Computer Communications and Networks
Course code:21BCA3C9L

UNIT 1 : INTRODUCTION TO COMPUTER NETWORKS

NETWORKS

A 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 and/or receiving data generated by other nodes on the network.

"Computer network" to mean a collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they are able to exchange information. The connection need not be via a copper wire; fiber optics, microwaves, infrared, and communication satellites can also be used.

Networks come in many sizes, shapes and forms, as we will see later. They are usually connected together to make larger networks, with the Internet being the most well-known example of a network of networks. There is considerable confusion in the literature between a computer network and a distributed system.

The key distinction is that in a distributed system, a collection of independent computers appears to its users as a single coherent system. Usually, it has a single model or paradigm that it presents to the users. Often a layer of software on top of the operating system, called middleware, is responsible for implementing this model. A well-known example of a distributed system is the World Wide Web. It runs on top of the Internet and presents a model in which everything looks like a document (Web page).

USES OF COMPUTER NETWORKS

1. Business Applications
   - to distribute information throughout the company (resource sharing). sharing physical resources such as printers, and tape backup systems, is sharing information
   - client-server model. It is widely used and forms the basis of much network usage.
   - communication medium among employees. email (electronic mail), which employees generally use for a great deal of daily communication.

- Telephone calls between employees may be carried by the computer network instead of by the phone company.
- Desktop sharing lets remote workers see and interact with a graphical computer screen
- doing business electronically, especially with customers and suppliers. This new model is called e-commerce (electronic commerce) and it has grown rapidly in recent years.

2. Home Applications
   - peer-to-peer communication
   - person-to-person communication
   - electronic commerce
   - entertainment.(game playing)
   - Online reservations for trains , hotels , airplanes etc
   - Online banking and shopping
   - Online personalized electronic newspapers , journals and libraries.
   - Access to WWW(world wide web)

3. <u>Mobile Users:</u>

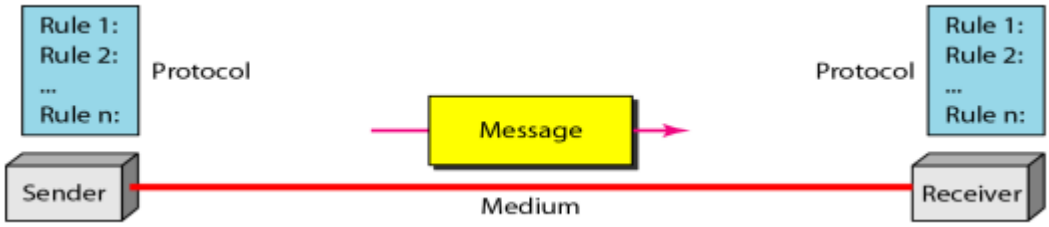
- Mobile computers such as notebook computers and PDAs are connected to office or home even when away from home
- Can be used as a portable electronic equipment to send and receive telephone calls , faxes , mail ,surf the web , access remote files

The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1. **Delivery**.
   The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. **Accuracy.** The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
3. **Timeliness.**
   The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.
4. **Jitter**.

Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 30 ms. If some of the packets arrive with 30-ms delay and others with 40-ms delay, an uneven quality in the video is the result.

A data communications system has five components



I. Message: The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

2 Sender: The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

3. Receiver: The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

4. Transmission medium: The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

5. Protocol: A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese. Data Representation Text Numbers Images Audio Video

Physical Structures

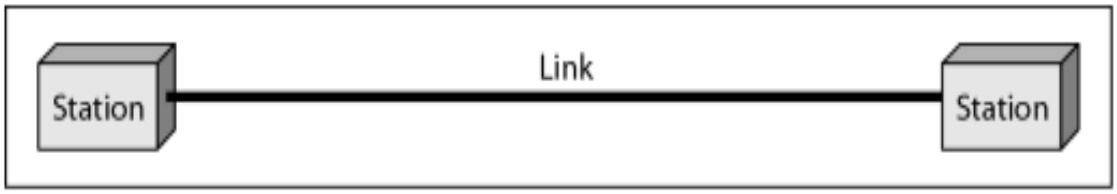
Before discussing networks, we need to define some network attributes.

Type of Connection 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**.

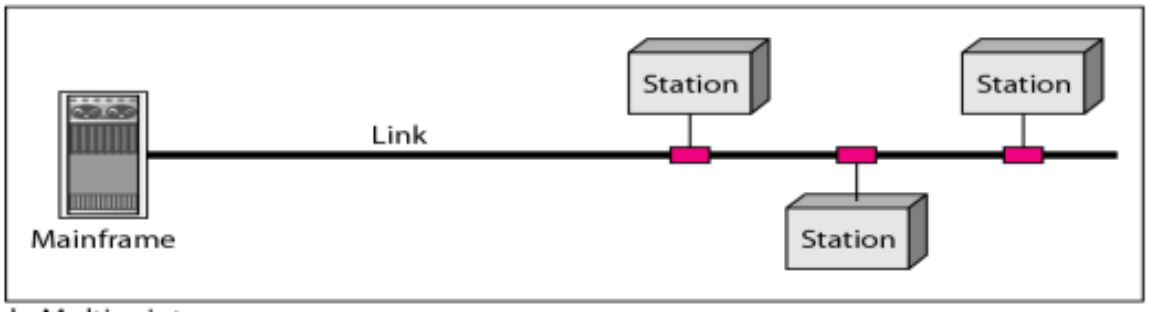
1.Point-to-Point: A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between

