Networking Interview Questions

This note is prepared for aspiring candidates interviewing for positions such as Software Engineer, DevOps Engineer, or faculty roles. It covers the questions typically asked in these interviews. Questions were gathered from various online sources and appropriate references are provided at the end.

Prepared By

Salman Farsi

CSE, CUET'18

Contact: salman.cuet.cse@gmail.com

LinkedIn: salmanfarsi0

GitHub: Salman1804102

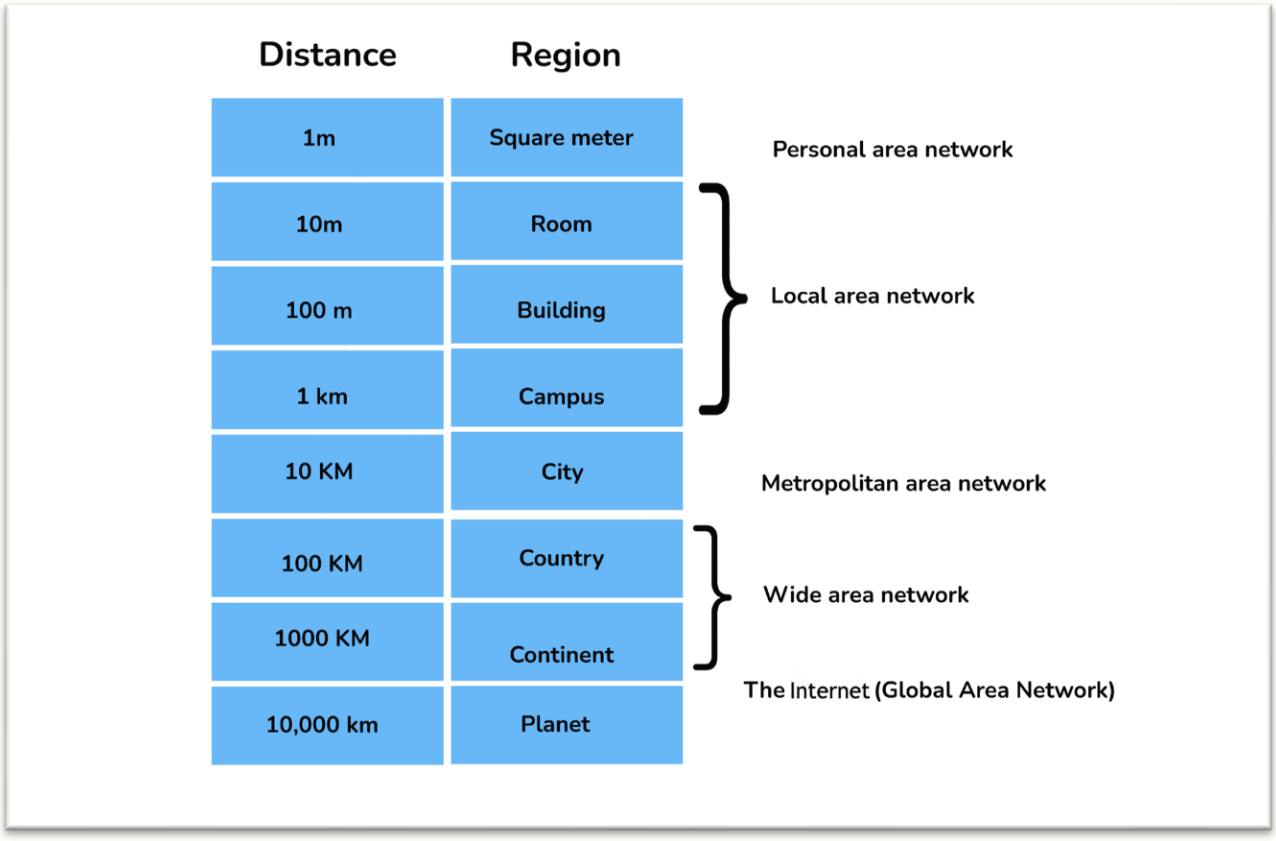
Contents

Define network

- A network is a set of devices that are connected with a physical media link. In a network, two or more nodes are connected by a physical link, or two or more networks are connected by one or more nodes.
- A network is a collection of devices connected to each other to allow the sharing of data.
- An example of a network is the internet. The internet connects millions of people across the world.

How are Network types classified? Explain different types of networks.

Network types can be classified and divided based on the area of distribution of the network. The below diagram would help to understand the same:



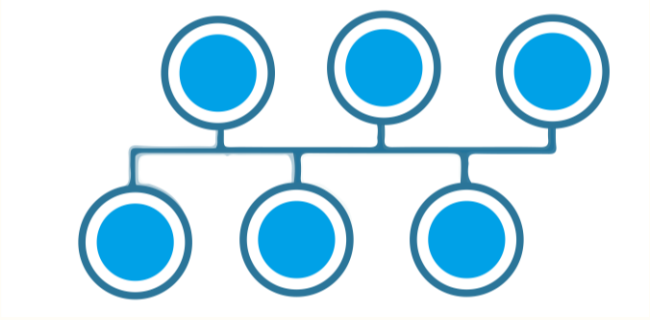
Below are a few types of networks:

Type	Description
PAN (Personal Area Network)	Let devices connect and communicate over the range of a person. E.g. connecting Bluetooth devices.
LAN (Local Area Network)	It is a privately owned network that operates within and nearby a single building like a home, office, or factory
MAN (Metropolitan Area Network)	It connects and covers the whole city. E.g. TV Cable connection over the city
WAN (Wide Area Network)	It spans a large geographical area, often a country or continent. The Internet is the largest WAN
GAN (Global Area Network)	It is also known as the Internet which connects the globe using satellites. The Internet is also called the Network of WANs.

Define different types of network topology

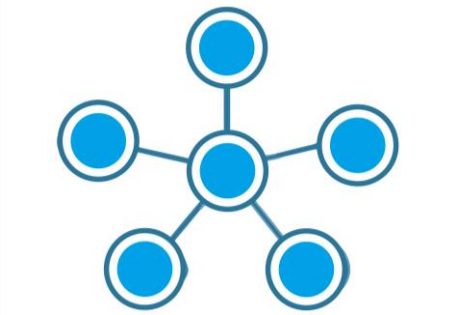
The different types of network topology are given below:

Bus Topology



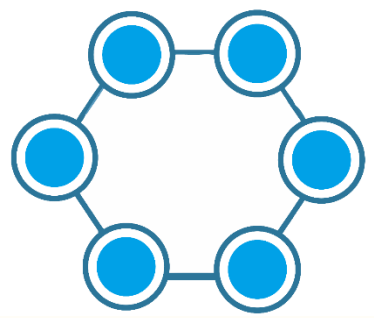
- All the nodes are connected using the central link known as the bus.
- It is useful to connect a smaller number of devices.
- If the main cable gets damaged, it will damage the whole network.

Star Topology:



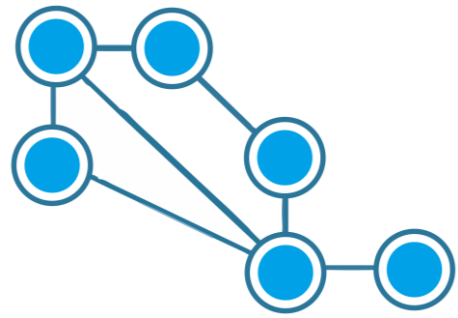
- All the nodes are connected to one single node known as the central node.
- It is more robust.
- If the central node fails the complete network is damaged.
- Easy to troubleshoot.
- Mainly used in home and office networks.

Ring Topology:



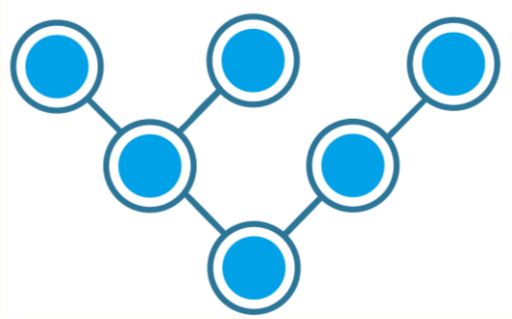
- Each node is connected to exactly two nodes forming a ring structure
- If one of the nodes is damaged, it will damage the whole network
- It is used very rarely as it is expensive and hard to install and manage

Mesh Topology:



- Each node is connected to one or many nodes.
- It is robust as failure in one link only disconnects that node.
- It is rarely used and installation and management are difficult.

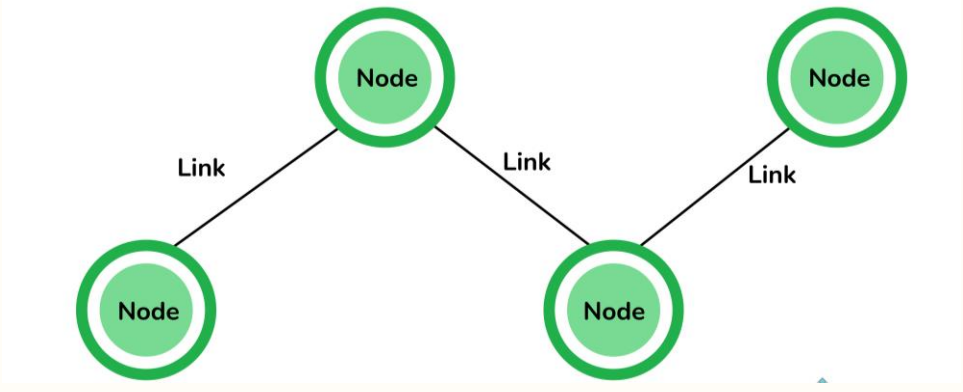
Tree Topology:



- A combination of star and bus topology also known as an extended bus topology.
- All the smaller star networks are connected to a single bus.
- If the main bus fails, the whole network is damaged.

Hybrid:

- It is a combination of different topologies to form a new topology.
- It helps to ignore the drawbacks of a particular topology and helps to pick the strengths from others.



Salman Farsi salman.cuet.cse.gmail.com LinkedIn

Why internet is called a network of networks?

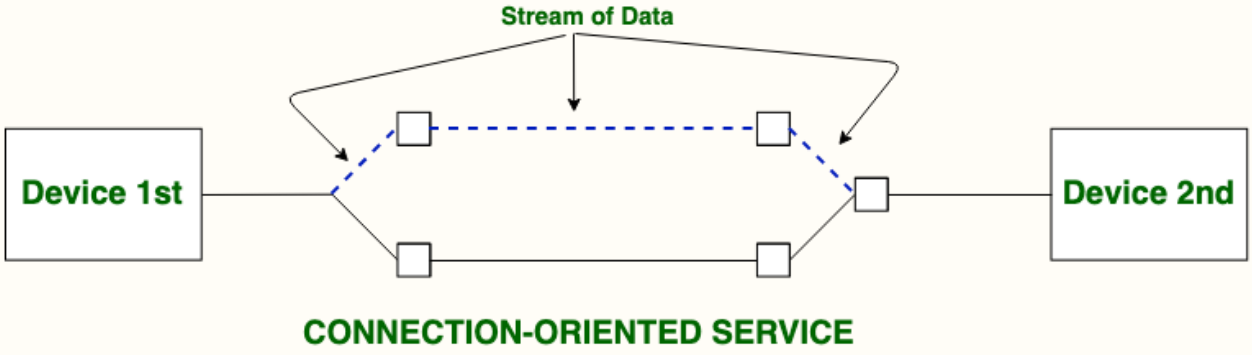
The Internet is a worldwide collection of networked computers, which are able to exchange information with each other in a very fast manner. The Internet is called a network of networks because it is a global network of computers that are linked together by cables and telephone lines making communication possible among them. It can be defined as a global network over a million smaller heterogeneous computer networks.

Difference Between Connection-oriented and Connection-less Services

Two basic forms of networking communication are connection-oriented and connection-less services. In order to provide dependable communication, connection-oriented services create a dedicated connection before transferring data. On the other hand, connection-less services prioritize speed and efficiency over reliability by transmitting data without establishing a connection. These types of services are offered by the network layer.

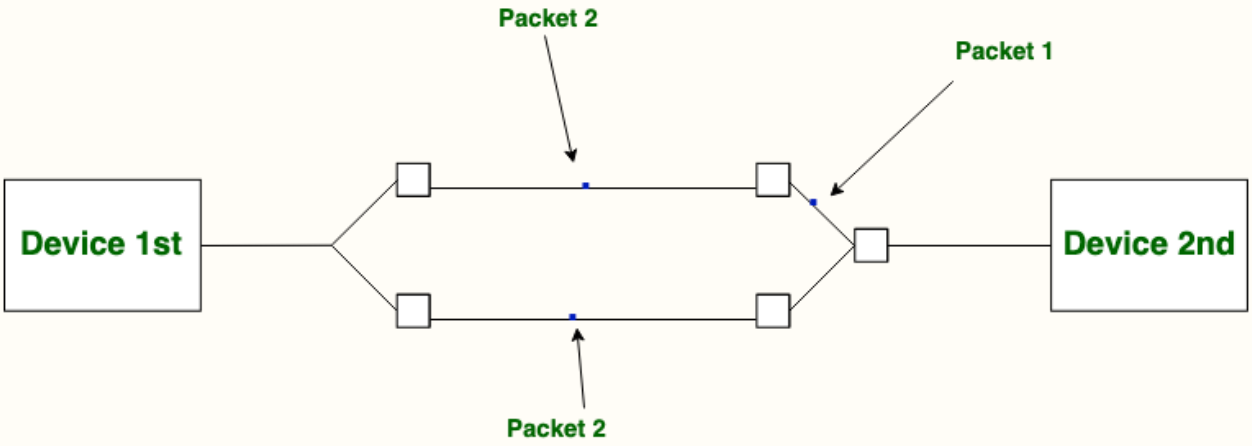
1. What is a Connection-Oriented Service?

