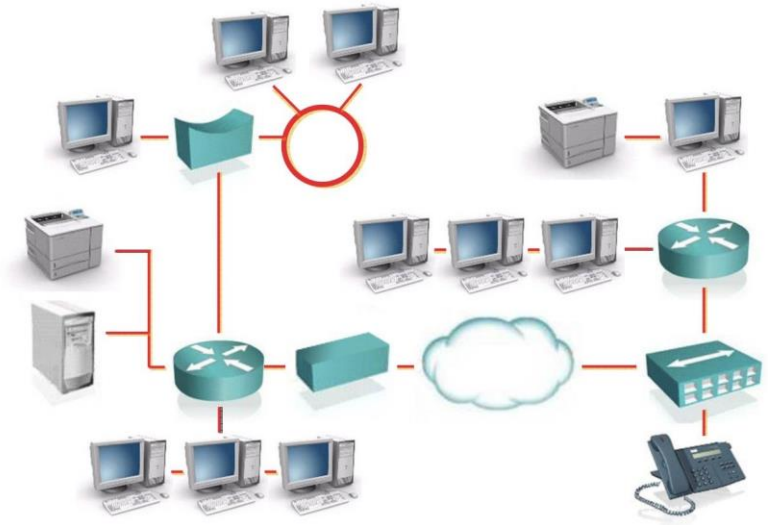
1) What is Networking?
2) Types of Networks (PAN, LAN, MAN, WAN, CAN , SAN, POLAN, VPN)
3) What is OSI ? 7 Layer of OSI Model
4) TCP/IP Model
5) OSI VS TCP/IP Model
6) What are Common Networking Protocols?
7) Transport
8) IP Deep Dive
9) Types of IP Address
10) Routers, Switches
11) DNS
12) Firewall
13) Network Speed in Details
14) Referencing all we have covered with AWS Networking

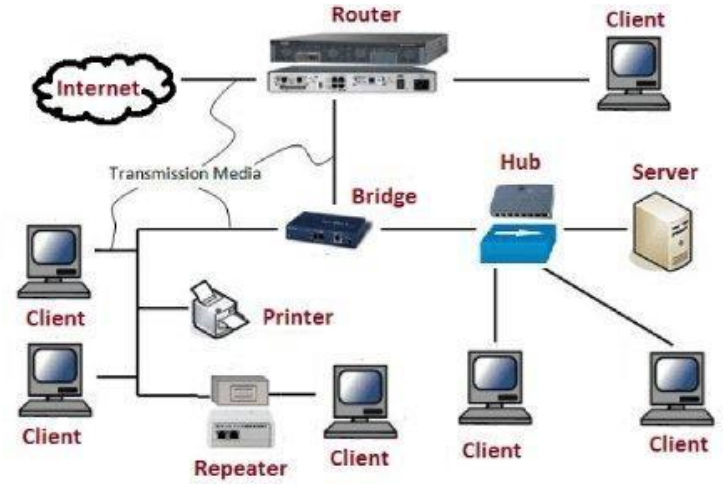
Learn Basic Networking For AWS (or Any) Cloud Networking

What is Networking?

“A computer network is a group of computers that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on or provided by the network nodes.” - Wikipedia

In more simple words:





Types of Networking

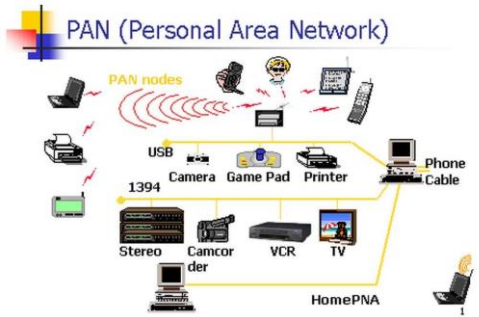
A network just a group of computers and other devices connected in some ways so as to be able to exchange data

Each devices on the network can be referred as Nodes or clients and each node has a unique address to communicate with each other , we call it IP address e.g. 192.168.0.21, 203.212.242.38 etc

Personal Area Network (PAN)

A Personal Area Network (PAN) is smallest network which is very personal to a user. It is a short-range network topology designed for peripheral devices (usually 30ft) used by an individual. The purpose of these types of networks is to transmit data between devices without being necessarily connected to the internet. This can be be wired or wireless

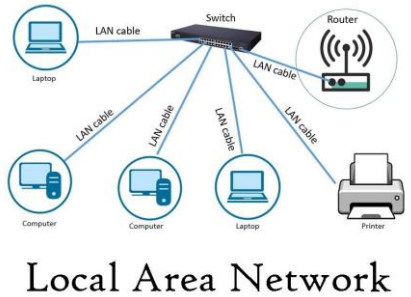
E.g. Bluetooth keyboard that's connected to a smart TV



Local Area Network (LAN)

A computer network spanned inside a building and operated under single administrative system is generally termed as Local Area Network (LAN)

It's is a proprietary computer network that enables designated users to have exclusive access to the same system connection at a common location, always within an area of less than a mile and most often within the same building. By doing so they're able to share devices, share resources such as printers, and exchange information as if they were all working from the same system. Resource sharing is possible with a network-aware operating system.



Wireless Local Area Network (WLAN)

Just like LAN but Wireless! these types of networks don't require that devices rely on physical cables to connect to the network.

