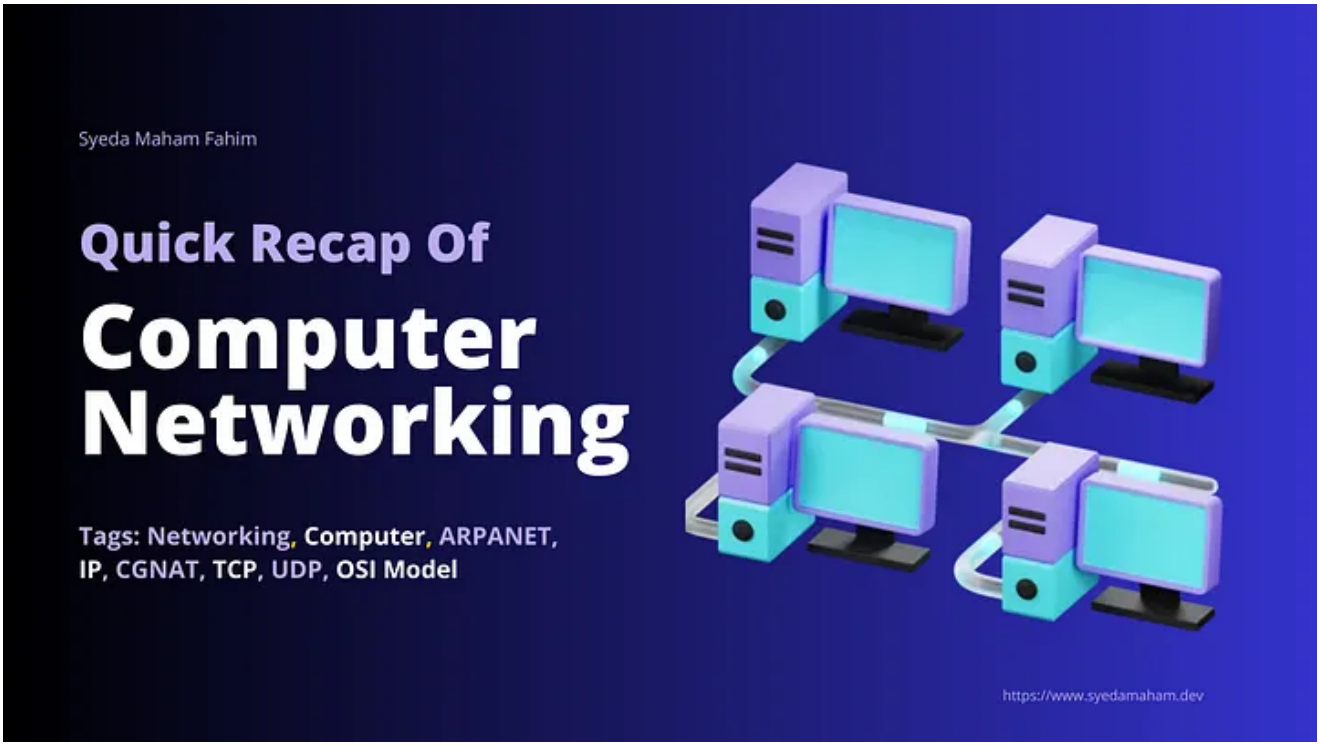
💻 Quick Recap of Computer Networking

SyedaMahamFahim · Follow
27 min read · Oct 9



Quick Recap to Computer Networking

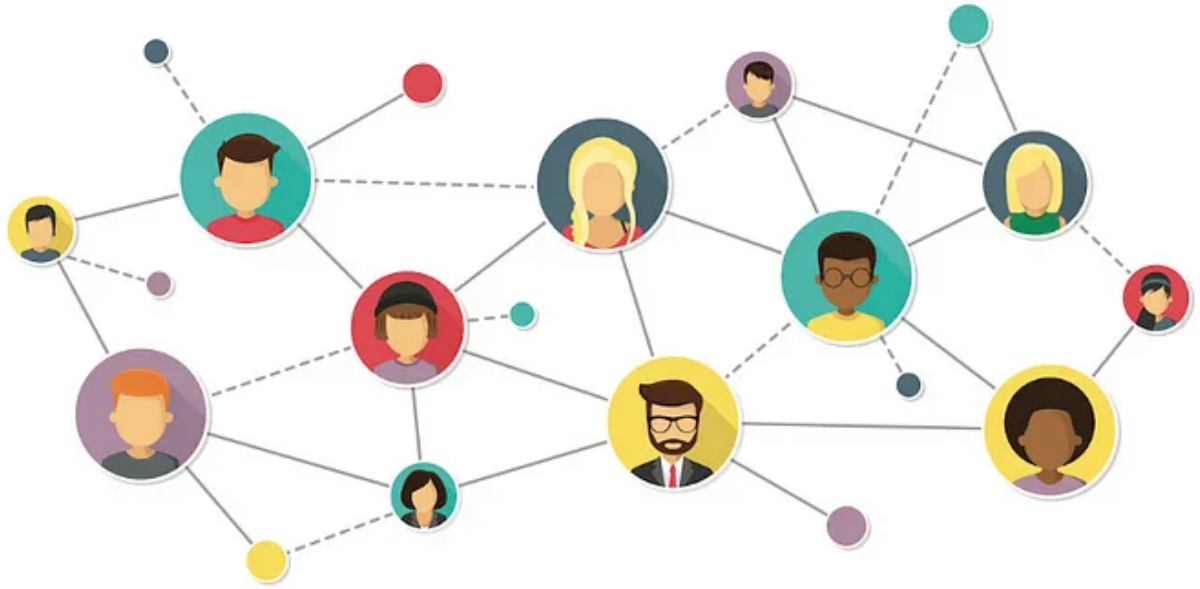
> *This articles serve as a comprehensive and concise review of fundamental computer networking concepts. It gives a quick overview for those who are already familiar with networking concepts, enabling them to efficiently refresh their knowledge.*

Think about a time when you chatted with a friend online or streamed a video. Ever wondered how all that works behind the scenes? It's like a big puzzle called computer networking. Let's dive into the basics of this fascinating topic and see why it matters in our connected lives.

Let's first understand the basic understanding of two words i.e. `Networking` and `Computer Networking`

Networking

Before we explore the concept of networking in computers, it is important to understand its significance in our daily lives. Networking involves establishing connections and building relationships with other individuals, particularly when it comes to meeting new people. This process allows us to expand our social and professional circles, exchange information and ideas, and potentially open up new opportunities for collaboration and growth.



Source: Lenfest Institute

Now, in the computer world, Networking is like the magic that connects computers and devices together so they can talk to each other, With networking, we can share information, like messages or pictures, etc.

Computer Network

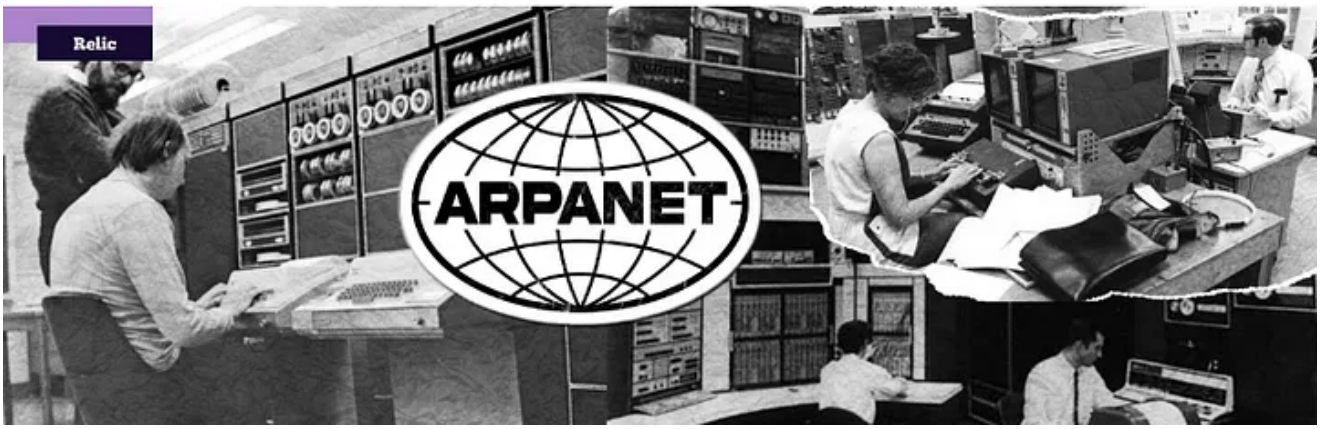
Computer networking is the art of connecting computers and devices together so they can share information and work as a team. Just like roads connect different places, computer networking connects different devices, like computers, smartphones, and servers, so they can communicate and exchange data. This is what makes the internet and all our online activities possible.

Source: The Techedvocate.org

How did it all start?

Have you ever wondered about the origins of this thing? Let's time-travel to the 1960s to understand this.

The breakthrough came in the 1960s with the creation of ARPANET, a pioneering computer network project funded by the U.S. Department of Defense's Advanced Research Projects Agency (ARPA, now known as DARPA). ARPANET was the first network to use the concept of "**packet switching,**" which involves breaking data into small packets and sending them separately through the network. This idea formed the basis of modern networking.



Source: Magzter.com

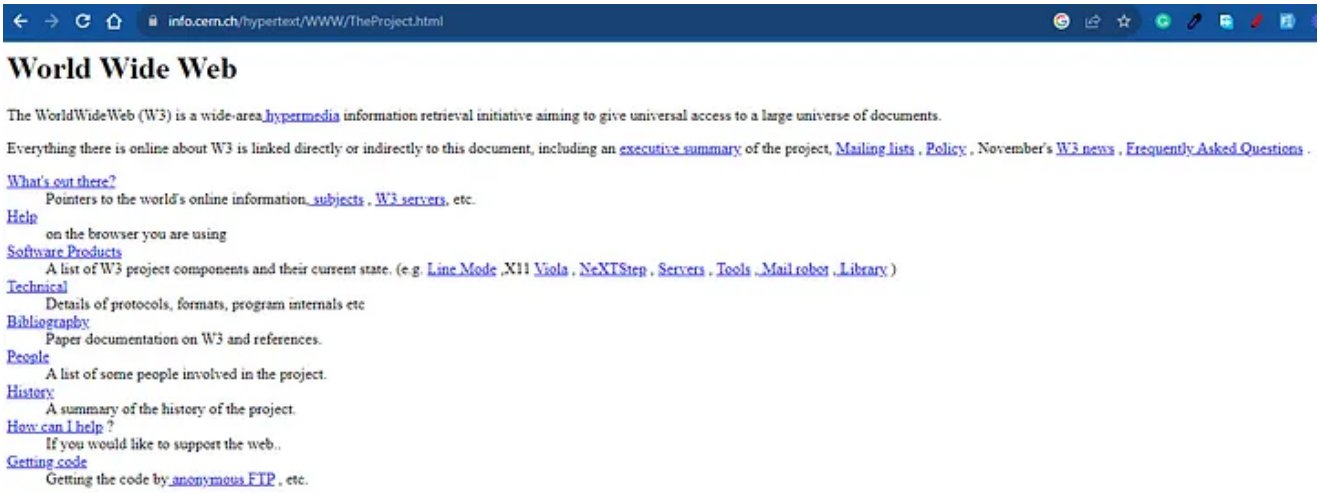
In 1969, the first message was sent over ARPANET between two computers located at the University of California, Los Angeles (UCLA) and the Stanford Research Institute (SRI).

At UCLA, a computer scientist named Leonard Kleinrock and his team developed the technology to send messages between computers using a process called packet switching. On October 29, 1969, Charley Kline, a student programmer at UCLA, attempted to send the word “LOGIN” to a computer at SRI over the ARPANET connection. The intention was to log in to the remote computer, but the system crashed after successfully sending just the letters “L” and “O.”

Despite the crash, this event was historically significant because it marked the first successful transmission of data between two computers connected by ARPANET, showcasing the potential of computer networks for communication.

Birth of the World Wide Web

The internet made significant progress after ARPANET, and the birth of the World Wide Web changed how people accessed it. Before the advent of the web, only research institutions and universities had internet access. Finding information required technical expertise in using command-line interfaces and directories. However, with the introduction of a user-friendly Graphical Interface, even non-technical people can easily access information. This innovation saved thousands of hours.



World First Website:

The web changed this landscape dramatically by

- introducing a user-friendly graphical interface.
- It standardized information organization
- introduced hyperlinks for seamless navigation
- incorporated multimedia elements, making web content engaging.
- Importantly, it democratized access, allowing people worldwide to connect via web browsers, erasing geographical and technical barriers.

