INTERVIEW QUESTIONS

“Computer Network”

2024…

By

Priyush Khobragade

Network:

An inter-connection of multiple devices known as host, that are connected using multiple paths for the purpose of sending/receiving data.

Basic Terms:

Client: A client is a computer or device that requests services or resources from a server. In a network, clients communicate with servers to access data, applications, or other network services.

Host: A host is any device that connects to a network and has an IP address, allowing it to communicate with other devices on the network. This can include computers, servers, printers, and routers.

Bandwidth: Bandwidth refers to the maximum rate of data transfer across a given path. It is usually measured in bits per second (bps) and determines how much data can be sent or received at a time.

Jitter: Jitter is the variation in the time between packets arriving, caused by network congestion, timing drift, or route changes. High jitter can lead to poor quality in real-time communications, such as VoIP or video conferencing.

Packet: A packet is a small unit of data transmitted over a network. It contains the data being sent as well as control information, such as the destination address, source address, and error-checking information.

Frame: A frame is a data packet at the data link layer of the OSI model. It includes the header and trailer needed for data link layer communication, encapsulating the packet for transmission.

Local Host: The local host refers to the computer or device you are currently using to access network resources. It is often used in the context of network configuration and diagnostics.

Bit Rate: Bit rate is the number of bits transmitted per unit of time, typically measured in bits per second (bps). It is a measure of the speed of data transfer.

Attenuation: Attenuation is the reduction in signal strength as it travels through a medium, such as a cable or wireless channel. High attenuation can result in weaker signals and reduced communication quality.

Distortion: Distortion refers to any change in the signal that alters the original waveform or data. It can be caused by various factors, including interference, noise, and transmission medium characteristics, leading to errors and degraded performance.

What is the Web?

The Web, short for the World Wide Web (WWW), is a system of interlinked hypertext documents and multimedia content that are accessed via the internet. The Web uses the Hypertext Transfer Protocol (HTTP) to transmit data and allows users to view and interact with web pages through web browsers. Key components of the Web include:

- **Web Pages**: Documents written in HTML (HyperText Markup Language) that can include text, images, videos, and links to other web pages.
- **Web Browsers:** Software applications (like Chrome, Firefox, Safari) that retrieve, interpret, and display web pages.
- **Web Servers**: Computers that store, process, and deliver web pages to users upon request.

Difference Between Web and Internet:

Aspect	Internet	Web
Definition	Global network of interconnected computer networks	System of interlinked hypertext documents accessed via the Internet
Protocols	Uses TCP/IP and other protocols	Primarily uses HTTP/HTTPS
Components	Includes routers, switches, and various types of networks	Includes web pages, web browsers, and web servers
Services	Email, FTP, VoIP, remote access, etc.	Web browsing (accessing and navigating web pages)
Scope	Infrastructure supporting multiple services	One specific service running on the Internet
Access	Can be accessed via various applications	Accessed through web browsers

👇Types of Transmission Media:

Transmission media are the physical pathways that connect computers, other devices, and people on a network. They can be categorized into two main types: guided (wired) media and unguided (wireless) media. Here's a detailed look at each type:

Guided (Wired) Transmission Media

Twisted Pair Cable:

- **Description**: Consists of pairs of insulated copper wires twisted together.
- **Types**:

  Unshielded Twisted Pair (UTP): Commonly used in Ethernet networks and telephone systems. It lacks shielding to protect against electromagnetic interference (EMI).

  Shielded Twisted Pair (STP): Includes a shielding layer to provide better protection against EMI. Used in environments with higher interference levels.

- **Advantages**: Cost-effective, easy to install and manage.
- **Disadvantages**: Limited bandwidth and distance compared to other media.

Coaxial Cable:

- **Description**: Composed of a central conductor wire, surrounded by an insulating layer, a metallic shield, and an outer insulating layer.
- **Uses**: Cable television, internet connections, and other broadband systems.
- **Advantages**: Higher bandwidth than twisted pair cables, better shielding against EMI.
- **Disadvantages**: Bulkier and more expensive than twisted pair cables, more difficult to install.

Fiber Optic Cable:

- **Description**: Uses light signals to transmit data through thin strands of glass or plastic fibers.
- **Types**:

  Single-mode Fiber: Designed for long-distance communication using a single light mode.

  Multi-mode Fiber: Suitable for shorter distances with multiple light modes.

- **Advantages**: Extremely high bandwidth, very low signal attenuation, immune to electromagnetic interference.
- **Disadvantages**: More expensive than copper cables, requires specialized equipment for installation and repair.

Unguided (Wireless) Transmission Media

Radio Waves:

- **Description**: Electromagnetic waves used for wireless communication over varying distances.
- **Uses**: AM/FM radio, television broadcasts, and wireless networking (Wi-Fi).
- **Advantages**: Good for long-range communication, does not require line-of-sight.
- **Disadvantages**: Susceptible to interference and signal degradation.

***Microwaves**:*

- **Description**: Electromagnetic waves with higher frequencies than radio waves, requiring line-of-sight transmission.
- **Types**:

  Terrestrial Microwaves: Used for point-to-point communication on the earth's surface.

  Satellite Microwaves: Used for long-distance communication via satellites.

- **Advantages**: High bandwidth, suitable for long-distance and point-to-point communication.
- **Disadvantages**: Requires line-of-sight, can be affected by weather conditions.

Infrared (IR):

- **Description**: Uses infrared light for short-range communication.
- **Uses**: Remote controls, short-range communication between devices (e.g., laptops, PDAs).
- **Advantages**: High security, does not penetrate walls, reducing interference.
- **Disadvantages**: Short-range, requires line-of-sight.

Bluetooth:

- **Description**: Wireless technology standard for exchanging data over short distances using UHF radio waves.
- **Uses**: Connecting peripherals (e.g., keyboards, mice, headphones) to computers and mobile devices.
- **Advantages**: Low power consumption, easy to set up, supports multiple devices.
- **Disadvantages**: Limited range (typically up to 100 meters), moderate data transfer rates.

Computer Network Devices:

Computer network devices, also known as networking hardware, are physical devices required for communication and interaction between devices on a computer network. Here's a detailed overview of the key computer network devices:

1. Router

- **Function**: Connects multiple networks and directs data packets between them.
- **Usage**: Commonly used to connect local area networks (LANs) to wide area networks (WANs) like the Internet.
- **Features**: Routes data based on IP addresses, supports NAT (Network Address Translation), often includes firewall capabilities.

2. Switch

- **Function**: Connects devices within a single network (usually a LAN) and uses MAC addresses to forward data to the correct destination.
- **Usage**: Central device in most Ethernet networks, creating a network segment and reducing collisions.
- **Features**: Can be unmanaged (simple and plug-and-play) or managed (offers advanced features like VLAN support and traffic management).

3. Hub

- **Function**: Basic networking device that connects multiple Ethernet devices, making them act as a single network segment.
- **Usage**: Used in small networks for connecting devices; largely replaced by switches.
- **Features**: Broadcasts incoming data packets to all ports, leading to potential collisions and inefficiency.

4. Modem

- **Function**: Modulates and demodulates signals for data transmission over telephone lines, cable systems, or satellite links.
- **Usage**: Connects home or office networks to the Internet via ISPs (Internet Service Providers).
- **Types**: DSL modems, cable modems, fiber-optic modems, and satellite modems.

5. Access Point (AP)

- **Function**: Provides wireless connectivity to devices within a network by connecting to a wired network.
- **Usage**: Used in Wi-Fi networks to extend wireless coverage.
- **Features**: Can support multiple wireless standards (e.g., 802.11ac, 802.11ax), offer security features like WPA3.

6. Bridge

- **Function**: Connects and filters traffic between two or more network segments at the data link layer (Layer 2).
- **Usage**: Used to reduce network traffic by dividing it into segments and controlling data flow between them.
- **Types**: Simple bridges, multiport bridges, and wireless bridges.

7. Gateway

- **Function**: Acts as a "gateway" between different networks, often converting protocols.
- **Usage**: Connects networks using different protocols, such as a LAN to the Internet.
- **Features**: Can include router and firewall functionalities, supports protocol conversion.

8. Repeater

- **Function**: Amplifies or regenerates signals to extend the distance over which data can travel.
- **Usage**: Used in long cable runs to prevent signal degradation in both wired and wireless networks.
- **Types**: Wired repeaters, wireless repeaters.

9. Firewall

- **Function**: Monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- **Usage**: Provides network security by blocking unauthorized access while permitting outward communication.
- **Types**: Hardware firewalls, software firewalls, and combined hardware/software solutions.

10. Network Interface Card (NIC)

- **Function**: Provides the physical interface for network connectivity in a device.
- **Usage**: Installed in devices to connect them to a network (wired or wireless).
- **Features**: Can be integrated on the motherboard or added as an expansion card; supports various speeds and standards.

11. Load Balancer

- **Function**: Distributes network or application traffic across multiple servers to ensure reliability and performance.
- **Usage**: Used in data centers and large network setups to balance the load and prevent any single server from being overwhelmed.
- **Types**: Hardware load balancers, software load balancers.

👉What is the network topology?

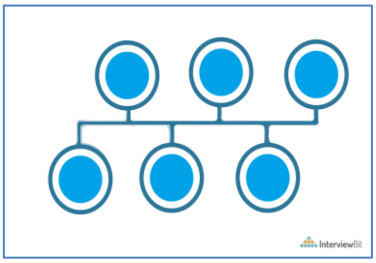
Network topology is a physical layout of the network, connecting the different nodes using the links. It depicts the connectivity between the computers, devices, cables, etc.

Define different types of network topology

The different types of network topology are given below:

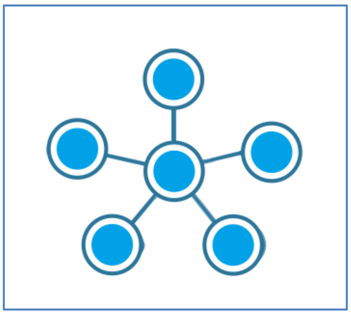
Bus Topology:

- 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.



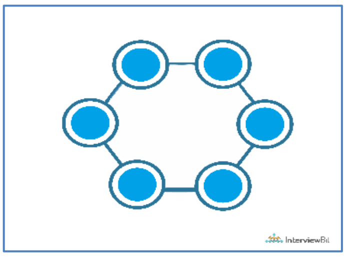
Star Topology:

- 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 are damaged, it will damage the whole network
- It is used very rarely as it is expensive and hard to install and manage

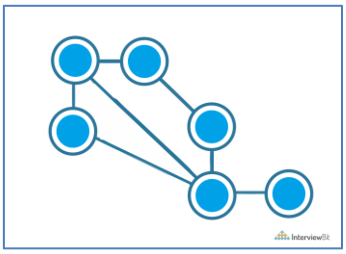


Mesh Topology:

- 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.

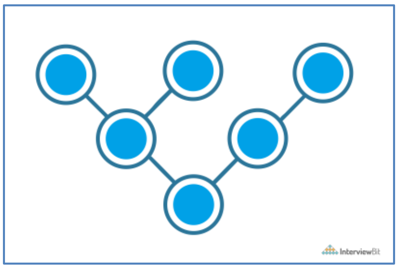
Tree Topology:

- 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 drawback of a particular topology and helps to pick the strengths from other.



👉Different Types of Networks:

- Networks can be divided on the basis of area of distribution. For example:

1. ● **PAN** (Personal Area Network): Its range limit is up to 10 meters. It is created for personal use. Generally, personal devices are connected to this network. For example computers, telephones, fax, printers, etc.
2. ● **LAN (Local Area Network**): It is used for a small geographical location like office, hospital, school, etc.
3. ● **HAN (House Area Network):** It is actually a LAN that is used within a house and used to connect homely devices like personal computers, phones, printers, etc.
4. ● **CAN (Campus Area Network):** It is a connection of devices within a campus area which links to other departments of the organization within the same campus.
5. ● **MAN (Metropolitan Area Network**): It is used to connect the devices which span to large cities like metropolitan cities over a wide geographical area.
6. ● **WAN (Wide Area Network):** It is used over a wide geographical location that may range to connect cities and countries.
7. ● **GAN (Global Area Network**): It uses satellites to connect devices over the global area.

👉VPN:

VPN or the Virtual Private 👉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.

Advantages of VPN:

- VPN is used to connect offices in different geographical locations remotely
- VPN encrypts the internet traffic and disguises the online identity
- VPN can be also used to bypass geographical locations.

👉What are the different types of VPN?

Few types of VPN are:

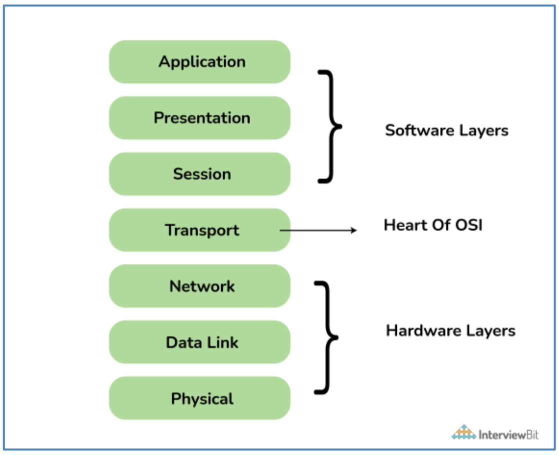
- **Access VPN:** Access VPN is used to provide connectivity to remote mobile users and telecommuters. It serves as an alternative to dial-up connections or ISDN (Integrated Services Digital Network) connections. It is a low-cost solution and provides a wide range of connectivity.
- **Site-to-Site VPN:**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

👉OSI Reference Model:

OSI stands for Open Systems Interconnection, where open stands to say non-proprietary. It is a 7-layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe. The OSI reference model was developed by ISO – 'International Organization for Standardization ', in the year 1984.

