Computer Network

What is Computer Networking?

Switches connect and help to internally secure computers, printers, servers, and other devices to networks in homes or organizations.

Routers connect networks to other networks and act as dispatchers. They analyze data to be sent across a network, choose the best routes for it, and send it on its way. Routers connect your home and business to the world and help protect information from outside security threats.

MAC and IP addresses uniquely define devices and network connections, respectively, in a network. A MAC address is a number assigned to a network interface card (NIC) by a device's manufacturer. An IP address is a number assigned to a network connection.

Types of computer networks

- a LAN's particular characteristic is that it connects devices that are in a single, limited area.
- Physical connectivity in WANs can be achieved by leased lines, cellular connections, satellite links, and other means.
- An enterprise may use both LANs and WANs across its campus, branches, and data centers.
- Service providers operate WANs to provide connectivity to individual users or organization

What is a Client?

A **client** is a computer hardware device or software that accesses a service made available by a server. The server is often (but not always) located on a separate physical computer.

What is a Server?

A **server** is a physical computer dedicated to run services to serve the needs of other computers. Depending on the service that is running, it could be a file server, database server, home media server, print server, or web server.

What is a Host?

A **host** is a computer, connected to other computers for which it provides data or services over a network.

To simplify this, suppose you want to download an image from another computer on your network. That computer is “hosting” the image and therefore, it is the host computer. On the other hand, if that same computer downloads an image from your computer, your computer becomes the host computer.

Server:

- Can be a physical device or software program
- Installed on a host computer
- Provides specific services
- Serves only clients

Host:

- Is always a physical computer or device
- Can run both server and client programs
- Provides specific services
- Serves multiple users and devices

What is a Host?

In computer networking, a packet is a small unit of data that is transmitted over a network. Packets are used to send data over a variety of networks, including the internet, local area networks (LANs), and wide area networks (WANs).

A packet typically consists of two parts: a header and a payload. The header contains information about the packet, such as its source and destination addresses, the type of data it is carrying, and the sequence number of the packet. The payload is the actual data that is being transmitted.

Packets are used for a variety of reasons. One reason is to improve efficiency. By dividing data into smaller packets, it can be transmitted more efficiently over a network. This is because packets can be routed independently of each other, and they can be sent over different paths to their destination.

Another reason for using packets is to improve reliability. If a packet is lost or damaged during transmission, it can be resent without having to resend the entire message. This is because each packet contains information about its sequence number, so the receiver can tell which packets are missing or damaged.

Packets are also used to improve security. By encrypting the data in a packet, it can be protected from unauthorized access.

What is jitter?

Information is transported from your computer in data packets across the internet. They are usually sent at regular intervals and take a set amount of time. Jitter is when there is a time delay in the sending of these data packets over your network connection. This is often caused by network congestion, and sometimes route changes.
Essentially, the longer data packets take to arrive, the more jitter can negatively impact the video and audio quality.

What is acceptable jitter for the internet?

Low jitter levels are unlikely to have a noticeable impact on your phone connection. Because of this, there are levels of "acceptable jitter." Acceptable jitter is what we are willing to accept as the minimum fluctuation in transmission.
Jitter is measured in milliseconds (ms). A delay of around 30 ms or more can result in distortion and disruption to a call.
For video streaming to work efficiently, jitter should be below 30 ms. If the receiving jitter is higher than this, it can start to slack, resulting in packet loss and problems with audio quality. Also, packet loss shouldn't be more than 1%, and network latency shouldn't go over 150 ms in one direction.

What Does Frame Mean?

In networking, a frame is a unit of data. A frame works to help identify data packets used in networking and telecommunications structures. Frames also help to determine how data receivers interpret a stream of data from a source.

Frames and packets may have different terminology attached to their use depending on the context or industry in question. In general, the frame is a formatting resource for data that needs to be split up into recognizable pieces in order to be interpreted by a receiver.

What is Local Host?

When you call an IP address on your computer, you try to contact another computer on the internet, but when you call the IP address 127.0.0.1, you are communicating with the local host. **Localhost** is always your computer. Your computer is talking to itself when you call the local host.

What is localhost used for?

Developers use the local host to test web applications and programs. Network administrators use the loopback to test network connections. Another use for the localhost is the host's file, where you can use the loopback to block malicious websites.

Bit rate

Network connections can send bits very fast. We measure that speed using the **bit rate**, the number of bits of data that are sent each second.

Latency

Latency is the time between the sending of a data message and the receiving of that message, measured in milliseconds.

Definition of Attenuation in Networking

Attenuation is the loss of signal strength in networking cables or connections. This typically is measured in decibels (dB) or voltage and can occur due to a variety of factors. It may cause signals to become distorted or indiscernible.

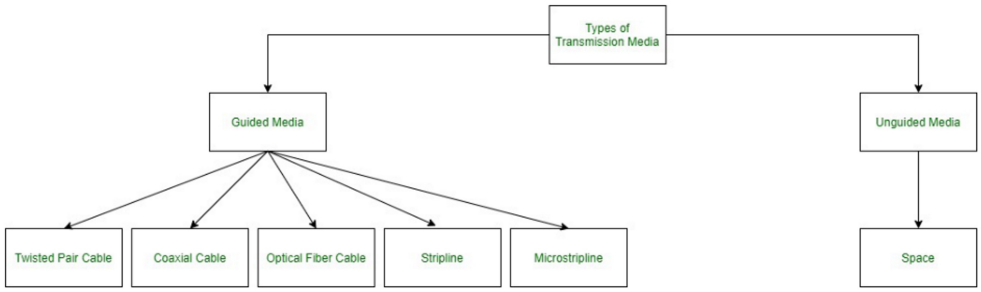
Distortion

Distortion describes an interruption of transmitting signals that cause an unclear reception. Distortion is commonly found in sound generated or received by a computer, video, or display signals and data cables such as network cables.

What's difference between The Internet and The Web ?

Internet is infrastructure while the Web is served on top of that infrastructure. Alternatively, the Internet can be viewed as a big book store while the Web can be viewed as a collection of books on that store.

Web applications use HTTP protocol which is a layer over TCP protocol. Whereas internet applications can use either TCP or UDP protocol.



Network Devices

HUB

Hub is one of the basic icons of networking devices which works at physical layer and hence connect networking devices physically together. Hubs are fundamentally used in networks that use **twisted pair cabling** to connect devices. They are designed to transmit the packets to the other appended devices without altering any of the transmitted packets received. They act as pathways to direct electrical signals to travel along. They transmit the information regardless of the fact if data packet is destined for the device connected or not.

Hub falls in two categories:

Active Hub: They are smarter than the passive hubs. They not only provide the path for the data signals infact they regenerate, concentrate and strengthen the signals before sending them to their destinations. Active hubs are also termed as **'repeaters'**.

Passive Hub: They are more like point contact for the wires to built in the physical network. They have nothing to do with modifying the signals.

Switches

Switches are the linkage points of an Ethernet network. Just as in hub, devices in switches are connected to them through twisted pair cabling. But the difference shows up in the manner both the devices; hub and a switch treat the data they receive. **Hub** works by sending the data to all the ports on the device whereas a **switch** transfers it only to that port which is connected to the destination device. A switch does so by having an in-built learning of the MAC address of the devices connected to it. Since the transmission of data signals are well defined in a **switch** hence the network performance is consequently enhanced. Switches operate in **full-duplex** mode where devices can send and receive data from the switch at the simultaneously unlike in half-duplex mode.

Bridges

A bridge is a computer networking device that builds the connection with the other bridge networks which use the same protocol. It works at the Data Link layer of the OSI Model and connects the different networks together and develops communication between them. It connects two local-area networks; two physical LANs into larger logical LAN or two segments of the same LAN that use the same protocol.

Routers

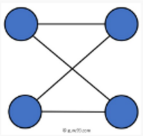
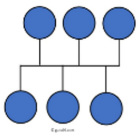
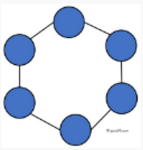
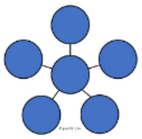
Routers are network layer devices and are particularly identified as Layer- 3 devices of the OSI Model. They process logical addressing information in the Network header of a packet such as IP Addresses. Router is used to create larger complex networks by complex traffic routing. It has the ability to connect dissimilar LANs on the same protocol.