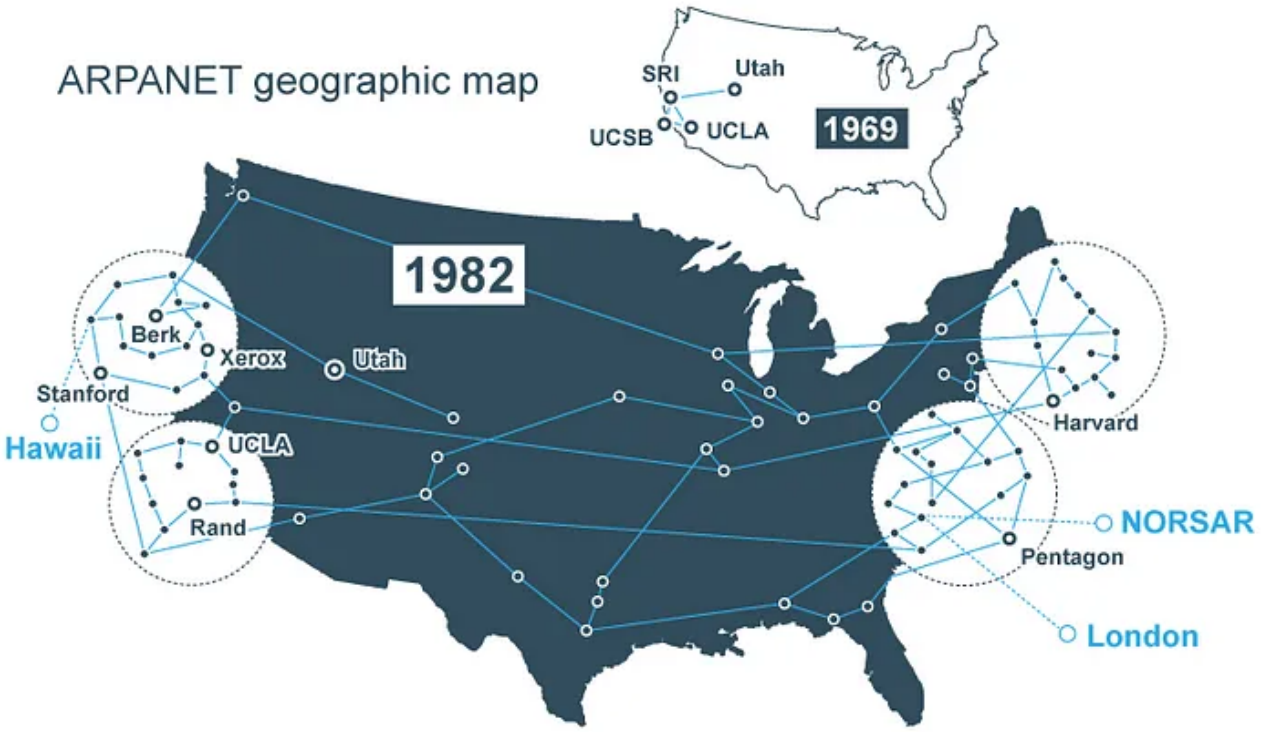
Before The Birth Of the Internet

Before the advent of computer networking and the widespread adoption of the internet, the methods we used to share information were quite different. Let's take a journey back in time to explore how people communicated and shared knowledge:

- Telephone
- Postal Mail
- Print Media
- Radio and Television (One-way communication)
- Fax Machine
- Face to Face Interactive
- Bulletin Board Systems (BBS)
- Local Networks

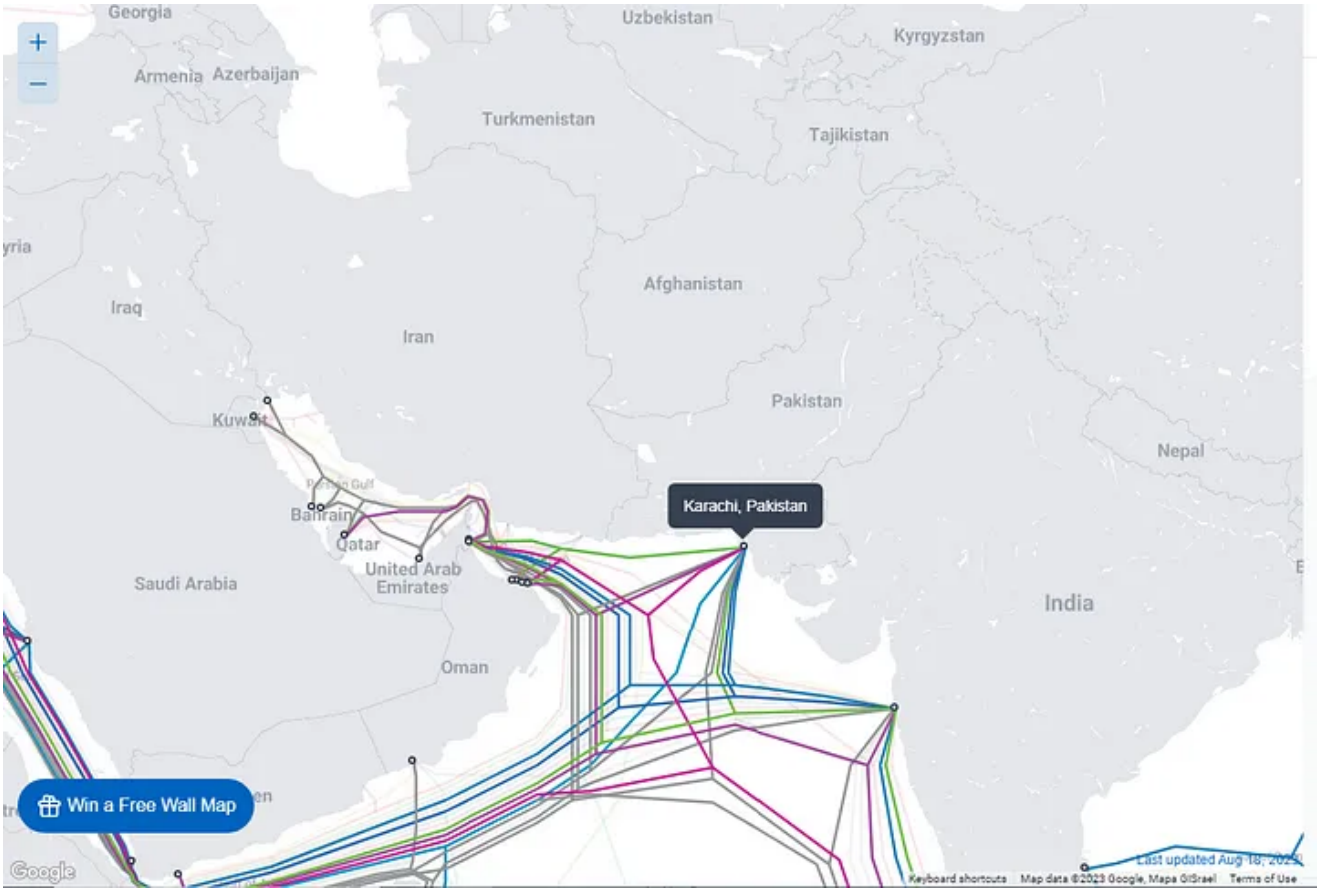
Today's Internet and ARPANET's Early Connectivity

Let's explore how today's internet is interconnected and take a journey back to understand how universities were connected through ARPANET.



Source: Portwsigger.net

The modern internet is a marvel of connectivity, today's internet relies on a mix of undersea cables, terrestrial wires, and satellites for global connectivity, while ARPANET's early days saw universities and research institutions connected through wired communication lines, It was a time when wireless technology was not as mature as it is today, and wired connections provided the reliability needed for this groundbreaking endeavour.



Cable Submarine

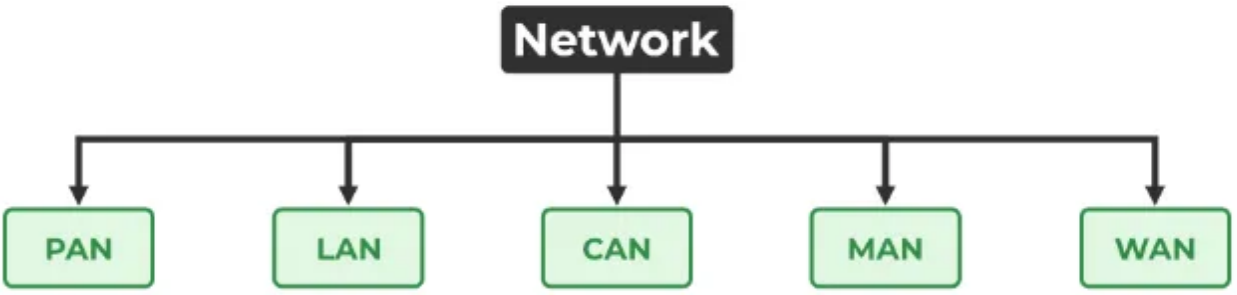
In this above screenshot, I have shown you how **Karachi, Pakistan** is connected to the global internet through the wire, You can explore how your country is connected to the world through wires using the website `https://www.submarinecablemap.com/`

Key Concepts in Computer Networking

First, we will explain some basic terms. After that, we will talk about how data is sent and received from the internet, and what happens behind the scenes.

1. Network Types

There are various types of networks, some of which are listed below:



Source: GreeksForGreeks

- **LAN (Local Area Network):** LANs cover small geographic areas like homes, offices, or campuses, connecting devices within that limited vicinity.
- **MAN (Metropolitan Area Network):** A network larger than a LAN but smaller than a WAN, usually covering a city or metropolitan area.
- **WAN (Wide Area Network):** WANs span larger geographical regions, linking multiple LANs, often utilizing public or leased communication lines.
- **PAN(Personal Area Network):** Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network, typically within a range of 10 meters.
- **Campus Area Network (CAN):** CAN is a group of interconnected LANs within a limited geographical area like a school campus, university campus, military bases etc.

2. Application Protocols

Protocols are rules that define how data is transmitted and received in computer networks. Just like we have rules for specific tasks at home, office, school, etc., in the online world, we call them Protocols

For example, in web communication, HTTP/HTTPS protocols are used to transmit and receive data, while for email, we use the SMTP protocol, etc. (We will discuss this in detail later in the article)

Internet Society

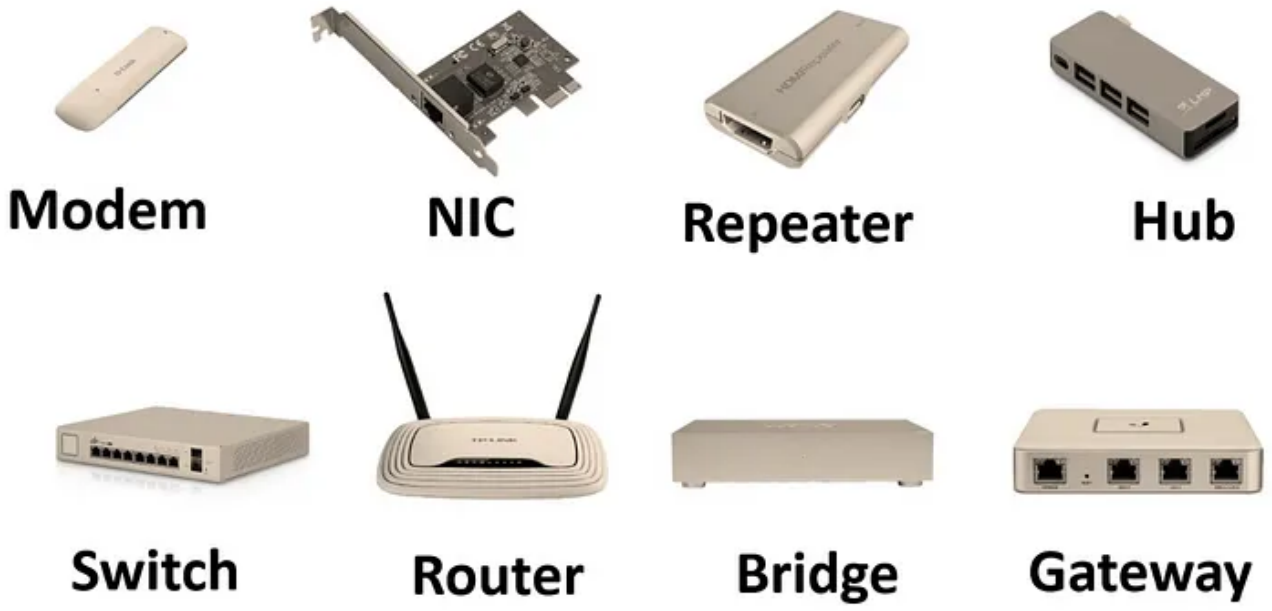
These protocols are designed by the ***Internet Society***.

Important Protocols

- **TCP:** It ensures data reaches its destination and doesn't get corrupted on its way
- **HTTP/HTTPS:** It is used in web communication. The data is being transferred between client and server.
- **FTP:** The File Transfer Protocol is instrumental in transferring files over a network.
- **SSH (Secure Shell):** Provides secure remote access to devices and servers over an encrypted connection.
- **SMTP (Simple Mail Transfer Protocol):** Used for sending email messages between email clients and servers.
- **POP3 (Post Office Protocol 3):** Retrieves email messages from a server to a client's computer.

3. Networking devices

Networking devices refer to hardware components or equipment used in computer networking to facilitate communication and data exchange between devices on a network.



Types of Network Devices

Source: IT release

Internal Devices

- **Network interface controller (NIC):** A hardware component that enables a computer to connect to a network, either wired or wirelessly.

External Devices

- **Router:** Connects different networks and directs data between them.
- **Modem:** Short for “modulator-demodulator,” it converts digital data from a computer into analogue signals for transmission over phone lines from ISP to our houses (for internet access) and vice versa.
- **Modem-Router-Dual**: The Internet is delivered from the modem to our houses and then distributed among our devices through a router. Nowadays, there are modem router-dual devices available which provide both functionalities in a single device.
- **Switch:** It helps all your computers and devices, like your tablet and game console, talk to each other and share things really fast. It connects devices within the same network, forwarding data based on MAC addresses.
- **Firewall:** Monitors and controls network traffic for security.

- **Cable:** Physical media (e.g., Ethernet cables) used to transmit data between devices in a network.
- **Hub:** An outdated network device that simply broadcasts data to all connected devices, less efficient than switches.
- **Repeater:** A repeater is used to extend the range of a radio signal so that the signal can cover longer distances, a repeater is an electronic device that receives a signal and re-transmits it.
- **Gateway:** A gateway is a device that connects different computers or networks, often dissimilar ones. It can also act as a switch. When a computer in a LAN network needs data, the gateway provides it if it's available in the LAN. If it's not, the gateway connects to the WAN to retrieve and transfer the data to the computer.

Portable Devices

- WIFI-Hotspot
- Portable Modem Dongle

4. ISP (Internet Service Provider)

- A company or organization that provides internet access and related services.
- Offers various connection methods (e.g., broadband, DSL, fibre optics, wireless).
- Connects individuals and businesses to the internet.
- May provide additional services like email, web hosting, and VPNs

Some of the leading internet service providers in Pakistan include PTCL and Stormfiber.

5. Port

- These are addresses to identify applications running on a device.
- Just like we have IP Addresses to identify unique devices, we have port or port addresses to identify unique applications on a device.