Connection-oriented service is related to the telephone system. It includes connection establishment and connection termination. In a connection-oriented service, the Handshake method is used to establish the connection between sender and receiver. Before data transmission starts, connection-oriented services create a dedicated communication channel between the sender and the recipient.



2. What is Connection-Less Service?

Connection-less service is related to the postal system. It does not include any connection establishment and connection termination. Connection-less Service does not give a guarantee of reliability. In this, Packets do not follow the same path to reach their destination. Connection-less Services deliver individual data packets without first making a connection. Since each packet is sent separately, delivery, order, and mistake correction cannot be guaranteed. As a result, the service is quicker but less dependable. UDP (User Datagram Protocol) is one example, which is frequently used for streaming where dependability is not as important as speed.



CONNECTIONIESS SERVICE

3. Difference Between Connection-oriented and Connection-less Services

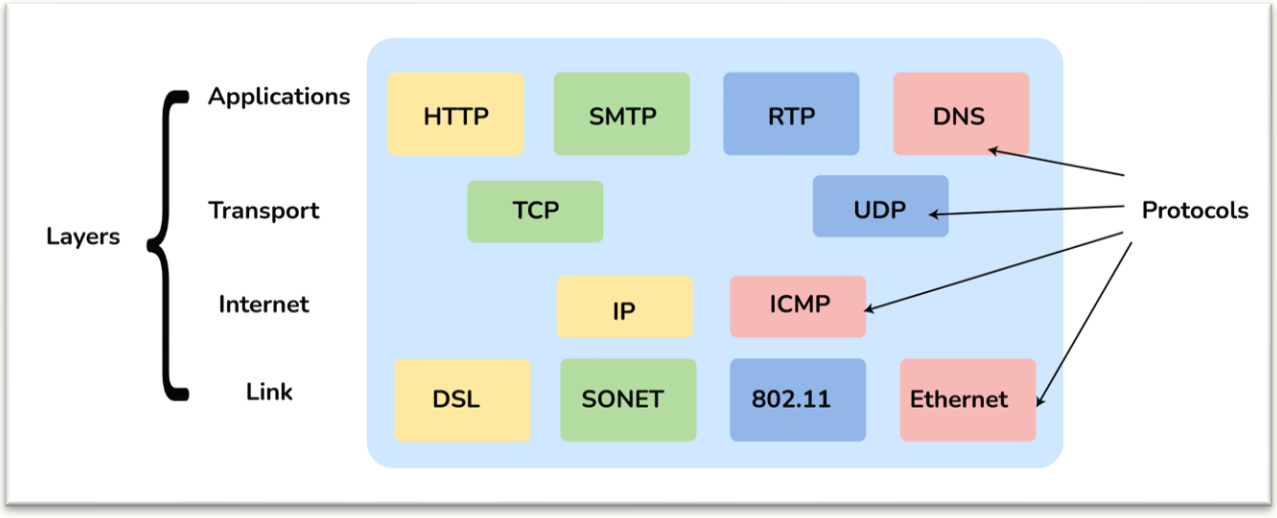
Connection-oriented Service	Connection-less Service
Connection-oriented service is related to the telephone system.	Connection-less service is related to the postal system.
Connection-oriented service is preferred by long and steady communication.	Connection-less Service is preferred by bursty communication.
Connection-oriented Service is necessary.	Connection-less Service is not compulsory.

Connection-oriented Service is feasible.	Connection-less Service is not feasible.
In connection-oriented Service, Congestion is not possible.	In connection-less Service, Congestion is possible.
Connection-oriented Service gives the guarantee of reliability.	Connection-less Service does not give a guarantee of reliability.
In connection-oriented Service, Packets follow the same route.	In connection-less Service, Packets do not follow the same route.
Connection-oriented services require a bandwidth of a high range.	Connection-less Service requires a bandwidth of low range.
Ex: TCP (Transmission Control Protocol)	Ex: UDP (User Datagram Protocol)
Connection-oriented requires authentication.	Connection-less Service does not require authentication.

What do you understand by TCP/IP?

TCP/IP is short for Transmission Control Protocol /Internet protocol. It is a set of protocol layers that is designed for exchanging data on different types of networks.

Define the 4 different layers of the TCP/IP Reference Model

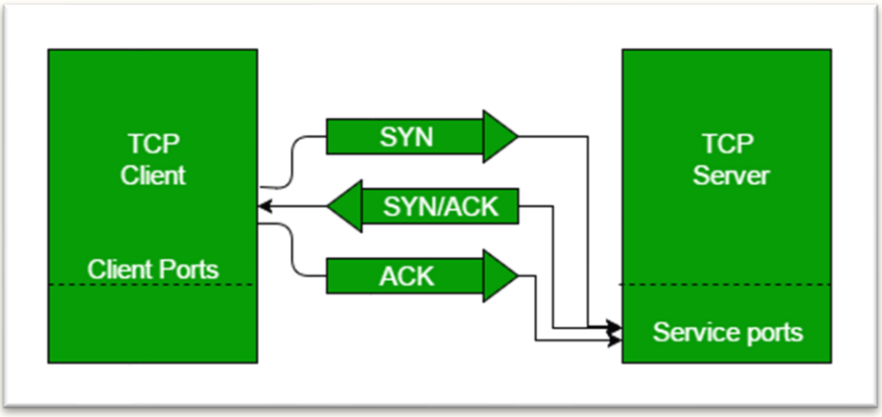


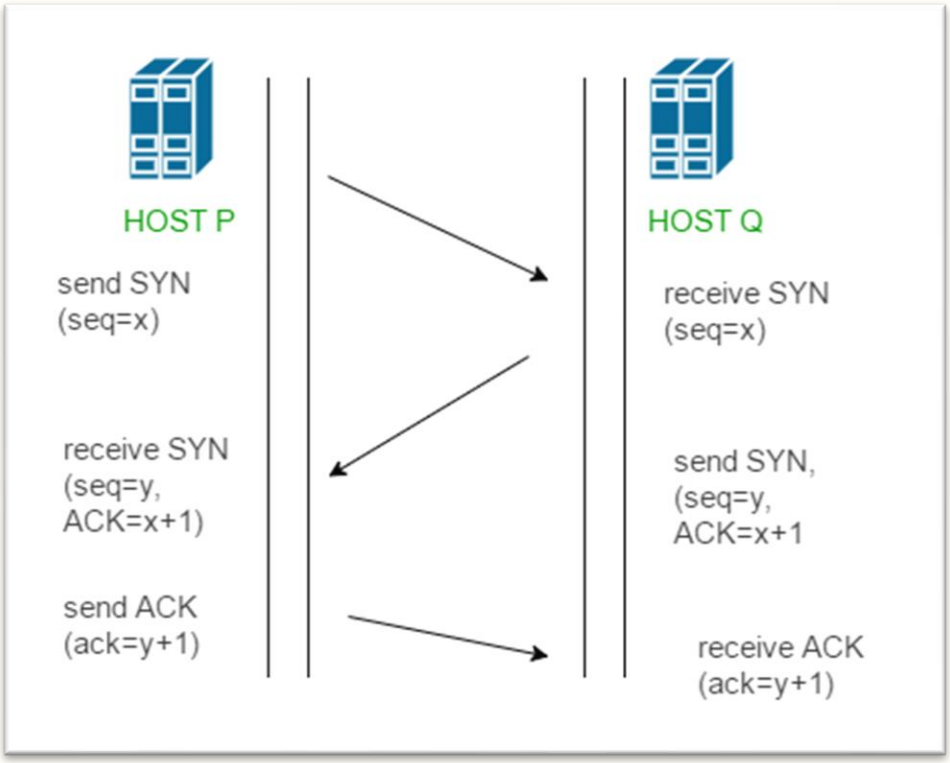
Layers of TCP/IP

Layer	Description
Link	Decides which links such as serial lines or classic Ethernet must be used to meet the needs of the connectionless internet layer.
Internet	• The internet layer is the most important layer which holds the whole architecture together. • It delivers the IP packets where they are supposed to be delivered.
Transport	Its functionality is almost the same as the OSI transport layer. It enables peer entities on the network to carry on a conversation.
Application	It contains all the higher-level protocols.

TCP 3-way Handshake Process

The process of communication between devices over the internet happens according to the current TCP/IP suite model. From the application layer, the information is transferred to the transport layer where our topic comes into the picture. The two important protocols of this layer are – TCP, and UDP(User Datagram Protocol) out of which TCP is prevalent(since it provides reliability for the connection established).





- **Step 1 (SYN):** In the first step, the client wants to establish a connection with a server, so it sends a segment with SYN(Synchronize Sequence Number) which informs the server that the client is likely to start communication and with what sequence number it starts segments with
- **Step 2 (SYN + ACK):** Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with
- **Step 3 (ACK):** In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer

Describe the OSI Reference Model

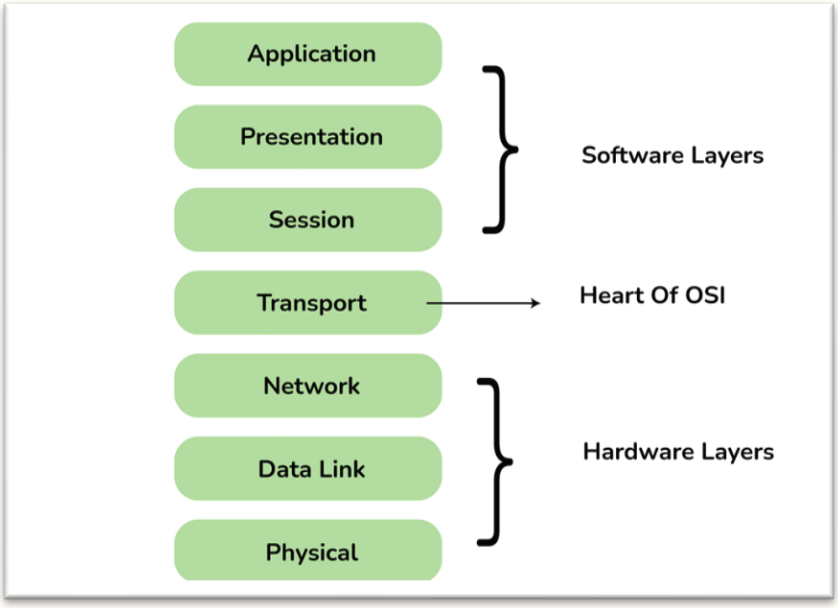
Open System Interconnections (OSI) is a network architecture model based on the ISO standards. It is called the OSI model as it deals with connecting the systems that are open for communication with other systems.

The OSI model has seven layers. The principles used to arrive at the seven layers can be summarized briefly below:

- Create a new layer if a different abstraction is needed.
- Each layer should have a well-defined function.
- The function of each layer is chosen based on internationally standardized protocols.

Define the 7 different layers of the OSI Reference Model

Here the 7 layers of the OSI reference model:



Layers of OSI Model

Layer	Unit Exchanged	Description
Physical	Bit	• It is concerned with transmitting raw bits over a communication channel. • Chooses which type of transmission mode is to be selected for the transmission. The available transmission modes are Simplex, Half Duplex and Full Duplex.,

Layer	Unit Exchanged	Description
Data Link	Frame	• The main task of this layer is to transform a raw transmission facility into a line that appears free of undetected transmission errors. • It also allows detecting damaged packets using the CRC (Cyclic Redundancy Check) error-detecting, code. • When more than one node is connected to a shared link, Data Link Layer protocols are required to determine which device has control over the link at a given time. • It is implemented by protocols like CSMA/CD, CSMA/CA, ALOHA, and Token Passing.
Network	Packet	• It controls the operation of the subnet. • The network layer takes care of feedback messaging through ICMP messages.
Transport	TPDU - Transaction Protocol Data Unit	• The basic functionality of this layer is to accept data from the above layers, split it up into smaller units if needed, pass these to the network layer, and ensure that all the pieces arrive correctly at the other end. • The Transport Layer takes care of Segmentation and Reassembly.
Session	SPDU - Session Protocol Data Unit	• The session layer allows users on different machines to establish sessions between them. • Dialogue control is using the full-duplex link as half-duplex. It sends out dummy packets from the client to the server when the client is ideal.
Presentation	PPDU - Presentation Protocol Data Unit	• The presentation layer is concerned with the syntax and semantics of the information transmitted.