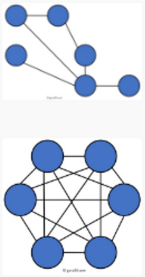
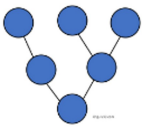
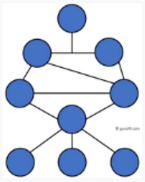
Gateways

Gateway is a device which is used to connect multiple networks and passes packets from one packet to the other network. Acting as the 'gateway' between different networking systems or computer programs, a gateway is a device which forms a link between them. It allows the computer programs, either on the same computer or on different computers to share information across the network through protocols. A router is also a gateway, since it interprets data from one network protocol to another.

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	Grop of receivers
Bandwidth usage	Moderate	High	Moderate
Latency	Low	High	Moderate

Topology	What it is	Image
P2P	The network consists of a direct link between two computers	
Bus	Uses a single cable which connects all the included nodes	
Ring	Every device has exactly two neighboring devices for communication purpose	
Star	All the computers connect with the help of a hub.	

Mesh	The mesh topology has a unique network design in which each computer on the network connects to every other.	
Tree	Tree topologies have a root node, and all other nodes are connected which forming a hierarchy.	
Hybrid Topology	Hybrid topology combines two or more topologies	

Basis	LAN	MAN	WAN
Full-Form	LAN stands for local area network.	MAN stands for metropolitan area network.	WAN stands for wide area network.
Geographic Span	Operates in small areas such as the same building or campus.	Operates in large areas such as a city.	Operates in larger areas such as country or continent.
Ownership	LAN's ownership is private.	MAN's ownership can be private or public.	While WAN also might not be owned by one organization.
Transmission Speed	The transmission speed of a LAN is high.	While the transmission speed of a MAN is average.	Whereas the transmission speed of a WAN is low.
Propagation delay	The propagation delay is short in a LAN.	There is a moderate propagation delay in a MAN.	Whereas, there is a long propagation delay in a WAN.

Congestion	There is less congestion in LAN.	While there is more congestion in MAN.	Whereas there is more congestion than MAN in WAN.
Design & Maintenance	LAN's design and maintenance are easy.	While MAN's design and maintenance are difficult than LAN.	Whereas WAN's design and maintenance are also difficult than LAN as well MAN.
Fault tolerance	There is more fault tolerance in LAN.	While there is less fault tolerance.	In WAN, there is also less fault tolerance.

Noise

Noise is any undesired signal in a communication circuit. Another definition calls noise unwanted disturbances superimposed on a useful signal, which tends to obscure its information content. There are many varieties of noise; however, the four most important to the telecommunication/data communication technologist are thermal noise, intermodulation noise, crosstalk and impulse noise.

Thermal noise

Thermal noise occurs in all transmission media and communication equipment, including passive devices. Every equipment element and the transmission medium itself contribute thermal noise to a communication system if the temperature of that element or medium is above absolute zero.

Intermodulation (IM) noise

Intermediation (IM) Noise is the result of the presence of intermodulation products. If two signals of frequencies F1 and F2 are passed through a nonlinear device or medium, the result will contain IM products that are spurious frequency energy components. IM products may be produced from harmonics of the desired signals in question.

Crosstalk

A disturbance caused by electromagnetic interference, along with a circuit or a cable pair. A telecommunication signal disrupts a signal in an adjacent circuit and can cause the signals to become confused and cross over each other.

OSI Model Defined

The OSI Model (Open Systems Interconnection Model) is a conceptual framework used to describe the functions of a networking system. The OSI model characterizes computing functions into a universal set of rules and requirements in order to support interoperability between different products and software.

Packet Traveling

When data leaves your computer, it is grouped into small chunks called **Packets**. These packets are essentially **little envelopes that carry data across the Internet**.

OSI Layer 1 – Physical

The Physical layer of the OSI model is responsible for the transfer of bits — the 1's and 0's which make up all computer code. Layer 1 is anything that carries 1's and 0's between two nodes.

The actual format of the data on the "wire" can vary with each medium. In the case of Ethernet, bits are transferred in the form of electric pulses. In the case of Wifi, bits are transferred in the form of radio waves. In the case of Fiber, bits are transferred in the form of pulses of light. Repeater simply repeats a signal from one medium to the other, allowing a series of cables to be daisy chained together and increase the range a signal can travel beyond the single cable limit. A Hub is simply a multi-port Repeater. If four devices are connected to a single Hub, anything sent by one device gets repeated to the other three.

OSI Layer 2 – Data Link

The Data Link layer of the OSI model is responsible for interfacing with the Physical layer. Effectively, Layer 2 is responsible for putting 1's and 0's on the wire, and pulling 1's and 0's from the wire. Layer 2 will then group together those 1's and 0's into chunks known as Frames.
The Network Interface Card (NIC) that you plug your Ethernet wire into handles the Layer 2 functionality. It receives signals from the wire, and transmits signals on to the wire.
There is an addressing system that exists at Layer 2 known as the Media Access Control address, or MAC address. The MAC address uniquely identifies each individual NIC. Each NIC is pre-configured with a MAC address by the manufacturer; in fact, it is sometimes referred to as the Burned In Address (BIA)

Aside from your NIC, a Switch also operates at this layer. A Switch's primary responsibility is to facilitate communication within Networks
The overarching function of the Data Link layer is to deliver packets from one NIC to another. Or to put it another way, the role of Layer 2 is to deliver packets from hop to hop.

OSI Layer 3 – Network

The Network layer of the OSI model is responsible for packet delivery from end to end. It does this by using another addressing scheme that can logically identify every node connected to the Internet. This addressing scheme is known as the Internet Protocol address, or the IP Address.It is considered logical because an IP address is not a permanent identification of a computer. Unlike the MAC address which is considered a physical address, the IP address is not burned into any computer hardware by the manufacturer.

Routers are Network Devices that operate at Layer 3 of the OSI model. A Router's primary responsibility is to facilitate communication between Networks. As such, a Router creates a boundary between two networks. In order to communicate with any device not directly in your network, a router must be used.

Question: If we already have a unique L2 addressing scheme on every NIC (like MAC addresses), why do we need yet another addressing scheme at L3 (like IP addresses)? Or vice versa?

The answer is that both addressing schemes accomplish different functions:

- Layer 2 uses MAC addresses and is responsible for packet delivery from hop to hop.
- Layer 3 uses IP addresses and is responsible for packet delivery from end to end.

When a computer has data to send, it encapsulates it in a IP header which will include information like the Source and Destination IP addresses of the two "ends" of the communication.

The IP Header and Data are then further encapsulated in a MAC address header, which will include information like the Source and Destination MAC address of the current "hop" in the path towards the final destination.

OSI Layer 4 – Transport

The Transport layer of the OSI model is responsible for distinguishing network streams.

At any given time on a user's computer there might be an Internet browser open, while music is being streamed, while a messenger or chat app is running. Each of these applications are sending and receiving data from the Internet, and all that data is arriving in the form of 1's and 0's on to that computer's NIC.

Layer 4 accomplishes this by using an addressing scheme known as Port Numbers.

Specifically, two methods of distinguishing network streams exist. They are known as the Transmission Control Protocol (TCP), or the User Datagram Protocol (UDP).

Both TCP and UDP have 65,536 port numbers (each), and a unique application stream is identified by both a Source and Destination port (in combination with their Source and Destination IP address).

Layer 2 is responsible for hop to hop delivery, and Layer 3 is responsible for end to end delivery, it can be said that **Layer 4 is responsible for service to service delivery**.

OSI Layer 5, 6, and 7

The Session, Presentation, and Application layers of the OSI model handle the final steps before the data transferred through the network (facilitated by layers 1-4) is displayed to the end user.

From a purely Network Engineering perspective, the distinction between Layers 5, 6, and 7 is not particularly significant. In fact, there is another popular Internet communication model known as the TCP/IP model, which groups these three layers into one single encompassing layer.