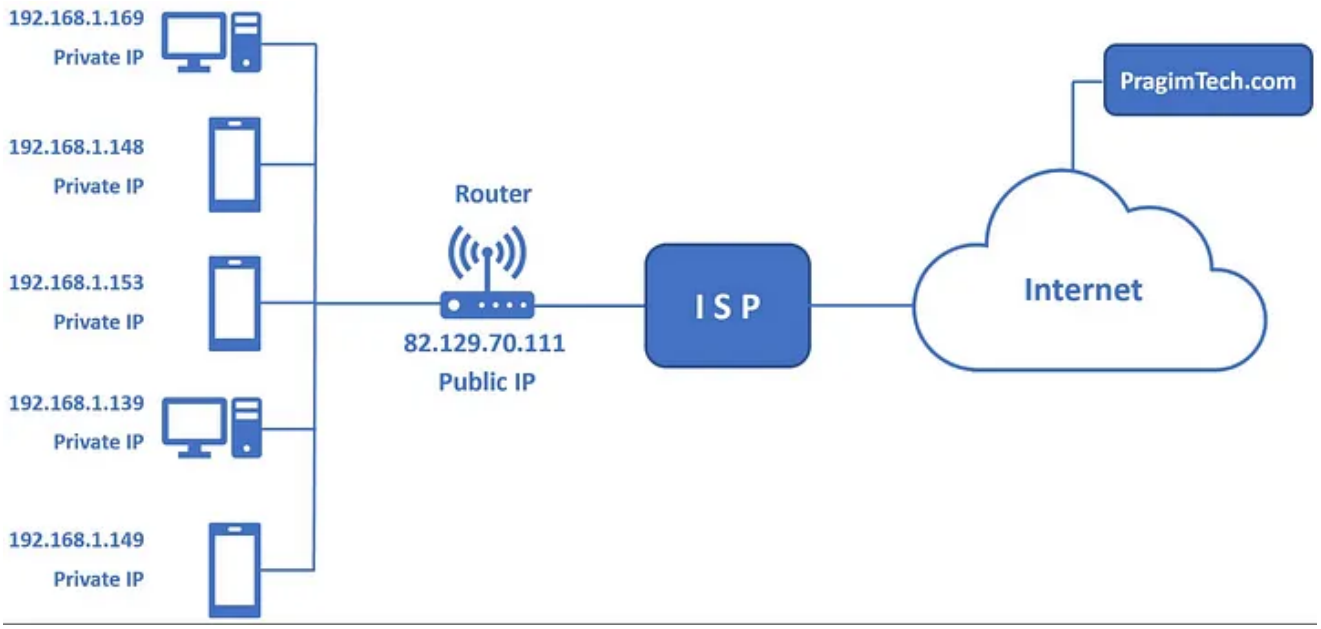
- When working on Google Chrome with multiple open tabs, it is important to be able to identify which tab is associated with specific data. For example, if a WhatsApp message is received, it needs to be directed to the web.whatsapp tab rather than the Facebook tab. This identification is made possible through the use of unique port numbers assigned to each application or process running on the device. These are known as ***Ephemeral Ports***. By using these port numbers, data can be sent accurately to the correct application or process.
- Once the process is done the port will be freed.

6. IP Addresses

IP is short for Internet Protocol. An IP address is a unique numerical label assigned to each device (like a computer, smartphone, or printer) it serves as the device's address on the network, allowing it to send and receive data to and from other devices.

Public and Private Addresses

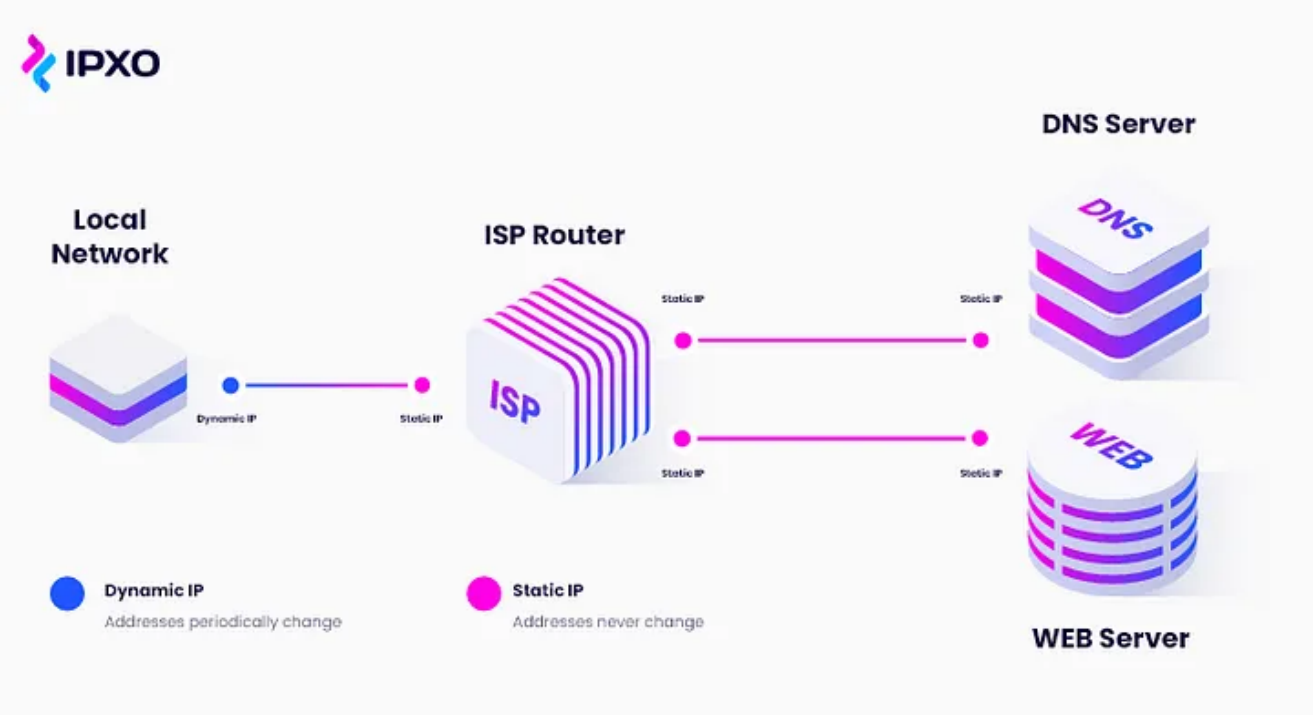
- **Public IP Address:** These addresses are assigned by Internet Service Providers (ISPs) and are used for devices that need to communicate directly with the Internet. Public IP addresses are visible to the internet and help identify devices on a global scale.
- **Private IP Address:** These addresses are used within a local network (like your home network or a corporate network) and are not visible on the Internet. Devices within the same local network share these private IP addresses.



Source: PragimTech.com

Static and Dynamic IP Addresses

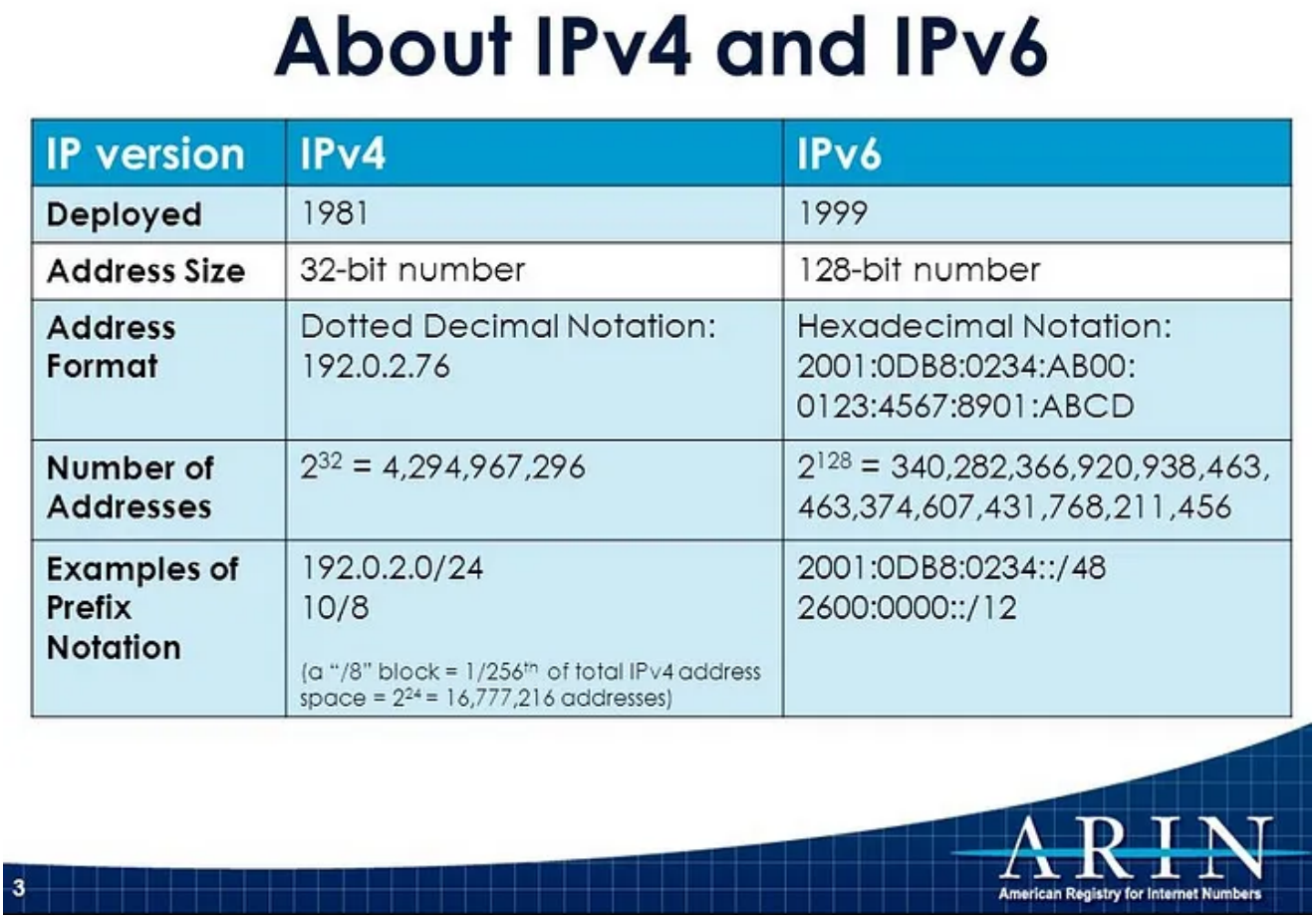
- **Static IP Address:** A static IP address is manually configured and does not change over time. It's often used for servers, routers, and networked devices that need a consistent address.
- **Dynamic IP Address:** A dynamic IP address is assigned automatically by a DHCP (Dynamic Host Configuration Protocol) server. These addresses can change each time a device connects to the network. It's common for consumer devices like laptops and smartphones to use dynamic IP addresses.



Source: IPXO.com

Versions

- **IPv4:** The older version of Internet Protocol, using a 32-bit address having 4.2 billion address
- **IPv6:** The newer version, uses a 128-bit address to accommodate the growing number of devices connected to the internet.



Source: ARIN

IPv4 uses a 32-bit address format, allowing for approximately 4.3 billion unique IP addresses. However, due to the explosive growth of the internet and the increasing number of connected devices, IPv4 address exhaustion has become a significant issue, leading to the development and adoption of IPv6 (Internet Protocol version 6), which uses a 128-bit address format and provides a vastly larger pool of IP addresses.

Classes of IP

- Class A => 0.0.0.0–127.255.255.255
- Class B => 128.0.0.0–191.255.255.255
- Class C => 192.0.0.0–223.255.255.255
- Class D => 224.0.0.0–239.255.255.255
- Class E => 240.0.0.0–255.255.255.255

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

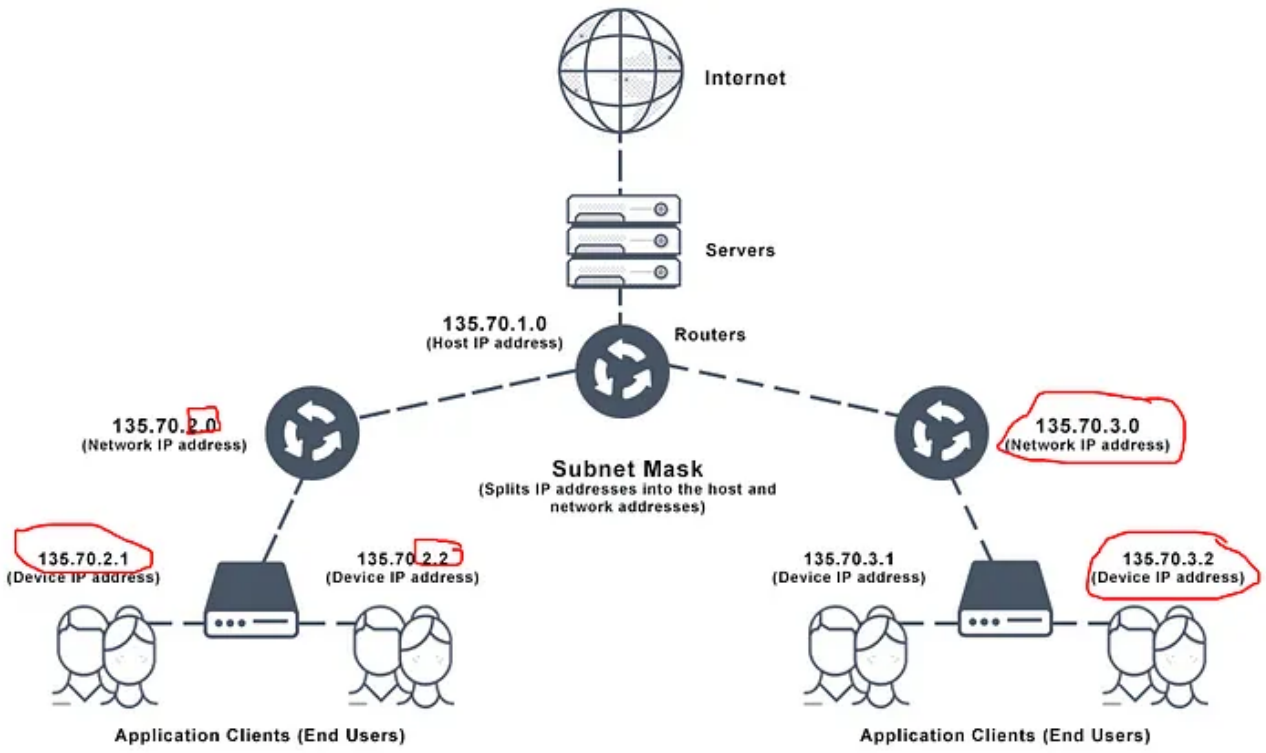
Source: **GreeksForGreeks**

Subnet

A subnet, short for “subnetwork,” is a division of an IP network into smaller, separate networks. Imagine a large neighbourhood with many houses. Subnetting is like dividing this neighbourhood into smaller blocks, each with its own set of houses. Each block, or subnet, has its own unique range of IP addresses

Subnet Mask

A subnet mask is like a filter for IP addresses. It divides an IP address into two parts, it helps computers and networks determine which part of an IP address is used to identify the network and which part is used to identify devices within that network



Source: AVI Network

A subnet mask is a 32-bit (for IPv4) or 128-bit (for IPv6) value that is used to determine the network portion and the host portion of an IP address. It is represented as a series of binary ones (1s) followed by binary zeros (0s). The subnet mask helps routers and devices determine whether two IP addresses are on the same network or need to be routed through different subnets.

