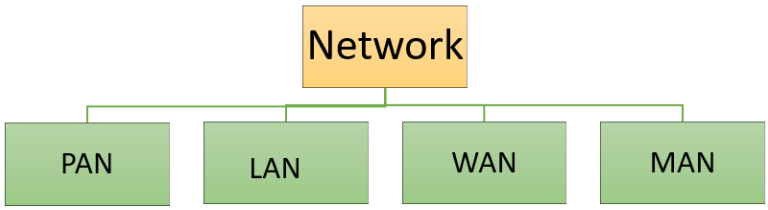
Types of Computer Networks: LAN, MAN, WAN, VPN

What Are the Important Types of Computer Networks?

There are various types of computer networks available. We can categorize them according to their size as well as their purpose.
The size of a network should be expressed by the geographic area and number of computers, which are a part of their networks. It includes devices housed in a single room to millions of devices spread across the world.



Some of the most popular network types are:

- PAN
- LAN
- MAN
- WAN

What is PAN (Personal Area Network)?

PAN is a computer network formed around a person. It generally consists of a computer, mobile, or personal digital assistant. PAN can be used for establishing communication among these personal devices for connecting to a digital network and the internet.

Characteristics of PAN

- It is mostly personal devices network equipped within a limited area.
- Allows you to handle the interconnection of IT devices at the surrounding of a single user.
- PAN includes mobile devices, tablet, and laptop.
- It can be wirelessly connected to the internet called WPAN.
- Appliances use for PAN: cordless mice, keyboards, and Bluetooth systems.

Advantages of PAN

Here, are important pros/benefits of using PAN network:

- PAN networks are relatively secure and safe
- It offers only short-range solution up to ten meters

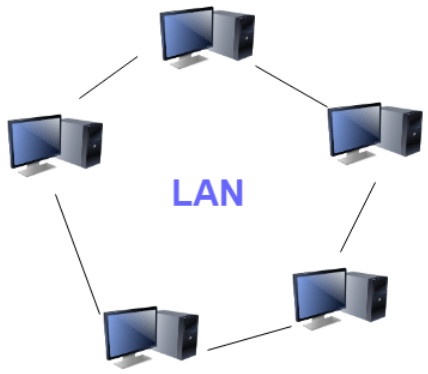
- Strictly restricted to a small area

Disadvantages of PAN

Here are important cons/ drawback of using PAN network:

- It may establish a bad connection to other networks at the same radio bands.
- Distance limits.

What is LAN?



A **L**ocal **A**rea **N**etwork (LAN) is a group of computer and peripheral devices which are connected in a limited area such as school, laboratory, home, and office building. It is a widely useful network for sharing resources like files, printers, games, and other application. The simplest type of LAN network is to connect computers and a printer in someone's home or office. In general, LAN will be used as one type of transmission medium.

It is a network which consists of less than 5000 interconnected devices across several buildings.

Characteristics of LAN

Here are important characteristics of a LAN network:

- It is a private network, so an outside regulatory body never controls it.
- LAN operates at a relatively higher speed compared to other WAN systems.
- There are various kinds of media access control methods like token ring and ethernet.

Advantages of LAN

Here are pros/benefits of using LAN:

- Computer resources like hard-disks, DVD-ROM, and printers can share local area networks. This significantly reduces the cost of hardware purchases.
- You can use the same software over the network instead of purchasing the licensed software for each client in the network.
- Data of all network users can be stored on a single hard disk of the server computer.

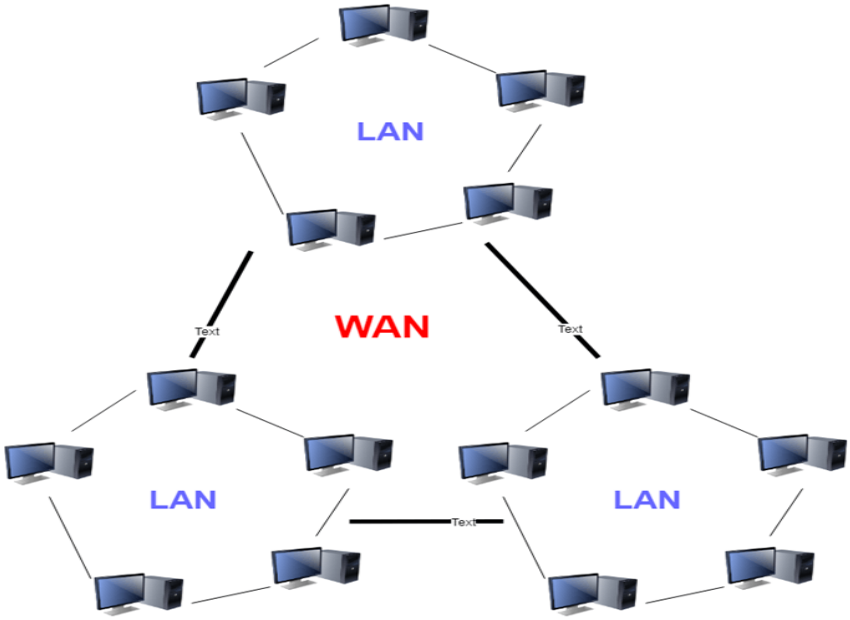
- You can easily transfer data and messages over networked computers.
- It will be easy to manage data at only one place, which makes data more secure.
- Local Area Network offers the facility to share a single internet connection among all the LAN users.

Disadvantages of LAN

Here are the important cons/ drawbacks of LAN:

- LAN will indeed save cost because of shared computer resources, but the initial cost of installing Local Area Networks is quite high.
- The LAN admin can check personal data files of every LAN user, so it does not offer good privacy.
- Unauthorized users can access critical data of an organization in case LAN admin is not able to secure centralized data repository.
- Local Area Network requires a constant LAN administration as there are issues related to software setup and hardware failures

What is WAN?



WAN (Wide Area Network) is another important computer network that which is spread across a large geographical area. WAN network system could be a connection of a LAN which connects with other LAN's using telephone lines and radio waves. It is mostly limited to an enterprise or an organization.

Characteristics of LAN:

- The software files will be shared among all the users; therefore, all can access to the latest files.
- Any organization can form its global integrated network using WAN.

Advantages of WAN

Here are the benefits/ pros of using WAN:

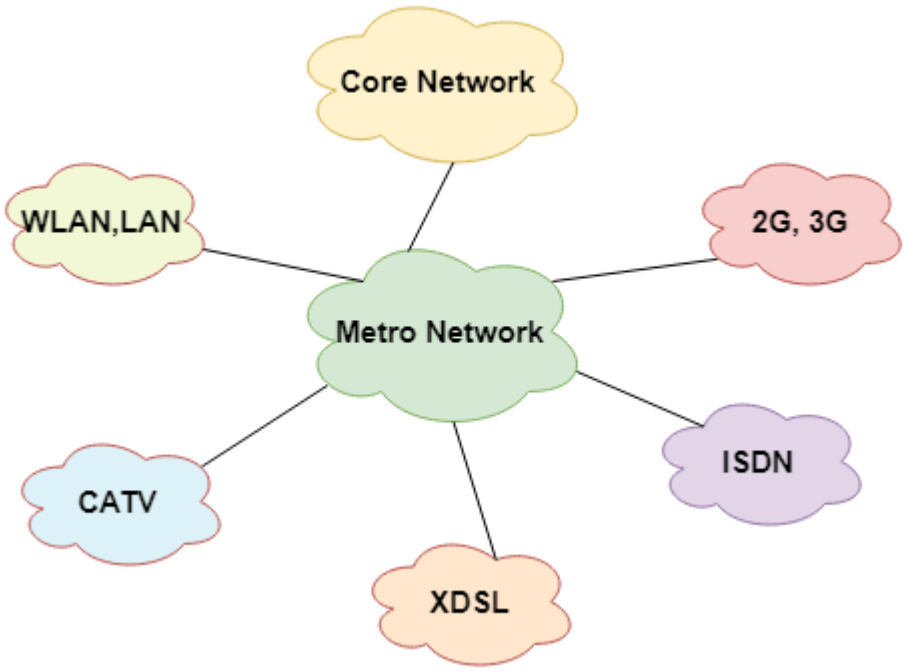
- WAN helps you to cover a larger geographical area. Therefore business offices situated at longer distances can easily communicate.
- Contains devices like mobile phones, laptop, tablet, computers, gaming consoles, etc.
- WLAN connections work using radio transmitters and receivers built into client devices.

Disadvantage of WAN

Here are drawbacks/cons of using WAN:

- The initial setup cost of investment is very high.
- It is difficult to maintain the WAN network. You need skilled technicians and network administrators.
- There are more errors and issues because of the wide coverage and the use of different technologies.
- It requires more time to resolve issues because of the involvement of multiple wired and wireless technologies.
- Offers lower security compared to other types of networks.

What is MAN?



A Metropolitan Area Network or MAN is consisting of a computer network across an entire city, college campus, or a small region. This type of network is large than a LAN, which is mostly limited to a single building or site. Depending upon the type of configuration, this type of network allows you to cover an area from several miles to tens of miles.

Characteristics of MAN

Here are important characteristics of the MAN network:

- It mostly covers towns and cities in a maximum 100 km range
- Mostly used medium is optical fibers, cables
- Data rates adequate for distributed computing applications.

Advantages of MAN

Here are pros/benefits of using MAN system:

- It offers fast communication using high-speed carriers, like fiber optic cables.
- It provides excellent support for an extensive size network and greater access to WANs.
- The dual bus in MAN network provides support to transmit data in both directions concurrently.
- A MAN network mostly includes some areas of a city or an entire city.

Disadvantages of MAN

Here are drawbacks/ cons of using the MAN network:

- You need more cable to establish MAN connection from one place to another.
- In MAN network it is tough to make the system secure from hackers

Virtual Private Network (VPN)

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.

What Is Network Topology?

The configuration, or topology, of a network is key to determining its performance. Network topology is the way a network is arranged, including the physical or logical description of how links and nodes are set up to relate to each other.

There are numerous ways a network can be arranged, all with different pros and cons, and some are more useful in certain circumstances than others. Admins have a range of options when it comes to choosing a network topology, and this decision must account for the size and scale of their business, its goals, and budget. Several tasks go into effective network topology management, including configuration management, visual mapping, and general performance monitoring. The key is to understand your objectives and requirements to create and manage the network topology in the right way for your business.

What Is Network Topology?

Network topology refers to how various nodes, devices, and connections on your network are physically or logically arranged in relation to each other. Think of your network as a city, and the topology as the road map. Just as there are many ways to arrange and maintain a city—such as making sure the avenues and boulevards can facilitate passage between the parts of town getting the most traffic—there are several ways to arrange a network. Each has advantages and disadvantages and depending on the needs of your company, certain arrangements can give you a greater degree of connectivity and security.

There are two approaches to network topology: physical and logical. Physical network topology, as the name suggests, refers to the physical connections and interconnections between nodes and the network—the wires, cables, and so forth. Logical network topology is a little more abstract and strategic, referring to the conceptual understanding of how and why the network is arranged the way it is, and how data moves through it.

Why Is Network Topology Important?

The layout of your network is important for several reasons. Above all, it plays an essential role in how and how well your network functions. Choosing the right topology for your company's operational model can increase performance while making it easier to locate faults, troubleshoot errors, and more effectively allocate resources across the network to ensure optimal network health. A streamlined and properly managed network topology can increase energy and data efficiency, which can in turn help to reduce operational and maintenance costs.

The design and structure of a network are usually shown and manipulated in a software-created network topology diagram. These diagrams are essential for a few reasons, but especially for how they can provide visual representations of both physical and logical layouts, allowing administrators to see the connections between devices when troubleshooting.

The way a network is arranged can make or break network functionality, connectivity, and protection from downtime. The question of, "What is network topology?" can be answered with an explanation of the two categories in the network topology.

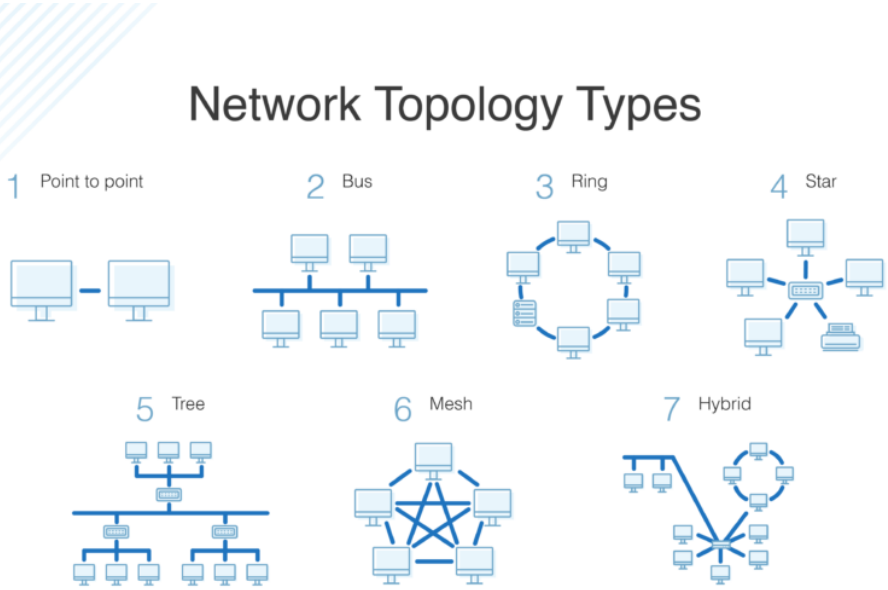
1. **Physical** – The physical network topology refers to the actual connections (wires, cables, etc.) of how the network is arranged. Setup, maintenance, and provisioning tasks require insight into the physical network.
2. **Logical** – The logical network topology is a higher-level *idea* of how the network is set up, including which nodes connect to each other and in which ways, as well as how data is transmitted through the network. Logical network topology includes any virtual and cloud resources.

Effective network management and monitoring require a strong grasp of both the physical and logical topology of a network to ensure your network is efficient and healthy.

What's the Most Common Type of Network Topology?

Building a local area network (LAN) topology can be make-or-break for your business, as you want to set up a resilient, secure, and easy-to-maintain topology.

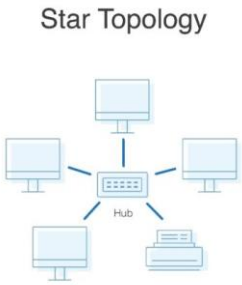
There are several different types of network topology and all are suitable for different purposes, depending on the overall network size and your objectives.



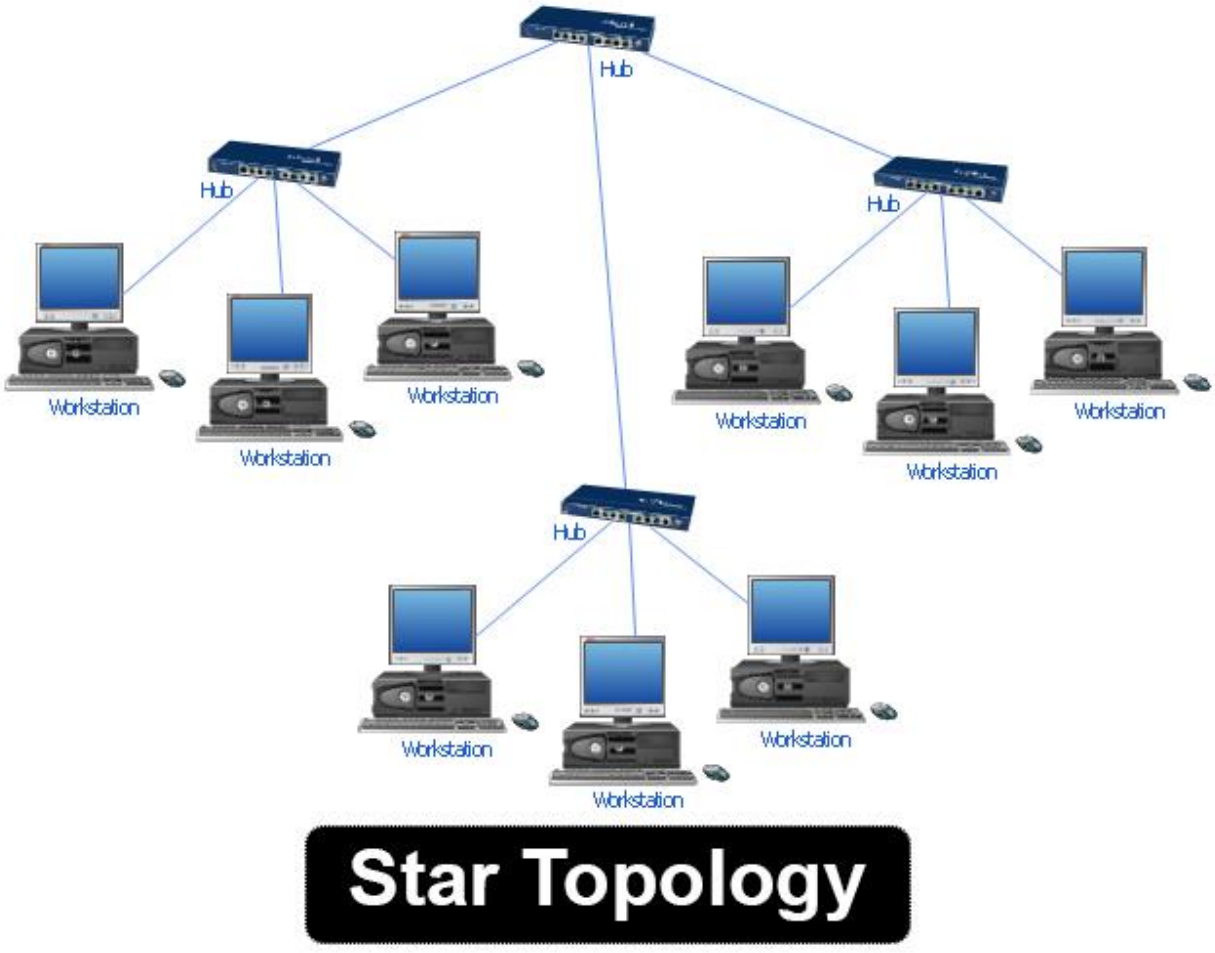
As with most things, there's no "right" or one-size-fits-all option. With this in mind, I'll walk you through the most common network topology definitions to give you a feel for the advantages and disadvantages of each.

What Is Star Topology?

A star topology, the most common network topology, is laid out so every node in the network is directly connected to one central hub via coaxial, twisted-pair, or fiber-optic cable. Acting as a server, this central node manages data transmission—as information sent from any node on the network has to pass through the central one to reach its destination—and functions as a repeater, which helps prevent data loss.



Distributed Star Topology



Advantages of Star Topology

Star topologies are common since they allow you to conveniently manage your entire network from a single location. Because each of the nodes is

independently connected to the central hub, should one go down, the rest of the network will continue functioning unaffected, making the star topology a stable and secure network layout.

Additionally, devices can be added, removed, and modified without taking the entire network offline.

On the physical side of things, the structure of the star topology uses relatively little cabling to fully connect the network, which allows for both straightforward setup and management over time as the network expands or contracts. The simplicity of the network design makes life easier for administrators, too, because it's easy to identify where errors or performance issues are occurring.

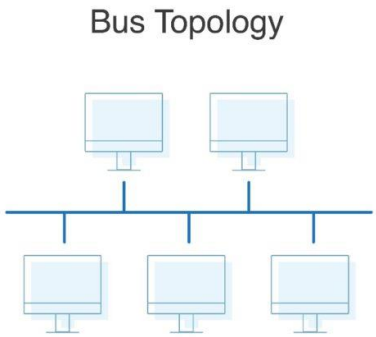
Disadvantages of Star Topology

On the flipside, if the central hub goes down, the rest of the network can't function. But if the central hub is properly managed and kept in good health, administrators shouldn't have too many issues.

The overall bandwidth and performance of the network are also limited by the central node's configurations and technical specifications, making star topologies expensive to set up and operate.

What Is Bus Topology?

A bus topology orients all the devices on a network along a single cable running in a single direction from one end of the network to the other—which is why it's sometimes called a "line topology" or "backbone topology." Data flow on the network also follows the route of the cable, moving in one direction.



Advantages of Bus Topology

Bus topologies are a good, cost-effective choice for smaller networks because the layout is simple, allowing all devices to be connected via a single coaxial or RJ45 cable. If needed, more nodes can be easily added to the network by joining additional cables.

Disadvantages of Bus Topology

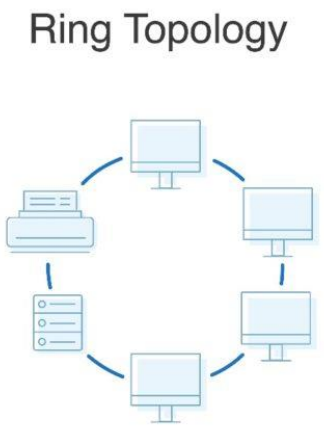
However, because bus topologies use a single cable to transmit data, they're somewhat vulnerable. If the cable experiences a failure, the whole network goes down, which can be time-consuming and expensive to restore, which can be less of an issue with smaller networks.

Bus topologies are best suited for small networks because there's only so much bandwidth, and every additional node will slow transmission speeds.

Furthermore, data is "half-duplex," which means it can't be sent in two opposite directions at the same time, so this layout is not the ideal choice for networks with huge amounts of traffic.

What Is Ring Topology? Single vs. Dual

Ring topology is where nodes are arranged in a circle (or ring). The data can travel through the ring network in either one direction or both directions, with each device having exactly two neighbors.



Pros of Ring Topology

Since each device is only connected to the ones on either side, when data is transmitted, the packets also travel along the circle, moving through each of the intermediate nodes until they arrive at their destination. If a large network is arranged in a ring topology, repeaters can be used to ensure packets arrive correctly and without data loss.

Only one station on the network is permitted to send data at a time, which greatly reduces the risk of packet collisions, making ring topologies efficient at transmitting data without errors.

By and large, ring topologies are cost-effective and inexpensive to install, and the intricate point-to-point connectivity of the nodes makes it relatively easy to identify issues or misconfigurations on the network.

Cons of Ring Topology

Even though it's popular, a ring topology is still vulnerable to failure without proper network management. Since the flow of data transmission moves unidirectionally between nodes along each ring, if one node goes down, it can take the entire network with it. That's why it's imperative for each of the nodes to be monitored and kept in good health. Nevertheless, even if you're vigilant and

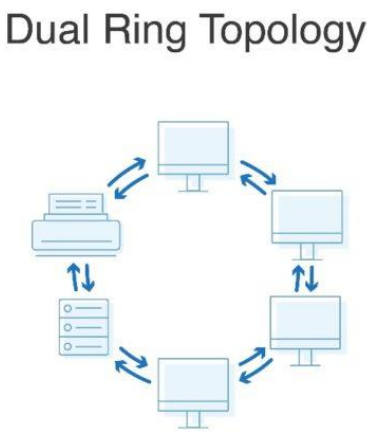
attentive to node performance, your network can still be taken down by a transmission line failure.

The question of scalability should also be taken into consideration. In a ring topology, all the devices on the network share bandwidth, so the addition of more devices can contribute to overall communication delays. Network administrators need to be mindful of the devices added to the topology to avoid overburdening the network's resources and capacity.

Additionally, the entire network must be taken offline to reconfigure, add, or remove nodes. And while that's not the end of the world, scheduling downtime for the network can be inconvenient and costly.

What Is Dual-Ring Topology?

A network with ring topology is half-duplex, meaning data can only move in one direction at a time. Ring topologies can be made full-duplex by adding a second connection between network nodes, creating a dual ring topology.



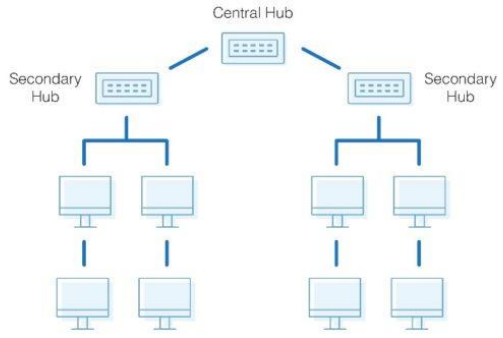
Advantages of Dual-Ring Topology

The primary advantage of dual ring topology is its efficiency: because each node has two connections on either side, information can be sent both clockwise and

counterclockwise along the network. The secondary ring included in a dual-ring topology setup can act as a redundant layer and backup, which helps solve for many of the disadvantages of traditional ring topology. Dual ring topologies offer a little extra security, too: if one ring fails within a node, the other ring is still able to send data.

What Is Tree Topology?

The tree topology structure gets its name from how the central node functions as a sort of trunk for the network, with nodes extending outward in a branch-like fashion. However, where each node in a star topology is directly connected to the central hub, a tree topology has a parent-child hierarchy to how the nodes are connected. Those connected to the central hub are connected linearly to other nodes, so two connected nodes only share one mutual connection. Because the tree topology structure is both extremely flexible and scalable, it's often used for wide area networks to support many spread-out devices.



Pros of Tree Topology

Combining elements of the star and bus topologies allows for the easy addition of nodes and network expansion. Troubleshooting errors on the network is also a straightforward process, as each of the branches can be individually assessed for performance issues.

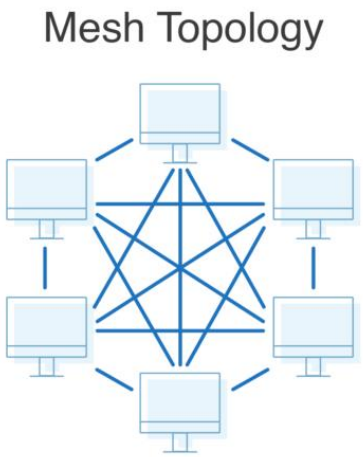
Cons of Tree Topology

As with the star topology, the entire network depends on the health of the root node in a tree topology structure. Should the central hub fail, the various node branches will become disconnected, though connectivity within—but not between—branch systems will remain.

Because of the hierarchical complexity and linear structure of the network layout, adding more nodes to a tree topology can quickly make proper management an unwieldy, not to mention costly, experience. Tree topologies are expensive because of the sheer amount of cabling required to connect each device to the next within the hierarchical layout.

What Is Mesh Topology?

A mesh topology is an intricate and elaborate structure of point-to-point connections where the nodes are interconnected. Mesh networks can be full or partial mesh. Partial mesh topologies are mostly interconnected, with a few nodes with only two or three connections, while full-mesh topologies are—surprise!—fully interconnected.



The web-like structure of mesh topologies offers two different methods of data transmission: routing and flooding. When data is routed, the nodes use logic to

determine the shortest distance from the source to destination, and when data is flooded, the information is sent to all nodes within the network without the need for routing logic.

Advantages of Mesh Topology

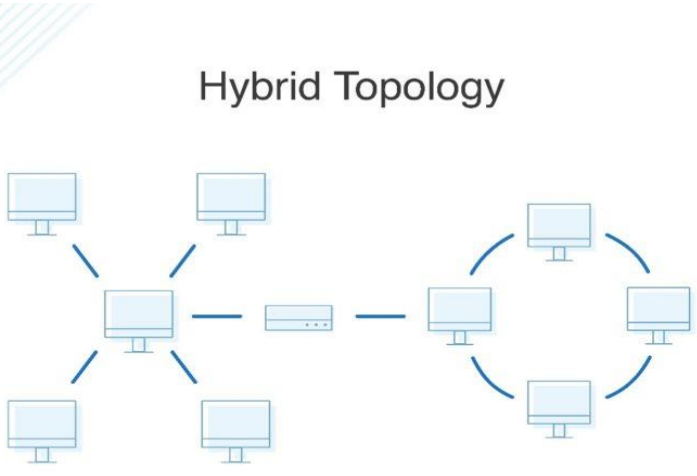
Mesh topologies are reliable and stable, and the complex degree of interconnectivity between nodes makes the network resistant to failure. For instance, no single device going down can bring the network offline.

Disadvantages of Mesh Topology

Mesh topologies are incredibly labor-intensive. Each interconnection between nodes requires a cable and configuration once deployed, so it can also be time-consuming to set up. As with other topology structures, the cost of cabling adds up fast, and to say mesh networks require a lot of cabling is an understatement.

What Is Hybrid Topology?

Hybrid topologies combine two or more different topology structures—the tree topology is a good example, integrating the bus and star layouts. Hybrid structures are most commonly found in larger companies where individual departments have personalized network topologies adapted to suit their needs and network usage.



Advantages of Hybrid Topology

The main advantage of hybrid structures is the degree of flexibility they provide, as there are few limitations on the network structure itself that a hybrid setup can't accommodate.

Disadvantages of Hybrid Topology

However, each type of network topology comes with its own disadvantages, and as a network grows in complexity, so too does the experience and know-how required on the part of the admins to keep everything functioning optimally. There's also the monetary cost to consider when creating a hybrid network topology.

Which Topology Is Best for Your Network?

No network topology is perfect, or even inherently better than the others, so determining the right structure for your business will depend on the needs and size of your network. Here are the key elements to consider:

- Length of cable needed
- Cable type
- Cost
- Scalability

Cable Length

Generally, the more cable involved in network topology, the more work it'll require to set up. The bus and star topologies are on the simpler side of things, both being fairly lightweight, while mesh networks are much more cable- and labor-intensive.

Cable Type

The second point to consider is the type of cable you'll install. Coaxial and twisted-pair cables both use insulated copper or copper-based wiring, while fiber-optic cables are made from thin and pliable plastic or glass tubes. Twisted-pair cables are cost-effective but have less bandwidth than coaxial cables. Fiber-optic cables are high performing and can transmit data far faster than twisted-pair or coaxial cables, but they also tend to be far more expensive to install,

because they require additional components like optical receivers. So, as with your choice of network topology, the wiring you select depends on the needs of your network, including which applications you'll be running, the transmission distance, and desired performance.

Cost

As I've mentioned, the installation cost is important to account for, as the more complex network topologies will require more time and funding to set up. This can be compounded if you're combining different elements, such as connecting a more complex network structure via more expensive cables (though using fiber-optic cables in a mesh network is overdoing it, if you ask me, because of how interconnected the topology is). Determining the right topology for your needs, then, is a matter of striking the right balance between installation and operating costs and the level of performance you require from the network.

Scalability

The last element to consider is scalability. If you anticipate your company and network expanding—or if you'd like it to be able to—it'll save you time and hassle down the line to use an easily modifiable network topology. Star topologies are so common because they allow you to add, remove, and alter nodes with minimal disruption to the rest of the network. Ring networks, on the other hand, have to be taken entirely offline for any changes to be made to any of the nodes.

How to Map Network Topology

When you're starting to design a network, topology diagrams come in handy. They allow you to see how the information will move across the network, which, in turn, allows you to predict potential choke points. Visual representation makes it easier to create a streamlined and efficient network design, while also acting as a good reference point if you find yourself needing to troubleshoot errors.

A topology diagram is also essential for having a comprehensive understanding of your network's functionality. In addition to assisting with the troubleshooting process, the bird's-eye view provided by a topology diagram can help you visually identify the pieces of the infrastructure your network is lacking, or which nodes need monitoring, upgrading, or replacing.

MANET

3.1 Concepts of types of MANET (Mobile Ad hoc Network)

MANET stands for Mobile adhoc Network also called as wireless adhoc network or adhoc wireless network. They consist of a set of mobile nodes connected wirelessly in a self-configured, self-healing network without having a fixed infrastructure. MANET nodes are free to move randomly as the network topology changes frequently.

Types of MANET –

Vehicular Ad hoc Network (VANETs) –

Enable effective communication with another vehicle or with the roadside equipments. Intelligent vehicular ad hoc networks(InVANETs) deals with another vehicle or with roadside equipments.

Smart Phone Ad hoc Network (SPANC) –

To create peer-to-peer networks without relying on cellular carrier networks, wireless access points, or traditional network infrastructure. Here peers can join or leave the network without destroying it.

Internet based Mobile Ad hoc Network (iMANETs) –

It supports internet protocols such as TCP/UDP and IP. To link mobile nodes and establish routes distributed and automatically.

Hub-Spoke MANET:

Multiple sub MANET's may be connected in hub-spoke VPN to create a geographically distributed MANET. Normal Ad-hoc routing algorithm does not apply directly.

Military or Tactical MANETs –

This is used by the military units. Emphasis on data rate, real-time demand, fast re-routing during mobility, security, radio range, etc.

Flying Ad hoc Network (FANETs) –

This is composed of unmanned aerial vehicles (commonly known as drones). Provides links to remote areas and mobility.

Mobile Ad hoc Networks (MANETs) are dynamically configured wireless networks where devices communicate directly with each other without relying on fixed infrastructure like routers or access points. Examples of MANETs include military operations, disaster relief, and vehicular networks.

Here's a more detailed breakdown:

Examples of MANETs:

- **Military Operations:**

  MANETs allow soldiers to communicate and share information in the field, even when traditional communication infrastructure is unavailable.

- **Disaster Relief:**

  In disaster situations, MANETs can be quickly deployed to facilitate communication between rescue teams and support personnel, especially when traditional networks are down.

- **Vehicular Networks (VANETs):**

  Vehicles can communicate with each other and roadside infrastructure to improve traffic flow, safety, and provide real-time information to drivers.

- **Emergency Response:**

  MANETs can be used in emergencies like fires or medical crises, allowing for communication between first responders and medical personnel.

- **Personal Area Networks (PANs):**

  Bluetooth-based MANETs can be used to create temporary networks between devices like smartphones and laptops for file sharing and other local communication.

- **Smart Homes:**

  MANETs can connect various smart devices within a home, enabling automated control and communication between devices.

- **Sensor Networks:**

  MANETs can facilitate communication between sensor nodes in applications like environmental monitoring or precision agriculture.

- **Commercial Applications:**

  MANETs are used in trade fairs, shopping malls, and other businesses that require dynamic network setup and access to databases.

