data storage, advanced analytics, and remote accessibility of SCADA systems, which were traditionally limited to local networks.

DNS in Browser Communications

The Domain Name System (DNS) is a crucial application-layer protocol that acts as the internet's phonebook, translating human-readable domain names into machine-readable IP addresses.

- **Client-Side:** When a user types a URL into a browser, the browser (the DNS client) first checks its local cache and the operating system's cache. If the address is not found, the client sends a DNS query to a local DNS recursive resolver (usually provided by the ISP).
- **Server-Side:** The recursive resolver interacts with a hierarchy of DNS servers (root, TLD, and authoritative name servers) to find the correct IP address. The authoritative name server, which holds the actual DNS records for the domain, returns the IP address to the resolver. The resolver then sends this IP back to the client, allowing the browser to initiate a direct HTTP request to

the web server at that IP address. The server then sends the webpage files back to the browser for display.

IP Addressing in 5G & Cloud

Proper IP addressing is fundamental for connectivity, scalability, and security in both 5G and cloud environments.

- **5G Networks:** 5G networks are designed to support a massive number of devices (mMTC - massive machine-type communications), making **IPv6** the cornerstone technology due to its vastly larger address space (340 undecillion addresses vs. IPv4's 4.3 billion). 5G also utilizes dynamic IP allocation, often using internal enterprise DHCP systems for 5G LANs, and employs Network Address Translation (NAT) in mobile routers to manage IP addresses efficiently.
- **Cloud Computing:** Cloud platforms allocate both **public** (internet-accessible) and **private** (internal-only) IP addresses to virtual machines (VMs), containers, and other resources. Dynamic IP addressing (via DHCP) is widely used for temporary resources, while static IPs can be assigned for stable services. NAT is commonly used to allow resources with private IPs to communicate with the external internet securely.

DHCP in Enterprise Wi-Fi Networks

The Dynamic Host Configuration Protocol (DHCP) is a critical application protocol in enterprise Wi-Fi networks.

- **Automatic Configuration:** DHCP automates the process of assigning IP addresses and other network configuration parameters (like subnet mask, default gateway, and DNS server addresses) to client devices (laptops, smartphones, etc.) as they connect to the network.
- **Efficient Management:** Instead of manually configuring each device's IP address, which is inefficient in a large, dynamic enterprise setting, DHCP allows for centralized management and dynamic allocation from a pool of available addresses.
- **Address Reusability:** DHCP uses a lease mechanism, allowing it to reclaim and reallocate IP addresses that are no longer in use, ensuring efficient use of the limited IPv4 address space often still present in enterprise networks.