Layer	Unit Exchanged	Description
		• It translates a message from a common form to the encoded format which will be understood by the receiver.
Application	APDU - Application Protocol Data Unit	• It contains a variety of protocols that are commonly needed by users. • The application layer sends data of any size to the transport layer.

How many layers are in OSI reference model?

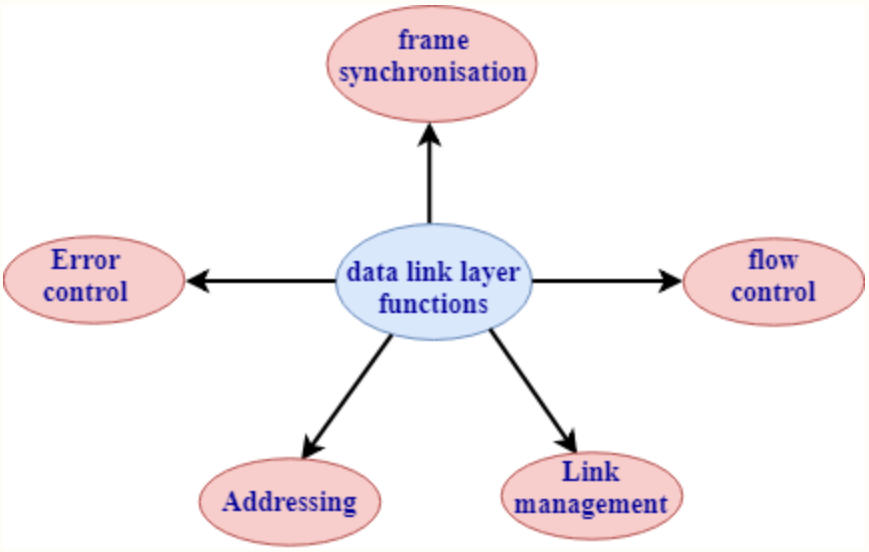
OSI reference model: OSI reference model is an ISO standard which defines a networking framework for implementing the protocols in seven layers.

1. Physical Layer

- It is the lowest layer of the OSI reference model.
- It is used for the transmission of an unstructured raw bit stream over a physical medium.
- Physical layer transmits the data either in the form of electrical/optical or mechanical form.
- The physical layer is mainly used for the physical connection between the devices, and such physical connection can be made by using twisted-pair cable, fibre-optic or wireless transmission media.

2. DataLink Layer

- It is used for transferring the data from one node to another node.
- It receives the data from the network layer and converts the data into data frames and then attach the physical address to these frames which are sent to the physical layer.
- It enables the error-free transfer of data from one node to another node. Functions of Data-link layer:

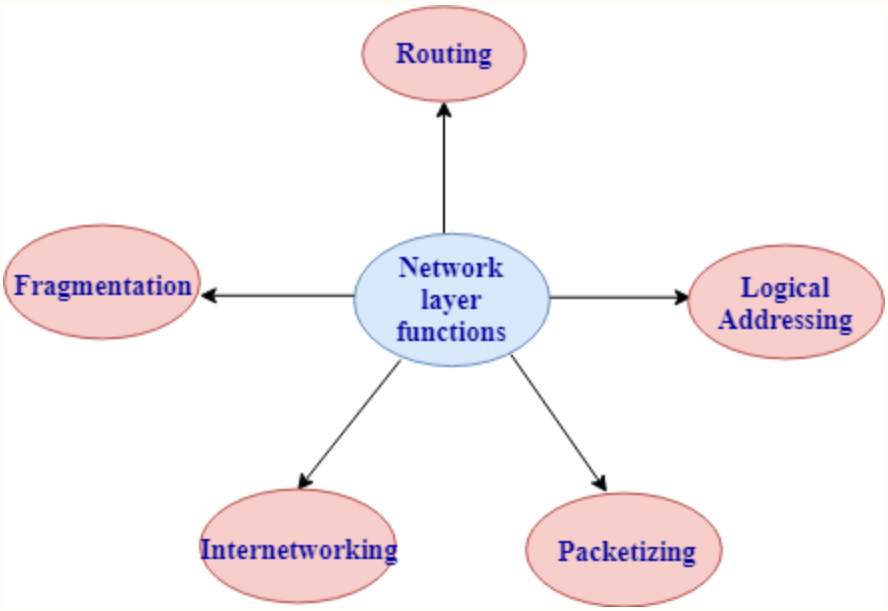


- **Frame synchronization:** Data-link layer converts the data into frames, and it ensures that the destination must recognize the starting and ending of each frame.
- Flow control: Data-link layer controls the data flow within the network.
- **Error control:** It detects and corrects the error occurred during the transmission from source to destination.
- **Addressing:** Data-link layer attaches the physical address with the data frames so that the individual machines can be easily identified.
- **Link management:** Data-link layer manages the initiation, maintenance, and, termination of the link between the source and destination for the effective exchange of data.

3. Network Layer

- Network layer converts the logical address into the physical address.
- It provides the routing concept means it determines the best route for the packet to travel from source to the destination.

Functions of network layer:



- **Routing:** The network layer determines the best route from source to destination. This function is known as routing.
- **Logical addressing:** The network layer defines the addressing scheme to identify each device uniquely.
- **Packetizing:** The network layer receives the data from the upper layer and converts the data into packets. This process is known as packetizing.
- **Internetworking:** The network layer provides the logical connection between the different types of networks for forming a bigger network.
- **Fragmentation:** It is a process of dividing the packets into the fragments.

4. Transport Layer

- It delivers the message through the network and provides error checking so that no error occurs during the transfer of data.
- It provides two kinds of services:
  - **Connection-oriented transmission:** In this transmission, the receiver sends the acknowledgement to the sender after the packet has been received.
  - **Connectionless transmission:** In this transmission, the receiver does not send the acknowledgement to the sender.

5. Session Layer

- The main responsibility of the session layer is beginning, maintaining and ending the communication between the devices.
- Session layer also reports the error coming from the upper layers.
- Session layer establishes and maintains the session between the two users.

6. Presentation Layer

- The presentation layer is also known as a Translation layer as it translates the data from one format to another format.
- At the sender side, this layer translates the data format used by the application layer to the common format and at the receiver side, this layer translates the common format into a format used by the application layer.

  Functions of presentation layer:

  - Character code translation
  - Data conversion
  - Data compression
  - Data encryption

7. Application Layer

- Application layer enables the user to access the network.
- It is the topmost layer of the OSI reference model.
- Application layer protocols are file transfer protocol, simple mail transfer protocol, domain name system, etc.
- The most widely used application protocol is HTTP(Hypertext transfer protocol). A user sends the request for the web page using HTTP.

What is the usage of OSI physical layer?

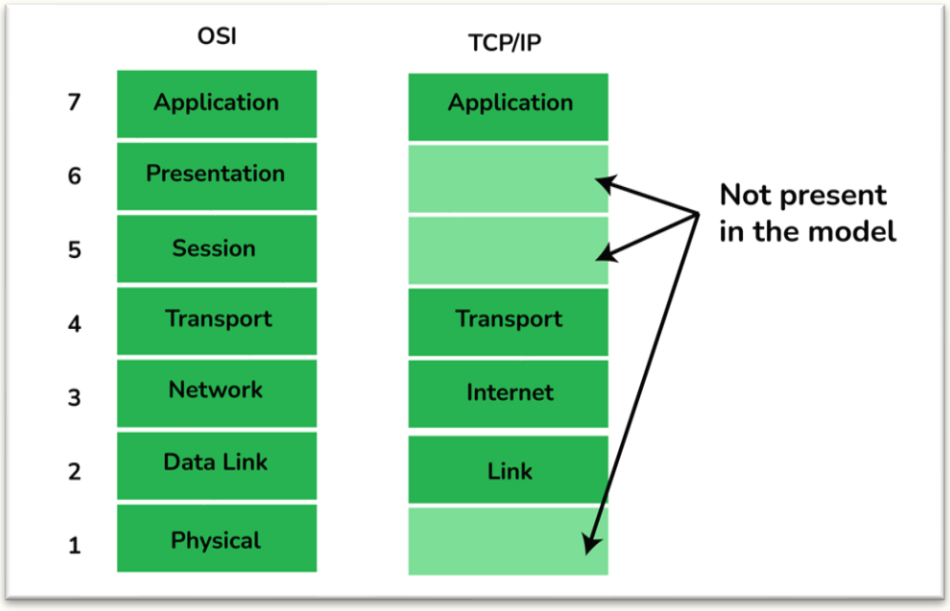
The OSI physical layer is used to convert data bits into electrical signals and vice versa. On this layer, network devices and cable types are considered and setup.

Explain the functionality of OSI session layer?

OSI session layer provides the protocols and means for two devices on the network to communicate with each other by holding a session. This layer is responsible for setting up the

session, managing information exchange during the session, and tear-down process upon termination of the session.

Differentiate OSI Reference Model with TCP/IP Reference Model



OSI Vs TCP/IP

OSI Reference Model	TCP/IP Reference Model
7 layered architecture	4 layered architecture
Fixed boundaries and functionality for each layer	Flexible architecture with no strict boundaries between layers
Low Reliability	High Reliability
Vertical Layer Approach	Horizontal Layer Approach

Following are the differences between the TCP/IP model and OSI model:

TCP/IP model	OSI model
Full form of TCP is transmission control protocol.	Full form of OSI is Open System Interconnection.
TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable than the OSI model.	OSI model is less reliable as compared to the TCP/IP model.
TCP/IP model uses horizontal approach.	OSI model uses vertical approach.
TCP/IP model uses both session and presentation layer in the application layer.	OSI Reference model uses separate session and presentation layers.
TCP/IP model developed the protocols first and then model.	OSI model developed the model first and then protocols.
In Network layer, TCP/IP model supports only connectionless communication.	In the Network layer, the OSI model supports both connection-oriented and connectionless communication.
TCP/IP model is a protocol dependent.	OSI model is a protocol independent.

What happens when you enter google.com in the web browser?

Below are the steps that are being followed:

- Check the browser cache first if the content is fresh and present in cache display the same.

- If not, the browser checks if the IP of the URL is present in the cache (browser and OS) if not then request the OS to do a DNS lookup using UDP to get the corresponding IP address of the URL from the DNS server to establish a new TCP connection.
- A new TCP connection is set between the browser and the server using three-way handshaking.
- An HTTP request is sent to the server using the TCP connection.
- The web servers running on the Servers handle the incoming HTTP request and send the HTTP response.
- The browser process the HTTP response sent by the server and may close the TCP connection or reuse the same for future requests.
- If the response data is cacheable then browsers cache the same.
- Browser decodes the response and renders the content.

Difference Between Segments, Packets and Frames

Feature	Segments	Packets	Frames
Layer	Transport layer (Layer 4)	Network layer (Layer 3)	Data Link layer (Layer 2)
Contains	Only raw data	Data + source and destination IP addresses	Data + IP addresses + MAC (hardware) addresses
Used in	Organizing data before sending	Routing data between different networks	Transferring data directly between connected devices
Size	Can be different sizes	Usually smaller, broken down for easier routing	Fixed size based on the network type (like Ethernet)
Header	Basic header with port numbers	More complex header with IP addresses	Most detailed header with MAC addresses
Main Job	Splitting data into manageable pieces	Routing data across networks	Handling actual physical transmission of data

Addressing	No addressing information	Uses IP addresses for routing	Uses MAC addresses for direct device communication

Summary of Differences:

- **Segment:** Used at the transport layer, contains data and transport layer headers (e.g., TCP or UDP headers).
- **Packet:** Used at the network layer, contains a segment and network layer headers (e.g., IP headers).
- **Frame:** Used at the data link layer, contains a packet and data link layer headers and trailers (e.g., Ethernet headers).

What is Framing?

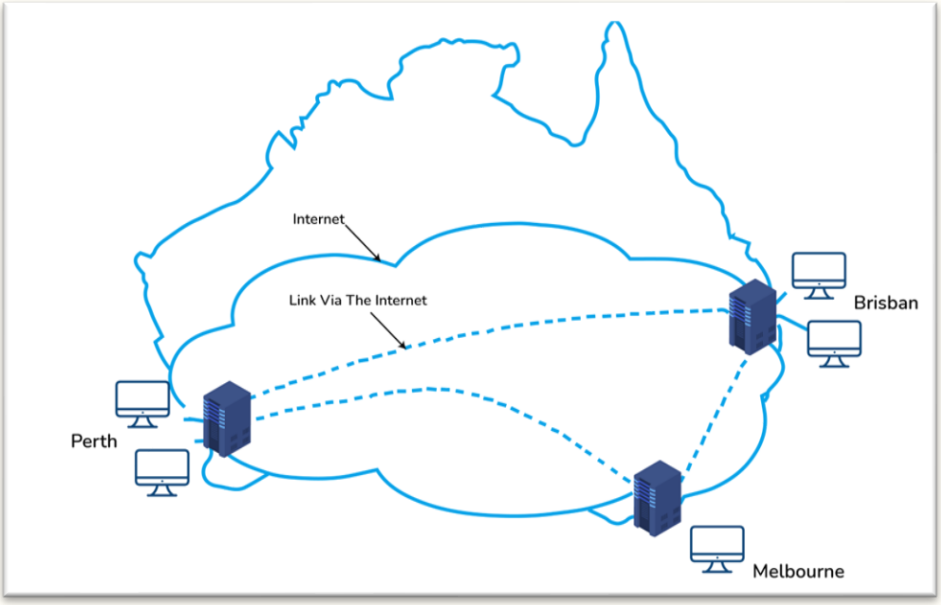
The data link layer receives packets from the network layer and delivers them to the physical layer for transmission. But when these packets are received at the destination end, it is not guaranteed to be error free. To achieve considerable error control and detection mechanisms, it is up to the data link layer to break the packets and form frames that are better for handling errors. The process of making frames from packets is known as framing.