The OSI model provides a theoretical foundation for understanding network communication. However, it is usually not directly implemented in its entirety in real-world networking hardware or software. Instead, specific protocols and technologies are often designed based on the principles outlined in the OSI model to facilitate efficient data transmission and networking operations.

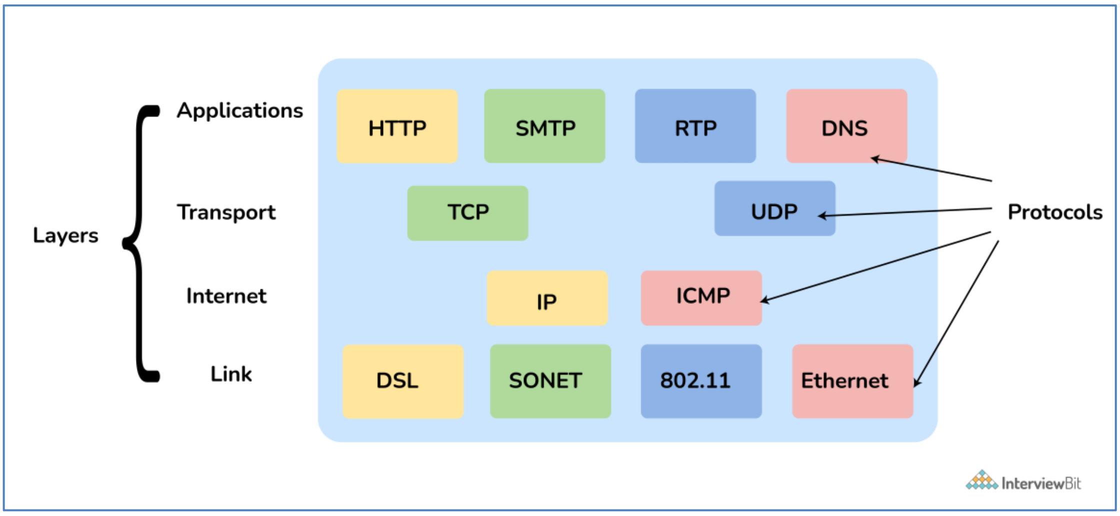
Layer	**Unit Exchanged**	**Description**
Physical	Bit	• It is concerned with transmitting raw bits over a communication channel. • Chooses which type of transmission mode is to be selected for the transmission. The available transmission modes are Simplex, Half Duplex and Full Duplex.,
Data Link	Frame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



👉TCP/IP Reference Model

It is a compressed version of the OSI model with only 4 layers. It was developed by the US Department of Defence (DoD) in the 1980s. The name of this model is based on 2 standard protocols used i.e. TCP (Transmission Control Protocol) and IP (Internet Protocol).

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.



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

👉Ethernet:

Ethernet is a widely used technology for local area networks (LANs). It defines the physical and data link layers of the OSI model, providing guidelines for how data should be transmitted over a network. Ethernet uses a protocol to control how devices on the same network segment communicate and share data.

- **Components**: Cables (e.g., Cat5, Cat6), network interface cards (NICs), switches, and routers.
- **Standards**: Defined by IEEE 802.3, covering various speeds and media types (e.g., 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps).

👉Switch & Its Types:

Switch: A switch is a network device that connects multiple devices within a LAN and uses MAC addresses to forward data to the correct destination. Unlike hubs, which broadcast data to all ports, switches send data only to the device it is intended for, reducing collisions and improving efficiency.

Types of Switches:

Unmanaged Switch:

- Function: Basic plug-and-play switches with no configuration options.
- Usage: Small home networks or simple office setups.
- Advantages: Easy to use, cost-effective.

Managed Switch:

- Function: Offers configuration options, monitoring, and management features.
- Usage: Enterprise environments where network management and performance are critical.
- Advantages: Supports VLANs, quality of service (QoS), SNMP, and more.

Smart Switch:

- Function: Offers some manageability with a web interface, but less complex than fully managed switches.
- Usage: Small to medium-sized businesses needing some advanced features without the complexity.
- Advantages: Balance between unmanaged and managed switches, cost-effective with reasonable features.

Layer 3 Switch:

- Function: Combines the capabilities of switches and routers, providing routing functions within a network.
- Usage: Large enterprise networks requiring advanced routing and switching.
- Advantages: Supports routing protocols, enhances network efficiency by reducing traffic on the network backbone.

Virtual LAN (VLAN):

Virtual LAN (VLAN): A VLAN is a logical subdivision of a physical network, allowing administrators to segment networks into different broadcast domains, even if the devices are physically on the same network switch. This segmentation improves security, reduces broadcast traffic, and enhances performance.

Usage: Commonly used in enterprise networks to separate different types of traffic (e.g., management, voice, data).

Benefits:

- Security: Isolates sensitive data from general network traffic.
- Performance: Reduces broadcast traffic and increases efficiency.
- Flexibility: Simplifies network management and reduces the need for physical reconfiguration.

Basics of Wi-Fi

Wi-Fi: Wi-Fi (Wireless Fidelity) is a technology that allows devices to connect to a network wirelessly using radio waves. It is based on the IEEE 802.11 standards and is commonly used for local area networking and Internet access.

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.

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

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

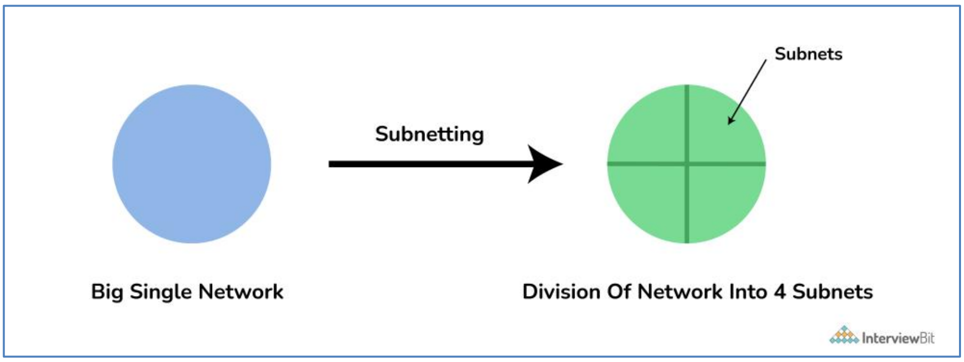
Ipv4	IPv6
IPv4 has 32-bit address length	IPv6 has 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end connection integrity is Unachievable	In IPv6 end to end connection integrity is Achievable
It can generate 4.29x109 address space	Address space of IPv6 is quite large it can produce 3.4x1038 address space
Security feature is dependent on application	IPSEC is inbuilt security feature in the IPv6 protocol
Address representation of IPv4 in decimal	Address Representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation performed only by sender
In IPv4 Packet flow identification is not available	In IPv6 packetflow identification are Available and uses flow label field in the header
In IPv4 checksumfield is available	In IPv6 checksumfield is not available
It has broadcast Message Transmission Scheme	In IPv6 multicast and any cast message transmission scheme is available
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided

Difference between Private and Public IP address:

Private	Public
Scope is local.	Scope is global.
It is used to communicate within the network.	It is used to communicate outside the network.
Private IP addresses of the systems connected in a network differ in a uniform manner.	Public IP may differ in uniform or non-uniform manner.
It works only in LAN.	It is used to get internet service.
It is used to load network operating system.	It is controlled by ISP.
It is available in free of cost.	It is not free of cost.
Private IP can be known by entering “ipconfig” on command prompt.	Public IP can be known by searching “what is my ip” on google.

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.



Comparison	Li-Fi	Wi-Fi
Full form	It stands for Light Fidelity.	It stands for Wireless Fidelity.
Invented/Coined	Coined by Prof. Harald Haas in 2011.	By NCR corporation in 1991.
Operation	Using LED bulbs, it uses light to communicate data.	It transmits data using radio waves using wifi router.
Technology	Present IrDA compliant devices	WLAN 802.11/b/g/n/ac/d standard compliant devices
Data Transfer Speed	About 1 Gbps	Ranges from 150Mbps to maximum of 2Gbps
Standard	IEEE 802.15.7	IEEE 802.11
Privacy	Light is blocked by the walls hence provide more secure data transfer.	Walls cannot block radio waves so we need to employ more techniques to achieve secure data transfer.
Bandwidth	Availability of unlimited bandwidth.	Availability of limited bandwidth.
Frequency of operation	10,000 times the radio’s frequency spectrum	2.4Ghz, 4.9Ghz and 5Ghz
Coverage Distance	About 10 meters	About 32 meters(vary based on transmit power and antenna type)

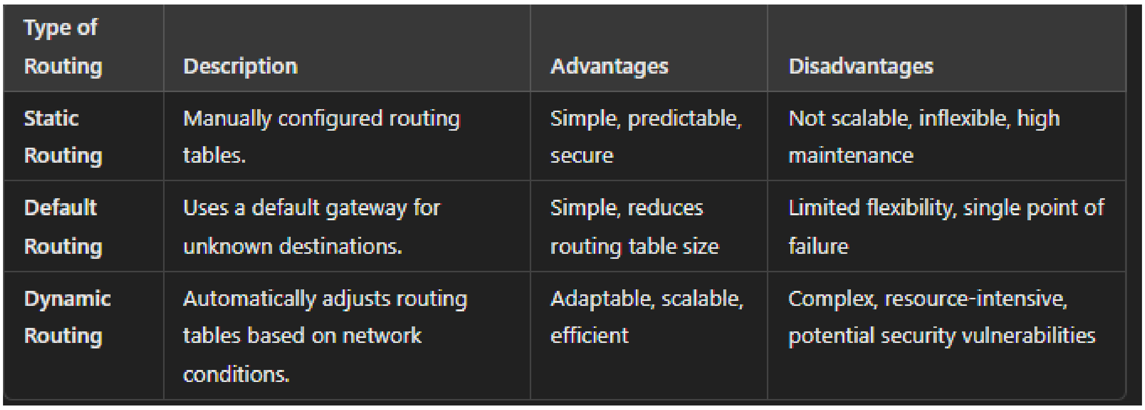
MAC Address	IP Address
Media Access Control Address	Internet Protocol Address
6 or 8-byte hexadecimal number	4 (IPv4) or 16 (IPv6) Byte address
It is embedded with NIC	It is obtained from the network
Physical Address	Logical Address
Operates at Data Link Layer	Operates at Network Layer.
Helps to identify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

What is NAT (Network Address Translation), and how does it facilitate private IP addresses?

NAT is a technique that translates private IP addresses used within a local network to a single public IP address assigned by the Internet Service Provider (ISP). This allows multiple devices with private IP addresses to access the internet using a single public IP.

Routing

Routing is the process of selecting paths in a network along which to send network traffic. There are several types of routing methods used in computer networks, including static routing, default routing, and dynamic routing. Here's a detailed overview of each type:



Type of Routing	Description	Advantages	Disadvantages
Static Routing	Manually configured routing tables.	Simple, predictable, secure	Not scalable, inflexible, high maintenance
Default Routing	Uses a default gateway for unknown destinations.	Simple, reduces routing table size	Limited flexibility, single point of failure
Dynamic Routing	Automatically adjusts routing tables based on network conditions.	Adaptable, scalable, efficient	Complex, resource-intensive, potential security vulnerabilities

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.

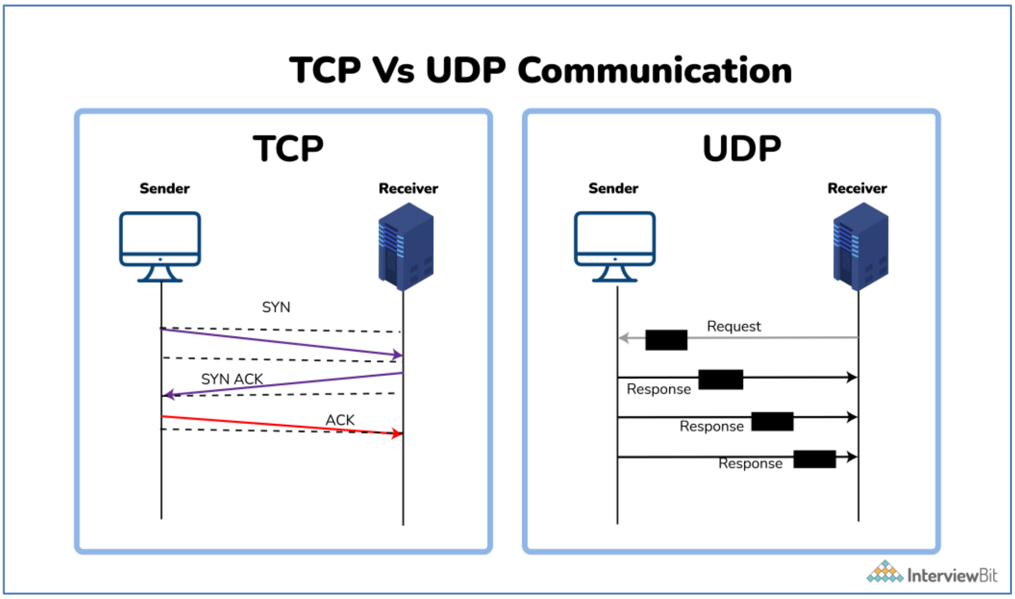
2. What is the UDP protocol?

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

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

👉**TCP 3-Way Handshake Process:**

- **Step 1 (SYN)**: In the first step, client wants to establish a connection with server, so it sends a segment with SYN(Synchronize Sequence Number) which informs server that 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 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 server and they both establish a reliable connection with which they will start eh actual data transfer.