- **Public Safety:**

  Police and other emergency services can utilize MANETs to communicate during events or in situations where traditional communication is compromised.

- **Research and Development:**
  MANETs are also used in research to study network protocols, routing algorithms, and other aspects of wireless communication.
  MANET stands for Mobile Adhoc Network also called a wireless adhoc network or Adhoc wireless network that usually has a routable networking environment on top of a Link Layer ad hoc network. They consist of a set of mobile nodes connected wirelessly in a self-configured, self-healing network without having a fixed infrastructure. MANET nodes are free to move randomly as the network topology changes frequently. Each node behaves as a router as it forwards traffic to other specified nodes in the network.

What is MANET?

A MANET is a decentralized wireless network consisting of mobile devices (nodes) that communicate with each other without relying on a fixed infrastructure. MANET forms a highly dynamic autonomous topology with the presence of one or multiple different transceivers between nodes. MANETs consist of a peer-to-peer, self-forming, self-healing network MANETs circa 2000-2015 typically communicate at radio frequencies (30MHz-5GHz). This can be used in road safety, ranging from sensors for the environment, home, health, disaster rescue operations, air/land/navy defense, weapons, robots, etc.

Characteristics of MANET

- **Dynamic Topologies:** Network topology which is typically multihop may change randomly and rapidly with time, it can form unidirectional or bi-directional links.
- **Bandwidth constrained, variable capacity links:** Wireless links usually have lower reliability, efficiency, stability, and capacity as compared to a wired network
- **Autonomous Behavior:** Each node can act as a host and router, which shows its autonomous behavior.
- **Energy Constrained Operation:** As some or all the nodes rely on batteries or other exhaustible means for their energy. Mobile nodes are characterized by less memory, power, and lightweight features.
- **Limited Security:** Wireless networks are more prone to security threats. A centralized firewall is absent due to the distributed nature of the operation for security, routing, and host configuration.
- **Less Human Intervention:** They require minimum human intervention to configure the network, therefore they are dynamically autonomous in nature.

Advantages of MANET

- Separation from central network administration.
- Each node can play both the roles ie. of router and host showing autonomous nature.
- Self-configuring and self-healing nodes do not require human intervention.
- Highly scalable and suits the expansion of more network hub.

Disadvantages of MANET

- Resources are limited due to various constraints like noise, interference conditions, etc.
- Lack of authorization facilities.
- More prone to attacks due to limited physical security.
- High latency i.e. There is a huge delay in the transfer of data between two sleeping nodes.

Improvement in MANET

- **Quality of Service (QoS):** Researchers are working to improve the quality of service of MANET by developing efficient routing protocols that provide better bandwidth, throughput, and latency.
- **Security:** To ensure the security of the MANET, researchers are developing efficient security mechanisms that provide encryption, authentication, and authorization facilities.
- **Power management:** To enhance the lifetime of MANET nodes, researchers are working on developing efficient power management techniques that reduce the energy consumption of nodes.
- **Multimedia support:** Researchers are working to provide multimedia support to MANET by developing efficient routing protocols that can handle multimedia traffic efficiently.
- **Standardization:** To ensure the interoperability of different MANET devices, researchers are working on developing standard protocols and interfaces that can be used by different MANET devices.

Applications of MANET

- Military and Defense Operations
- Healthcare
- Sensor Networks
- Wireless Sensor Networks
- Internet of Things (IoT)

VANET

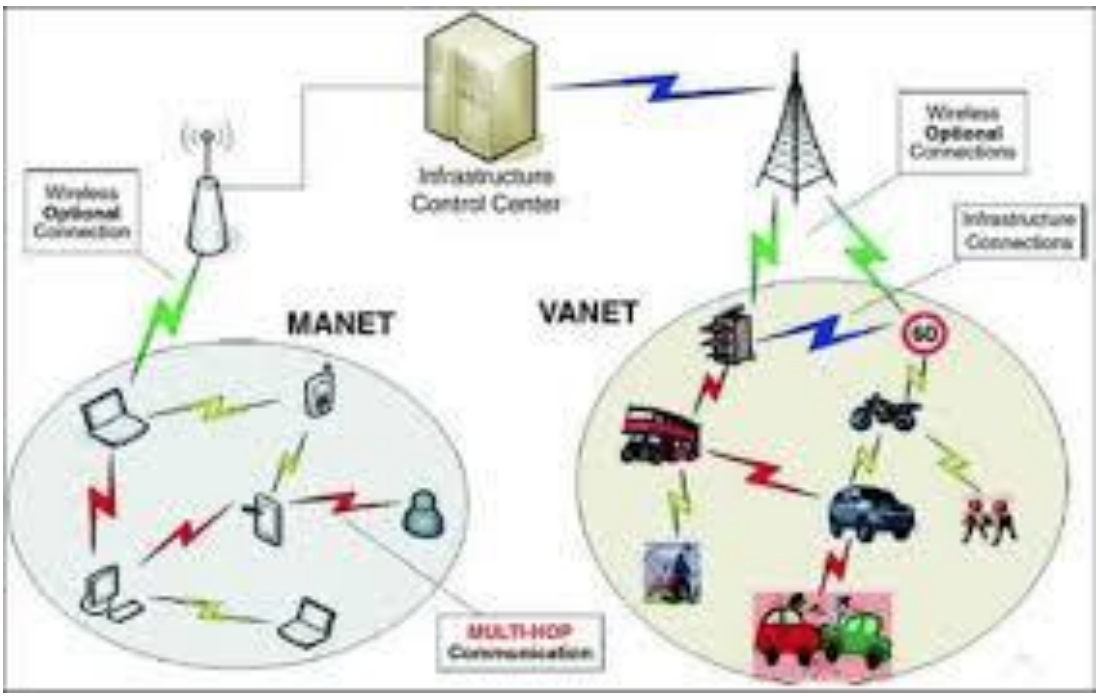
VANET, or Vehicular Ad hoc Network, is a type of mobile ad hoc network where vehicles act as nodes, communicating with each other and with roadside infrastructure to create a wireless network. This technology enables various applications for safety, convenience, and efficiency in transportation.

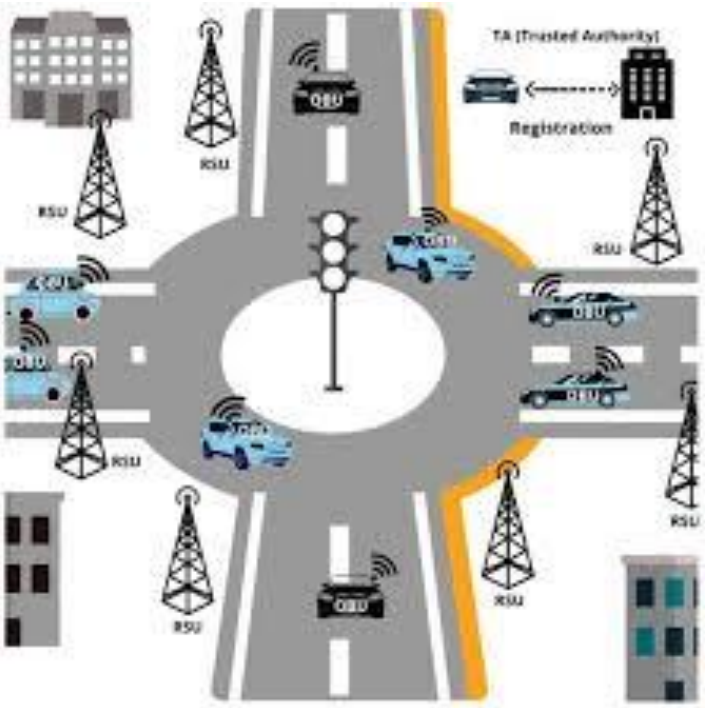
Examples of VANET applications:

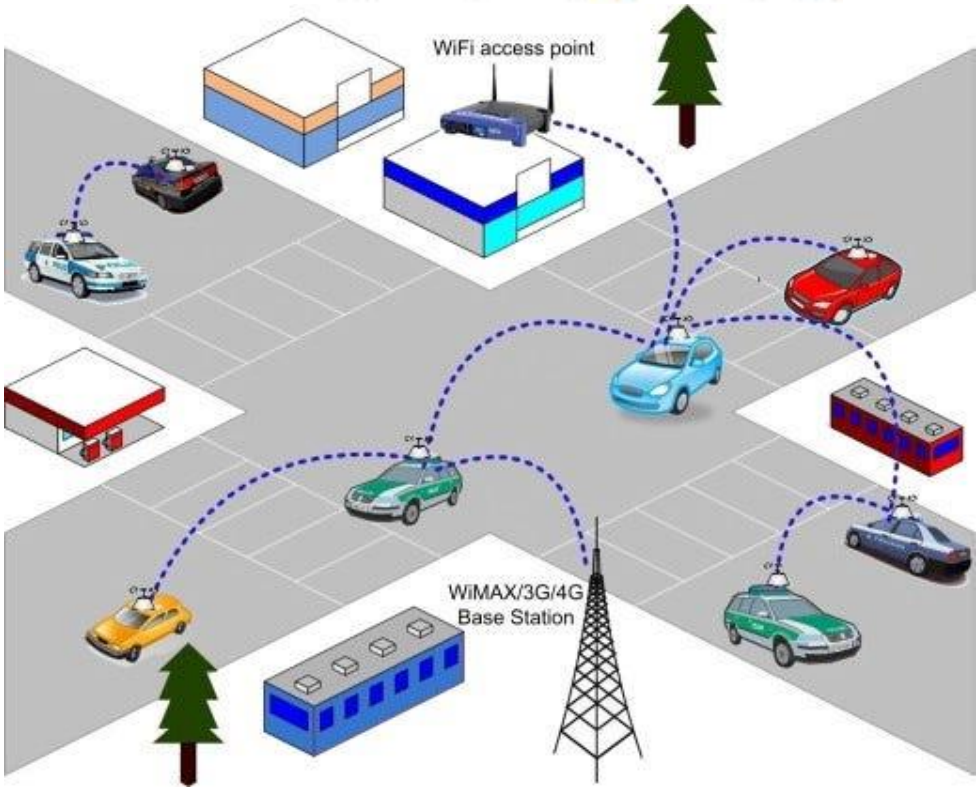
- **Safety:**
- **Emergency Electronic Brake Lights:** Alerts drivers to braking vehicles even when they are not visible (e.g., obscured by other vehicles).
- **Collision Avoidance:** Enables vehicles to communicate and prevent collisions by sharing information about speed, direction, and proximity.
- **Accident and Hazard Warnings:** Disseminates information about accidents or hazards on the road to other vehicles, helping them avoid delays and potential dangers.
- **Emergency Vehicle Notification:** Alerts other drivers to the presence and location of emergency vehicles, allowing them to yield the right-of-way.
  Traffic Management:
- **Real-time Traffic Information:** Provides up-to-date traffic conditions, including congestion, accidents, and road closures, to navigation systems and drivers.
- **Dynamic Route Guidance:** Suggests optimal routes based on real-time traffic conditions, minimizing travel time and fuel consumption.
- **Platooning:** Allows vehicles to closely follow each other in "road trains" by wirelessly sharing acceleration and steering information, potentially improving traffic flow.
  Comfort and Convenience:
- **In-Vehicle Infotainment:** Provides access to internet services, entertainment, and personalized content while on the road.

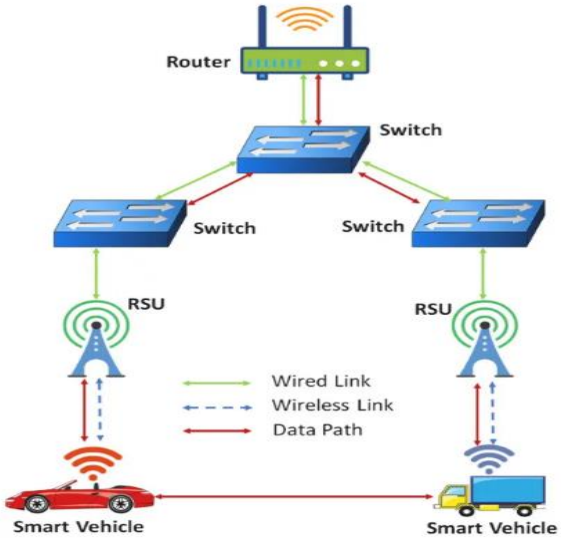
- **On-the-Road Services:** Advertises nearby businesses, services (e.g., restaurants, gas stations), and special offers to drivers.
- **Electronic Toll Collection:** Enables automatic toll payment as vehicles pass through toll booths.
Other applications:
- **Smart Parking:** Helps drivers find available parking spaces in real-time.
- **Remote Diagnostics and Maintenance:** Allows vehicles to communicate with service centers for remote diagnostics and maintenance.
- **Autonomous Driving:** VANETs are crucial for the development and implementation of autonomous vehicles, enabling them to communicate and coordinate with each other and the surrounding environment.

In essence, VANETs create a dynamic and intelligent transportation ecosystem, enhancing safety, efficiency, and convenience for drivers and passengers alike.



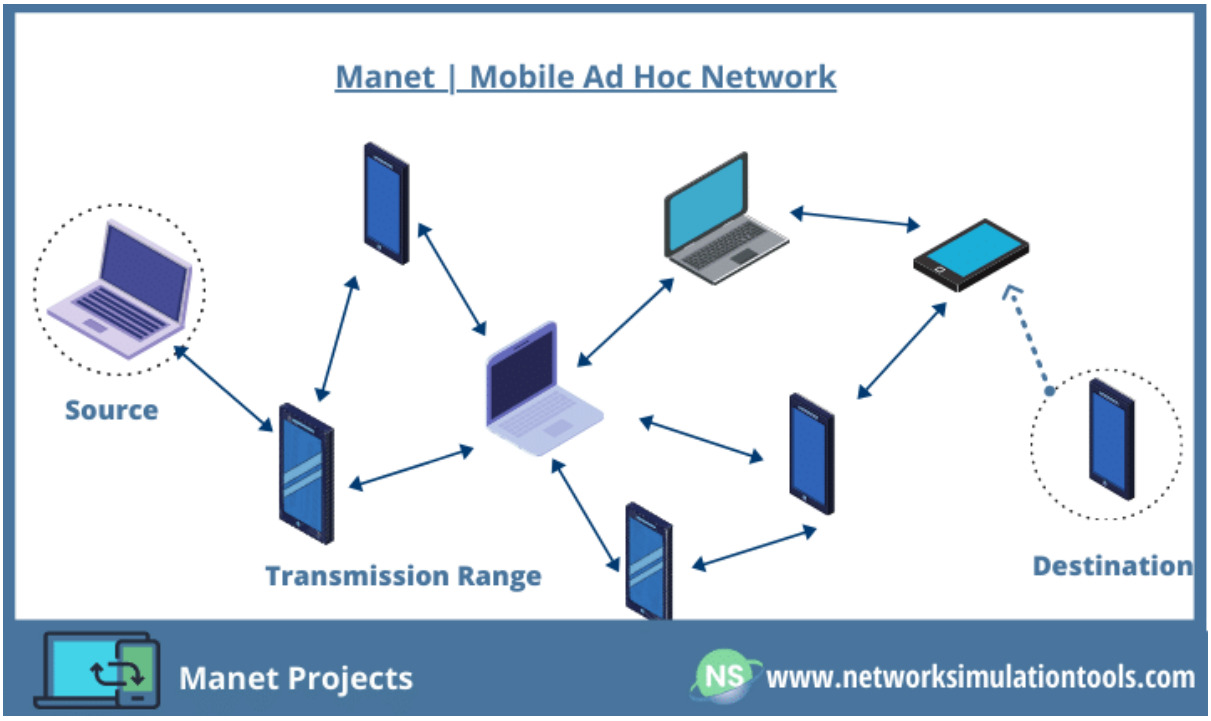

TA [Trusted Authority]
Registration
OBU
RSU


WiFi access point
WiMAX/3G/4G
Base Station



SPANs

Smartphone Ad hoc Networks (SPANs) are examples of ad hoc networks where mobile devices communicate directly with each other without relying on a central access point like a Wi-Fi router or cellular tower. These networks are often used in situations where traditional infrastructure is unavailable or unreliable, or to create temporary, localized networks.



Here are some examples of SPANs in action:

- **Emergency Communication:**

  During natural disasters or other crises, SPANs can enable quick communication between individuals and first responders when traditional

networks are down. For example, users in Hong Kong protests have used apps like FireChat and Bridgefy to communicate during events where access to traditional networks was limited.

- **Remote Areas:**

  SPANs can provide communication in remote locations where cellular or Wi-Fi coverage is lacking, such as in rural communities or during outdoor events.

- **Events and Gatherings:**

  SPANs can be used to create temporary, localized networks for sharing information and communicating at events like concerts or conferences.

- **Military and Emergency Services:**

  These networks can be deployed by military and emergency services for quick communication in the field.

- **Content Sharing:**

  SPANs can be used to share various types of content, including pictures, videos, and other multimedia, among nearby devices.

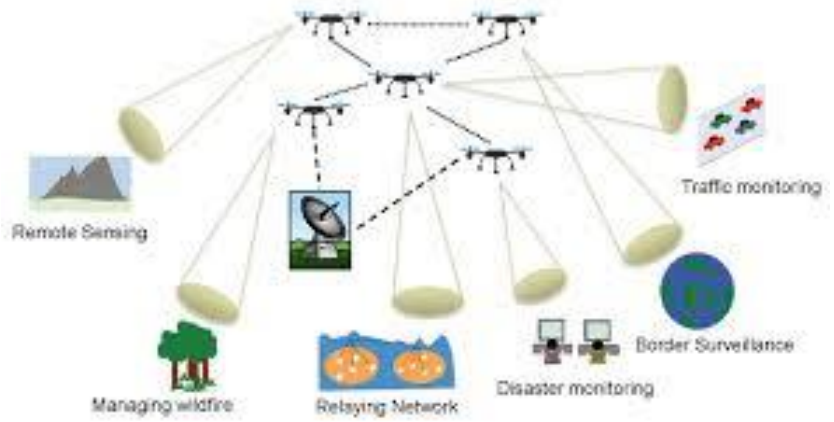
- **Research and Development:**

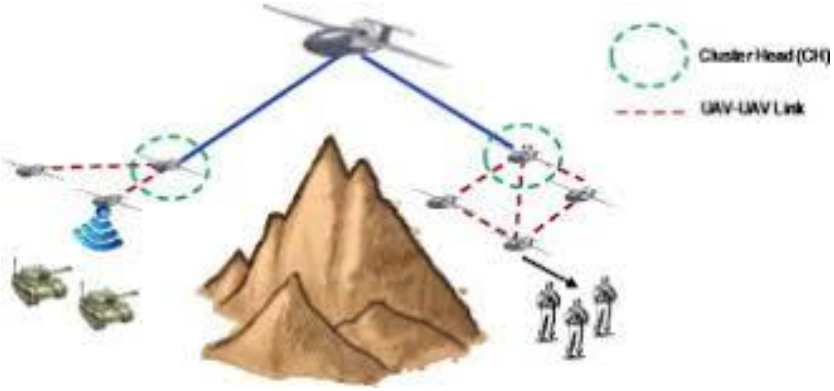
  SPANs are also used in research for studying various aspects of ad hoc networking like routing protocols, security, and energy consumption.

- **Crowdsourcing:**
  SPANs can be used to gather data from a large group of people, such as in surveys or studies.
  In essence, SPANs leverage the built-in wireless capabilities of smartphones (like Bluetooth or Wi-Fi Direct) to create dynamic, self-organizing networks on demand.

FANET

Flying Ad hoc Networks (FANETs) are networks formed by a collection of Unmanned Aerial Vehicles (UAVs) or drones that communicate with each other wirelessly, without the need for a fixed infrastructure. They are a type of Mobile Ad hoc Network (MANET) but with unique characteristics due to the high mobility and three-dimensional movement of UAVs.





Here are some examples of FANET applications:

Military:

- **Surveillance and Reconnaissance:**

  FANETs can be used for real-time surveillance of a battlefield or other areas, providing situational awareness to ground forces.

- **Target Tracking:**

  UAVs can track and follow moving targets, relaying information to command centers.

- **Border Monitoring:**

  FANETs can be deployed to monitor and patrol borders, detecting potential incursions or illegal activities.

- **Search and Rescue:**
  In disaster situations, FANETs can be used to locate survivors and deliver supplies.
  Civilian:

- **Environmental Monitoring:**

  FANETs can be used to monitor air and water quality, track wildlife, or assess damage from natural disasters.

- **Traffic Monitoring:**

  UAVs can provide real-time traffic information, helping to manage congestion and improve traffic flow.
- **Agricultural Monitoring:**

  FANETs can be used to assess crop health, monitor irrigation, and apply pesticides or fertilizers.
- **Goods Delivery:**

  Drones can be used to deliver packages and other goods, potentially revolutionizing logistics and e-commerce.
- **Construction:**

  FANETs can be used for site surveying, progress monitoring, and infrastructure inspection.
- **Disaster Relief:**

  FANETs can be used to deliver supplies, assess damage, and coordinate rescue efforts in disaster-stricken areas.
- **Public Safety:**

  FANETs can assist with crowd control, search and rescue operations, and event monitoring.
- **Filmmaking and Photography:**

  Drones equipped with cameras can capture aerial footage for movies, documentaries, and other media.
- **Infrastructure Inspection:**

  FANETs can be used to inspect bridges, power lines, and other critical infrastructure.
- **Precision Agriculture:**
  FANETs can be used to monitor crops, optimize irrigation, and apply pesticides or fertilizers.
  Key Characteristics of FANETs:
- **High Mobility:**

  UAVs in FANETs can move at high speeds and change direction rapidly, making communication challenging.
- **Dynamic Topology:**

  The network topology is constantly changing as UAVs move and communicate with each other.
- **Limited Resources:**

  UAVs have limited battery life, processing power, and storage capacity.

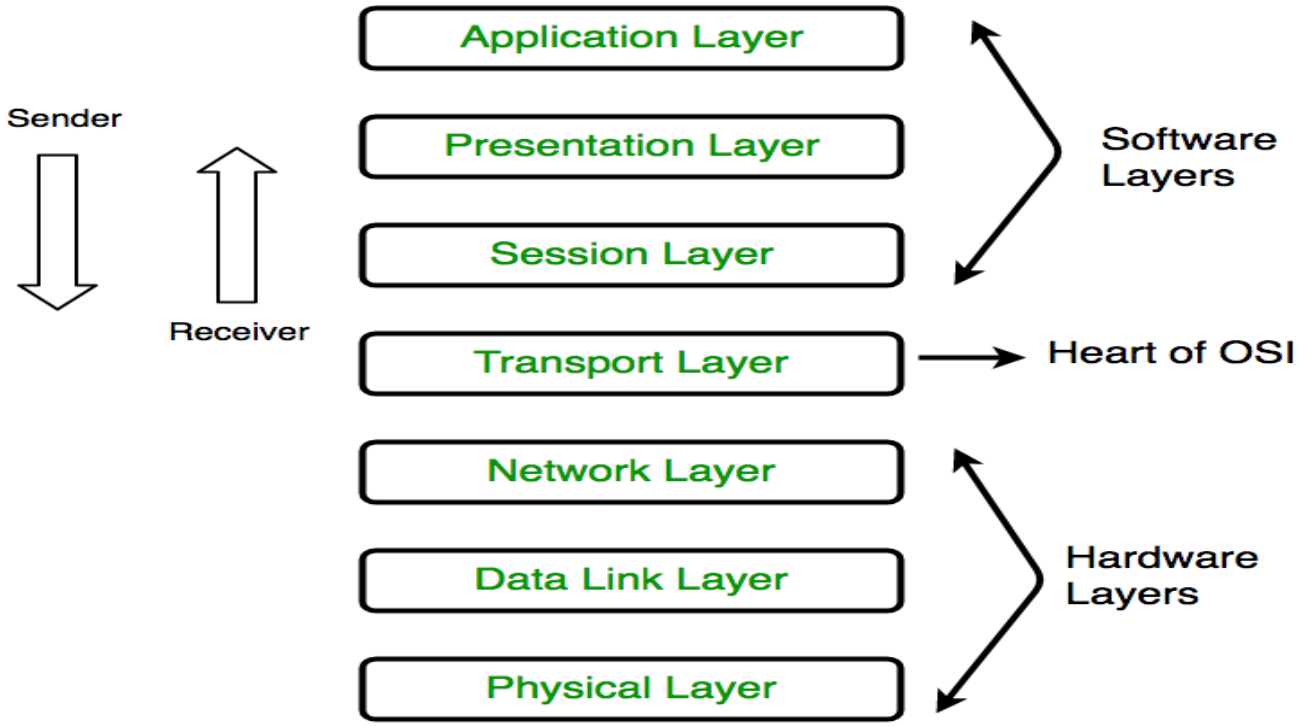
- **3D Movement:**

  FANETs operate in three dimensions, unlike other ad hoc networks that typically operate on a 2D plane.

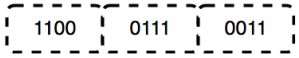
- **Low Node Density:**
  The number of UAVs in a FANET can vary greatly, but often it is relatively sparse.

Layers of OSI Model

OSI stands for **Open Systems Interconnection**. It has been developed by ISO – '**International Organization of Standardization**', in the year 1984. It is a 7 layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.



1. Physical Layer (Layer 1) :
The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.** It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.



The functions of the physical layer are :

1. **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
2. **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
3. **Physical topologies:** Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topolgy.
4. **Transmission mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

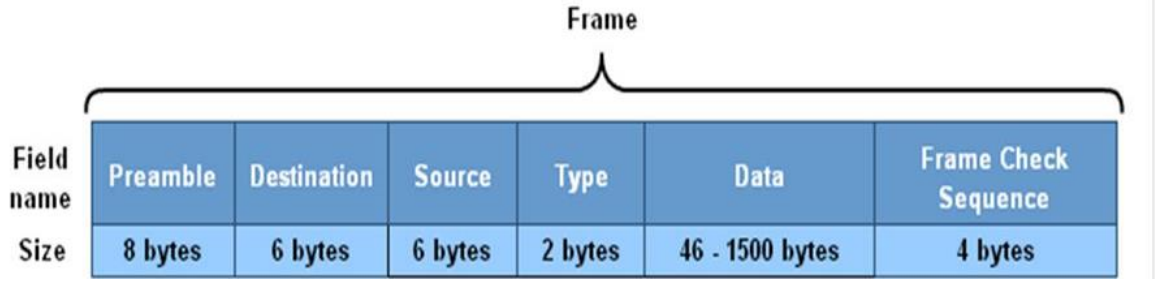
* Hub, Repeater, Modem, Cables are Physical Layer devices.
** Network Layer, Data Link Layer and Physical Layer are also known as **Lower Layers** or **Hardware Layers**.

2. Data Link Layer (DLL) (Layer 2) :
The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address. Data Link Layer is divided into two sub layers :

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

The packet received from Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.
The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.
The functions of the data Link layer are :

A Common Data Link Layer Protocol for LANs



1. **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. **Physical addressing:** After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
3. **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames manage by CRC (Cyclic Redundancy Check).

4. **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus , flow control coordinates that amount of data that can be sent before receiving acknowledgement.
5. **Access control:** When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

** Packet in Data Link layer is referred as **Frame**.*
*** Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.*
**** Switch & Bridge are Data Link Layer devices.*

3. Network Layer (Layer 3) :
Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP address are placed in the header by the network layer.
The functions of the Network layer are :

1. **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.
2. **Logical Addressing:** In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

* *Segment* in Network layer is referred as **Packet**.
** Network layer is implemented by networking devices such as routers.

4. Transport Layer (Layer 4) :
Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.
At sender's side: Transport layer receives the formatted data from the upper layers, performs **Segmentation** and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.
Note: The sender need to know the port number associated with the receiver's application.
Generally, this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default port assigned.
• **At receiver's side:**Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.
The functions of the transport layer are :

1. **Segmentation and Reassembly:** This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segment produced has a header associated with it. The transport layer at the destination station reassembles the message.

2. **Service Point Addressing:** In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

The services provided by the transport layer :

1. **Connection Oriented Service:** It is a three-phase process which include
   – Connection Establishment
   – Data Transfer
   – Termination / disconnection
   In this type of transmission, the receiving device sends an acknowledgement, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.
2. **Connection less service:** It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

** Data in the Transport Layer is called as **Segments**.*

*** Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.*

*Transport Layer is called as **Heart of OSI** model.*

5. Session Layer (Layer 5) :

This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.

The functions of the session layer are :

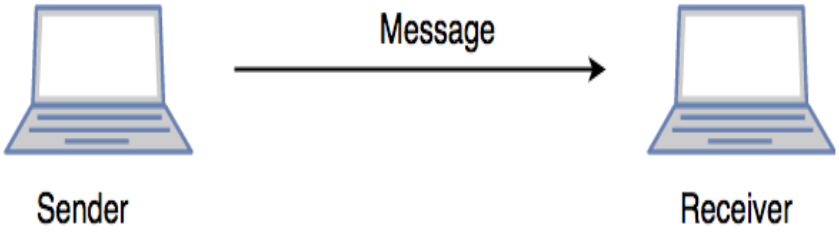
1. **Session establishment, maintenance and termination:** The layer allows the two processes to establish, use and terminate a connection.
2. **Synchronization:** This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
3. **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

***All the below 3 layers(including Session Layer) are integrated as a single layer in the TCP/IP model as "Application Layer".*

***Implementation of these 3 layers is done by the network application itself. These are also known as **Upper Layers** or **Software Layers**.*

SCENARIO:

Let's consider a scenario where a user wants to send a message through some Messenger application running in his browser. The "Messenger" here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data) and converted into bits (0's and 1's) so that it can be transmitted.



6. Presentation Layer (Layer 6) :
Presentation layer is also called the **Translation layer**.The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.
The functions of the presentation layer are :

1. **Translation :** For example, ASCII to EBCDIC.
2. **Encryption/ Decryption :** Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
3. **Compression:** Reduces the number of bits that need to be transmitted on the network.

7. Application Layer (Layer 7) :
At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.
Ex: Application – Browsers, Skype Messenger etc.
***Application Layer is also called as Desktop Layer.*
The functions of the Application layer are :

1. Network Virtual Terminal
2. FTAM-File transfer access and management
3. Mail Services
4. Directory Services

OSI model acts as a reference model and is not implemented in the Internet because of its late invention. Current model being used is the TCP/IP model

The OSI (Open Systems Interconnection) model is a conceptual framework that standardizes the functions of a telecommunication or computing system into seven layers. It provides a common language and structure for understanding how different network devices and software communicate. Each layer has specific functions and protocols, and they work together to transmit data between devices.

Here's a breakdown of the seven layers:

1. Physical Layer: This layer handles the physical transmission of data through the network medium (cables, wireless signals). It deals with the electrical, mechanical, and physical specifications of the network.

2. Data Link Layer: This layer ensures error-free transfer of data frames between two directly connected nodes. It uses MAC addresses for identifying devices and handles error detection and correction within a network segment.

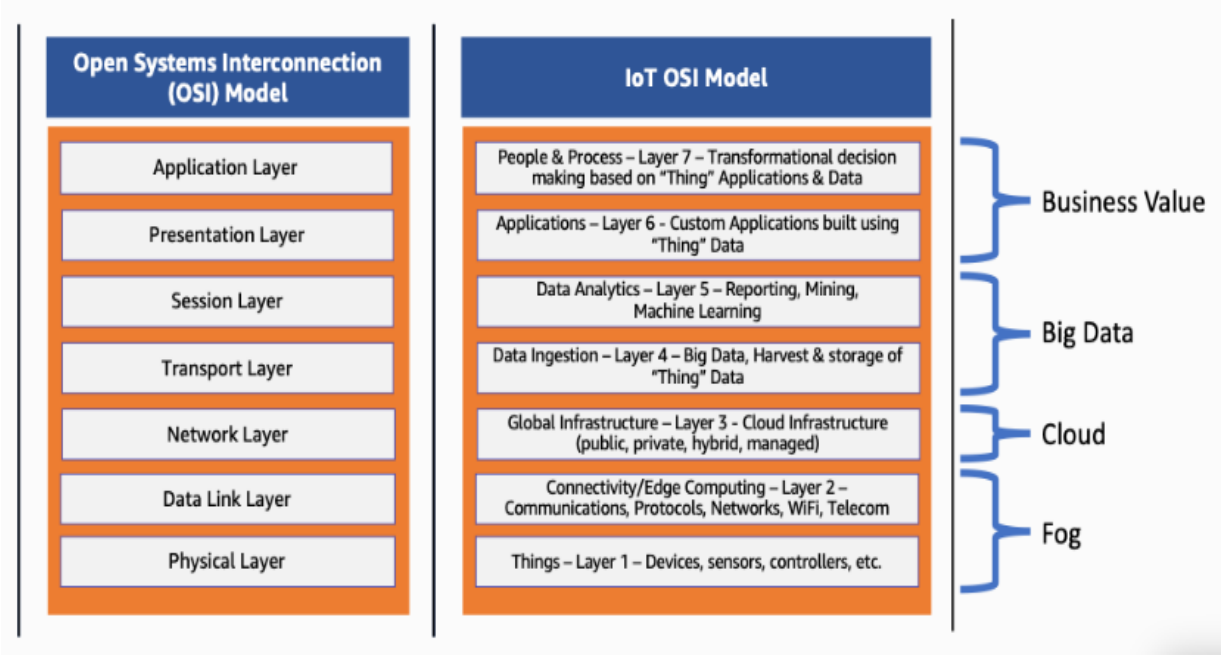
3. Network Layer: This layer is responsible for routing data packets to their destination across networks. It uses IP addresses and routing protocols to determine the best path for data transmission.

4. Transport Layer: This layer manages data flow, error checking, and delivery between applications. It uses protocols like TCP (Transmission Control Protocol) for reliable, connection-oriented communication and UDP (User Datagram Protocol) for faster, connectionless communication.