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.



a. Point-to-point

2.Multipoint: A multipoint (also called multi-drop) 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



b. Multipoint

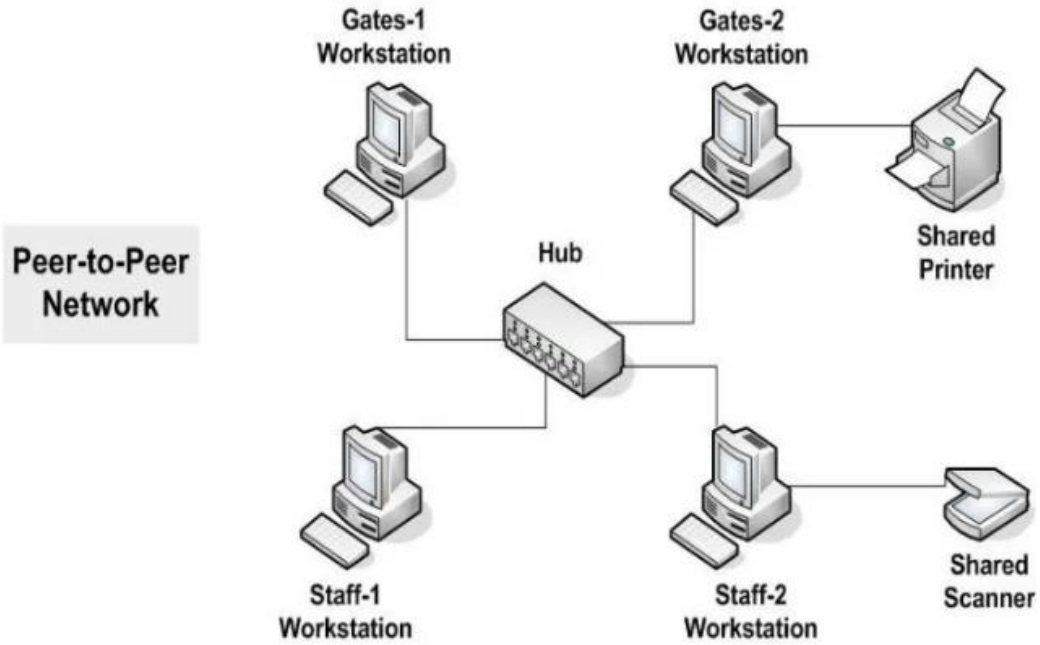
Defining Network Architecture

Network architecture is the logical and structural layout of the network, consisting of transmission equipment, software and communication protocols, and infrastructure (i.e. wired or wireless) transmission of data and connectivity between components.

The two types of widely used network architectures are **peer-to-peer** aka **P2P** and **client/server** aka **tiered**.

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 and all 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 thats connected to this network would act as the server for the files stored on it.



Peer — to — Peer Model

Advantages of a peer-to-peer network

- Does not require a dedicated server which means its less costly.
- If one computer stops working, the other computers connected to the network will continue working.

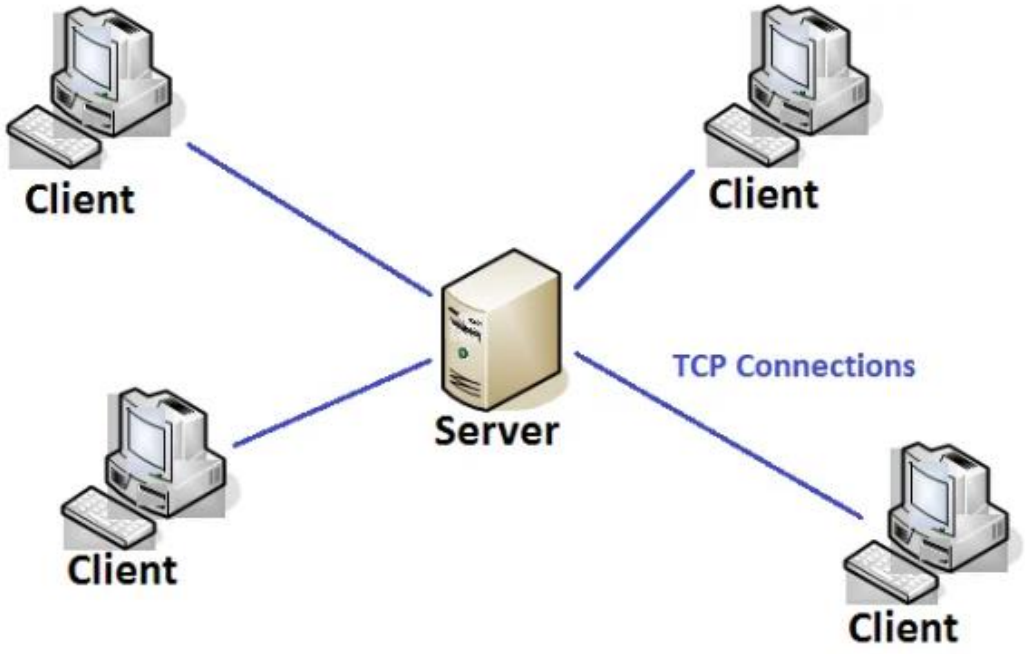
- Installation and setup is quite painless because of the built-in support in modern operating systems.

Disadvantages of a peer-to-peer network

- 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 access becomes 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) acts 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.



