Computer Networks

Network : Computers connected together.

Internet : Collection of these computer networks.

Protocol : a protocol is a set of rules and conventions that dictate how data is formatted and transmitted over a network.

Types : TCP, UDP, IDP

TCP :

TCP, or Transmission Control Protocol, is a core communication protocol that operates at the transport layer of the Internet Protocol (IP) suite. It is designed to provide reliable, connection-oriented communication between devices on a network. TCP ensures the accurate and orderly transmission of data by incorporating mechanisms for error checking, flow control, and sequential data delivery.

UDP :

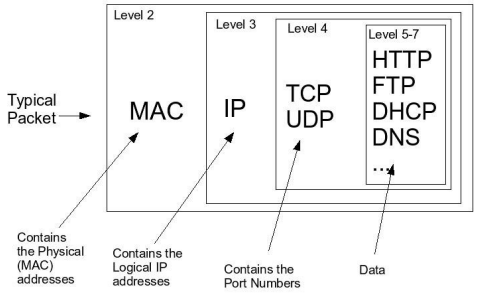
UDP is a connectionless, lightweight transport layer protocol in the Internet Protocol suite. It provides fast, low-latency communication without guarantees of packet delivery or order. UDP is often used in real-time applications like online gaming and streaming where speed is prioritized over reliability.

HTTP :

HTTP, or Hypertext Transfer Protocol, is the foundation of data communication on the World Wide Web. It defines how messages are formatted and transmitted, allowing for the exchange of text, images, videos, and other multimedia content between web browsers and servers. HTTP operates over a client-server model where requests from clients (such as web browsers) are responded to by servers, enabling the retrieval and display of web content.

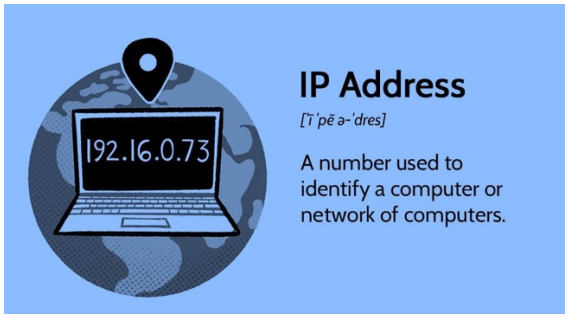
Packets :

Packets are small units of data used for transmission over a network. Each packet typically includes both the actual information being sent and control information, such as source and destination addresses, enabling efficient and reliable data transfer across computer networks.



IP Address :

An IP address, or Internet Protocol address, is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves two main purposes: identifying the host or network interface and providing the location of the host in the network. IP addresses are essential for routing data packets between devices on the Internet. There are two types of IP addresses: IPv4 addresses, expressed as four sets of numbers separated by dots (e.g., 192.168.1.1), and IPv6 addresses, which use a longer alphanumeric format to accommodate the growing number of devices on the internet.



1) LAN (Local Area Network):

A LAN is a network that is limited to a small geographic area, such as a single building, office, or campus.

Devices within a LAN can communicate with each other directly at high data transfer rates. LANs are often used for local resource sharing, such as printers and files, and to facilitate communication among devices.

2) WAN (Wide Area Network):

A WAN is a network that covers a broad geographic area, potentially spanning cities, countries, or even continents.

WANs connect multiple LANs and use various communication technologies, such as leased lines, satellites, and public networks (like the Internet). WANs enable long-distance communication and the sharing of resources over vast geographical distances.

3) MAN (Metropolitan Area Network):

A MAN is a network that falls between a LAN and a WAN in terms of geographic scope, typically covering a metropolitan area like a city.

MANs provide connectivity to a larger geographical area than LANs but are more localized compared to WANs. They are often used to connect multiple LANs within a city, facilitating efficient communication and resource sharing over a larger region.

Modem :

A modem, short for modulator-demodulator, is a device that enables digital data to be transmitted over analog communication channels. It converts digital data from a computer or other digital devices into analog signals for transmission over analog communication lines, such as telephone lines or cable systems. At the receiving end, the modem demodulates the analog signals back into digital data.

Router :

data traffic between them. It operates at the network layer of the OSI (Open Systems Interconnection) model and plays a crucial role in routing data packets between devices on a local network and other networks, such as the Internet.

ISP :

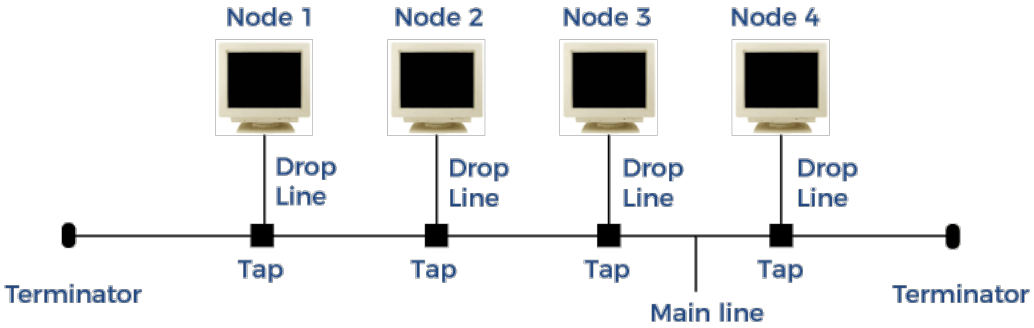
ISP stands for Internet Service Provider. An ISP is a company or organization that provides internet access to customers. ISPs offer a range of services, including connecting users to the internet, hosting websites, and offering email services. They facilitate the transfer of data between the user's devices and the global network of the internet.

