**Computer Networking**

**Computer Network –** A group of computers which are connected to each other for the purpose of sharing their resources, called as computer network.

Computer Networking is the practice of connecting computers together to enable communication and data exchange between them.

Network is nothing more than two connected computers sharing resources with one another.

Network connection is of two types –

* Physical Connection – Connection through the wires, cables etc. which is connected by network interface card which allow them to communicate with eacth other
* Logical Connection – Sharing the data across the computers through the physical connection.

Basic Networking Rules –

* Computers in network must use the same procedures for sending and receiving of data, called as ‘Communication Protocol’
* Data must delivered uncorrupted
* Computers in a network must be capable of determining the origin and destination of the information. (ip & mac address)

Types of Computer Netwoks –

1. Personal Area Network (PAN)
2. Local Area Network (LAN)
3. Wireless Local Area Network (WLAN)
4. Campus Area Network (CAN)
5. Metropolitan Area Network (MAN)
6. Wide Area Network (WAN)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| PAN | LAN | WLAN | CAN | MAN | WAN |
| - Ultra small networks use to share data from one device to another.  - e.g  smart phone to laptop,  smart watch to smart phone | A computer network within a small geographical area such as single room, building   * e.g   Home Network, Small Office Network | A LAN that is fully dependent on wireless connectivity.  Most home networks are WLAN.   * e.g   wifi | A computer network of multiple interconnected LAN’s in a limited geographical area.   * e.g   College campus, business campus | A computer network that interconnects users with a computer resources in a city   * e.g   cable TV network,  telephone company network | A computer network that extends over a large geographical distance, typically multiple cities and countries   * e.g   Internet |

Network Architecture –

Network architecture refers to the design and structure of a computer network, specifying its layout, components, protocols, and technologies.

Network architecture is like the blueprint for a computer network, showing how devices connect and communicate with each other.

|  |  |
| --- | --- |
| Client Server | Peer to Peer |
| Client-server architecture is a common computing model where one system (the client) requests services or resources from another system (the server). This model is prevalent in many types of applications and services. Here are some examples of client-server systems:  Web Browsers and Web Servers: When you use a web browser (client) to access a website, it sends a request to the web server hosting that site. The server processes the request and sends back the web page content, which the browser displays.  Email Clients and Email Servers: Email clients (e.g., Microsoft Outlook, Gmail) communicate with email servers (e.g., Microsoft Exchange, IMAP/SMTP servers) to send, receive, and store emails.  File Sharing: In networked environments, client computers request files or data from file servers. This is commonly used in enterprise settings for file storage and sharing.  Database Systems: Clients (e.g., desktop applications, web applications) interact with database servers to perform data retrieval, storage, and manipulation. SQL databases like MySQL, PostgreSQL, or Oracle are examples.  Print Servers: Clients send print jobs to a print server, which manages and coordinates the printing process for various printers.  Game Servers: Multiplayer online games often employ client-server architecture. The game clients connect to a central game server that manages game sessions, player interactions, and game state.  DNS (Domain Name System): When a client requests a web address, it communicates with DNS servers to resolve the domain name to an IP address, allowing the client to connect to the appropriate web server.  Remote Desktop Services: Clients can remotely access the desktop and applications of a remote server, often used for system administration, technical support, or remote work scenarios.  Chat and Instant Messaging: Clients connect to chat servers to send and receive messages in real-time. Examples include applications like WhatsApp, Slack, and Skype.  Client-server architecture is fundamental to modern networking and computing, enabling the efficient distribution of services and resources across networks and the internet. | Peer-to-peer (P2P) architecture is another common computing model in which individual devices, or "peers," directly communicate and share resources with each other without the need for a centralized server. Here are some examples of peer-to-peer systems:  1. File Sharing: P2P file-sharing networks, such as BitTorrent, allow users to share files directly with one another. Users download pieces of a file from multiple peers simultaneously, making it efficient for distributing large files.  2. Instant Messaging: Some instant messaging applications, like early versions of Skype, used a P2P model for communication. Users' devices directly exchanged messages and calls without central servers mediating the communication.  3. Voice and Video Calls: Some voice and video calling applications, like early versions of Skype, also used a P2P model for direct communication between users.  4. Collaborative Software: Certain collaborative software tools, like some peer-to-peer collaboration platforms or decentralized project management tools, enable users to share files and information directly without relying on central servers.  5. Decentralized Cryptocurrencies: Blockchain-based cryptocurrencies, like Bitcoin, use a P2P network to validate and record transactions. Nodes in the network communicate directly to maintain the blockchain.  6. P2P Streaming: Some media streaming services use P2P technology to distribute content. Users share parts of the content with each other, reducing the load on centralized servers.  7. Gaming: Some online multiplayer games use a P2P model, allowing players to connect directly to each other to facilitate gameplay. This is different from dedicated game servers, which are a client-server model.  8. IoT Device Communication: In some Internet of Things (IoT) scenarios, devices communicate with each other directly using P2P connections. For example, smart home devices like lights and sensors may communicate directly with each other for control and data sharing.  9. Mesh Networks: Mesh networks, used in some wireless networking scenarios, enable devices to relay data directly to each other, creating a self-healing and self-routing network without a centralized server.  Peer-to-peer architecture is known for its decentralized nature, which can provide benefits like robustness and scalability. However, it may face challenges in terms of security and stability, particularly in larger networks or systems where centralized control and management are required. |