Define Bandwidth

Bandwidth is the data transfer capacity of a computer network in bits per second (Bps). The term may also be used colloquially to indicate a person's capacity for tasks or deep thoughts at a point in time.

Tell me something about VPN (Virtual Private Network)

VPN or the Virtual Private Network is a private WAN (Wide Area Network) built on the internet. It allows the creation of a secured tunnel (protected network) between different networks using the internet (public network). By using the VPN, a client can connect to the organization’s network remotely. The below diagram shows an organizational WAN network over Australia created using VPN:



What are the advantages of using a VPN?

Below are few advantages of using VPN:

- VPN is used to connect offices in different geographical locations remotely and is cheaper when compared to WAN connections.
- VPN is used for secure transactions and confidential data transfer between multiple offices located in different geographical locations.
- VPN keeps an organization's information secured against any potential threats or intrusions by using virtualization.
- VPN encrypts the internet traffic and disguises the online identity.

What are the different types of VPN?

Few types of VPN are:

- **Access VPN:** Access VPN is used to provide connectivity to remote mobile users and telecommuters. It serves as an alternative to dial-up connections or ISDN (Integrated Services Digital Network) connections. It is a low-cost solution and provides a wide range of connectivity.

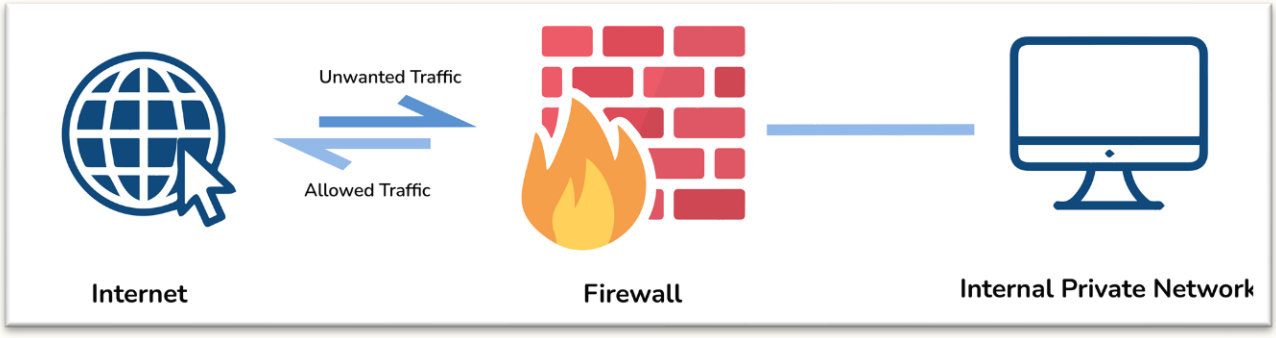
- **Site-to-Site VPN:** A Site-to-Site or Router-to-Router VPN is commonly used in large companies having branches in different locations to connect the network of one office to another in different locations. There are 2 sub-categories as mentioned below:
- **Intranet VPN**: Intranet VPN is useful for connecting remote offices in different geographical locations using shared infrastructure (internet connectivity and servers) with the same accessibility policies as a private WAN (wide area network).
- **Extranet VPN:** Extranet VPN uses shared infrastructure over an intranet, suppliers, customers, partners, and other entities and connects them using dedicated connections.

What is the use of a router and how is it different from a gateway?

The router is a networking device used for connecting two or more network segments. It directs the traffic in the network. It transfers information and data like web pages, emails, images, videos, etc. from source to destination in the form of packets. It operates at the network layer. The gateways are also used to route and regulate the network traffic but, they can also send data between two dissimilar networks while a router can only send data to similar networks.

What is the firewall?

The firewall is a network security system that is used to monitor the incoming and outgoing traffic and blocks the same based on the firewall security policies. It acts as a wall between the internet (public network) and the networking devices (a private network). It is either a hardware device, software program, or a combination of both. It adds a layer of security to the network.



Compare the hub vs switch

Hub	Switch
Operates at Physical Layer	Operates at Data Link Layer
Half-Duplex transmission mode	Full-Duplex transmission mode
Ethernet devices can be connectedsend	LAN devices can be connected
Less complex, less intelligent, and cheaper	Intelligent and effective
No software support for the administration	Administration software support is present
Less speed up to 100 MBPS	Supports high speed in GBPS
Less efficient as there is no way to avoid collisions when more than one nodes sends the packets at the same time	More efficient as the collisions can be avoided or reduced as compared to Hub

Hub: Hub is a networking device which is used to transmit the signal to each port (except one port) to respond from which the signal was received. Hub is operated on a Physical layer. In this packet filtering is not available. It is of two types: Active Hub, Passive Hub.

Switch: Switch is a network device which is used to enable the connection establishment and connection termination on the basis of need. Switch is operated on the Data link layer. In this packet filtering is available. It is a type of full duplex transmission mode and it is also called an efficient bridge.

What are Unicasting, Anycasting, Multicasting and Broadcasting?

- **Unicasting:** If the message is sent to a single node from the source then it is known as unicasting. This is commonly used in networks to establish a new connection.
- **Anycasting:** If the message is sent to any of the nodes from the source then it is known as anycasting. It is mainly used to get the content from any of the servers in the Content Delivery System.

- **Multicasting:** If the message is sent to a subset of nodes from the source then it is known as multicasting. Used to send the same data to multiple receivers.
- **Broadcasting:** If the message is sent to all the nodes in a network from a source then it is known as broadcasting. DHCP and ARP in the local network use broadcasting

What is the DNS?

DNS is the Domain Name System. It is considered as the devices/services directory of the Internet. It is a decentralized and hierarchical naming system for devices/services connected to the Internet. It translates the domain names to their corresponding IPs. For e.g. interviewbit.com to 172.217.166.36. It uses port 53 by default.

DNS:

1. DNS is an acronym that stands for Domain Name System.DNS was introduced by Paul Mockapetris and Jon Postel in 1983.
2. It is a naming system for all the resources over the internet which includes physical nodes and applications. It is used to locate resources easily over a network.
3. DNS is an internet which maps the domain names to their associated IP addresses.
4. Without DNS, users must know the IP address of the web page that you wanted to access.

DNS Forwarder: A forwarder is used with a DNS server when it receives DNS queries that cannot be resolved quickly. So it forwards those requests to external DNS servers for resolution. A DNS server which is configured as a forwarder will behave differently than the DNS server which is not configured as a forwarder.

NIC: NIC stands for Network Interface Card. It is a peripheral card attached to the PC to connect to a network. Every NIC has its own MAC address that identifies the PC on the network. It provides a wireless connection to a local area network. NICs were mainly used in desktop computers.

What is protocol?

A protocol is a set of rules which is used to govern all the aspects of information communication.

What are the main elements of a protocol?

The main elements of a protocol are:

- Syntax: It specifies the structure or format of the data. It also specifies the order in which they are presented.
- Semantics: It specifies the meaning of each section of bits.
- Timing: Timing specifies two characteristics: When data should be sent and how fast it can be sent.

What are the different Routing Protocols?

Routing protocols are essential for determining how data is transmitted between different networks. They help routers find the best path for data packets to travel across complex networks. Below is a simplified explanation of each protocol you mentioned:

RIP (Routing Information Protocol)

What It Is:

RIP is one of the oldest routing protocols used in networking. It is a distance-vector routing protocol, which means it calculates the best route based on the number of hops (or steps) to the destination.

How It Works:

- Distance-Vector: RIP uses a simple metric called "hop count" to determine the best path. Each router in the network tells its neighbors about the networks it can reach, and how many hops away they are.
- Maximum Hops: RIP limits the maximum hop count to 15. If a network is more than 15 hops away, it is considered unreachable.
- Updates: RIP sends updates every 30 seconds to share routing information, which can lead to slower convergence (the time it takes for all routers to have a consistent view of the network).
- Simple and Easy to Configure: Due to its simplicity, RIP is easy to set up but is not suitable for large or complex networks due to its limitations.

EGP (Exterior Gateway Protocol)

What It Is:

EGP is a type of routing protocol used to exchange routing information between different autonomous systems (AS), which are large networks or collections of networks under a single administrative control.

How It Works:

- Exterior Gateway: EGP is designed to manage routing between different autonomous systems rather than within a single AS.
- Simple Protocol: The original EGP is now mostly obsolete, having been replaced by BGP (Border Gateway Protocol), which is more advanced and widely used for routing between large networks on the Internet.
- Inter-AS Communication: EGP protocols allow different organizations or networks to communicate with each other, making the global Internet possible.

EIGRP (Enhanced Interior Gateway Routing Protocol)

What It Is:

EIGRP is a more advanced routing protocol developed by Cisco. It is a hybrid protocol, combining the best features of both distance-vector and link-state routing protocols.

How It Works:

- Hybrid Approach: EIGRP uses both hop count and more sophisticated metrics like bandwidth, delay, and reliability to determine the best path.
- Rapid Convergence: EIGRP is known for quickly updating the routing table when network changes occur, which means it adapts to changes in the network very fast.
- DUAL Algorithm: EIGRP uses the Diffusing Update Algorithm (DUAL) to ensure a loop-free and efficient path selection.
- Compatibility: While it is a Cisco proprietary protocol, it is widely used in many enterprise networks due to its efficiency and scalability.

OSPF (Open Shortest Path First)

What It Is:

OSPF is a link-state routing protocol used within a single autonomous system. It is one of the most commonly used protocols in large enterprise networks.

How It Works:

- Link-State Protocol: OSPF creates a complete map (or topology) of the network. Each router calculates the shortest path to every other router using an algorithm called Dijkstra's Shortest Path First.
- Area Hierarchy: OSPF networks can be divided into different areas, which helps manage large and complex networks more efficiently.
- Fast Convergence: OSPF quickly responds to changes in the network, making it highly reliable for dynamic and large-scale networks.
- Cost Metric: OSPF uses a "cost" metric, usually based on bandwidth, to determine the best path for data packets.

IGP (Interior Gateway Protocol)

What It Is:

IGP is a type of routing protocol used within a single autonomous system, like a corporate network. It contrasts with EGP, which is used between different autonomous systems.

How It Works:

- Interior Gateway: IGP protocols manage routing within an organization's internal network.
- Examples of IGP: Common IGPs include RIP, OSPF, and EIGRP.
- Choosing the Best Path: IGPs help routers within the same organization or network to find the best path for data packets.

Summary:

- RIP: Simple, hop-based routing; suitable for small networks.
- EGP: Used for routing between large networks; mostly replaced by BGP.
- EIGRP: Advanced, hybrid protocol with fast convergence; Cisco proprietary.
- OSPF: Link-state protocol with fast convergence and area hierarchy; widely used in large networks.

- IGP: General term for protocols used within a single network, including RIP, OSPF, and EIGRP.

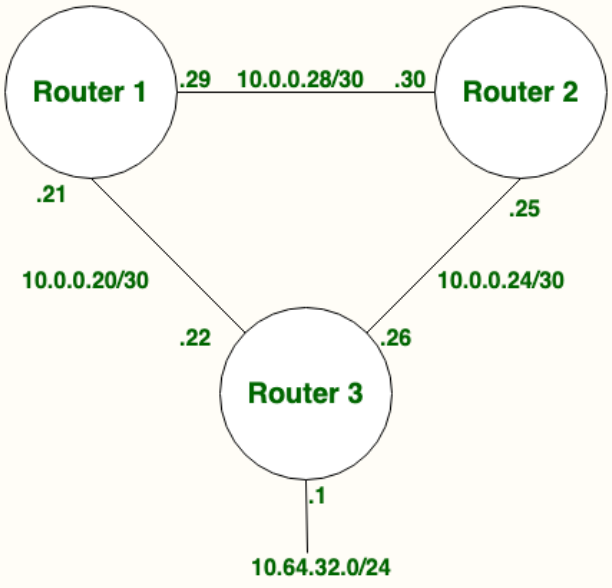
These protocols are critical for ensuring that data is routed efficiently across networks, whether within a small organization or across the global Internet.

Explain Static Routing and Dynamic Routing:

Routing is a vital communication mechanism that governs how data packets travel from source to destination. Effective routing ensures that data is transferred across networks in an efficient, reliable, and timely manner. There are two main forms of routing: static and dynamic. In this article, we will discuss the differences between static and dynamic routing.