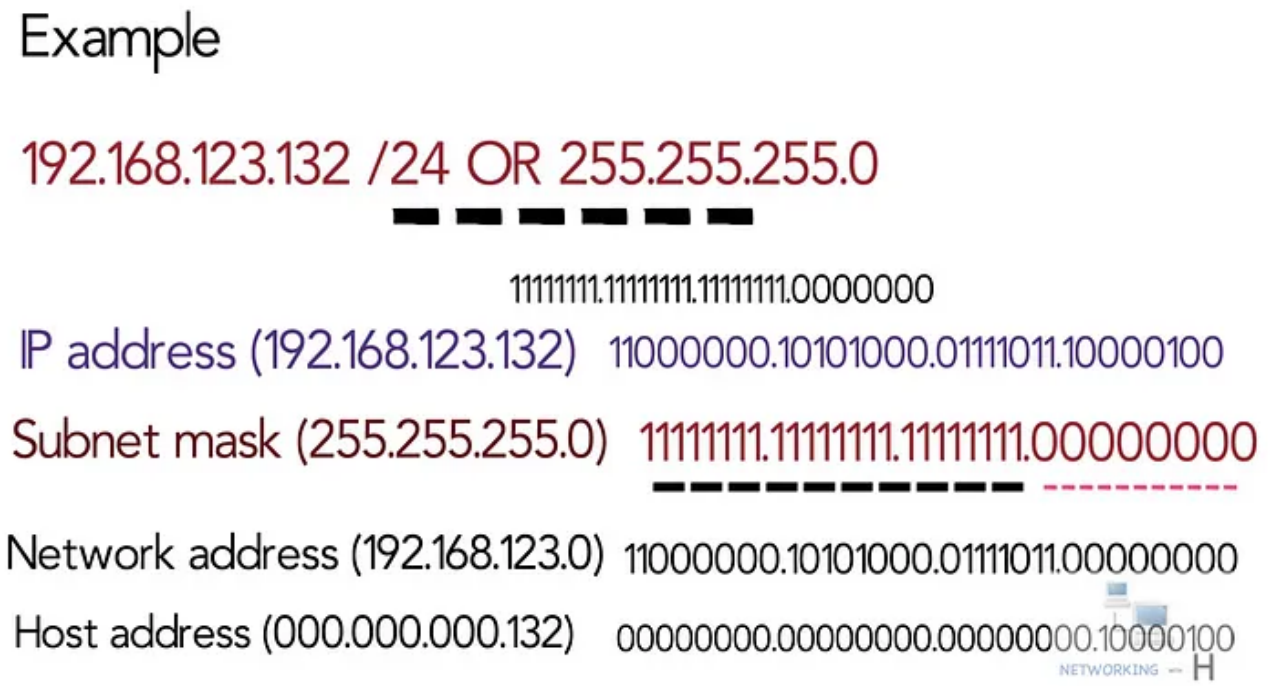
Table: CIDR and Subnet Examples

Address Class	No of Network Bits	No of Host Bits	Subnet mask	CIDR notation
A	8	24	255.0.0.0	/8
A	9	23	255.128.0.0	/9
A	12	20	255.240.0.0	/12
A	14	18	255.252.0.0	/14
B	16	16	255.255.0.0	/16
B	17	15	255.255.128.0	/17
B	20	12	255.255.240.0	/20
B	22	10	255.255.252.0	/22
C	24	8	255.255.255.0	/24
C	25	7	255.255.255.128	/25
C	28	4	255.255.255.240	/28
C	30	2	255.255.255.252	/30

Source: **steves-internet-guide.**

CIDR Notation

Classless Inter-Domain Routing (CIDR) notation is a way of representing subnets in a concise format. It combines the IP address and the subnet mask using a forward slash (/) followed by the subnet prefix length in bits. For example, “192.168.1.0/24” represents the same subnet as “192.168.1.0” with a subnet mask of “255.255.255.0.”



Source: Networking with h

7. Socket

It represents an endpoint for sending or receiving data across a computer network.

Source: Networking Signal

Intuitive Example:

- Think of sockets as mailboxes for your house.

- Each mailbox (socket) has a unique street address (IP address) and a slot number (port number).
- You (your computer) can send and receive letters (data) through these mailboxes.
- The street address (IP address) ensures that your letter goes to the right house (device).
- The slot number (port number) specifies which mailbox (socket) within the house (device) the letter should be delivered to.
- Sockets make sure your messages reach the right place (device) and enable conversations (data exchange) over the network.

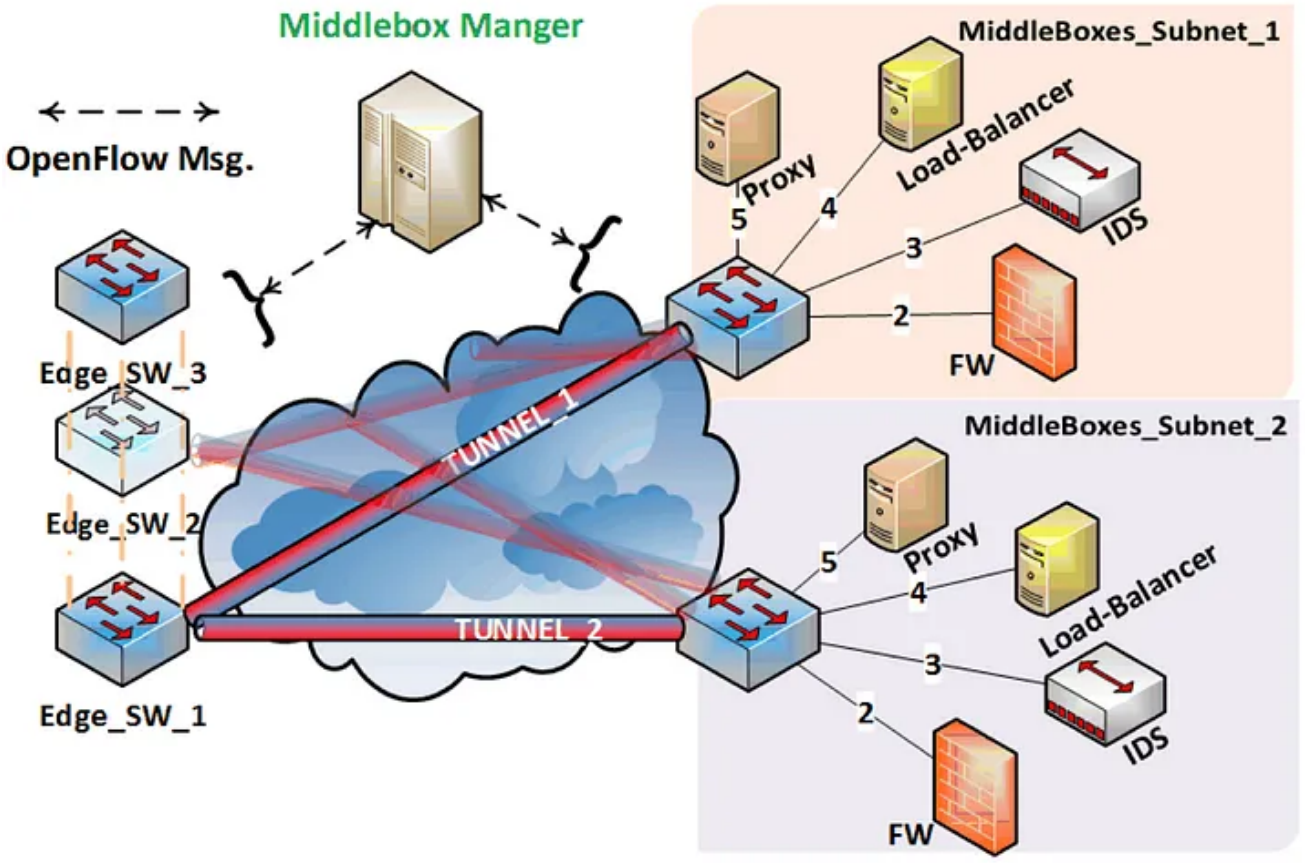
8. Packets

In computer networking, packets are small units of data that travel across computer networks, It is like breaking down big data into smaller, manageable parts for efficient and reliable delivery

9. Middle Boxes

In computer networking, “middleboxes” refer to various devices or components placed within a network infrastructure between the sender and receiver of data. These middleboxes serve specific purposes, such as security, optimization, or monitoring.

Examples of middleboxes include firewalls, load balancers, proxy servers, and intrusion detection systems.



Source: mdpi.com

Intuitive Example:

- Imagine you're driving on a road from one city to another.
- One checkpoint (middle box) checks for any dangerous items in your car (firewall).
- Another checkpoint balances the traffic to avoid jams (load balancer).
- Some checkpoints keep an eye out for anything suspicious (intrusion detection).

They act as intermediaries that can inspect, filter, or modify data as it passes through the network, helping to enhance security, performance, or management of network traffic.

10. NAT And CGNAT (Carrier-Grade Network Address Translation)

- NAT is a network technology used by (ISPs) to share a single public IP address among multiple devices in their network

- CGNAT is an advanced form of Network Address Translation (NAT). It's designed for large-scale networks, such as those used by ISPs, where a limited number of public IP addresses need to serve a large number of customers.
- ISPs implemented CGNAT to address the IPv4 address exhaustion issue.
- It involves translating private IP addresses of devices within a local network to a single public IP address when communicating over the internet. (We will explore how it works in the following section.)

How We Transferred or Received Data On the Internet?

At the present time, many `ISPs` use `CGNAT` as a technique for transferring and receiving data. CGNAT is employed by ISPs to manage the allocation of IP addresses more efficiently due to the limited availability of IPv4 addresses.

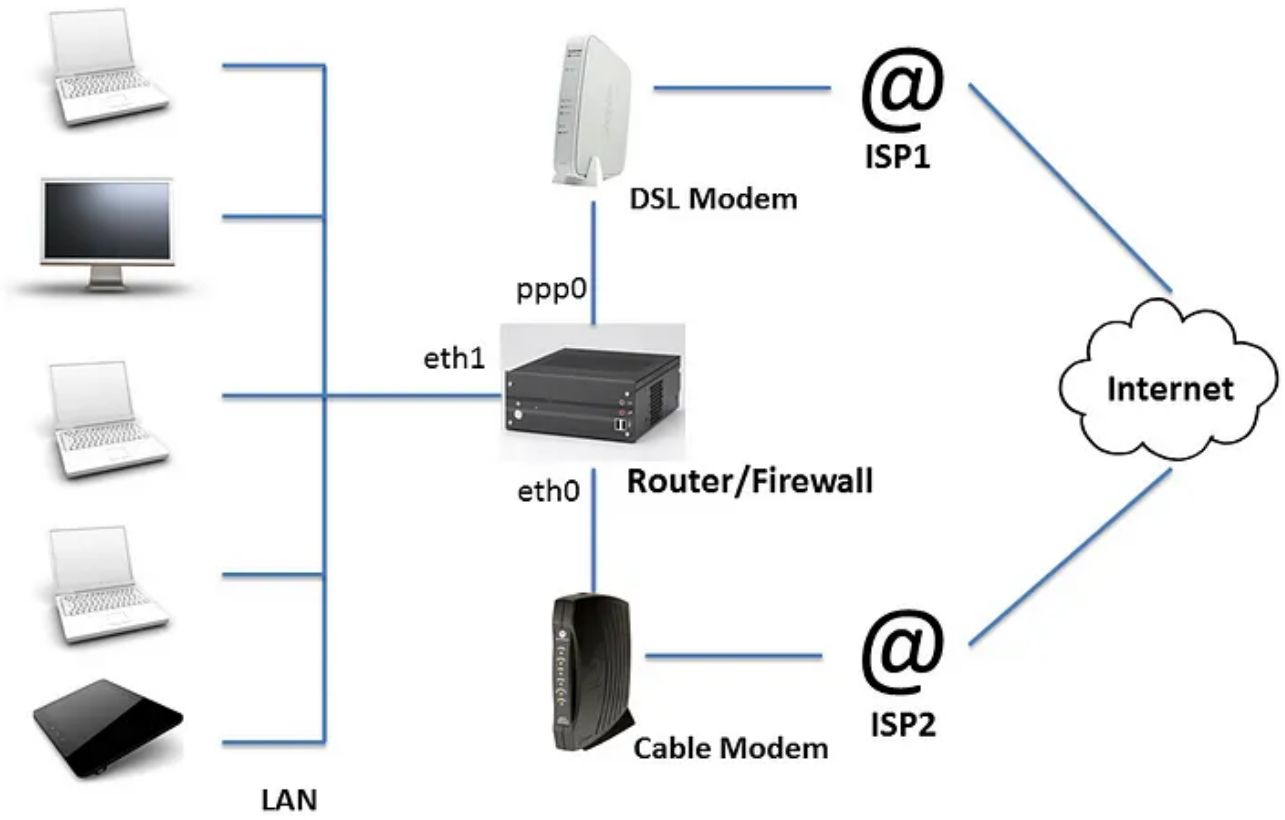


Figure from Net-ISP-Balance

In order to access information on the internet, every individual device requires its own public IP address. However, most devices use IPv4, which has only 4.2 billion public IP addresses. Therefore, public IP addresses are only available through

local internet service providers. Our devices only have private IP addresses, so how can we access the internet? Let's understand this concept in simple terms.