Error control in Transmission Control Protocol (TCP) is a fundamental aspect of ensuring reliable data transmission over networks. TCP employs several mechanisms to detect and correct errors, ensuring that data is delivered accurately and in the correct sequence. Here are the key components of error control in TCP:

1. Checksums

- **Purpose**: Detect errors in transmitted segments.
- **Mechanism**: Each segment includes a checksum field, which is a value calculated from the segment's data and header. The receiver calculates the checksum from the received segment and compares it with the transmitted checksum. If they don't match, an error is detected, and the segment is discarded.

2. Acknowledgments (ACKs)

- **Purpose**: Confirm successful receipt of data segments.
- **Mechanism**: The receiver sends an acknowledgment (ACK) back to the sender for successfully received segments. If the sender does not receive an ACK within a certain timeframe, it assumes the segment was lost or corrupted and retransmits it.

3. Sequence Numbers

- **Purpose**: Ensure data is delivered in the correct order and detect missing or duplicate segments.
- **Mechanism**: Each byte of data is assigned a unique sequence number. The receiver uses these sequence numbers to reorder segments if they arrive out of order and to detect any missing segments.

4. Retransmissions

- **Purpose**: Recover from lost or corrupted segments.
- **Mechanism**: If an ACK is not received within a specified timeout period, the sender retransmits the segment. TCP uses algorithms like the retransmission timeout (RTO) to dynamically adjust the timeout period based on network conditions.

5. Cumulative Acknowledgments

- **Purpose**: Simplify acknowledgment process and improve efficiency.
- **Mechanism**: Instead of acknowledging each segment individually, TCP can acknowledge all bytes up to a certain sequence number, indicating that all prior bytes have been received correctly.

6. Selective Acknowledgments (SACK)

- **Purpose**: Improve performance in the presence of multiple segment losses.
- **Mechanism**: When enabled, SACK allows the receiver to inform the sender about all segments that have been received successfully, enabling the sender to retransmit only the missing segments.

7. Flow Control

- **Purpose**: Prevent the sender from overwhelming the receiver.
- **Mechanism**: TCP uses a sliding window mechanism where the receiver advertises a window size indicating how much data it can accept. The sender must respect this window size to avoid overwhelming the receiver's buffer.

8. Congestion Control

- **Purpose**: Prevent network congestion.
- **Mechanism**: TCP employs various algorithms (like slow start, congestion avoidance, fast retransmit, and fast recovery) to adjust the rate of data transmission based on network congestion signals. This helps in minimizing segment loss due to congestion.

9. Duplicate ACKs and Fast Retransmit

- **Purpose**: Quickly recover from lost segments without waiting for a timeout.
- **Mechanism**: If the sender receives a certain number of duplicate ACKs for the same segment, it assumes the next segment is lost and retransmits it immediately (fast retransmit), without waiting for the retransmission timeout to expire.

Application:

The application layer is the topmost layer in the OSI model and the TCP/IP protocol suite. It provides protocols and services for end-user applications to interact over a network. Here are some of the key protocols operating in the application layer:

HTTP/HTTPS (Hypertext Transfer Protocol / Hypertext Transfer Protocol Secure):

- Purpose: Used for transferring web pages on the internet.
- HTTP: Unsecured communication.
- HTTPS: Secure communication using SSL/TLS encryption.

FTP/SFTP (File Transfer Protocol / Secure File Transfer Protocol)

- FTP: Transfers files between a client and server.
- SFTP: Secure version of FTP, uses SSH for encryption.

SMTP (Simple Mail Transfer Protocol)

- Purpose: Transfers email between mail servers.
- Common Use: Email delivery from a client to a server or between servers.

IMAP/POP3 (Internet Message Access Protocol / Post Office Protocol version 3)

- IMAP: Allows users to access and manage their email on a server.
- POP3: Downloads emails from the server to the client.

DNS (Domain Name System)

- Purpose: Translates domain names into IP addresses.
- Function: Helps locate and address internet resources using human-readable names.

DHCP (Dynamic Host Configuration Protocol)

- Purpose: Automatically assigns IP addresses to devices on a network.
- Function: Simplifies IP address management.

Telnet

- Purpose: Provides a command-line interface for communication with a remote device.
- Security: Lacks encryption, often replaced by SSH for secure connections.

SSH (Secure Shell):

- Purpose: Provides secure remote login and other secure network services over an unsecured network.
- Function: Encrypted command-line interface for managing network devices.

SNMP (Simple Network Management Protocol)

- Purpose: Manages and monitors network devices.
- Function: Collects and organizes information about managed devices on IP networks.

LDAP (Lightweight Directory Access Protocol)

- Purpose: Accesses and maintains distributed directory information services.
- Function: Used for authentication and authorization, often in enterprise environments.

NTP (Network Time Protocol)

- Purpose: Synchronizes clocks of networked devices.
- Function: Ensures accurate timekeeping across devices in a network.

RDP (Remote Desktop Protocol)

- Purpose: Provides a user with a graphical interface to connect to another computer over a network connection.
- Common Use: Remote management and access of Windows computers.

SMB (Server Message Block) / CIFS (Common Internet File System)

- Purpose: Provides shared access to files, printers, and serial ports.
- Common Use: File sharing in Windows-based networks.

MQTT (Message Queuing Telemetry Transport)

- -Purpose: Lightweight messaging protocol for small sensors and mobile devices.
- -Common Use: Internet of Things (IoT) applications.

CoAP (Constrained Application Protocol)

- Purpose: Designed for use with constrained devices and networks.
- Common Use: IoT applications, particularly where low bandwidth is a consideration.

Domain Name System (DNS):

DNS is a hostname to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.

Requirement

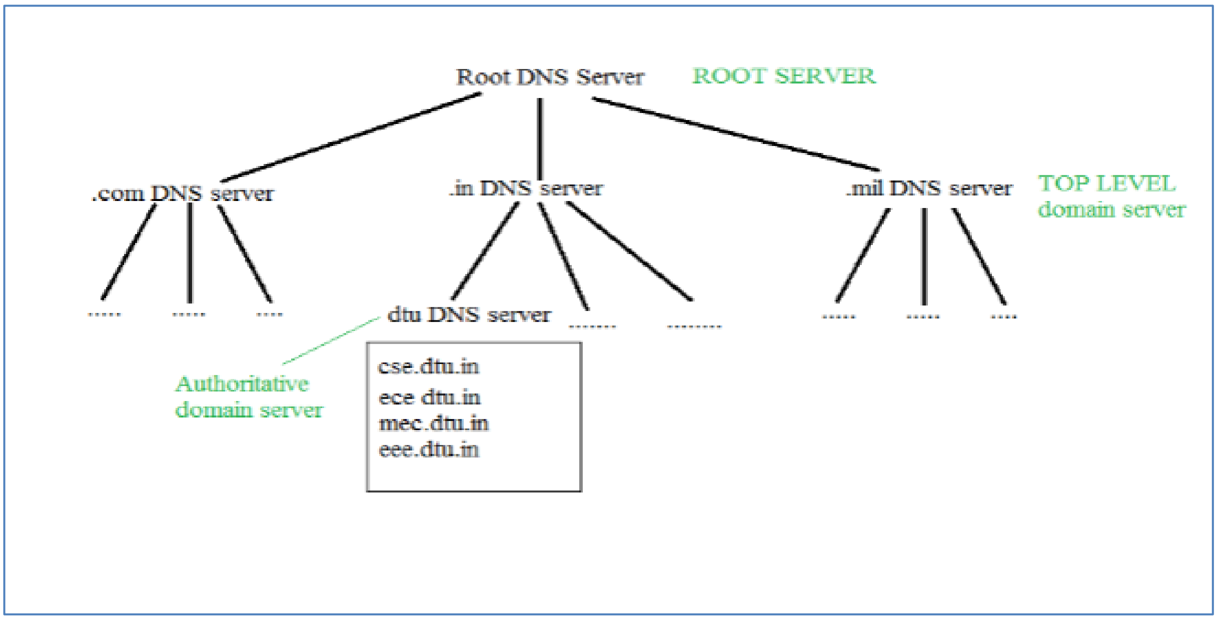
Every host is identified by the IP address but remembering numbers is very difficult for the people and also the IP addresses are not static therefore a mapping is required to change the domain name to IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.

Domain:

There are various kinds of DOMAIN :

1. **Generic domain** : .com(commercial) .edu(educational) .mil(military) .org(non profit organization) .net(similar to commercial) all these are generic domain.
2. Country domain .in (india) .us .uk
3. Inverse domain if we want to know what is the domain name of the website. Ip to domain name mapping.So DNS can provide both the mapping for example to find the ip addresses of geeksforgeeks.org then we have to type nslookup www.geeksforgeeks.org.

Organization of Domain :



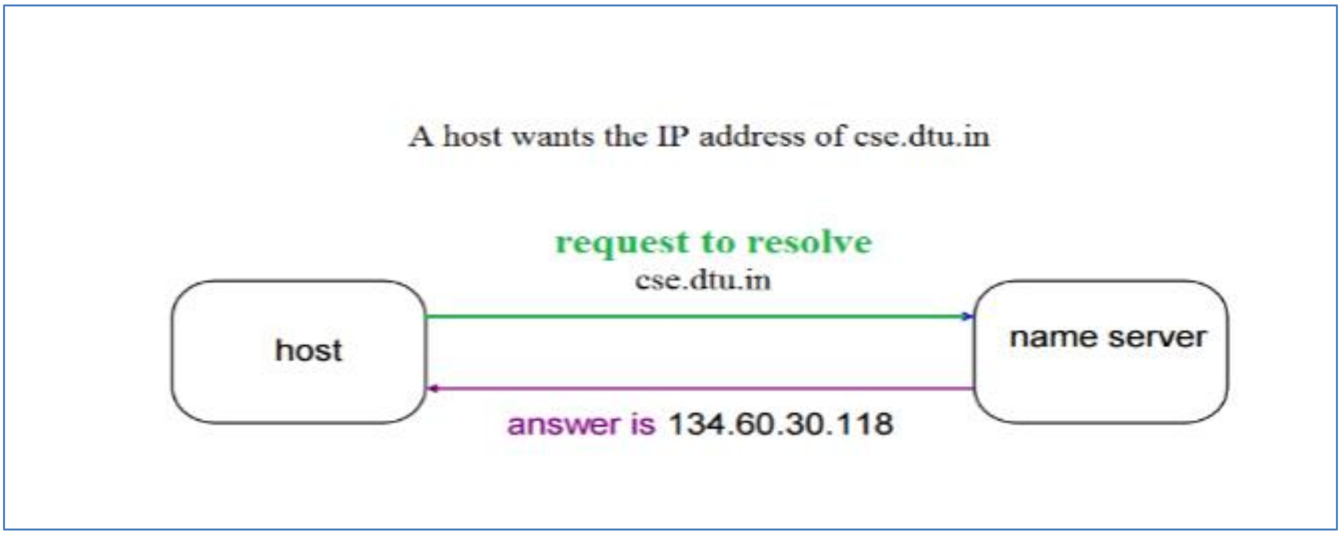
t is very difficult to find out the IP address associated with a website because there are millions of websites and with all those websites we should be able to generate the IP address immediately, there should not be a lot of delay for that to happen organization of database is very important.

DNS record – Domain name, IP address what is the validity?? what is the time to live ?? and all the information related to that domain name. These records are stored in a tree-like structure.

Namespace - Set of possible names, flat or hierarchical. The naming system maintains a collection of bindings of names to values – given a name, a resolution mechanism returns the corresponding value –

Name server - It is an implementation of the resolution mechanism. DNS (Domain Name System) = Name service in Internet – Zone is an administrative unit, domain is a subtree.

Name to Address Resolution

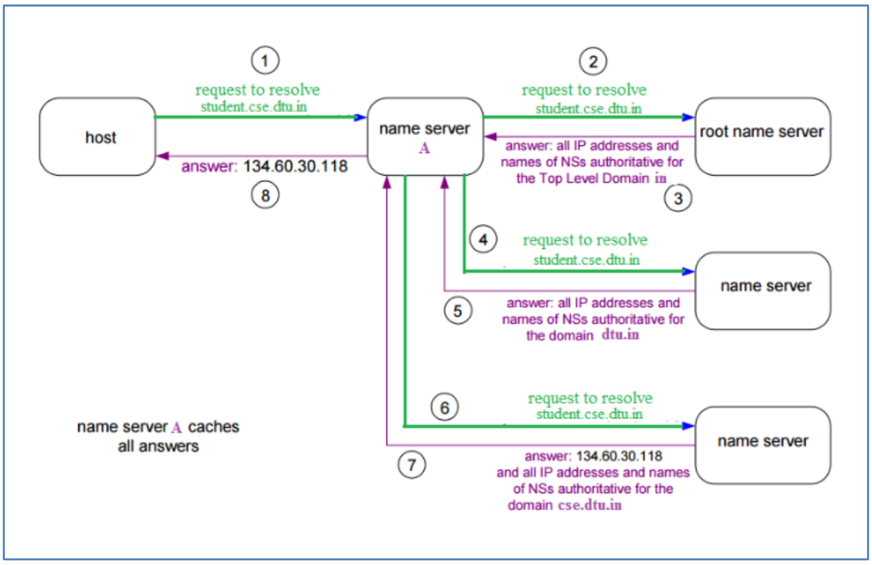


The host request the DNS name server to resolve the domain name. And the name server returns the IP address corresponding to that domain name to the host so that the host can future connect to that IP address.

Hierarchy of Name Servers Root name servers – It is contacted by name servers that can not resolve the name. It contacts authoritative name server if name mapping is not known. It then gets the mapping and return the IP address to the host.

Top level server – It is responsible for com, org, edu etc and all top level country domains like uk, fr, ca, in etc. They have info about authoritative domain servers and know names and IP addresses of each authoritative name server for the second level domains.

Authoritative name servers This is organization's DNS server, providing authoritative hostName to IP mapping for organization servers. It can be maintained by organization or service provider. In order to reach cse.dtu.in we have to ask the root DNS server, then it will point out to the top level domain server and then to authoritative domain name server which actually contains the IP address. So the authoritative domain server will return the associative ip address.