5. Session Layer: This layer establishes, manages, and terminates communication sessions between applications.

6. Presentation Layer: This layer handles data formatting, encryption, and compression to ensure data is in a usable format for the application layer.

7. Application Layer: This is the layer closest to the user, providing the interface for applications to access network services like email, file transfer, and web browsing.



Packet Switching

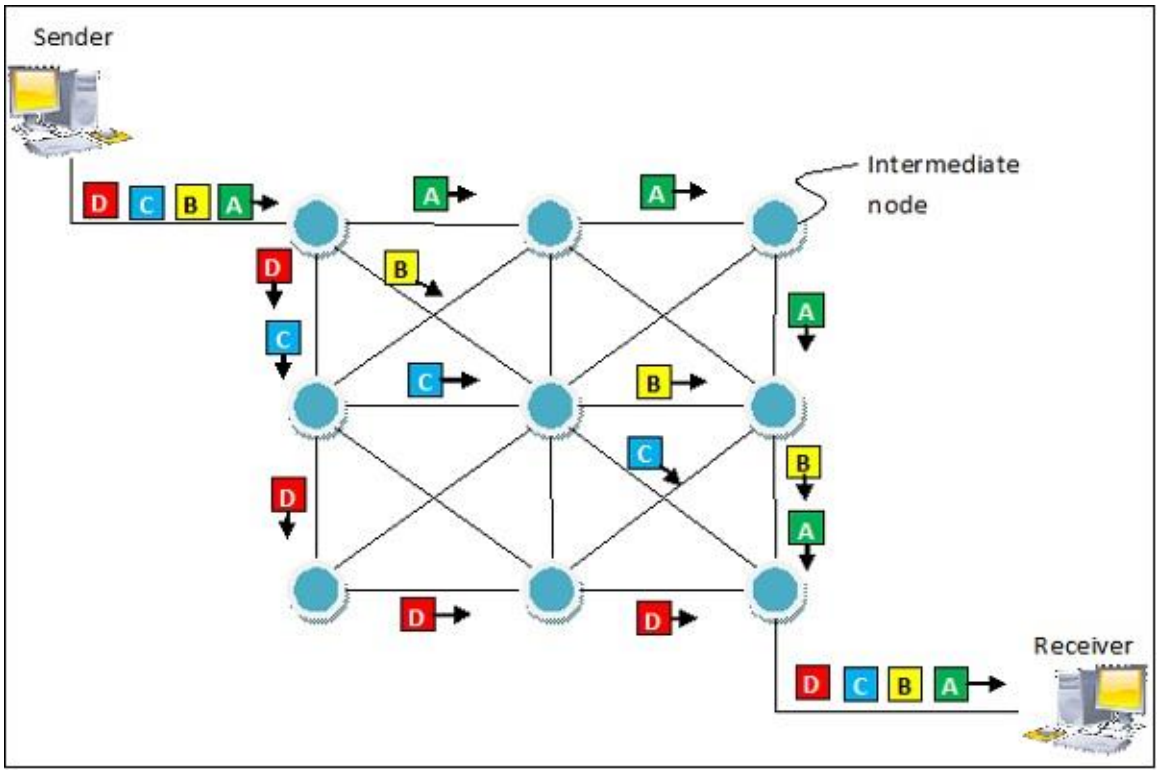
Packet switching is a connectionless network switching technique. Here, the message is divided and grouped into a number of units called packets that are individually routed from the source to the destination. There is no need to establish a dedicated circuit for communication.

Process

Each packet in a packet switching technique has two parts: a header and a payload. The header contains the addressing information of the packet and is used by the intermediate routers to direct it towards its destination. The payload carries the actual data.

A packet is transmitted as soon as it is available in a node, based upon its header information. The packets of a message are not routed via the same path. So, the packets in the message arrives in the destination out of order. It is the responsibility of the destination to reorder the packets in order to retrieve the original message.

The process is diagrammatically represented in the following figure. Here the message comprises of four packets, A, B, C and D, which may follow different routes from the sender to the receiver.



Advantages and Disadvantages of Packet Switching

Advantages

- Delay in delivery of packets is less, since packets are sent as soon as they are available.
- Switching devices don't require massive storage, since they don't have to store the entire messages before forwarding them to the next node.
- Data delivery can continue even if some parts of the network faces link failure. Packets can be routed via other paths.
- It allows simultaneous usage of the same channel by multiple users.
- It ensures better bandwidth usage as a number of packets from multiple sources can be transferred via the same link.

Disadvantages

- They are unsuitable for applications that cannot afford delays in communication like high

quality voice calls.

- Packet switching high installation costs.
- They require complex protocols for delivery.
- Network problems may introduce errors in packets, delay in delivery of packets or loss of packets. If not properly handled, this may lead to loss of critical information.

Functions of Presentation Layer

1. **Translation:** Before being transmitted, information in the form of characters and numbers should be changed to bit streams. The presentation layer is responsible for interoperability between encoding methods as different computers use different encoding methods. It translates data between the formats the network requires and the format the computer.
2. **Encryption:** It carries out encryption at the transmitter and decryption at the receiver.
3. **Compression:** It carries out data compression to reduce the bandwidth of the data to be transmitted. The primary role of Data compression is to reduce the number of bits to be 0transmitted. It is important in transmitting multimedia such as audio, video, text etc.

Secure Sockets Layer (SSL) protocol

The Secure Sockets Layer (SSL) protocol was developed by Netscape Communications Corporation.

SSL ensures the data that is transferred between a client and a server remains private. This protocol enables the client to authenticate the identity of the server.

When your server has a digital certificate, SSL-enabled browsers can communicate securely with your server, using SSL. With SSL, you can easily establish a security-enabled Web site on the Internet, or on your private intranet. A browser that does not support HTTP over SSL cannot request URLs using HTTPS. The non-SSL browsers do not allow submission of forms that require secure communications.

SSL uses a *security handshake* to initiate a secure connection between the client and the server. During the handshake, the client and server agree on the security keys to use for the session and the algorithms to use for encryption. The client authenticates the server; optionally, the server can request the client certificate. After the handshake, SSL encrypts and decrypts all the information in both the HTTPS request and the server response, including:

- The URL requested by the client
- The contents of any submitted form
- Access authorization information, like user names and passwords
- All data sent between the client and the server

HTTP

- HTTP stands for **Hyper Text Transfer Protocol**.
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.
- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.
- HTTP is used to carry the data in the form of MIME-like format.
- HTTP is similar to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in the way the messages are sent from the client to the

server and from server to the client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

File Transfer Protocol (FTP) is an application layer protocol that is used to transfer the files between the local devices (PC, smartphone, etc.) to a server. It transfers both text and binary files over the Internet.

- FTP opens two connections between the computers − one for the *commands* and *replies* (control connection) and a second one for *data transfers* (data connection).
- FTP is built on a client-server model architecture using the control connection and data connection between the client and server.

Telnet/FTP

Telnet and FTP are two very commonly used application-layer protocols on the Internet. They have been around for over 20 years now.

Telnet is an application-layer protocol and allows a user to connect to an account on another remote machine. A client program on one machine can connect with a server program running on another machine using this protocol. Users utilizing Telnet interact with the remote machine in the same way as they would with a local machine. Telnet was one of the earliest protocols and in the early days was used primarily to allow users in one location to access accounts or machines in another location.

The Telnet client has two primary functions:

- Interacting with the user terminal on the local host
- Communicating with the remote telnet server

4.2.3. Concepts of Application Layer protocols and terminologies:

SMTP

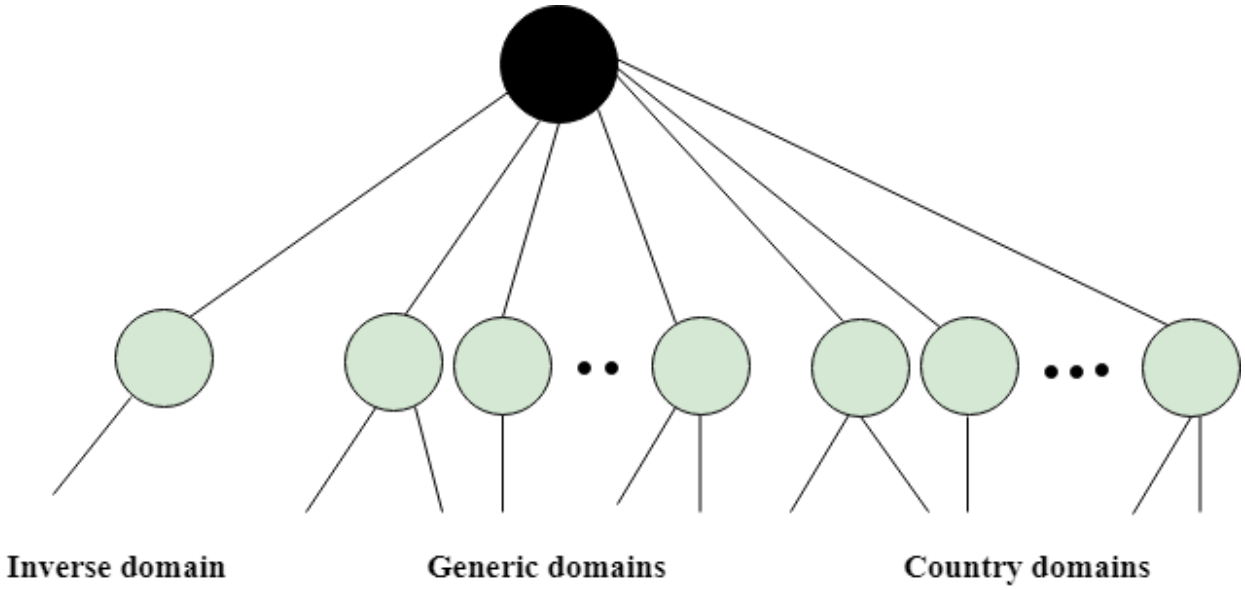
- SMTP stands for Simple Mail Transfer Protocol.
- SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called **Simple Mail Transfer Protocol**.
- It is a program used for sending messages to other computer users based on e-mail addresses.
- It provides a mail exchange between users on the same or different computers, and it also supports:
    - It can send a single message to one or more recipients.
    - Sending message can include text, voice, video or graphics.
    - It can also send the messages on networks outside the internet.
- The main purpose of SMTP is used to set up communication rules between servers. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform. They also have a way of handling the errors such as incorrect email address. For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.

DNS

An application layer protocol defines how the application processes running on different systems, pass the messages to each other.

- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
- For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address.

DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.

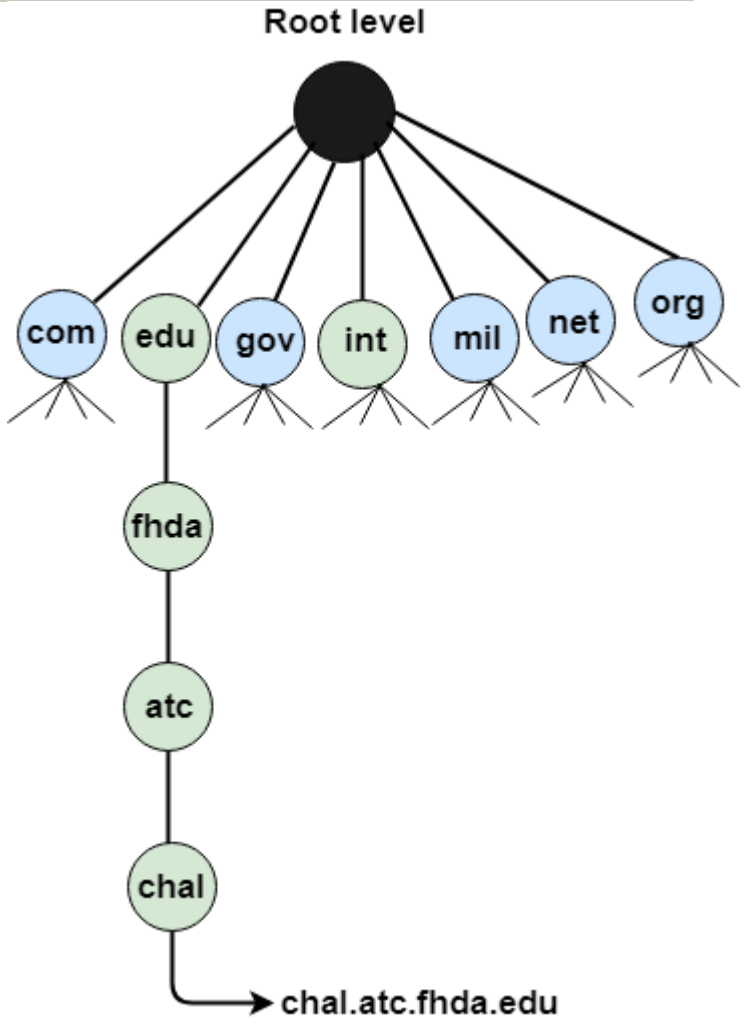


Generic Domains

- It defines the registered hosts according to their generic behavior.
- Each node in a tree defines the domain name, which is an index to the DNS database.
- It uses three-character labels, and these labels describe the organization type.

Label	Description
aero	Airlines and aerospace companies
biz	Businesses or firms
com	Commercial Organizations
coop	Cooperative business Organizations
edu	Educational institutions
gov	Government institutions

info	Information service providers
int	International Organizations
mil	Military groups
museum	Museum & other nonprofit organizations
name	Personal names
net	Network Support centers
org	Nonprofit Organizations
pro	Professional individual Organizations



Country Domain

The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three character organizational abbreviations.

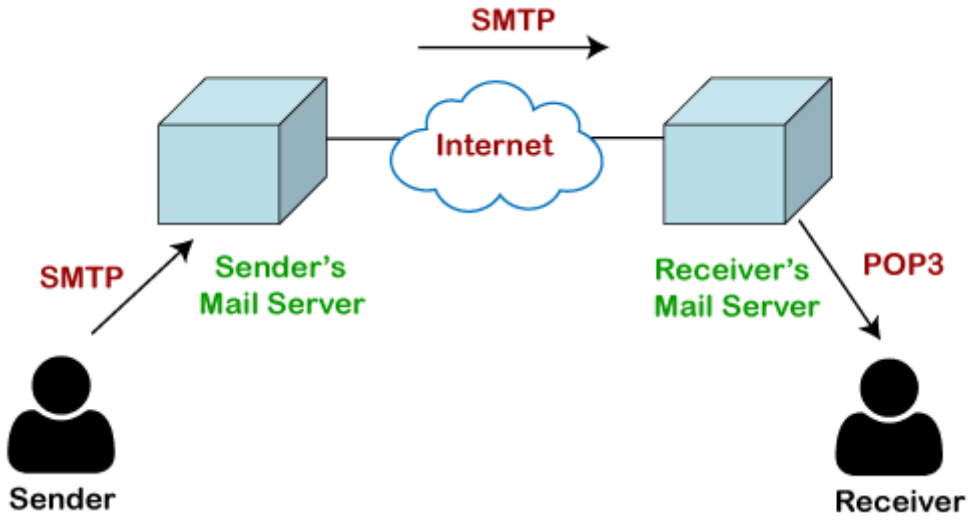
Inverse Domain

The inverse domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients. To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.

POP Protocol

The POP protocol stands for Post Office Protocol. As we know that SMTP is used as a message transfer agent. When the message is sent, then SMPT is used to deliver the message from the client to the server and then to the recipient server. But the message is sent from the recipient server to the actual server with the help of the Message Access Agent. The Message Access Agent contains two types of protocols, i.e., POP3 and IMAP.

How is mail transmitted?



Suppose sender wants to send the mail to receiver. First mail is transmitted to the sender's mail server. Then, the mail is transmitted from the sender's mail server to the receiver's mail server over the internet. On receiving the mail at the receiver's mail server, the mail is then sent to the user. The whole process is done with the help of Email protocols. The transmission of mail from the sender to the sender's mail server and then to the receiver's mail server is done with the help of the SMTP

protocol. At the receiver's mail server, the POP or IMAP protocol takes the data and transmits to the actual user.

Since SMTP is a push protocol so it pushes the message from the client to the server. As we can observe in the above figure that SMTP pushes the message from the client to the recipient's mail server. The third stage of email communication requires a pull protocol, and POP is a pull protocol. When the mail is transmitted from the recipient mail server to the client which means that the client is pulling the mail from the server.

What is: IP Address

IP (Internet Protocol) addresses are used to identify hardware devices on a network. The addresses allow these devices to connect to one another and transfer data on a local network or over the internet.

Each address is a string of numbers separated by periods. There are four numbers in total and each number can range between 0 and 255. An example of an IP address would be: 506.457.14.512

We need billions of IP addresses to identify every computer, router and website on the internet. One day we'll run out of unique addresses and a new IPv6 protocol has been designed to meet this need.

How Do I Find Out my IP Address?

If your computer is connected to both your local network and the internet, then it will have two IP addresses. You'll have a private IP address locally, and a public IP address on the internet.

A **private IP address** is used to connect your computer or device to your home or business network. This address is normally assigned by your network router.

Private IP addresses are in the range 40.xxx.xxx.xxx or 192.168.xxx.xxx. An example of a private IP address is 192.168.1.1.

There are a few ways to discover your private IP address. For example, on Windows you can type *ipconfig* on the command prompt. Similarly, Mac users can type the command *ifconfig* in the Terminal app.

Your **public IP address** is used to connect your home or business network to the internet. This address is assigned by your internet service provider (ISP).

To find your public IP address, simply go to WhatIsMyIP.com in your web browser. This site will display your public IP address and other information.

If you have a WordPress website, it will also have a public IP address. You can learn its address by visiting your hosting provider or checking the email they sent you when you signed up.

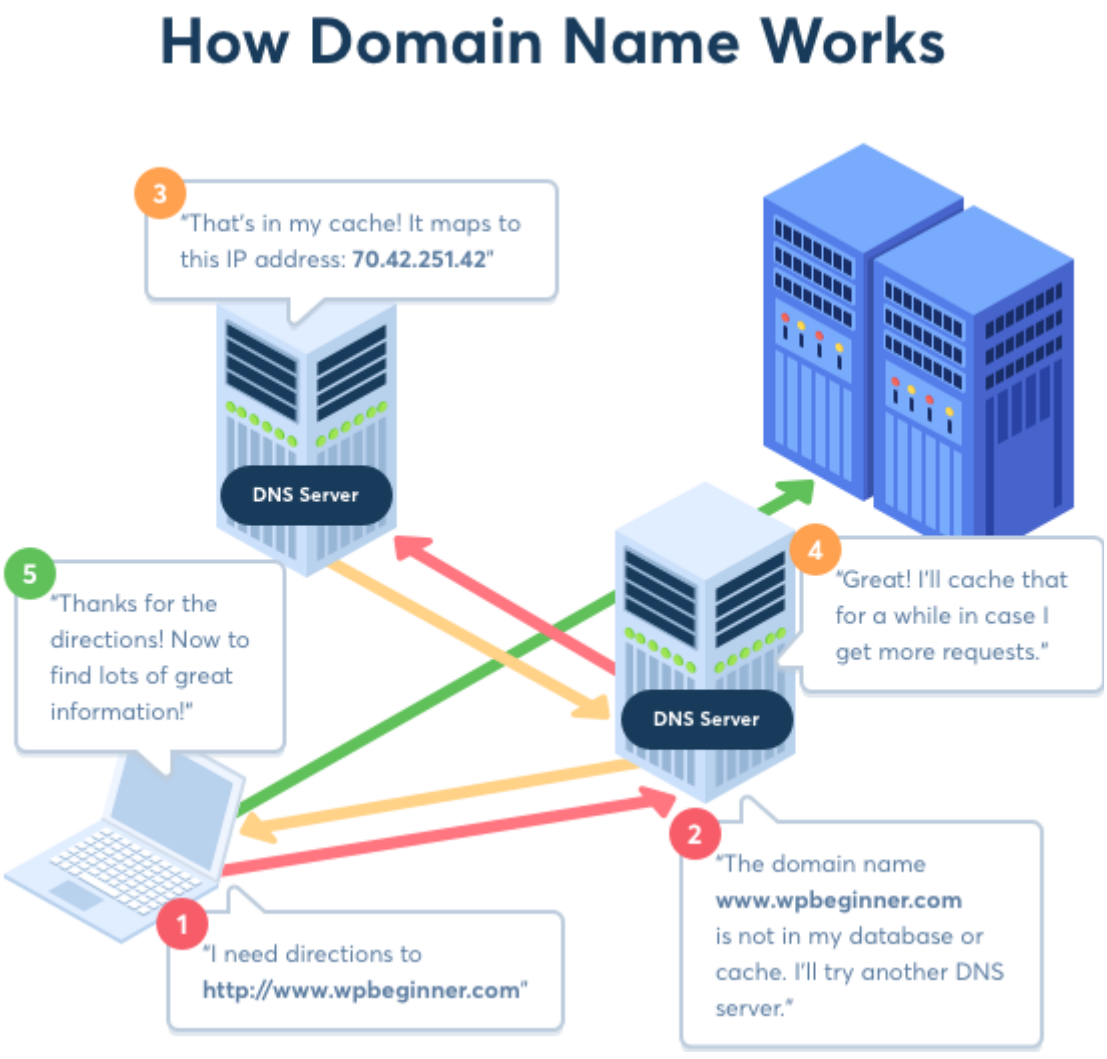
Alternatively, you can use WhatIsMyIP's DNS Lookup tool. Once you type in your website's URL the website will display its IP address.

IP Addresses and Domain Names

Humans are more comfortable with names than numbers. It's easier to remember a domain name like wpbeginner.com than a long list of numbers like 192.124.249.166.

The internet's Domain Name System (DNS) is like a phone book. When you type a domain name like wpbeginner.com, it automatically looks up the number, the IP address, and connects you to the website.

What's interesting is that your WordPress site doesn't know its IP address, just the URL. That makes it easier to switch to a new hosting provider, where your website's URL is likely to change.



Dynamic and Static IP Addresses

Most internet users have a **dynamic IP address** that automatically changes from time to time. This is better for internet service providers that need to deal with customers joining and leaving the service, and changing address.

Most websites have a **static IP address** that doesn't change. This is important because the DNS system uses your website's IP address when someone navigates to your site or sends you an email.

If you plan on hosting your own website, then you will need to purchase a static IP address from your internet service provider, which will cost you extra.

The IPv4 and IPv6 Protocols

The original Internet Protocol is IPv4. As we've seen, it defines an IP address as a 32-bit number like 506.457.14.512. That only allows for around 4 billion IP addresses, and that's not enough for ongoing use.

IPv6 is a new protocol that was introduced in 1998. Deployment commenced in the mid-2000s and is ongoing. When you visit WhatIsMyIP.com you can discover whether you've been assigned an IPv6 IP Address.

The new protocol uses 128-bit IP addresses that look like 4ggr:1925:5656:7:600:t4tt:tc54:98vt.

This means that IPv6 is able to provide about 340 trillion trillion trillion IP addresses. That's more than enough to meet the growing need for IP addresses for websites, computers, smartphones, smartwatches, and smart refrigerators for years to come.

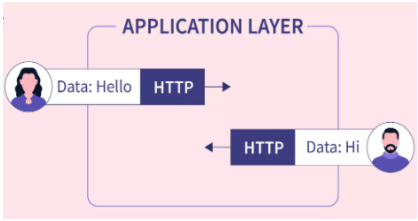
We hope this article helped you learn more about IP addresses. You may also want to see our Additional Reading list below for related articles on useful WordPress tips, tricks, and ideas.

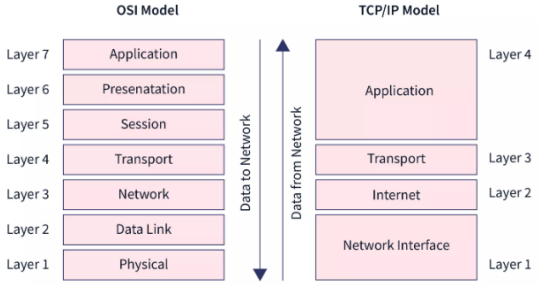
4.4 Differences between HTTP and HTTPS

- HTTP stands for HyperText Transfer Protocol and HTTPS stands for HyperText Transfer Protocol Secure.
- In HTTP, URL begins with “http://” whereas URL starts with “https://”
- HTTP uses port number 80 for communication and HTTPS uses 443
- HTTP is considered to be insecure and HTTPS is secure
- HTTP Works at Application Layer and HTTPS works at Transport Layer
- In HTTP, Encryption is absent and Encryption is present in HTTPS as discussed above
- HTTP does not require any certificates and HTTPS needs SSL Certificates
- HTTP speed is faster than HTTPS and HTTPS speed is slower than HTTP
- HTTP does not improve search ranking while HTTPS improves search ranking.
- HTTP does not use data hashtags to secure data, while HTTPS will have the data before sending it and return it to its original state on the receiver side.

What is the Application Layer?

The application layer is the topmost layer of the OSI model and the TCP/IP model. In TCP/IP model, the application layer is formed by combining the top three layers, i.e., the application layer, the presentation layer, and the session layer. It is the layer closest to the end-user, implying that the application layer and the end-user can interact directly with the software application.





It does not provide service to other layers because it is the topmost layer. The Application layer uses Transport and any levels below it to communicate with or transfer data to a remote host.

Consumers frequently require protocols from the Application Layer. One of the most often used application protocols is HTTP (HyperText Transfer Protocol), the foundation for the World Wide Web. Domain Name System (DNS), Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), and TELNET are some of the protocols used in the application layer.

What Are the Services Provided by the Application Layer?

The application layer provides the following services.

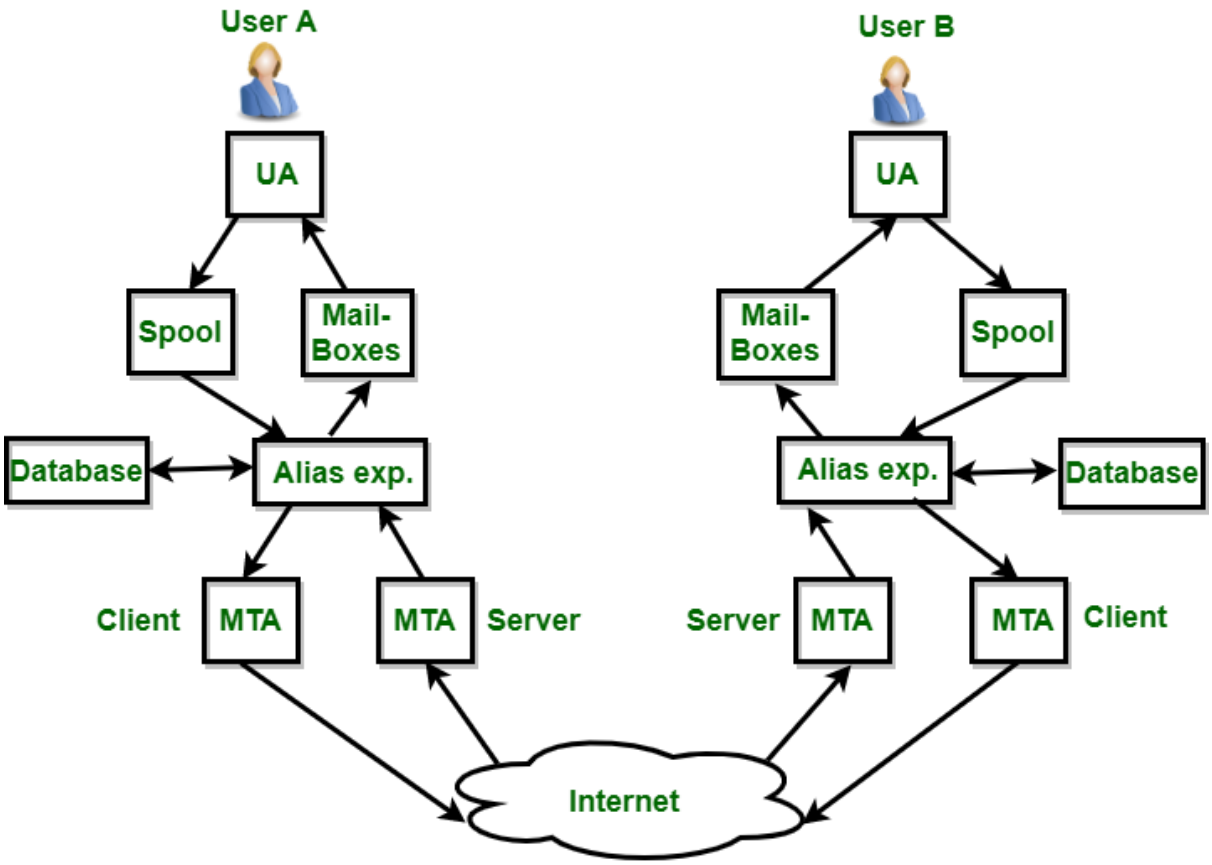
1. The application layer guarantees that the receiver is recognized, accessible, and ready to receive data from the sender.
2. It enables authentication between devices for an extra layer of network security.
3. It determines the protocol and data syntax rules at the application level.
4. The protocols of the application layer also define the basic syntax of the message being forwarded or retrieved.
5. It also checks whether the sender's computer has the necessary communication interfaces, such as an Ethernet or Wi-Fi interface.
6. Finally, the data on the receiving end is presented to the user application.

Electronic Mail (e-mail) is one of most widely used services of Internet. This service allows an Internet user to send a **message in formatted manner (mail)** to the other Internet user in any part of world. Message in mail not only contain text, but it also contains images, audio and videos data. The person who is sending mail is called **sender** and person who receives mail is called **recipient**. It is just like postal mail service.

Components of E-Mail System :
The basic components of an email system are : User Agent (UA), Message Transfer Agent (MTA), Mail Box, and Spool file. These are explained as following below.

1. **User Agent (UA) :**
   The UA is normally a program which is used to send and receive mail. Sometimes, it is called as mail reader. It accepts variety of commands for composing, receiving and replying to messages as well as for manipulation of the mailboxes.

2. **Message Transfer Agent (MTA) :**
   MTA is actually responsible for transfer of mail from one system to another. To send a mail, a system must have client MTA and system MTA. It transfer mail to mailboxes of recipients if they are connected in the same machine. It delivers mail to peer MTA if destination mailbox is in another machine. The delivery from one MTA to another MTA is done by Simple Mail Transfer Protocol.



3. **Mailbox :**
   It is a file on local hard drive to collect mails. Delivered mails are present in this file. The user

can read it delete it according to his/her requirement. To use e-mail system each user must have a mailbox . Access to mailbox is only to owner of mailbox.

4. **Spool file :**
   This file contains mails that are to be sent. User agent appends outgoing mails in this file using SMTP. MTA extracts pending mail from spool file for their delivery. E-mail allows one name, an **alias**, to represent several different e-mail addresses. It is known as **mailing list**, Whenever user have to sent a message, system checks recipients's name against alias database. If mailing list is present for defined alias, separate messages, one for each entry in the list, must be prepared and handed to MTA. If for defined alias, there is no such mailing list is present, name itself becomes naming address and a single message is delivered to mail transfer entity.

Services provided by E-mail system :

- **Composition –**
  The composition refer to process that creates messages and answers. For composition any kind of text editor can be used.
- **Transfer –**
  Transfer means sending procedure of mail i.e. from the sender to recipient.
- **Reporting –**
  Reporting refers to confirmation for delivery of mail. It help user to check whether their mail is delivered, lost or rejected.
- **Displaying –**
  It refers to present mail in form that is understand by the user.
- **Disposition –**
  This step concern with recipient that what will recipient do after receiving mail i.e save mail, delete before reading or delete after reading.

Concepts of email and working of email account and services in application layer services

Email operates within the application layer of the OSI model, using protocols like SMTP, POP3, and IMAP to send and receive messages. It involves a client-server interaction where an email client (like Gmail, Outlook) communicates with mail servers to send, receive, and manage emails.

Here's a breakdown:

1. Client-Server Interaction:

- **Email Clients:**
  These are the user interfaces (like webmail or desktop applications) that allow users to compose, send, receive, and manage emails.
- **Mail Servers:**
  These are servers that handle the storage and routing of emails. They act as intermediaries between email clients.

2. Protocols:

- **SMTP (Simple Mail Transfer Protocol):**
  Used for sending emails from a client to a mail server and between mail servers. It's an application layer protocol that relies on TCP for reliable transmission.
- **POP3 (Post Office Protocol version 3):**
  Used for retrieving emails from a mail server to an email client. It downloads emails to the client and typically deletes them from the server.
- **IMAP (Internet Message Access Protocol):**
  Also used for retrieving emails, but it keeps emails on the server and allows users to manage them through different devices.

3. Email Account Concepts:

- **Email Address:** This is the unique identifier for an email account, like user@example.com.
- **Mailboxes:** Each email account has a mailbox on the mail server where incoming emails are stored.
- **User Interface:** The email client provides the user interface for interacting with emails, including composing, sending, receiving, and managing emails.

4. Email Services in the Application Layer:

- **Email Composition:** Creating and editing email messages.
- **Email Transfer:** Sending messages from the sender's email client to the recipient's email client via the mail servers.
- **Email Reporting:** Providing feedback on the delivery status of emails.
- **Email Displaying:** Presenting emails in a user-friendly format.
- **Email Disposition:** Managing emails after they have been read, such as saving or deleting them.

URL and URL types (Absolute, Relative)

URL stands for Uniform Resource Locator. Any internet location available on the server is called a web URL, web address, or website. Each website or webpage has a unique address called URL. e.g., the website of **geeksforgeeks** website has an address or URL called https://www.geeksforgeeks.org/

Types of URL: URL gives the address of files created for webpages or other documents like an image, pdf or a doc file, etc.