Client/Server Model

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.

What is network topology?

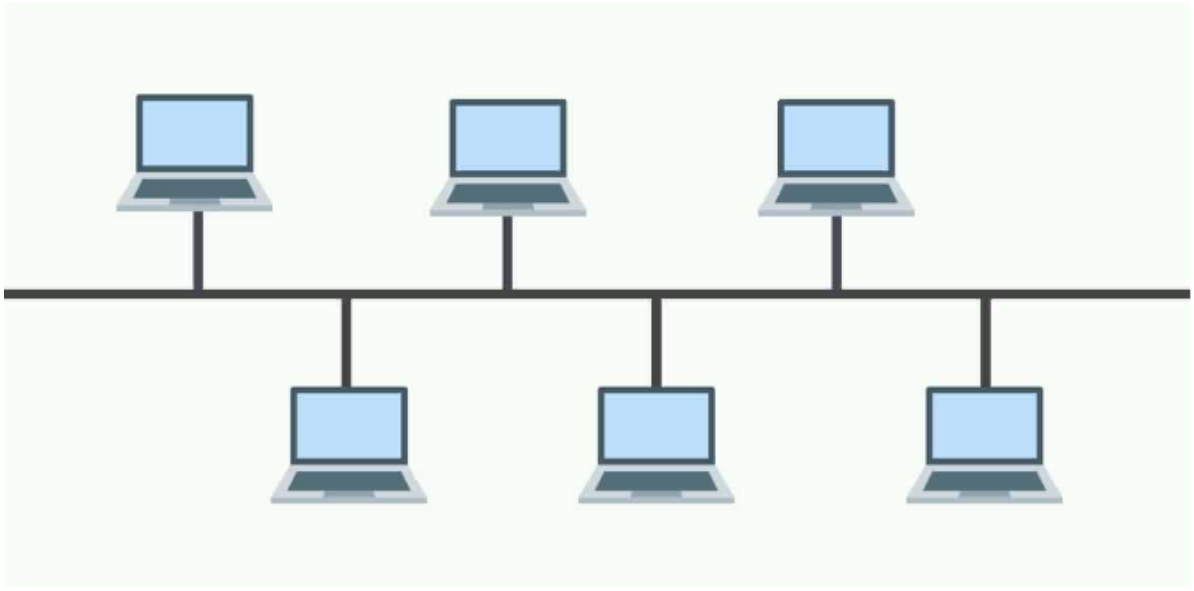
Network topology refers to the physical or logical arrangement of nodes (such as computers, switches, routers, or other devices) and the connections between them in a computer network.

- **The Blueprint of a Network** In simple terms, network topology is like the blueprint or map of a network. It outlines the layout and structure of the network, showing how the devices are interconnected and how data is transmitted between them. It defines the paths that information takes from one node to another and influences the efficiency, scalability, and reliability of the network.
- **Types of Network Topologies** There are different types of network topologies, including bus, star, ring, mesh, tree, and hybrid topologies. Each topology has its own characteristics, advantages, and limitations, and organizations choose the most suitable one based on their specific requirements and network design goals.

Types of network topology

There are many different types of topologies that enterprise networks have built on today and in the past. Some of the network topologies we're going to look at include **bustopology**, **ring topology**, **star topology**, **mesh topology**, and **hybrid topology**.

Bus topology



Bus topology is a network type where every device is connected to a single cable that runs from one end of the network to the other. This type of network topology is often referred to as **line topology**. In a bus topology, data is transmitted in one direction only. If the bus topology has two endpoints then it is referred to as a **linear bus topology**.

Smaller networks with this type of topology use a coaxial or RJ45 cable to link devices together. However, the bus topology layout is outdated and you're unlikely to encounter a company using a bus topology today.

Advantages

Bus topologies were often used in smaller networks. One of the main reasons is that they **keep the layout simple**. All devices are connected to a single cable so you don't need to manage a complex topological setup.

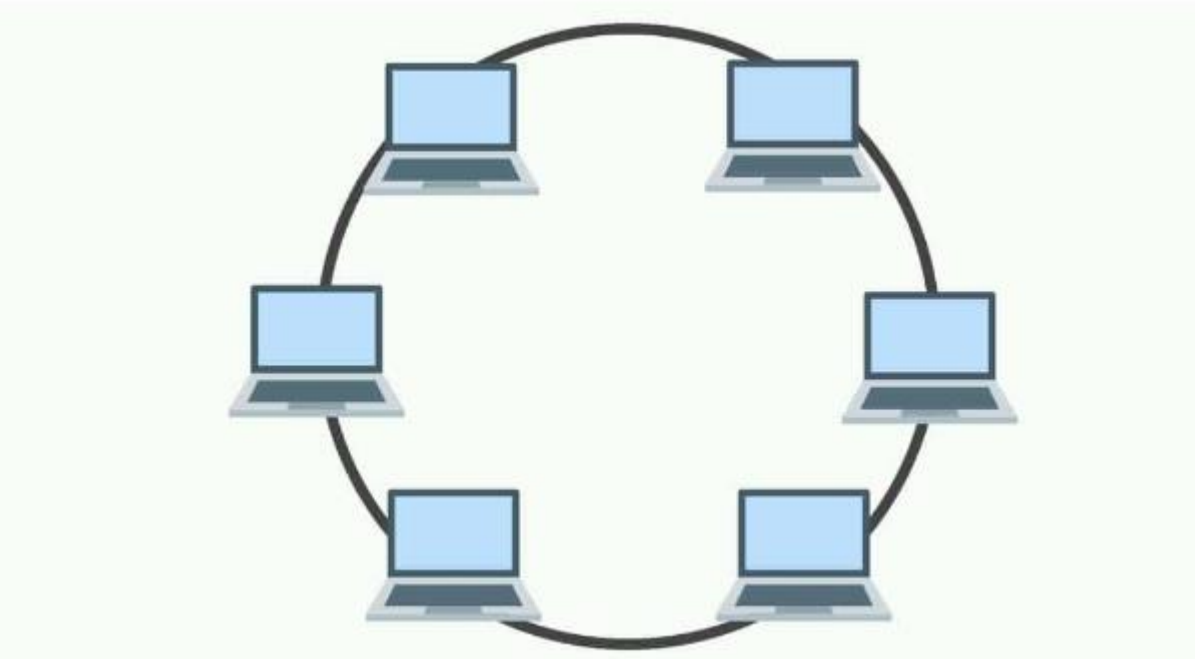
The layout also helped make bus topologies cost-effective because they **can be run with a single cable**. In the event that more devices need to be added then you could simply join your cable to another cable.