Topologies :

Network topology refers to the layout or arrangement of devices and connections in a computer network. Different topologies dictate how devices are connected and how data is transmitted between them. Here are some common network topologies:

1) Bus Topology:

In a bus topology, all devices share a single communication line, known as the bus. Data travels along the bus, and each device has a unique address. When a device wants to communicate, it sends the data to the bus, and all devices receive the data. However, only the intended recipient processes the data.



Bus Topology

Advantages: Simple and easy to implement.
Disadvantages: Limited scalability and potential for collisions.

2) Ring Topology:

In a ring topology, devices are connected in a closed loop or ring. Each device is connected to exactly two other devices, forming a circular path for data transmission. Data travels in one direction around the ring.

Advantages: Simplicity and equal access to the network.
Disadvantages: Network failure at one point can disrupt the entire network.

3) Star Topology:

In a star topology, all devices are connected to a central hub or switch. Devices communicate with the hub, which manages data flow. If one device wants to communicate with another, it sends data to the hub, which then forwards it to the intended recipient.

Advantages: Centralized management, easy to add or remove devices.
Disadvantages: Dependence on the central hub; if it fails, the network may be affected.

4) Tree Topology:

In a tree topology, network devices are arranged in a hierarchical structure resembling a tree. This topology combines characteristics of the bus and star

topologies, offering a centralized main bus (backbone) with branches connected to it in a hierarchical manner.

5) Mesh Topology:

In a mesh topology, every device is connected to every other device in the network. This provides multiple paths for data transmission, enhancing reliability and fault tolerance.

Advantages: Redundancy and fault tolerance.
Disadvantages: Costly to implement and complex to manage in large networks.

OSI Model :

The OSI (Open Systems Interconnection) model is a conceptual framework that standardizes the functions of a telecommunication or computing system into seven abstraction layers. Each layer serves a specific purpose and interacts with adjacent layers, allowing for interoperability between different systems and devices. The layers, from the lowest to the highest, are as follows:

Physical Layer (Layer 1):

Deals with the physical connection between devices, specifying hardware characteristics such as cables, connectors, and signaling.
Functions: Transmitting raw binary data over a physical medium.

Data Link Layer (Layer 2):

Manages the link between directly connected nodes, addressing issues such as framing, error detection, and flow control.
Functions: Organizing raw bits into frames, ensuring reliable point-to-point communication.

Network Layer (Layer 3):

Concerned with logical addressing, routing, and forwarding of data between devices on different networks.
Functions: Determining the best path for data to travel across multiple networks.

Transport Layer (Layer 4):

Provides end-to-end communication, ensuring data integrity, error recovery, and flow control.
Functions: Segmenting, reassembling, and managing data flow between source and destination devices.

Session Layer (Layer 5):