• What is Static Routing?

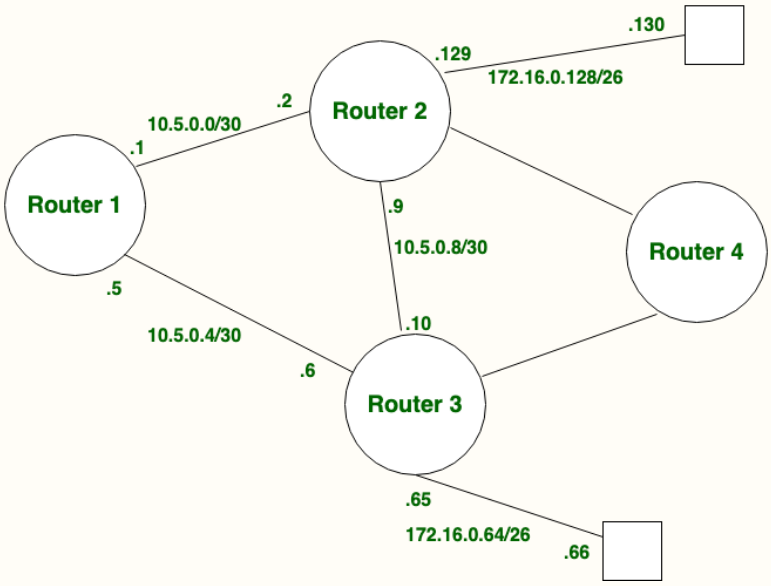
Static Routing is also known as non-adaptive routing which doesn't change the routing table unless the network administrator changes or modifies them manually. Static routing does not use complex routing algorithms and It provides higher or more security than dynamic routing.



• What is Dynamic Routing?

Dynamic routing is also known as adaptive routing which changes the routing table according to the change in topology. Dynamic routing uses complex routing algorithms and it does not provide

high security like static routing. When the network change(topology) occurs, it sends the message to the router to ensure that changes then the routes are recalculated for sending updated routing information.



Static Routing Vs Dynamic Routing

Static Routing	Dynamic Routing
In static routing routes are user-defined.	In dynamic routing, routes are updated according to the topology.
Static routing does not use complex routing algorithms.	Dynamic routing uses complex routing algorithms.
Static routing provides high or more security.	Dynamic routing provides less security.
Static routing is manual.	Dynamic routing is automated.
Static routing is implemented in small networks.	Dynamic routing is implemented in large networks.
In static routing, additional resources are not required.	In dynamic routing, additional resources are required.

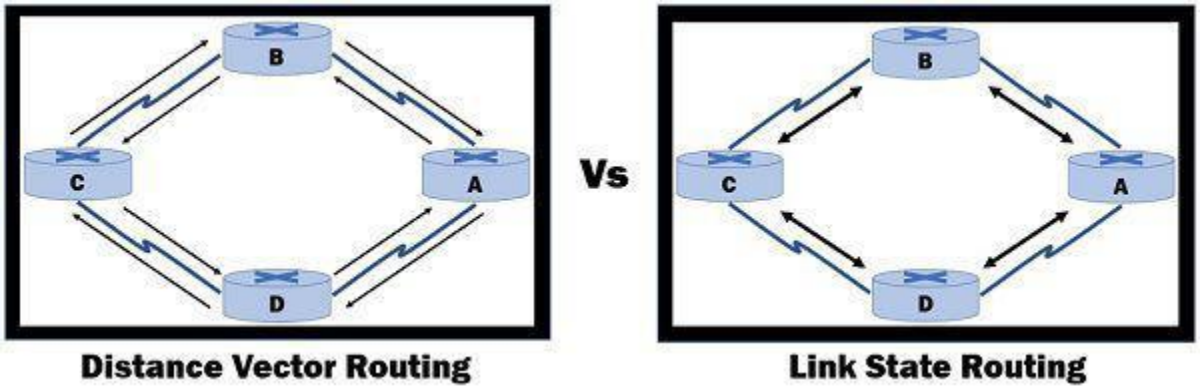
In static routing, failure of the link disrupts the rerouting.	In dynamic routing, failure of the link does not interrupt the rerouting.
Less Bandwidth is required in Static Routing.	More Bandwidth is required in Dynamic Routing.
Static Routing is difficult to configure.	Dynamic Routing is easy to configure.
Another name for static routing is non-adaptive routing.	Another name for dynamic routing is adaptive routing.

Difference between Distance vector routing and Link State routing

Routing, a process in computer networks, is responsible for the best path to transmit data packets from one node to another.

What is Distance Vector Routing?

Distance Vector Routing is an algorithm that is subject to change where a router calculates distances to every possible destination based on its immediate neighbors only, the router's routing table is shared with routers that are directly connected, during regular intervals, this received information makes the routers update their tables while route computation employs Bellman-Ford algorithm most of the time, in spite of being relatively simple, however, Distance Vector Routing has some problems such as Count to Infinity or persistent routing loops.



What is Link State Routing?

Link State Routing, as opposed to Distance Vector Routing, is a dynamic routing algorithm such that each router maintains knowledge of the entire network, instead of sharing information only with neighbors, routers flood their link state information across the entire network to make sure all routers have the same view of the network topology, Dijkstra's Algorithm and other Link State Routing algorithms are employed in order to compute shortest path to all destinations, it does not lead to persistent loop but it can result in more network traffic due to flooding link state information.

Comparison between Distance Vector Routing and Link State Routing

Distance Vector Routing	Link State Routing
Bandwidth required is less due to local sharing, small packets and no flooding.	Bandwidth required is more due to flooding and sending of large link state packets.
Based on local knowledge, since it updates table based on information from neighbours.	Based on global knowledge, it have knowledge about entire network.
Make use of Bellman Ford Algorithm.	Make use of Dijakstra's algorithm.
Traffic is less.	Traffic is more.
Converges slowly i.e, good news spread fast and bad news spread slowly.	Converges faster.
Count of infinity problem.	No count of infinity problem.
Persistent looping problem i.e, loop will be there forever.	No persistent loops, only transient loops.
Practical implementation is RIP and IGRP.	Practical implementation is OSPF and ISIS.

What is Count to Infinity and Persistent Loop Problem in Distant Vector Routing?

Count to Infinity Problem:

The count to infinity problem in distance vector routing arises when a network link fails, causing routers to gradually increase their distance metric (hop count) towards infinity as they try to find an alternate route. This happens because routers exchange outdated information, leading to slow

convergence and delayed recognition that the destination is unreachable. The problem persists until the metric reaches a predefined "infinity" value (e.g., 16 hops in RIP), signaling the route's unavailability.

Persistent Loop Problem:

The persistent loop problem occurs when incorrect routing updates create a circular path, causing data packets to circulate endlessly between routers. This loop continues until the routing tables are corrected, leading to network congestion, packet loss, and inefficiency.

Solutions

- **Split Horizon:** Prevents a router from advertising a route back in the direction it was learned.
- **Route Poisoning:** Advertises an infinite metric for failed routes to quickly indicate unreachability.
- **Hold-Down Timers:** Delays changes in routing tables to prevent rapid, incorrect updates.

These techniques help improve network stability and convergence, mitigating the count to infinity and persistent loop problems.

What is the FTP protocol?

FTP is a File Transfer Protocol. It is an application layer protocol used to transfer files and data reliably and efficiently between hosts. It can also be used to download files from remote servers to your computer. It uses port 27 by default.

What is the TCP protocol?

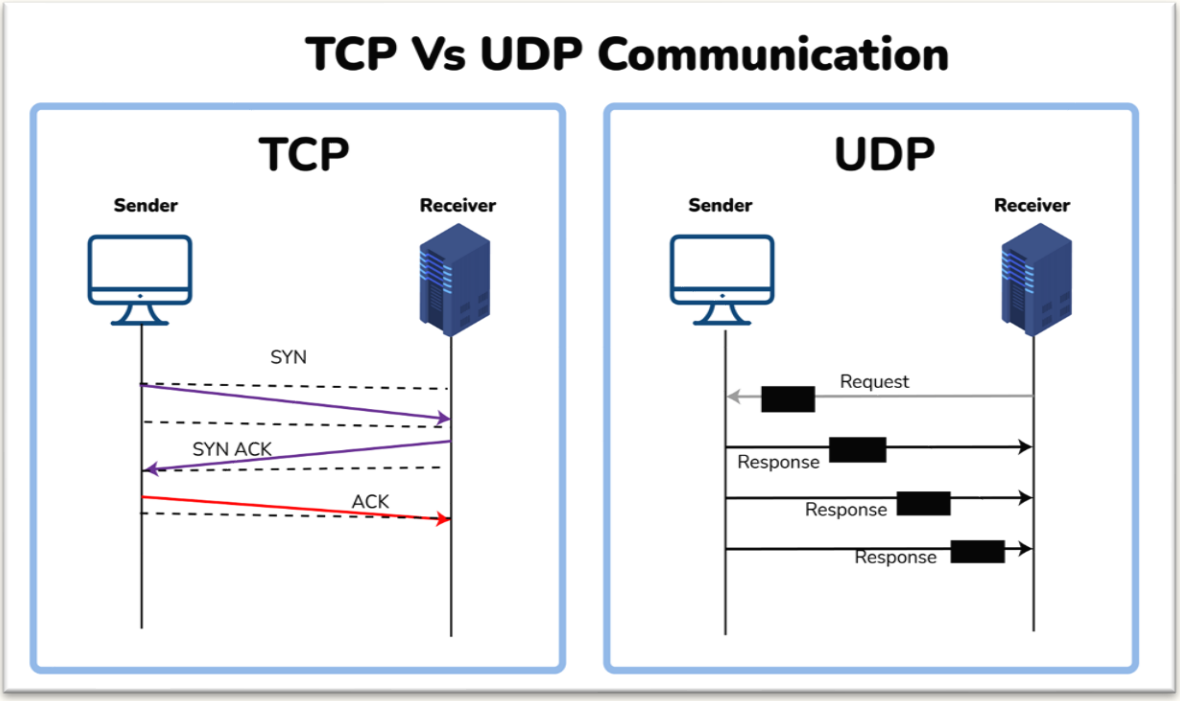
TCP or TCP/IP is the Transmission Control Protocol/Internet Protocol. It is a set of rules that decides how a computer connects to the Internet and how to transmit the data over the network. It creates a virtual network when more than one computer is connected to the network and uses the three ways handshake model to establish the connection which makes it more reliable.

What is the UDP protocol?

UDP is the User Datagram Protocol and is based on Datagrams. Mainly, it is used for multicasting and broadcasting. Its functionality is almost the same as TCP/IP Protocol except for the three ways of handshaking and error checking. It uses a simple transmission without any hand-shaking which makes it less reliable.

Compare between TCP and UDP

TCP/IP	UDP
Connection-Oriented Protocol	Connectionless Protocol
More Reliable	Less Reliable
Slower Transmission	Faster Transmission
Packets order can be preserved or can be rearranged	Packets order is not fixed and packets are independent of each other
Uses three ways handshake model for connection	No handshake for establishing the connection
TCP packets are heavy-weight	UDP packets are light-weight
Offers error checking mechanism	No error checking mechanism
Protocols like HTTP, FTP, Telnet, SMTP, HTTPS, etc use TCP at the transport layer	Protocols like DNS, RIP, SNMP, RTP, BOOTP, TFTP, NIP, etc use UDP at the transport layer



What is the ICMP protocol?

ICMP is the Internet Control Message Protocol. It is a network layer protocol used for error handling. It is mainly used by network devices like routers for diagnosing the network connection issues and crucial for error reporting and testing if the data is reaching the preferred destination in time. It uses port 7 by default.

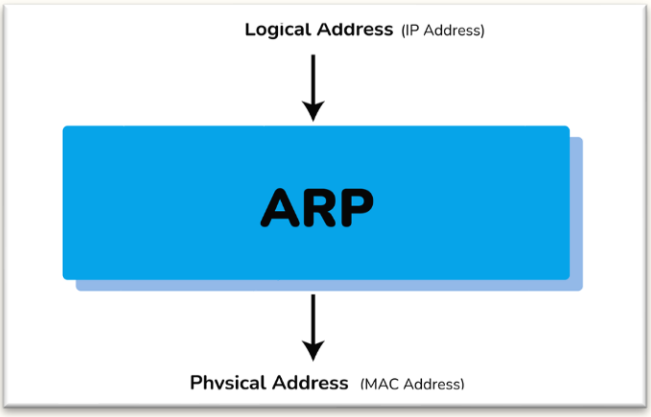
What do you mean by the DHCP Protocol?

DHCP is the Dynamic Host Configuration Protocol.

It is an application layer protocol used to auto-configure devices on IP networks enabling them to use the TCP and UDP-based protocols. The DHCP servers auto-assign the IPs and other network configurations to the devices individually which enables them to communicate over the IP network. It helps to get the subnet mask, IP address and helps to resolve the DNS. It uses port 67 by default.