Disadvantages

However, relying on one cable does mean that **bus topologies have a single point of failure**. If the cable fails then the entire network will go down. A cable failure would cost organizations a lot of time while they attempt to resume service. Further to this, **high network traffic would decrease network performance** because all the data travels through one cable.

This limitation makes bus topologies suitable only for smaller networks. The primary reason is that the more network nodes you have, the slower your transmission speeds are going to be. It is also worth noting that bus topologies are limited in the sense that they are **half-duplex**,

Ring topology



n networks with ring topology, computers are connected to each other in a circular format. **Every device in the network will have two neighbors** and no more or no less. Ring topologies were commonly used in the past but you would be hard-pressed to find an enterprise still using them today.

The first node is connected to the last node to link the loop together. As a consequence of being laid out in this format packets need to travel through all network nodes on the way to their destination.

Advantages

With ring topologies, the **risk of packet collisions is very low** due to the use of token-based protocols, which only allow one station to transmit data at a given time. This is compounded by the fact that **data can move through network nodes at high speeds** which can be expanded on when more nodes are added.

Dual ring topologies provided an extra layer of protection because they were **more resistant to failures**. For instance, if a ring goes down within a node then the other ring can step up and back it up. Ring topologies were also **low cost to install**.

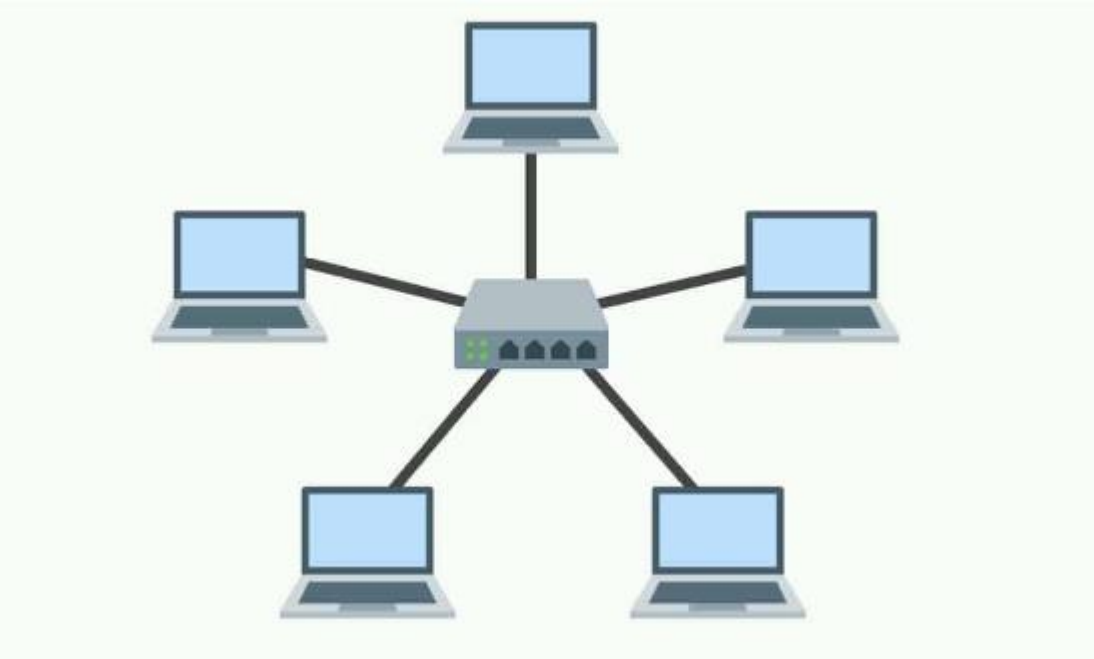
Disadvantages

One of the reasons why ring topologies were replaced is because they are very vulnerable to failure. The **failure of one node can take the entire network out of operation**. This means that ring topology networks need to be constantly managed to ensure that all network nodes are in good health. However, even if

the nodes were in good health your network **could still be knocked offline by a transmission line failure!**

Ring topologies also **raised scalability concerns**. For instance, bandwidth is shared by all devices within the network. In addition, **the more devices that are added** to a network **the more communication delay** the network experiences. This means that the number of devices added to a network topology needed to be monitored carefully to make sure that the network resources weren't stretched beyond their limit.