The last item we need to discuss before we move on from the OSI Model is that of **Encapsulation** and **Decapsulation**. These terms refer to **how data is moved through the layers from top to bottom when sending and from bottom to top when receiving**.

As the data is handed from layer to layer, each layer adds the information it requires to accomplish its goal before the complete datagram is converted to 1s and 0s and sent across the wire. For example:

- Layer 4 will add a TCP header which would include a Source and Destination port
- Layer 3 will add an IP header which would include a Source and Destination IP address
- Layer 2 would add an Ethernet header which would include a Source and Destination MAC address

Host

The term **host** is a generic term that implies **any sort of end-device on the Internet**. In typical internet communication or network traffic, the two hosts in communication are often labelled as the Client or the Server. The **Client is the entity initiating the request** and is looking to acquire a piece of information or data or a service. While the **Server is the entity receiving the request** and has the information, data, or service that the Client wants.

Network

A Network is simply two or more connected devices

Switch

A Switch is a network device whose primary purpose is to facilitate communication within networks. Switches operate at Layer 2 of the OSI model, which means they only look into each data-gram up to the Layer 2 header. The Layer 2 header contains information that enables hop to hop delivery, such as the Source and Destination MAC address.

Router

A Router is a network device whose primary purpose is to facilitate communication between networks. Each interface on a router creates a network boundary.

Routers operate at Layer 3 of the OSI Model, which means they only look into each datagram up to the Layer 3 header. The Layer 3 header contains information that enables end to end delivery, such as the Source and Destination IP Address.

Address Resolution Protocol (ARP)

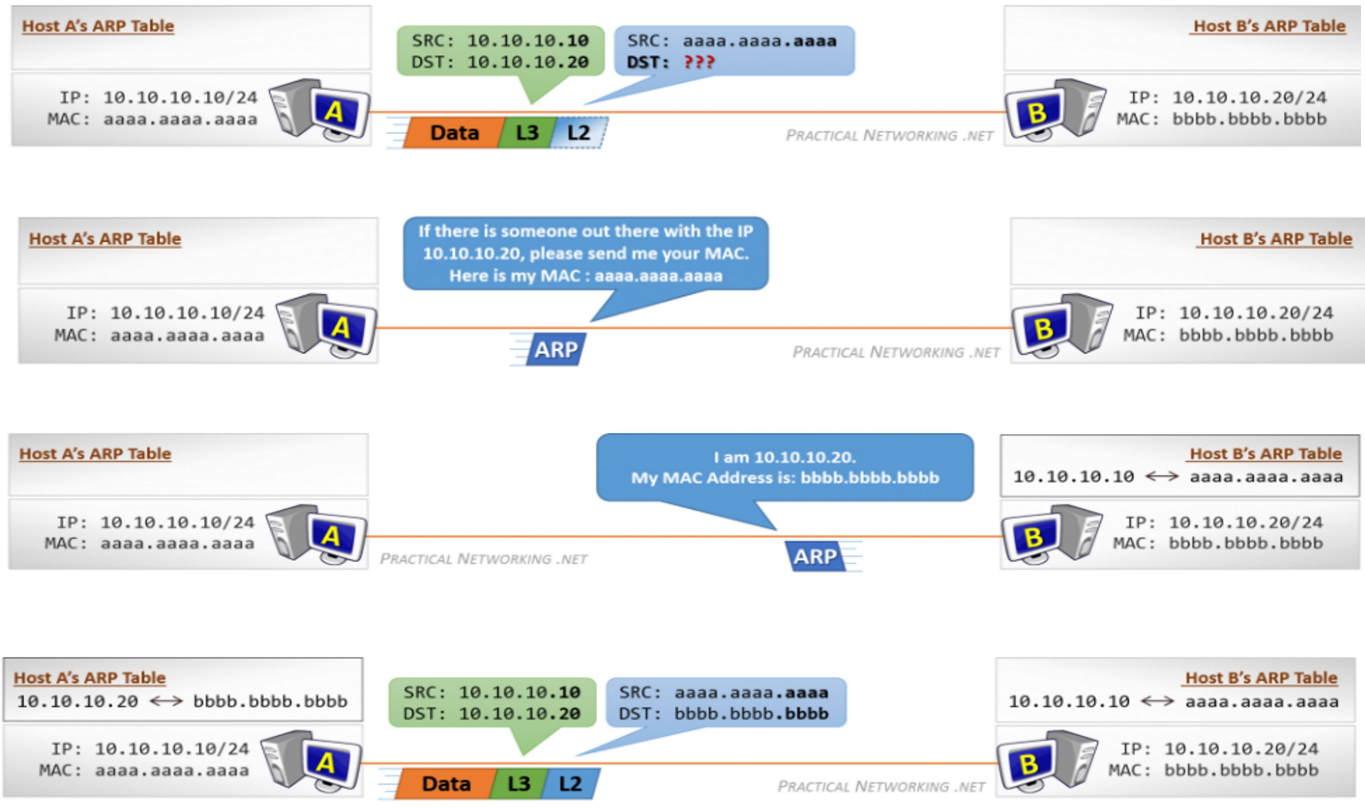
Earlier we discussed that MAC addresses are a Layer 2 addressing scheme. We also discussed that IP addresses are a Layer 3 addressing scheme. What bridges these two addressing schemes is the Address Resolution Protocol (ARP).

Typically, when two hosts are communicating, they already know each other's IP address. They can know each other's IP address from a variety of methods: sometimes it is manually provided by a user, sometimes by another protocol (often DNS). However, what is definitely not known is their MAC addresses. The hosts will use ARP to discover the appropriate MAC address. To put it another way, ARP will use the known IP address, and discover the unknown MAC address. The discovered mapping is then added and stored in an ARP Table, which is a mapping of IP addresses to correlating MAC addresses.

To summarize ARP's operation:

- When a Client is speaking to a host in the same network, it will ARP for the MAC address of the host
- When a Client is speaking to a host in a different network, it will ARP for the MAC address of the Default Gateway

Host to Host Communication



Host to Host through a Switch

Switch Functions

A Switch primarily has four functions: Learning, Flooding, Forwarding, and Filtering

Learning

One of the goals of the Switch is to create a **MAC Address Table**, mapping each of its **switchports to the MAC address** of the connected devices. The MAC address table starts out empty, and every time a Switch receives anything, it takes a look at the Source MAC address field of the incoming frame. It uses the Source MAC and the switchport the frame was received on to build an entry in the MAC Address Table.

Flooding

However, despite the learning process above, it is unavoidable that a Switch will at some point receive a frame destined to a MAC address of which the Switch does not know the location.

In such cases, the Switch's only option is to simply duplicate the frame and send it out *all* ports. This action is known as Flooding.

Flooding assures that *if* the intended device exists and *if* it is connected to the switch, it will definitely receive the frame.

Of course, so will every other device connected to that particular Switch. And though not ideal, this is perfectly normal. The NIC of each connected device will receive the frame and take a look at the Destination MAC address field. If they are not the intended recipient, they will simply silently drop the frame.

If they *are* the intended device, however, then the Switch can rest satisfied knowing it was able to deliver the frame successfully.

Moreover, when the intended device receives the frame, a response will be generated, which when sent to the Switch will allow the switch to learn and create a MAC Address Table mapping that unknown device to its switchport.

Forwarding

Ideally, of course, the Switch will have an entry in its MAC Address Table for every Destination MAC it comes across.

When this happens, the Switch happily forwards the frame out the appropriate switchport.

There are three methods by which a Switch can forward frames. They are briefly described below.

- **Store and Forward** – The Switch copies the entire frame (header + data) into a memory buffer and inspects the frame for errors before forwarding it along. This method is the slowest, but allows for the best error detection and additional features like prioritizing certain types of traffic for faster processing.
- **Cut-Through** – The Switch stores nothing, and inspects only the bare minimum required to read the Destination MAC address and forward the frame. This method is the quickest, but provides no error detection or potential for additional features.
- **Fragment Free** – This method is a blend of the prior two. The Switch inspects only the first portion of the frame (64 bytes) before forwarding the frame along. If a transmission error occurred, it is typically noticed within the first 64 bytes. As such, this method provides "good enough" error detection, while gaining the speed and efficiency of avoiding storing the entire frame in its memory before forwarding it

Filtering

And finally, the last function of the switch is filtering. Mainly, this function states that a Switch will never forward a frame back out the same port which received the frame.