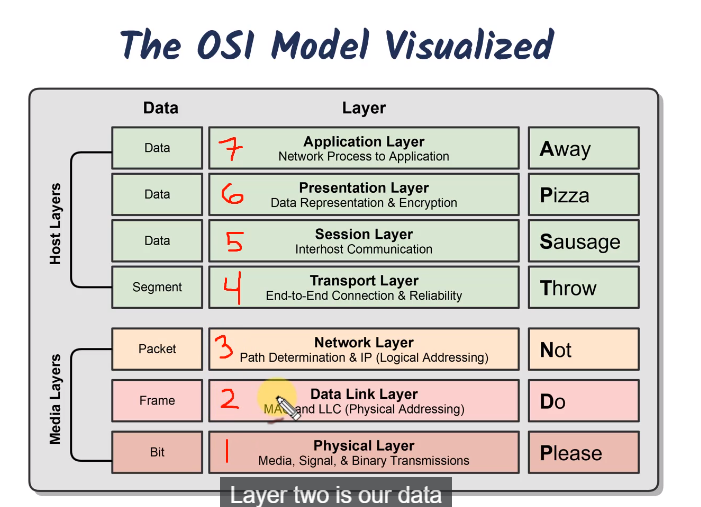
Computer Networking Protocols

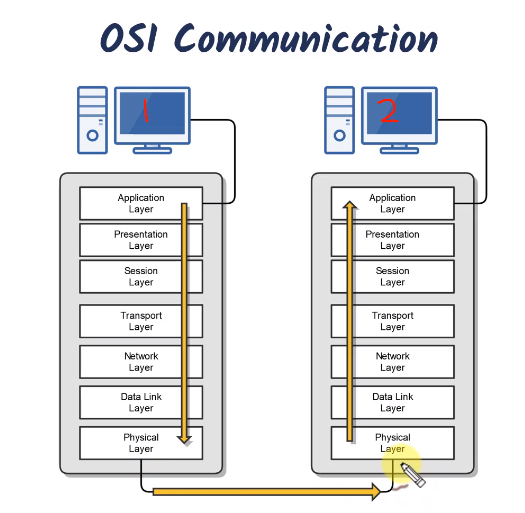
Computers communicate with each other with protocol. Protocols are rules which sets that how machines exchange data and enables effective communication. It is a set of rules and conventions that govern how data is transmitted, received, and processed in a computer network, ensuring that devices can communicate effectively.