Star topology



A star topology is a topology where every node in the network is connected to one central switch. Every device in the network is directly connected to the switch and indirectly connected to every other node. The relationship between these elements is that the central network hub is a server and other devices are treated as clients. The central node has the responsibility of managing data transmissions across the whole network and acts as a repeater. With star topologies, computers are connected with a coaxial cable, twisted pair, or optical fiber cable.

Advantages

Star topologies are most commonly-used because you **can manage the entire network from one location**: the central switch. As a consequence, if a node that isn't the central node goes down then the network will remain up. This gives star topologies a layer of protection against failures that aren't always present with

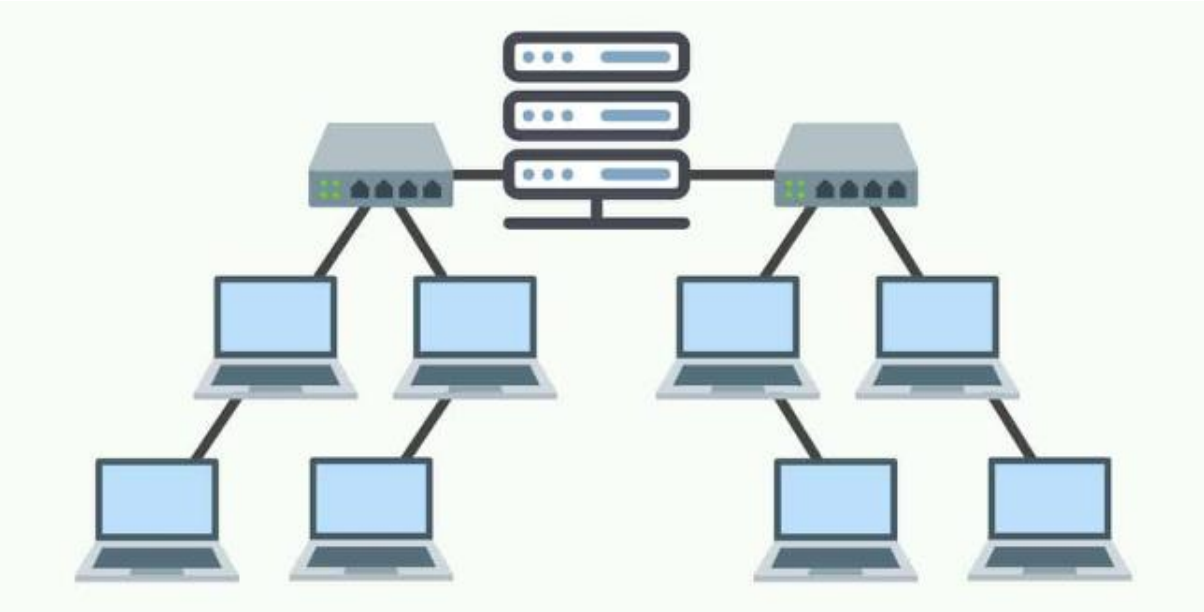
other topology setups. Likewise, you **can add new computers without having to take the network offline** like you would have to do with a ring topology.

In terms of physical network structure, star topologies require fewer cables than other topology types. This makes them **simple to set up and manage** over the long-term. The simplicity of the overall network design makes it much easier for administrators to run troubleshooting when dealing with network performance faults.

Disadvantages

Though star topologies may be relatively safe from failure, **if the central switch goes down then the entire network will go down**. As such, the administrator needs to manage the health of the central node closely to make sure that it doesn't go down. The performance of the network is also **tied to the central node's configurations and performance**. Star topologies are easy to manage in most ways but they are far from cheap to set up and use

Tree topology



As the name suggests, a tree topology network is a structure that is shaped like a tree with its many branches. Tree topologies **have a root node** that is connected to another node hierarchy. The **hierarchy is parent-child** where there is only one mutual connection between two connected nodes. As a general rule, a tree topology needs to have three levels to the hierarchy to be classified this way. This form of topology is **used within Wide Area Networks** to sustain lots of spread-out devices.