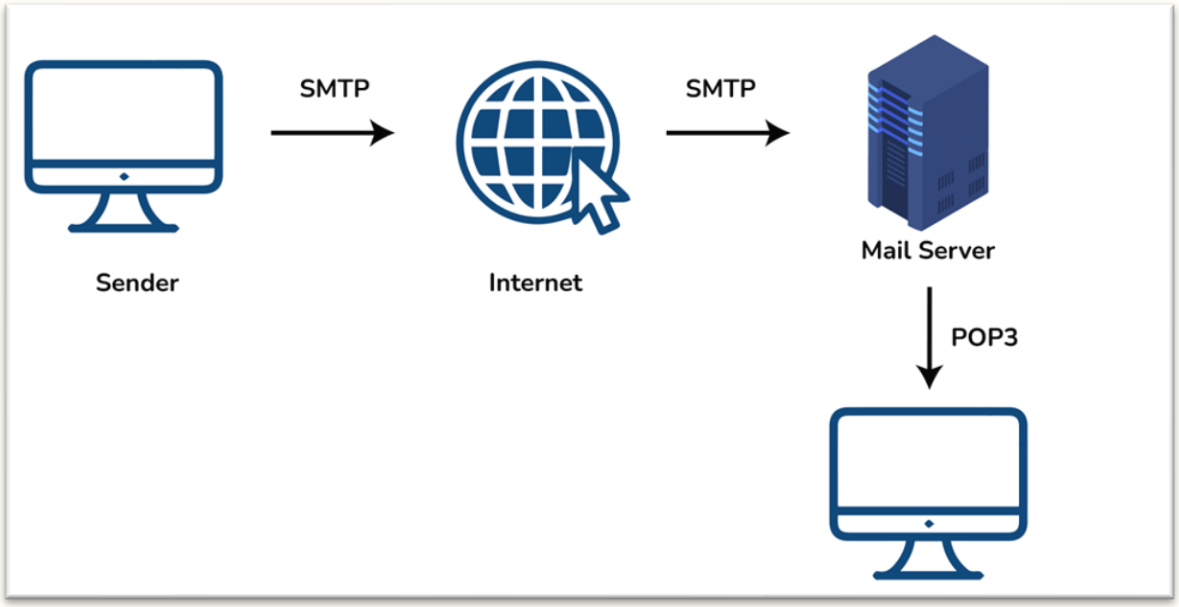
What is the ARP protocol?

ARP is Address Resolution Protocol. It is a network-level protocol used to convert the logical address i.e. IP address to the device's physical address i.e. MAC address. It can also be used to get the MAC address of devices when they are trying to communicate over the local network.



What is the SMTP protocol?

SMTP is the Simple Mail Transfer Protocol. SMTP sets the rule for communication between servers. This set of rules helps the software to transmit emails over the internet. It supports both End-to-End and Store-and-Forward methods. It is in always-listening mode on port 25.



What are the HTTP and the HTTPS protocol?

HTTP is the HyperText Transfer Protocol which defines the set of rules and standards on how the information can be transmitted on the World Wide Web (WWW). It helps the web browsers and

web servers for communication. It is a 'stateless protocol' where each command is independent with respect to the previous command. HTTP is an application layer protocol built upon the TCP. It uses port 80 by default.

HTTPS is the HyperText Transfer Protocol Secure or Secure HTTP. It is an advanced and secured version of HTTP. On top of HTTP, SSL/TLS protocol is used to provide security. It enables secure transactions by encrypting the communication and also helps identify network servers securely. It uses port 443 by default.

What is IP?

An IP, or Internet Protocol address, is a unique set of numbers assigned to each device connected to a network, like the Internet. It's like an address for your computer, phone, or any other device, allowing them to communicate with each other. When you visit a website, your device uses the IP address to find and connect to the website's server.

What is the MAC address and how is it related to NIC?

MAC address is the Media Access Control address. It is a 48-bit or 64-bit unique identifier of devices in the network. It is also called the physical address embedded with Network Interface Card (NIC) used at the Data Link Layer. NIC is a hardware component in the networking device using which a device can connect to the network.

Differentiate the MAC address with the IP address

The difference between MAC address and IP address are as follows:

MAC Address	IP Address
Media Access Control Address	Internet Protocol Address
6 or 8-byte hexadecimal number	4 (IPv4) or 16 (IPv6) Byte address
It is embedded with NIC	It is obtained from the network
Physical Address	Logical Address
Operates at Data Link Layer	Operates at Network Layer.

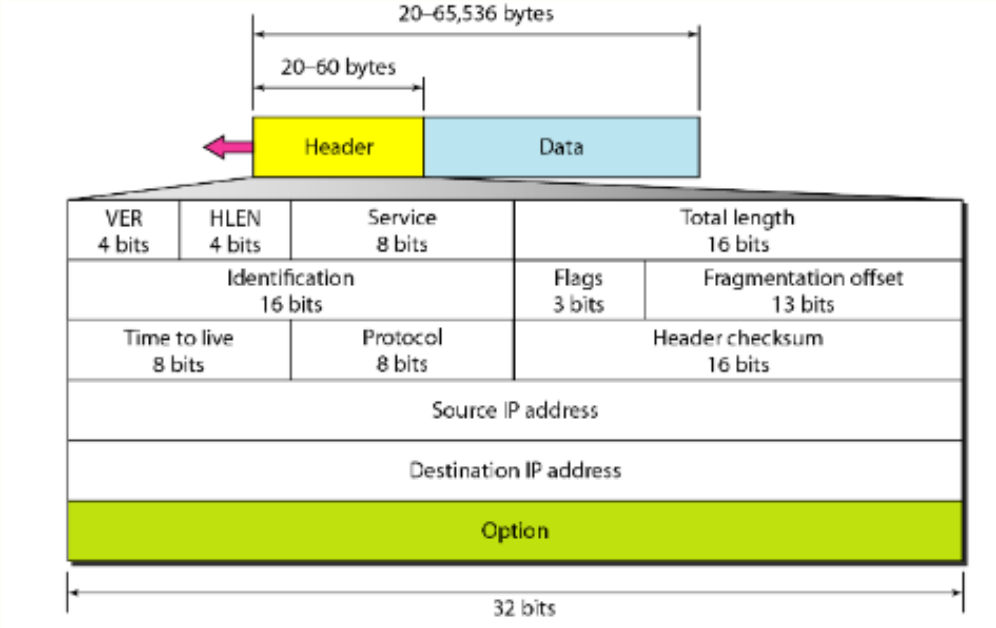
MAC Address	IP Address
Helps to identify the device	Helps to identify the device connectivity on the network.

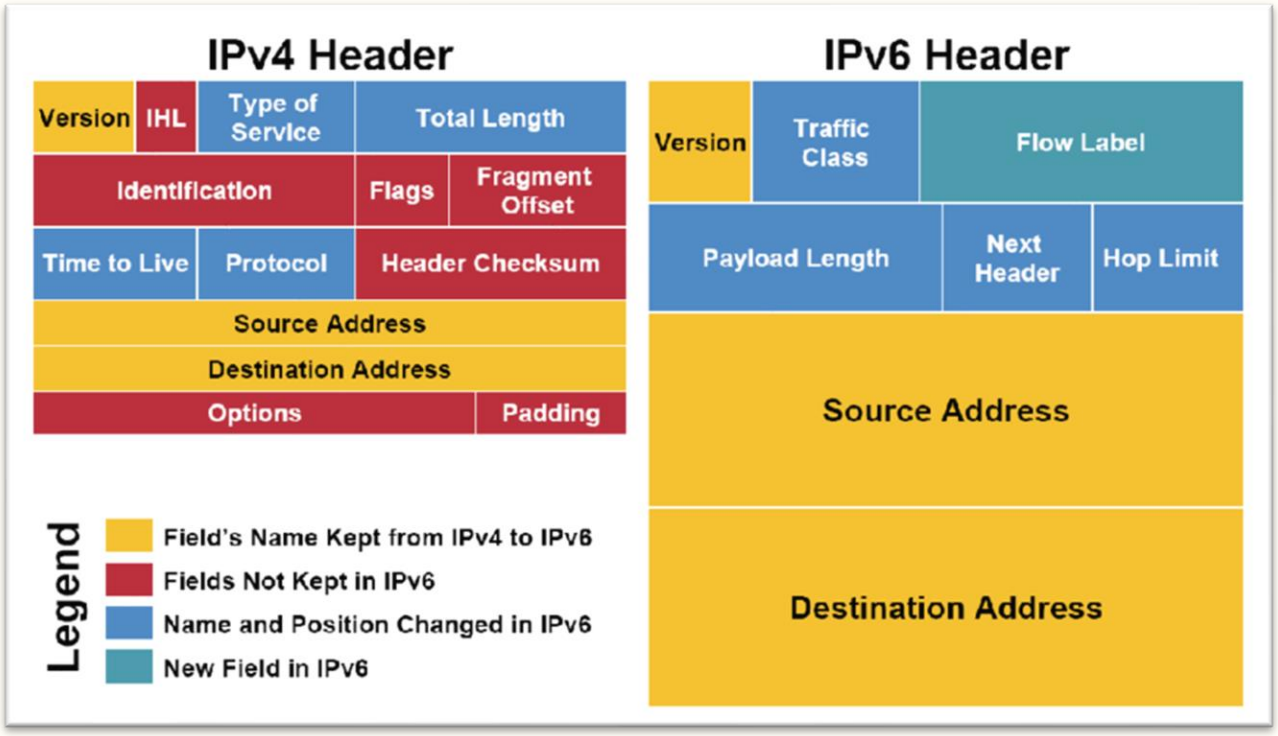
What is an IPv4 address? What are the different classes of IPv4?

An IP address is a 32-bit dynamic address of a node in the network. An IPv4 address has 4 octets of 8-bit each with each number with a value up to 255.

IPv4 classes are differentiated based on the number of hosts it supports on the network. There are five types of IPv4 classes and are based on the first octet of IP addresses which are classified as Class A, B, C, D, or E.

IPv4 Class	IPv4 Start Address	IPv4 End Address	Usage
A	0.0.0.0	127.255.255.255	Used for Large Network
B	128.0.0.0	191.255.255.255	Used for Medium Size Network
C	192.0.0.0	223.255.255.255	Used for Local Area Network
D	224.0.0.0	239.255.255.255	Reserved for Multicasting
E	240.0.0.0	255.255.255.254	Study and R&D





What are Private and Special IP addresses?

Private Address: For each class, there are specific IPs that are reserved specifically for private use only. This IP address cannot be used for devices on the Internet as they are non-routable.

IPv4 Class	Private IPv4 Start Address	Private IPv4 End Address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Special Address: IP Range from 127.0.0.1 to 127.255.255.255 are network testing addresses also known as loopback addresses are the special IP address.

What is IP address, private IP address, public IP address, APIPA?

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

Private IP Address - There are three ranges of IP addresses that have been reserved for IP addresses. They are not valid for use on the internet. If you want to access the internet on these private IPs, you must use a proxy server or NAT server.

Public IP Address - A public IP address is an address taken by the Internet Service Provider which facilitates communication on the internet.

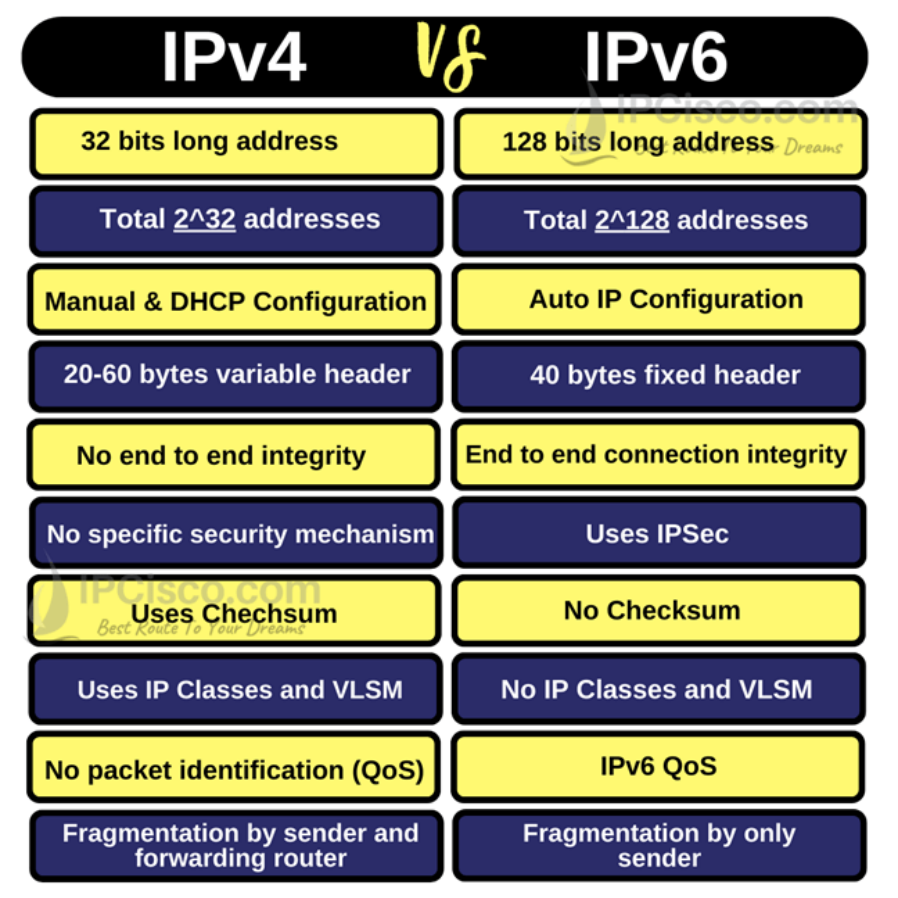
APIPA stands for Automatic Private IP Addressing (APIPA) : It is a feature or characteristic in operating systems (eg. Windows) which enables computers to self-configure an IP address and subnet mask automatically when their DHCP (Dynamic Host Configuration Protocol: A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol) server isn't reachable.