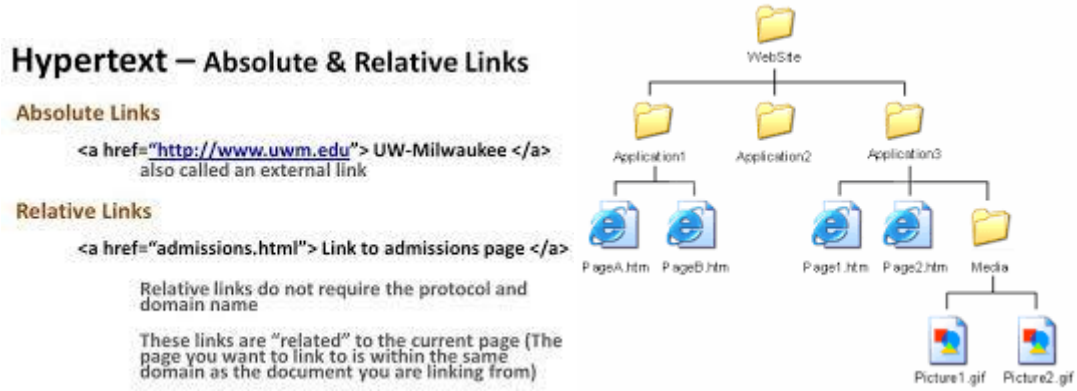
Type:

- It specifies the type of the server in which the file is located.
- **address:** It specifies the address or location of the internet server.
- **path:** It specifies the location of the file on the internet server.
- There are two types of URLs:

Table of Content

Absolute URL

This type of URL contains both the domain name and directory/page path. An absolute URL gives complete location information. It begins with a protocol like "http://" and continues, including every detail. An absolute URL typically comes with the following syntax.



Syntax:

```
protocol://domain/path
```

For web browsing, absolute URLs are types in the address bar of a web browser. For example, if it is related to our project page link on **geeksforgeeks** website, the URL should be mentioned as https://www.geeksforgeeks.org/gate/computer-science-projects/ this gives the complete information about the file location path.

Note: The protocol may be of the following types.

```
http://, https://, ftp://, gopher://, etc.
```

Relative URL

This type of URL contains the path excluding the domain name. Relative means "in relation to", and a relative URL tells a URL location on terms of the current location. Relative path is used for reference to a given link of a file that exist within the same domain.

Let us assume a web developer setting up a webpage and want to link an image called "geeksforgeeks.jpg".

```
<img src="geeksforgeeks.jpg">
```

It would internally be interpreted like the following.

```
<img src="./geeksforgeeks.jpg">
```

The dot(.) before the "/" in the *src* attribute is a "special character". It means the location should be started from the current directory to find the file location.

Electronic Mail

In this tutorial, we will be covering one of the most popular Internet services that is Electronic Mail(E-mail) in detail.

Electronic mail is often referred to as E-mail and it is a method used for **exchanging digital messages**.

- Electronic mail is mainly designed for **human use**.
- It allows a message to includes **text, image, audio** as well as **video**.
- This service allows one message to be **sent to one or more than one recipient**.
- The E-mail systems are mainly based on the **store-and-forward model** where the E-mail server system accepts, forwards, deliver and store the messages on behalf of users who only need to connect to the infrastructure of the Email.

- The Person who **sends the email** is referred to as **the Sender** while the person who receives an email is referred to as **the Recipient**.

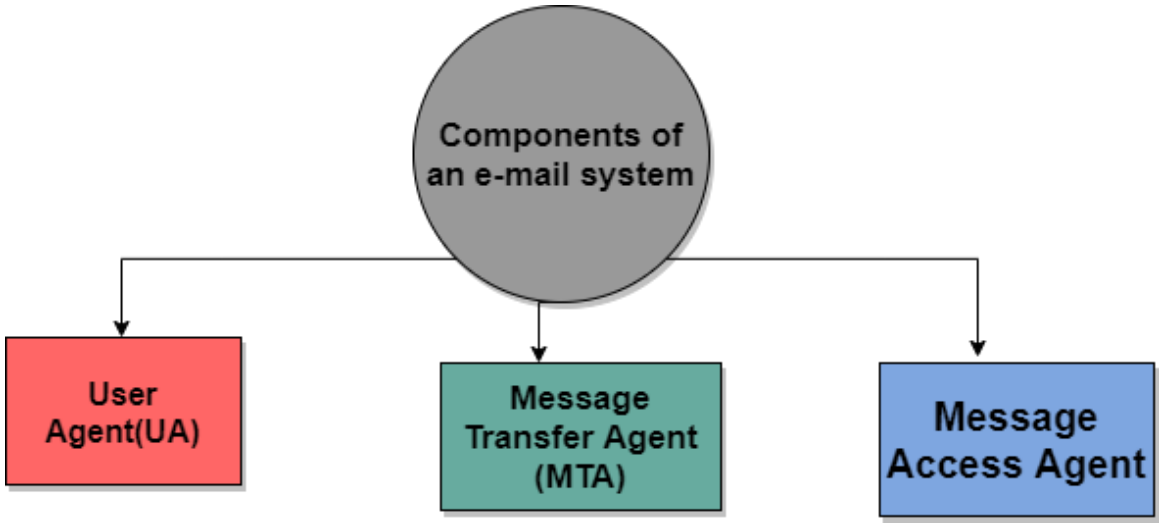
Need of an Email

By making use of Email, we can send any message at any time to anyone.

- We can send the same message to several peoples at the same time.
- It is a very fast and efficient way of transferring information.
- The email system is very fast as compared to the Postal system.
- Information can be easily forwarded to coworkers without retyping it.

Components of E-mail System

The basic Components of an Email system are as follows:



1.User Agent(UA)

It is a program that is mainly used to send and receive an email. It is also known as an email reader. User-Agent is used to compose, send and receive emails.

- It is the first component of an Email.
- User-agent also handles the mailboxes.
- The User-agent mainly provides the services to the user in order to make the sending and receiving process of message easier.

Given below are some services provided by the User-Agent:

1.Reading the Message
2.Replying the Message
3.Composing the Message
4.Forwarding the Message.
5.Handling the Message.

2.Message Transfer Agent

The actual process of transferring the email is done through the Message Transfer Agent(MTA).

- In order to send an Email, a system must have an MTA client.
- In order to receive an email, a system must have an MTA server.
- The protocol that is mainly used to define the MTA client and MTA server on the internet is called SMTP(Simple Mail Transfer Protocol).
- The SMTP mainly defines how the commands and responses must be sent back and forth

3.Message Access Agent

In the first and second stages of email delivery, we make use of SMTP.

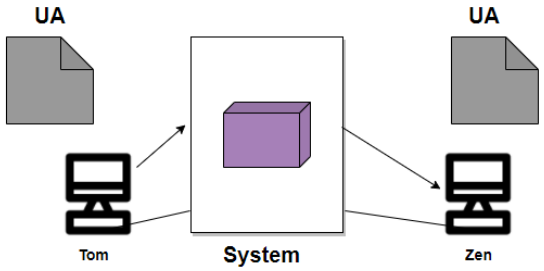
- SMTP is basically a Push protocol.
- The third stage of the email delivery mainly needs the pull protocol, and at this stage, the message access agent is used.
- The two protocols used to access messages are POP and IMAP4.

Architecture of Email

Now its time to take a look at the architecture of e-mail with the help of four scenarios:

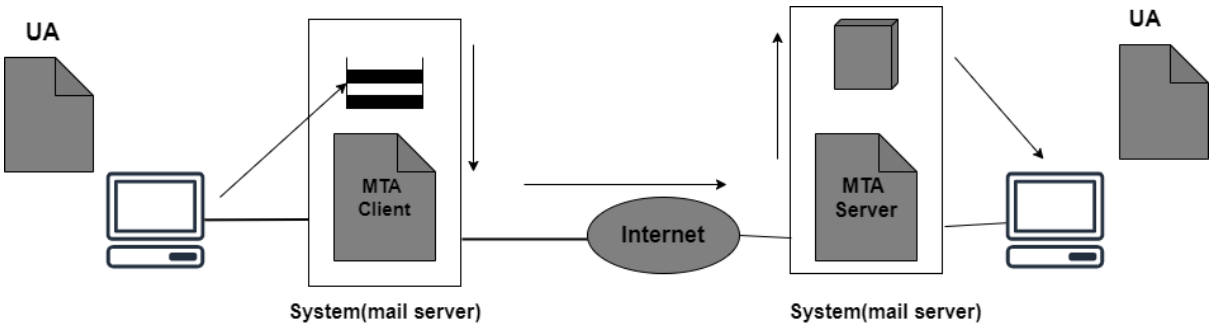
First Scenario

When the sender and the receiver of an E-mail are on the same system, then there is the need for only two user agents.



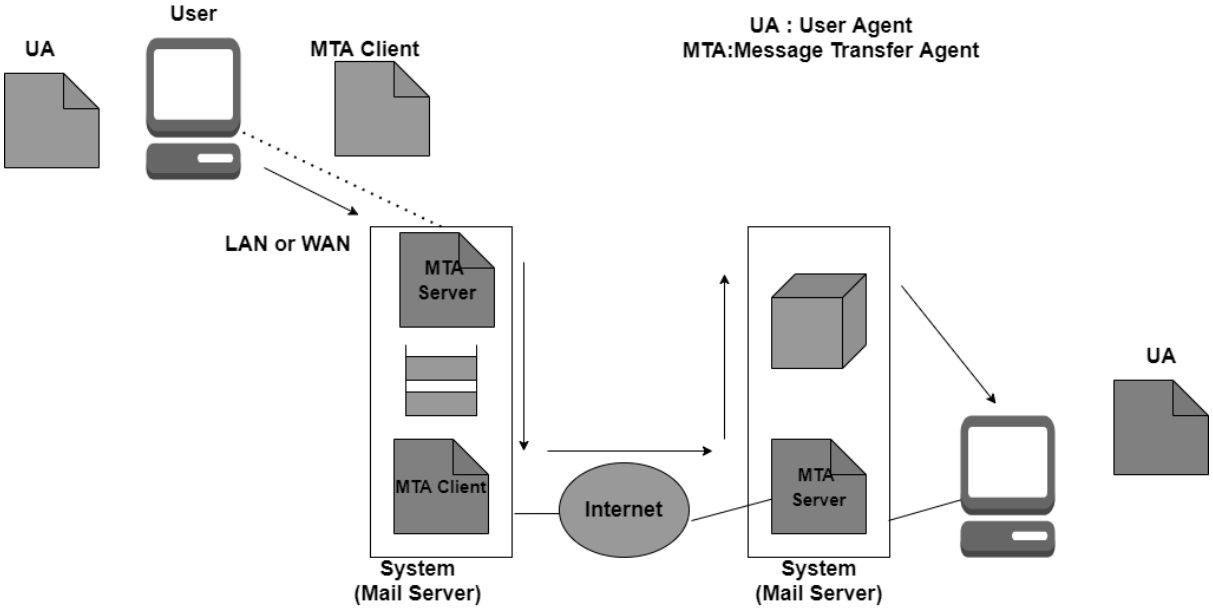
Second Scenario

In this scenario, the sender and receiver of an e-mail are basically users on the two different systems. Also, the message needs to send over the Internet. In this case, we need to make use of User Agents and Message transfer agents(MTA).



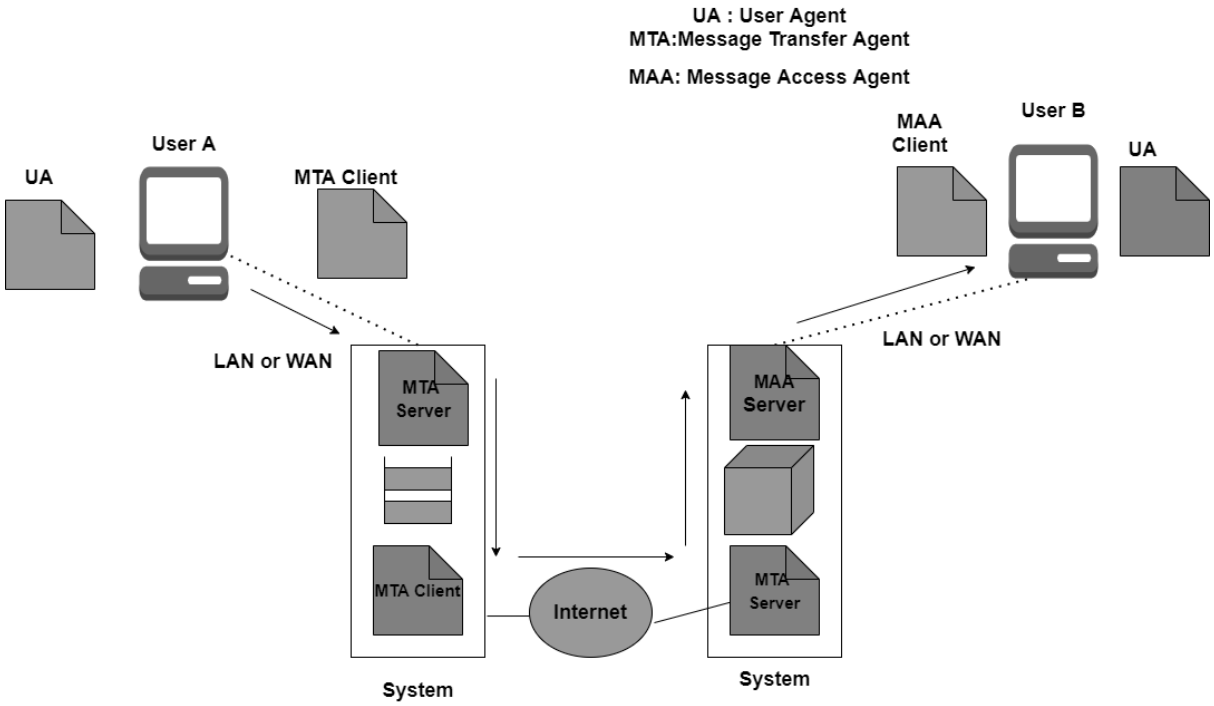
Third Scenario

In this scenario, the sender is connected to the system via a point-to-point WAN it can be either a dial-up modem or a cable modem. While the receiver is directly connected to the system like it was connected in the second scenario.
Also in this case sender needs a User agent(UA) in order to prepare the message. After preparing the message the sender sends the message via a pair of MTA through LAN or WAN.



Fourth Scenario

In this scenario, the receiver is also connected to his mail server with the help of WAN or LAN.
When the message arrives the receiver needs to retrieve the message; thus there is a need for another set of client/server agents. The recipient makes use of MAA(Message access agent) client in order to retrieve the message.
In this, the client sends the request to the Mail Access agent(MAA) server and then makes a request for the transfer of messages.
This scenario is most commonly used today.



Structure of Email

The message mainly consists of two parts:

1.Header

2.Body

Header

The header part of the email generally contains the sender's address as well as the receiver's address and the subject of the message.

Body

The Body of the message contains the actual information that is meant for the receiver.

Email Address

In order to deliver the email, the mail handling system must make use of an addressing system with unique addresses.

The address consists of two parts:

- Local part
- Domain Name

Local Part

It is used to define the name of the special file, which is commonly called a user mailbox; it is the place where all the mails received for the user is stored for retrieval by the Message Access Agent.

Domain Name

It is the second part of the address is Domain Name.

4.3.3 Concepts of search engine and purpose.

A search engine is a software system that helps users find information on the internet by searching and retrieving relevant data based on user queries. It works by crawling the web, indexing content, and then using algorithms to match search terms with indexed information, providing a list of results. Search engines are used for a wide range of purposes, including research, shopping, staying informed, and finding specific information quickly.

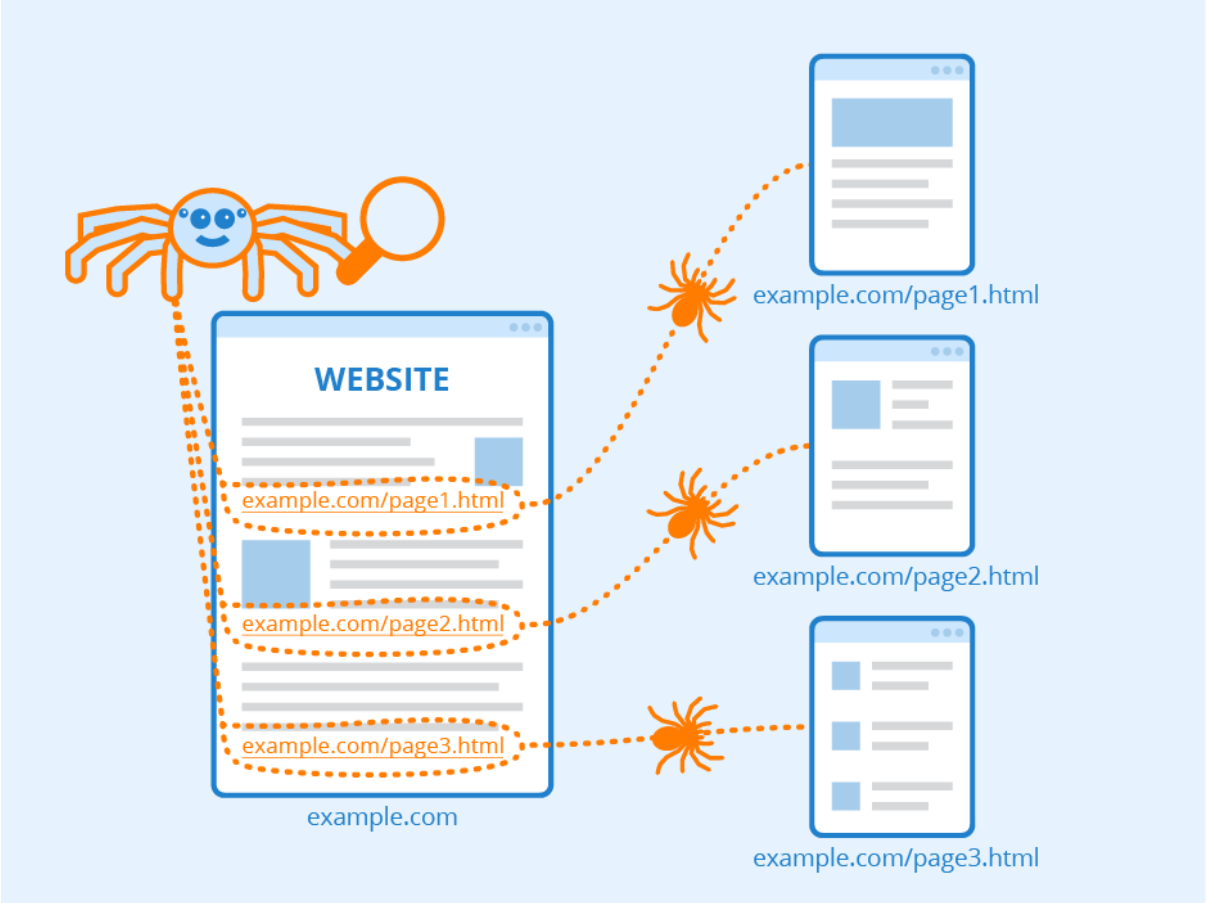
Here's a more detailed look at the concept and uses:

Concept:

- **Crawling:**

  Search engines use automated programs (like bots or spiders) to explore the internet, following links and gathering information from web pages.

  [illegible] .



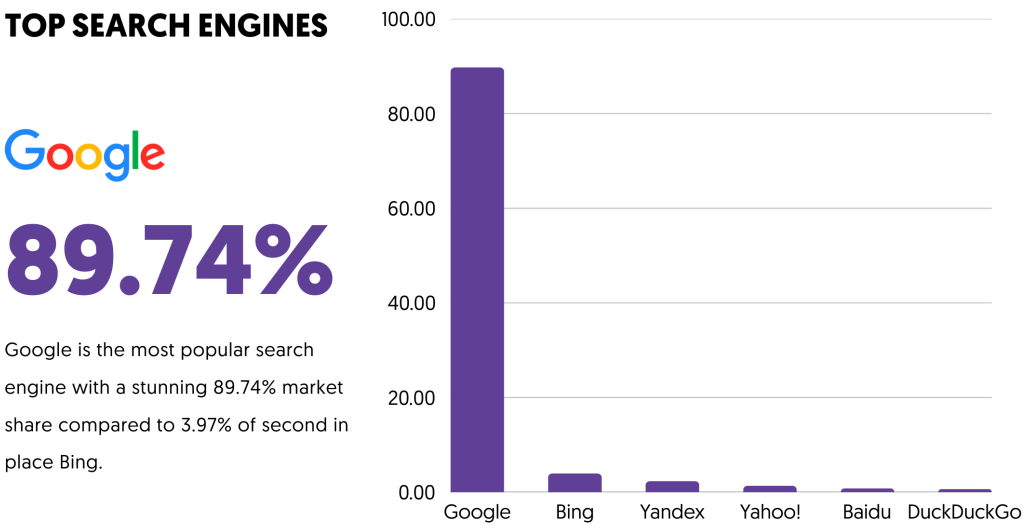
- **Indexing:**

  The collected data is organized and stored in a searchable index, similar to a library catalog.

- **Query Processing:**

  When a user enters a search query, the search engine matches the terms against its index using algorithms.

- **Result Ranking:**
  The search engine then ranks the results based on relevance, quality, and other factors, presenting the most relevant results to the user.
  Uses:



- **Research:**

  Search engines are essential tools for academic research, finding information on various topics, and accessing scholarly articles.

- **Shopping:**

  Users can search for products, compare prices, and find deals on online stores.

- **News and Information:**

  Search engines provide access to current events, news articles, and information on a wide range of topics.

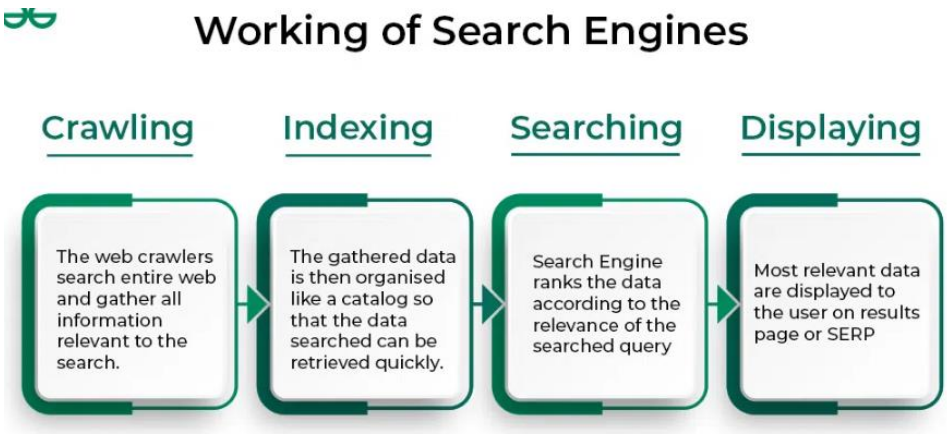
- **Finding Specific Information:**

  Users can quickly locate specific websites, videos, images, or other online content using search engines.

- **Keeping Up with Interests:**

  Search engines help users stay updated on their hobbies, favorite topics, and social media trends.

- **Business and Marketing:**
  Businesses use search engines to understand their target audience, analyze market trends, and optimize their online presence through search engine optimization (SEO).



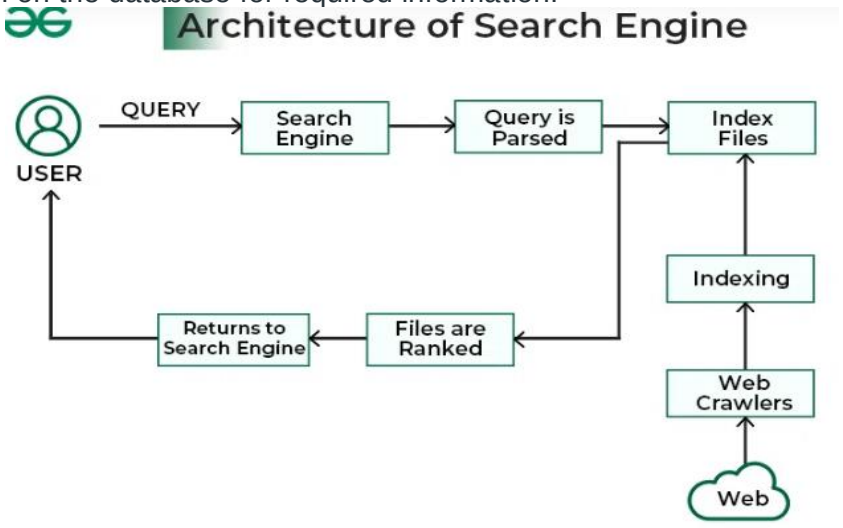
Architecture Of Search Engine

If we talk about the architecture or the framework of a search engine, it can be described in three main components –

• **Web crawlers** – As the name suggests these acts as spiders which crawl all over the web to collect required information. These are special bots that search throughout the internet and accumulates data using various links.

• **Database** – It is a collection of data which is gathered by the web crawlers after searching throughout the world wide web.

• **Search Interface** – It provides a medium or interface for users so that they can access and search on the database for required information.



APPLICATION LAYER

The application layer in the OSI model is the closest layer to the end user which means that the application layer and end user can interact directly with the software application. The application layer programs are based on client and servers.

The Application layer includes the following functions:

- **Identifying communication partners:** The application layer identifies the availability of communication partners for an application with data to transmit.
- **Determining resource availability:** The application layer determines whether sufficient network resources are available for the requested communication.
- **Synchronizing communication:** All the communications occur between the applications requires cooperation which is managed by an application layer.

Services of Application Layers

- **Network Virtual terminal:** An application layer allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal, which in turn, talks to the host. The remote host thinks that it is communicating with one of its own terminals, so it allows the user to log on.
- **File Transfer, Access, and Management (FTAM):** An application allows a user to access files in a remote computer, to retrieve files from a computer and to manage files in a remote computer. FTAM defines a hierarchical virtual file in terms of file structure, file attributes and the kind of operations performed on the files and their attributes.
- **Addressing:** To obtain communication between client and server, there is a need for addressing. When a client made a request to the server, the request contains the server address and its own address. The server response to the client request, the request contains the destination address, i.e., client address. To achieve this kind of addressing, DNS is used.
- **Mail Services:** An application layer provides Email forwarding and storage.
- **Directory Services:** An application contains a distributed database that provides access for global information about various objects and services.
- **Authentication:** It authenticates the sender or receiver's message or both.

Network Application Architecture

Application architecture is different from the network architecture. The network architecture is fixed and provides a set of services to applications. The application

architecture, on the other hand, is designed by the application developer and defines how the application should be structured over the various end systems.

Application architecture is of two types:

- **Client-server architecture:** An application program running on the local machine sends a request to another application program is known as a client, and a program that serves a request is known as a server. For example, when a web server receives a request from the client host, it responds to the request to the client host.

  Characteristics of Client-server architecture:

- In Client-server architecture, clients do not directly communicate with each other. For example, in a web application, two browsers do not directly communicate with each other.
- A server is fixed, well-known address known as IP address because the server is always on while the client can always contact the server by sending a packet to the sender's IP address.

  Disadvantage Of Client-server architecture:

  It is a single-server based architecture which is incapable of holding all the requests from the clients. For example, a social networking site can become overwhelmed when there is only one server exists.

- **P2P (peer-to-peer) architecture:** It has no dedicated server in a data center. The peers are the computers which are not owned by the service provider. Most of the peers reside in the homes, offices, schools, and universities. The peers communicate with each other without passing the information through a dedicated server, this architecture is known as peer-to-peer architecture. The applications based on P2P architecture includes file sharing and internet telephony.

  Features of P2P architecture

- **Self scalability:** In a file sharing system, although each peer generates a workload by requesting the files, each peer also adds a service capacity by distributing the files to the peer.
- **Cost-effective:** It is cost-effective as it does not require significant server infrastructure and server bandwidth.

  Client and Server processes

- A network application consists of a pair of processes that send the messages to each other over a network.

- In P2P file-sharing system, a file is transferred from a process in one peer to a process in another peer. We label one of the two processes as the client and another process as the server.
- With P2P file sharing, the peer which is downloading the file is known as a client, and the peer which is uploading the file is known as a server. However, we have observed in some applications such as P2P file sharing; a process can be both as a client and server. Therefore, we can say that a process can both download and upload the files.

File Transfer, Access and Management

FTAM is an OSI standard that provides file transfer services between client (initiator) and server (responder) systems in an open environment. It also provides access to files and management of files on diverse systems. In these respects, it strives to be a universal file system. FTAM has worked well as a way to bring mainframe information systems into distributed environments, but FTAM has not caught on otherwise.

FTAM is designed to help users access files on diverse systems that use compatible FTAM implementations. It is similar to FTP (File Transfer Protocol) and NFS (Network File System), both of which operate in the TCP/IP environment. Users can manipulate files down to the record level, which is how FTAM stores files. In this respect, FTAM has some relational database features. For example, users can lock files or lock individual records.

FTAM is a system in which connection-oriented information about the user and the session is maintained by a server until the session is taken down. In a stateless system, such as NFS, requests are made independently of one another in a connectionless manner. There are advantages to stateless operation. If the server crashes, the request simply goes away and the client makes another request. This simplifies recovery after the crash. In a stateful system, both systems must be aware that one or the other has crashed so they can restore the states and prevent data corruption.

Files are transferred between systems by first establishing a connection-oriented session. The FTAM client contacts the FTAM server and requests a session. Once the session is established, file transfer can take place. FTAM uses the concept of a virtual filestore, which provides a common view of files. The FTAM file system hides the differences between different vendor systems. FTAM specifies document types as files with straight binary information or text files in which each line is terminated with a carriage return. Data is interpreted as records and FTAM provides the virtual filestore capabilities that store record-oriented structured files.

So far, FTAM, like other OSI protocols, has not caught on as a useful system for transferring files between different vendor systems in the LAN environment. Many of the implementations so far have failed to interoperate with one another. FTAM

has worked well as a way to bring mainframe information systems into distributed environments.

FTP

- FTP stands for File transfer protocol.
- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other servers.

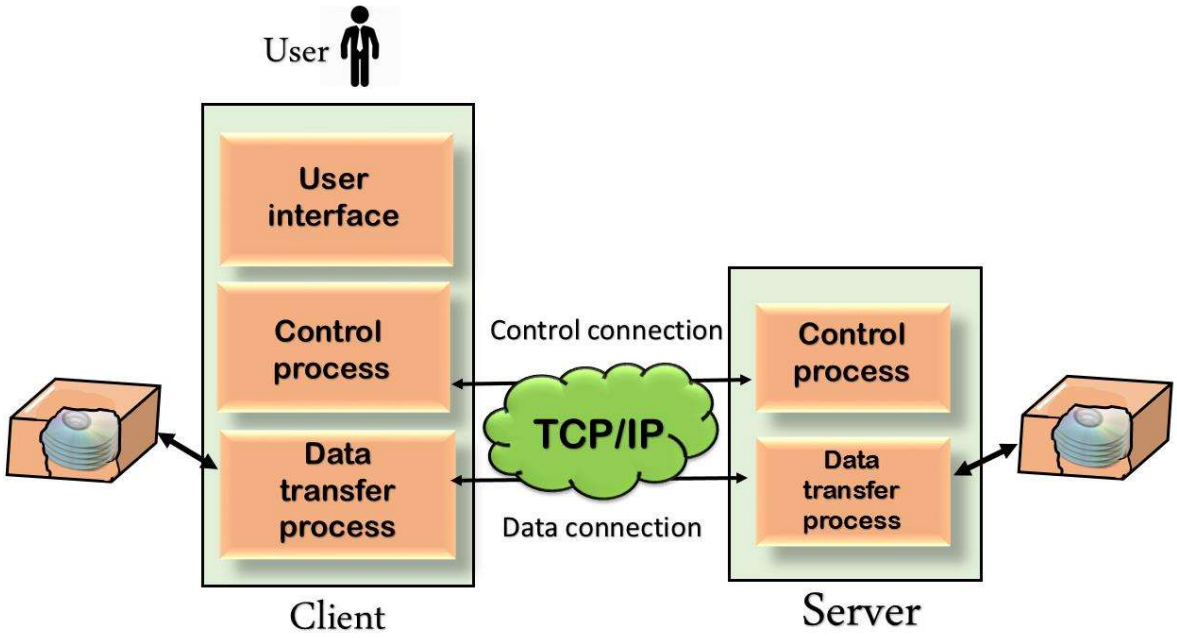
Objectives of FTP

- It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

Why FTP?

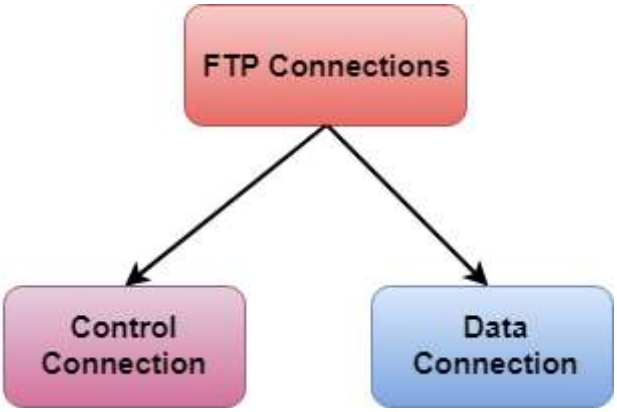
Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

Mechanism of FTP



The above figure shows the basic model of the FTP. The FTP client has three components: the user interface, control process, and data transfer process. The server has two components: the server control process and the server data transfer process.

There are two types of connections in FTP:



- **Control Connection:** The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.
- **Data Connection:** The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

FTP Clients

- FTP client is a program that implements a file transfer protocol which allows you to transfer files between two hosts on the internet.
- It allows a user to connect to a remote host and upload or download the files.
- It has a set of commands that we can use to connect to a host, transfer the files between you and your host and close the connection.
- The FTP program is also available as a built-in component in a Web browser. This GUI based FTP client makes the file transfer very easy and also does not require to remember the FTP commands.