Advantages

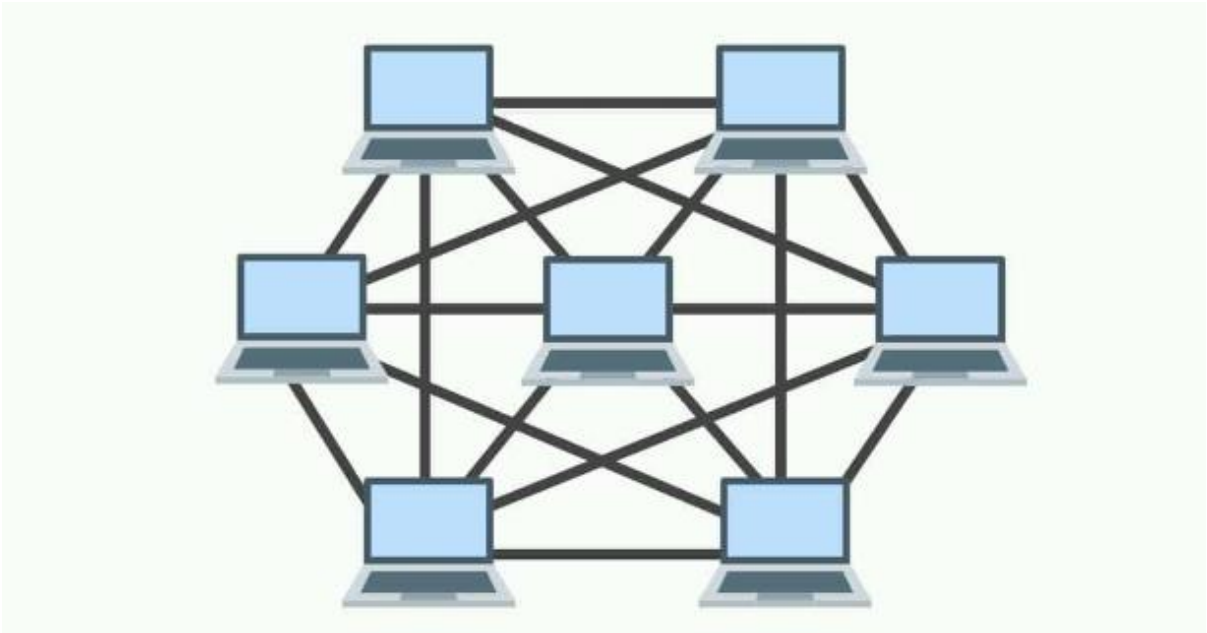
The main reason why tree topologies are **used is to extend bus and star topologies**. Under this hierarchical format, it is easy to add more nodes to the network when your organization grows in size. This format also **lends itself well to finding errors and troubleshooting** because you can check for network performance issues systematically throughout the tree.

Disadvantages

The most significant weakness of tree topology is the root node. **If the root node fails then all of its subtrees become partitioned**. There will still be partial connectivity within the network amongst other devices such as the failed node's parent.

Maintaining the network system is not simple either because **the more nodes you add, the more difficult it becomes to manage** the network. Another disadvantage of a tree topology is the number of cables you need. Cables are required to connect every device throughout the hierarchy which makes the network layout more complex when compared to a simpler topology.

Mesh topology



A mesh topology is a point-to-point connection where nodes are interconnected. In this form of topology, **data is transmitted via two methods**: **routing** and **flooding**. Routing is where nodes use routing logic to work out the shortest distance to the packet's destination. In contrast, flooding is where data is sent to all nodes within the network. Flooding doesn't require any form of routing logic to work.

There are **two forms of mesh topology**: **partial mesh topology** and **full mesh topology**. With partial mesh topology, most nodes are interconnected but there are a few which are only connected to two or three other nodes. A full mesh topology is where every node is interconnected

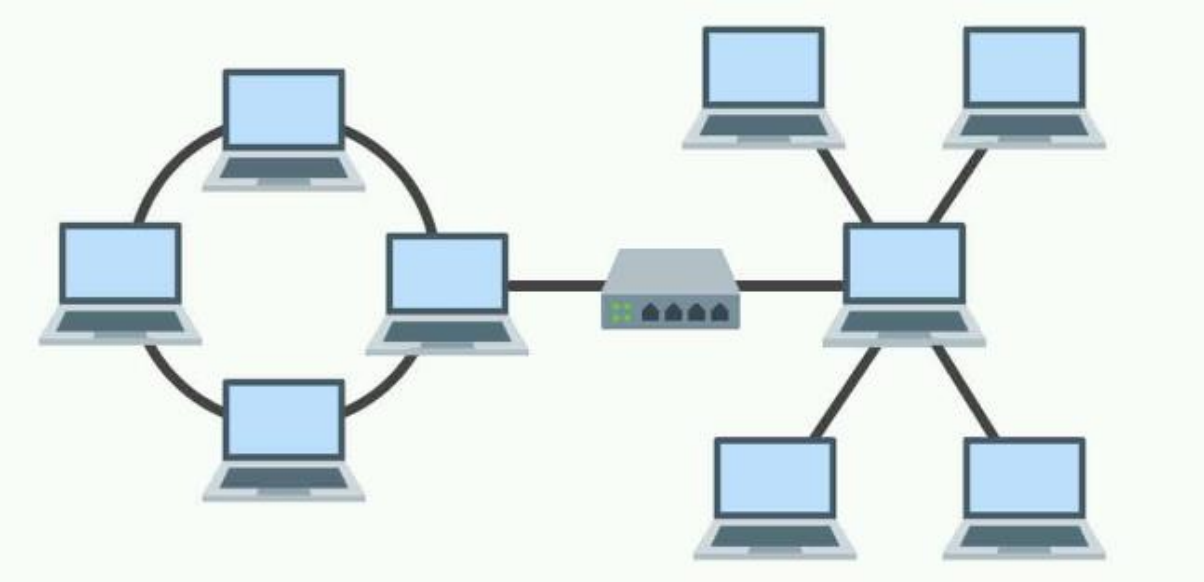
Advantages

Mesh topologies are used first and foremost because they are reliable. The **interconnectivity of nodes makes them extremely resistant to failures**. There is no single machine failure that could bring down the entire network. The absence of a single point of failure is one of the reasons why this is a popular topology choice. This setup is also secure from being compromised.

Disadvantages

However, mesh topologies are far from perfect. They **require an immense amount of configuration** once they are deployed. The topological layout is more complex than many other topologies and this is reflected by how long it takes to set up. You'll need to accommodate a whole host of new wiring which can add up to be quite expensive.