Most commonly, this happens when a Switch needs to flood a frame — the frame will get duplicated and sent out every switchport *except the switchport which received the frame*.

Rarely, a host will send a frame with a destination MAC address of itself. This is usually a host experiencing some sort of error condition or being malicious. Either way, when this happens, the Switch simply discards the frame.

Broadcasts

There is often some confusion about a switch in regards to a Broadcast and a Switch's flooding behavior. The confusion is understandable, because the end result is the same, but it is also important to understand the distinction.

A Broadcast is a frame addressed to everyone on the local network (ffff.ffff.ffff), and Flooding is an action a switch can take. A broadcast frame, by definition, will always be flooded by a switch. But a switch will never broadcast a frame (since broadcasting is not a function of a switch).

Host to Host through a Router

Router Functions

Populating a Routing Table

Routing Table is the map of all networks in existence. The Routing Table starts empty, and is populated as the Router learns of new routes to each network.

The simplest method is what is known as a Directly Connected route. Essentially, when a Router interface is configured with a particular IP address, the Router will know the Network to which it is directly attached.

But it is very likely it might have to one day forward a packet to that network. Therefore, there must exist another way of learning networks, beyond simply what the router is directly connected to.

That other way is known as a Static Route. A Static Route is a route which is manually configured by an administrator. It would be as if you explicitly told R1 that the 33.33.33.x network exists behind R2, and to get to it, R1 has to send packets to R2's interface (configured with the IP address 22.22.22.2).

In the end, after R1 learned of the two Directly Connected routes, and after R1 was configured with the one Static Route, R1 would have a Routing Table that looked like this image.

The Routing Table is populated with many Routes. Each Route contains a mapping of Networks to Interfaces or Next-Hop addresses.

Every time a Router receives a packet, it will consult its Routing Table to determine how to forward the packet.

Again, the Routing Table is a map of every network that exists (from the perspective of each router). If a router receives a packet destined to a network it does not have a route for, then as far as that router is concerned, that network must not exist. Therefore, a router will discard a packet if its destination is in a network not in the Routing Table.

Finally, there is a third method for learning routes known as Dynamic Routing. This involves the routers detecting and speaking to one another automatically to inform each other of their known routes. There are various protocols that can be used for Dynamic Routing, each representing different strategies

Populating an ARP Table

The Address Resolution Protocol (ARP) is the bridge between Layer 3 and Layer 2. When provided with an IP address, ARP resolves the correlating MAC address. Devices employ ARP to populate an ARP Table, or sometimes called an ARP Cache, which is a mapping of IP address to MAC addresses.

A router will use its Routing Table to determine the next IP address which should receive a packet. If the Route indicates the destination exists on a directly connected network, then the "next IP address" is the Destination IP address of the packet – the final hop for that packet.

Either way, the Router will use a L2 header as the vessel to deliver the packet to the correct NIC.

Unlike the Routing Table, the ARP Table is populated 'as needed'. Which means in the image above, R1 will not initiate an ARP Request for Host B's MAC address until it has a packet which must be delivered to Host B.

But as we discussed before, an ARP Table is simply a mapping of IP addresses to MAC addresses. When R1's ARP Table will be fully populated, it will look like this image.

Top 9 Networking Command

1. Ping

Ping is used to testing a network host capacity to interact with another host. Just enter the command Ping, followed by the target host's name or IP address.

2. NetStat

Netstat is a Common TCP – IP networking command-line method present in most

Windows, Linux, UNIX, and other operating systems. The netstat provides the statistics and information in the use of the current TCP-IP Connection network about the protocol.

3. Ip Config

The command IP config will display basic details about the device's IP address configuration.

4. Hostname

To communicate with each and other, the computer needs a unique address. A hostname can be alphabetic or alphanumeric and contain specific symbols used specifically to define a specific node or device in the network.

5. Tracert

The tracert command is a **Command Prompt** command which is used to get the network packet being sent and received and the number of hops required for that packet to reach to target. This command can also be referred to as a traceroute.
The syntax for Tracert Command
`tracert [-d] [-h MaxHops] [-w TimeOut]  target`

6. Nslookup

It provides name server information for the DNS (Domain Name System), i.e. the default DNS server's name and IP Address.
The syntax for Nslookup is as follows.
`Nslookup`
or
`Nslookup [domain_name]`

7. Route

In IP networks, routing tables are used to direct packets from one subnet to another. The Route command provides the device's routing tables

8. ARP

ARP stands for Address Resolution Protocol. Although network communications can readily be thought of as an IP address, the packet delivery depends ultimately on the media access control (MAC). This is where the protocol for address resolution comes into effect. You can add the remote host IP address, which is an arp -a command, in case you have issues to communicate with a given host. The ARP command provides information like Address, Flags, Mask, IFace, Hardware Type, Hardware Address, etc.

9. Path Ping

We discussed the Ping command and the Tracert command. There are similarities between these commands. The pathping command which provides a combination of the best aspects of Tracert and Ping.
This command takes 300 seconds to gather statistics and then returns reports on latency and packet loss statistics at intermediate hops between the source and the target in more detail than those reports provided by Ping or Tracert commands.

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 Secure (HTTPS), could be a combination of the Hypertext Transfer Protocol with the SSL/TLS(Secure Sockets Layer/Transport Layer Security) convention to supply encrypted communication and secure distinguishing proof of an arranged web server. 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).

An SSL certificate also includes identifying information about a website, including its domain name and, optionally, identifying information about the site’s owner. If the web server’s SSL certificate is signed by a publicly trusted certificate authority (CA), like SSL.com, digitally signed content from the server will be trusted by end users’ web browsers and operating systems as authentic.

What is TLS?

TLS (Transport Layer Security), released in 1999, is the successor to the SSL (Secure Sockets Layer) protocol for authentication and encryption.

What is an API Gateway?

An API Gateway acts as a mediator between client applications and backend services in microservices architecture. It is a software layer that functions as a single endpoint for various APIs performing tasks such as request composition, routing, and protocol translation. The API gateway controls requests and responses by managing the traffic of APIs while enforcing security policies. This simplifies API management by providing one central point of control which aids developers in focusing on building individual services rather than being encumbered by complex networks of APIs.

API Gateway vs Microservices

As organizations adopt microservices architecture, API gateways are becoming increasingly popular. The gateway acts as a single entry point for all backend services and simplifies development, deployment and management of the system for developers. Microservices present unique challenges such as managing cross-cutting concerns and service discovery, but a well-implemented API gateway can help address these issues.

Each backend service is designed to function as an independent application in a microservices architecture which can make it tricky to navigate client requests correctly or merge multiple services into one response. Building modern applications often requires dealing with numerous backends that may have separate routes or interfaces that must be handled uniquely. Enter the API gateway – it addresses this challenge by functioning as a singular interface between multiple backends, enabling developers to handle request-processing flow seamlessly from end-to-end.

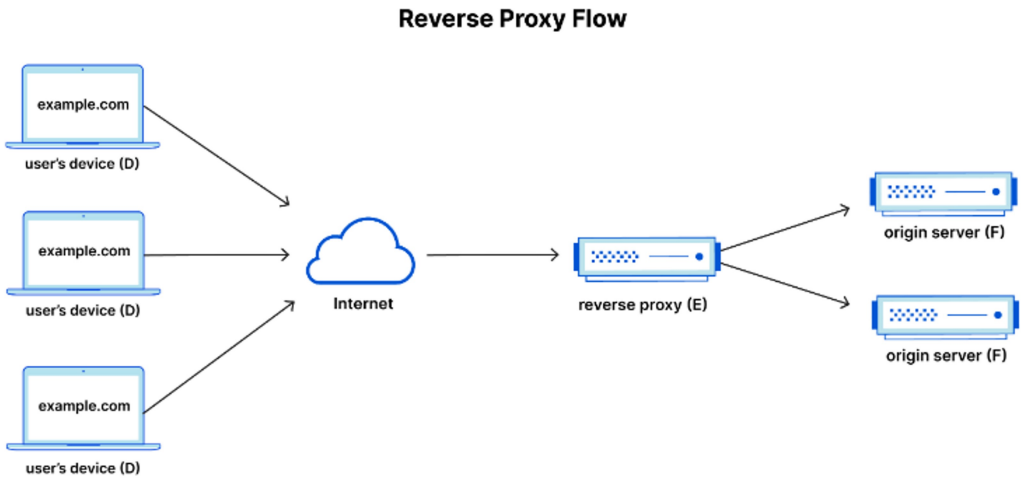
API Gateway Features

API Gateway technology offers a range of benefits such as efficient management of incoming requests that easily routes them to pertinent backend services. Moreover, it can automatically translate protocols so that clients can interact with the service effortlessly.