Advantages of FTP:

- **Speed:** One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.
- **Efficient:** It is more efficient as we do not need to complete all the operations to get the entire file.
- **Security:** To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.

- **Back & forth movement:** FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

Disadvantages of FTP:

- The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provides encryption.
- FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.
- Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.
- It is not compatible with every system.

E-mail Protocols are set of rules that help the client to properly transmit the information to or from the mail server. Here in this tutorial, we will discuss various protocols such as **SMTP, POP,** and **IMAP.**

SMTP

SMTP stands for **Simple Mail Transfer Protocol**. It was first proposed in 1982. It is a standard protocol used for sending e-mail efficiently and reliably over the internet.

Key Points:

- SMTP is application level protocol.
- SMTP is connection oriented protocol.
- SMTP is text based protocol.
- It handles exchange of messages between e-mail servers over TCP/IP network.
- Apart from transferring e-mail, SMPT also provides notification regarding incoming mail.
- When you send e-mail, your e-mail client sends it to your e-mail server which further contacts the recipient mail server using SMTP client.
- These SMTP commands specify the sender’s and receiver’s e-mail address, along with the message to be send.
- The exchange of commands between servers is carried out without intervention of any user.

- In case, message cannot be delivered, an error report is sent to the sender which makes SMTP a reliable protocol.

SMTP Commands

The following table describes some of the SMTP commands:

S.N.	Command Description
1	**HELLO** This command initiates the SMTP conversation.
2	**EHELLO** This is an alternative command to initiate the conversation. ESMTP indicates that the sender server wants to use extended SMTP protocol.
3	**MAIL FROM** This indicates the sender's address.
4	**RCPT TO** It identifies the recipient of the mail. In order to deliver similar message to multiple users this command can be repeated multiple times.
5	**SIZE** This command let the server know the size of attached message in bytes.
6	**DATA** The **DATA** command signifies that a stream of data will follow. Here stream of data refers to the body of the message.
7	**QUIT** This commands is used to terminate the SMTP connection.
8	**VERFY** This command is used by the receiving server in order to verify whether the given username is valid or not.

9	**EXPN** It is same as VRFY, except it will list all the users name when it used with a distribution list.

IMAP

IMAP stands for **Internet Mail Access Protocol.** It was first proposed in 1986.

Key Points:

- IMAP allows the client program to manipulate the e-mail message on the server without downloading them on the local computer.
- The e-mail is hold and maintained by the remote server.
- It enables us to take any action such as downloading, delete the mail without reading the mail.It enables us to create, manipulate and delete remote message folders called mail boxes.
- IMAP enables the users to search the e-mails.
- It allows concurrent access to multiple mailboxes on multiple mail servers.

IMAP Commands

The following table describes some of the IMAP commands:

S.N.	Command Description
1	**IMAP_LOGIN** This command opens the connection.
2	**CAPABILITY** This command requests for listing the capabilities that the server supports.
3	**NOOP** This command is used as a periodic poll for new messages or message status updates during a period of inactivity.
4	**SELECT** This command helps to select a mailbox to access the messages.

5	**EXAMINE** It is same as SELECT command except no change to the mailbox is permitted.
6	**CREATE** It is used to create mailbox with a specified name.
7	**DELETE** It is used to permanently delete a mailbox with a given name.
8	**RENAME** It is used to change the name of a mailbox.
9	**LOGOUT** This command informs the server that client is done with the session. The server must send BYE untagged response before the OK response and then close the network connection.

POP

POP stands for Post Office Protocol. It is generally used to support a single client. There are several versions of POP but the POP 3 is the current standard.

Key Points

- POP is an application layer internet standard protocol.
- Since POP supports offline access to the messages, thus requires less internet usage time.
- POP does not allow search facility.
- In order to access the messaged, it is necessary to download them.
- It allows only one mailbox to be created on server.
- It is not suitable for accessing non mail data.
- POP commands are generally abbreviated into codes of three or four letters. Eg. STAT.

POP Commands

The following table describes some of the POP commands:

S.N.	Command Description

1	**LOGIN** This command opens the connection.
2	**STAT** It is used to display number of messages currently in the mailbox.
3	**LIST** It is used to get the summary of messages where each message summary is shown.
4	**RETR** This command helps to select a mailbox to access the messages.
5	**DELE** It is used to delete a message.
6	**RSET** It is used to reset the session to its initial state.
7	**QUIT** It is used to log off the session.

Comparison between POP and IMAP

S.N.	POP	IMAP
1	Generally used to support single client.	Designed to handle multiple clients.
2	Messages are accessed offline.	Messages are accessed online although it also supports offline mode.
3	POP does not allow search facility.	It offers ability to search emails.

4	All the messages have to be downloaded.	It allows selective transfer of messages to the client.
5	Only one mailbox can be created on the server.	Multiple mailboxes can be created on the server.
6	Not suitable for accessing non-mail data.	Suitable for accessing non-mail data i.e. attachment.
7	POP commands are generally abbreviated into codes of three or four letters. Eg. STAT.	IMAP commands are not abbreviated, they are full. Eg. STATUS.
8	It requires minimum use of server resources.	Clients are totally dependent on server.
9	Mails once downloaded cannot be accessed from some other location.	Allows mails to be accessed from multiple locations.
10	The e-mails are not downloaded automatically.	Users can view the headings and sender of e-mails and then decide to download.
10	POP requires less internet usage time.	IMAP requires more internet usage time.

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.

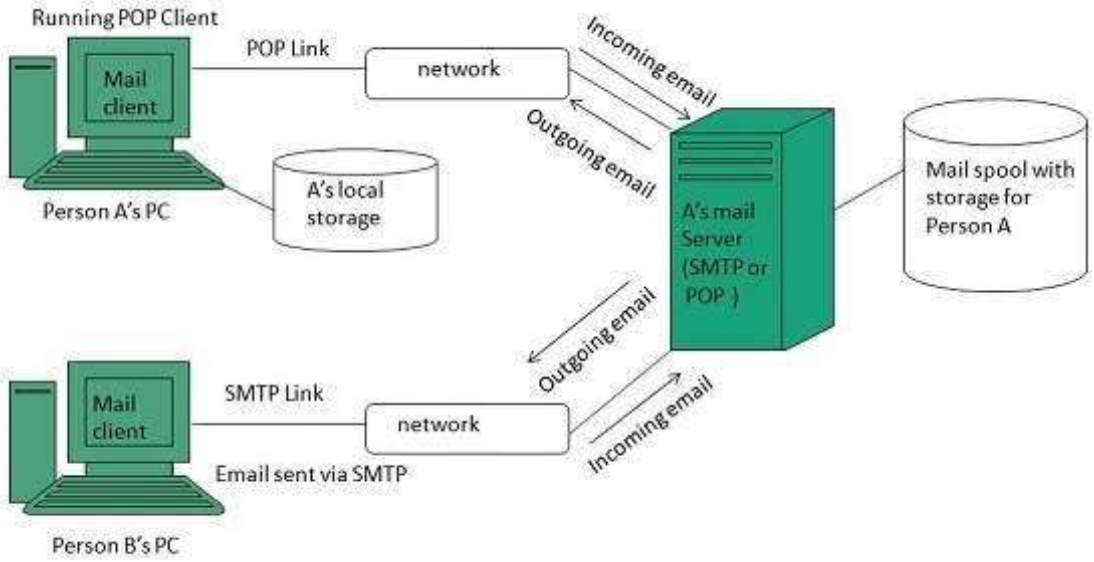
Following example will take you through the basic steps involved in sending and receiving emails and will give you a better understanding of working of email system:

- 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:

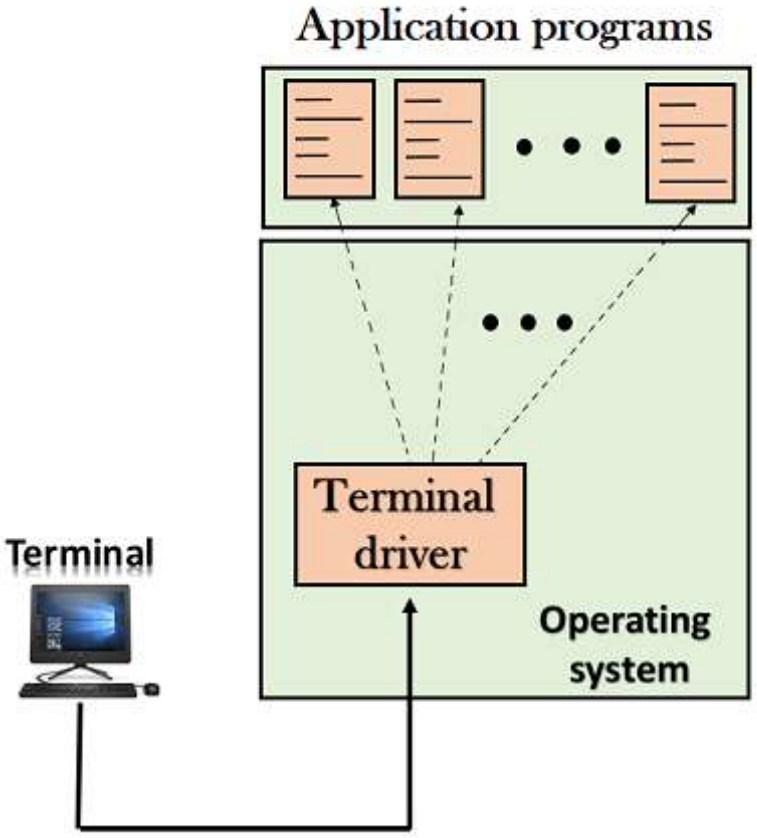


Telnet

- The main task of the internet is to provide services to users. For example, users want to run different application programs at the remote site and transfers a result to the local site. This requires a client-server program such as FTP, SMTP. But this would not allow us to create a specific program for each demand.
- The better solution is to provide a general client-server program that lets the user access any application program on a remote computer. Therefore, a program that allows a user to log on to a remote computer. A popular client-server program Telnet is used to meet such demands. Telnet is an abbreviation for **Terminal Network**.
- Telnet provides a connection to the remote computer in such a way that a local terminal appears to be at the remote side.

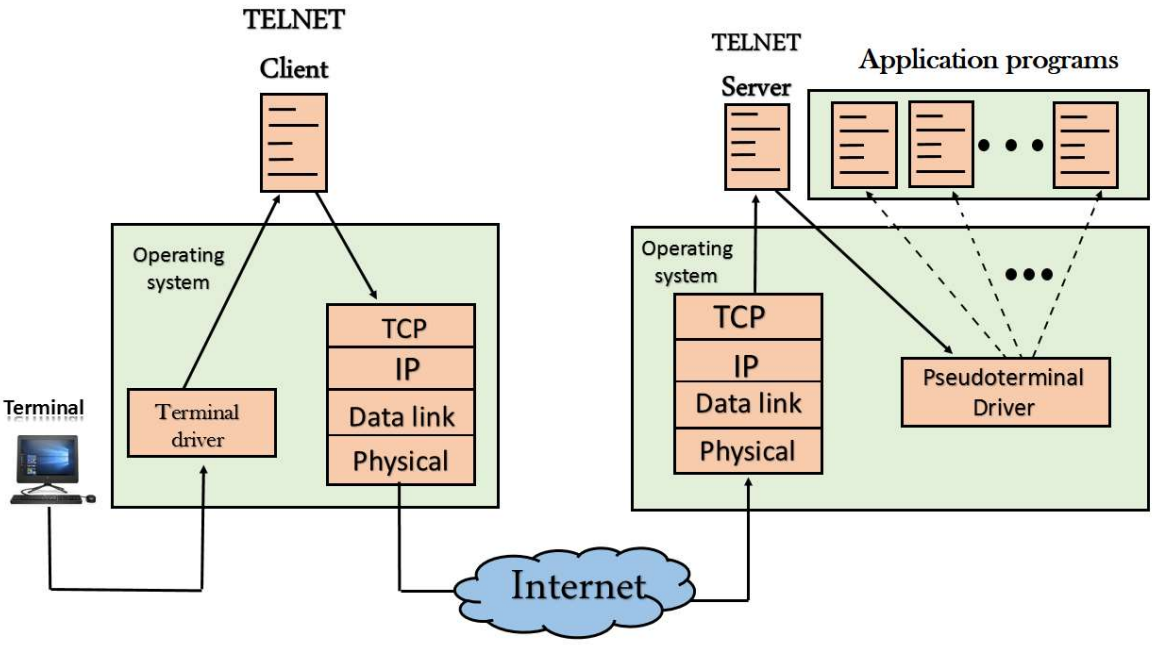
There are two types of login:

Local Login



- When a user logs into a local computer, then it is known as local login.
- When the workstation running terminal emulator, the keystrokes entered by the user are accepted by the terminal driver. The terminal driver then passes these characters to the operating system which in turn, invokes the desired application program.
- However, the operating system has special meaning to special characters. For example, in UNIX some combination of characters have special meanings such as control character with "z" means suspend. Such situations do not create any problem as the terminal driver knows the meaning of such characters. But, it can cause the problems in remote login.

Remote login



- When the user wants to access an application program on a remote computer, then the user must perform remote login.

How remote login occurs

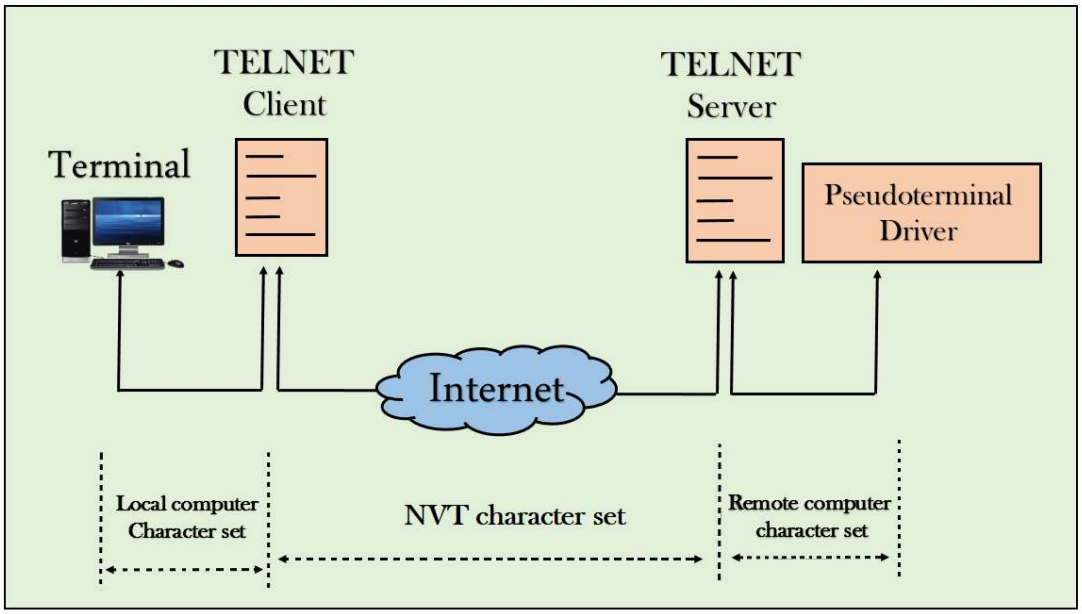
At the local site

The user sends the keystrokes to the terminal driver, the characters are then sent to the TELNET client. The TELNET client which in turn, transforms the characters to a universal character set known as network virtual terminal characters and delivers them to the local TCP/IP stack

At the remote site

The commands in NVT forms are transmitted to the TCP/IP at the remote machine. Here, the characters are delivered to the operating system and then pass to the TELNET server. The TELNET server transforms the characters which can be understandable by a remote computer. However, the characters cannot be directly passed to the operating system as a remote operating system does not receive the characters from the TELNET server. Therefore it requires some piece of software that can accept the characters from the TELNET server. The operating system then passes these characters to the appropriate application program.

Network Virtual Terminal (NVT)



- The network virtual terminal is an interface that defines how data and commands are sent across the network.
- In today's world, systems are heterogeneous. For example, the operating system accepts a special combination of characters such as end-of-file token running a DOS operating system *ctrl+z* while the token running a UNIX operating system is *ctrl+d*.
- TELNET solves this issue by defining a universal interface known as network virtual interface.
- The TELNET client translates the characters that come from the local terminal into NVT form and then delivers them to the network. The Telnet server then translates the data from NVT form into a form which can be understandable by a remote computer.

HTTP

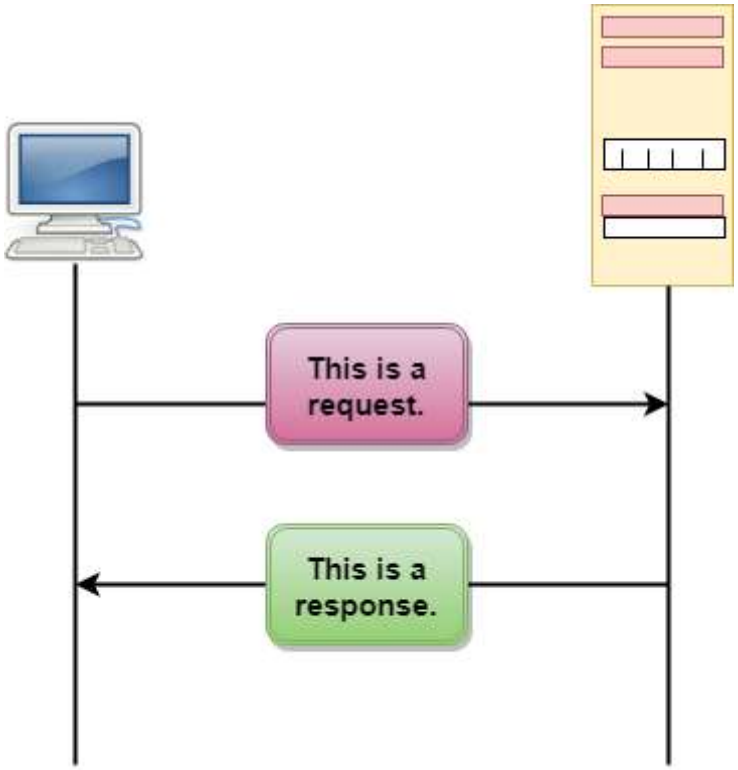
- HTTP stands for **HyperText Transfer Protocol**.
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.
- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.
- HTTP is used to carry the data in the form of MIME-like format.
- HTTP is similar to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in the way the messages are sent from the

client to the server and from server to the client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

Features of HTTP:

- **Connectionless protocol:** HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection. The connection between client and server exist only during the current request and response time only.
- **Media independent:** HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content. It is required for both the client and server to specify the content type in MIME-type header.
- **Stateless:** HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages.

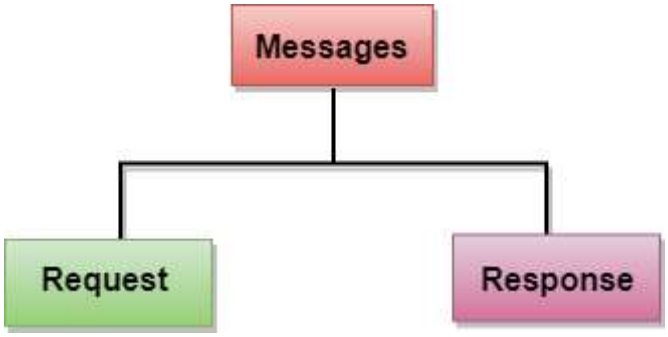
HTTP Transactions



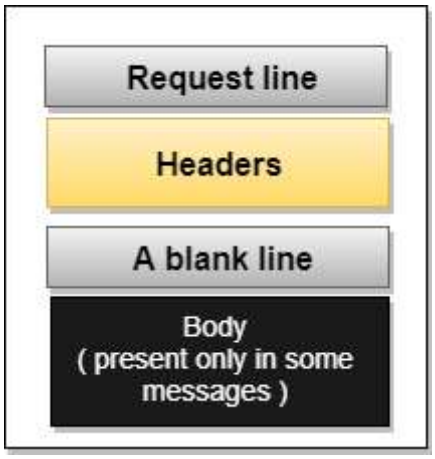
The above figure shows the HTTP transaction between client and server. The client initiates a transaction by sending a request message to the server. The server replies to the request message by sending a response message.

Messages

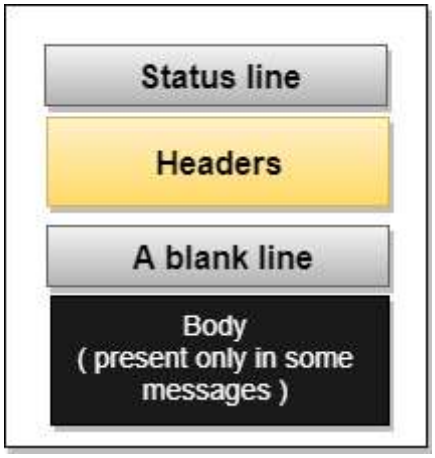
HTTP messages are of two types: request and response. Both the message types follow the same message format.



Request Message: The request message is sent by the client that consists of a request line, headers, and sometimes a body.



Response Message: The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body.



Uniform Resource Locator (URL)

- A client that wants to access the document in an internet needs an address and to facilitate the access of documents, the HTTP uses the concept of Uniform Resource Locator (URL).
- The Uniform Resource Locator (URL) is a standard way of specifying any kind of information on the internet.

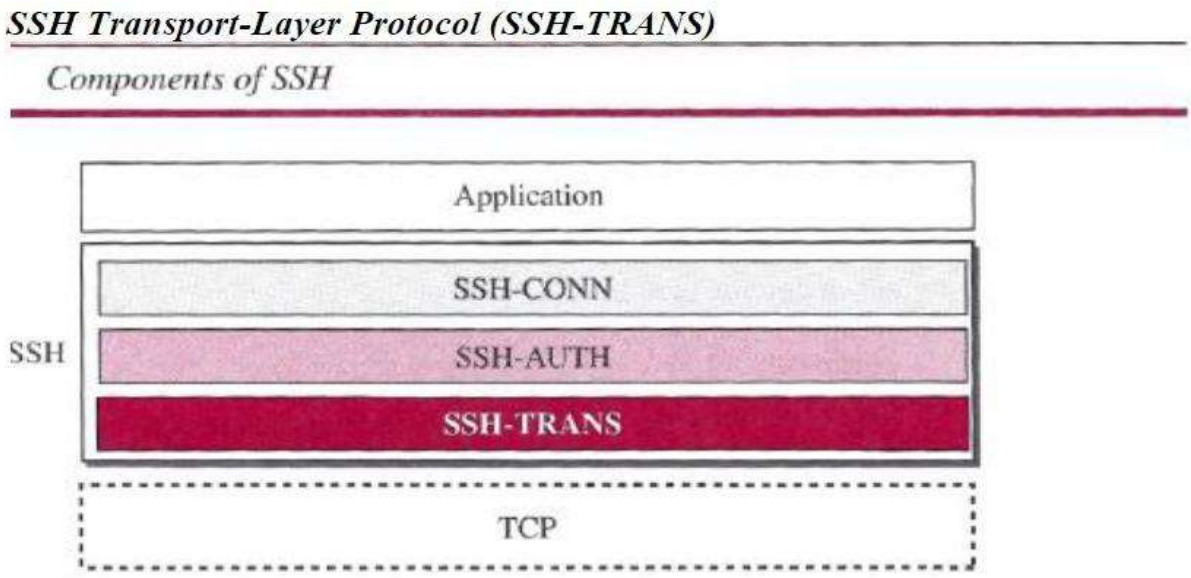
- The URL defines four parts: method, host computer, port, and path.

- **Method:** The method is the protocol used to retrieve the document from a server. For example, HTTP.
- **Host:** The host is the computer where the information is stored, and the computer is given an alias name. Web pages are mainly stored in the computers and the computers are given an alias name that begins with the characters "www". This field is not mandatory.
- **Port:** The URL can also contain the port number of the server, but it's an optional field. If the port number is included, then it must come between the host and path and it should be separated from the host by a colon.
- **Path:** Path is the pathname of the file where the information is stored. The path itself contain slashes that separate the directories from the subdirectories and files.

SECURE SHELL (SSH)

Secure Shell (SSH) is a secure application program that can be used today for several purposes such as remote logging and file transfer; it was originally designed to replace TELNET.
There are two versions of SSH: SSH-l and SSH-2

Components



SSH Transport-Layer Protocol (SSH-TRANS)

SSH first uses a protocol that creates secured channel on top of the TCP.
When the procedure implementing this protocol is called, the client and server first use the TCP protocol to establish an insecure connection.

SSH Authentication Protocol (SSH-AUTH)

- After a secure channel is established between the client and the server and the server is authenticated for the client
- SSH can call another procedure that can authenticate the client for the server. The client authentication process in SSH is very similar to what is done in Secure Socket Layer (SSL)
- The request includes the user name, server name, the method of authentication, and the required data.

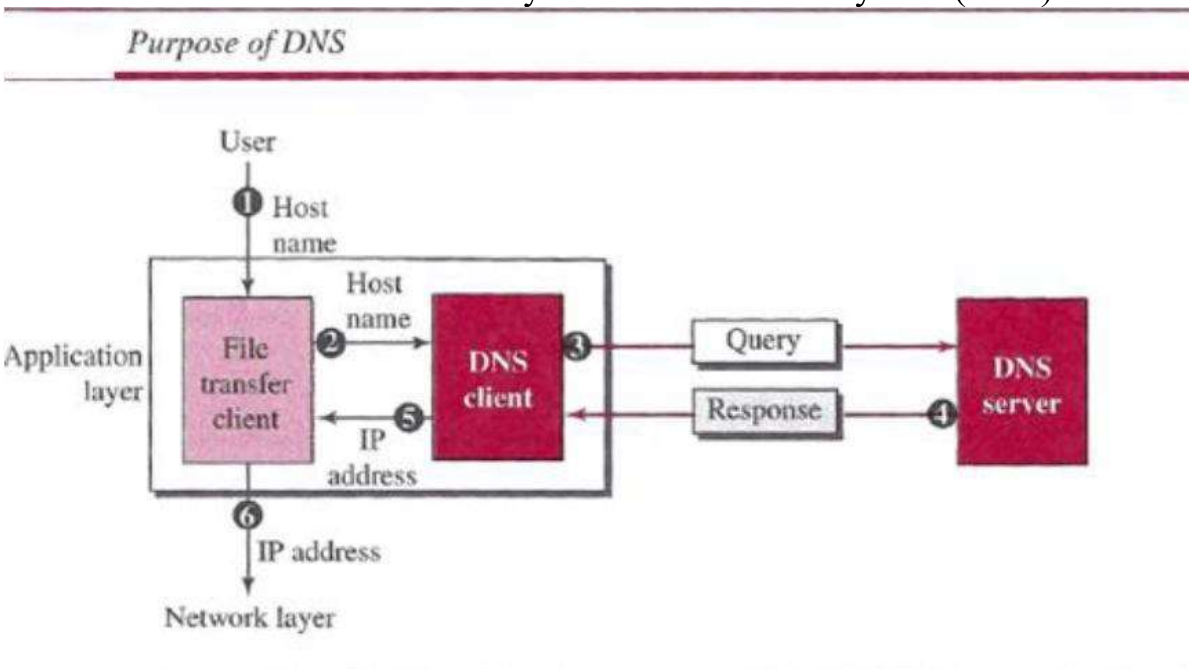
The server responds with either a success message, which confirms that the client is authenticated, or a failed message

SSH Connection Protocol (SSH-CONN)

One of the services provided by the SSH-CONN protocol is multiplexing. SSH-CONN takes the secure channel established by the two previous protocols and lets the client create multiple logical channels over it.
Each channel can be used for a different purpose, such as remote logging, file transfer, and so on

DOMAIN NAME SYSTEM (DNS)

The host that needs mapping can contact the closest computer holding the needed information. This method is used by the Domain Name System (DNS).



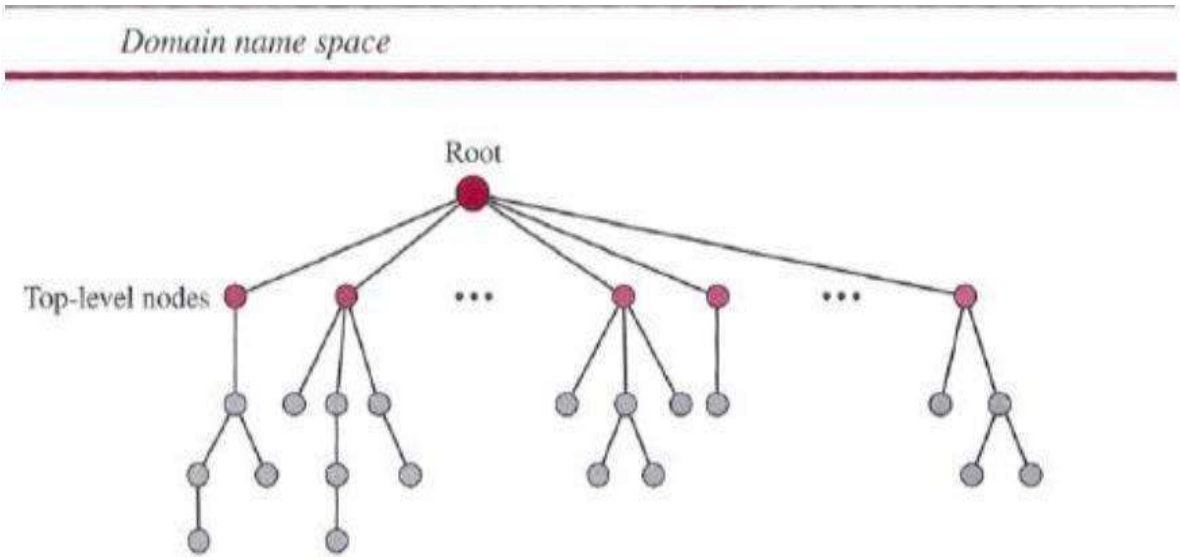
A user wants to use a file transfer client to access the corresponding file transfer

server running on a remote host.
The user knows only the file transfer server name, such as *afilesource.com.*

Name Space

A **name** space that maps each address to a unique name can be organized in two ways: flat or hierarchical.
In a *flat name space,* a name is assigned to an address. A name in this space is a sequence of characters without structure.
In a *hierarchical name space,* each name is made of several parts.

Domain Name Space



Domain Name Space

To have a hierarchical name space, a domain name space was designed. In this design the names are defined in an inverted-tree structure with the root at the top.

Label

Each node in the tree has a label, which is a string with a maximum of 63 characters. The root label is a null string (empty string).

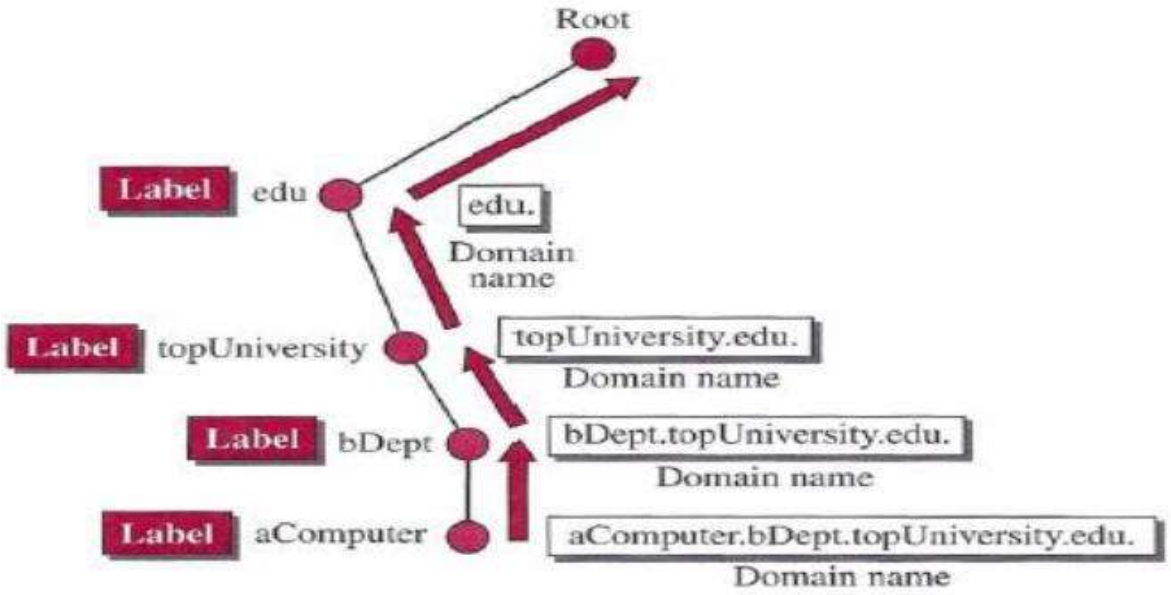
Domain Name

If a label is terminated by a null string, it is called a fully qualified domain name (FQDN).
If a label is not terminated by a null string, it is called a partially qualified domain name PQDN).