- When responses come back from the internet, the CGNAT device uses this port information to route the data packets back to the correct device in the local network.
- When data packets (send a request or data) from devices (laptop, PC etc) in a local network are sent out to the internet, the CGNAT device in the ISP's network translates the source private IP address and port of each packet to the single public IP address and unique port number, effectively hiding the individual devices behind one public IP address.

Intuitive Example

let's walk through the process of how your laptop knows to open Google when you type it in your web browser, from your service provider to your web browser:

Imagine the internet is a big party:

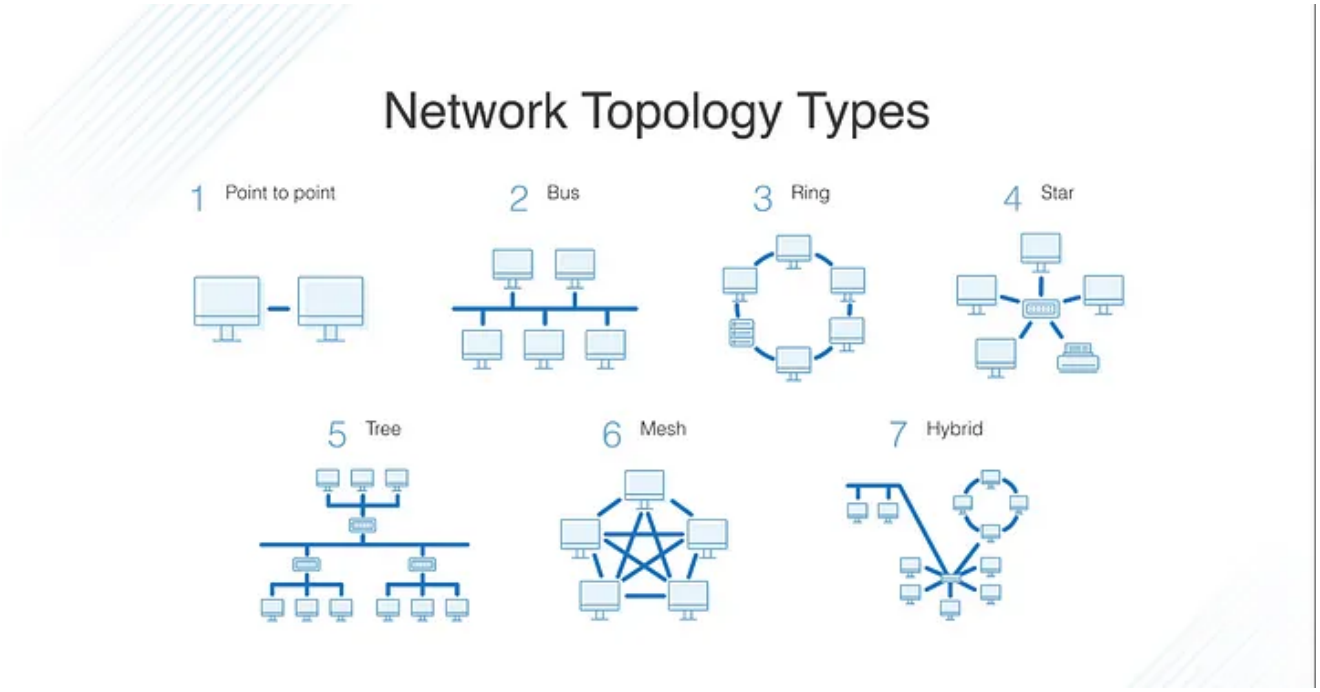
- Each device has a name called Private IP Address.
- Each device needs a special ticket (Public IP Address) to join.
- But, instead of giving each device its own ticket, the internet is divided into groups led by companies (ISPs), sharing one ticket (IP Address) among many.
- Devices have small rooms (Ports) for private conversations.
- CGNAT helps devices share tickets and have separate rooms.
- When you want a website (Google), you ask your ISP (party host).
- Your ISP uses its big-ticket (IP Address), not yours, to find websites.
- Your ISP asks for a special address book (DNS server) where the website lives.
- Your ISP sends your request to the website's house (server) using its big ticket.
- The website sends its invitation (web page) back to your device through your ISP.
- Your web browser gets the web page and shows it to you.

- ISP give a dynamic IP address to every device on its group.

Network Topologies

Network topologies refer to the physical connections of a computer network. These topologies define how data is transmitted between devices and how they are interconnected.

Here are some of the most common network topologies:



Source: DNSSTUFF

1. **Point-to-Point Topology:** In a point-to-point topology, there's a dedicated connection between two devices.
2. **Bus Topology:** In a bus topology, all devices are connected to a single central cable called the "bus.". It's relatively simple but can be less reliable if the main cable fails.
3. **Ring Topology:** In a ring topology, each device is connected to exactly two other devices, forming a circular or ring-like structure. If one device or cable fails, it can disrupt the entire network.
4. **Star Topology:** In a star topology, all devices are connected to a central hub or switch. If one cable or device fails, it doesn't affect the others, making it reliable.

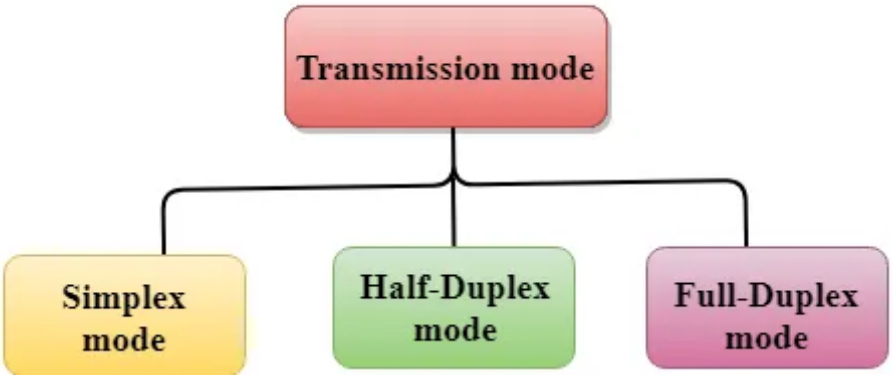
5. **Tree Topology:** A tree topology combines the characteristics of a star and bus topology. It has a root node (like a central hub) with branches connecting to other hubs or switches.

6. **Mesh Topology:** In a mesh topology, every device is connected to every other device. Common in critical infrastructure and large-scale networks.

7. **Hybrid Topology:** A hybrid topology is a combination of two or more of the above topologies. For example, a network might have a star topology within each department and connect these departmental stars using a bus topology. This allows for flexibility and scalability.

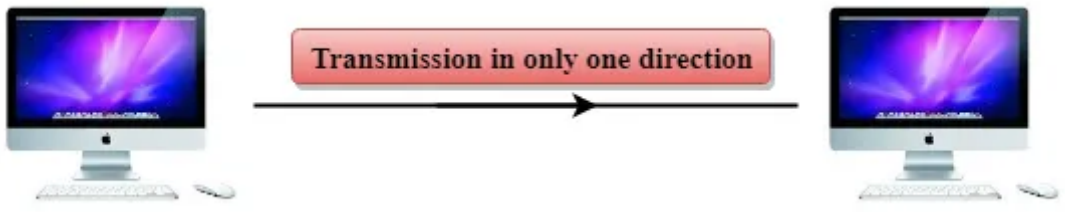
Transmission/Communication modes

The way in which data is transmitted from one device to another device is known as **transmission mode**.



Source JAVATPOINT

1) Simplex Mode



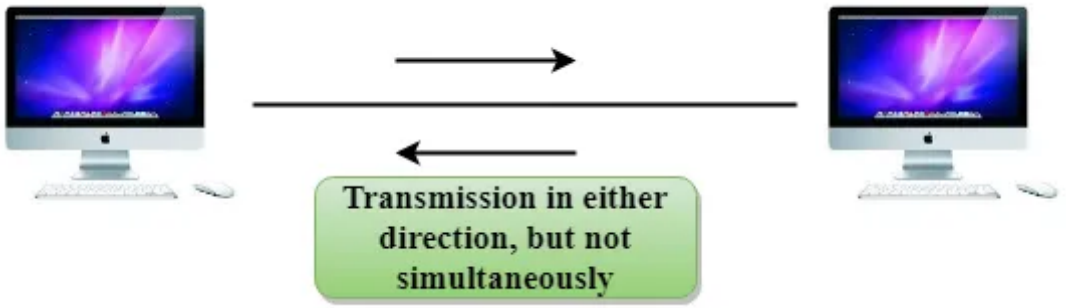
Source JAVATPOINT

Advantage: The station can utilize the entire bandwidth of the communication channel so that more data can be transmitted at a time.

Disadvantage: Communication is unidirectional, so it has no inter-communication between devices.

Examples: Keyboard and Monitor

2) Half-duplex mode



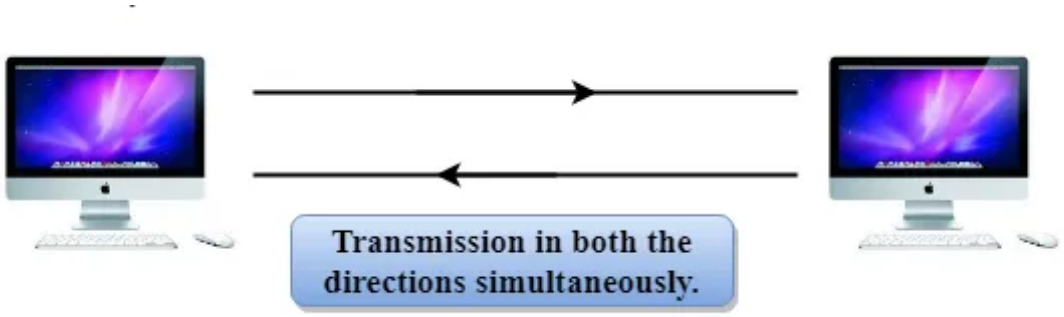
Source JAVATPOINT

Advantage: Both devices can send and receive the data and can utilize the entire bandwidth of the communication channel during the transmission of data.

Disadvantage: When one device is sending the data, then another has to wait, this causes a delay in sending the data at the right time

Examples: Walkie-talkie

3) Full-duplex mode



Source JAVATPOINT

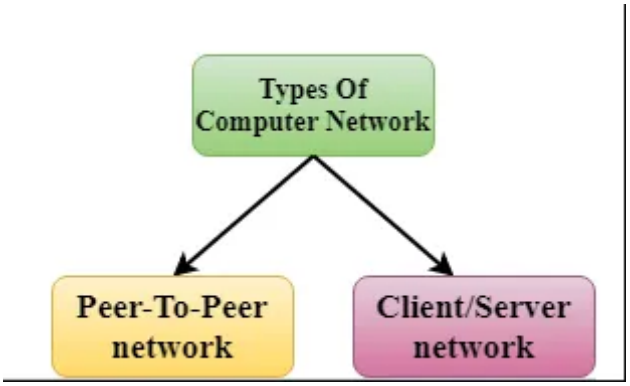
Advantage: Both stations can send and receive the data at the same time.

Disadvantage: If there is no dedicated path exists between the devices, then the capacity of the communication channel is divided into two parts.

Examples: Telephone etc

Computer Network Architecture

A set of layers and protocols is known as network architecture.

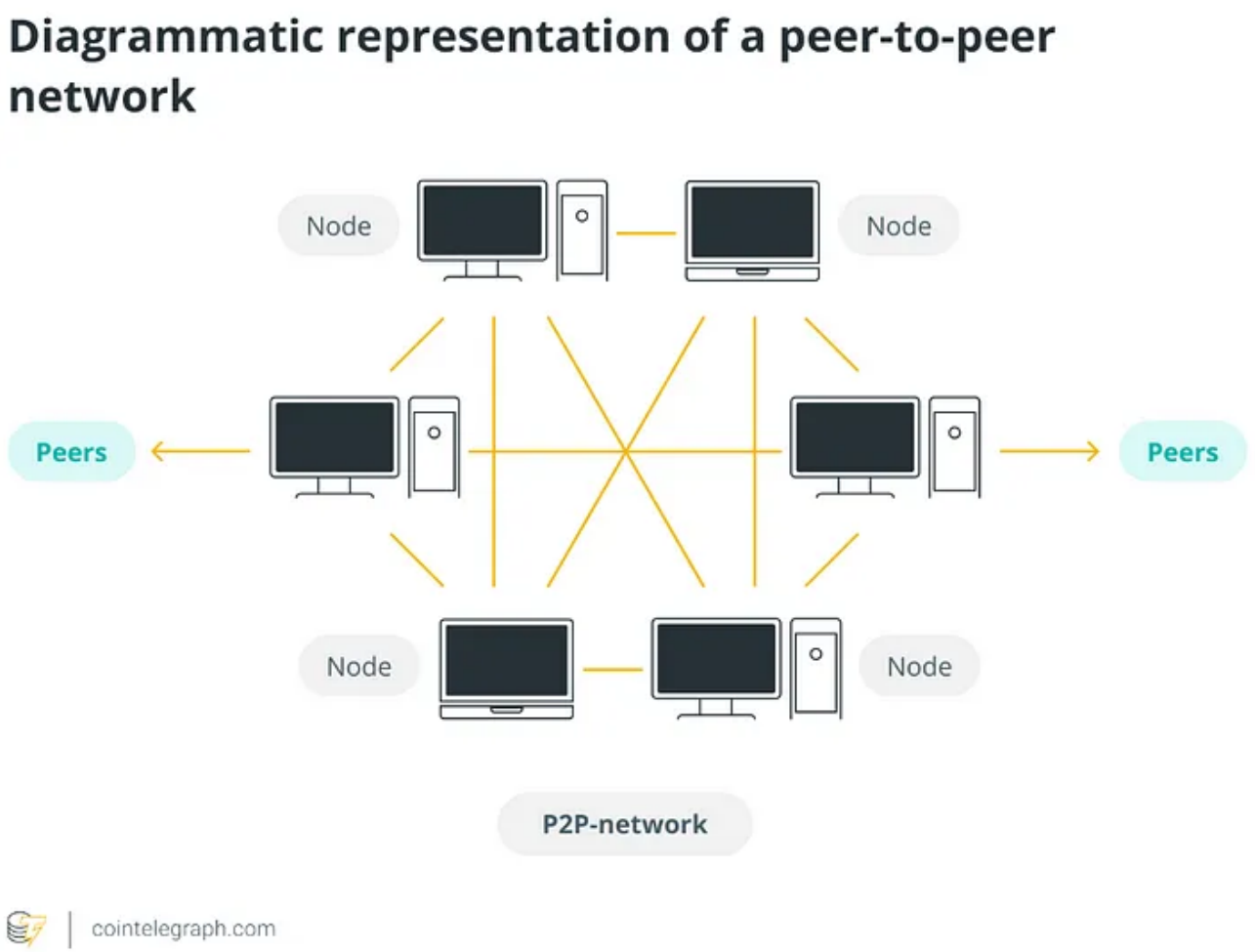


Source JAVATPOINT

Peer-to-Peer Network (P2P):

A peer-to-peer network is a type of computer network where all connected devices (computers, smartphones, etc.) are considered equal peers. In a P2P network, each device can send and receive data directly from any other device on the network without the need for a central server. It's a decentralized approach to networking that can be very efficient and resilient.