1
request to resolve student.cse.dtu.in
2
request to resolve student.cse.dtu.in
host
name server A
root name server
answer: 134.60.30.118
8
answer: all IP addresses and names of NSs authoritative for the Top Level Domain in
3
4
request to resolve student.cse.dtu.in
name server
5
answer: all IP addresses and names of NSs authoritative for the domain dtu.in
6
request to resolve student.cse.dtu.in
name server
name server A caches all answers
7
answer: 134.60.30.118 and all IP addresses and names of NSs authoritative for the domain cse.dtu.in

The client machine sends a request to the local name server, which , if root does not find the address in its database, sends a request to the root name server , which in turn, will route the query to an intermediate or authoritative name server. The root name server can also contain some hostName to IP address mappings . The intermediate name server always knows who the authoritative name server is. So finally the IP address is returned to the local name server which in turn returns the IP address to the host

Mapping Names to Addresses

In this case, the server checks the generic domains or the country domains to find the mapping. If the domain name is from the generic section, the resolver receives a domain name such as “chal .atc: fhda.edu”. The query is sent by the resolver to the local DNS server for resolution. If the local server cannot resolve the query, it either refers the resolver to other servers or asks other servers directly. If the domain name is from the country domain section, the resolver receives a domain name such as “ch .fhda.cu.ca.us”. The procedure is the same.

Mapping Addresses to Names

A client can send as IP address to a server to be mapped to a domain name. This is called a PTR query. To answer queries of this kind, DNS uses the inverse domain. However, in the request, the IP address is reversed and two labels, in- addr and arpa are appended to create a domain acceptable by the inverse domain section. For example. if the resolver receives the IP address 132.34.45.121 , the resolver first inverts the address and then adds the two labels before sending. the domain name sent is “121.45.34.132.in-addr.arpa” , which is received by the local DNS and resolved.

DNS spoofing, also known as DNS cache poisoning, is a malicious attack where corrupt DNS data is introduced into the cache of a DNS resolver. This causes the resolver to return an incorrect IP address, redirecting traffic to the attacker's site, which can be used for phishing, spreading malware, or intercepting sensitive data.

How DNS Spoofing Works:

- **Inserting Malicious Data**: The attacker exploits a vulnerability in the DNS server to insert false DNS entries.
- **Caching the False Data**: The DNS server caches the malicious data, believing it to be legitimate.
- **Redirecting Traffic**: When users request the IP address for the affected domain, the server provides the incorrect IP, redirecting users to the attacker's malicious site.
- Methods of DNS Spoofing:
- **Man-in-the-Middle (MitM)**: The attacker intercepts communication between a user and a DNS server, injecting false DNS responses.
- **DNS Cache Poisoning:** The attacker sends forged DNS responses to a DNS server, tricking it into caching incorrect information.

👉 Explain the Working of HTTP and HTTPs:

In address bar of a browser, have you noticed either *http://* or *https://* at the time of browsing a website? If neither of these are present then most likely, it's *http://* Let's find out the difference...

In short, both of these are protocols using which the information of a particular website is exchanged between Web Server and Web Browser. But what's difference between these two? Well, extra ***s*** is present in *https* and that makes it secure! What a difference :) A very short and concise difference between *http* and *https* is that *https* is much more secure compared to *http*.

Let us dig a little more.
Hyper**T**ext **T**ransfer **P**rotocol (HTTP is a protocol using which hypertext is transferred over the Web. Due to its simplicity, *http* has been the most widely used protocol for data transfer over the Web but the data (i.e. hypertext) exchanged using *http* isn't as secure as we would like it to be. In fact, hyper-text exchanged using *http* goes as plain text i.e. anyone between the browser and server can read it relatively easy if one intercepts this exchange of data. But why do we need this security over the Web? Think of 'Online shopping' at Amazon or Flipkart. You might have noticed that as soon as we click on the Check-out on these online shopping portals, the address bar gets changed to use *https*. This is done so that the subsequent data transfer (i.e. financial transaction etc.) is made secure. And that's why *https* was introduced so that a secure session is a setup first between Server and Browser. In fact, cryptographic protocols such as SSL and/or TLS turn *http* into *https* i.e. **https** = **http** + **cryptographic protocols**. Also, to achieve this security in *https*, Public Key Infrastructure (PKI) is used because public keys can be used by several Web Browsers while private key can be used by the Web Server of that particular website. The distribution of these public keys is done via Certificates which are maintained by the Browser. You can check these certificates in your browser settings. We'll detail out this setting up secure session procedure in another post.

Also, another syntactic difference between *http* and *https* is that *http* uses default port 80 while *https* uses default port 443. But it should be noted that this security in *https* is achieved at the cost of processing time because Web Server and Web Browser needs to exchange encryption keys using Certificates before actual data can be transferred. Basically, setting up of a secure session is done before the actual hypertext exchange between server and browser.

HTTP	**HTTPS**
HTTP stands for HyperText Transfer Protocol. In HTTP, the URL begins with "http://".	HTTPS stands for HyperText Transfer Protocol Secure. In HTTPS, the URL starts with "https://".
HTTP uses port number 80 for communication.	HTTPS uses port number 443 for communication.
Hyper-text exchanged using HTTP goes as plain text i.e. anyone between the browser and server can read it relatively easily if one intercepts this exchange of data and due to which it is Insecure.	HTTPS is considered to be secure but at the cost of processing time because Web Server and Web Browser need to exchange encryption keys using Certificates before actual data can be transferred.
HTTP Works at the Application Layer.	HTTPS works at Transport Layer.
HTTP does not use encryption, which results in low security in comparison to HTTPS.	HTTPS uses Encryption which results in better security than HTTP.
HTTP speed is faster than HTTPS.	HTTPS speed is slower than HTTP.
HTTP does not use data hashtags to secure data.	HTTPS will have the data before sending it and returning it to its original state on the receiver side.
HTTP is used to transfer text, video, and images via web pages.	HTTPS is used to transfer data securely via a network.

👉**DHCP** is an abbreviation for Dynamic Host Configuration Protocol. It is an application layer protocol used by hosts for obtaining network setup information. The DHCP is controlled by a DHCP server that dynamically distributes network configuration parameters such as IP addresses, subnet masks, and gateway addresses.

What is a Dynamic host configuration protocol?

- Dynamic – Automatically
- Host – Any computer that is connected to the network
- Configuration – To configure a host means to provide network information (IP address, subnet mask, Gateway address) to a host
- Protocol – Set of rules

👉Packet Traveling (IMP):

A packet is a formatted unit of data that travels across a network from a source to a destination. The journey of a packet involves multiple steps and passes through various layers of the network model. Here's a simplified overview of how a packet travels from one device to another over the internet:

1. Application Layer:

- **Source Device**: The journey begins at the application layer of the source device, where the data is generated by an application (e.g., a web browser requesting a web page).

2. Transport Layer:

- **Segmentation**: The data is segmented into smaller pieces, and each segment is encapsulated with a transport layer header (e.g., TCP or UDP header). This header includes information like source and destination ports and sequence numbers for reassembly.

3. Network Layer:

- **Packet Creation:** Each segment is further encapsulated with a network layer header (e.g., IP header), forming a packet. The IP header includes the source and destination IP addresses.

4. Data Link Layer:

- **Frame Creation**: The packet is then encapsulated into a frame by adding a data link layer header and trailer (e.g., Ethernet header and trailer). The header includes the source and destination MAC addresses.
- **Local Delivery**: The frame is placed onto the physical medium (e.g., Ethernet, Wi-Fi) and sent to the nearest network device, usually a router or switch.

5. Physical Layer:

- **Transmission**: The frame is converted into electrical signals, light pulses, or radio waves and transmitted over the physical medium (e.g., cables, fiber optics, wireless).

6. Intermediate Devices:

- **Switches**: If the frame is within the same local network, switches forward it to the appropriate device based on MAC addresses.
- **Routers**: When the frame reaches a router, the router removes the data link layer header and examines the network layer (IP) header. The router determines the best path to the destination IP address, re-encapsulates the packet with a new data link layer header, and forwards it to the next hop in the path, possibly another router.

7. Repeating Process:

- The packet may pass through multiple routers and networks. At each hop, the router examines the IP header, determines the next hop, and forwards the packet.

8. Destination Network:

- When the packet reaches the router connected to the destination network, the router forwards it to the appropriate device using the data link layer.

9. Destination Device:

- **Reception**: The destination device receives the frame, removes the data link layer header and trailer, and extracts the packet.
- **Network Layer Processing:** The device examines the IP header and passes the segment to the transport layer.
- **Transport Layer Processing**: The transport layer reassembles the segments if necessary, checks for errors, and forwards the data to the appropriate application layer process based on port numbers.

10. Application Layer:

- The application on the destination device receives the data and processes it (e.g., the web browser displays the requested web page).

Common Networking commands:

1. ping

- Purpose: Tests the reachability of a host on an IP network and measures the round-trip time for messages sent from the source to the destination.
- Usage: ping [hostname or IP address]

2. netstat

- Purpose: Displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.
- Usage: netstat -an

3. tracert (Windows) / traceroute (Linux/macOS)

- Purpose: Traces the route taken by packets to reach a destination.
- Usage:
- Windows: tracert [hostname or IP address]
- Linux/macOS: traceroute [hostname or IP address]

4. nslookup

- Purpose: Queries the Domain Name System (DNS) to obtain domain name or IP address mapping.
- Usage: nslookup [domain name]

5. pathping (Windows)

- Purpose: Combines the functionality of ping and tracert to identify network latency and packet loss.
- Usage: pathping [hostname or IP address]

6. netdiag (Windows)

- Purpose: Diagnoses network problems and tests various network components.
- Usage: netdiag /test:winsock /v
- Note: netdiag is part of the Windows Support Tools and may need to be installed separately.

7. hostname

- Purpose: Displays or sets the system's hostname.
- Usage: hostname

8. arp

- Purpose: Displays the ARP table, which maps IP addresses to MAC addresses.
- Usage: arp -a

👉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 SSL?

SSL (Secure Sockets Layer) and its successor, **TLS (Transport Layer Security)**, are protocols for establishing authenticated and encrypted links between networked computers. Although the SSL protocol was deprecated with the release of TLS 1.0 in 1999, it is still common to refer to these related technologies as “SSL” or “SSL/TLS.”

👉What is an SSL certificate?

An **SSL certificate** (also known as a TLS or SSL/TLS certificate) is a digital document that binds the identity of a website to a cryptographic key pair consisting of a public key and a private key. The public key, included in the certificate, allows a web browser to initiate an encrypted communication session with a web server via the TLS and HTTPS protocols. The private key is kept secure on the server, and is used to digitally sign web pages and other documents (such as images and JavaScript files).

👉What is TLS?

TLS (Transport Layer Security), released in 1999, is the successor to the **SSL (Secure Sockets Layer)** protocol for authentication and encryption. TLS 1.3 is defined in in **RFC 8446** (August 2018).

Do I need a dedicated IP address to use SSL/TLS?

At one time it was a mandatory requirement to have a dedicated IP for each SSL certificate on a web server. This is no longer the case due to a technology called Server Name Indication (SNI). Your hosting platform will specifically have to support SNI. You can find out more information about SNI in this SSL.com article.

What port is recommended to use SSL/TLS over?

For maximum compatibility, port 443 is the standard, thus recommended, port used for secured SSL/TLS communications. However, any port can be used.

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

What is Multiplexing?

Multiplexing is a technique used to combine and send the multiple data streams over a single medium. The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as a multiplexer.

Multiplexing is achieved by using a device called Multiplexer (**MUX**) that combines n input lines to generate a single output line. Multiplexing follows many-to-one, i.e., n input lines and one output line.

Demultiplexing is achieved by using a device called Demultiplexer (**DEMUX**) available at the receiving end. DEMUX separates a signal into its component signals (one input and n outputs). Therefore, we can say that demultiplexing follows the one-to-many approach.

Why Multiplexing?

- The transmission medium is used to send the signal from sender to receiver. The medium can only have one signal at a time.
- If there are multiple signals to share one medium, then the medium must be divided in such a way that each signal is given some portion of the available bandwidth. For example: If there are 10 signals and bandwidth of medium is100 units, then the 10 unit is shared by each signal.
- When multiple signals share the common medium, there is a possibility of collision. Multiplexing concept is used to avoid such collision.
- Transmission services are very expensive.

How Bluetooth works:

Bluetooth is a wireless communication technology that enables devices to communicate and exchange data over short distances using radio waves. Here's a simplified explanation of how Bluetooth works:

1. Bluetooth Radio Frequency:

- Bluetooth operates in the 2.4 GHz ISM (Industrial, Scientific, and Medical) band, which is a globally available unlicensed frequency band.
- Within this band, Bluetooth uses frequency-hopping spread spectrum (FHSS) to avoid interference from other wireless devices operating in the same frequency range.

2. Bluetooth Devices:

- Each Bluetooth-enabled device contains a Bluetooth radio transceiver, which allows it to send and receive data wirelessly.
- Devices are classified as "master" or "slave," depending on their role in a Bluetooth connection. A master device initiates and controls the connection, while slave devices respond to connection requests from the master.

3. Bluetooth Pairing:

- Before devices can communicate, they must establish a pairing relationship. This involves exchanging security credentials, such as passkeys or PINs, to authenticate the connection.
- Pairing can be initiated manually by the user or automatically using methods like Bluetooth Low Energy (BLE) pairing, which requires no user input.