- **API Traffic Management:** Businesses can now simplify their complex backend systems to ensure seamless user experiences. An API gateway manages incoming requests and routes them based on key factors such as request path, headers, and query parameters, among others. It allows for efficient distribution of traffic and ensures proper load balancing among target endpoints.
- **Protocol Translation:** When using an API Gateway, differentiation is resolved through its ability to convert one protocol into another. By translating data transmission modes at ease, the gateway makes interaction between clients and back-end services much more straightforward.
- **Caching:** This is one key aspect that plays a critical role by enabling frequent storage of commonly used data so that back-end infrastructure handles lesser traffic while achieving optimum performance levels.
- **Load Balancing:** By implementing Load Balancing through an API Gateway, incoming requests can be effectively shared among multiple instances of a backend service to improve both the scalability and availability of that service.
- **Developer Portal:** Developers can take full advantage of an extensive developer portal made available through the implementation of an API Gateway. With the aid of this inclusive platform, they can easily discover APIs alongside tools for testing and consumption. Additionally, these resourceful sites contain helpful documentation, code samples and numerous other assets allowing for quick starts.

What is a reverse proxy?

A reverse proxy is a server that sits in front of web servers and forwards client (e.g. web browser) requests to those web servers. Reverse proxies are typically implemented to help increase security, performance, and reliability.



Below we outline some of the benefits of a reverse proxy:

- Load balancing - A popular website that gets millions of users every day may not be able to handle all of its incoming site traffic with a single origin server. Instead, the site can be distributed among a pool of different servers, all handling requests for the same site. In this case, a reverse proxy can provide a load balancing solution which will distribute the incoming traffic evenly among the different servers to prevent any single server from becoming overloaded. In the event that a server fails completely, other servers can step up to handle the traffic.

- **Protection from attacks** - With a reverse proxy in place, a web site or service never needs to reveal the IP address of their origin server(s). This makes it much harder for attackers to leverage a targeted attack against them, such as a DDoS attack (Distributed Denial-of-Service). Instead the attackers will only be able to target the reverse proxy, such as Cloudflare's CDN, which will have tighter security and more resources to fend off a cyber attack.

- Global server load balancing **(GSLB)** - In this form of load balancing, a website can be distributed on several servers around the globe and the reverse proxy will send clients to the server that's geographically closest to them. This decreases the distances that requests and responses need to travel, minimizing load times.

- **Caching** - A reverse proxy can also cache content, resulting in faster performance.

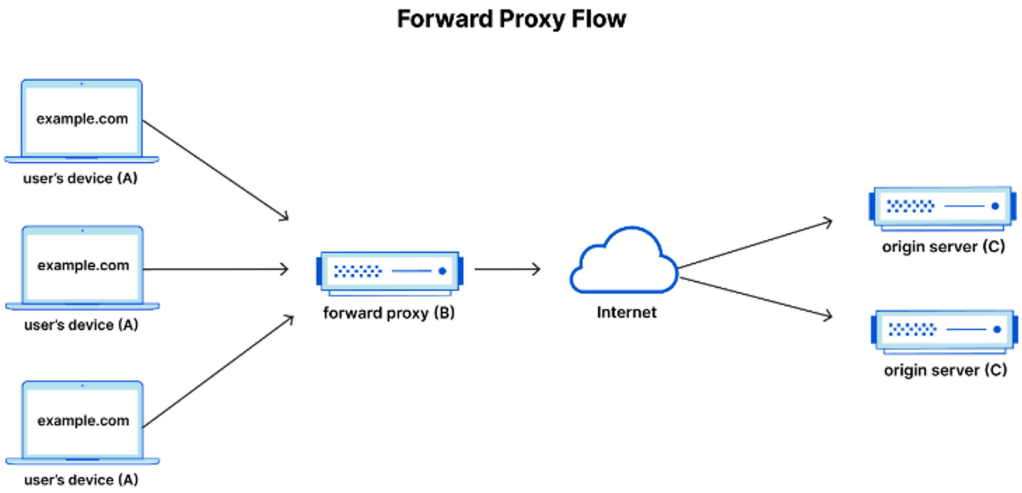
- **SSL encryption** - Encrypting and decrypting SSL (or TLS) communications for each client can be computationally expensive for an origin server. A reverse proxy can be configured to decrypt all incoming requests and encrypt all outgoing responses, freeing up valuable resources on the origin server.

How to implement a reverse proxy

Some companies build their own reverse proxies, but this requires intensive software and hardware engineering resources, as well as a significant investment in physical hardware. One of the easiest and most cost-effective ways to reap all the benefits of a reverse proxy is by signing up for a CDN (content delivery network) service.

What is a proxy server?

A forward proxy, often called a proxy, proxy server, or web proxy, is a server that sits in front of a group of client machines. When those computers make requests to sites and services on the Internet, the proxy server intercepts those requests and then communicates with web servers on behalf of those clients, like a middleman.



Why would anyone add this extra middleman to their Internet activity? There are a few reasons one might want to use a forward proxy:

- **To avoid state or institutional browsing restrictions** - Some governments, schools, and other organizations use firewalls to give their users access to a limited version of the Internet.

- **To block access to certain content** - Conversely, proxies can also be set up to block a group of users from accessing certain sites.

- **To protect their identity online** - In some cases, regular Internet users simply desire increased anonymity online, but in other cases, Internet users live in places where the government can impose serious consequences to political dissidents. Criticizing the government in a web forum or on social media can lead to fines or imprisonment for these users. If one of these dissidents uses a forward proxy to connect to a website where they post politically sensitive comments, the IP address used to post the comments will be harder to trace back to the dissident. Only the IP address of the proxy server will be visible.

What Is Load Balancing?

Load balancing refers to efficiently distributing incoming network traffic across a

group of backend servers, also known as a server farm or server pool.
Modern high-traffic websites must serve hundreds of thousands, if not millions, of concurrent requests from users or clients and return the correct text, images, video, or application data, all in a fast and reliable manner. To cost-effectively scale to meet these high volumes, modern computing best practice generally requires adding more servers.
A load balancer acts as the "traffic cop" sitting in front of your servers and routing client requests across all servers capable of fulfilling those requests in a manner that maximizes speed and capacity utilization and ensures that no one server is overworked, which could degrade performance. If a single server goes down, the load balancer redirects traffic to the remaining online servers. When a new server is added to the server group, the load balancer automatically starts to send requests to it.

Load Balancing Algorithms

Different load balancing algorithms provide different benefits; the choice of load balancing method depends on your needs:

- **Round Robin** – Requests are distributed across the group of servers sequentially.
- **Least Connections** – A new request is sent to the server with the fewest current connections to clients. The relative computing capacity of each server is factored into determining which one has the least connections.
- **Least Time** – Sends requests to the server selected by a formula that combines the
  fastest response time and fewest active connections. Exclusive to NGINX Plus.
- **Hash** – Distributes requests based on a key you define, such as the client IP address or the request URL.
- **IP Hash** – The IP address of the client is used to determine which server receives the request.
- **Random with Two Choices** – Picks two servers at random and sends the request to the one that is selected by then applying the Least Connections algorithm.

Benefits of Load Balancing

- Reduced downtime
- Scalable
- Redundancy
- Flexibility
- Efficiency

Traditional ARP

the Address Resolution Protocol (ARP) is the process by which a known L3 address is mapped to an unknown L2 address. The purpose for creating such a mapping is so a packet's L2 header can be properly populated to deliver a packet to the next NIC in the path between two end points.