WLANs use high-frequency signals (e.g. 2.4 GHz band or 5 GHz band), lasers, and infrared beams to enable devices (also known as clients) to communicate with each other without the need of electrical conductors (wires) to transmit data. This type of flexible data communication makes it easy for users to move around a coverage area without the need of cables to maintain network connectivity.
E.g. WiFi

Types of Networking

Types of Networking

Wide Area Network (WAN)

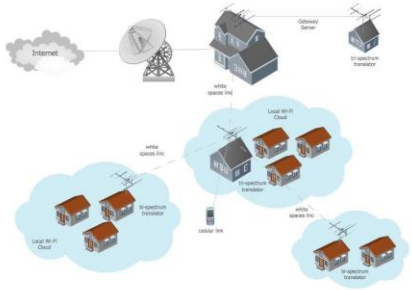
Slightly more complex than a LAN, a WAN connects computers together across longer physical distances. This allows computers and low-voltage devices to be remotely connected to each other over one large network to communicate even when

Metropolitan Area Network (MAN)

These types of networks are larger than LANs but smaller than WANs – and incorporate elements from both types of networks. MANs span an entire geographic area typically a town or city.. Ownership and maintenance is handled by either a single person or company

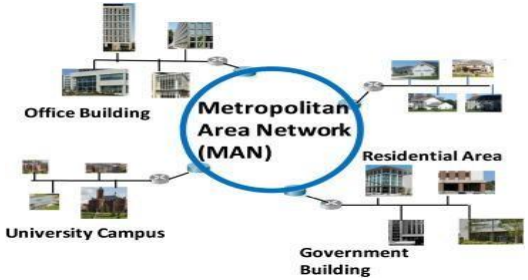
Types of Networking

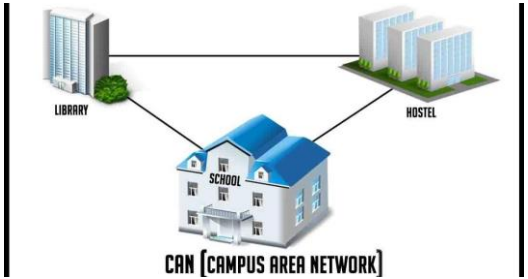
Campus Area Network (CAN)



they’re miles apart.

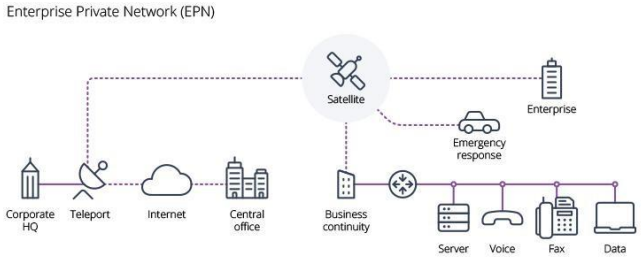
The Internet is the most basic example of a WAN, connecting all computers together around the world. Because of a WAN’s vast reach, it is typically owned and maintained by multiple administrators or the public.





Enterprise Private Network (EPN)

These types of networks are built and owned by businesses that want to securely connect its various locations to share computer resources.



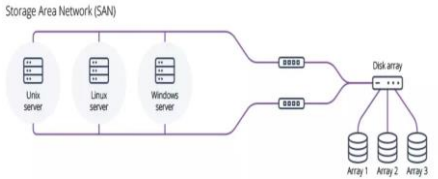
Types of Networking

Larger than LANs, but smaller than metropolitan area networks (MANs, explained below), these types of networks are typically seen in universities, large K-12 school districts or small businesses. They can be spread across several buildings that are fairly close to each other so users can share resources.

Storage-Area Network (SAN)

A storage area network (SAN), or network behind the servers, is a special purpose high-speed computer network that provides any-to-any access to storage. The main purpose of a SAN is to transfer data between different storage devices and between the computer network and storage devices.

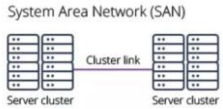
These types of networks don't rely on a LAN or WAN. Instead, they move storage resources away from the network and place them into their own high-performance network



System Area Network (SAN)

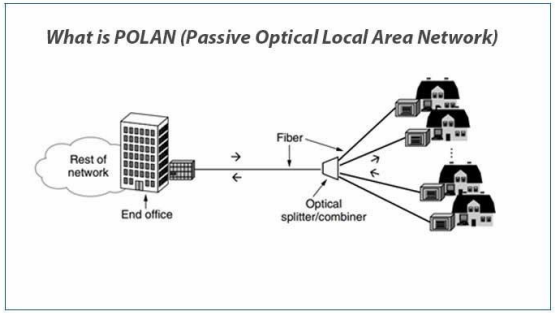
A System Area Network (also called a SAN) is a local network uniquely designed for high-speed interconnection in a cluster environment. These networks include server-to-server, processor-to-processor, and Storage Area Networks all operating as one entity

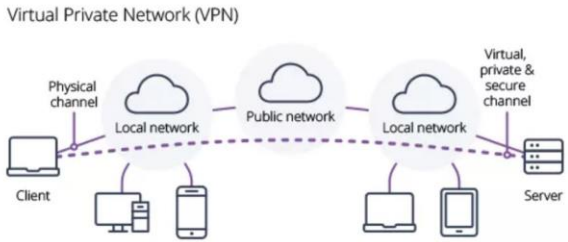
As SANs are designed to be used in parallel computing environments, typical examples include use in scientific applications, database server clusters, and file server clusters.



Virtual Private Network (VPN)
Passive Optical Local Area Network (POLAN)

As technology moves away from switch-based ethernet LANs, Passive Optical Local Area Networks (POLAN), is installed into **structured cabling** design. It is built on a point-to-multipoint LAN architecture, using optical splitters to send a signal from one fiber into multiple signals across devices.





L

earn Computer Networking With Kiran

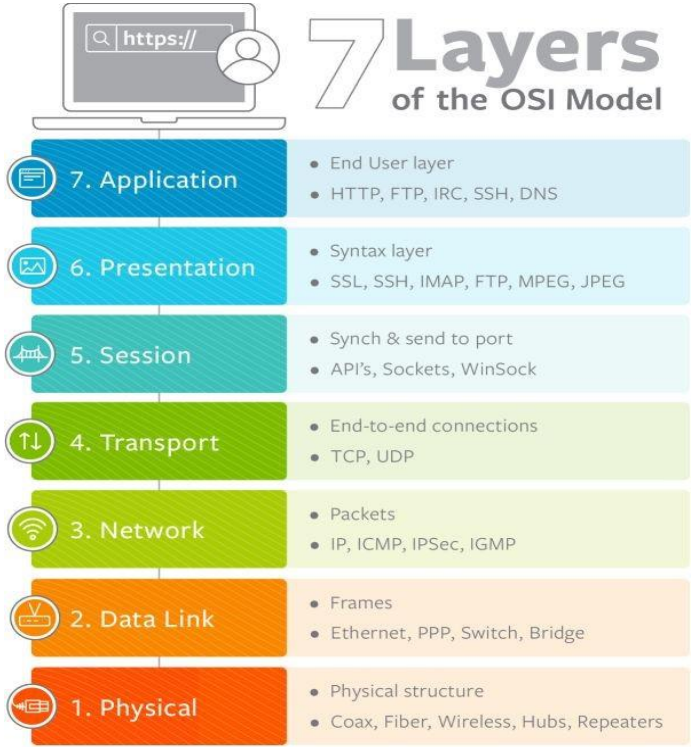
Types of Networking

By extending a private network across the Internet, a VPN lets its users send and receive data as if their devices were connected to the private network – even if they're not. Through a virtual point-to-point connection, users can access a private network remotely.