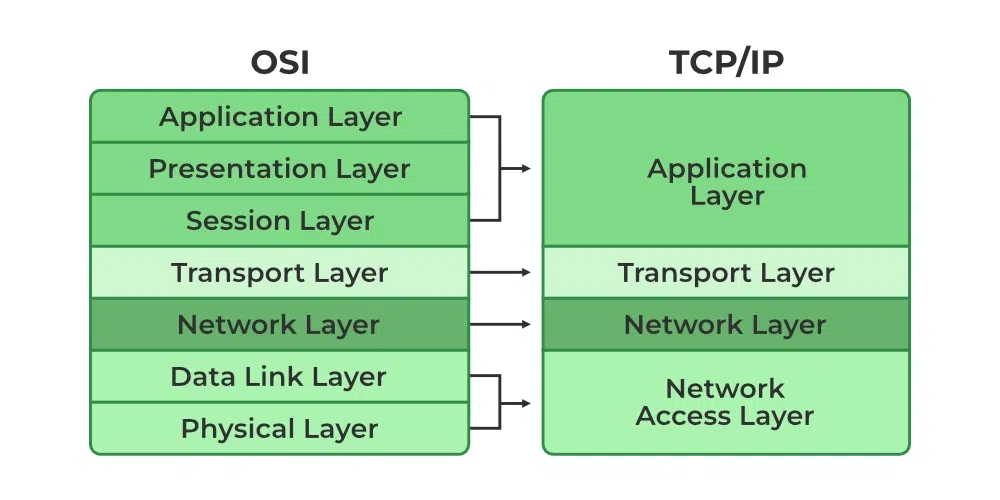
Common networking protocols include TCP/IP (Transmission Control Protocol/Internet Protocol), HTTP (Hypertext Transfer Protocol), and SMTP (Simple Mail Transfer Protocol).

Open System interconnection (OSI Model) –

This conceptual framework shows that how data is transmitted from one system to another system throughout the network. It gives an idea that how network operate. This model never implemented (only regference model to understand the data flow) while TCP/IP model used over an OSI Model







TCP/ IP Model

Transmission Control Protocol/ Internet Protocol

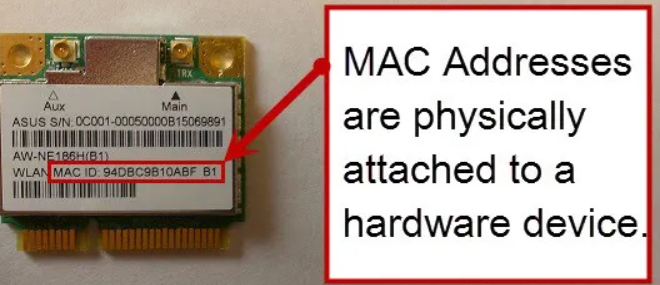
Most commonly used protocol suite in the networking world.

It is the standard of the computer networking

It is based on a 4 layer model which is same like an osi model.

MAC Adrresses

Media Access Control (MAC) it is also known as a hardware address



or physical address is a unique number assigned & written on

network interface card (NIC)/ Network Adapter card in the device.

It works in OSI Model 1st & 2nd layer ( Physical & Data Link layer)

and in TCP/IP model works in 1st layer ( Network Access Layer)

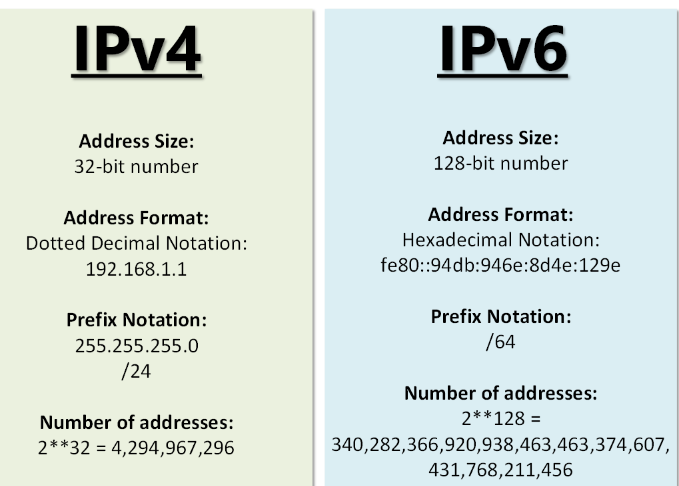
Represented in 6 bytes ( Hexadecimal) which is 48 bits, 1st 3 bytes (24 bits) assigned by the IEEE (Institute of Electrical and Electronics Engineers) to the manufacturer( like, dell, hp) . This 3 bytes also known as OUI ( organizationally unique Identifier).

Last 3 bytes (24 bits) are assigned sequentially, which are unique numbers.

There are approximate 16.7 million unique mac addresses.