The "next NIC" in the path will become the target of the ARP request.

If a host is speaking to another host on the *same* IP network, the target for the ARP request is the other host's IP address. If a host is speaking to another host on a *different* IP network, the target for the ARP request will be the Default Gateway's IP address.

In the same way, if a Router is delivering a packet to the destination host, the Router's ARP target will be the Host's IP address. If a Router is delivering a packet to the next Router in the path to the host, the ARP target will be the other Router's Interface IP address – as indicated by the relative entry in the Routing table.

ARP Process

The Address Resolution itself is a two step process – a request and a response.

It starts with the initiator sending an ARP Request as a broadcast frame to the entire network. This request *must* be a broadcast, because at this point the initiator does not know the target's MAC address, and is therefore unable to send a unicast frame to the target.

Since it was a broadcast, all nodes on the network will receive the ARP Request. All nodes will take a look at the content of the ARP request to determine whether they are the intended target. The nodes which are *not* the intended target will silently discard the packet.

The node which *is* the target of the ARP Request will then send an ARP Response back to the original sender. Since the target knows who sent the initial ARP Request, it is able to send the ARP Response unicast, directly back to the initiator.

What Is Horizontal Scaling?

Horizontal scaling is a strategy used to enhance the performance of a dedicated server node by adding more server instances to the existing pool of servers so that the load can be equally distributed. Horizontal scaling is also known as scaling out the infrastructure.
In horizontal scaling, we do not change the capacity of the individual server. Instead, we decrease the load on individual servers. We implement several connected ideas to achieve this effect, such as a distributed file system, clustering, and load–balancing.
To counter this slowdown, you can add another server to the network. This way, the workload is distributed evenly among the servers.
The recent increase in online traffic has made many popular websites use horizontal scaling. The list includes instantly recognizable names such as Gmail and YouTube, Yahoo, Facebook, eBay, and Amazon.
Cassandra and MongoDB are two great examples of horizontal scaling solutions.

Advantages of Horizontal Scaling

1. Easily scalable tools.
2. Easy to upgrade.
3. Better use of smaller systems.
4. The cost of implementing is less expensive compared to scaling up.
5. Horizontal scaling can be used to implement Infinite Scale, where you can use endless instances to enable limitless growth.

Disadvantages of Horizontal Scaling

1. The architectural design is highly complicated.
2. You might have to pay high licensing fees.
3. Horizontal scaling solutions can increase your utility costs, such as cooling and electricity.

What is Vertical Scaling?

Vertical Scaling is an attempt to increase the capacity of a single machine. Here the resources, such as processing power, storage, memory, and bandwidth, are added to an existing infrastructure node. Vertical Scaling is also called the Scale-up approach.
Vertical Scaling is implemented to increase the capacity of existing hardware or software capacity by adding additional resources. It can enhance your server architecture without significantly affecting your infrastructure. However, you should know that any vertical scaling scheme could get as big as the size of the individual server.
Good examples of Vertical Scaling are MySQL and Amazon RDS.

Advantages of Vertical Scaling

1. Reduced software costs as the underlying hardware nodes often don't increase.
2. Easy Implementation.
3. Lower licensing fees.

4. Vertical scaling solutions often consume less power.
5. Cooling costs are lower than horizontal scaling.
6. Application compatibility is maintained.

Disadvantages of Vertical Scaling

1. The limited scope of scaling.
2. Greater risk of outages and hardware failures.
3. Finite scope of upgradeability in the future.
4. The cost of implementation is expensive.

What is caching?

Caching is the process of storing copies of files in a cache, or temporary storage location, so that they can be accessed more quickly. Web browsers cache HTML files, JavaScript, and images in order to load websites more quickly, while DNS servers cache DNS records for faster lookups and CDN servers cache content to reduce latency.

What does a browser cache do?

Every time a user loads a webpage, their browser has to download quite a lot of data in order to display that webpage. To shorten page load times, browsers cache most of the content that appears on the webpage, saving a copy of the webpage's content on the device's hard drive. This way, the next time the user loads the page, most of the content is already stored locally and the page will load much more quickly. Browsers store these files until their time to live (TTL) expires or until the hard drive cache is full. (TTL is an indication of how long content should be cached.) Users can also clear their browser cache if desired.

What does clearing a browser cache accomplish?

Once a browser cache is cleared, every webpage that loads will load as if it is the first time the user has visited the page. If something loaded incorrectly the first time and was cached, clearing the cache can allow it to load correctly. However, clearing one's browser cache can also temporarily slow page load times.

What is CDN caching?

A CDN, or content delivery network, caches content (such as images, videos, or webpages) in proxy servers that are located closer to end users than origin servers. (A proxy server is a server that receives requests from clients and passes them along to other servers.) Because the servers are closer to the user making the request, a CDN is able to deliver content more quickly.

VIP

A Virtual IP (VIP) address is a concept used in computer networking and systems to abstract and manage network resources. It's an IP address that is not assigned to a specific physical device but rather to a group of servers, devices, or network interfaces.

Here's how it typically works:

1. High Availability and Load Balancing: VIPs are often used in high-availability configurations or for load balancing across multiple servers. When clients send requests to a VIP, a device or software (like a load balancer) forwards the requests to one of the actual servers, distributing the load and improving overall system performance.
2. Failover and Redundancy: In a high-availability setup, if one server fails, the VIP can be quickly reassigned to another server, ensuring continuous service availability without requiring clients to change their connection settings.
3. Scalability: VIPs can also be used to seamlessly scale services by adding more servers and directing traffic to them as needed. This supports applications that require high scalability, such as web servers serving a large number of requests.
4. Flexibility: The use of VIPs allows for flexibility in managing network configurations without affecting the clients directly.

What is Container Networking?

Container Networking is an emerging application sandboxing mechanism used in home desktops and web-scale enterprise networking solutions similar in concept to a virtual machine. Isolated inside the container from the host and all other containers are a full-featured Linux environment with its own users, file system, processes, and network stack. All applications inside the container are permitted to access or modify files or resources available inside the container only.

It is possible to run multiple containers at the same time, each with their own installations and dependencies. This is particularly useful in instances when newer versions of an application may require a dependency upgraded that may cause conflicts with other application dependencies running on the server. Unlike virtual machines, containers share host resources rather than fully simulating all hardware on the computer, making containers smaller and faster than virtual machines and reducing overhead. Particularly in the context of web-scale applications, containers were designed as a replacement to VMs as a deployment platform for microservice architectures.

Containers also have the characteristic of portability, for example, Docker, a container engine, allows developers to package a container and all its dependencies together. That container package can then be made available to download. Once downloaded, the container can immediately be run on a host.

Containerization or virtualization: What’s the right path for you?

Virtualization enables you to run multiple operating systems on the hardware of a single physical server, while containerization enables you to deploy multiple applications using the same operating system on a single virtual machine or server.

Differentiating Performance from Scalability

- Response time: This is the most widely used metric of performance and it is simply a direct measure of how long it takes to process a request.
- Throughput: A straightforward count of the number of requests that the application can process within a defined time interval. For Web applications, a count of page

impressions or requests per second is often used as a measure of throughput.
- System availability: Usually expressed as a percentage of application running time minus the time the application can't be accessed by users.

The ability to overcome performance limits by adding resources is defined as scalability.

Latency indicates how long it takes for packets to reach their destination. Throughput is the term given to the number of packets that are processed within a specific period of time.

1G Vs. 2G Vs. 3G Vs. 4G Vs. 5G

Simply, the "G" stands for "GENERATION" . While you connected to internet, the speed of your internet is depends upon the signal strength that has been shown in alphabets like 2G, 3G, 4G etc. right next to the signal bar on your home screen. Each Generation is defined as a set of telephone network standards , which detail the technological implementation of a particular mobile phone system. The speed increases and the technology used to achieve that speed also changes. For eg, 1G offers 2.4 kbps, 2G offers 64 Kbps and is based on GSM, 3G offers 144 kbps-2 mbps whereas 4G offers 100 Mbps - 1 Gbps and is based on LTE technology

How does a VPN work?