Hybrid topology



When a topology is composed of two or more different topologies it is referred to as a hybrid topology. Hybrid topologies are **most-commonly encountered in larger enterprises** where individual departments have network topologies that different from another topology in the organization. Connecting these topologies together will result in a hybrid topology. As a consequence, the capabilities and vulnerabilities depend on the types of topology that are tied together.

Advantages

There are many reasons why hybrid topologies are used but they all have one thing in common: **flexibility**. There are few constraints on the network structure that a hybrid topology cannot accommodate, and you **can incorporate multiple topologies into one hybrid setup**. As a consequence, hybrid topologies are very scalable. The scalability of hybrid setups makes them well-suited to larger networks.

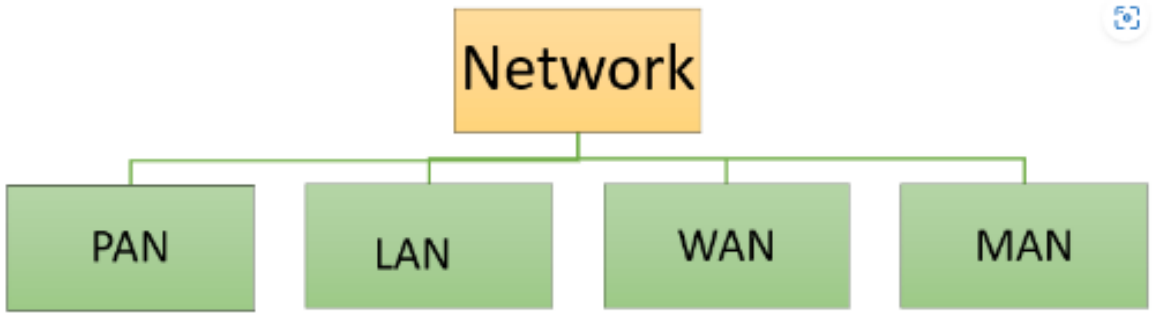
Disadvantages

Unfortunately, hybrid topologies **can be quite complex**, depending on the topologies that you decide to use. Each topology that is part of your hybrid topology will have to be managed according to its unique network requirements. This makes administrators' jobs more difficult because they are going to have to attempt to manage multiple topologies rather than a single one. In addition, setting up a hybrid topology **can end up being quite costly**.

Different Types of Computer Networks

There are various types of Computer Networking options available. The classification of network in computers can be done 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. Following are the popular types of Computer Network:



- PAN (Personal Area Network)
- LAN (Local Area Network)
- MAN (Metropolitan Area Network)
- WAN (Wide Area Network)

PAN (Personal Area Network) 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

Below are the main 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 the important pros/benefits of 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

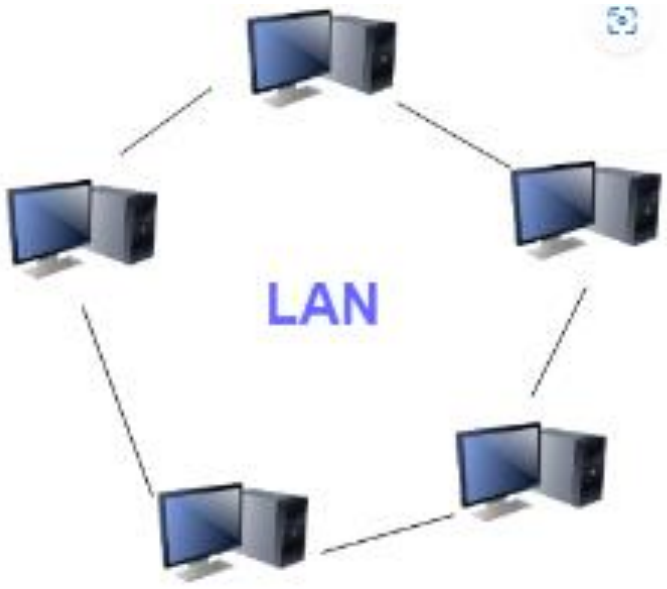
Disadvantages of PAN

Here are the cons/drawbacks of using PAN network:

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

What is a LAN (Local Area Network)?

A **Local Area Network** (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.



Local Area Network (LAN)

Characteristics of LAN

Here are the 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 the pros/benefits of 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.