Used over an LAN network.

IP Address



Internet Protocol – It is a logical address

(not physically written anywhere) used for

identifying and locating devices on a network.

Associated with ‘network Layer’ in both OSI

(layer 3) & TCP model (layer 2).

There are 2 versions of Ip address 1. IPv4 2. IPv6

This IP addresses are assigned by a Network

Administrator or Internet Service Provider (ISP)

Used over WAN network.

Duplex Communication

Duplex communication refers to the two different modes in which data can be transmitted between two devices.

Half duplex communication – Can send or receive data, but not both at the same time.

Full Duplex communication : Can send & receive data simultanrously.

Network Transmission Types

It is the process of sending data between devices or nodes in a computer network.

Unicast - One to one communication at a time. ( Communicate with 1 machine at a time)

Multicast – one to many communication at a time ( can communicate with multiple machines at a time)

Broadcast – One to all communication at a time ( Can communicate with all the the machines at a time )

Ethernet

It is a widely used technology for connecting devices in a local area network (LAN).It uses cables to transmit data between computers, printers & others devices It typically involves connecting devices to a central hub or switch, which acts as a traffic cop, directing data to the right destination.

Network Topology

Network Topology is the physical and logical arrangements of nodes and connection in a computing network. Different networks have different needs, which is why a variety of network topologies exist.

Physical Network Topology : Describes the placement of network devices and how they are physically connected.

Logical Network Topology : It describes the how data flows through the network

Wired Network Topology

|  |  |  |  |
| --- | --- | --- | --- |
| BUS | RING | STAR | MESH |
| Devices are connected via T-connector.  Al devices are connected to a single coaxial network cable.  Only one device can be active at a time on a network.  Antiquated Topology. (No more in use) | All devices are connected in a circular fashion.  Each computer connected to a 2 other computers.  Failure of single node can take down the entire network.  Data travels either Unidirectional or  Bidirectional. | All devices are connected to central connecting device which is usually ‘switch’.  Used in large and small networks.  Central device is a single point of failure. | All the devices are connected to each other by separate cabling.  Expensive to install  Commonly used in WAN’s |

Wireless Network Topology

Wireless Network utilize radio frequencies to communicate . There are 3 specific topologies in it 1. Ad hoc 2. Infrastructure 3. Mesh

1. Ad hoc Topology – Peer to Peer wireless network where no wireless access point (wap) infrastructure exists. In this topology One device connecting to another device over a wireless network . e.g. Personal Area Network
2. Infrastructure - Wireless commonly uses a wireless acess point (WAP) as its central connecting device. Commonly used in homes and small offices.
3. Mesh - Wireless mesh networks are ideal for applications that need flexibility, quick deployment, and mobility, such as outdoor public Wi-Fi, smart outdoor lighting, or emergency response networks.

Networking Devices - This are hardware equipment’s that play a crucial role in the communication and data exchange within a computer network.



1. Network Interface Card – This network adapter

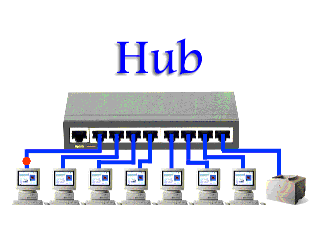
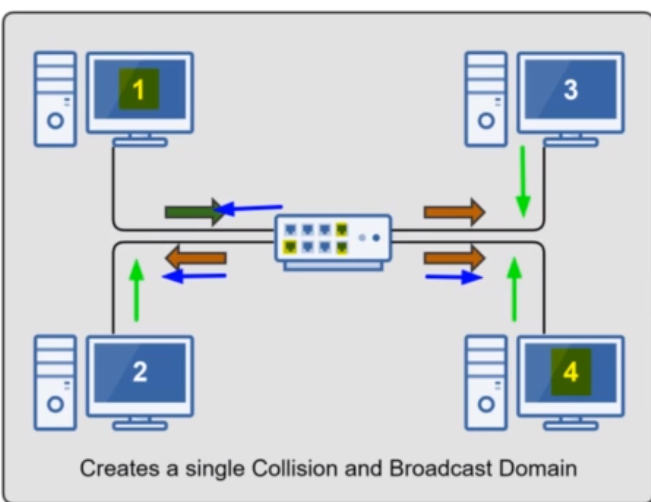
is already installed in a networking device.