Intuitive Example: Imagine a group of friends sitting in a circle, and they can all talk to each other directly without needing a leader. Each friend can share their snacks or information with anyone else in the group.



Picture from CoinTelegraph

Client Server Network

The client-server model is a common architecture in computer networking where devices on a network are divided into two categories: clients and servers.

1. **Client:** A client is a device (like a computer or smartphone) that requests services or resources from a server. It typically runs applications like web browsers, email clients, or games that need information or functionality provided by servers.

2. **Server:** A server is a more powerful device (often a dedicated computer) that provides services or resources to clients. Servers host databases, websites, email services, and more. They wait for client requests and respond by providing the requested data or performing specific tasks.

Intuitive Example

Think of it as going to a restaurant:

- The client is like the customer who comes to the restaurant (server) to order food (services).
- The server (restaurant) takes the order, prepares the food, and serves it to the customer (client).

The client-server model is widely used in applications where centralized control and resource management are essential, such as websites, email systems, and databases.

I have already explained how data transfer works. It is similar to a client-server network example.

Models

The early software for communication subsystems was a single, complex, unstructured program with numerous interacting components, making it hard to test and modify. To address this, the ISO introduced a layered approach. In this approach, networking is divided into distinct layers, each with specific tasks. Networking functions are thus organized by these layers for greater manageability and efficiency.

Layered Architecture

- The main aim of the layered architecture is to divide the design into small pieces.
- Each lower layer adds its services to the higher layer to provide a full set of services to manage communications and run the applications.
- It provides interaction between subsystems.
- Any modification in a layer will not affect the other layers.

Layered architecture comprises services, protocols, and interfaces as its fundamental components.

- **Service:** Services refer to the actions that a layer offers to the layer above it.
- **Protocol:** Protocols are a set of regulations that a layer follows to communicate with its peer entity, and these regulations pertain to the content and sequence of the messages transmitted.

- **Interface:** Interfaces serve as the conduit for transmitting messages from one layer to another.

Important Concepts Before Understanding Model

Translation

The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from a sender-dependent format into a common format and changes the common format into a receiver-dependent format at the receiving end.

Encryption

Encryption is needed to maintain privacy. Encryption is the process of converting the sender-transmitted information into another form and sending the resulting message over the network.

Compression

Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, and video.

- Lossy (where the original data can be perfectly reconstructed from the compressed data)
- Lossless (Cant recover origin data)

Encoding

Encoding is the process of converting data from one format or representation to another.

Decoding

Decoding is the reverse process of encoding. It involves converting data from its encoded or transformed format back into its original form or a human-readable format.

Secure Socket Layer (SSL)

SSL was designed to encrypt data transmission, ensuring that data exchanged between the client and server remains confidential and tamper-proof. It also

provided authentication to verify the identity of the server.

Synchronization

In computer networking, synchronization is like making sure data arrives in the right order and at the right time.

Dialog control

Dialog control, in the context of the Session Layer, refers to the management of communication between two devices to prevent conflicts and ensure orderly conversations. It's like having rules in place for who gets to speak and when during a discussion. Dialog control ensures that devices take turns sending and receiving data, preventing chaos and collisions in the communication process.

Checkpoint

Checkpoints are the specific points in the data exchange where progress has been made. If data is interrupted or fails, We can use these checkpoints to resume the session from the last known good point, reducing data loss and retransmission.

Authentication

Authentication is the process of verifying the identity of a user, device, or entity attempting to access a system or network.

Authorization

Authorization follows authentication and involves granting or denying permissions and access rights to authenticated users or devices. It defines what actions or resources a user or device is allowed to access within a network or system, enforcing security policies.

Checksum

It's a short piece of information derived from the data itself, and it's used to verify the data's integrity during transmission.

1. **Data Preparation:** A unique checksum value is calculated based on the data before sending it.
2. **Transmission:** The data and its checksum are sent to the receiver.
3. **Receiving and Verification:** The receiver gets the data and recalculates the checksum from it.

4. **Comparison:** If the recalculated checksum matches the received checksum, the data is error-free. If they differ, there might be transmission errors.

Connection-Oriented Transmission

- In connection-oriented transmission, a dedicated path or connection is established between the sender and receiver before data is exchanged.
- Full Data is transferred.
- TCP is an example where full transfer of data is required like web browsing etc

Connectionless Transmission

- No dedicated connection is established
- Connectionless protocols, like UDP (User Datagram Protocol), are often used for real-time applications like video streaming and online gaming, where speed is more important than perfect data order.

MAC (Media Access Control) address

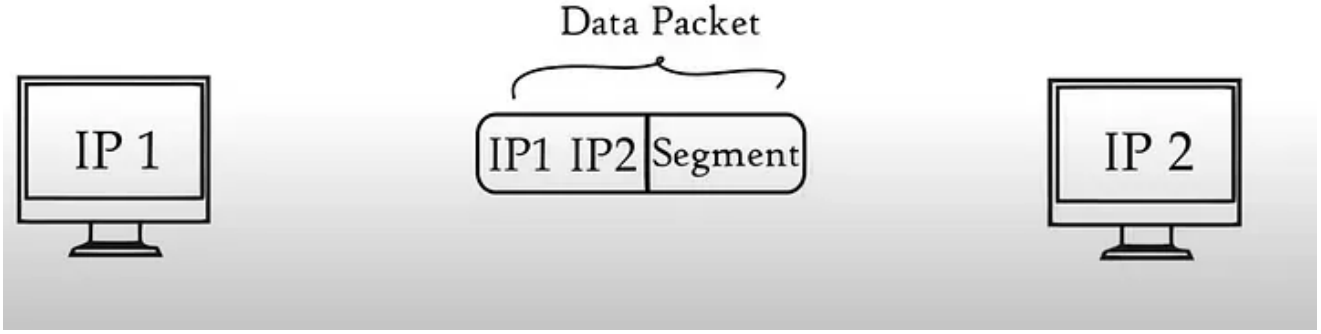
Each MAC address is globally unique. This means that no two network devices in the world should have the same MAC address. Manufacturers assign unique MAC addresses to their network hardware and unique serial numbers for the NIC.

For example, a MAC address might look like “00:1A:2B:3C:4D:5E.”

Logical Addressing

Logical addressing is a higher-level addressing scheme that operates at the network layer (Layer 3) of the OSI model. It assigns addresses to devices based on their network location and can change as devices move across different networks.

In this IP address of the sender and receiver are assigned to segment to form Packets

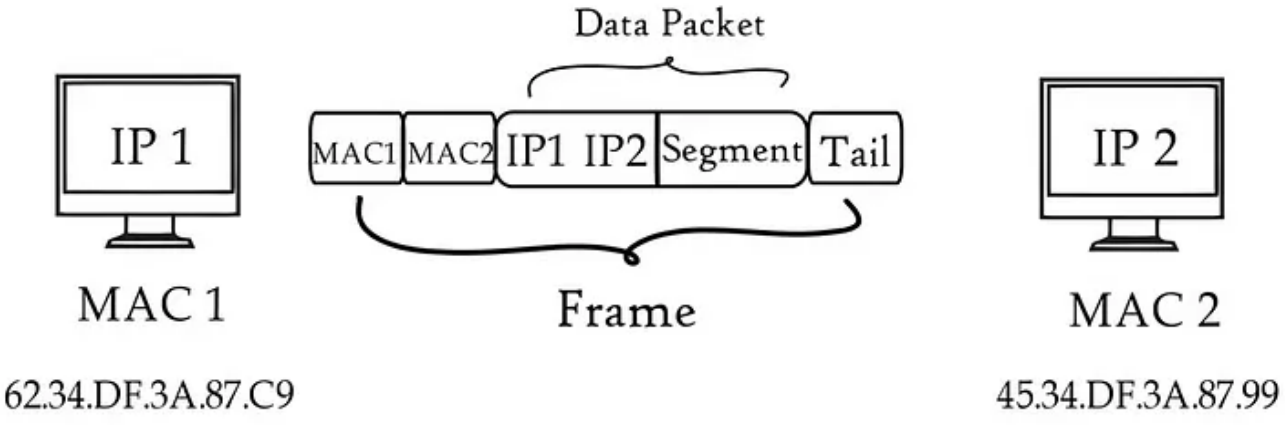


Source: Unknown

Physical Addressing

Physical addressing refers to the hardware-based addressing of network devices. It assigns a unique, fixed address to each device's network interface card (NIC) at the data link layer (Layer 2) of the OSI model.

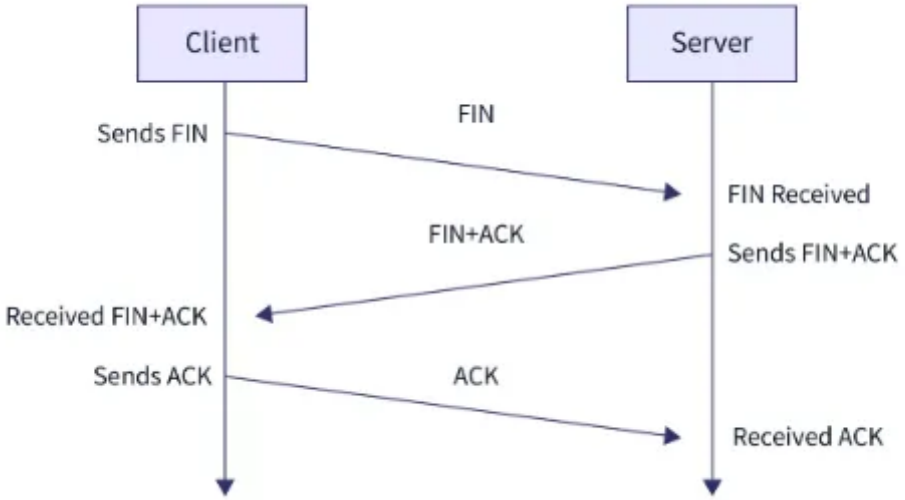
MAC addresses of each user are assigned to the packet to form a frame



Source: Unknown

Three Way Handshake

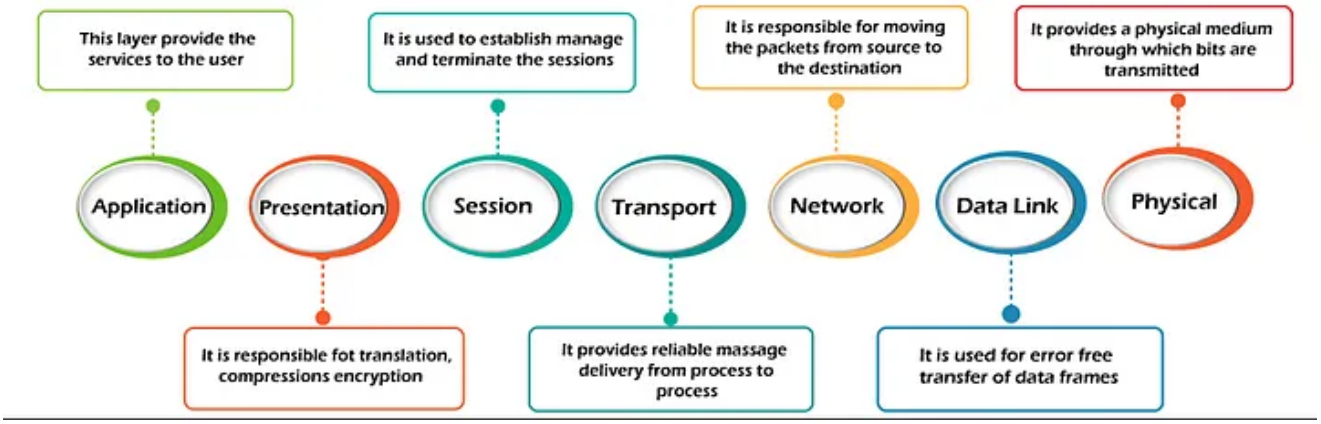
- This is a pre-connection process.
- First, our computer will ask our friend's computer "Hey, I want to make a connection with you. Can I?".
- The friend's computer replies "Yeah, sure.".
- And then our computer will respond, "Okay!, I am creating a connection now.".
- And then the connection is established.
- This is known as the Three Way Handshake.



Source: Unknown

OSI Model

- OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984
- Each layer is self-contained so that tasks assigned to each layer can be performed independently.



Picture from JavaTPoint

1. Physical Layer (The Physical Connection)

This is the bottom layer, dealing with the actual hardware. It's all about how the bits, the smallest units of data, are transmitted over physical mediums like cables or wireless signals. Think of it as the cables, connectors, and electrical signals.