Difference Between Classful Addressing and Classless Addressing

Parameter	Classful Addressing	Classless Addressing
Basics	In Classful addressing IP addresses are allocated according to the classes- A to E.	Classless addressing came to replace the classful addressing and to handle the issue of rapid exhaustion of IP addresses.
Practical	It is less practical.	It is more practical.
Network ID and Host ID	The changes in the Network ID and Host ID depend on the class.	There is no such restriction of class in classless addressing.

VLSM	It does not support the Variable Length Subnet Mask (VLSM).	It supports the Variable Length Subnet Mask (VLSM).
Bandwidth	Classful addressing requires more bandwidth. As a result, it becomes slower and more expensive as compared to classless addressing.	It requires less bandwidth. Thus, fast and less expensive as compared to classful addressing.
CIDR	It does not support Classless Inter-Domain Routing (CIDR).	It supports Classless Inter-Domain Routing (CIDR).
Updates	Regular or periodic updates	Triggered Updates
Troubleshooting and Problem detection	Troubleshooting and problem detection are easy than classless addressing because of the division of network, host and subnet parts in the address.	It is not as easy compared to classful addressing.
Division of Address	• Network • Host • Subnet	• Host • Subnet

Difference Between IPv4 and IPv6



Benefits of IPv6 over IPv4

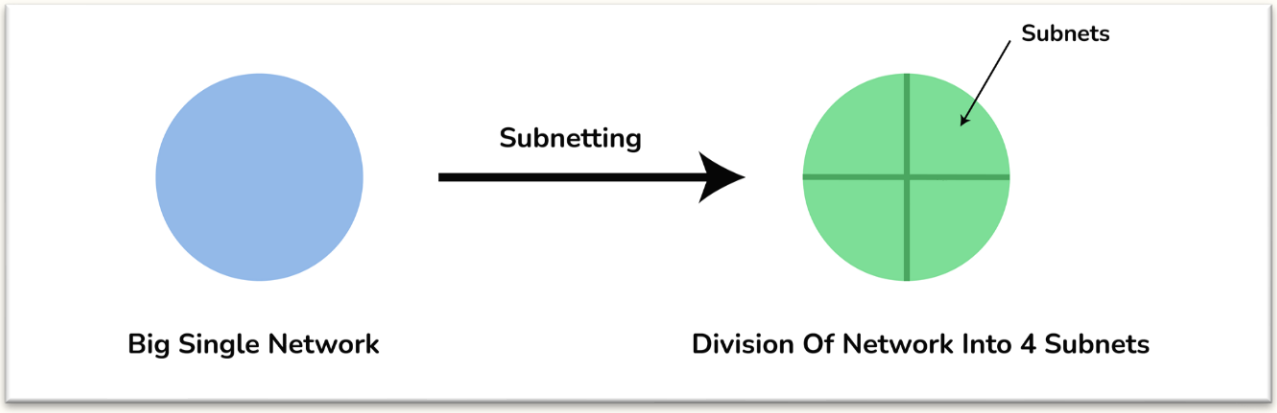
The recent Version of IP IPv6 has a greater advantage over IPv4. Here are some of the mentioned benefits:

- **Larger Address Space:** IPv6 has a greater address space than IPv4, which is required for expanding the IP Connected Devices. IPv6 has 128 bit IP Address rather and IPv4 has a 32-bit Address.
- **Improved Security:** IPv6 has some improved security which is built in with it. IPv6 offers security like Data Authentication, Data Encryption, etc. Here, an Internet Connection is more Secure.
- **Simplified Header Format:** As compared to IPv4, IPv6 has a simpler and more effective header Structure, which is more cost-effective and also increases the speed of Internet Connection.

- **Prioritize:** IPv6 contains stronger and more reliable support for QoS features, which helps in increasing traffic over websites and increases audio and video quality on pages.
- **Improved Support for Mobile Devices:** IPv6 has increased and better support for Mobile Devices. It helps in making quick connections over other Mobile Devices and in a safer way than IPv4.

What is a subnet?

A subnet is a network inside a network achieved by the process called subnetting which helps divide a network into subnets. It is used for getting a higher routing efficiency and enhances the security of the network. It reduces the time to extract the host address from the routing table.



Key differences between Subnetting and Supernetting

Features	Subnetting	Supernetting
Definition	It is a method of dividing a single physical network into numerous smaller logical sub-networks.	It is the inverse of subnetting, in which many networks are integrated into a single network.

Purpose	It is utilized to decrease address depletion	It is utilized to simplify and speeds up the routing process.
Procedure	It transforms host bits into network bits and helps to increase the number of network bits.	It converts network bits to host bits and helps to increase the number of host bits.
Mask bits	Mask bits are relocated to the right of the default mask during subnetting.	Supernetting shifts the mask bits to the left of the normal mask.
Implementation	It is implemented via VLSM and FL techniques.	It is implemented via the CIDR technique.

What do you understand by ping command?

The "ping" is a utility program that allows you to check the connectivity between the network devices. You can ping devices using its IP address or name.

Additional Questions

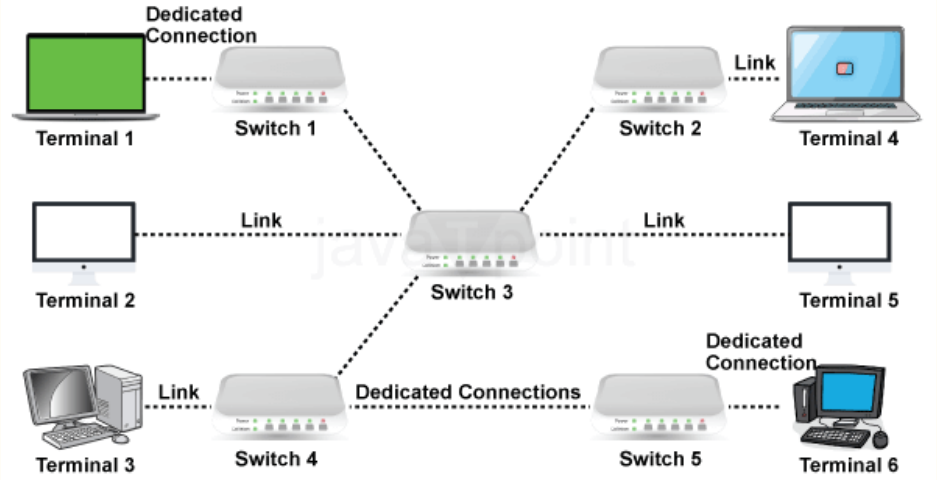
Differentiate between Circuit Switching, Message Switching, and Packet Switching

Introduction

Switched communication networks route data between a number of intermediate nodes as it travels from source to destination. Nodes accomplish data transmission between certain locations on a network via a mechanism called switching.

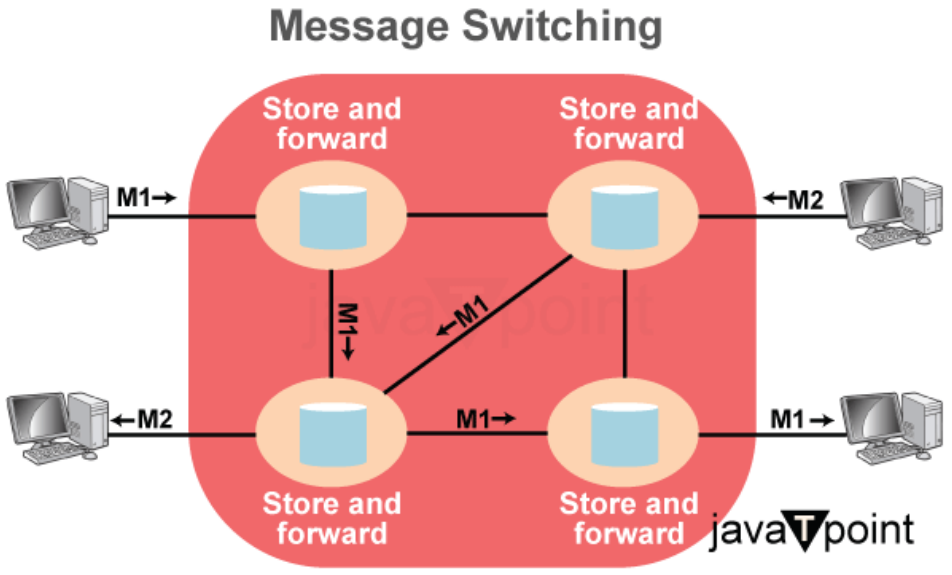
1. Circuit Switching

Circuit Switching establishes a dedicated communication path between two nodes for the duration of the call or session. A continuous, reserved circuit is set up between the sender and receiver, ensuring that the bandwidth is exclusively allocated to this connection whether or not data is being transmitted. This method, exemplified by traditional telephone networks, provides a constant connection with consistent delay. However, it is inefficient when no data is transmitted, and any disruption in the circuit can result in a failed connection.



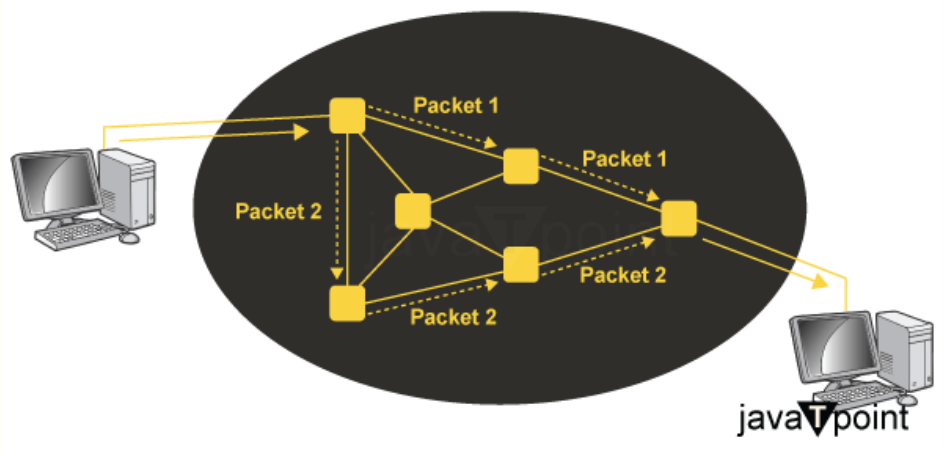
2. Message Switching

Message Switching involves sending data in its entirety as a message through multiple intermediate nodes from the source to the destination. This method uses a store-and-forward approach where each node stores the entire message before forwarding it. There is no direct connection between sender and receiver, and messages are routed hop-by-hop. While message switching makes efficient use of network resources and allows for easy traffic regulation, it can be slow due to storage and forwarding delays, making it unsuitable for real-time applications.



3. **Packet Switching**

Packet Switching divides data into smaller packets that are sent independently through the network. Each packet contains its own header with routing information, and packets are routed individually. There are two main types of packet switching: connection-less, where packets are routed independently and may arrive out of order, and connection-oriented, where packets are sent in sequence along a predetermined route. Packet switching is efficient and adaptable to varying network loads, handling data from multiple sources effectively, though it may lead to packets arriving out of order or experiencing variable delays.



Circuit-Switched Networks	Message-Switched Networks	Packet-Switched Networks
Communication is performed through a dedicated path.	No dedicated path exists.	No dedicated path exists.
Provides real-time or continuous transmission of data.	Too slow for real-time or interactive data transmission.	Provides near real-time data transmission.
No data storing is required.	Messages are stored for later retrieval.	Packets are queued for delivery; they are not stored.
The switch path is established for the entire connection time.	The route is established for each message.	The route is established for each packet.
For small messages, the data transmission time is negligible compared to the time required to setup and tear-down the connection.	The message delivery time can be substantially long.	The packet delivery time is very short.
The connection is blocked if the end-user is busy or not available. Once the connection starts, no blocking may occur.	No message blocking can occur as long as the storage capacity is sufficiently large.	Packet blocking can occur, however, the blocked packets will be retransmitted to the end-user.
As the network load increases, more blocking can occur.	As the load increases, messages on average experience longer delivery delay.	As the load increases, packets on average experience longer queuing delay, although still very short compared to message switching.
The length of transmission is unlimited.	Messages have no theoretical maximum length and can be very long.	Packets have a maximum length.