This allow a device to connect to a network.

It serves as a bridge between a computer and the network.

It enables a computer to connect to and communicate with a network , facilitating data transmission and network access.

Also known as Network Interface Controller, Network adapter, LAN adapter & ethernet card.



1. Hubs – Used to connect devices together within

a network. Used in early networks, replaced by Switches.

Hubs are basic networking devices

that broadcast data to all connected devices, while switches

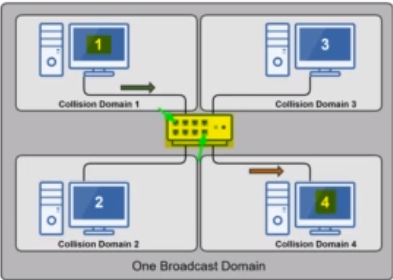
are smarter devices that selectively forward data only to the

intended recipient, making switches more efficient and secure.

Dumb network device (OSI layer 1)

“Multi-port Repeater” ( If there are 4 computers in star topology connected by hub. And computer wants to send something to computer 4, it will send the data to computer 4 as well as computer 1& 3 also.)

1. Switches – Connects devices same like hub. Integillient network device (OSI layer 2)



Memorizes the MAC address of each device

connected to it via MAC Address Table, Sometimes

called as “content addressable memory (CAM)

table. More fast, secure & accurate than hub.

Standard in today’s network infrastructure.



1. Wireless Access Point (WAP) – It is a device that

extends the wired network to wireless network.

( It’s basically use to extend the the range of router,

and it looks also same like a router only this doesn’t

have ports) Routers can be used as a WAP but WAP

cannot used as a “Router”. Its OSI 2nd layer device which is “Data Link layer”.



1. Wireless Ranger Extender – Extends the range

of wireless network by acting as a wireless repeater.

The range of it is around 50-100 feets indoors.

It works same like a WAP .

1. Router -

1st computer Network – **ARPANET**

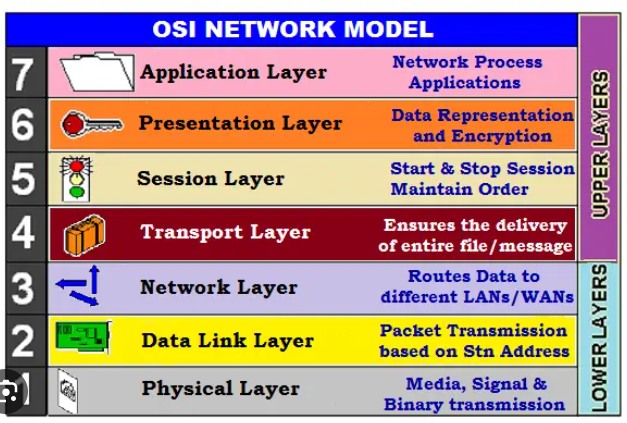
* **Advanced Research Project Agency Network**

**Characteristics of Computer Network –**

1. Resource Sharing
2. Communication Speed
3. Backup
4. Scalability
5. Reliability
6. Software & Hardware Sharing
7. Security

**Computer Networking Layers**

Computer Networking architecture is layers to promote modularity, interoperability, and efficient troubleshooting, making it easier to design, maintain, and scale complex networks.



Computer networking like building

with colorful building blocks. To make things easier,

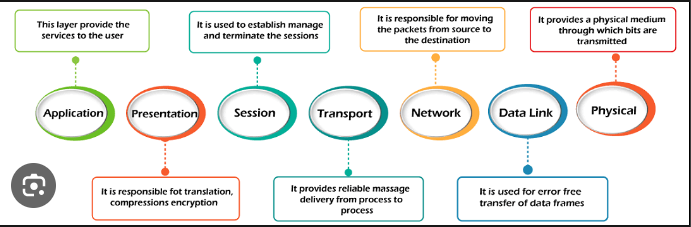
we stack these blocks in layers.

**Modularity:** Each layer is like a different type of block,

and they fit neatly on top of each other. It's like Lego blocks

that snap together. If you want to change something, you

can replace just one layer without affecting the others.