OSI Model

The open systems interconnection (OSI) model is a conceptual model created by the International Organization for Standardization which enables diverse communication systems to communicate using standard protocols. In plain English, the OSI provides a standard for different computer systems to be able to communicate with each other.

The OSI Model can be seen as a universal language for computer networking. It's based on the concept of splitting up a communication system into seven abstract layers, each one stacked upon the last.



7) Application Layer: Human-Computer interaction layer, where application can access network services. few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

6) Presentation Layer: Ensure that data is in useable format, al so this is where encryption happens. A good example of this is encryption and decryption of data for secure transmission - this happens at Layer 6.

5) Session Layer: Maintain Session and is responsible for controlling ports and sessions. Functions at this layer involve setup, coordination (how long should a system wait for a response, for example) and termination between the applications at each end of the session.

4) Transport Layer: Transmit data using transmission protocol such as TCP,UDP. The best known example of the Transport Layer is the Transmission Control Protocol (TCP), which is built on top of the Internet Protocol (IP), commonly known as TCP/IP. TCP and UDP port numbers work at Layer 4, while IP addresses work at Layer 3, the Network Layer.

3) Network Layer: Decides which physical path data will take. In its most basic sense, this layer is responsible for packet forwarding, including routing through different routers

2) Data Link Layer: Defines format of the data on the network. It's in charge of data encapsulation under the form of packets and their interpretation at the physical layer

1) Physical Layer: Transmit raw bit stream over the physical medium. This can include everything from the cable type, radio frequency link (as in an 802.11 wireless systems), as well as the layout of pins, voltages and other physical requirements

TCP/IP Model

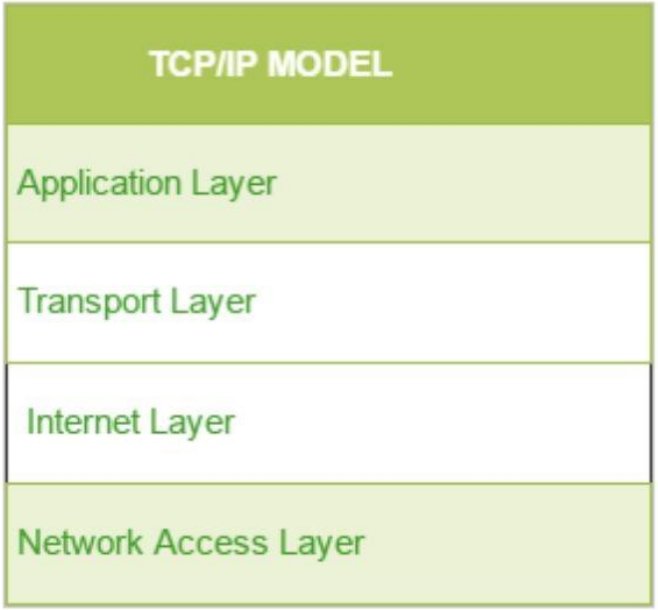
Internet uses TCP/IP protocol suite, also known as Internet suite. This defines Internet Model which contains four layered architecture. OSI Model is general communication model but Internet Model is what the internet uses for all its communication.The internet is independent of its underlying network architecture so is its Model. This model has the following layers:

Application Layer: This layer defines the protocol which enables user to interact with the network.For example, FTP, HTTP etc.

Transport Layer: This layer defines how data should flow between hosts. Major protocol at this layer is Transmission Control Protocol (TCP). This layer ensures data delivered between hosts is in-order and is responsible for end-to-end delivery.

Internet Layer: Internet Protocol (IP) works on this layer. This layer facilitates host addressing and recognition. This layer defines routing.

Network Access Layer: Provides the same functionality as the physical, the data link and network layers in the OSI model.



OSI Model vs TCP/IP Model

Differences between OSI Model and TCP/IP Model are:

- OSI layers 5, 6, 7 are combined into one Application Layer in TCP/IP

- OSI layers 1, 2 are combined into one Network Access Layer in TCP/IP – however TCP/IP does not take responsibility for sequencing and acknowledgement functions, leaving these to the underlying transport layer.

- TCP/IP is a functional model designed to solve specific communication problems, and which is based on specific, standard protocols. OSI is a generic, protocol-independent model intended to describe all forms of network communication.

- In TCP/IP, most applications use all the layers, while in OSI simple applications do not use all seven layers. Only layers 1, 2 and 3 are mandatory to enable any data communication.