4. Bluetooth Protocol Stack:

- Bluetooth uses a layered protocol stack, with each layer responsible for different aspects of communication:
  - **Physical Layer (PHY):** Handles transmission and reception of radio signals.
  - **Link Layer (LL):** Manages connections, data packet formatting, and error correction.
  - **Host Controller Interface (HCI):** Provides a standardized interface between the Bluetooth hardware and higher-level protocols.
  - **Logical Link Control and Adaptation Protocol (L2CAP):** Handles data segmentation and reassembly, quality of service (QoS), and multiplexing of higher-layer protocols.
  - **Bluetooth Core Protocols:** Include protocols for device discovery, connection establishment, and data transfer.
  - **Bluetooth Profile Protocols:** Define specific applications or services, such as hands-free calling (HFP), file transfer (FTP), or audio streaming (A2DP).

5. Bluetooth Connection Establishment:

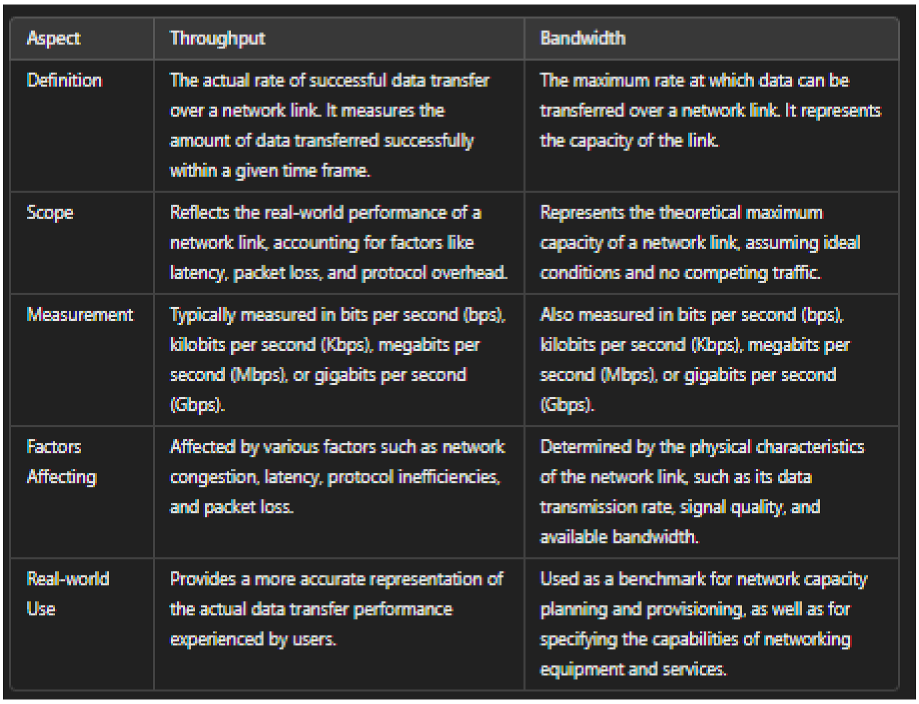
- Once paired, devices can establish connections using one of several Bluetooth profiles, depending on the desired application.
- The master device initiates a connection request, and the slave device responds by acknowledging the request and establishing a connection.
- After connection establishment, devices can exchange data packets using the Bluetooth protocol stack.

6. Bluetooth Applications:

- Bluetooth technology is used in a wide range of applications, including:
  - Wireless audio streaming (e.g., headphones, speakers).
  - Hands-free calling in vehicles (e.g., Bluetooth-enabled car kits).
  - Wireless file transfer between devices (e.g., smartphones, tablets).
  - Wearable devices (e.g., fitness trackers, smartwatches).
  - Home automation and IoT (Internet of Things) applications.

7. Bluetooth Versions and Standards:

- Bluetooth technology is continuously evolving, with new versions and standards introduced to improve performance, increase data rates, and reduce power consumption. Major Bluetooth versions include Bluetooth 1.x, 2.x, 3.x, 4.x, 5.x, and the latest version, Bluetooth 5.2.



Aspect	Throughput	Bandwidth
Definition	The actual rate of successful data transfer over a network link. It measures the amount of data transferred successfully within a given time frame.	The maximum rate at which data can be transferred over a network link. It represents the capacity of the link.
Scope	Reflects the real-world performance of a network link, accounting for factors like latency, packet loss, and protocol overhead.	Represents the theoretical maximum capacity of a network link, assuming ideal conditions and no competing traffic.
Measurement	Typically measured in bits per second (bps), kilobits per second (Kbps), megabits per second (Mbps), or gigabits per second (Gbps).	Also measured in bits per second (bps), kilobits per second (Kbps), megabits per second (Mbps), or gigabits per second (Gbps).
Factors Affecting	Affected by various factors such as network congestion, latency, protocol inefficiencies, and packet loss.	Determined by the physical characteristics of the network link, such as its data transmission rate, signal quality, and available bandwidth.
Real-world Use	Provides a more accurate representation of the actual data transfer performance experienced by users.	Used as a benchmark for network capacity planning and provisioning, as well as for specifying the capabilities of networking equipment and services.

What is the FTP protocol?

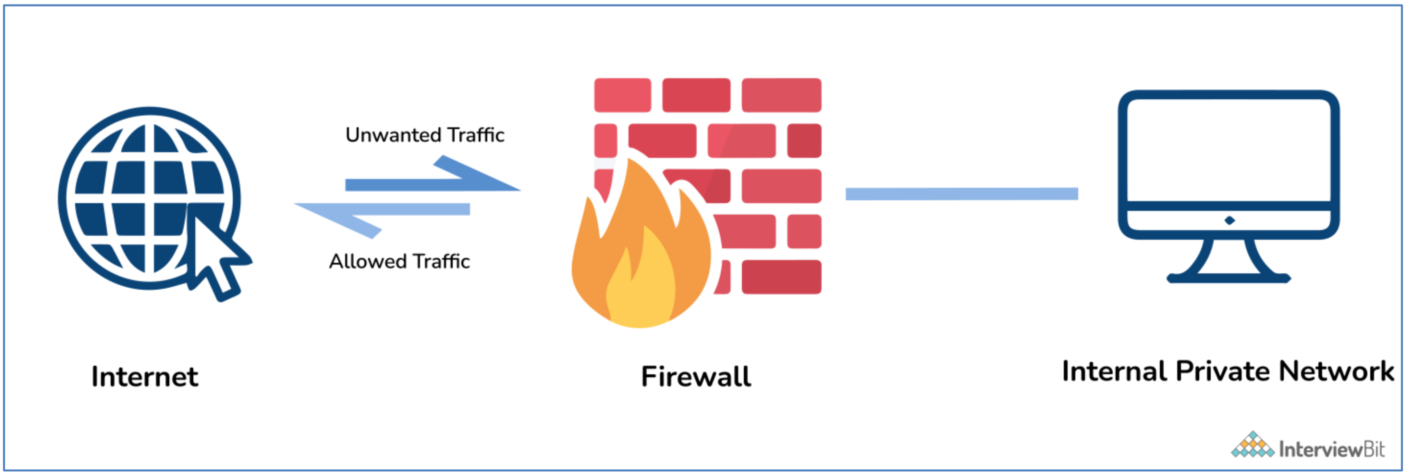
FTP is a File Transfer Protocol. It is an application layer protocol used to transfer files and data reliably and efficiently between hosts. It can also be used to download files from remote servers to your computer. It uses port 27 by default.

8. 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.

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.



Firewalls are generally of two types: *Host-based* and *Network-based.*

1. **Host- based Firewalls :** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.

2. **Network-based Firewalls :** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

Firewalls are network security devices that monitor and control incoming and outgoing network traffic based on predetermined security rules. Here are the types of firewalls in short:

1. Packet Filtering Firewall:

- **Operation:** Examines individual packets of data as they pass through the firewall.
- **Criteria:** Filters packets based on predetermined rules such as source and destination IP addresses, ports, and protocols.
- **Advantages:** Simple and efficient, suitable for basic network security needs.

- **Limitations:** Limited ability to inspect packet contents or handle complex protocols.

2. Stateful Inspection Firewall:

- **Operation:** Tracks the state of active connections and inspects the context of packets.
- **Criteria:** Examines packet headers and contents to determine if they belong to an established connection.
- **Advantages:** Offers improved security by understanding the context of traffic flows.
- **Limitations:** More resource-intensive than packet filtering firewalls, may impact performance.

3. Proxy Firewall (Application Layer Firewall):

- **Operation:** Acts as an intermediary between client and server, intercepting and inspecting traffic at the application layer.
- **Criteria:** Analyzes application-layer protocols (e.g., HTTP, FTP) and filters based on content.
- **Advantages:** Provides deep packet inspection and granular control over application traffic.
- **Limitations:** May introduce latency due to proxying, requires additional processing power.

4. Next-Generation Firewall (NGFW):

- **Operation:** Combines traditional firewall features with advanced security capabilities such as intrusion prevention, deep packet inspection, and application awareness.
- **Criteria:** Inspects traffic at multiple layers (network, application, user) and uses threat intelligence to identify and block malicious activity.
- **Advantages:** Offers comprehensive security features to protect against modern threats.
- **Limitations:** Higher cost and complexity compared to traditional firewalls.

5. Unified Threat Management (UTM) Firewall:

- **Operation:** Integrates multiple security functions, including firewall, antivirus, intrusion detection/prevention, VPN, and content filtering, into a single appliance.
- **Criteria:** Provides all-in-one security solution for small to medium-sized businesses.
- **Advantages:** Simplifies security management and reduces hardware footprint.
- **Limitations:** May lack the advanced features and scalability of standalone NGFWs.

6. Cloud Firewall:

- **Operation:** Deployed in cloud environments to protect virtualized infrastructure and cloud-based applications.
- **Criteria:** Offers security controls for cloud workloads, virtual networks, and internet-facing services.
- **Advantages:** Scalable, flexible, and integrates with cloud-native security services.
- **Limitations:** Relies on cloud provider's infrastructure and may have limited visibility into on-premises networks.

Feature	Unicast	Broadcast	Multicast
Definition	A communication where a message is sent from one sender to one receiver.	A communication where a message is sent from one sender to all receivers.	A communication where a message is sent from one sender to a group of receivers
Transmission	Data is sent to a single recipient	Data is sent to all recipients in a network	Data is sent to a group of recipients
Addressing	Uses a unique destination address	Uses a special broadcast address	Uses a special multicast address
Delivery	Guaranteed delivery	Not all devices may be interested in the data	Not all devices may be interested in the data
Network Traffic	Generates the least amount of network traffic	Generates the most amount of network traffic	Generates moderate network traffic
Security	More secure because data is sent to a specific recipient	Less secure because data is sent to all devices in the network	Moderately secure because data is sent to a specific group of devices
Examples	Email, file transfer	DHCP requests, ARP requests	Video streaming, online gaming
Destination	Single receiver	All receivers	Group of receivers
Bandwidth usage	Moderate	High	Moderate
Latency	Low	High	Moderate

👉Basic Network Attacks in Computer Network:

How are computer networks vulnerable? What are some of the more prevalent types of attacks today?

- **Malware** – short for malicious software which is specifically designed to disrupt, damage, or gain authorized access to a computer system. Much of the malware out there today is self-replicating: once it infects one host, from that host it seeks entry into other hosts over the Internet, and from the newly infected hosts, it seeks entry into yet more hosts. In this manner, self-replicating malware can spread exponentially fast.

- **Virus** – A malware which requires some form of user's interaction to infect the user's device. The classic example is an e-mail attachment containing malicious executable code. If a user receives and opens such an attachment, the user inadvertently runs the malware on the device.

- **Worm** – A malware which can enter a device without any explicit user interaction. For example, a user may be running a vulnerable network application to which an attacker can send malware. In some cases, without any user intervention, the application may accept the malware from the Internet and run it, creating a worm.

- **Botnet** – A network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g. to send spam.

- **DoS** (Denial of Service) – A DoS attack renders a network, host, or other pieces of infrastructure unusable by legitimate users. Most Internet DoS attacks fall into one of three categories :

    - **Vulnerability attack**: This involves sending a few well-crafted messages to a vulnerable application or operating system running on a targeted host. If the right sequence of packets is sent to a vulnerable application or operating system, the service can stop or, worse, the host can crash.

    - **Bandwidth flooding**: The attacker sends a deluge of packets to the targeted host—so many packets that the target's access link becomes clogged, preventing legitimate packets from reaching the server.

    - **Connection flooding**: The attacker establishes a large number of half-open or fully open TCP connections at the target host. The host can become so bogged down with these bogus connections that it stops accepting legitimate connections.

- **DDoS (Distributed DoS**) – DDoS is a type of DOS attack where multiple compromised systems, are used to target a single system causing a Denial of Service (DoS) attack. DDoS attacks leveraging botnets with thousands of comprised hosts are a common occurrence today. DDoS attacks are much harder to detect and defend against than a DoS attack from a single host.

- **Packet sniff**er – A passive receiver that records a copy of every packet that flies by is called a packet sniffer. By placing a passive receiver in the vicinity of the wireless transmitter, that receiver can obtain a copy of every packet that is transmitted! These packets can contain all kinds of sensitive information, including passwords, social security numbers, trade secrets, and private personal messages. some of the best defenses against packet sniffing involve cryptography.

- **IP Spoofing** – The ability to inject packets into the Internet with a false source address is known as IP spoofing, and is but one of many ways in which one user can masquerade as another user. To solve this problem, we will need end-point authentication, that is, a mechanism that will allow us to determine with certainty if a message originates from where we think it does.

- **Man-in-the-Middle Attack** – As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data.

- **Compromised-Key Attack** – A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key. An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack.

Phishing – The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

DNS spoofing – Also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect IP address.

Rootkit – Rootkits are stealthy packages designed to benefit administrative rights and get the right of entry to a community tool. Once installed, hackers have complete and unrestricted get right of entry to the tool and can, therefore, execute any movement including spying on customers or stealing exclusive data with no hindrance.