**Interoperability:** These blocks are made to work together. Each layer has a specific job, and they talk to each other nicely. It's like puzzle pieces that all connect, so everything runs smoothly.

**Efficient Troubleshooting:** If something goes wrong, it's easier to figure out where the issue is because we have these clear layers. It's like finding a problem in one color of blocks without messing up the rest.

The most commonly referenced model for understanding these layers is the **OSI (Open Systems Interconnection)** model, which consists of seven layers. Here's an overview of each OSI layer and its functions:

Hub : It is a basic networking component that connects multiple devices together at the physical layer, broadcasting incoming data to all connected devices, but it lacks the intelligence to manage or route network traffic efficiently.

Switch : It is a more intelligent networking component that efficiently forwards data packets to their intended destinations within a local network, improving network performance compared to hubs.

Bridge : It is a networking component that connects and filters traffic between two or more network segments, making forwarding decisions based on the data link layer (Layer 2) addresses to improve network segmentation and security.

Gateway : It is a networking component that serves as an entry and exit point between two different networks or protocols, facilitating communication and data transfer between them, often connecting a local network to the internet.

Modem : A "modem device" (short for modulator-demodulator) is a device that converts digital data from a computer into analog signals for transmission over analog communication channels (like telephone lines or cable systems) and vice versa, allowing computers to communicate with each other or access the internet through these channels

Router :

Repeater : It is a hardware component that amplifies and retransmits network signals to extend the reach of a network, improving the signal quality and allowing data to travel over longer distances.

**Basic Terminology of computer Network :**

1. **Network :** It is a collection of computers and devices that are connected together to enable communication and data exchange.
2. **Nodes :** It can be a device such as computer, smartphones or server, that is connected to a network, can be used for to share the data and information.
3. **Protocol :** It is a “set of rules” which are used in a digital communication to connect network devices and exchange information between them.
4. **Topology :** Topology means physical and logical arrangement of nodes on a network. E.g. bus, star, mesh, ring, tree
5. **Service Provider Networks:** A network operated by a company or organization that provides telecommunications, internet, or other communication services to customers. These networks are responsible for transmitting data, voice, and other types of communication between different locations, often over long distances
6. **IP Address:** An IP address is a unique numerical identifier that is assigned to every device on a network. IP addresses are used to identify devices and enable communication between them.
7. **DNS :** "Domain Name System."

DNS is like the internet's phone book. It is a system used to translate human-friendly domain names, like www.example.com, into the numerical IP (Internet Protocol) addresses that computers use to identify each other on the internet.

1. **Firewall :** Firewall is a system that designed to prevent unauthorized access from entering a private network. Network administrator creates a “Access Control List” which has the information of ip address, protocol, Destination and port number, So accordingly Network Administrator sets a rules/list in firewall that which ip address need to allow & which need to deny.

Public IP vs Private IP

|  |  |
| --- | --- |
| Public IP | Private IP |
| 1. Public IP are used on global internet and It is a globally unique address that is assigned to a device by an Internet Service Provider (ISP) or network administrator. 2. Public IP addresses are used for communication between devices on the internet. When you access a website, send an email, or stream a video online, your device uses its public IP address to interact with other devices on the internet. 3. Public IP addresses are typically written in standard decimal notation, such as "203.0.113.1" or "8.8.8.8." 4. It's important to note that public IP addresses are a finite and exhaustible resource, and their allocation is carefully managed to ensure the efficient use of address space. The transition to IPv6, which offers a vastly larger pool of IP addresses, is one of the strategies employed to address the growing need for unique IP addresses in the modern internet. | 1. Private IP are used in private networks. (home networks, corporate intranets, LAN) 2. Cannot directly access from the public network 3. Private IP addresses are not globally unique. 4. The assignment and management of private IP addresses are the responsibility of the local network administrator. 5. 5. Private IP addresses are also written in decimal notation, but they often fall within specific reserved address ranges, (e.g., 192.168.x.x, 10.x.x.x, 172.16.x.x to 172.31.x.x). These reserved ranges are defined by the Internet Assigned Numbers Authority (IANA) for private network use. |

Network Architecture –

It means network layout that tells how computers are arranged and how tasks are allocated to the computer.

Types of Computer Network Architecture :