Common Network Protocols

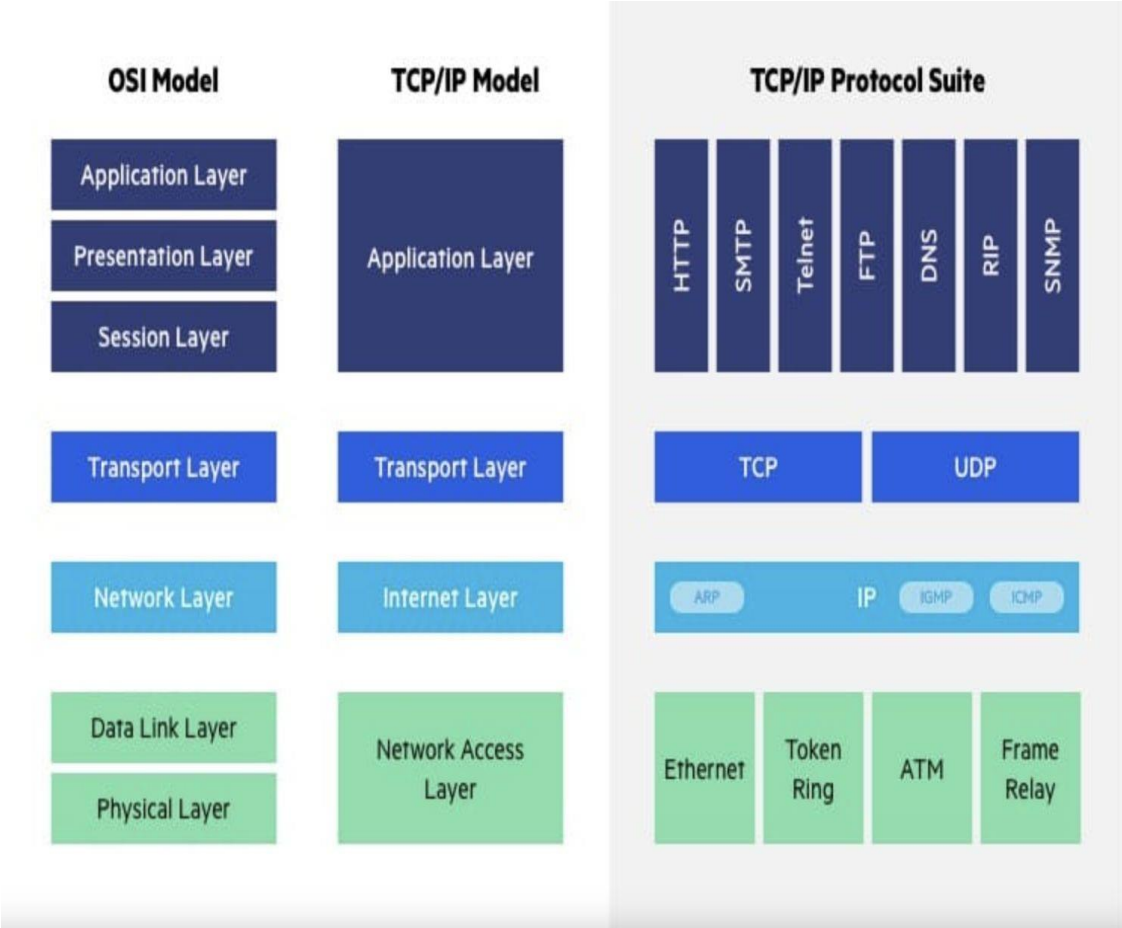
What is Network Protocol?

In networking, a protocol is a standardized way of doing certain actions and formatting data so that two or more devices are able to communicate with and understand each other. It define the rules that govern the communications between two computers connected to the network. **What is do ?**

Addressing and routing of messages, error detection and recovery, sequence and flow controls etc.

Protocol Specifications

A protocol specification consists of the syntax, which defines the kinds and formats of the messages exchanged, and the semantic, which specifies the action taken by each entity when specific events occur. **Example**:



HTTP protocol for communication between web browsers and servers.

Commonly Used Protocols as follows

Transmission Control Protocol (TCP)

TCP is a popular communication protocol which is used for communicating over a network. It divides any message into series of packets that are sent from source to destination and there it gets reassembled at the destination.

Internet Protocol (IP)

IP is designed explicitly as addressing protocol. It is mostly used with TCP. The IP addresses in packets help routing them through different nodes in a network until it reaches the destination system. TCP/IP is the most low-latency linking between different applications. popular protocol connecting the networks.

User Datagram Protocol (UDP)

UDP is a substitute communication protocol to Transmission Control Protocol implemented in primarily for creating loss-tolerating and

Post office Protocol (POP)

POP3 is designed for receiving incoming E-mails.

IMAP and IMAP4: Internet Message Access Protocol (version 4)

IMAP is an email protocol that lets end users access and manipulate messages stored on a mail server from their email client as if they were present locally on their remote device. IMAP follows a client-server model, and lets multiple clients access messages on a common mail server concurrently. IMAP includes operations for creating, deleting, and renaming mailboxes; checking for new messages; permanently removing messages; setting and removing flags; and much more. The current version of IMAP is version 4 revision 1.

Simple mail transport Protocol (SMTP)

SMTP is designed to send and distribute outgoing E-Mail.

File Transfer Protocol (FTP)

FTP allows users to transfer files from one machine to another. Types of files may include program files, multimedia files, text files, and documents, etc.

Telnet: Terminal emulation protocol

Telnet is an application layer protocol that enables a user to communicate with a remote device. A Telnet client is installed on the user's machine, which accesses the command line interface of another remote machine that runs a Telnet server program.

Secure Shell (SSH) SSH, also known as Secure Shell or Secure Socket Shell, is a network protocol

that gives users, particularly system administrators, a secure way to access a computer over an unsecured network.

Hyper Text Transfer Protocol (HTTP)

HTTP is designed for transferring a hypertext among two or more systems. HTML tags are used for creating links. These links may be in any form like text or images. HTTP is designed on Client-server principles which allow a client system for establishing a connection with the server machine for making a request. The server acknowledges the request initiated by the client and responds accordingly.

DHCP: Dynamic Host Configuration Protocol

DHCP is a communication protocol that enables network administrators to automate the assignment of IP addresses in a network. In an IP network, every device connecting to the internet requires a unique IP. DHCP lets network admins distribute IP addresses from a central point and automatically send a new IP address when a device is plugged in from a different place in the network. DHCP works on a client-server model.

RTMP: Real-Time Messaging Protocol it is part of the technology that makes live streaming possible. RTMP's primary role is to deliver content from an encoder to an online video host

Hyper Text Transfer Protocol Secure (HTTPS)

HTTPS is abbreviated as Hyper Text Transfer Protocol Secure is a standard protocol to secure the communication among two computers one using the browser and other fetching data from web server. HTTP is used for transferring data between the client browser (request) and the web server (response) in the hypertext format, same in case of HTTPS except that the transferring of data is done in an encrypted format. So it can be said that https thwart hackers from interpretation or modification of data throughout the transfer of packets.

ARP: Address Resolution Protocol

The Address Resolution Protocol helps map IP addresses to physical machine addresses (or a MAC address for Ethernet) recognized in the local network. A table called an ARP cache is used to maintain a correlation between each IP address and its corresponding MAC address. ARP offers the rules to make these correlations, and helps convert addresses in both directions.