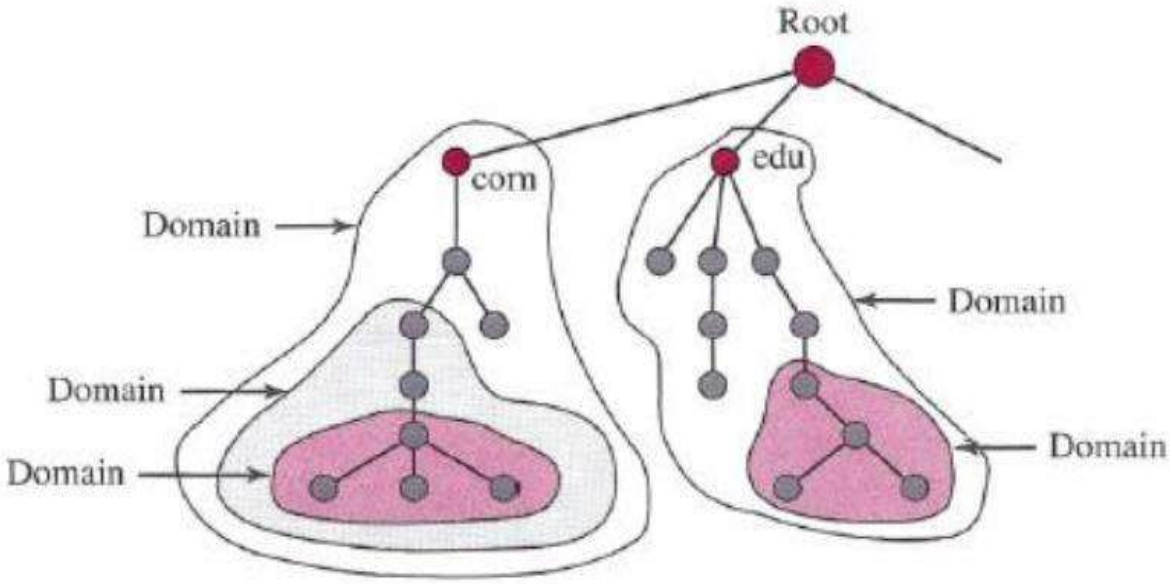
Domain

A domain is a sub tree of the domain name space. The name of the domain is the name of the node at the top of the sub tree.

Domain names and labels



Domains



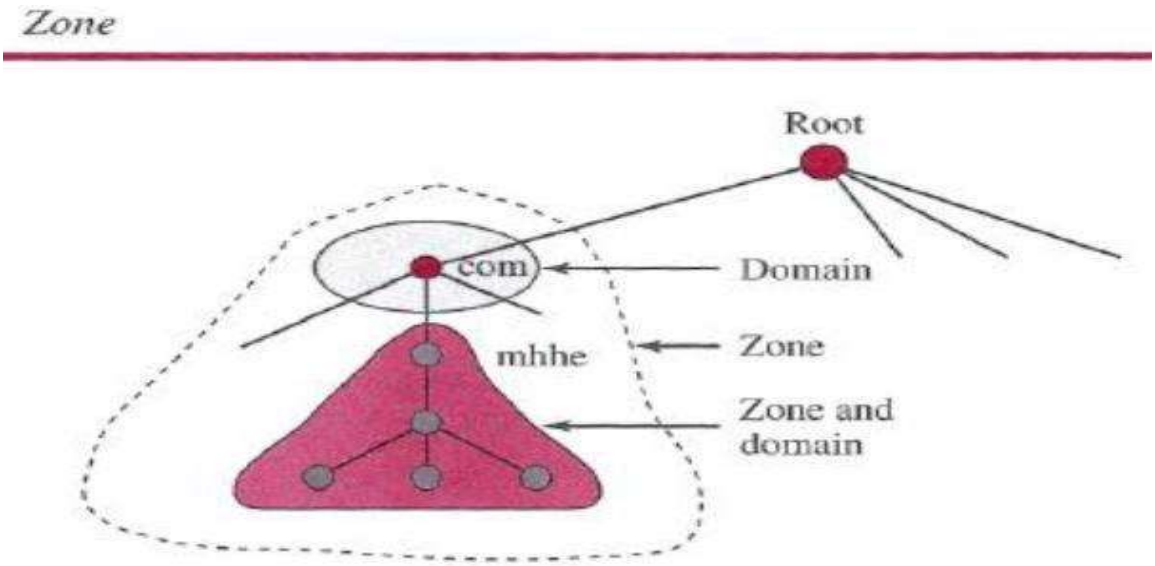
Distribution of Name Space

The information contained in the domain name space must be stored. However, it is very inefficient and also not reliable to have just one computer store such a huge amount of information. It is inefficient because responding to requests from all over the world places a heavy load on the system it is not reliable because any failure makes the data inaccessible.

Zone

Since the complete domain name hierarchy cannot be stored on a single server, it is divided among many servers. What a server is responsible for or has authority over is called a *zone.*

The server makes a database called a *zone file* and keeps all the information for every node under that domain.



Unit-1: Introduction to Network

1.1 Basics of network

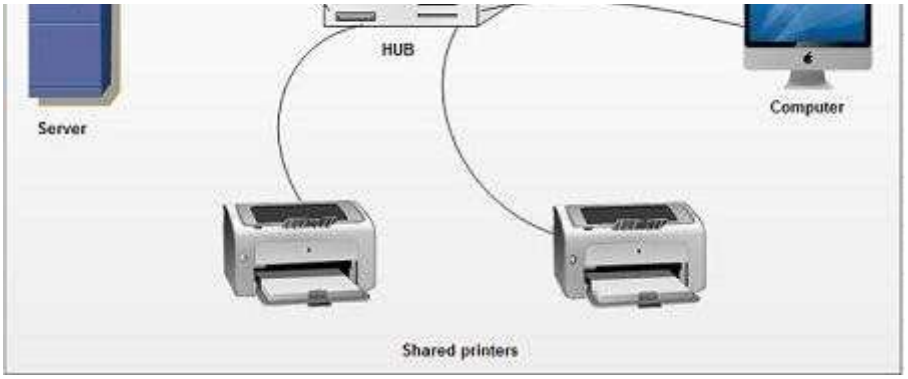
1.1.1 Types of networks

1.1.2 Different topologies (Bus, ring, star, mesh, tree)

1.2 Types of networks (LAN, MAN, WAN)

1.3 Terminologies (Intranet, Internet, Unicast, Broadcast, Multicast)

Introduction to Network/ Basics of network

- A **computer network is** a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending or receiving data from the other node/device through the network.
- **Computer Network** is a group of computers connected with each other through wires, optical fibres or optical links so that various devices can interact with each other through a network.
- A network set up by connecting two or more computers and other supporting hardware devices through communication channels is called a computer network. It enables computers to communicate with each other and to share commands, data, etc., including the hardware and software resources.
- Each computing device in a network is called a node or station. The nodes can be routers, personal computers, and servers. Data transformation is done via the network using rules known as protocols. The protocols are the set of rules which every node of the network should follow for transferring information over the wired or wireless network.
- The aim of the computer network is the sharing of resources among various devices.
- In the case of computer network technology, there are several types of networks that vary from simple to complex level.
- 

How Does a Computer Network Work?

Computer Networks simply work using nodes and links. Data Communication Equipment is simply termed as Nodes. For example, Modems, Hubs, Switches, etc. whereas links in Computer networks can be referred to as a connection between two nodes. We have several types of links like cable wires, optical fibers, etc.

Whenever a Computer Network is working, nodes have the work of sending and receiving data via the links. Computer Network provides some set of protocols that helps in following the rules and protocols.

Computer Network Criteria

1. Performance
2. Reliability
3. Security

Performance

It can be measured in many ways and depends on the number of factors

- No of users
- Type of transmission medium
- Response time
- Transit time
- Hardware
- Software

Reliability

This is measured by the following factors

- Frequency of failure
- The recovery time of a network after a failure.
- Catastrophe

Security

As data is being travelled from node to node through the network to reach its final destination, during that time it can be tampered or can be stolen so the security of information is the top priority.

Network security issues include protecting data from the following

- Unauthorized access
- Viruses

Applications OF COMPUTER NETWORKS

1. **Resource sharing:** Resource sharing is the sharing of resources such as programs, printers, and data among the users on the network without the requirement of the physical location of the resource and user.
2. **Server-Client model:** Computer networking is used in the **server-client model**. A server is a central computer used to store the information and maintained by the

system administrator. Clients are the machines used to access the information stored in the server remotely.

3. **Communication medium:** Computer network behaves as a communication medium among the users. For example, a company contains more than one computer has an email system which the employees use for daily communication.
4. **E-commerce:** Computer network is also important in businesses. We can do the business over the internet. For example, amazon.com is doing their business over the internet, i.e., they are doing their business over the internet.

Uses of Computer Network:

- It allows you to share resources such as printers, scanners, etc.
- You can share expensive software and database among network users.
- It facilitates communications from one computer to another computer.
- It allows the exchange of data and information among users through a network.

Need of computer network

1. **Internet access**: We can easily access information all because of the internet which provides a variety of information and communication facilities, using standardized communication protocols.
2. **eCommerce**: also known as electronic commerce, refers to buying or selling product, service etc through the internet. It has been one of the world most profitable business in the world which is only possible of a computer network.
3. **Entertainment:** It includes games, online video streaming and many other which is only possible because of the computer network.
4. **VoIP:** Through Voice over Internet protocol, telephone calls are made digitally using Internet Protocols instead of the regular analog phone lines.

Advantages of Computer Network

1. **File sharing**: Fundamental goals of a computer network is to allow file sharing and remote file access.
2. **Server-Client model**: Client-server model is a distributed application framework. The server is a master system which stores the data and provides the processing service. A client is a user system which accesses the data from the server and can perform processing in its system or in a server system.
3. **Resource sharing**: All the resources such as printers, modems, scanners and fax machines etc can be shared by all the system in a computer network.
4. **Better connectivity and communications**: A computer network allows all the user or computers at a different location to communicate easily, widely used example is email, video conference etc.

Disadvantages of Computer Network

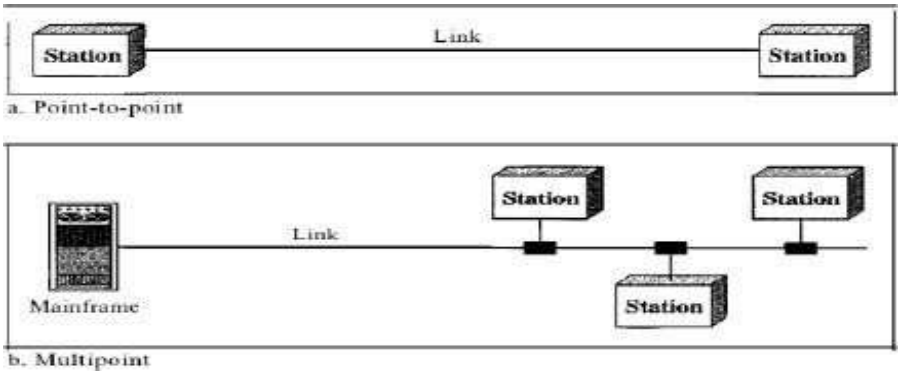
1. **Lack of data security and privacy** due to the huge number of the user accessing the internet from every corner of the earth, handling data is a challenging task and data can be stolen which violate the privacy of the user.

2. **Presence of computer viruses and the malware:** A virus can easily spread through an interconnected workstation or over the internet which can damage or steal the data from the computer system in a computer network.
3. **Lack of Independence:** In most cases, the client is dependent on the centralized server and client user lack any freedom whatsoever. the centralized server can make hinder in the decision making of the user system.
4. **Lack of Robustness:** As a client is dependent on the centralized server, if the centralized server breaks down, the entire system of networks would be useless and also if any of the links between the end system fail then the network will standstill.
5. **Need an efficient handler:** As a computer network consisting of many devices and software, so to handle the smooth functioning of the transmission of information, it requires high technical skills and knows- how its administration and its operations.

TYPES OF CONNECTIONS: A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. There are two possible types of connections: point-to-point and multipoint.

(1) **Point-to-Point:** A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections. use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible. When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

(2) **Multipoint:** A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.



Network Architecture

Network architecture is the design of a computer network. It is a framework for the specification of a network's physical components and their functional organization and configuration, its operational principles and procedures, as well as communication protocols used.

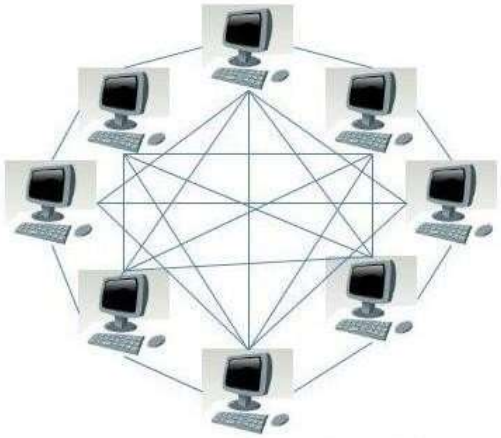
There are two major types of network architectures:

- Peer-To-Peer Architecture
- Client/Server Architecture

Peer-To-Peer Architecture

- In a peer-to-peer network, tasks are allocated to every device on the network.
- Furthermore, there is no real hierarchy in this network, all computers are considered equal andall have the same abilities to use the resources available on this network.
- Instead of having a central server which would act as the shared drive, each computer that's

connected to this network would act as the server



Peer-to-Peer Network Model

Advantages of Peer-To-Peer Network:

- It is less costly as it does not contain any dedicated server.
- If one computer stops working but, other computers will continue working.
- It is easy to set up and maintain as each computer manages itself.

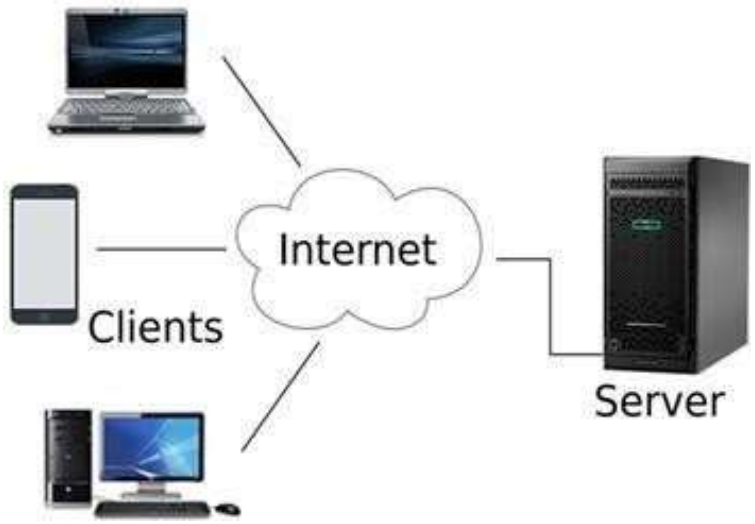
Disadvantages of Peer-To-Peer Network:

- In the case of Peer-To-Peer network, it does not contain the centralized system. Therefore, itcannot back up the whole data as the data is different in different locations.
- Security and data backups are to be done to each individual computer.
- As the numbers of computers increases on a P2P network; performance,

security, and accessbecome a major headache.

Client/Server Architecture

- Client-server architecture, architecture of a computer network in which many clients (remote processors) request and receive service from a centralized server (host computer).
- In a client/server network, a centralized, really powerful computer(server) act as a hub in which other computers or workstations(clients) can connect to. This server is the heart of the system, which manages and provides resources to any client that requests them.
- A server performs all the major operations such as security and network management.
- A server is responsible for managing all the resources such as files, directories, printer, etc.
- All the clients communicate with each other through a server. For example, if client1 wants tosend some data to client 2, then it first sends the request to the server for the permission. Theserver sends the response to the client 1 to initiate



its communication with the client 2.

Advantages of a client/server network

- Resources and data security are controlled through the server.
- Not restricted to a small number of computers.
- Server can be accessed anywhere and across multiple platforms.

Disadvantages of a client/server network

- Can become very costly due to the need of a server as well as networking devices such as hubs,routers, and switches.
- If and when the server goes down, the entire network will be affected.
- Technical staff needed to maintain and ensure network functions efficiently.

1.1.1 /1.2 Types of Computer Networks

There are two primary types of computer networking: wired networking and wireless networking.

1. **Wired Network:** As we all know, "wired" refers to any physical medium made up of cables. Copper wire, twisted pair, or fiber optic cables are all options. A wired network employs wires to link devices to the Internet or another network, such as laptops or desktop PCs.
2. **Wireless Network:** "Wireless" means without wire, media that is made up of electromagnetic waves (EM Waves) or infrared waves. Antennas or sensors will be present on all wireless devices. Cellular phones, wireless sensors, TV remotes, satellite dish receivers, and laptops with WLAN cards are all examples of wireless devices. For data or voice communication, a wireless network uses radio frequency waves rather than wires.

As a general rule, wired networking offers greater speed, reliability and security compared to wirelessnetworks; wireless networking tends to provide more flexibility, mobility and scalability.

Some of the different networks based on size are:

- Local area network, or LAN
- Metropolitan area network, or MAN
- Wide area network, or WAN

Local Area Networks (LAN):

- Local area networks, generally called LANs, are privately-owned networks within a single building orcampus of up to a few kilometers in size.
- They are widely used to connect personal computers and workstations in company offices and organizations to share resources (e.g., printers) and exchange information.
- **LANs are distinguished from other kinds of networks by three characteristics:**
  (1) Their size,
  (2) Their transmission technology
  (3) Their topology.
- A LAN can also be formed with two computers connected over a network. Hub, Switches, Cables, and Optical fibers are used to connect various computers and devices to a network.
- Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps.
- The most common LAN topologies are bus, ring, and star
- Examples of LAN are networking in a home, school, college, office, etc.
- Group of interconnected computers within a small area. (room, building, campus)
- Two or more pc's can from a LAN to share files, folders, printers, applications and other devices. Coaxial or CAT 5 cables are normally used for connections.
- Due to short distances, errors and noise are minimum.
- Data transfer rate is 10 to 100 mbps. Example: A computer lab in a school.
- LANs are restricted in size, which means that the worst-case transmission time is bounded and known in advance.
- Knowing this bound makes it possible to use certain kinds of designs that would not

otherwise be possible. It also simplifies network management.

- Traditional LANs run at speeds of 10 Mbps to 100 Mbps, have low delay (microseconds or nanoseconds), and make very few errors. Newer LANs operate atup to 10 Gbps.

Characteristics of LAN:

- LANs are private networks, not subject to external control
- Simple and better performance
- Work in a restricted geographical area

Advantages:

- Resource sharing
- Software applications sharing
- Easy and Cheap communication
- Data Security
- Internet sharing
- High data transfer rate
- Ease of setup
- Centralized Data
- Low Cost

Disadvantages

- Restricted to local area
- Covers small area
- The cables and connectors get damaged easily
- Requires administrative time

Metropolitan Area Network (MAN):

- A metropolitan area network, or MAN, covers a city.
- A MAN is a computer network that interconnects users with computer resources in a geographical area or region larger than that covered by a LAN.
- It canbe an interconnection between several LANs by bridging them with backbone lines.
- This type of network is created by linking existing LAN networks to cover a large geographical area. MAN is smaller than LAN but larger than WAN.
- A MAN is larger than a LAN but smaller than a WAN. This is the type of computer network that connects computers over a geographical distance through a shared communication path over a city, town, or metropolitan area.
- Design to extend over a large area.
- Connecting number of LAN's to form larger network, so that resources can be shared.

- Networks can be up to 5 to 50 km. Owned by organization or individual.
- Data transfer rate is low compare to LAN. Example: Organization with different branches located in the city.
- Examples of MAN are networking in government agencies, airports, libraries, etc.

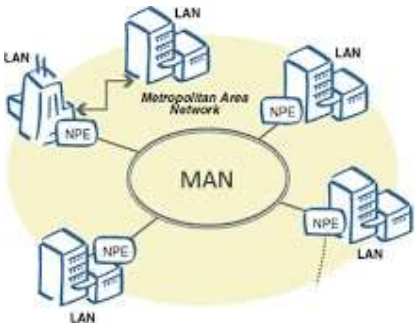


Fig: Metropolitan Area Network

Characteristics:

- Generally, covers towns and cities (up to 50km)
- Transmission medium used for MAN is optical fiber, coaxial cable etc.
- Data rates adequate for distributed computing applications
- The size of the MAN is in the range of 5km to 50km.
- The MAN ranges from the campus to the entire city.
- The MAN is maintained and managed by either the user group or the Network provider.
- Users can achieve the sharing of regional resources by using MAN.
- The data transmission rates can be medium to high

Uses Of Metropolitan Area Network:

- MAN is used in communication between the banks in a city.
- It can be used in an Airline Reservation.
- It can be used in a college within a city.
- It can also be used for communication in the military.

Advantages

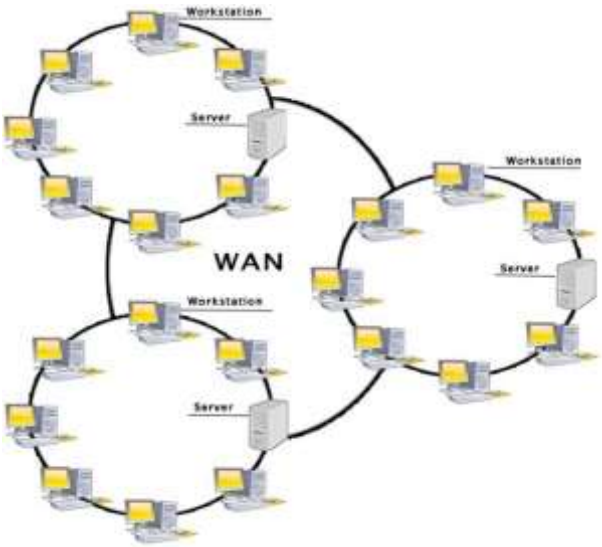
- **Less Expensive:** It is less expensive to set up a MAN and to connect it to a WAN.
- **High Speed:** The speed of data transfer is more than WAN.
- **Local Emails:** It can send local emails fast.
- **Access to the Internet:** It allows you to share your internet connection, and thus multiple users can have access to high-speed internet.
- **Easy to set up:** You can easily set up a MAN by connecting multiple LANs.
- **High Security:** It is more secure than WAN.

Disadvantages

- Complex, more cabling required and expensive
- Difficult to handle due to large network size
- Risk of hacking
- High installation cost as it requires fiber optics

Wide Area Network (WAN)

- A WAN is a type of computer network that covers a large geographical area. WAN is also defined as the connection of several LANs linked together to cover an entire city or country. The WAN network is provided via several methods such as telephone lines, fiber optics cable, and also through satellite links.
- Are country and worldwide network.
- Contains multiple LAN's and MAN's.
- Distinguished in terms of geographical range.
- Uses satellites and microwave relays.
- Data transfer rate depends upon the ISP provider and varies over the location.
- Best example is the internet
- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.



Characteristics

• Covers large distances (states, countries, continents)

• Communication medium used are satellite, public telephone networks which are connected by routers

Advantages Of WAN are-

- Covers vast area
- Multiple users can share and access the internet at the same time
- High Bandwidth
- Covers large geographical area
- Shared software and resources with connecting workstations
- Information can be exchanged to anyone else worldwide in the network

Disadvantages Of WAN are-

- High initial investment cost
- Hard to handle as the network is vast and complex.
- Less secure
- Data security
- Network is very complex and management is difficult
- As size increases, the networks become more expensive

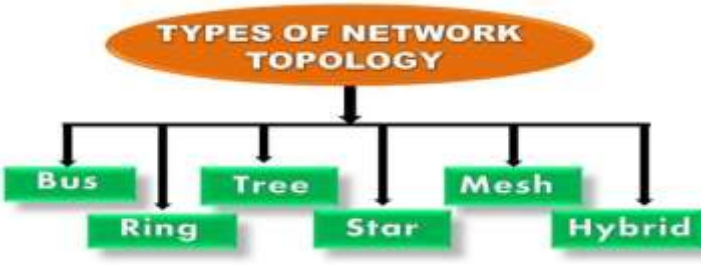
1.1.2 Different topologies (Bus, ring, star, mesh, tree)

Physical Topology

- The term *physical topology* refers to the way in which a network is laid out physically.
- Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.
- The physical arrangement of the computer system/node, which is connected to each other via communication medium is called topologies.

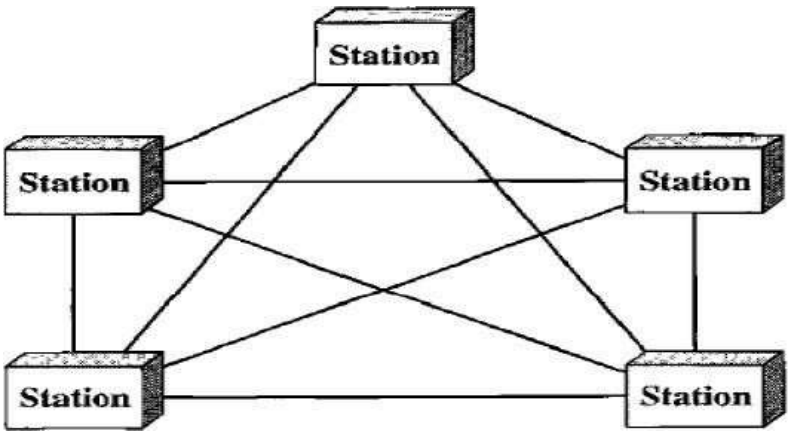
Types of topology:

(1) Mesh topology.
(2) Star topology.
(3) Tree (Hierarchical) topology.
(4) Bus topology.
(5) Ring topology.



MESH:

- In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects.
- A mesh topology is the one where every node is connected to every other node in the network.
- A mesh topology can be a **full mesh topology** or a **partially connected mesh topology**.



- In a ***full mesh topology***, every computer in the network has a connection to each of the other computers in that network. The number of connections in this network can be calculated using the following formula (***n*** is the number ofcomputers in the network): **n(n-1)/2**

- To find the numberof physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to n - I nodes, node 2 must be connected to n – 1 node, and finally node n must be connected to n - 1 nodes. We need n(n - 1) physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need n(n -1) /2 duplex-mode links. To accommodate that many links, every device on the network must have n – 1 input/output portsto be connected to the other n - 1 stations.
- In a ***partially connected mesh topology***, at least two of the computers in the network have connections to multiple other computers in that network. It is an inexpensive way to implement redundancy in a network. In the event that one of the primary computers or connections in the network fails, the rest of the network continues to operate normally.

Following are the advantages of Mesh topology:

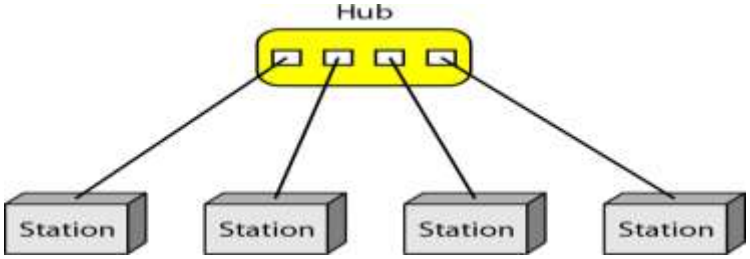
- Easy to transmit data.
- We can send data from many devices simultaneously. Mesh topology will handle much traffic as compared to other topologies.

- If one link is broken or remains faulty, data transfer can occur between nodes using other links. Hence data transmission is uninterrupted and reliable.
- The physical margins will not allow other persons to enter and access the messages.
- Fault detection and isolation are easy.

Following are the disadvantages of Mesh topology:

1. Very high cabling required.
2. Cost in efficient to implement.
3. Complex to implement and takes large space to install the network.
4. Installation and maintenance are very difficult.

STAR:



- In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub.
- The devices are not directly linked to one another.
- Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.
- The star topology is used in local-area networks (LANs).
- High-speed LANs often use a star topology with a central hub

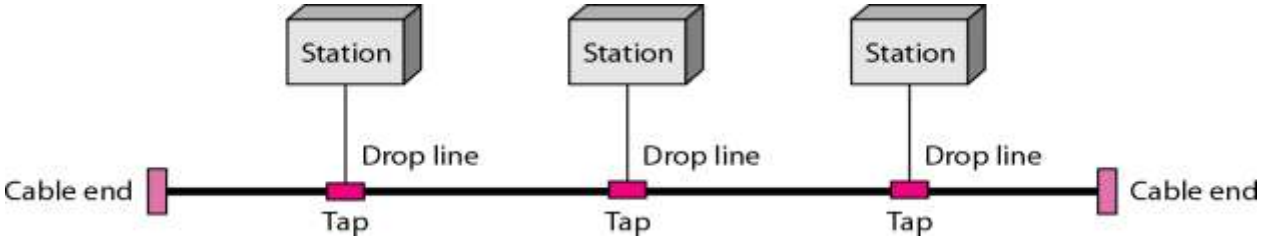
Advantages of star topology

- Centralized management of the network, through the use of the central computer, hub, or switch.
- Easy to add another computer to the network.
- If one computer on the network fails, the rest of the network continues to function normally.
- The star topology is used in local-area networks (LANs), High-speed LANs often use a star topology with a central hub.
- A star topology is less expensive than a mesh topology.
- Easy to install
- If a node fails, it will not affect other nodes.
- Easy to reconfigure and upgrade(configured using a central device).

Disadvantages of star topology

- The star topology ,we must required a network device like Hub, Switch etc.
- If two nodes want to share the data ,sharing is only possible through HUB.
- If HUB is failed the entire network will be failed.
- We can't send private data.

BUS:



- A bus topology is multipoint
- Every computer and network device is connected to a single cable in a bus topology network.
  a **line topology**, a **bus topology** is a network setup in which each computer and network device are connected to a single cable or backbone.
- Nodes are connected to the bus cable by drop lines and taps.
- A drop line is a connection running between the device and the main cable.
- A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.
- As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels fartherand farther. For this reason, there is a limit on the number of taps a bus can support and on the distancebetween those taps.

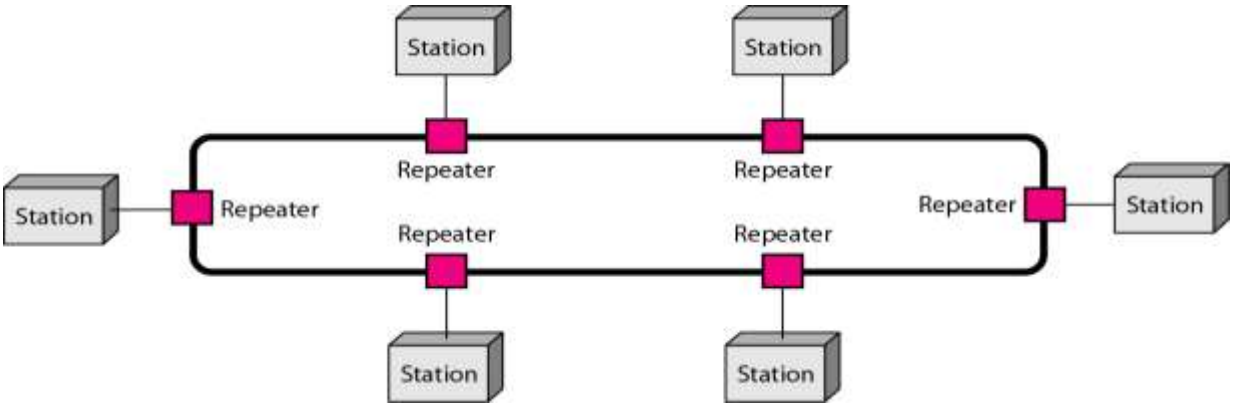
Following are the advantages of Bus topology:

1. Simple to use and install.
2. If a node fails, it will not affect other nodes.
3. Less cabling is required.
4. Cost-efficient to implement.

Following are the disadvantages of Bus topology:

1. Efficiency is less when nodes are more(strength of signal decreases).
2. If the bus fails, the network will fail.
3. A limited number of nodes can connect to the bus due to limited bus length.
4. Security issues and risks are more as messages are broadcasted to all nodes.
5. Congestion and traffic on the bus as it is the only source of communication.

RING:



- A **ring topology** is a network configuration in which device connections createa circular data path. In a ring network, packets of data travel from one device tothe next until they reach their destination. Most ring topologies allow packets to travel only in one direction, called a **unidirectional** ring network. Others permit data to move in either direction, called **bidirectional**.
- The major disadvantage of a ring topology is that if any individual connection in the ring is broken, the entire network is affected.
- Ring topologies may be used in either local area networks (LANs) or wide area networks (WANs).

Advantages

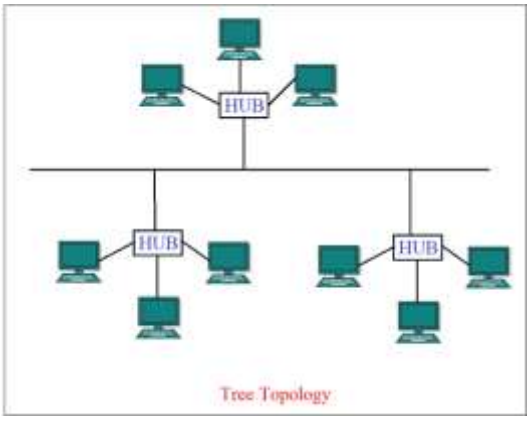
- Data transmission is relatively straightforward because packets only move in one direction.
- There is no requirement for a central controller to manage communication between nodes.
- Easy installation & Reconfiguration
- Simplified Faulty connections

Disadvantages

- In a Unidirectional Ring, a data packet must traverse through all nodes.
- All computers must be turned on in order for them to connect with one another.

Tree Topology:

Tree topology is a computer network topology in which all the nodes are directly or indirectly connected to the main bus cable. Tree topology is a combination of Bus and Star topology.



In a tree topology, the whole network is divided into segments, which can be easily managed and maintained. There is a main hub and all the other sub-hubs are connected to each other in this topology.

Following are the advantages of Tree topology:

- Large distance network coverage.
- Fault finding is easy by checking each hierarchy.
- Least or no data loss.
- A Large number of nodes can be connected directly or indirectly.
- Other hierarchical networks are not affected if one of them fails.

Following are the disadvantages of Tree topology:

- Cabling and hardware cost is high.
- Complex to implement.