👉Denial of Service (DoS):

A **Denial of Service (DoS)** attack is a malicious attempt to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of illegitimate traffic or resource requests. Here's an overview of DoS attacks and some prevention strategies:

Types of DoS Attacks:

1. **Traditional DoS:** Involves flooding a target system with excessive traffic, such as SYN flood, UDP flood, or ICMP flood attacks.
2. **Distributed DoS (DDoS):** Utilizes multiple compromised devices (botnets) to launch coordinated attacks against a target, amplifying the volume of traffic and making mitigation more challenging.
3. **Application Layer DoS:** Targets vulnerabilities in web applications or services to exhaust server resources, such as HTTP flood or Slowloris attacks.

Prevention Measures:

1. **Network Security Measures:**
   - Implement firewalls, intrusion detection/prevention systems (IDS/IPS), and routers with rate limiting and access control lists (ACLs) to filter and block malicious traffic.
   - Use content delivery networks (CDNs) or DDoS mitigation services to absorb and mitigate large-scale attacks.
2. **Traffic Monitoring and Analysis:**
   - Monitor network traffic for unusual patterns or spikes in traffic volume.
   - Use network monitoring tools to identify and block suspicious traffic in real-time.
3. **Service Configuration:**
   - Configure services and applications to limit resource consumption and handle high traffic loads efficiently.
   - Enable rate limiting, throttling, and connection limits to prevent abuse and protect against DoS attacks.
4. **Security Updates and Patch Management:**
   - Keep systems, applications, and network devices up-to-date with the latest security patches and updates to address known vulnerabilities.
   - Regularly audit and secure configurations to minimize attack surface.
5. **Incident Response Planning:**
   - Develop and regularly test incident response plans to effectively mitigate and recover from DoS attacks.
   - Establish communication protocols and coordination with internet service providers (ISPs) and law enforcement agencies.
6. **Anomaly Detection and Behavioral Analysis:**
   - Deploy anomaly detection systems to identify abnormal behavior and deviations from baseline traffic patterns.

☜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

☜*Where are ports? What are the Port numbers of some common protocols?*

A **port** is basically a physical docking point which is basically used to connect the external devices to the computer or we can say that A port act as an interface between computer and the external devices, e.g., we can hard drives, printers to the computer with the help of ports.

Features of Computer ports:

- We can connect external devices to the computer with the help of ports and cables.
- These are basically slots on mother board where we connect external devices or we can plugged in external devices through cables.
- Mouse, keyboards, printers, speakers are some of the example of external devices that connected to the computer through ports.
    1. TELNET: Port number of telnet is 23.
    2. FTP: Port number for FTP is 20 for data and 21 for control.
    3. TFTP: Port number of TFTP is 69.

    4. SMTP: Port number of TFTP is 25.
    5. LPD: Port number of TFTP is 545.
    6. SNMP: Port number of TFTP is 61(TCP) and 62(UDP).
    7. DNS: Port number of TFTP is 53.
    8. DHCP: Port number of TFTP is 67(TCP) and 68(UDP).

☜*What is FTP? How is FTP different from Secure FTP?*

- FTP stands for File Transfer Protocol. It is a protocol which is used to transfer or copies the file from one host to another host. But there may be some problems like different file name and different file directory while sending and receiving the file in different hosts or systems. And in FTP, a secure channel is not provided to transfer the files between the hosts or systems. It is used in port no-21.

  SFTP stands for **Secure File Transfer Protocol**. It is a protocol which provides the secure channel, to transfer or copies the file from one host to another host or systems. SFTP establishes the control connection under SSH protocol and It is used in port no-22.

  There are some difference between them which are given below:

.	FTP	SFTP
1.	FTP stands for File Transfer Protocol.	SFTP stands for Secure File Transfer Protocol.
2.	In FTP, secure channel is not provided to transfer the files between the hosts.	In SFTP, secure channel is provided to transfer the files between the hosts.
3.	FTP (File transfer protocol) is a part of TCP/IP protocol.	Secure File Transfer Protocol is a SSH protocol.
4.	FTP (File transfer protocol) usually runs on port no-21.	SFTP (Secure File Transfer Protocol) runs on port no-22.
5.	FTP establishes the connection under TCP protocol.	SFTP establishes the control connection under SSH protocol.
6.	FTP do not encrypt the data before sending.	SFTP, data is encrypted before sending.

👉What is SMTP :

Email is emerging as one of the most valuable services on the internet today. Most of the internet systems use SMTP as a method to transfer mail from one user to another. SMTP is a push protocol and is used to send the mail whereas POP (post office protocol) or IMAP (internet message access protocol) are used to retrieve those emails at the receiver's side.

SMTP Fundamentals SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is the always-on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection on that port (25). After successfully establishing the TCP connection the client process sends the mail instantly.

SMTP Protocol

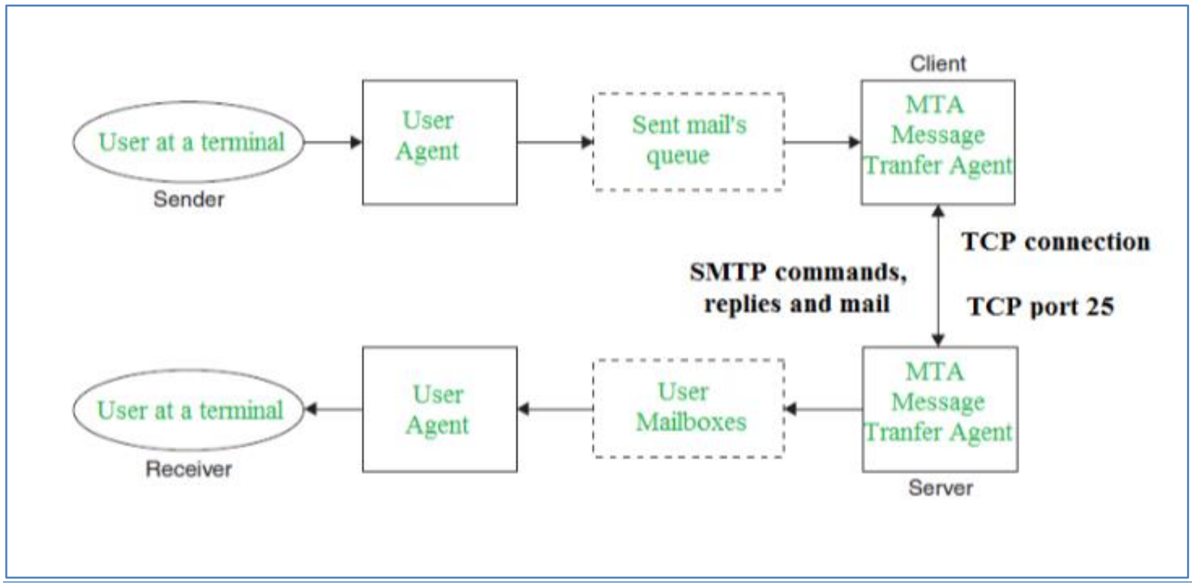
The SMTP model is of two types:

1. End-to- end method
2. Store-and- forward method

The end to end model is used to communicate between different organizations whereas the store and forward method are used within an organization. An SMTP client who wants to send the mail will contact the destination's host SMTP directly in order to send the mail to the destination. The SMTP server will keep the mail to itself until it is successfully copied to the receiver's SMTP.
The client SMTP is the one which initiates the session let us call it as the client- SMTP and the server SMTP is the one which response to the session request and let us call it as receiver-SMTP. The client-SMTP will start the session and the receiver-SMTP will respond to the request.

Model of SMTP system

In the SMTP model user deals with the user agent (UA) for example Microsoft Outlook, Netscape, Mozilla, etc. In order to exchange the mail using TCP, MTA is used. The users sending the mail do not have to deal with the MTA it is the responsibility of the system admin to set up the local MTA. The MTA maintains a small queue of mails so that it can schedule repeat delivery of mail in case the receiver is not available. The MTA delivers the mail to the mailboxes and the information can later be downloaded by the user agents.



Both the SMTP-client and MSTP-server should have 2 components:

1. User agent (UA)
2. Local MTA

Communication between sender and the receiver: The senders, user agent prepare the message and send it to the MTA. The MTA functioning is to transfer the mail across the network to the receivers MTA. To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA.

SENDING EMAIL: Mail is sent by a series of request and response messages between the client and a server. The message which is sent across consists of a header and the body. A null line is used to terminate the mail header. Everything which is after the null line is considered as the body of the message which is a sequence of ASCII characters. The message body contains the actual information read by the receipt.

RECEIVING EMAIL: The user agent at the server-side checks the mailboxes at a particular time of intervals. If any information is received it informs the user about the mail. When the user tries to read the mail it displays a list of emails with a short description of each mail in the mailbox. By selecting any of the mail user can view its contents on the terminal.

Some SMTP Commands:

- HELO - Identifies the client to the server, fully qualified domain name, only sent once per session
- MAIL - Initiate a message transfer, fully qualified domain of originator
- RCPT - Follows MAIL, identifies an addressee, typically the fully qualified name of the addressee and for multiple addressees use one RCPT for each addressee
- DATA - send data line by line

What happens when you type URL in your browser?

Steps are:

1. URL is typed in the browser.
2. If the requested object is in the browser cache and is fresh, move on to Step 8.

3. DNS lookup to find the IP address of the server.

   Suppose we typed www.amazon.in, then this URL is converted into corresponding IP address of the host using DNS(Domain Name System). But, it is not so. Amazon has multiple servers in multiple locations to cater to the huge volume of requests they receive per second. Thus we should let Amazon decide which server is best suited to our needs.
4. Following is a summary of steps happening while DNS service is at work:

   - **Check browser cache**: browsers maintain a cache of DNS records for some fixed duration. So, this is the first place to resolve DNS queries.
   - **Check OS cache**: if the browser doesn't contain the record in its cache, it makes a system call to underlying Operating System to fetch the record as OS also maintains a cache of recent DNS queries.
   - **Router Cache**: if above steps fail to get a DNS record, the search continues to your router which has its own cache
   - **ISP cache**: if everything fails, the search moves on to your ISP. First, it tries in its cache, if not found - ISP's DNS recursive search comes into the picture. DNS lookup is again a complex process which finds the appropriate IP address from a list of many options available for websites like Google.

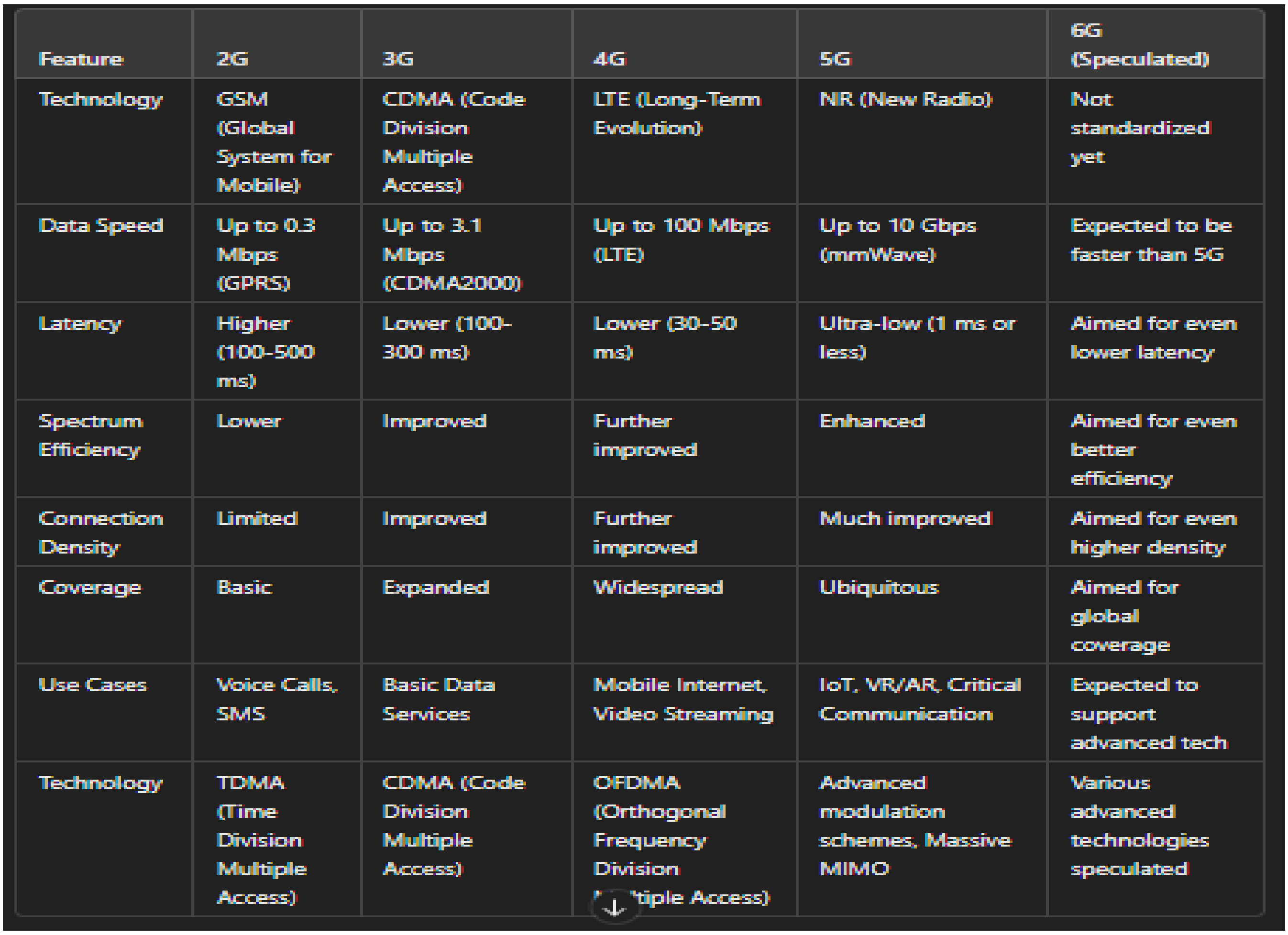
5. Browser initiates a TCP connection with the server.