Common Network Protocols

Transport

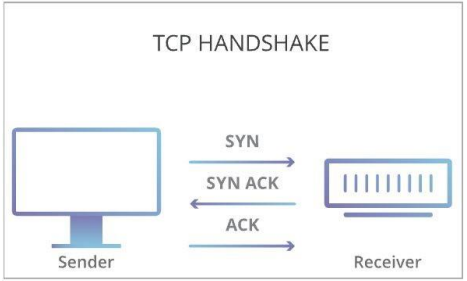
What is Transport?

The IP layer gets packets from one node to another, but it is not well-suited to transport. First, IP routing is a “best-effort” mechanism, which means packets can and do get lost sometimes. Additionally, data that does arrive can arrive out of order. Finally, IP only supports sending to a specific host; normally, one wants to send to a given application running on that host. Email and web traffic, or two different web sessions, should not be commingled! The Transport layer is the layer above the IP layer that handles these sorts of issues, often by creating some sort of connection abstraction. Far and away the most popular mechanism in the Transport layer is the Transmission Control Protocol (TCP/IP) and User Datagram Protocol (UDP/IP)

Transmission Control Protocol (TCP)

Transmission Control Protocol (TCP) is connection-oriented, meaning once a connection has been established, data can be transmitted in two directions. TCP has built-in systems to check for errors and to guarantee data will be delivered in the order it was sent, making it the perfect protocol for transferring information like still images, data files, and web pages.

But while TCP is instinctively reliable, its feedback mechanisms also result in a larger overhead, translating to greater use of the available bandwidth on your network.

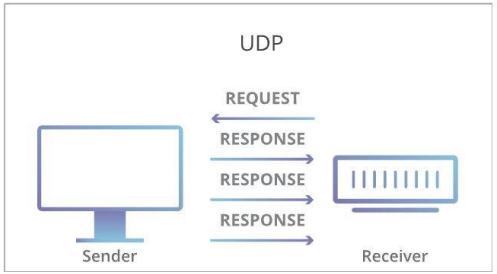


User Datagram Protocol (UDP/IP)

User Datagram Protocol (UDP) is a simpler, connectionless Internet protocol wherein error-checking and recovery services are not required.

With UDP, there is no overhead for opening a connection, maintaining a connection, or terminating a connection; data is continuously sent to the recipient, whether or not they receive it.

Although UDP isn't ideal for sending an email, viewing a webpage, or downloading a file, it is largely preferred for real-time communications like broadcast or multitask network transmission.



IP Deep Dive

What is Internet Protocol (IP)?

The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination. Data traversing the Internet is divided into smaller pieces, called packets. IP information is attached to each **packet**, and this information helps routers to send packets to the right place. Every device or domain that connects to the Internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives where it is needed.

Once the packets arrive at their destination, they are handled differently depending on which transport protocol is used in combination with IP. The most common transport protocols are TCP and UDP.

What is an IP address? How does IP addressing work?

An IP address is a unique identifier assigned to a device or domain that connects to the Internet. Each IP address is a series of characters, such as '192.168.1.1'. Via DNS resolvers, which translate human-readable domain names into IP addresses, users are able to access websites without memorizing this complex series of characters. Each IP packet will contain both the IP address of the device or domain sending the packet and the IP address of the intended recipient, much like how both the destination address and the return address are included on a piece of mail.

In more simple words:

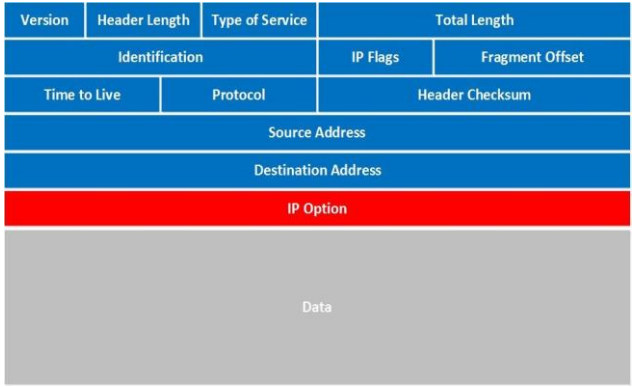
An IP address is a string of numbers separated by periods. IP addresses are expressed as a set of four numbers — an example address might be 192.158.1.38. Each number in the set can range from 0 to 255. So, the full IP addressing range goes from 0.0.0.0 to 255.255.255.255. IP address is unique to each device and In one network two devices can't have same IP address (otherwise conflict happens)

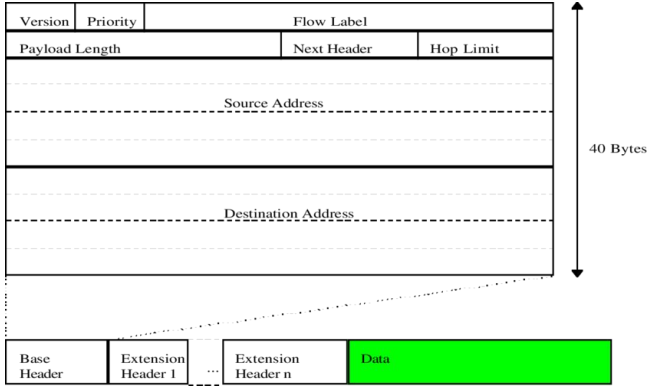
In Short: An **IP address** is a unique **address** that identifies a device on the internet or a local network. **IP** stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

Important note: IP addresses are not random. They are mathematically produced and allocated by the Internet Assigned Numbers Authority (IANA), a division of the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is a non-profit organization that was established in the United States in 1998 to help maintain the security of the internet and allow it to be usable by all. Each time anyone registers a domain on the internet, they go through a domain name registrar, who pays a small fee to ICANN to register the domain.