A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host. This means that if you surf online with a VPN, the VPN server becomes the source of your data. This means your Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online. A VPN works like a filter that turns all your data into "gibberish". Even if someone were to get their hands on your data, it would be useless.

What are the benefits of a VPN connection?

Secure encryption: To read the data, you need an *encryption key* . Without one, it would take millions of years for a computer to decipher the code in the event of a brute force attack . With the help of a VPN, your online activities are hidden even on public networks.

Disguising your whereabouts : VPN servers essentially act as your proxies on the internet. Because the demographic location data comes from a server in another country, your actual location cannot be determined. In addition, most VPN services do not store logs of your activities. Some providers, on the other hand, record your behavior, but do not pass this information on to third parties. This means that any potential record of your user behavior remains permanently hidden.

Access to regional content: Regional web content is not always accessible from everywhere. Services and websites often contain content that can only be accessed from certain parts of the world. Standard connections use local servers in the country to determine your location. This means that you cannot access content at home while traveling, and you cannot access international content from home. With **VPN location spoofing** , you can switch to a server to another country and effectively “change” your location.

Secure data transfer: If you work remotely, you may need to access important files on your company’s network. For security reasons, this kind of information requires a secure connection. To gain access to the network, a VPN connection is often required. VPN services connect to private servers and use encryption methods to reduce the risk of data leakage.

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.

Private VS Public IP Address

S.No.	PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
1.	The scope of Private IP is local.	The scope of Public IP is global.
2.	It is used to communicate within the network.	It is used to communicate outside the network.
3.	Private IP addresses of the systems connected in a network differ in a uniform manner.	Public IP may differ in a uniform or non-uniform manner.
4.	It works only on LAN.	It is used to get internet service.
5.	It is used to load the network operating system.	It is controlled by ISP.
6.	It is available free of cost.	It is not free of cost.
7.	Private IP can be known by entering “ipconfig” on the command prompt.	Public IP can be known by searching “what is my ip” on google.

8.	Range:
	`10.0.0.0 - 10.255.255.255,`
	`172.16.0.0 - 172.31.255.255,`
	`192.168.0.0 - 192.168.255.255`
		Range: Besides private IP addresses, the rest are public.

	Example: 192.168.1.10	Example: 17.5.7.8
9.	Private IP uses numeric code that is not unique and can be used again	Public IP uses a numeric code that is unique and cannot be used by other
10.	Private IP addresses are secure	Public IP address has no security and is subjected to attack
11.	Private IP addresses require NAT to communicate with devices	Public IP does not require a network translation

S.NO	Static Routing	Dynamic Routing
1.	In static routing routes are user-defined.	In dynamic routing, routes are updated according to the topology.
2.	Static routing does not use complex routing algorithms.	Dynamic routing uses complex routing algorithms.
3.	Static routing provides high or more security.	Dynamic routing provides less security.
4.	Static routing is manual.	Dynamic routing is automated.
5.	Static routing is implemented in small networks.	Dynamic routing is implemented in large networks.
6.	In static routing, additional resources are not required.	In dynamic routing, additional resources are required.
7.	In static routing, failure of the link disrupts the rerouting.	In dynamic routing, failure of the link does not interrupt the rerouting.

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.

Parameters	Modem	Router
Definition	A modem is a device that modulates and demodulates the electrical signal and maintains a dedicated connection between the internet and home/office network.	The router is a networking device that enables multiple devices to connect to wired or wireless networks.
Operating Layer of OSI model.	It works on **the data link** layer of the OSI model.	It works on the **physical, data-link, and network** layers of the OSI model.
How does it work?	It acts like a signal modulate and demodulator, which means it modulates the electrical signal to a digital signal and sends it to a PC or computer, demodulates the signal from digital to analog, and sends it to the internet.	It routes the data packets from one source to a defined destination by following the routing table. It enables multiple network devices to connect over the given network.
Security	The modem transmits the data without any authentication; hence it is not secure.	The router provides complete security with passwords and checks each data packet before transmitting it over a given network.
Cable Used	RJ45 to connect with router, and RJ11 to connect with a telephone line.	RJ45 cable is used.
Placed	A modem is placed between the telephone line and computer or router.	A router is placed between the modem and other networking devices.

Wireless Communication - Bluetooth

Bluetooth wireless technology is a short range communications technology intended to replace the cables connecting portable unit and maintaining high levels of security. Bluetooth technology is based on Ad-hoc technology also known as Ad-hoc Pico nets, which is a local area network with a very limited coverage.

"Ad hoc" is Latin for "to this" meaning "for this" or "for this purpose". The term "ad hoc network" refers to the ability for members of a network to establish a network connection between devices.

What is WiFi Hotspot

A WiFi hotspot is a physical location that has been provided to give users the ability to use their devices away from home. These hotspots became popular over a decade ago at eating establishments such as coffee houses and are now found anywhere people congregate (malls, airports, hotels, etc.).

E-mail System

E-mail system comprises of the following three components:

- Mailer
- Mail Server
- Mailbox

Mailer

It is also called mail program, mail application or mail client. It allows us to manage, read and compose e-mail.

Mail Server

The function of mail server is to receive, store and deliver the email. It is must for mail servers to be Running all the time because if it crashes or is down, email can be lost.

Mailboxes

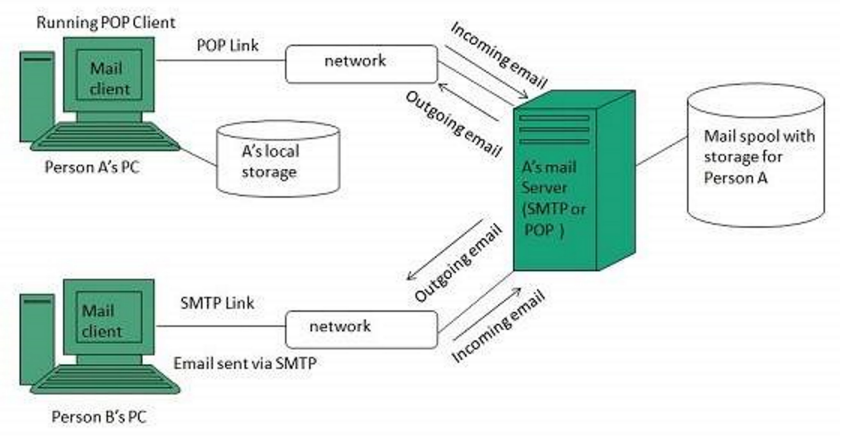
Mailbox is generally a folder that contains emails and information about them.

Working of E-mail

Email working follows the client server approach. In this client is the mailer i.e. the mail application or mail program and server is a device that manages emails.
Following example will take you through the basic steps involved in sending and receiving emails and will give you a better understanding of working of email system:

- Suppose person A wants to send an email message to person B.
- Person A composes the messages using a mailer program i.e. mail client and then select Send option.
- The message is routed to Simple Mail Transfer Protocol to person B's mail server.
- The mail server stores the email message on disk in an area designated for person B. The disk space area on mail server is called mail spool.
- Now, suppose person B is running a POP client and knows how to communicate with B's mail server.
- It will periodically poll the POP server to check if any new email has arrived for B.As in this case, person B has sent an email for person B, so email is forwarded over the network to B's PC. This is message is now stored on person B's PC.