Difference between Socket and Port?

Both Socket and Port are the terms used in Transport Layer. A port is a logical construct assigned to network processes so that they can be identified within the system. A socket is a combination of port and IP address. Port number can be represented by a single number (example: 1028) on the other hand socket address can be represented by (tcp, hostname,1028). An incoming packet has a port number which is used to identify the process that needs to consume the packet. The lowest numbered 1024 port numbers are used for the most commonly used services. These ports are called the well-known ports. Higher-numbered ports are available for general use by applications and are known as ephemeral ports.

Differences Between Virtual Circuits and Datagram Networks

Computer networks that provide connection-oriented services are called Virtual Circuits while those providing connection-less services are called Datagram networks. For prior knowledge, the

Internet that we use is based on a Datagram network (connection-less) at the network level as all packets from a source to a destination do not follow the same path.

Criteria	Virtual Circuit Networks	Datagram Networks
Connection Establishment	Prior to data transmission, a connection is established between sender and receiver.	No connection setup is required.
Routing	Routing decisions are made once during connection setup and remain fixed throughout the duration of the connection.	Routing decisions are made independently for each packet and can vary based on network conditions.
Flow Control	Uses explicit flow control, where the sender adjusts its rate of transmission based on feedback from the receiver.	Uses implicit flow control, where the sender assumes a certain level of available bandwidth and sends packets accordingly.
Congestion Control	Uses end-to-end congestion control, where the sender adjusts its rate of transmission based on feedback from the network.	Uses network-assisted congestion control, where routers monitor network conditions and may drop packets or send congestion signals to the sender.
Error Control	Provides reliable delivery of packets by detecting and retransmitting lost or corrupted packets.	Provides unreliable delivery of packets and does not guarantee delivery or correctness.
Overhead	Requires less overhead per packet because connection	Requires more overhead per packet because each packet contains information about its

	setup and state maintenance are done only once.	destination address and other routing information.
Example Protocol	ATM, Frame Relay	IP (Internet Protocol)

What is choke packets

Choke Packets are used to manage network congestion by signaling senders to reduce their data transmission rate. For example, if a router in a busy network detects that its buffer is nearly full, it might send a choke packet to connected devices. This packet instructs the sender to slow down its data transmission, thereby helping to alleviate congestion and prevent packet loss.

What is warning bit in packet

Warning Bit is a flag in the packet header that indicates potential congestion. For instance, when a router detects increasing traffic levels that might lead to congestion, it sets the warning bit in packets it forwards. This serves as a preemptive alert to the sender, prompting them to lower their sending rate to avoid exacerbating the congestion issue.

What is congestion

Congestion occurs when network traffic exceeds the available capacity, leading to delays and packet loss. An example is during peak hours on a busy network, where too many users are accessing the internet simultaneously. This excessive demand can cause routers to become overwhelmed, resulting in slower speeds and higher rates of packet loss. To manage this, techniques such as choke packets and warning bits are used to help regulate traffic and maintain network performance.

What is Tunneling?

Tunneling is a networking technique that involves encapsulating data packets from one protocol within packets of another protocol to facilitate secure and efficient transmission across different networks. By wrapping the original data in an outer packet, tunneling allows data to traverse networks that might not natively support the original protocol. At the destination, the outer packet is removed to reveal the original data. This method is commonly used in technologies like VPNs (Virtual Private Networks), where data is securely transmitted over the internet as if it were part of a private network, ensuring privacy and enabling access to resources.

What is Telnet?

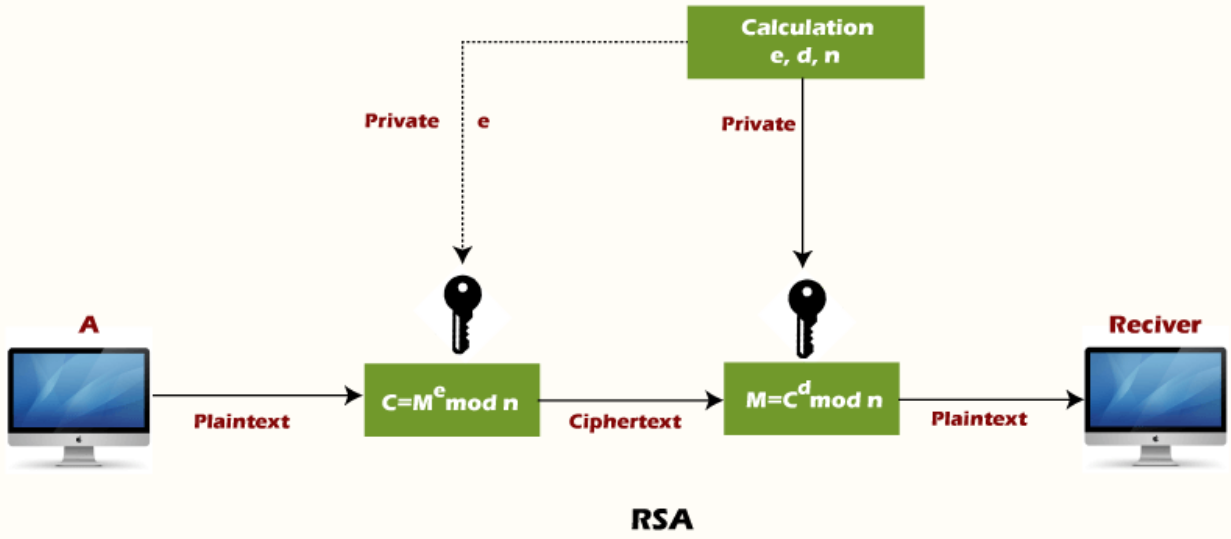
Telnet is a network protocol used to virtually access a computer and provide a two-way, collaborative and text-based communication channel between two machines.
It follows a user command TCP/IP networking protocol that creates remote sessions. On the web, HTTP and File Transfer Protocol (FTP) enable users to request specific files from remote computers. With Telnet, users can log on as a regular user with privileges that allow them to access the specific applications and data on that computer.

What is RSA Algorithm?

RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone and the Private key is kept private.

An example of asymmetric cryptography:

1. A client (for example browser) sends its public key to the server and requests some data.
2. The server encrypts the data using the client's public key and sends the encrypted data.
3. The client receives this data and decrypts it.



RSA

RSA algorithm uses the following procedure to generate public and private keys:

- Select two large prime numbers, p and **q**.
- Multiply these numbers to find **n = p x q,** where **n** is called the modulus for encryption and decryption.
- Choose a number **e** less than **n**, such that n is relatively prime to **(p - 1) x (q -1).** It means that **e** and **(p - 1) x (q - 1)** have no common factor except 1. Choose "e" such that 1<e < φ (n), e is prime to φ (n),

  gcd (e,d(n)) =1
- If **n = p x q,** then the public key is <e, n>. A plaintext message **m** is encrypted using public key <e, n>. To find ciphertext from the plain text following formula is used to get ciphertext C.

  $C = m^e \bmod n$

  Here**, m** must be less than **n**. A larger message (>n) is treated as a concatenation of messages, each of which is encrypted separately.
- To determine the private key, we use the following formula to calculate the d such that:

  $D_e \bmod \{(p - 1) \times (q - 1)\} = 1$

  Or

  $D_e \bmod \varphi(n) = 1$
- The private key is <d, n>. A ciphertext message **c** is decrypted using private key <d, n>. To calculate plain text **m** from the ciphertext c following formula is used to get plain text

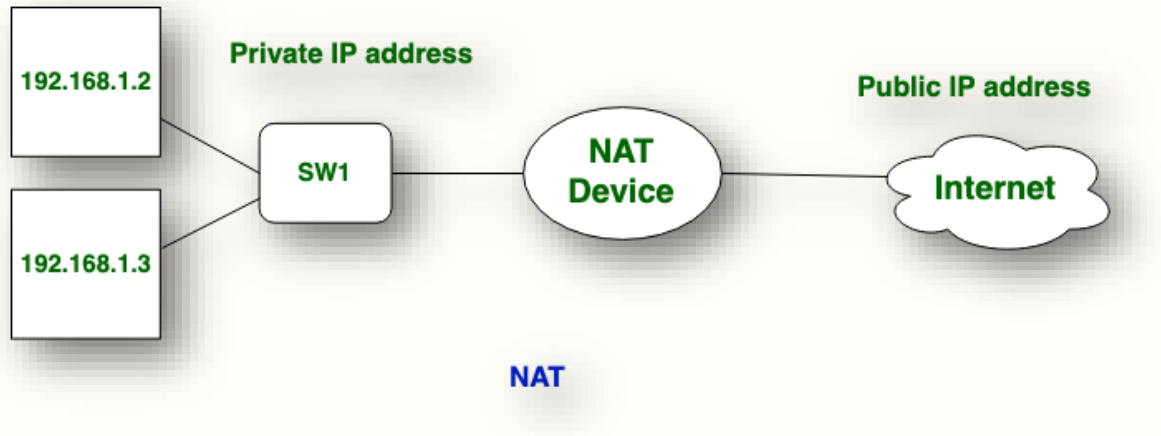
m.

$m = c^d \bmod n$

What are PAT and NAT? What are their differences?

What is Network Address Translation (NAT)?

It is a Private IP address or local address that is translated into the public IP address. NAT is used to slow down the rate of decrease of the available IP address by translating the local IP or Private IP address into a global or public IP address. NAT can be a one-to-one relation or many-to-one relation.



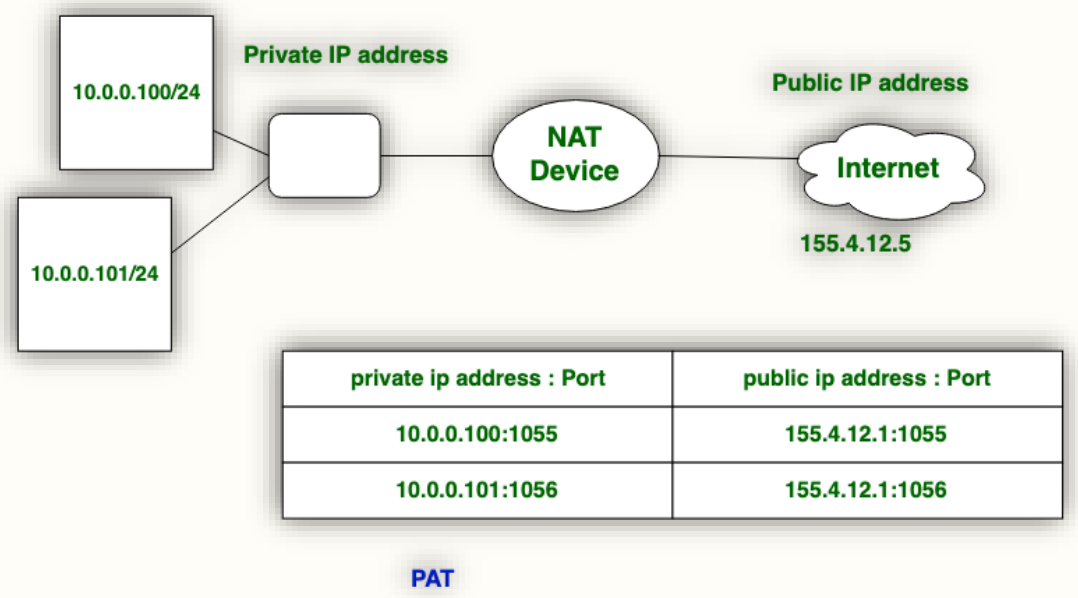
Ex: Consider a home network with three devices: a computer, a smartphone, and a smart TV. Without NAT, each of these devices would need to have a unique public IP address to connect to the internet. However, with NAT, all of these devices can share a single public IP address and communicate with the internet by using their private IP addresses. When one of the devices sends a request to the internet, NAT translates the private IP address of the device into the public IP address of the network and sends the request over the internet.

What is Port Address Translation (PAT)?

In Port Address Translation (PAT), Private IP address are translated into the public IP address through port numbers. PAT also uses IPv4 address but with port number. It have two types:

1. Static

2. Overloaded PAT



Ex: Consider a home network with three devices: a computer, a smartphone, and a smart TV. Without PAT, each of these devices would need to have a unique public IP address to connect to the internet. However, with PAT, all of these devices can share a single public IP address and communicate with the internet by using unique port numbers. When the computer sends a request to the internet, PAT assigns it a unique port number and translates the private IP address of the computer into the public IP address of the network. The destination server on the internet receives the request and responds to the unique port number, allowing the computer to receive the response.

References:

[1] https://www.javatpoint.com/networking-interview-questions

[2] https://www.geeksforgeeks.org/networking-interview-questions

[3] https://www.shiksha.com/online-courses/articles/networking-interview-questions-answers/

[4] https://www.interviewbit.com/networking-interview-questions/

[5] https://chatgpt.com/