IP Deep Dive

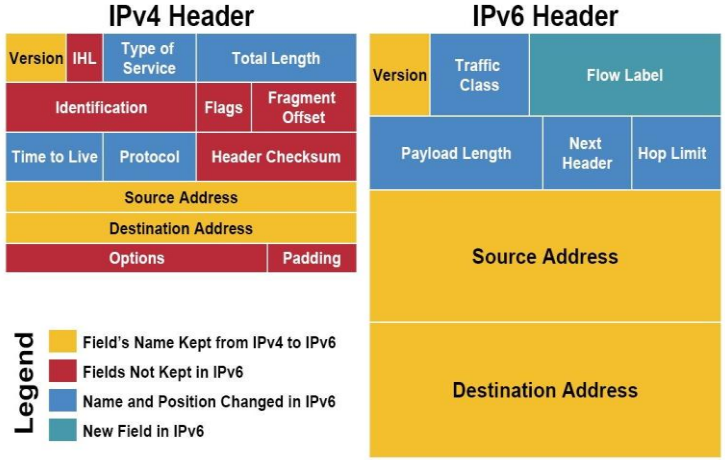
IPv6





IPv4 What is IP Packet?

In networking, a packet is a small segment of a larger message. Data sent over computer networks, such as the Internet, is divided into packets. These packets are then recombined by the computer or device that receives them.



What is IP Version?

Packets that hold Internet Protocol data carry a 4-bit **IP version number** as the first field of its header. Currently, only IPv4 and IPv6 packets are seen on the Internet, having IP version numbers 4 and 6, respectively.

As the version number is carried in a 4-bit field, only numbers 0-15 can be assigned, but only version 4 and 6 is active and getting used, others are either reserved or obsololate, read here for more.

IPv4

IPv4 is an IP version widely used to identify devices on a network using an addressing system. It was the first version of IP deployed for production in the ARPANET in 1983. It uses a 32-bit address scheme to store 2^32 addresses which is more than 4 billion addresses. It is considered the primary Internet Protocol and carries 94% of Internet traffic.

IPv6

IPv6 is the most recent version of the Internet Protocol. This new IP address version is being deployed to fulfill the need for more Internet addresses. It was aimed to resolve issues that are associated with IPv4. With 128-bit address space, it allows 340 undecillion unique address space. IPv6 is also called IPng (Internet Protocol next generation).Internet Engineer Task Force initiated it in early 1994. The design and development of that suite are now called IPv6.

The address 127.0.0.1 was reserved for the loopback (sometimes called "localhost") IP—this is the IP of the TCP/IP protocol itself on every host machine.

Class E

Class E networks are defined by having the first four network address bits as 1. That encompasses addresses from 240.0.0.0 to 255.255.255.255. While this class is reserved, its usage was never defined. As a result, most network implementations discard these addresses as illegal or undefined. The exception is 255.255.255.255, which is used as a broadcast address.

Types Of IP Addresses

Based on Class

Early in the development of IP, the IANA (Internet Assigned Numbers Authority) designated five classes of IP address: A, B, C, D, and E

Class A

In a Class A network, the first eight bits, or the first dotted decimal, is the network part of the address, with the remaining part of the address being the host part of the address. There are 128 possible Class A networks. 0.0.0.0 to 127.0.0.0

first few bits	first byte	network bits	host bits	name	application
0	0-127	8	24	class A	a few very large networks
10	128-191	16	16	class B	institution-sized networks
110	192-223	24	8	class C	sized for smaller entities

Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Addresses per network	Total addresses in class	Start address	End address
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	2,147,483,648 (2^{31})	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	1,073,741,824 (2^{30})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	536,870,912 (2^{29})	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	268,435,456 (2^{28})	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	268,435,456 (2^{28})	240.0.0.0	255.255.255.255

Class B

In a Class B network, the first 16 bits are the network part of the address. All Class B networks have their first bit set to 1 and the second bit set to 0. In dotted decimal notation, that makes 128.0.0.0 to 191.255.0.0 as Class B networks. There are 16,384 possible Class B networks.

Class C

In a Class C network, the first two bits are set to 1, and the third bit is set to 0. That makes the first 24 bits of the address the network address and the remainder as the host address. Class C network addresses range from 192.0.0.0 to 223.255.255.0. There are over 2 million possible Class C networks.

Class D

Addresses are used for multicasting applications. Unlike the previous classes, the Class D is not used for "normal" networking operations. Class D addresses have their first three bits set to "1" and their fourth bit set to "0". Class D addresses are 32-bit network addresses, meaning that all the values within the range of 224.0.0.0 – 239.255.255.255 are used to uniquely identify multicast groups. There are no host addresses within the Class D address range, as all hosts within a group share the group's IP address for receiver purposes.

These classes were identified based on the pattern of high-order bits (the high-value bits at the beginning of the first octet). The result is that certain ranges of networks are grouped into classes in a pattern based on the binary values of those high-order bits, as detailed in Table

things (IoT) products, the number of private IP addresses you are likely to have in your own home is growing.

Public IP Address : A public IP address is an address where one primary address is associated with your whole network. In this type of IP address, each of the connected devices has the same IP address.

This type of public IP address is provided to your router by your Internet Service Provider(ISP).

Typically, ISPs have a large pool of IP addresses that they distribute to their customers. Your public IP address is the address that all the devices outside your internet network will use to recognize your network.

Public IP addresses come in two forms – dynamic and static.

Dynamic IP addresses change automatically and regularly. ISPs buy a large pool of IP addresses and assign them automatically to their customers. Periodically, they re-assign them and put the older IP addresses back into the pool to be used for other customers

Types of IP Address

Based on Accessibility

Private IP Addresses

A private IP address is a unique IP number assigned to every device that connects to your home internet network, which includes devices like computers, tablets, smartphones, which is used in your household.

It also likely includes all types of Bluetooth devices you use, like printers or printers, smart devices like TV, etc. With a rising industry of internet of

Static IP

In contrast to Dynamic IP addresses, **static IP addresses** remain consistent. Once the network assigns an IP address, it remains the same. Most individuals and businesses do not need a static IP address, but for businesses that plan to host their own server, it is crucial to have one. This is because a static IP address ensures that websites and email addresses tied to it will have a consistent IP address — vital if you want other devices to be able to find them consistently on the web.

Website IP Addresses: If you're planning to start a website and you do go with a web hosting service provider, you'll potentially encounter two types of website IP address options: **Shared IP Address** and **Dedicated IP Address**

Shared IP Addresses: Shared IP address is used by small business websites that do not yet get many visitors or have many files or pages on their site. The IP address is not unique and it is shared with other websites.