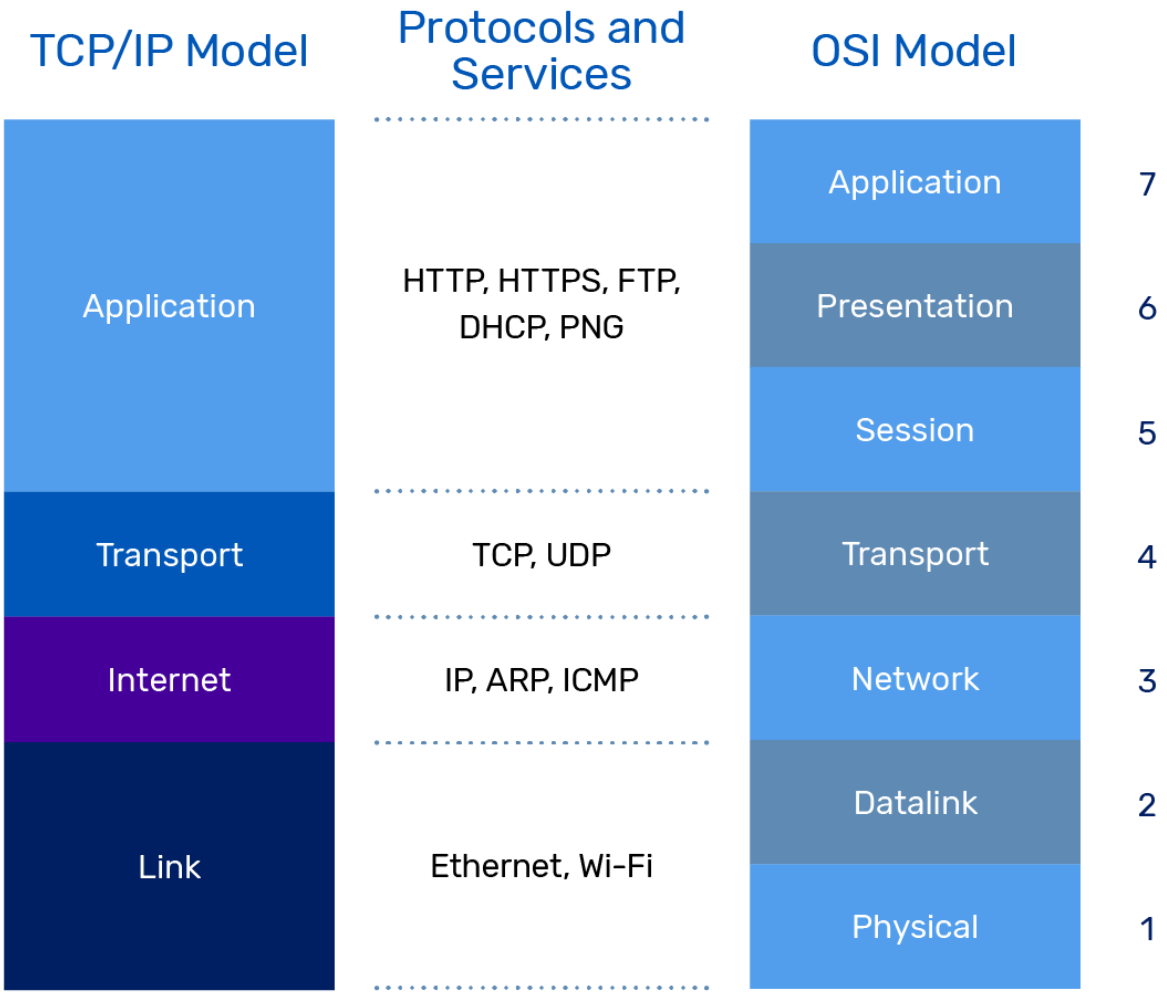
Manages sessions or connections between applications on different devices.
Functions: Establishing, maintaining, and terminating communication sessions.

Presentation Layer (Layer 6):

Concerned with data format translation, encryption, and compression to ensure that data is presented in a readable format.
Functions: Translating data formats, handling encryption and compression.

Application Layer (Layer 7):

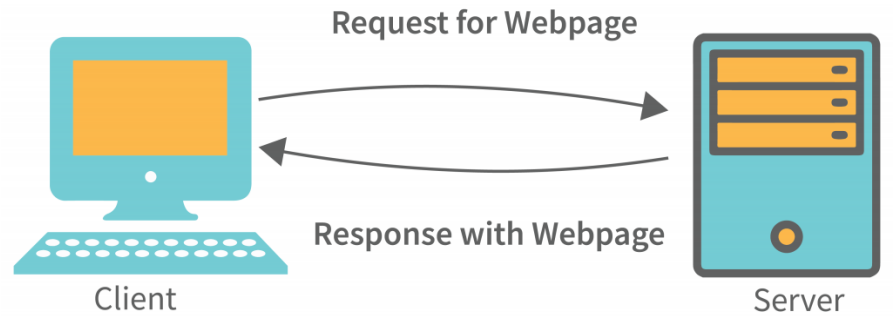
Provides network services directly to end-users and applications, supporting communication between software applications.
Functions: Interacting with software applications, providing network services, and managing user interfaces.



Architectures :

1) Client – Server Architecture :

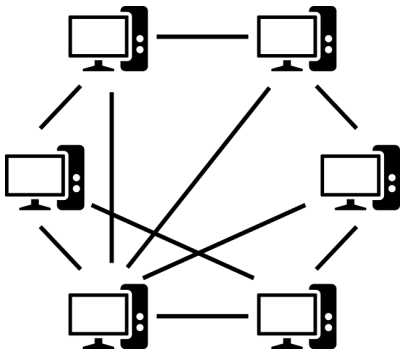
Client-server architecture is a computing model where clients, such as software applications or devices, request services or resources from servers. In this model, clients initiate requests, and servers fulfill these requests by providing the necessary services or resources. Clients handle user interactions and present information, while servers manage data storage, processing logic, and resource sharing. The communication follows a request-response pattern, creating a structured framework for networked applications. Examples include web browsers (clients) requesting web pages from web servers.



In the client-server interaction, clients send requests specifying the desired services, and servers respond with the requested information. This architecture allows for centralized control over data and processing, facilitating efficient resource management. While it provides scalability and centralized management advantages, the model may face challenges such as single points of failure and potential network congestion due to heavy client requests. Overall, client-server architecture is a foundational framework for various networked applications, enabling structured communication between clients and servers.

2) Peer to Peer Architecture :

Peer-to-peer (P2P) architecture is a decentralized network model where devices, referred to as peers, communicate and share resources directly with each other without the need for a centralized server. In a P2P network, each peer has both client and server capabilities, allowing them to both request and provide resources. This architecture is often associated with file sharing and collaborative applications.



In a P2P network, each peer can act as a client by making requests for resources and as a server by responding to requests from other peers. There is no central point of control, and each peer has equal status in the network. Peers can dynamically join or leave the network without affecting its overall functionality.