1.3 Terminologies (Intranet, Internet, Unicast, Broadcast, Multicast)

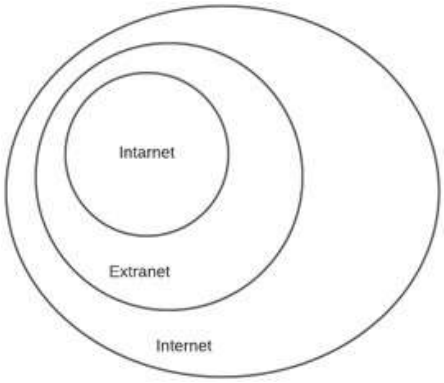
Internet:

- Internet is used to connect the different networks of computers simultaneously.
- It is a public network therefore anyone can access the internet. On the internet, there are multiple users and it provides an unlimited of information to the users.

Intranet:

Intranet is the type of internet that is used privately.

- It is a private network therefore anyone can't access the intranet.
- On the intranet, there is a limited number of users and it provides a piece of limited information to its users.



The difference between the internet and intranet:

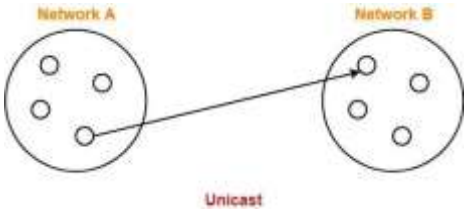
S.NO	Internet	Intranet
1.	Internet is used to connect different networks of computers simultaneously.	Intranet is owned by private firms.
2.	On the internet, there are multiple users.	On an intranet, there are limited users.
3.	Internet is unsafe.	Intranet is safe.
4.	On the internet, there is more number of visitors.	In the intranet, there is less number of visitors.
5.	Internet is a public network.	Intranet is a private network.
6.	Anyone can access the Internet.	In this, anyone can't access the Intranet.
7.	The Internet provides unlimited information.	Intranet provides limited information.

S.NO	Internet	Intranet
8.	Using Social media on your phone or researching resources via Google.	A company used to communicate internally with its employees and share information
9.	The Internet is a global network that connects millions of devices and computers worldwide.	An intranet is a private network that connects devices and computers within an organization.
10.	It is open to everyone and allows access to public information, such as websites and online services.	An intranet is only accessible to authorized users within the organization.
11.	It is used for communication, sharing of information, e-commerce, education, entertainment, and other purposes.	An intranet is primarily used for internal communication, collaboration, and information sharing within an organization.
12.	Users can access the Internet from any location with an Internet connection and a compatible device.	Access to an intranet is restricted to authorized users within the organization and is typically limited to specific devices and locations.
13.	Security measures, such as firewalls, encryption, and secure sockets layer (SSL) protocols, are used to protect against threats like hacking, viruses, and malware.	Intranets employ similar security measures to protect against unauthorized access and ensure the privacy and integrity of shared data.

S.NO	Internet	Intranet
14.	The Internet is a public network that is not owned by any particular organization or group.	Intranets are private networks that are owned and managed by the organization that uses them.
15.	Examples of Internet-based services include email, social media, search engines, and online shopping sites.	Examples of intranet-based services include internal communications, knowledge management systems, and collaboration tools

Unicast-

- Transmitting data from one source host to one destination host is called as **unicast**.
- It is a one to one transmission.



Example-

Host A having IP Address 11.1.2.3 sending data to host B having IP Address 20.12.4.2.

Here,

- Source Address = IP Address of host A = 11.1.2.3
- Destination Address = IP Address of host B = 20.12.4.2

2. Broadcast-

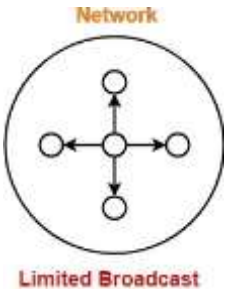
- Transmitting data from one source host to all other hosts residing in the same or other network is called as **broadcast**.
- It is a one to all transmission.

Based on recipient's network, it is classified as-

1. Limited Broadcast
2. Direct Broadcast

A. Limited Broadcast-

- Transmitting data from one source host to all other hosts residing in the same network is called as **limited broadcast**.



NOTE

Limited Broadcast Address for any network

= All 32 bits set to 1

= 11111111.11111111.11111111.11111111

= 255.255.255.255

Example-

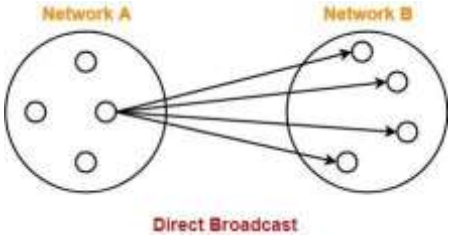
Host A having IP Address 11.1.2.3 sending data to all other hosts residing in the same network.

Here,

- Source Address = IP Address of host A = 11.1.2.3
- Destination Address = 255.255.255.255

B. Direct Broadcast-

- Transmitting data from one source host to all other hosts residing in some other network is called as **direct broadcast**.



NOTE

Direct Broadcast Address for any network is the IP Address where-

- Network ID is the IP Address of the network where all the destination hosts are present.
- Host ID bits are all set to 1.

Example-

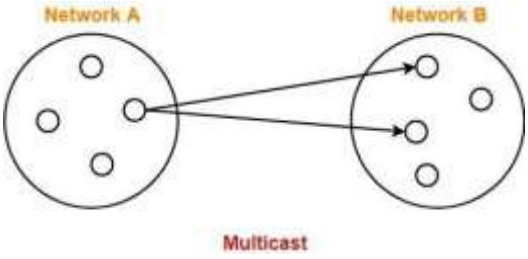
Host A having IP Address 11.1.2.3 sending data to all other hosts residing in the network having IP Address 20.0.0.0

Here,

- Source Address = IP Address of host A = 11.1.2.3
- Destination Address = 20.255.255.255

Multicast-

- Transmitting data from one source host to a particular group of hosts having interest in receiving the data is called as **multicast**.
- It is a one to many transmission.



Examples-

- Sending a message to a particular group of people on whatsapp
- Sending an email to a particular group of people
- Video conference or teleconference

Difference Between Unicast, Broadcast, and Multicast in Computer Network

Here is a list of the differences between Unicast, Broadcast, and Multicast in Computer Network.

Parameters	Unicast	Broadcast	Multicast
Basics	There is only one receiver and one sender.	There are multiple receivers and one sender.	There are multiple receivers and multiple senders.
Meaning and Definition	Unicast information transfer is helpful for transferring data from a single client to all the recipients over the same network.	Broadcast data transfer occurs when one sender transmits data to multiple recipients at any given time.	Multiple senders and recipients participate in the process of data transfer in Multicasting.
Mapping	It is a one-to-one type of data transfer.	It is a one-to-many type of data transfer.	It is a many-to-many type of data transfer.
Uses	It is very helpful when a single sender transmits data to a single recipient.	Broadcasting is mainly helpful for audio and video distribution by television networks.	These are helpful in the stock exchange, multimedia delivery, etc.

Unit-2: Internet and Intranet

2.1 Concepts of Internet and Intranet

2.1.1 Working of Internet and its architecture

2.1.2 Working of Intranet and its architecture

2.1.3 Network Devices terminologies: Hub, modem, switch, Routers, Gateways, Access point

2.2 Types of Cables: co-axial, UTP, Fiber Optic cable

2.1 Concepts of Internet and Intranet

Internet

Internet is called the network of networks. It is a global communication system that links together thousands of individual networks. In other words, internet is a collection of interlinked computer networks, connected by copper wires, fiber-optic cables, wireless connections, etc. As a result, a computer can virtually connect to other computers in any network. These connections allow users to interchange messages, to communicate in real time (getting instant messages and responses), to share data and programs and to access limitless information.

It can be defined in many ways as follows:

- Internet is a world-wide global system of interconnected computer networks.
- Internet uses the standard Internet Protocol (TCP/IP).
- Every computer in internet is identified by a unique IP address.
- IP Address is a unique set of numbers (such as 110.22.33.114) which identifies a computer location.
- A special computer DNS (Domain Name Server) is used to give name to the IP Address so that user can locate a computer by a name.
- For example, a DNS server will resolve a name **http://www.tutorialspoint.com** to a particular IP address to uniquely identify the computer on which this website is hosted.
- Internet is accessible to every user all over the world.

Advantages:

- Internet allows us to communicate with the people sitting at remote locations. There are various apps available on the wed that uses Internet as a medium for communication. One can find various social networking sites such as:
    - Facebook
    - Twitter
    - Yahoo
    - Google+
    - Flickr
    - Orkut
- One can surf for any kind of information over the internet. Information regarding various topics such as Technology, Health & Science, Social Studies, Geographical Information, Information Technology, Products etc can be surfed with help of a search engine.
- Apart from communication and source of information, internet also serves a medium for entertainment. Following are the various modes for entertainment over internet.
    - Online Television
    - Online Games
    - Songs
    - Videos
    - Social Networking Apps
- Internet allows us to use many services like:
    - Internet Banking
    - Matrimonial Services
    - Online Shopping
    - Online Ticket Booking
    - Online Bill Payment
    - Data Sharing
    - E-mail
- Internet provides concept of **electronic commerce**, that allows the business deals to be conducted on electronic systems

Disadvantages

- There are always chances to loose personal information such as name, address, credit card number. Therefore, one should be very careful while sharing such information. One should use credit cards only through authenticated sites.
- Another disadvantage is the **Spamming**.Spamming corresponds to the unwanted e-mails in bulk. These e-mails serve no purpose and lead to obstruction of entire system.
- **Virus** can easily be spread to the computers connected to internet. Such virus attacks may cause your system to crash or your important data may get deleted.
- Also a biggest threat on internet is pornography. There are many pornographic sites that can be found, letting your children to use internet which indirectly affects the children healthy mental life.
- There are various websites that do not provide the authenticated information. This leads to misconception among many people.

Uses of the internet

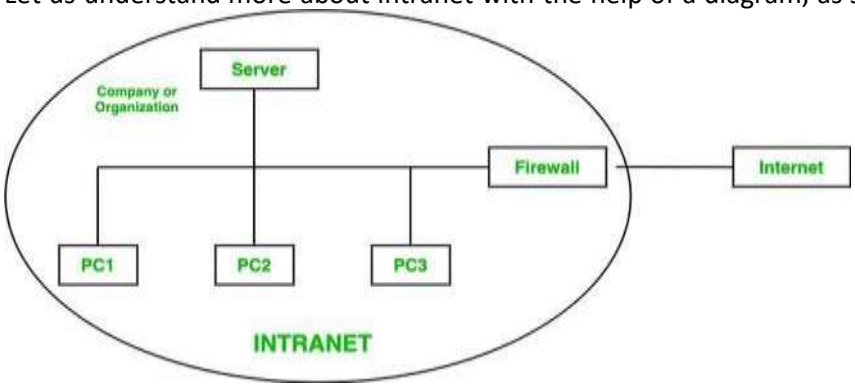
- Using social media and content sharing.
- Instant messaging, video conferencing, Internet Relay Chat (IRC), Internet telephony, and email are all examples of electronic communication. These all are used through the Internet.
- Access to online degree programs, courses, and workshops for education and self-improvement.
- Searching for jobs: To advertise available positions, submit job applications, and hire candidates identified on social networking sites like LinkedIn, both employers and applicants use the Internet.

Applications of Internet:

- **Download programs and files**
- To send and receive E-Mails
- Voice and video Conferencing
- E-Commerce
- File sharing
- Browsing various types of Information
- Search the web addresses for access through the search engine and chatting

Intranet

- Intranet is a kind of private network. For example, an intranet is used by different organizations and only members/staff of that organization have access to this. It is a system in which multiple PCs of an organization (or the PCs you want to connect) are connected to each other through intranet. As this is a private network, so no one from the outside world can access this network. So many organizations and companies have their own intranet network and only its members and staff have access to this network. This is also used to protect your data and provide data security to a particular organization, as it is a private network and does not leak data to the outside world.
- Let us understand more about intranet with the help of a diagram, as shown below:



- Here in this diagram, a company or an organization has created its own private network or intranet for its work(intranet network is under the circle). The company or organization has many employees(in this diagram, we have considered 3). So, for their access, they have PC 1, PC 2, and PC 3(In the real world there are many employees as per the requirements of an organization). Also, they have their own server for files or data to store, and to protect this private network, there is a Firewall. This firewall protects and gives security to the intranet server and its data from getting leaked to any unwanted user. So, a user who has access to the intranet can only access this network. So, no one

from the outside world can access this network. Also, an intranet user can access the internet but a person using the internet cannot access the intranet network.

Applications of Intranet

- Sharing the detail of company rules/policies & regulations
- Access employee database
- Access product & customer data
- Sharing some common information
- Intranet also use for launching personal or department-specific home pages
- Submission of reports
- Corporate telephone directories

Advantages of Intranet

- Fast, easy, low-cost to implement
- Based on open standards
- Allows connectivity with other systems
- Access to internal and external information
- Improves communication

Disadvantages of Intranet

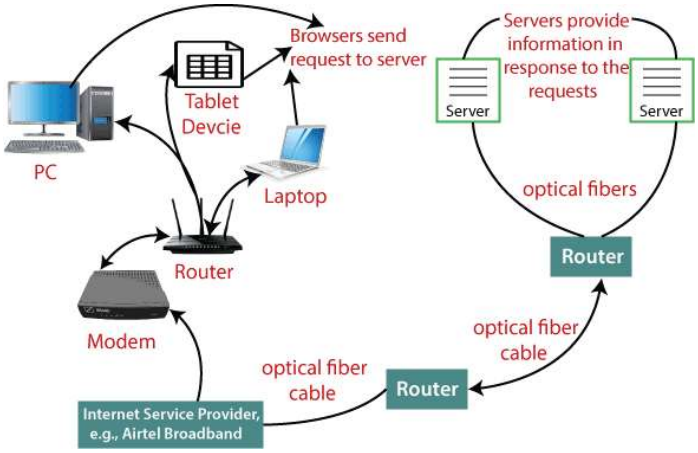
- the loss of control
- Unauthorized access
- Limited bandwidth for the business
- Information overload lowers productivity
- Hidden or unknown complexity and costs

2.1.1 Working of Internet and its architecture

How does internet work?

- The internet works with the help of clients and servers. A device such as a laptop, which is connected to the internet is called a client, not a server as it is not directly connected to the internet. However, it is indirectly connected to the internet through an Internet Service Provider (ISP) and is identified by an IP address, which is a string of numbers. Just like you have an address for your home that uniquely identifies your home, an IP address acts as the shipping address of your device. The IP address is provided by your ISP, and you can see what IP address your ISP has given to your system.
- A server is a large computer that stores websites. It also has an IP address. A place where a large number of servers are stored is called a data center. The server accepts requests send by the client through a browser over a network (internet) and responds accordingly.
- To access the internet we need a domain name, which represents an IP address number, i.e., each IP address has been assigned a domain name. For example, youtube.com, facebook.com, paypal.com are used to represent the IP addresses. Domain names are created as it is difficult for a person to remember a long string of numbers. However, internet does not understand the domain name, it understands the IP address, so when you enter the domain name in the browser search bar, the internet has to get the IP addresses of this domain name from a huge phone book, which is known as DNS (Domain Name Server).
- For example, if you have a person's name, you can find his phone number in a phone book by searching his name. The internet uses the DNS server in the same way to find the IP address of the domain name. DNS servers are managed by ISPs or similar organizations.

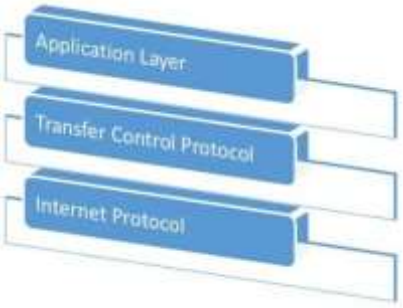
Now after understanding the basics, let us see how internet works?



Internet Architecture

internet architecture is a meta-network, which refers to a congregation of thousands of distinct networks interacting with a common protocol. In simple terms, it is referred as an internetwork that is connected using protocols. Protocol used is TCP/IP. This protocol connects any two networks that differ in hardware, software and design.

- **Process**
- TCP/IP provides end to end transmission, i.e., each and every node on one network has the ability to communicate with any other node on the network.
- **Layers of Internet Architecture**
- Internet architecture consists of three layers −



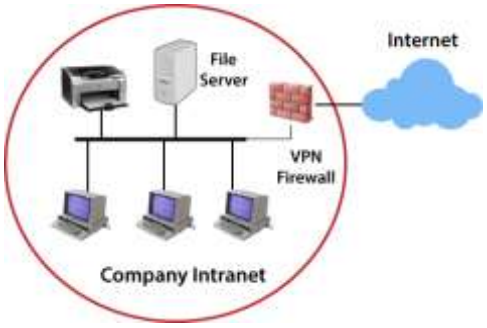
The three layers of internet

- **IP**
- In order to communicate, we need our data to be encapsulated as Internet Protocol (IP) packets. These IP packets travel across number of hosts in a network through routing to reach the destination. However IP does not support error detection and error recovery, and is incapable of detecting loss of packets.
- **TCP**
- TCP stands for "Transmission Control Protocol". It provides end to end transmission of data, i.e., from source to destination. It is a very complex protocol as it supports recovery of lost packets.
- **Application Protocol**
- Third layer in internet architecture is the application layer which has different protocols on which the internet services are built. Some of the examples of internet services include email (SMTP facilitates email feature), file transfer (FTP facilitates file transfer feature), etc.

2.1.2 Working of Intranet and its architecture

How the Intranet Works:

- Intranet basically comprises three components: a web server, an intranet platform, and applications. The web server is hardware that contains all the intranet software and data. It manages all requests for files hosted over the server and finds the requested files and then delivers it to the user's computer.

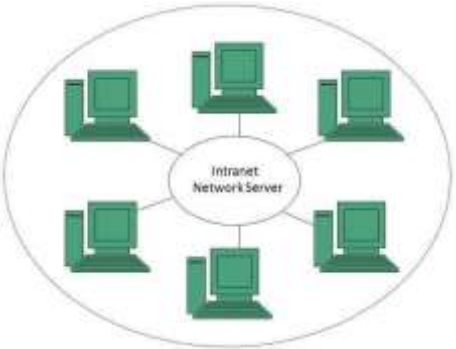


- The intranet platform, which is software, allows communication tools, collaboration apps, and databases to work seamlessly with each other. It is tailored to the specific needs of a business.
- The applications are required to enable users to work smoothly. They are the computing tools that allow users to do their work, communicate, and coordinate with each other and retrieve and store information.
- Furthermore, the user who wants to access the intranet is required to have a special network password and should be connected to the LAN. A user who is working remotely can gain access to the intranet through a virtual private network (VPN) that allows them to sign in to the intranet to access the information.

Intranet architecture

Intranet is defined as private network of computers within an organization with its own server and firewall. Moreover we can define Intranet as:

- Intranet is system in which multiple PCs are networked to be connected to each other. PCs in intranet are not available to the world outside of the intranet.
- Usually each company or organization has their own Intranet network and members/employees of that company can access the computers in their intranet.
- Every computer in internet is identified by a unique IP address.
- Each computer in Intranet is also identified by a IP Address, which is unique among the computers in that Intranet.



2.1.3 Network Devices terminologies: Hub, modem, switch, Routers, Gateways, Access point

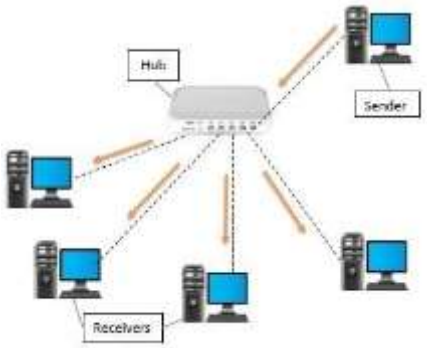
What are network devices?

- Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another.

Network devices types:

Hubs

- A hub is a physical layer networking device which is used to connect multiple devices in a network. They are generally used to connect computers in a LAN.
- Hub is a networking device that operates on the physical layer i.e. the 1st layer of the OSI model, unlike switches that operate in data link layer. Hub connect multiple devices to itself that send and receive data through it. It is a multiport repeater that comes with add-on functionalities, such as indicating any issues with the device. They come in different variants such as 4, 8, and 16 port hubs.
- Hub works as a central connection among all network equipment and handles a data type called frames. It is connected to multiple devices that allow forwarding. Any data coming from one of the connected devices in the hub can be forwarded to another connected device.
- A hub is one of the simplest networking devices that connects several computers or other network devices when referring to networking (network devices hub).
- ***a hub is a hardware device that allows multiple devices or connections to connect to a computer.***
- A USB hub, for example, allows multiple USB devices to connect with one computer, even if that computer only has one USB connection. Depending on the hub, the number of ports on a USB hub can range from 4 to over 100



There are mainly three types of hub in computer network

- **Passive Hub:**
  A passive hub is a basic hub that simply provides a physical connection between multiple devices. It does not require any external power source and operates using the power provided by the devices that are connected to it. Passive hubs typically have a limited number of ports and are used in small-scale networks.
- **Active Hub:**
  An active hub, also known as a powered hub, is a hub that requires an external power source to operate. It contains active electronic components that amplify and regenerate signals, which allows it to extend the distance over which devices can communicate with each other.

- **Intelligent Hub:**
  An intelligent hub is a type of hub that includes additional features such as network management capabilities, error detection, and troubleshooting tools. This type of hub is also known as a managed hub.

The top three advantages of the hub network device are:

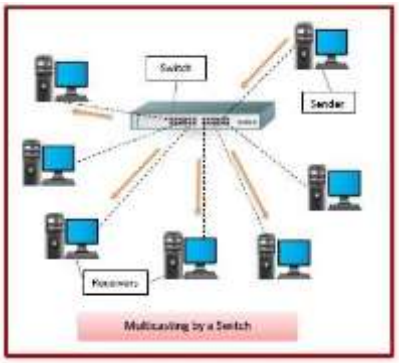
- Easy to install
- Inexpensive
- It does not affect the performance of the network seriously

The top three disadvantages of the hub network device are:

- Can not filter information
- It can not reduce the network traffic
- Broadcast of the data happens to all the port

Switches:

- Switches are networking devices operating at **layer 2 or a data link layer of the OSI model**.
- They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.
- A switch has many ports, to which computers are plugged in.
- When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s).
- It supports unicast, multicast as well as broadcast communications.



Features of Switches

- A switch operates in the layer 2, i.e. data link layer of the OSI model.
- It is an intelligent network device that can be conceived as a multiport network bridge.
- It uses MAC addresses (addresses of medium access control sublayer) to send data packets to selected destination ports.
- It uses packet switching technique to receive and forward data packets from the source to the destination device.
- It is supports unicast (one-to-one), multicast (one-to-many) and broadcast (one-to-all) communications.
- Transmission mode is full duplex, i.e. communication in the channel occurs in both the directions at the same time. Due to this, collisions do not occur.
- Switches are active devices, equipped with network software and network management capabilities.
- Switches can perform some error checking before forwarding data to the destined port.
- The number of ports is higher – 24/48.

Types of Switches

There are variety of switches that can be broadly categorised into 4 types −

- **Unmanaged Switch** − These are inexpensive switches commonly used in home networks and small businesses. They can be set up by simply plugging in to the network, after which they instantly start operating. When more devices needs to be added, more switches are simply added by this plug and play method. They are referred to as u managed since they do not require to be configured or monitored.
- **Managed Switch** − These are costly switches that are used in organisations with large and complex networks, since they can be customized to augment the functionalities of a standard switch. The augmented features may be QoS (Quality of Service) like higher security levels, better precision control and complete network management. Despite their cost, they are preferred in growing organizations due to their scalability and flexibility. Simple Network Management Protocol (SNMP) is used for configuring managed switches.
- **LAN Switch** − Local Area Network (LAN) switches connects devices in the internal LAN of an organization. They are also referred as Ethernet switches or data switches. These switches are particularly helpful in reducing network congestion or bottlenecks. They allocate bandwidth in a manner so that there is no overlapping of data packets in a network.
- **PoE Switch** − Power over Ethernet (PoE) switches are used in PoE Gogabit Ethernets. PoE technology combine data and power transmission over the same cable so that devices connected to it can receive both electricity as well as data over the same line. PoE switches offer greater flexibility and simplifies the cabling connections

The top three advantages of the switch network device are:

- Increases the available bandwidth of the network.
- It helps in reducing the workload on individual host PCs
- Increases the performance of the network

The top three disadvantages of the switch network device are:

- They are more costly than network bridges.
- Broadcast traffic can be problematic.
- Network connectivity problems are challenging to track down via the network switch.

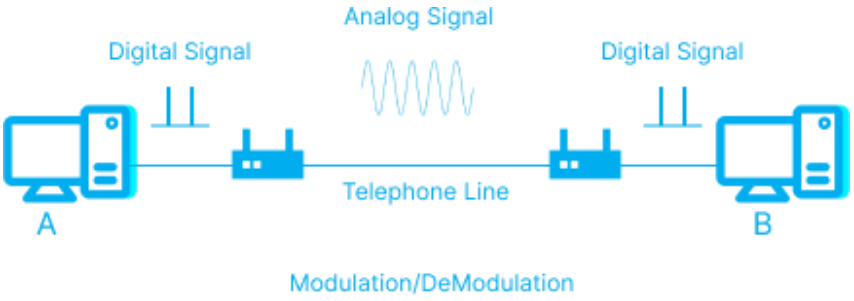
Modem(modulator- demodulator)

What is Modem in Computer Network?

- A modem is an electronic device that converts digital signals into analog signals and also vice-versa.
- It is used to transmit data over communication channels such as telephone lines, cable lines, or wireless networks.
- The modem is capable of encoding and decoding digital signals so that they can be transmitted through the communication channel.
- When the analog signal reaches the receiving modem, it decodes it back into digital signals that can be read by the computer or digital device.
- **Modems work on both the Physical and Data Link layers.**

Working of Modem in Computer Network

- A modem works by converting digital signals into analog signals and vice versa.
- The modem consists of two main components: the modulator and the demodulator. The modulator is responsible for converting digital signals into analog signals,.
- while the demodulator is responsible for converting analog signals into digital signals.



When a user sends data from the computer, the modem converts the digital signals into analog signals that can be transmitted over the communication channel. The modem sends the analog signal over the telephone line, cable line, or wireless network to the receiving modem. The receiving modem then decodes the analog signal back into digital signals that can be read by the computer or digital device.

Characteristics of Modem in Computer Network

- Modems are used to convert digital signals to analog signals.
- They help in the connection of devices to the internet.
- A modem can only connect a limited number of systems to the internet.
- Modems are susceptible to computer hacking, limiting the possibility of secure transmission.
- The cost of a modem is determined by the number of features it provides. Additional features will increase the cost of the modem.
- When a modem is linked to a hub, it slows down.
- They cannot monitor communication between the LAN and the internet.
- To communicate with telephone lines, modems require an RJ11 jack and an RJ45 jack to connect to computers.
- Device drives must be installed in the operating system for modem configuration and communication.

Types of Modem in Computer Network

- **External Modem**
  External Modem in Computer System is connected to the computer system with the help of a serial cable. It's also extremely simple to install and has a fast data transfer rate. It is expensive, but it is still used in workplaces due to its high-speed data transfer, mostly to avoid interruptions in network access.
- **Internal Modem**
  As the name implies, The internal modem is installed over the motherboard of a computer. It looks similar to an electronic circuit and it is installed in the motherboard slot. Due to the complexity of the installation process and the slow data transfer speed, it is used for dedicated computers in houses or small spaces.
- **Wireless Modem**
  Wireless modems connect to computer systems without the requirement of a cable, and most people use wireless modems for personal usage.

These modems use radio frequencies to send data over the air and have a fast transmission speed.

- **Dial-Up Modem**
  Dial-up modems link the computer to the internet by connecting the ISP over a traditional telephone line. It uses the PSTN (Public Switched Telephone Network). The speed is 56kb/sec.
- **Cable Modem**
  The cable modem is referred to as a broadband device as it enables the computer to communicate with the ISP via a landline connection. It is connected to the landline via a coaxial wire and to the computer via an ethernet cable.
- **DSL Modem**
  DSL is an abbreviation for Digital Subscriber Line, which allows data transmission over a standard telephone line. It has a fast data transfer speed and is thus widely used in businesses and residences. It may be used to connect to a computer or router to provide internet access through the ethernet or USB port.
- **Satellite Modem**
  Satellite modems are expensive modems that do not require a phone line to connect to the internet. It uses satellite technology to send or receive data.
- **Half-Duplex Modem**
  As the name implies, it only permits data to be transmitted in one direction at a time which means that if it is getting the signal from one end, it will stop receiving the signal from the other end. After one end's transmission has finished, only the other end can communicate data.
- **Full Duplex Modem**
  Full-duplex modems can send data from both ends simultaneously. It means that it can receive data from both ends simultaneously and without interruption.

Advantages of Modem in Computer Network

- **Easy to install:** Modems are easy to install and set up. Most modems come with easy-to-follow instructions, and they can be installed in a matter of minutes.
- **Cost-effective:** Modems are cost-effective compared to other networking devices such as routers, switches, and hubs.
- **Compatibility:** Modems are compatible with a wide range of digital devices such as computers, laptops, tablets, and smartphones.
- **Access to the Internet:** Modems provide access to the Internet, which is essential for most businesses and individuals.

Disadvantages of Modem in Computer Network

- **Slow Speeds:** Some types of modems, such as dial-up modems, are very slow and cannot transmit data at high speeds.
- **Limited Range:** Some types of modems, such as wireless modems, have a limited range and may not be able to transmit data over long distances.
- **Security Concerns:** Modems may be vulnerable to security threats such as hacking and malware attacks. It is important to take necessary precautions to protect your modem and network from such threats.
- **Dependence on Service Provider:** Modems are dependent on the internet service provider (ISP) for internet connectivity. If the ISP experiences any issues or downtime, it may affect the modem's ability to connect to the internet.

The top three advantages of the modem network device are:

- Easily allows connecting LAN to internet
- Converts digital signal into an analog signal

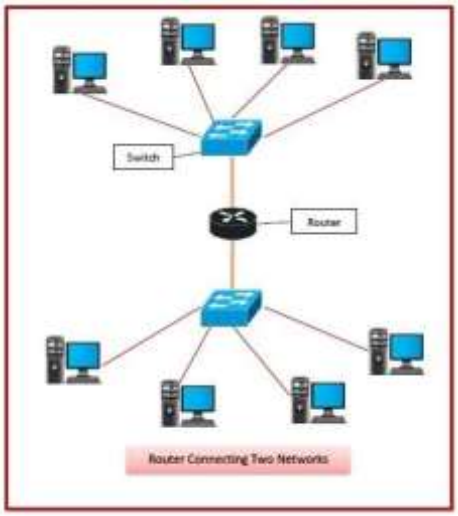
- When compared to the hub, the speed is slow

The top three disadvantages of the modem network device are:

- It only serves as a bridge between the LAN and the internet.
- It cannot maintain its network traffic.
- The modem is unaware of its destination path.

Router

- The router in computer network is a device that is used to connect multiple computer networks together.
- It can be considered the central hub that controls the traffic from each network and directs them according to the requirement.
- The router in computer network works on **the 3rd layer of the OSI model** and uses routing tables to determine the best path for the packet to travel so that it can reach the destination.



Features of Routers

- A router is a layer 3 or network layer device.
- It connects different networks together and sends data packets from one network to another.
- A router can be used both in LANs (Local Area Networks) and WANs (Wide Area Networks).
- It transfers data in the form of IP packets. In order to transmit data, it uses IP address mentioned in the destination field of the IP packet.
- Routers provide protection against broadcast storms.
- Routers are more expensive than other networking devices like hubs,bridges and switches.
- It also allows the devices on private networks to access the public network by using network address translation.

Types of Routers in Computer Networks

- **Wired Routers:** As the name suggests they are connected by wires to different devices of a network and they are the most common types of routers available and used.
- **Wireless Routers:** They can use the wirelessly as mentioned in the name so there is no need to maintain wires for connectivity. They are mainly used in households and small businesses.
- **Edge Routers:** They are mainly used by service providers as they are used to connect the large network to the internet.
- **Core Routers:** They are designed for high-speed data transfer and are mainly used for large networks and because of this they are sometimes referred to as the core of large networks.

The top three advantages of the router network device are:

- Connects various network architectures such as ethernet and token ring, among others.
- Reduces network traffic by establishing collision domains as well as broadcast domains.
- Chooses the best path across the internetwork using dynamic routing algorithms.

The top three disadvantages of the router network device are:

- They work with routable network protocols.
- More expensive than other network devices.
- They are slower because they must analyze data from layer 1 to layer 3.

Gateway

- A gateway is a network node that forms a passage between two networks operating with different transmission protocols.
- The most common type of gateways, the network gateway operates at layer 3, i.e. network layer of the OSI (open systems interconnection) model.
- However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model. It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway.
- Only the internal traffic between the nodes of a LAN does not pass through the gateway.

Features of Gateways

- Gateway is located at the boundary of a network and manages all data that inflows or outflows from that network.
- It forms a passage between two different networks operating with different transmission protocols.

- A gateway operates as a protocol converter, providing compatibility between the different protocols used in the two different networks.
- The feature that differentiates a gateway from other network devices is that it can operate at any layer of the OSI model.
- It also stores information about the routing paths of the communicating networks.
- When used in enterprise scenario, a gateway node may be supplemented as proxy server or firewall.
- A gateway is generally implemented as a node with multiple NICs (network interface cards) connected to different networks. However, it can also be configured using software.
- It uses packet switching technique to transmit data across the networks.

Types of Gateways

- **Unidirectional Gateways** − They allow data to flow in only one direction. Changes made in the source node are replicated in the destination node, but not vice versa. They can be used as archiving tools.
- **Bidirectional Gateways** − They allow data to flow in both directions. They can be used as synchronization tools.