6. Browser sends an HTTP request to the server.

7. Server handles the incoming request

8. Browsers displays the html content

9. Client interaction with server



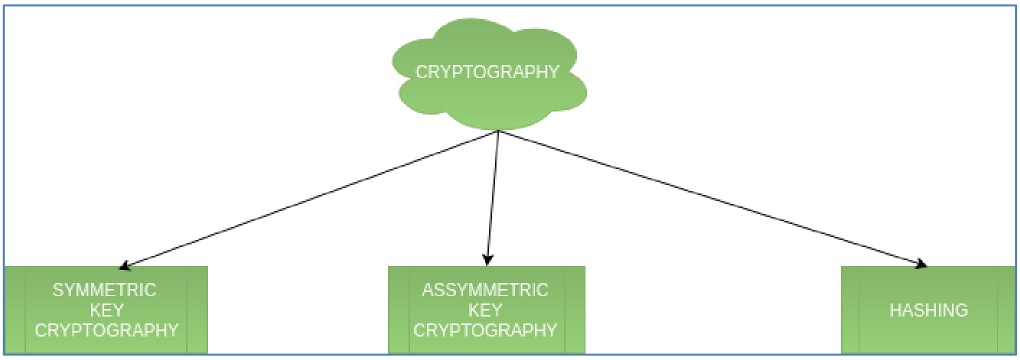
Feature	2G	3G	4G	5G	6G (Speculated)
Technology	GSM (Global System for Mobile)	CDMA (Code Division Multiple Access)	LTE (Long-Term Evolution)	NR (New Radio)	Not standardized yet
Data Speed	Up to 0.3 Mbps (GPRS)	Up to 3.1 Mbps (CDMA2000)	Up to 100 Mbps (LTE)	Up to 10 Gbps (mmWave)	Expected to be faster than 5G
Latency	Higher (100-500 ms)	Lower (100-300 ms)	Lower (30-50 ms)	Ultra-low (1 ms or less)	Aimed for even lower latency
Spectrum Efficiency	Lower	Improved	Further improved	Enhanced	Aimed for even better efficiency
Connection Density	Limited	Improved	Further improved	Much improved	Aimed for even higher density
Coverage	Basic	Expanded	Widespread	Ubiquitous	Aimed for global coverage
Use Cases	Voice Calls, SMS	Basic Data Services	Mobile Internet, Video Streaming	IoT, VR/AR, Critical Communication	Expected to support advanced tech
Technology	TDMA (Time Division Multiple Access)	CDMA (Code Division Multiple Access)	OFDMA (Orthogonal Frequency Division Multiple Access)	Advanced modulation schemes, Massive MIMO	Various advanced technologies speculated

S.NO.	Router	Gateway
1.	It is a hardware device which is responsible for receiving, analyzing and forwarding the data packets to other networks.	It is a device that is used for the communication among the networks which have a different set of protocols.
2.	It supports the dynamic routing.	It does not support dynamic routing.
3.	The main function of a router is routing the traffic from one network to the other.	The main function of a gateway is to translate one protocol to the other.
4.	A router operates on layer 3 and layer 4 of the OSI model.	A gateway operates upto layer 5 of the OSI model.
5.	Working principle of a router is to install routing details for multiple networks and routing traffic based upon the destination address.	5. Working principle of a gateway is to differentiate what is inside the network and what is outside the network.
6.	It is hosted on only the dedicated applications.	It is hosted on dedicated applications, physical servers or virtual applications.
7.	The additional features provided by a router are Wireless networking, Static routing, NAT, DHCP server etc.	The additional features provided by a gateway are network access control, protocol conversion etc.

🖎Cryptography:

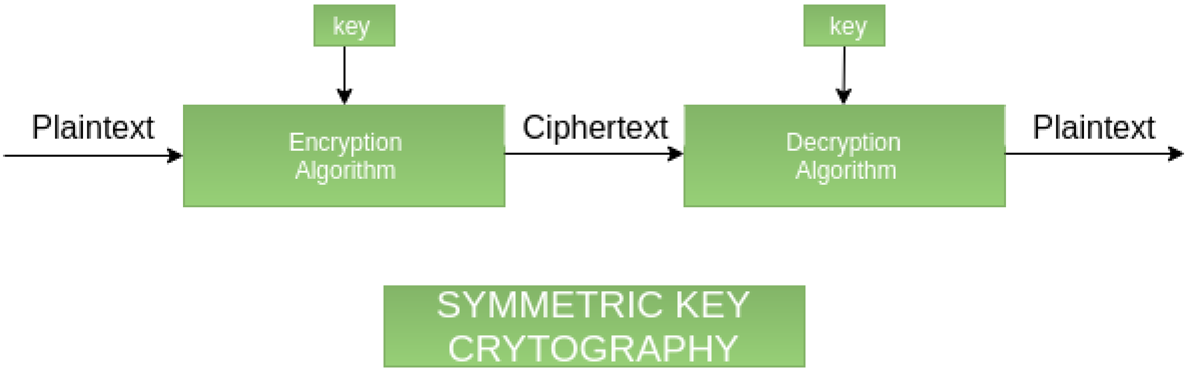
Cryptography is an important aspect when we deal with network security. 'Crypto' means secret or hidden. Cryptography is the science of secret writing with the intention of keeping the data secret.

Cryptography is classified into symmetric cryptography, asymmetric cryptography and hashing. Below are the description of these types.



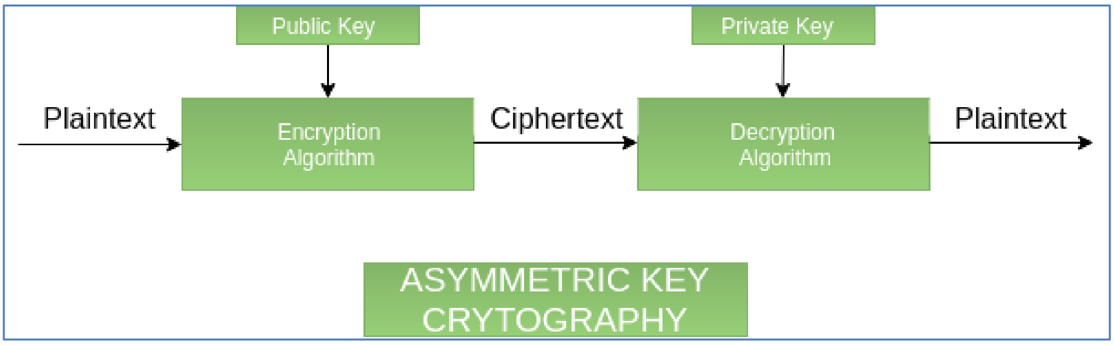
Symmetric key cryptography –

It involves usage of one secret key along with encryption and decryption algorithms which help in securing the contents of the message. The strength of symmetric key cryptography depends upon the number of key bits. It is relatively faster than asymmetric key cryptography. There arises a key distribution problem as the key has to be transferred from the sender to the receiver through a secure channel.



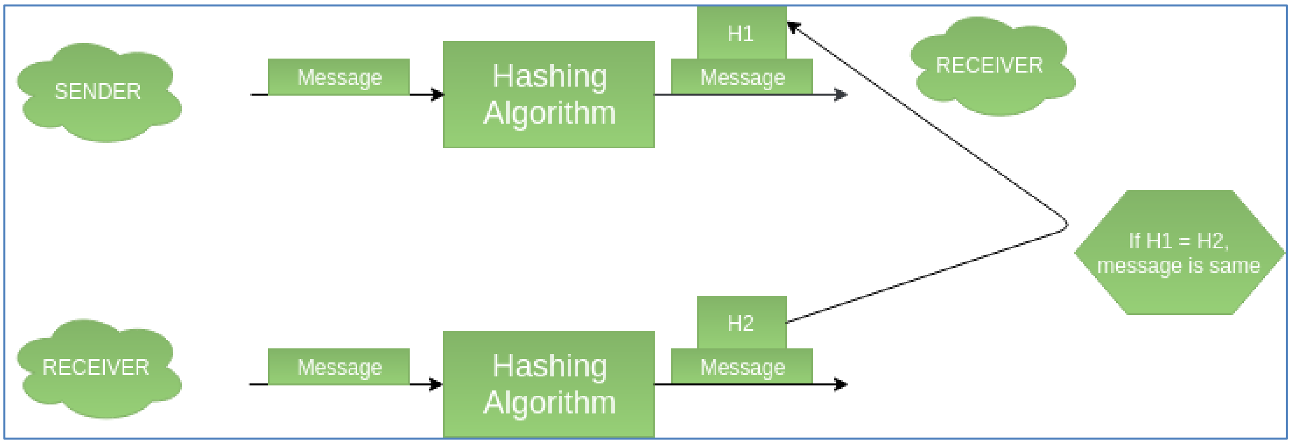
Asymmetric key cryptography -

It is also known as public-key cryptography because it involves usage of a public key along with the secret key. It solves the problem of key distribution as both parties use different keys for encryption/decryption. It is not feasible to use for decrypting bulk messages as it is very slow compared to symmetric key cryptography.

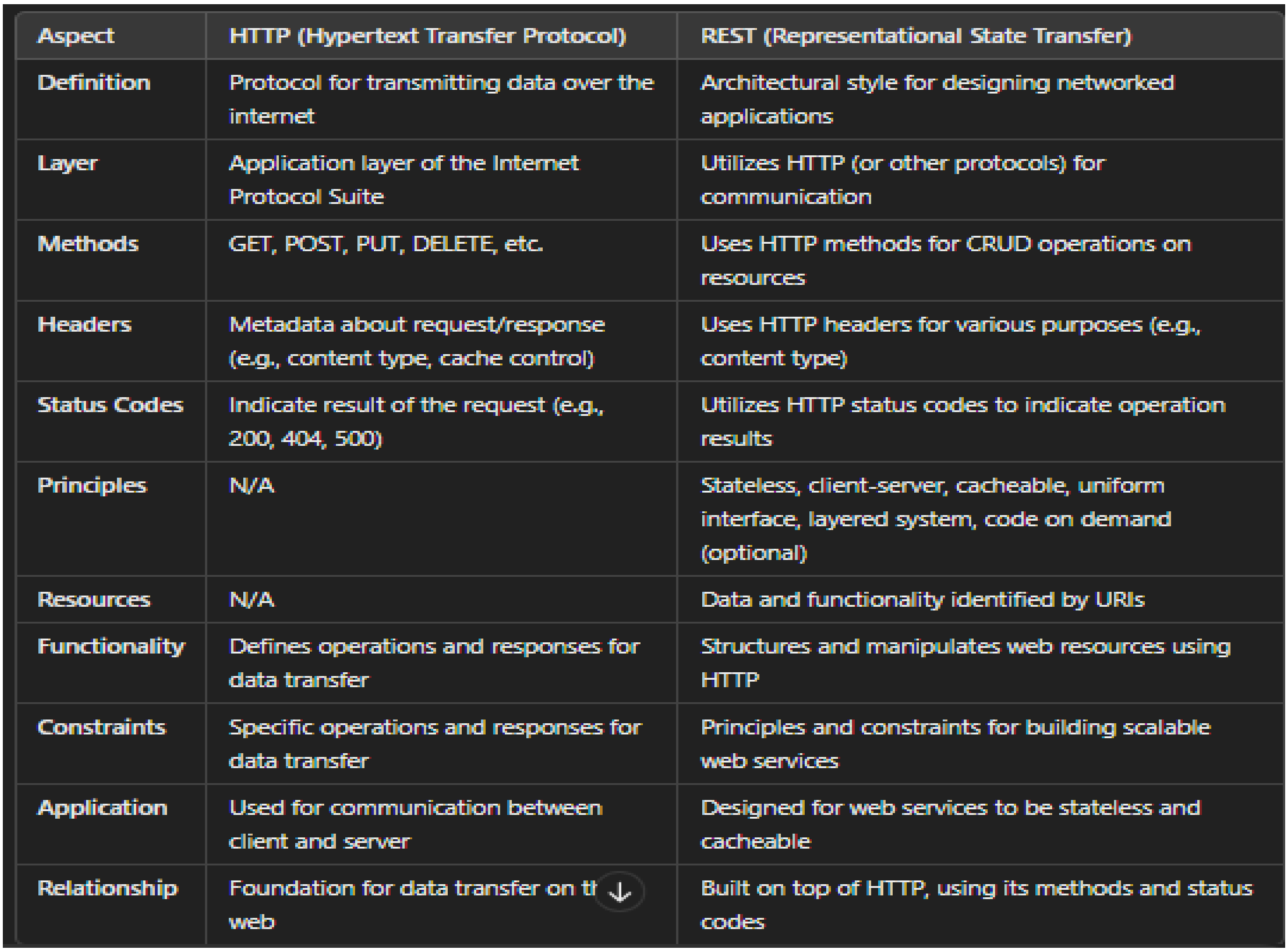


Hashing –

It involves taking the plain-text and converting it to a hash value of fixed size by a hash function. This process ensures the integrity of the message as the hash value on both, sender's and receiver's side should match if the message is unaltered.



- **Encryption** – Process of converting electronic data into another form, called ciphertext, which cannot be easily understood by anyone except the authorized parties. This assures data security.
- **Decryption**– Process of translating code to data.