Dedicated IP Addresses: Dedicated IP address is assigned uniquely to each website. Dedicated IP addresses helps you avoid any potential backlists because of bad behavior from others on your server. The dedicated IP address also gives you the option of pulling up your website using the IP address alone, instead of your domain name. It also helps you to access your website when you are waiting on a domain transfer.

Router & Switches

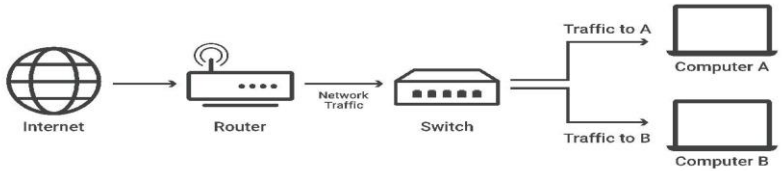
What is Router?

A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.

What is Switch?

A network switch connects devices within a network (often a local area network, or LAN*) and forwards data packets to and from those devices. Unlike a router, a switch only sends data to the single device it is intended for (which may be another switch, a router, or a user's computer), not to networks of multiple devices.

this means is that routers are necessary for an Internet connection, while switches are only used for interconnecting devices.
Homes and small offices need routers for Internet access, but most do not need a network switch, unless they require a large amount of Ethernet* ports. However, large offices, networks, and data centers with dozens or hundreds of computers usually do require switches.



DNS

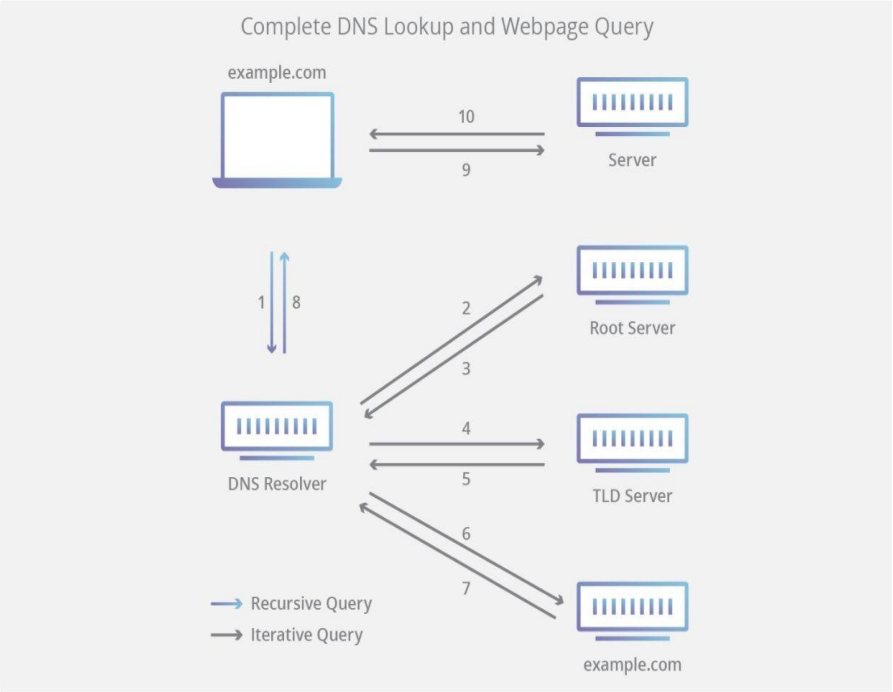
What is DNS?

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

Steps in a DNS lookup & Retrieving Web Page / Content

1. A user types ‘example.com’ into a web browser and the query travels into the Internet and is received by a DNS recursive resolver.
2. The resolver then queries a DNS root nameserver (.).
3. The root server then responds to the resolver with the address of a Top Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, our request is pointed toward the .com TLD.
4. The resolver then makes a request to the .com TLD.
5. The TLD server then responds with the IP address of the domain’s nameserver, example.com.
6. Lastly, the recursive resolver sends a query to the domain’s nameserver.
7. The IP address for example.com is then returned to the resolver from the nameserver.
8. The DNS resolver then responds to the web browser with the IP address of the domain requested initially.



9. Once the 8 steps of the DNS lookup have returned the IP address for example.com, the browser is able to make the request for the web page:The browser makes a HTTP request to the IP address.
10. The server at that IP returns the webpage to be rendered in the browser (step 10)

DNS

What is DNS Record?

DNS records (aka zone files) are instructions that live in authoritative DNS servers and provide information about a domain including what IP address is associated with that domain and how to handle requests for that domain. These records consist of a series of text files written in what is known as DNS syntax. DNS syntax is just a string of characters used as commands that tell the DNS server what to do. All DNS records also have a 'TTL', which stands for time-to-live, and indicates how often a DNS server will refresh that record.

You can think of a set of DNS records like a business listing on Yelp. That listing will give you a bunch of useful information about a business such as their location, hours, services offered, etc. All domains are required to have at least a few essential DNS records for a user to be able to access their website using a domain name, and there are several optional records that serve additional purposes.

Most common types of DNS record

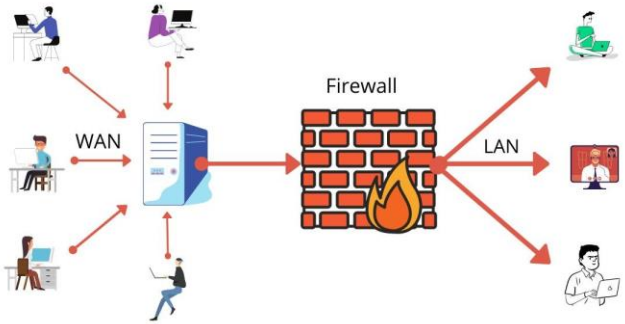
- **A record** - The record that holds the IP address of a domain.
- **CNAME record** - Forwards one domain or subdomain to another domain, does NOT provide an IP address.
- **MX record** - Directs mail to an email server.
- **TXT record** - Lets an admin store text notes in the record.
- **NS record** - Stores the name server for a DNS entry.
- **SOA record** - Stores admin information about a domain.
- **SRV record** - Specifies a port for specific services.

- **PTR record** - Provides a domain name in reverse-lookups.

Firewall

What is a Firewall?