- The Physical Layer is the first layer in the OSI (Open Systems Interconnection) model.
- Its primary job is to transmit raw bits (0s and 1s) over a physical medium, such as copper wires, optical fibres, or radio waves.
- It establishes, maintains and deactivates the physical connection.
- Example: Ethernet cables, Network interface cards Hubs, switches, routers, etc
- Functions: Bit Encoding, Line Configuration, Data Transmission, Topology, Type of Signals

2. Data-Link Layer (Getting Data from A to B)

This layer is responsible for ensuring that data moves reliably between two directly connected devices. It's like a bridge that connects two islands, making sure data can safely cross from one side to the other. It also manages errors and flow control.

- The Data Link Layer, the second layer in the OSI model, manages the transmission of data within a local network:
- **Frame Creation:** It encapsulates packets from the Network Layer into frames for local transmission.
- **MAC Addressing:** Assigns MAC addresses to devices for local network identification.
- **Error Handling:** Detects and, in some cases, corrects errors in data transmission.
- **Flow Control:** Manages data transmission rates to prevent congestion.

- **Media Access Control (MAC):** Controls access to shared network segments, like Ethernet.
- **Logical Link Control (LLC):** Handles logical flow control and error checking.
- **Switching:** Used in modern networks for efficient data forwarding.
- **Ethernet:** A common technology associated with this layer.

3. Network Layer (Finding the Best Path)

Imagine you're sending a package across the country. The network layer is like a GPS system that figures out the best route for your data to travel. It uses IP addresses to navigate and determine where your data should go.

- The Network Layer handles the movement of data between different networks, using logical addressing (like computer addresses) and routing (finding the best way to get there).
- The network layer is responsible for transferring data from one network to another.
- **Data Packets:** Data in this layer are called packets. IP addresses of the sender and receiver are attached to segments in order to form packets.
- **Logical addressing** is done with the help of an IP address and mask. The network layer only deals with logical addressing and does not handle any physical addressing.
- **Routing** is the method used to move data from source to destination.
- **Path determination** is the process of identifying the optimal path out of multiple paths from source to destination.

4. Transport Layer (Reliable Delivery)

Now, think of this layer as a postal service. It takes your data, splits it into smaller packages if needed, and ensures they all arrive in the correct order at the destination. It's all about reliability and completeness.

- The Transport layer is Layer 4, which ensures that messages are transmitted in the order in which they are sent and that there is no duplication of data.

- **Segments:** Data received from the Session layer is divided into small data units called segments. Each segment contains a sequence number and port number. The port number helps each segment reach the correct application, and the sequence number helps reassemble segments in the correct order.
- **Flow Control:** It manages the flow of data to prevent congestion and ensure efficient communication. For example, if you are downloading a file from a server at an internet speed of 5mbps, but the server can send the file at a speed of 50mbps, flow control manages this and asks the server to slow down the speed. As a result, the server sends it at a speed of 5mbps.
- **Error Control:** If some data does not arrive at the destination, the transport layer uses an automatic repeat request to retransmit the corrupted data. The transport layer adds a checksum to each layer to check if the data is corrupted or not.
- **Multiplexing and Demultiplexing:** It allows multiple applications on a device to use the network simultaneously by assigning unique identifiers to each application's data.
- **Connection control:** Maybe connection-oriented or connectionless

5. Session Layer (Setting Up and Tearing Down)

This layer is like a conversation manager. It establishes, maintains, and terminates communication sessions between computers. Think of it as the software that manages your video call or chat session.

- **Session Establishment and Termination:** One of the primary functions of the Session Layer is to establish, maintain, and terminate communication sessions between two devices.
- **Synchronization:** Ensures that data is properly synchronized during the session
- **Dialog Control:** Manages dialogue by controlling when each device can transmit data.
- **Token Management:** Can manage tokens, ensuring that only one device has permission to transmit at a time.

- **Checkpointing and Recovery:** It allows for the creation of checkpoints during a session. If a session is interrupted or fails, the Session Layer can use these checkpoints to resume the session from the last known good point, reducing data loss and retransmission.
- **Security and Authentication:** Can also handle security aspects, including user authentication and encryption
- **Session Termination:** When a session is complete, the Session Layer manages its termination

6. Presentation Layer (Making Data Understandable):

Data can be in different formats or languages. This layer translates data between what the application understands and what the lower layers deal with. It handles things like encryption, compression, and data formatting.

- The Presentation Layer is the sixth layer in the OSI model, situated just below the Application Layer.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- **Data Format Conversion:** Think of the Presentation Layer as a language translator. It takes data prepared by the Application Layer and converts it into a format that both the sender and receiver can understand. This is essential because different devices and systems may use various data formats and character encodings. For instance, if one system uses Windows and another uses macOS, this layer ensures smooth communication by translating data appropriately.
- **Encryption** is done. At the sender side, data is encrypted and at the receiver side data is decrypted. A secure socket layer (SSL)is used for encryption and decryption
- **Compression** is done

7. Application Layer (User Interaction):

Finally, this is where you, the user, interact with the network. It's the layer where software applications like web browsers, email clients, and games reside. It

provides a user-friendly interface for accessing network services.

- **User-Friendly Interface:** It's the part of the network where you interact with the internet, often through graphical interfaces.
- **Data Formatting:** The Application Layer is responsible for preparing data in a format that different applications can understand. For example, it structures email messages with headers, text, and attachments following established standards. Imagine it as the translator that makes sure your email looks right before sending it.
- **Protocol Selection:** It's like choosing the right tool for the job. The Application Layer selects the appropriate protocol based on the type of service or data being sent. For instance, web browsing relies on HTTPS/HTTP, email uses SMTP, and file transfers employ FTP. It ensures that the right set of rules is in place for successful communication.
- **Handoff to Lower Layers:** Once the data is prepared and the suitable protocol is chosen, the Application Layer passes this to the Presentation Layer

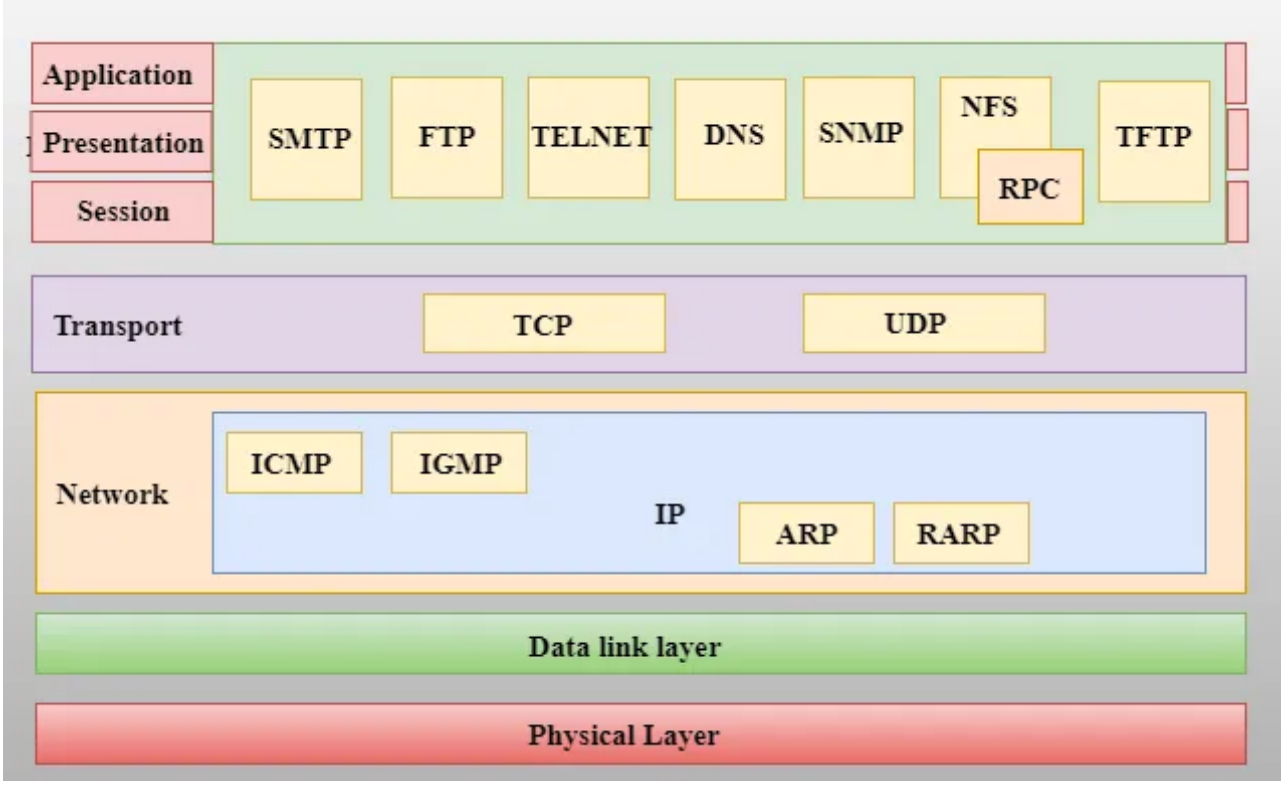
Each layer has its own job, and they all collaborate to ensure that your emails, videos, and web pages can travel across the internet reliably and securely.

NOTE: IF YOU WANT TO LEARN OSI IN DETAIL THEN *https://www.javatpoint.com/osi-model, THIS ARTICLE IS RECOMMENDED AND THIS YOUTUBE VIDEO https://www.youtube.com/watch?v=vv4y_uOneC0*

TCP/IP

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in the TCP/IP model by a single layer called the application layer.

- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.



Picture from JavaTPoint

User Datagram Protocol (UDC)

UDP, or User Datagram Protocol, is a communication protocol in computer networking. Here's a simple explanation:

1. **Connectionless:** Unlike some other protocols, UDP is connectionless. This means it doesn't establish a formal connection before sending data. It's like sending a postcard without knowing if it will arrive or not; you just drop it in the mailbox and hope for the best.

2. **Speed:** UDP is fast because it doesn't have the overhead of setting up and closing connections like TCP (another communication protocol).

3. **No Guaranteed Delivery:** UDP doesn't guarantee that your data will arrive at its destination.

4. **Used for Streaming and Real-Time:** UDP is often used for streaming audio and video or real-time online gaming.

Conclusion

In this brief introduction to computer networks, we've explored their evolution, from ARPANET to today's interconnected web. We've delved into essential concepts like the OSI model, IP addresses, subnets, and the role of ISPs. We've likened subnets to neighbourhoods, explaining their role in organizing IP addresses. With these insights, you're better equipped to navigate the world of computer networks, a vital foundation of our digital age.

References

Lenfest Institute, The Techedvocate.org, Magzter.com , World First Website, Portwsigger.net, Cable Submarine, GreeksForGreeks, IT release, PragimTech.com, IPXO.com, ARIN, AVI Network,steves-internet-guide, Networking with h, Networking Signal , mdpi.com , Net-ISP-Balance , DNSSTUFF , JAVATPOINT, CoinTelegraph , ChatGPT, Kunal kushwaha computer networking course

LET'S CONNECT

***Linkedin**: https://www.linkedin.com/in/syedamahamfahim/*

***Github:** https://github.com/SyedaMahamFahim*

***Portfolio**: https://www.syedamaham.dev/*

Computer Networking | Cgnat | Tcp | Udp Protocol | Internet

Written by SyedaMahamFahim

13 Followers

More from SyedaMahamFahim

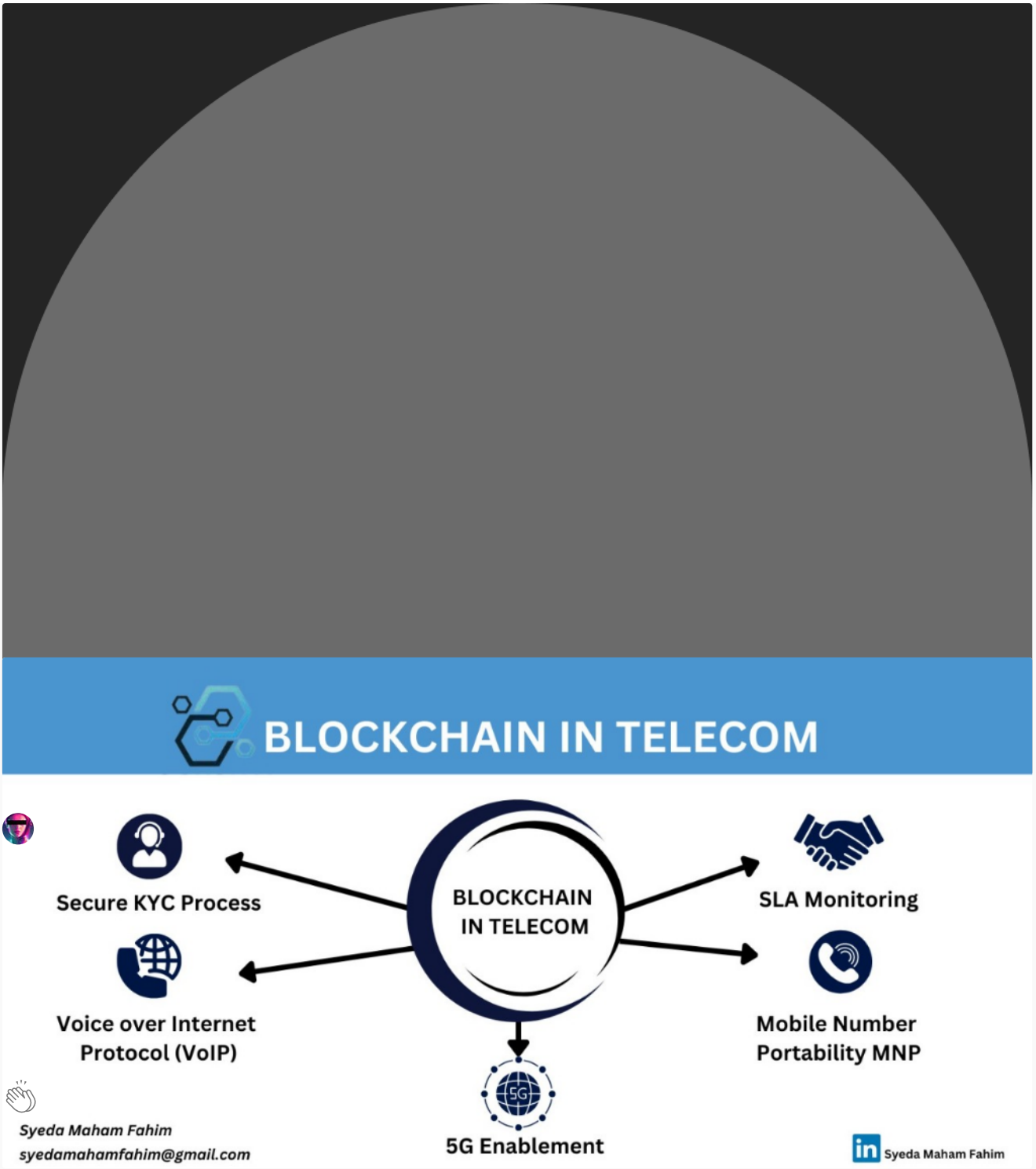
SyedaMahamFahim

A Quick Recap of Object-Oriented Programming (OOP) in Java

This article serves as a comprehensive and concise review of key object-oriented programming (OOP) concepts in Java. It provides a quick...