Aspect	HTTP (Hypertext Transfer Protocol)	REST (Representational State Transfer)
Definition	Protocol for transmitting data over the internet	Architectural style for designing networked applications
Layer	Application layer of the Internet Protocol Suite	Utilizes HTTP (or other protocols) for communication
Methods	GET, POST, PUT, DELETE, etc.	Uses HTTP methods for CRUD operations on resources
Headers	Metadata about request/response (e.g., content type, cache control)	Uses HTTP headers for various purposes (e.g., content type)
Status Codes	Indicate result of the request (e.g., 200, 404, 500)	Utilizes HTTP status codes to indicate operation results
Principles	N/A	Stateless, client-server, cacheable, uniform interface, layered system, code on demand (optional)
Resources	N/A	Data and functionality identified by URIs
Functionality	Defines operations and responses for data transfer	Structures and manipulates web resources using HTTP
Constraints	Specific operations and responses for data transfer	Principles and constraints for building scalable web services
Application	Used for communication between client and server	Designed for web services to be stateless and cacheable
Relationship	Foundation for data transfer on th web	Built on top of HTTP, using its methods and status codes

👉How Hotspot works

A hotspot refers to a physical location where people can access the internet wirelessly, typically using Wi-Fi technology. Here's how a hotspot works:

1. Internet Connection:

- A hotspot requires an internet connection to provide access to the internet. This connection can be established through various means, such as:
  - Wired broadband connection (e.g., DSL, cable, fiber-optic).
  - Cellular data connection (e.g., 4G LTE, 5G).
  - Satellite internet connection.

2. Wireless Access Point:

- The internet connection is shared using a wireless access point (WAP) or router that broadcasts a Wi-Fi signal.
- The WAP/router is configured to create a wireless network with a specific SSID (Service Set Identifier) and security settings (e.g., WPA2 password).

3. Connectivity:

- Users with Wi-Fi-enabled devices (e.g., smartphones, tablets, laptops) can discover and connect to the wireless network provided by the hotspot.
- When users connect to the hotspot, they authenticate using the security credentials (e.g., password) configured on the wireless network.

4. Data Transmission:

- Once connected, users can access the internet using the hotspot's internet connection.
- Data transmitted between the user's device and the internet is encrypted and sent over the Wi-Fi network to the WAP/router.
- The WAP/router forwards the data packets to the internet gateway, which could be a modem, router, or cellular tower, depending on the type of internet connection used by the hotspot.

5. Routing and Address Translation:

- The internet gateway routes the data packets to their destination on the internet, based on their IP addresses.
- If necessary, the gateway performs network address translation (NAT) to translate the private IP addresses of connected devices to a public IP address for communication over the internet.

6. Data Retrieval and Response:

- The requested data (e.g., web pages, files) is retrieved from the destination server on the internet and sent back to the hotspot's internet gateway.
- The gateway forwards the data packets back to the WAP/router, which then transmits the data wirelessly to the user's device connected to the hotspot.

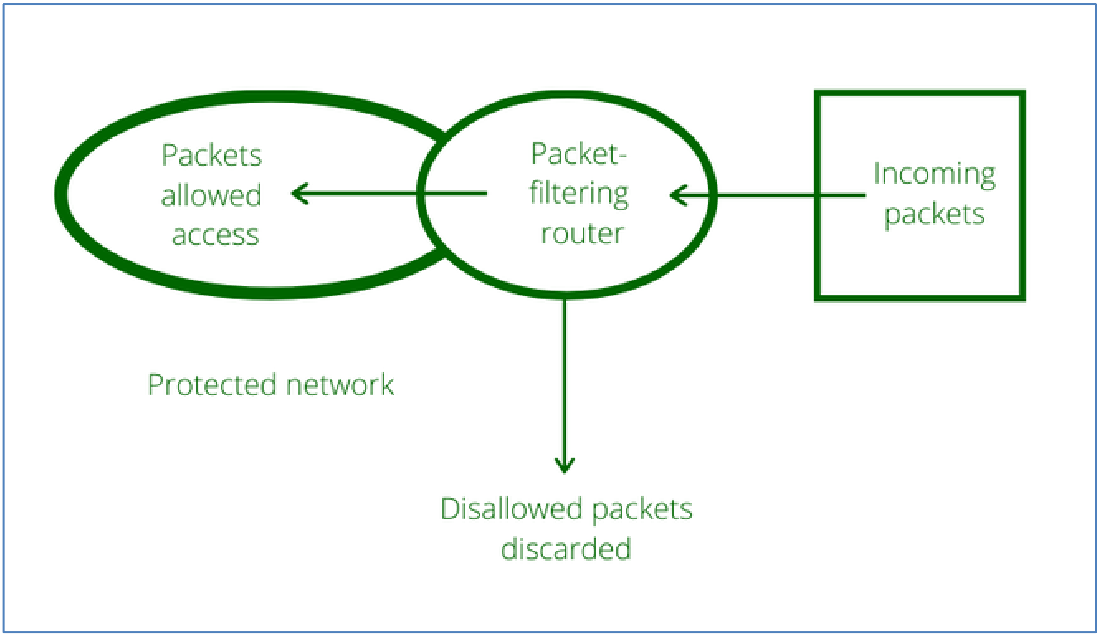
7. Billing and Management (Optional):

- In commercial or public hotspots, users may be required to pay for access to the internet or agree to terms of service before connecting.
- Hotspot operators may use captive portal authentication, which redirects users to a login page where they enter their credentials or accept the terms of service before gaining access.

8. Range and Coverage:

- The range and coverage area of a hotspot depend on factors such as the transmit power of the WAP/router, the presence of obstacles or interference, and environmental conditions.
- Hotspots can provide internet access in public spaces (e.g., cafes, airports, hotels), private residences, or vehicles (e.g., mobile hotspots in cars).

👉**Packet Filters –**

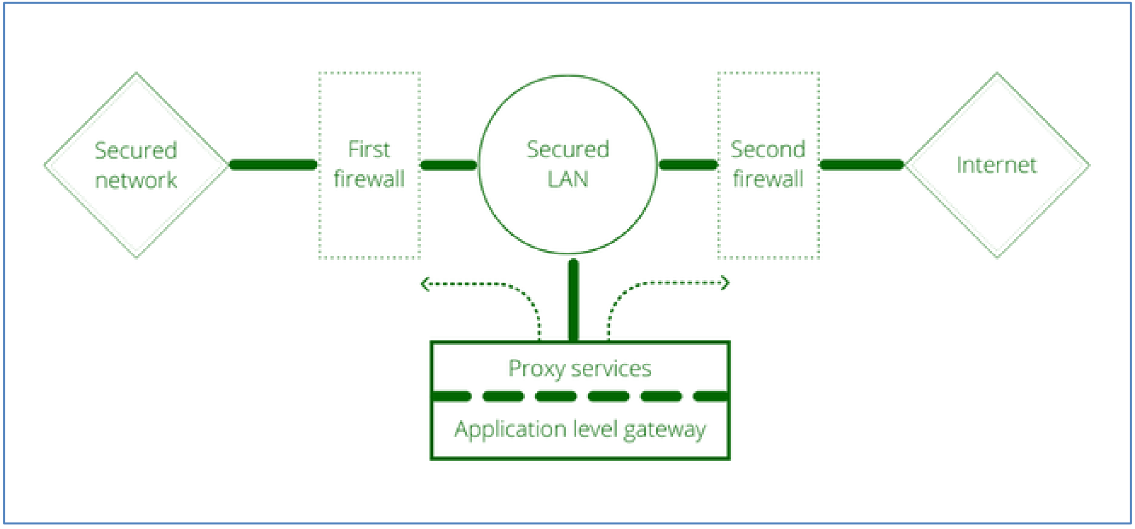


- Packet filter firewall

It works in the network layer of the OSI Model. It applies a set of rules (based on the contents of IP and transport header fields) on each packet and based on the outcome, decides to either forward or discard the packet.
Packet filter firewall controls access to packets on the basis of packet source and destination address or specific transport protocol type. It is done at the OSI (Open Systems Interconnection) data link, network, and transport layers. Packet filter firewall works on the network layer of the OSI model.
Packet filters consider only the most basic attributes of each packet, and they don't need to remember anything about the traffic since each packet is examined in isolation. For this reason, they can decide packet flow very quickly.
Example: Filter can be set to block all UDP segments and all Telnet connections. This type of configuration prevents outsiders from logging onto internal hosts using Telnet and insider from logging onto external hosts using Telnet connections.

Application Gateways –

Application level gateway



-

Application-level gateway is also called a bastion host. It operates at the application level. Multiple application gateways can run on the same host but each gateway is a separate server with its own processes.

These firewalls, also known as application proxies, provide the most secure type of data connection because they can examine every layer of the communication, including the application data.

Example: Consider FTP service. The FTP commands like getting the file, putting the file, listing files, and positioning the process at a particular point in a directory tree. Some system admin blocks put command but permits get command, list only certain files, or prohibit changing out of a particular directory. The proxy server would simulate both sides of this protocol exchange. For example, the proxy might accept get commands and reject put commands.

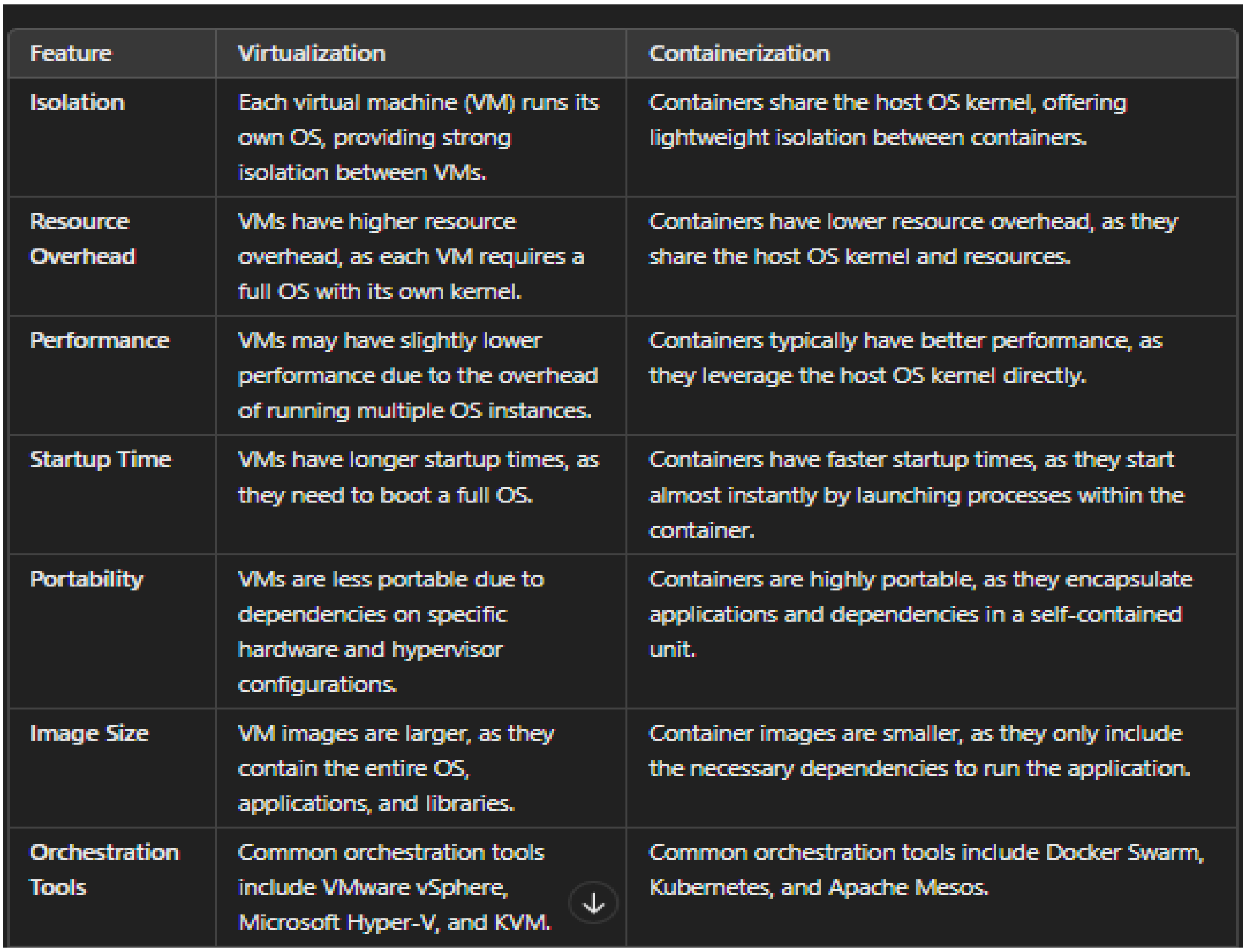
It works as follows:

- Step-1: User contacts the application gateway using a TCP/IP application such as HTTP.
- Step-2: The application gateway asks about the remote host with which the user wants to establish a connection. It also asks for the user id and password that is required to access the services of the application gateway.
- Step-3: After verifying the authenticity of the user, the application gateway accesses the remote host on behalf of the user to deliver the packets.

🖎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.



Feature	Virtualization	Containerization
Isolation	Each virtual machine (VM) runs its own OS, providing strong isolation between VMs.	Containers share the host OS kernel, offering lightweight isolation between containers.
Resource Overhead	VMs have higher resource overhead, as each VM requires a full OS with its own kernel.	Containers have lower resource overhead, as they share the host OS kernel and resources.
Performance	VMs may have slightly lower performance due to the overhead of running multiple OS instances.	Containers typically have better performance, as they leverage the host OS kernel directly.
Startup Time	VMs have longer startup times, as they need to boot a full OS.	Containers have faster startup times, as they start almost instantly by launching processes within the container.
Portability	VMs are less portable due to dependencies on specific hardware and hypervisor configurations.	Containers are highly portable, as they encapsulate applications and dependencies in a self-contained unit.
Image Size	VM images are larger, as they contain the entire OS, applications, and libraries.	Container images are smaller, as they only include the necessary dependencies to run the application.
Orchestration Tools	Common orchestration tools include VMware vSphere, Microsoft Hyper-V, and KVM.	Common orchestration tools include Docker Swarm, Kubernetes, and Apache Mesos.