In computing, a **firewall** is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.
The primary goal of a firewall is to block malicious traffic requests and data packets while allowing legitimate traffic through.



Types Of Firewall

Packet filtering: A packet-filtering firewall is a management program that can block network traffic IP protocol, an IP address, and a port number. This type of firewall is the most basic form of protection and is meant for smaller networks.A small amount of data is analyzed and distributed according to the filter's standards.

Proxy service: An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network. However, this also may impact throughput capabilities and the applications they can support.

Stateful inspection: Now thought of as a "traditional" firewall, a stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

Unified threat management (UTM) firewall: A UTM typically combines, in a loosely coupled way, the functions of a stateful inspection firewall with intrusion prevention and antivirus. It may also include additional services and often cloud management. UTMs focus on simplicity and ease of use

Next Generation Firewall (NGFW): Firewalls have evolved beyond simple packet filtering and stateful inspection. Most companies are deploying next-generation firewalls to block modern threats such as advanced malware and application-layer attacks.
According to Gartner, Inc.'s definition, a next-generation firewall must include: Standard firewall capabilities like stateful inspection, Integrated intrusion prevention, Application awareness and control to see and block risky apps, Upgrade paths to include future information feeds, Techniques to address evolving security threats

Networking Speed Details, Bandwidth, Throughput

Network speed measures the transfer rate of data from a source system to a destination system.
Network bandwidth is the amount of data that can be transferred per second ("the size of the pipe").
Combine the two, and you have what is known as **network throughput**.

Broadband – Broadband tells you how quickly data can be transferred, which is your overall measurement for the speed of your internet connection. This is significant for determining the speed at which your internet can perform certain tasks, such as streaming a movie

Bit – Internet speed is measured in bits per second (bps). This is the smallest unit of computer information, so you'll often see internet speeds referred to as megabits per second (Mbps)

Byte – 1 byte is equal to 8 bits. We use bytes to refer to how much memory is available or being transferred

Mbps – "Megabits per second" is how we gauge internet speeds. This number represents the bandwidth of an internet connection, which is how much data can be transferred each second.

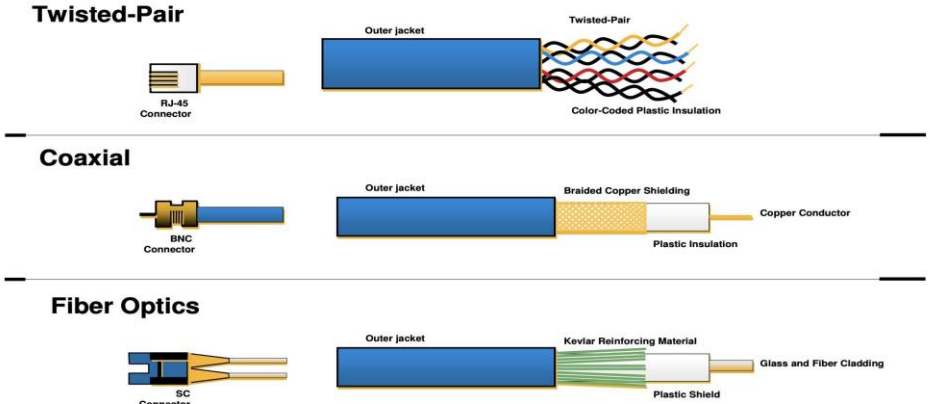
MBps – "Megabytes per second" measures the file size when talking about how much data can be transferred each second. You might also see this figure represented as MB.

Latency: Latency measures the delay in data transfer, telling you how fast data gets from a source to its destination. Internet connection types vary considerably when it comes to latency

Referencing all we have covered with AWS Networking

In AWS we have below main networking services, that is getting used by each and every Cloud engineer who are running private or public facing application on AWS

Amazon VPC



	Twisted Pair	Coaxial	Fiber Optic	Wireless LAN
Bandwidth	Up to 1 Gbps	10–100 Mbps	Up to 10 Gbps or higher	Up to 54 Mbps
Distance	Up to 100 m	Up to 500 m	Up to 60 km	Up to 100 m
Price	Least expensive	Inexpensive	Most expensive	Moderate

It's Define and provision a logically isolated network for your AWS resources

Learn Computer Networking With Kiran

Ref: Conceptually think of this as your isolated home network but at huge scale, where only if you add a public connection it will start accessing public internet otherwise it will stay isolated private network.

Amazon API Gateway

Create, maintain, and secure APIs at any scale

AWS Shield

Safeguard applications running on

AWS against DDoS attacks

AWS Transit Gateway

Connect VPCs and on-premises networks through a central hub

AWS Cloud Map

Discover AWS services connected to your applications

AWS WAF

Protect your web applications from common web exploits

Ref: conceptually think this as Next Generation Firewall (NGFW), which work on layer 7 of OSI model

AWS PrivateLink

Provide private connectivity between VPCs, services, and on-premises applications

Amazon CloudFront

Securely deliver data, videos, applications, and APIs to customers globally with low latency, and high transfer speeds

AWS Firewall Manager

Centrally configure and manage firewall rules

Ref: Conceptually think it as a network fire we just discussed few slide back

Elastic Load Balancing

Automatically distribute traffic across a pool of resources, such as instances, containers, IP addresses, and Lambda functions

Amazon Route 53

Route users to Internet applications with a managed DNS service

Ref: Conceptually refer it to the DNS chapter we have covered

AWS Direct Connect

Establish a private, dedicated connection between AWS and your datacenter, office, or colocation environment

AWS App Mesh

Provide application-level networking for containers and microservices

AWS Global Accelerator

Direct traffic through the AWS Global network to improve global application performance

AWS Virtual Private Network (VPN) - Client

Connect your users to AWS or on-premises resources using a Virtual Private Network

AWS Virtual Private Network (VPN) - Site to Site

Create an encrypted connection between your network and your Amazon VPCs or AWS Transit Gateways

Note: In the AWS Networking DeepDive Series we will cover each and every network services, each services has multiple subservices / components and we will cover everything in-depth! And what we have learned from this course and document , will be extremely useful while learning these 😇

Good luck!

I hope you'll use this knowledge and build awesome solutions.

If any issue contact me in Linkedin:
https://www.linkedin.com/in/kiranreddy-adulla/