The top three advantages of the gateway network device are:

- Allows to broaden the network
- Handles traffic issues effectively
- Permits to link two different kinds of networks

The top three disadvantages of the gateway network device are:

- Never filter data
- Costly and difficult to manage
- Protocol conversion is performed, thus resulting in a slower transmission rate.

Access Point

- In terms of networking, an access point (AP) is a wireless network device that acts as a portal for devices to connect to a local area network.
- Access points can extend an existing network's wireless coverage and increase the number of users who can connect. Wireless access points (WAPs) are devices that combine a transmitter and receiver (transceiver) to form a wireless LAN (WLAN). The access point ***operates at the OSI model's Data Link layer (Layer 2).***

The top three advantages of the access point network device are:

- Installing is easier and faster.
- Allows data transmission even when the user is moving.
- It is simple to extend to places where wires and cables are inaccessible.

The top three disadvantages of the access point network device are:

- The range of network devices is limited, which causes issues for many users.
- Installing this network device is difficult and time-consuming.

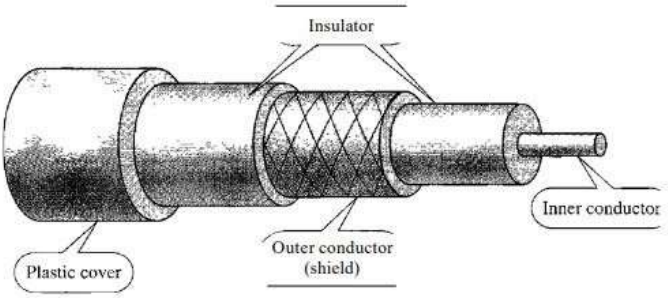
- Because these network devices are susceptible to interference, fog and radiation can cause them to malfunction.

2.2 Types of Cables: co-axial, UTP, Fiber Optic cable

Coaxial Cables

- Coaxial cable (or coax) carries signals of higher frequency ranges than those in twistedpair cable, in part because the two media are constructed quite differently.
- Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two.
- The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating

sheath, and the whole cable is protected by a plastic cover see Figure



- There are two types of coaxial cabling: ThinNet and ThickNet.

1. **ThinNet**
   - ThinNet is a flexible coaxial cable about ¼ inch thick. ThinNet is used for short-distance. ThinNet connects directly to a workstation's network adapter card using a British Naval Connector (BNC). The maximum length of thinnet is 185 to 200 meters.
2. **ThickNet.**
   - ThickNet coaxial cable is thicker cable than ThinNet. ThickNet cable is about ½ inch thick and can support data transfer over longer distances than ThinNet. ThickNet has a maximum supported cable length of 500 meters and usually is used as a backbone to connect several smaller ThinNet-based networks.

- **There are two Ethernet media standards defined for coaxial cable-based Ethernet**.
- **Those standards are**:

1. 10Base2 and
2. 10Base5.

1. **10Base2** has a bandwidth speed of 10 Mbps, to a maximum distance of 200 meters. 10 denotes bandwidth speed and 2 denotes 200 meters. Base denotes baseband type of signal. Coaxial cable used for 10Base2 Ethernet media standard is ThinNet.
2. **10Base5** has a bandwidth speed of 10 Mbps, to a maximum distance of 500 meters. 10 denotes bandwidth speed and 5 denotes 500 meters. Base denotes baseband type of signal. Coaxial cable used for 10Base5 Ethernet media standard is ThickNet.

- The bandwidth available for both 10Base2 (Thinnet Ethernet) and 10Base5 (Thicknet Ethernet) were 10 Mbps (Megabits per second).

Type of Cable used to wire Local Area Networks (LAN) these days is Twisted Pair cable. It is extremely difficult to find a live business network using coaxial cable.

Applications:

• Television distribution
• Cable TV

• Long distance telephone transmission
• Can carry 10,000 voice calls simultaneously
• Short distance computer systems links
• Local area networks
• More expensive than twisted pair, not as popular for LANs

Advantages:

- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive

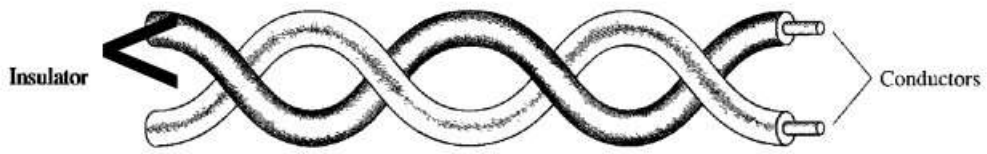
Disadvantages:

- Single cable failure can disrupt the entire network

Twisted Pair Cables

- A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together, as shown in Figure

Figure 7.3 *Twisted-pair cable*



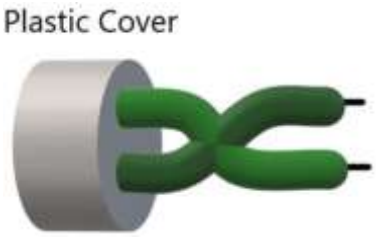
- One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference.
- The receiver uses the difference between the two.
- In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.
- If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources (e,g., one is closer and the other is farther).
- This results in a difference at the receiver
- This means, if two wires are correlated to each other, the noise or crosstalk can affect one wire, and the difference between the two levels would vary. When these wires are twisted, both wires have a similar effect of noise. This way, the receiver receives the correct signal. The number of a twist on the cable defines the quality of signals carried by them.
- Therefore, more twisted means better quality signals..

Two types of twisted pair cables are

a. Unshielded Twisted Pair (UTP)
b. Shielded Twisted Pair (STP).

Unshielded Twisted Pair (UTP) cables

- These are a pair of two insulated copper wires twisted together without any other insulation or shielding and hence are called unshielded twisted pair cables.
- They reduce the external interference due to the presence of insulation. Unshielded twisted pair cables are arranged in pairs so that we can add a new connection whenever required.
- The DSL or telephone lines in our houses have one extra pair in them. When UTP are arranged in pairs, each pair is coded with a different color as defined by the 25-pair color code developed by AT&T Corporation. The Electronic Industries Association divides UTP into 7 categories based on some standards.
- Categories are based upon cable quality where 1 is the highest quality and 7 is the lowest quality. Each cable in a category is put to a different use as needed.



Advantages:

⇢ Least expensive
⇢ Easy to install
⇢ High-speed capacity

Disadvantages:

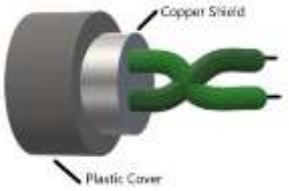
⇢ Susceptible to external interference
⇢ Lower capacity and performance in comparison to STP
⇢ Short distance transmission due to attenuation

Applications:

Used in telephone connections and LAN networks

Shielded Twisted Pair (STP) cables

- These types of cables have extra insulation or protective covering over the conductors in the form of a copper braid covering.
- This covering provides strength to the overall structure of the cable. It also reduces noise and signal interference in the cable.
- The shielding ensures that the induced signal can be returned to the source via ground and only circulate around the shield without affecting the main propagating signal.
- The STP cables are also color-coded like the UTP cables as different color pairs are required for analog and digital transmission.
- These cables are costly and difficult to install.



-

Advantages:

- ⇢ Better performance at a higher data rate in comparison to UTP
- ⇢ Eliminates crosstalk
- ⇢ Comparatively faster

Disadvantages:

- ⇢ Comparatively difficult to install and manufacture
- ⇢ More expensive

Applications:

- The shielded twisted pair type of cable is most frequently used in extremely cold climates, where the additional layer of outer covering makes it perfect for withstanding such temperatures or for shielding the interior components.

Applications of Twisted pair cables :

- Twisted Pair cables are used in telephone lines to provide data and voice channels.
- The DSL lines make use of these cables.
- Local Area Networks (LAN) also make use of twisted pair cables.
- They can be used for both analog and digital transmission.
- RJ-45 is a very common application of twisted pair cables.

Advantages

- Cost-effective
- easy to install
- Performs best over short distance

Disadvantages

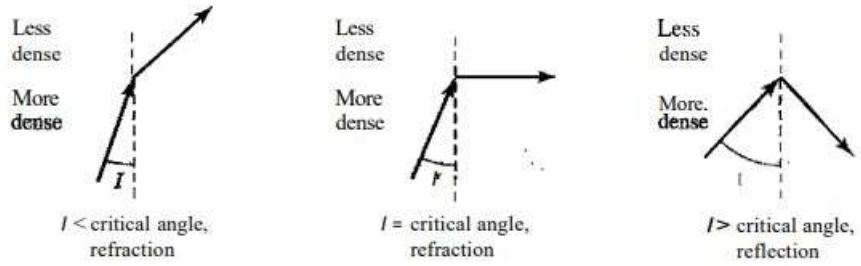
- Lower durability (must be routinely maintained)
- Susceptible to EMI
- Higher attenuation

Shielded Twisted Pair	Unshielded Twisted Pair
STP - Shielded Twisted Pair cable.	UTP - Unshielded Twisted Pair cable.
STP is costlier in price than UTP.	UTP is cheap in price compared with STP.
STP require grounding of cable.	UTP requires no grounding of cable.
STP reduces electromagnetic interference more than UTP	Electromagnetic interference is more in UTP
Low crosstalk in STP	Crosstalk in UTP is more than STP
STP is fast compared with UTP	UTP is slow compared to STP

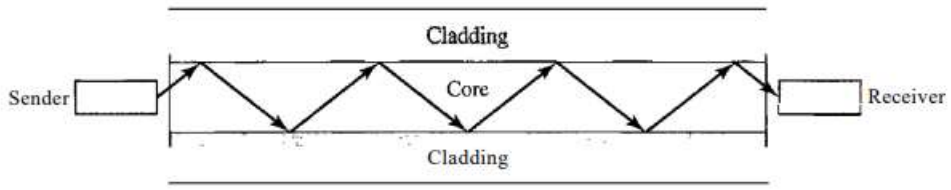
Fiber-Optic Cable

- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- To understand optical fiber, we first need to explore several aspects of the nature of light. Light travels in a straight line as long as it is moving through a single uniform substance.
- If a ray of light traveling through one substance suddenly enters another substance (of a different density), the ray changes direction. Figure shows how a ray of light changes

direction when going from a more dense to a less dense substance.



- As the figure shows, if the angle of incidence I (the argle the ray makes with the line perpendicular to the interface between the two substances) is less than the critical angle, the ray refracts and moves closer to the surface. If the angle of incidence is equal to the critical angle, the light bends along the interface. If the angle is greater than the critical angle, the ray reflects (makes a turn) and travels again in the denser substance. Note that the critical angle is a property of the substance, and its value differs from one substance to another.
- Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it. See Figure



Advantages:

- Increased capacity and bandwidth
- Lightweight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

Disadvantages:

- Difficult to install and maintain
- High cost
- Fragile

Difference Between Twisted pair cable, Co-axial cable, and Optical fiber

Characteristics	UTP	STP	Coaxial Cables	Fiber Optic Cables
Bandwidth	10 Mbps - 100 Mbps	10 Mbps - 100 Mbps	10 Mbps	100 Mbps -1 Gbps
Maximum cable segment	100 meters	100 meters	200 - 500 meters	2 k.m. - 100 k.m.
Interference rating	Poor	Better than UTP	Better than Twisted Pair Cable	Very good as compared to any other cable
Installation cost	Cheap	Costly than UTP	Costlier than twisted pair wires	Costliest to install
Bend radius	360 degrees / feet	360 degrees / feet	360 degrees / feet or 30 degrees / feet	30 degrees / feet
Security	Low	Low	Low	High

Unit-3: Mobile Ad hoc network

3.1 Concepts and types of MANET (Mobile Ad hoc network)
3.1.1 VANET (Vehicular Ad hoc Network)
3.1.2 Smart phone Ad hoc Network (SPANC)
3.1.3 Flying Ad hoc network (FANET)
3.2 concepts of OSI(Open Source Interconnection) layers
3.2.1 types of layers
3.2.2 Introduction of OSI Layers and their purpose: Physical layer, Data link layer and Network Layer Transport layer and Session Layer.

3.1 Concepts and types of MANET (Mobile Ad hoc network)

Introduction of Mobile Ad hoc Network (MANET)

MANET stands for Mobile Adhoc Network also called a wireless Adhoc network or Adhoc wireless network that usually has a routable networking environment on top of a Link Layer ad hoc network.. They consist of a set of mobile nodes connected wirelessly in a self-configured, self-healing network without having a fixed infrastructure. MANET nodes are free to move randomly as the network topology changes frequently. Each node behaves as a router as they forward traffic to other specified nodes in the network.

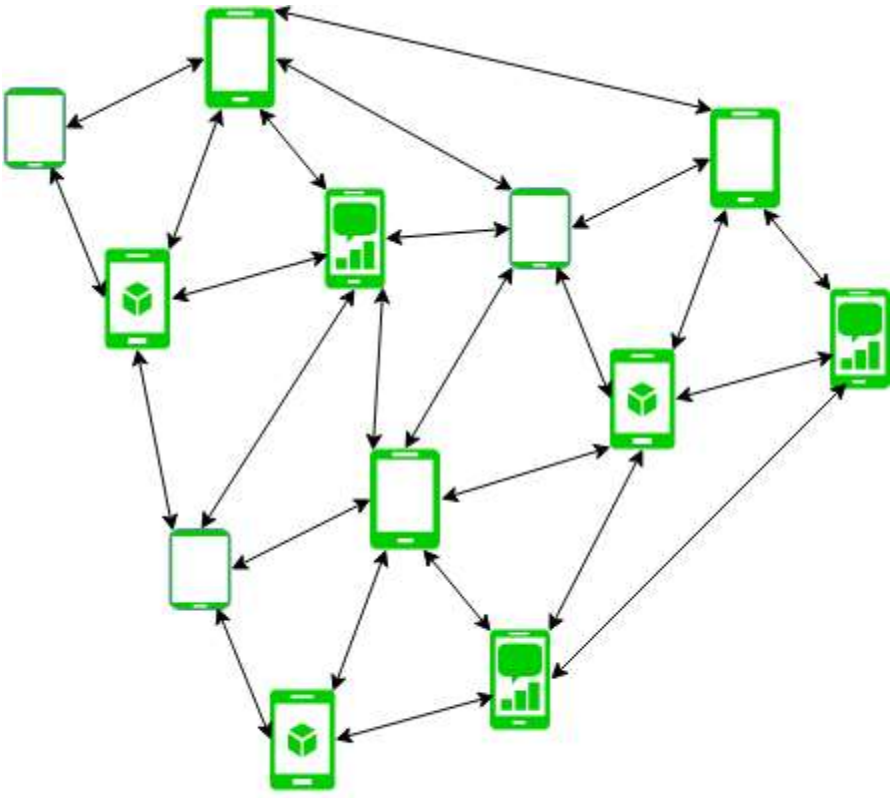


Figure - Mobile Ad Hoc Network

MANET may operate a standalone fashion or they can be part of larger internet. They form a highly dynamic autonomous topology with the presence of one or multiple different transceivers between nodes. The main challenge for the MANET is to equip each device to continuously maintain the information required to properly route traffic. MANETs consist of a peer-to-peer, self-forming, self-healing network MANET's circa 2000-2015 typically communicate at radio frequencies (30MHz-5GHz). This can be used in road safety, ranging from sensors for the environment, home, health, disaster rescue operations, air/land/navy defense, weapons, robots, etc.

Characteristics of MANET –

- **Dynamic Topologies:**
  Network topology which is typically multihop may change randomly and rapidly with time, it can form unidirectional or bi-directional links.
- **Bandwidth constrained, variable capacity links:**
  Wireless links usually have lower reliability, efficiency, stability, and capacity as compared to a wired network
- **Autonomous Behavior:**
  Each node can act as a host and router, which shows its autonomous behavior.
- **Energy Constrained Operation:**
  As some or all the nodes rely on batteries or other exhaustible means for their energy. Mobile nodes are characterized by less memory, power, and lightweight features.
- **Limited Security:**
  Wireless networks are more prone to security threats. A centralized firewall is absent due to the distributed nature of the operation for security, routing, and host configuration.
- **Less Human Intervention:**
  They require minimum human intervention to configure the network, therefore they are dynamically autonomous in nature.

Advantages:

Flexibility: MANETs are highly flexible, as they can be easily deployed in various environments and can be adapted to different applications and scenarios. This makes them ideal for use in emergency situations or military operations, where there may not be a pre-existing network infrastructure.

Scalability: MANETs can easily scale to accommodate a large number of nodes, making them suitable for large-scale deployments. They can also handle dynamic changes in network topology, such as the addition or removal of nodes.

Cost-effective: Since MANETs do not require any centralized infrastructure, they are often more cost-effective than traditional wired or wireless networks. They can also be used to extend the range of existing networks without the need for additional infrastructure.

Rapid Deployment: MANETs can be rapidly deployed in areas where infrastructure is not available, such as disaster zones or rural areas.

Disadvantages:

Security: MANETs are vulnerable to security threats, such as attacks by malicious nodes, eavesdropping, and data interception. Since the network is decentralized, there is no central authority to ensure the security of the network.

Reliability: MANETs are less reliable than traditional networks, as they are subject to interference, signal attenuation, and other environmental factors that can affect the quality of the connection.

Bandwidth: Since MANETs rely on wireless communication, bandwidth can be limited. This can lead to congestion and delays, particularly when multiple nodes are competing for the same channel.

Routing: Routing in MANETs can be complex, particularly when dealing with dynamic network topologies. This can result in inefficient routing and longer delays in data transmission.

Power Consumption: Since MANETs rely on battery-powered devices, power consumption can be a significant issue. Nodes may need to conserve power to extend the life of the battery, which can limit the amount of data that can be transmitted.

3.1.1 VANET (Vehicular Ad hoc Network)

Enable effective communication with another vehicle or with the roadside equipments. Intelligent vehicular ad hoc networks(InVANETs) deals with another vehicle or with roadside equipment. VANETs use wireless communication technologies, such as WIFI or cellular, to enable vehicles to communicate with each other and with infrastructure devices, such as traffic lights or road-side units.

Uses: VANETs can be used to support a wide range of applications, such as:

- **Intelligent Transportation Systems (ITS):** VANETs can be used to improve traffic flow and reduce congestion by providing real-time traffic information and routing advice to drivers.
- **Road Safety:** VANETs can be used to improve road safety by providing information about the location of other vehicles, road conditions, and potential hazards.
- **Entertainment and infotainment:** providing in-vehicle entertainment and internet access to the passengers
- **Emergency Services:** VANETs can be used to support emergency services by providing real-time information about accidents or other incidents on the road.
- **Commercial Services:** VANETs can be used for commercial services such as providing location-based advertisement and other location-based service to the driver or passengers.

  VANETs are considered as one of the most critical application of the Internet of Things (IoT) technology and the 5G technology.

Advantages:

- Improves traffic flow and reduces congestion.
- Enhances road safety by providing real-time information about road conditions, potential hazards, and the location of other vehicles.
- Enables in-vehicle entertainment and internet access to passengers.
- Supports emergency services by providing real-time information about accidents or other incidents on the road.
- Provides location-based advertising and other services to the driver or passengers.

Disadvantages:

- Vulnerable to attacks and security breaches.
- Requires a large number of vehicles to form an effective network.
- Limited coverage area, as VANETs rely on wireless communication technologies such as Wi-Fi or cellular.

3.1.2 Smart phone Ad hoc Network (SPANC)

To create peer-to-peer networks without relying on cellular carrier networks, wireless access points, or traditional network infrastructure. Here peers can join or leave the network without destroying it. ad-hoc network that utilizes smartphones as the primary nodes for communication. In SPANC, smartphones can act as both routers and hosts, creating a decentralized network without the need for a central infrastructure. This allows for increased flexibility and scalability in wireless communication, especially in emergency or disaster scenarios where traditional communication infrastructure may be unavailable. Some examples of SPANC applications include disaster response, search and rescue, and urban crowd management.

Uses: Smart Phone Ad hoc Network (SPANC) can be used for a variety of applications, including:

- **Emergency communication:** In the event of a natural disaster or other emergency, SPANCs can be used to establish a communication network quickly, allowing people to contact emergency services or stay in touch with loved ones.
- **Remote areas:** SPANCs can be useful in remote areas where traditional wireless networks are not available, such as rural communities or wilderness areas.
- **Event networking:** SPANCs can be used to create a temporary network for events or gatherings, allowing attendees to communicate and share information.
- **Military and emergency services:** SPANCs can be used by military and emergency services to establish a quick and reliable communication network in the field.
- **Content sharing:** SPANCs can be used to share various types of content such as pictures and videos, as well as other forms of multimedia.
- **Research and Development:** SPANCs can be used in various research and development projects such as security, routing, and energy consumption.
- **Crowdsourcing:** SPANCs can be used to gather data from a large group of people, such as in a survey or study.
- **Advertising and marketing:** SPANCs can be used to deliver targeted advertising and marketing messages to a specific group of people.

Advantages:

- Enables communication without relying on traditional network infrastructure or wireless access points.
- Provides a decentralized network without the need for a central infrastructure.
- Useful in emergency or disaster scenarios where traditional communication infrastructure may be unavailable.
- Can be used to establish a communication network quickly in the event of a natural disaster or other emergency.

Disadvantages:

- Limited coverage area, as SPANCs rely on the range of smartphone Wi-Fi capabilities.
- Requires a large number of smartphones to form an effective network.
- Vulnerable to attacks and security breaches.

3.1.3 Flying Ad hoc network (FANET)

This is composed of unmanned aerial vehicles (commonly known as drones). Provides links to remote areas and mobility. Flying Ad-hoc Networks (FANETs) are a specialized type of mobile ad-hoc network that are designed specifically for use in aerial vehicles, such as drones, UAVs, and UGVs. They enable communication and coordination among a group of flying vehicles in a decentralized and self-organizing manner.

FANETs provide a flexible and reliable communication infrastructure for aerial vehicles, allowing for real-time data collection and transmission, as well as navigation and control. They can operate in a standalone mode or can be connected to other networks, such as satellite or cellular networks, to provide extended communication capabilities.

Uses: FANETs have several potential uses in various fields such as:

- **Military and defense:** FANETs can be used for reconnaissance, surveillance, and intelligence gathering, as well as for communication and coordination among military personnel and units.
- **Emergency response:** FANETs can be used to provide communication and coordination among emergency responders in the field, enabling effective response to natural disasters or other emergency situations.
- **Civil aviation:** FANETs can be used for air traffic management and control, as well as for communication and coordination among commercial and private aircraft.
- **Environmental monitoring:** FANETs can be used to collect and transmit data for environmental monitoring and research, such as for monitoring air and water quality, or for monitoring wildlife populations.
- **Agriculture:** FANETs can be used for precision agriculture, such as for monitoring crop health and for controlling crop-dusting drones.
- **Search and Rescue:** FANETs can be used to provide communication and coordination among search and rescue teams, enabling efficient and effective search and rescue operations.
- **Infrastructure inspection:** FANETs can be used for inspecting and monitoring large-scale infrastructure, such as bridges, buildings, and power lines.
- **Media and Entertainment:** FANETs can be used for live streaming and for capturing high-quality video and images for use in media and entertainment.

Advantages:

- Provides flexibility and mobility as the network can be set up and moved quickly.
- Suitable for disaster response, search and rescue operations, and remote sensing applications.
- Can cover large areas with minimal infrastructure requirements.
- Can operate in harsh environments where traditional communication infrastructure is not available.

Disadvantages:

- Limited endurance of the flying platforms.
- Communication range is affected by weather conditions.
- Lack of standardization in FANETs technology.
- Difficult to maintain and manage due to the dynamic nature of the network.

The OSI Model

- An Open Systems Interconnection (OSI) Model is a set of protocols that allows any two different systemsto communicate regardless of their underlying architecture.
- The purpose of the OSI Model is to show howto facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.
- The OSI Model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.
- The OSI model is a layered framework for the design of network systems that allows communication between all types of computersystems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.

Seven layers of the OSI model

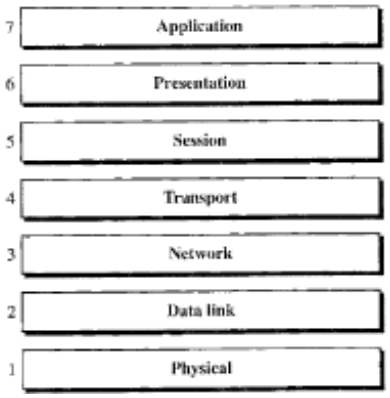
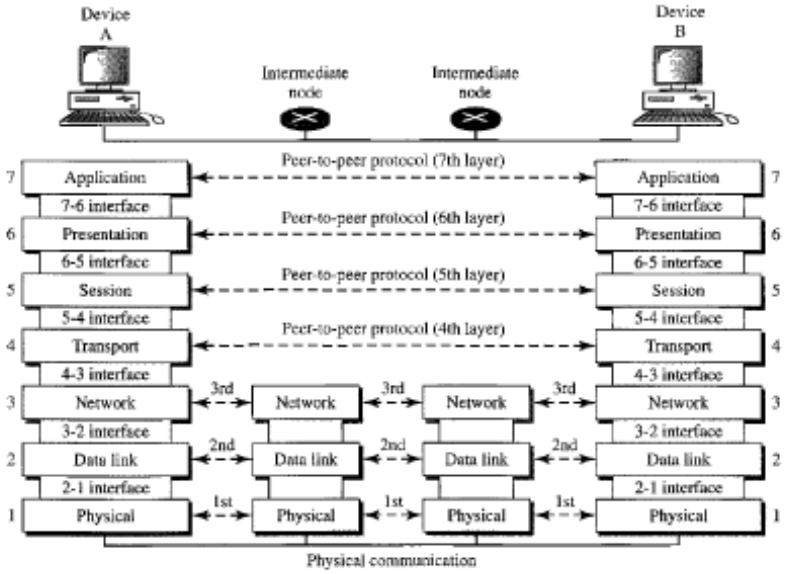
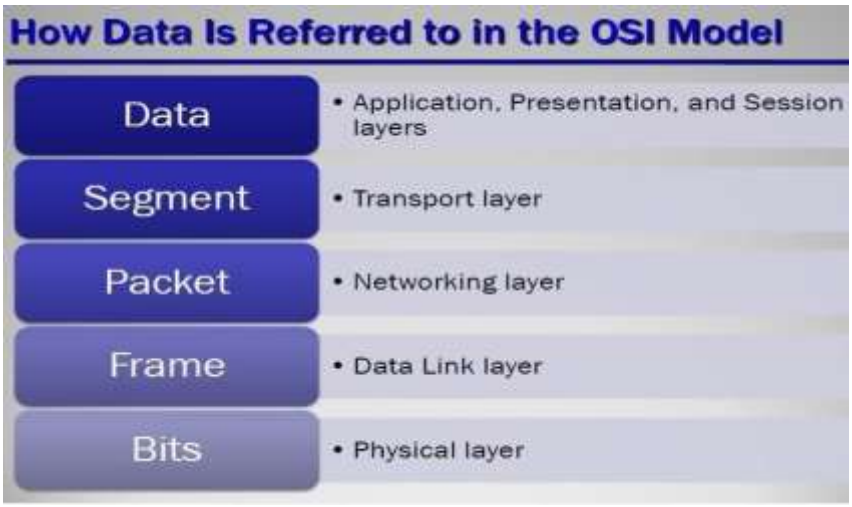
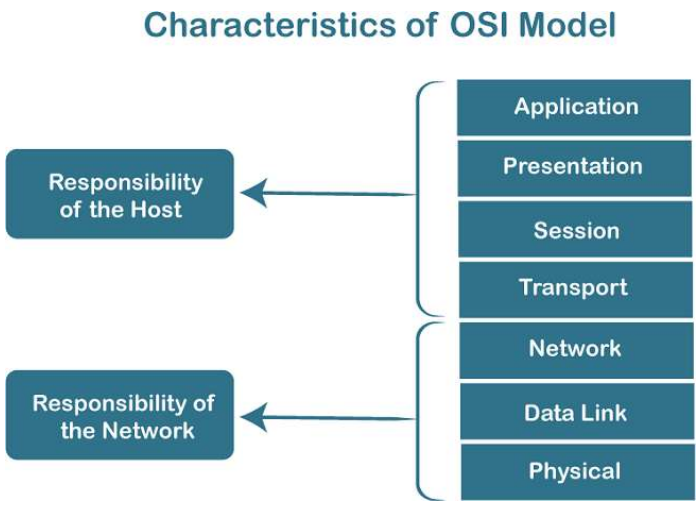


Figure 2.3 *The interaction between layers in the OSI model*



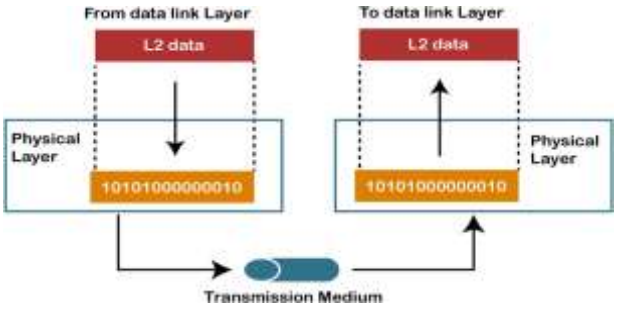


Characteristics of OSI Model:



- The OSI model is divided into two layers: upper layers and lower layers.
- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical m

Physical Layer:



The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.
The physical layer is also concerned with the following:

- **Physical characteristics of interfaces and medium**. The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.
- **Representation of bits**. The physical layer data consists of a stream of bits (sequence of 0s or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical oroptical. The physical layer defines the type of encoding.
- **Data rate**. The transmission rate-the number of bits sent each second-is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.
- **Synchronization of bits**. The sender and receiver not only must use the same bit rate but alsomust be synchronized at the bit level. In other words, the sender and the receiver clocks mustbe synchronized.
- **Line configuration**. The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link.In a multipoint configuration, a link is shared among several devices.
- **Physical topology**. The physical topology defines how devices are connected to make a network. Devices can be connected by using a mesh topology (every device is connected to every other device), a star topology (devices are connected through a central device), a ring topology (each device is connected to the next, forming a ring), a bus topology (every deviceis on a common link), or a hybrid topology (this is a combination of two or more topologies).
- **Transmission mode**. The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex. In simplex mode, only one device can send;the other can only receive. The simplex mode is a one-way communication. In the half-duplexmode, two devices can send and receive, but not at the same time. In a full-duplex (or simplyduplex) mode, two devices can send and receive at the same time.

2. Data Link Layer

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer).

Other responsibilities of the data link layer include the following:

- **Framing**. The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
- **Physical addressing**. If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is theaddress of the device that connects the network to the next one.
- **Flow control**. If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
- **Error control**. The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize

  duplicate frames. Error control is normally achieved through a trailer added to the end of theframe.
- **Access control**. When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

3. Network Layer

The network layer is responsible for the source-to-destination delivery of a packet, possibly acrossmultiple networks (links). Whereas the data link layer oversees the delivery of the packet betweentwo systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination. If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery.

Other responsibilities of the network layer include the following:

- **Logical addressing**. The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layeradds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.
- **Routing**. When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches)route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

4. Transport Layer

The transport layer is responsible for process-to-process delivery of the entire message. A processis an application program running on a host. Whereas the network layer oversees source-to- destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to- destination level.

Other responsibilities of the transport layer include the following:

- **Service-point addressing**. Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process(running program) on the other. The transport layer header must therefore include a type of address called a service-point address (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.
- **Segmentation and reassembly**. A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replacepackets that were lost in transmission.
- **Connection control**. The transport layer can be either connectionless or connection oriented.A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection-oriented transport layer makes a connection with the transport layer at the destination machine first before deliveringthe packets. After all the data are transferred, the connection is terminated.
- **Flow control**. Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.
- **Error control**. Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to-process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

5. Session Layer

The services provided by the first three layers (physical, data link, and network) are not sufficientfor some processes. The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems.

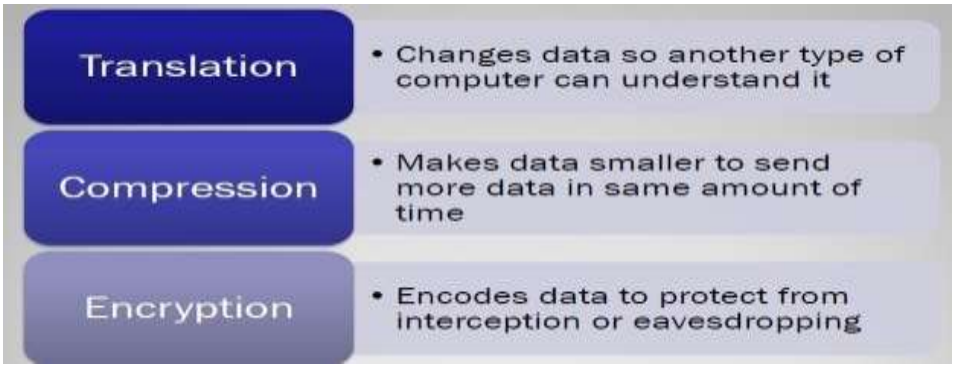
Specific responsibilities of the session layer include the following:

- **Dialog control.** The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half

duplex (one way at a time)or full-duplex (two ways at a time) mode.

- **Synchronization**. The session layer allows a process to add checkpoints, or synchronization points, to a stream of data.

6.Presentation Laye: The presentation layer is concerned with the syntax and semantics of the information exchangedbetween two systems.



Specific responsibilities of the presentation layer include the following:

- **Translation**. The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.
- **Encryption**. To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.
- **Compression.** Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such astext, audio, and video.

6. Application Layer

The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

Specific services provided by the application layer include the following:

- **Network virtual terminal.** A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.
- **File transfer, access, and management.** This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for usein the local computer, and to manage or control files in a remote computer locally.
- **Mail services.** This application provides the basis for e-mail forwarding and

storage.

- **Directory services**. This application provides distributed database sources and access for global information about various objects and services.