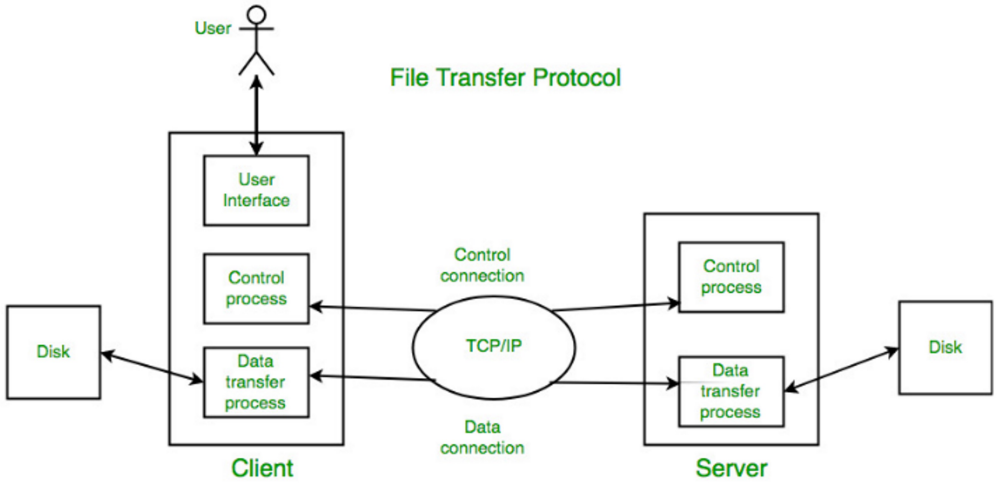
The following diagram gives pictorial representation of the steps discussed above:



File Transfer Protocol (FTP) in Application Layer

File Transfer Protocol(FTP) is an application layer protocol that moves files between local and remote file systems. It runs on top of TCP, like HTTP. To transfer a file, 2 TCP connections are used by FTP in parallel: control connection and data connection.

Mechanism of File Transfer Protocol



Types of Connection in FTP

1. Control Connection: For sending control information like user identification, password, commands to change the remote directory, commands to retrieve and store files, etc., FTP makes use of a control connection. The control connection is initiated on port number 21.

2. Data connection: For sending the actual file, FTP makes use of a data connection. A data connection is initiated on port number 20.

What is a Firewall?

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.

Network Layer vs. Application Layer Inspection

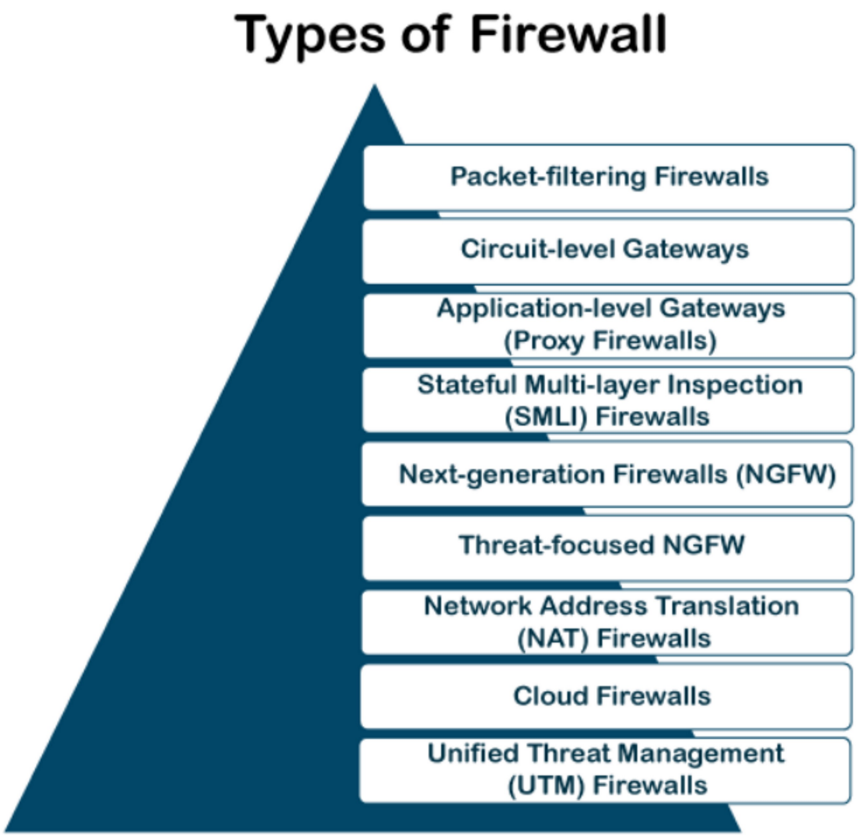
Network layer or packet filters inspect packets at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set where the source and destination of the rule set is based upon Internet Protocol (IP) addresses and ports. Firewalls that do network layer inspection perform better than similar devices that do application layer inspection. The downside is that unwanted applications or malware can pass over allowed ports, e.g. outbound Internet traffic over web protocols HTTP and HTTPS, port 80 and 443 respectively.

Types of Firewall

There are mainly three types of firewalls, such as **software firewalls, hardware firewalls, or both**, depending on their structure.

A hardware firewall is a physical device that attaches between a computer network and a gateway sometimes referred to as an **Appliance Firewall**. On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software. This type of

firewall is also called a **Host Firewall**.



Packet-filtering Firewalls

A packet filtering firewall is the most basic type of firewall. It acts like a management program that monitors network traffic and filters incoming packets based on configured security rules.

Circuit-level Gateways

These types of firewalls typically operate at the session-level of the OSI model by verifying **TCP (Transmission Control Protocol)** connections and sessions.
Like packet-filtering firewalls, these firewalls do not check for actual data, although they inspect information about transactions. Therefore, if a data contains malware, but follows the correct TCP connection, it will pass through the gateway. That is why circuit-level gateways are not considered safe enough to protect our systems.

Application-level Gateways (Proxy Firewalls)

Proxy firewalls operate at the application layer as an intermediate device to filter incoming traffic between two end systems (e.g., network and traffic systems). That is why these firewalls are called **'Application-level Gateways'**.
Unlike basic firewalls, these firewalls transfer requests from clients pretending to be original clients on the web-server. This protects the client's identity and other suspicious information, keeping the network safe from potential attacks. Once the connection is established, the proxy firewall inspects data packets coming from the source. If the contents of the incoming data packet are protected, the proxy firewall transfers it to the client. This approach creates an additional layer of security between the client and many different sources on the network.

Stateful Multi-layer Inspection (SMLI) Firewalls

Stateful multi-layer inspection firewalls include both packet inspection technology and TCP handshake verification.
In simple words, when a user establishes a connection and requests data, the SMLI firewall creates a database (state table). The database is used to store session information such as source IP address, port number, destination IP address, destination port number, etc. Connection information is stored for each session in the

state table. Using stateful inspection technology, these firewalls create security rules to allow anticipated traffic.
In most cases, SMLI firewalls are implemented as additional security levels. These types of firewalls implement more checks and are considered more secure than stateless firewalls.

Next-generation Firewalls (NGFW)

Many of the latest released firewalls are usually defined as **'next-generation firewalls'**. However, there is no specific definition for next-generation firewalls. These firewalls include **deep-packet inspection (DPI),** surface-level packet inspection, and TCP handshake testing, etc.
NGFW includes higher levels of security than packet-filtering and stateful inspection firewalls.

Threat-focused NGFW

Threat-focused NGFW includes all the features of a traditional NGFW. Additionally, they also provide advanced threat detection and remediation. These types of firewalls are capable of reacting against attacks quickly. With intelligent security automation, threat-focused NGFW set security rules and policies, further increasing the security of the overall defense system.

Network Address Translation (NAT) Firewalls

Network address translation or NAT firewalls are primarily designed to access Internet traffic and block all unwanted connections. These types of firewalls usually hide the IP addresses of our devices, making it safe from attackers.
When multiple devices are used to connect to the Internet, NAT firewalls create a unique IP address and hide individual devices' IP addresses.
In general, NAT firewalls works similarly to proxy firewalls. Like proxy firewalls, NAT firewalls also work as an intermediate device between a group of computers and external traffic.

Cloud Firewalls

Whenever a firewall is designed using a cloud solution, it is known as a cloud firewall or **FaaS (firewall-as-service)**. Cloud firewalls are typically maintained and run on the Internet by third-party vendors. This type of firewall is considered similar to a proxy firewall. The reason for this is the use of cloud firewalls as proxy servers.
The most significant advantage of cloud firewalls is scalability. Because cloud firewalls have no physical resources, they are easy to scale according to the organization's demand or traffic-load. Most organizations use cloud firewalls to secure their internal networks or entire cloud infrastructure.

Unified Threat Management (UTM) Firewalls

UTM firewalls are a special type of device that includes features of a stateful inspection firewall with anti-virus and intrusion prevention support. Such firewalls are designed to provide simplicity and ease of use. These firewalls can also add many other services, such as cloud management, etc.