13 min read · Jun 5

2

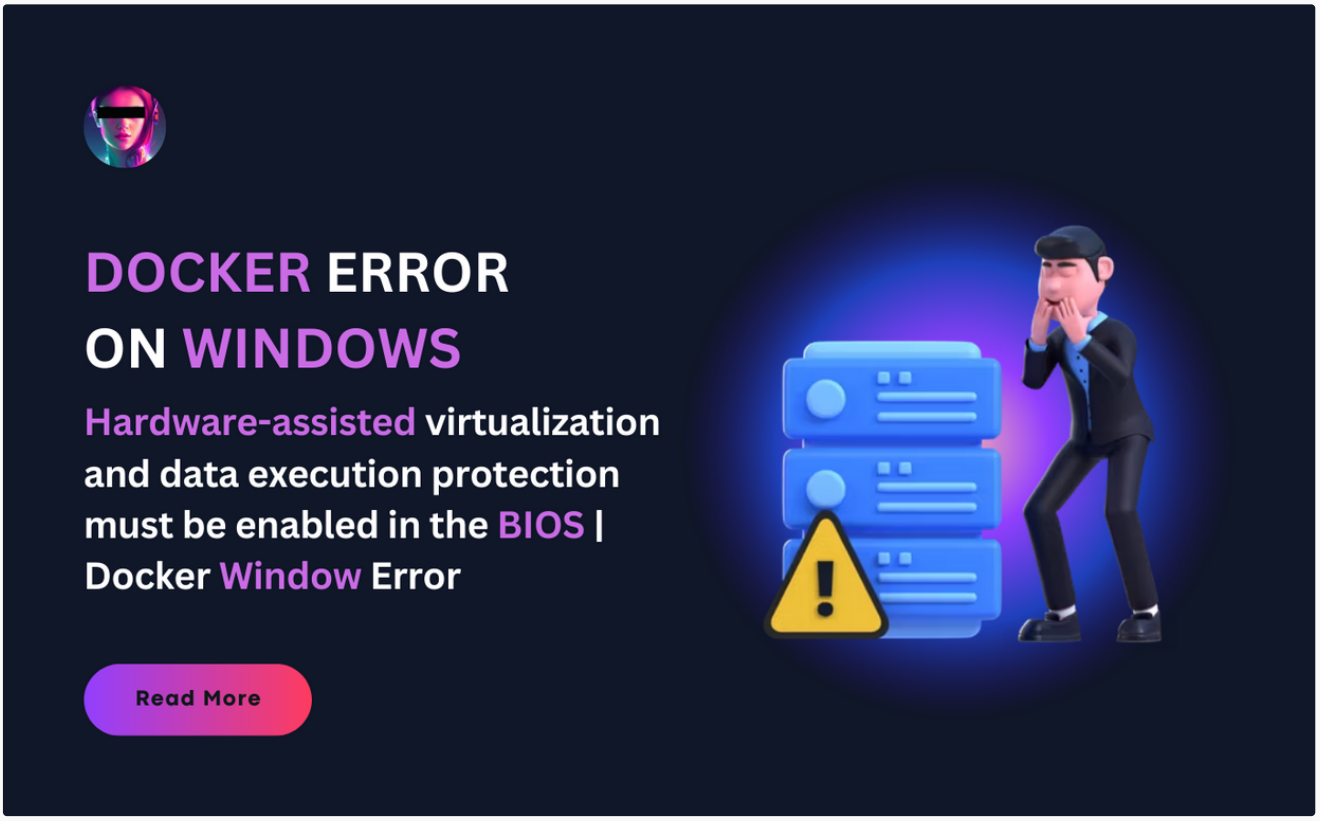


SyedaMahamFahim

Blockchain In Telecom Industry

Blockchain technology has the potential to solve big issues in the Telecom industry because it creates transparency through its distributed...

5 min read · Jan 17



SyedaMahamFahim

Hardware-assisted virtualization and data execution protection must be enabled in the BIOS | Docker...

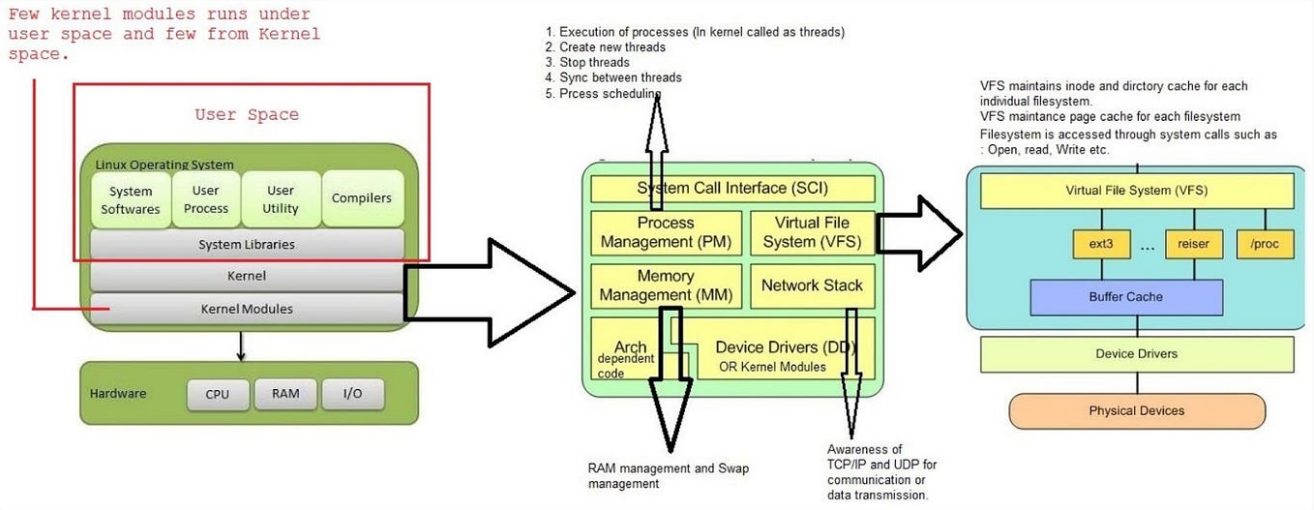
Uh oh, you thought you were ready to dive into the exciting world of Docker containerization, but then, BOOOOOOOOM! You encountered an...

4 min read · Apr 11

104

See all from SyedaMahamFahim

Recommended from Medium



Rohit Gupta

An Introduction to Linux : Navigating the Operating System Landscape with Everyday Analogies

Ever wondered about the wizardry behind the Linux operating system? Join us in the whimsical journey where we will demystify Linux using...

4 min read · Nov 27

121

Neeramitra Reddy in The Startup

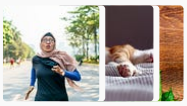
3 Advanced (and Unique) ChatGPT Uses You've Likely Not Seen Before

Valuable "meta" use cases I've found in 10 months of tinkering with ChatGPT

· 11 min read · Nov 28

4.3K 65

Lists



Self-Improvement 101

20 stories · 990 saves

Branding

33 stories · 98 saves

Staff Picks

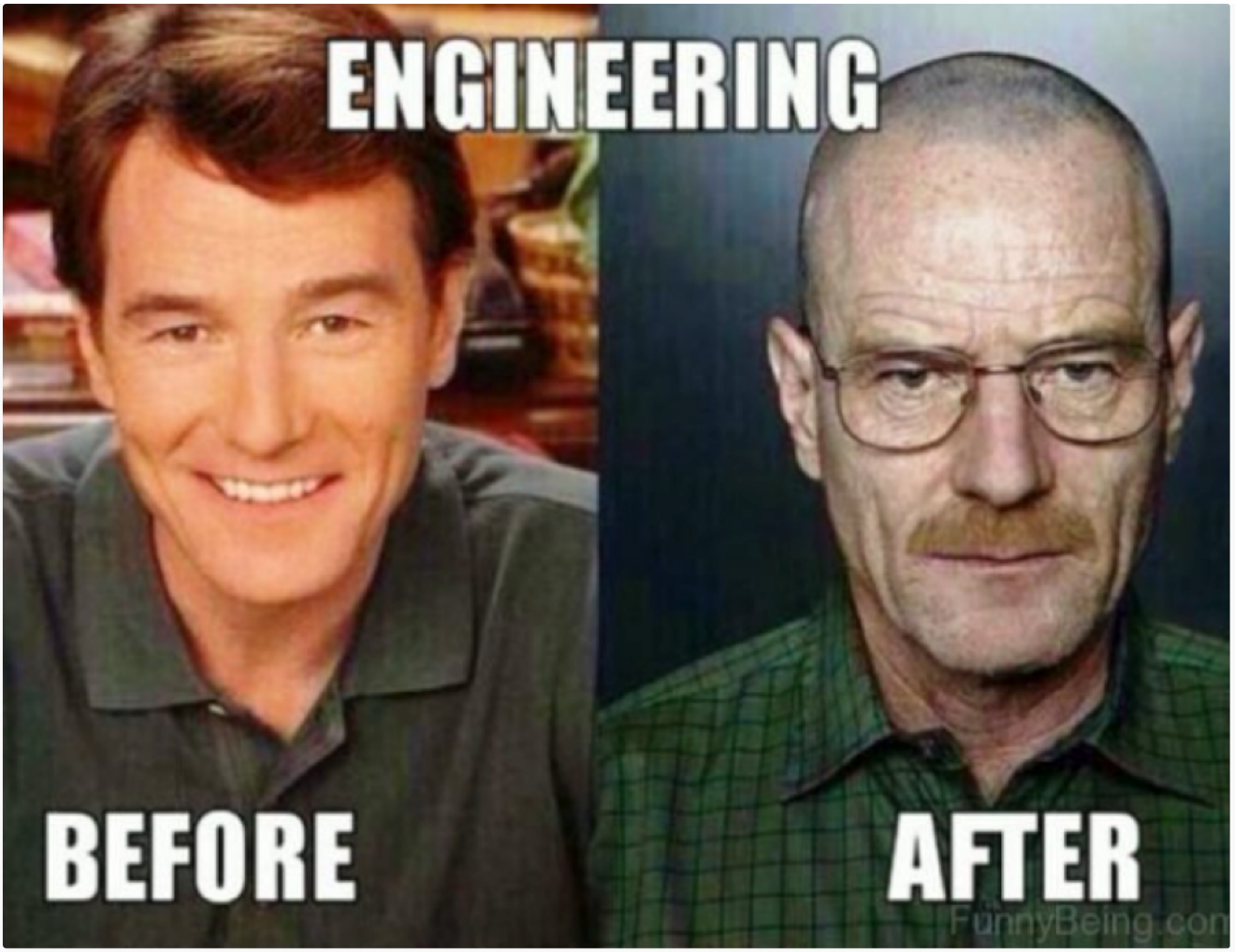
521 stories · 489 saves

Rohit Verma

My Interview Experience at Google [L5 Offer]

Comprehensive Insights: A Deep Dive into the Journey from Preparation Through Interviews to Securing the Offer.

9 min read · Nov 25



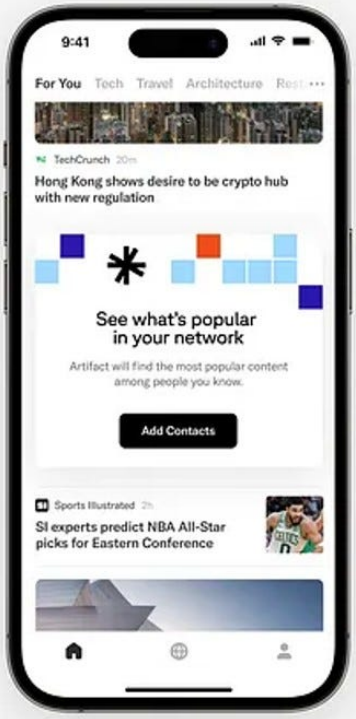
David Goudet

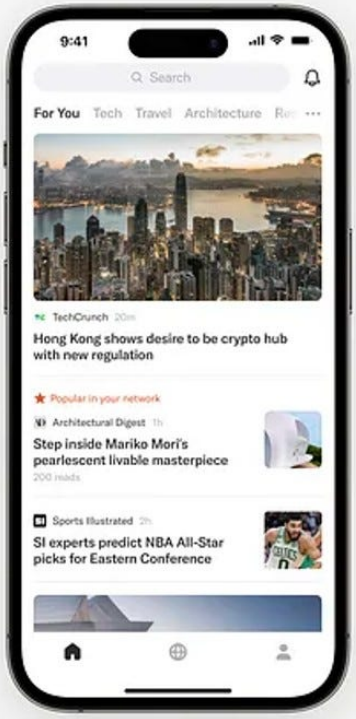
This is Why I Didn't Accept You as a Senior Software Engineer

An Alarming Trend in The Software Industry

5 min read · Jul 25

4.1K 51





ARTIFACT

Gowtham Oleti

Apps I Use And Why You Should Too.

Let’s skip past the usual suspects like YouTube, WhatsApp and Instagram. I want to share with you some less familiar apps that have become...

11 min read · Nov 14

1.96K 42

See more recommendations