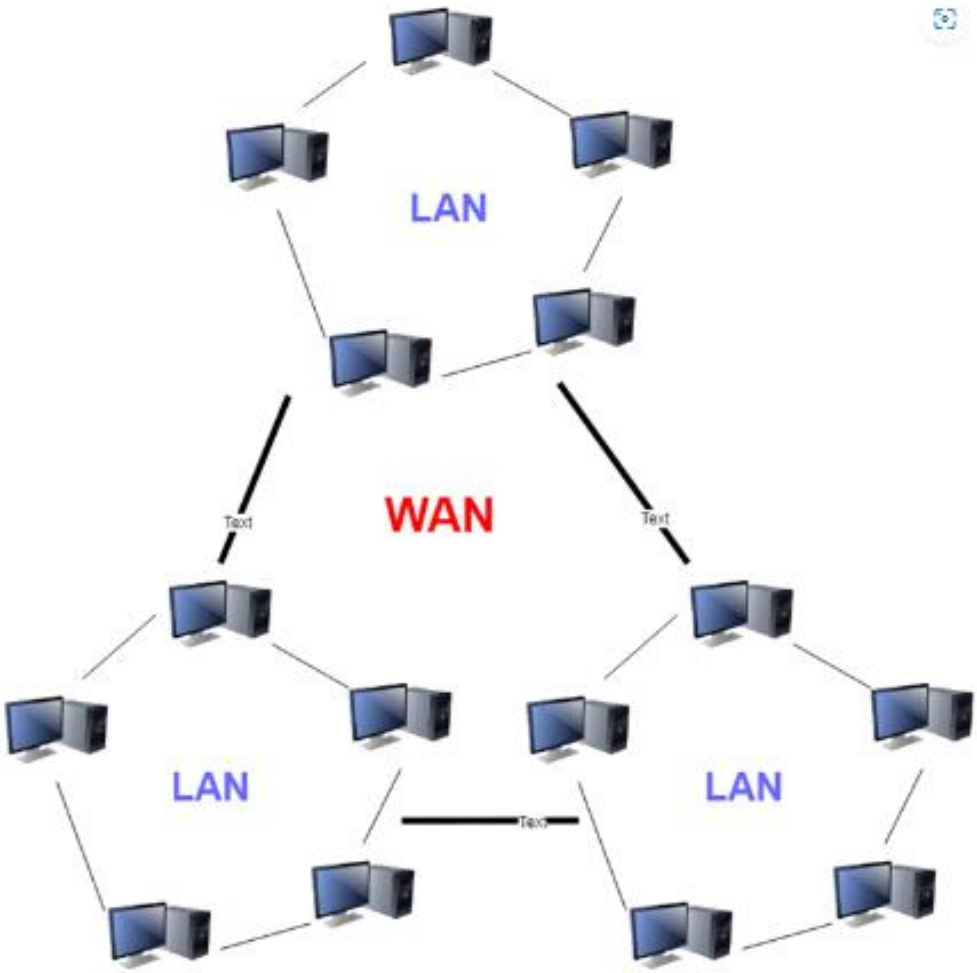
Disadvantages of LAN

Here are the 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 (Wide Area Network)?

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.



Wide Area Network (WAN)

Characteristics of WAN

Below are the characteristics of WAN:

- 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 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.

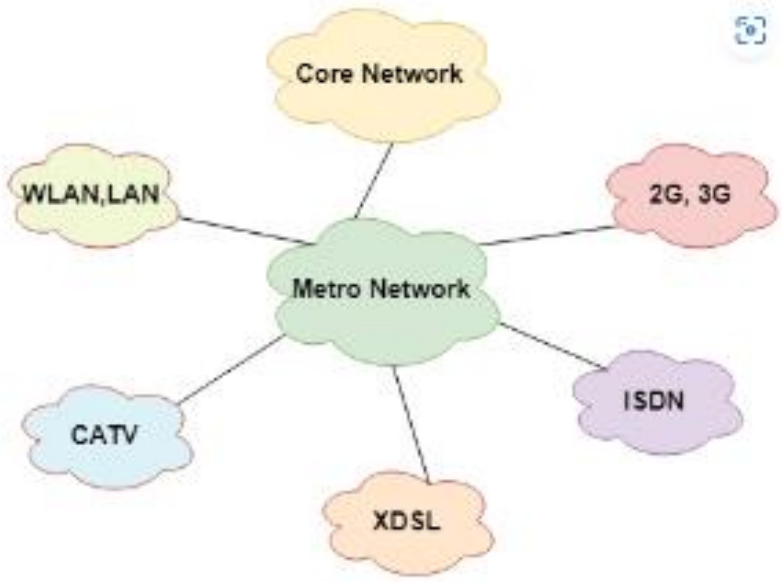
Disadvantages of WAN

Here are the drawbacks/cons of WAN network:

- 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 network in computer.

What is MAN (Metropolitan Area Network)?

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.



Metropolitan Area Network (MAN)

Characteristics of MAN

Here are important characteristics of the MAN network:

- It mostly covers towns and cities in a maximum 50 km range
- Mostly used medium is optical fibers, cables

- Data rates adequate for distributed computing applications.

Advantages of MAN

Here are the pros/benefits of MAN network:

- 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

Other Types of Computer Networks

Apart from above mentioned computer networks, here are some other important types of networks:

- WLAN (Wireless Local Area Network)
- Storage Area Network
- System Area Network
- Home Area Network
- POLAN- Passive Optical LAN
- Enterprise private network
- Campus Area Network
- Virtual Area Network

THE INTERNET

The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. Count the ways you've used the Internet recently. Perhaps you've sent electronic mail (e-mail) to a business associate, paid a utility bill, read a newspaper from a distant city, or looked up a local movie schedule-all by using the Internet. Or maybe you

researched a medical topic, booked a hotel reservation, chatted with a fellow Trekkie, or comparison-shopped for a car.

The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.

A network is a group of connected communicating devices such as computers and printers. An internet (note the lowercase letter i) is two or more networks that can communicate with each other. The most notable internet is called the Internet (uppercase letter I), a collaboration of more than hundreds of thousands of interconnected networks.

Private individuals as well as various organizations such as government agencies, schools, research facilities, corporations, and libraries in more than 100 countries use the Internet. Millions of people are users. Yet this extraordinary communication system only came into being in 1969.

In the mid-1960s, mainframe computers in research organizations were standalone devices. Computers from different manufacturers were unable to communicate with one another. The Advanced Research Projects Agency (ARPA) in the Department of Defense (DoD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort. In 1967, at an Association for Computing Machinery (ACM) meeting,

ARPA presented its ideas for ARPANET, a small network of connected computers. The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an inteiface message processor (IMP). The IMPs, in tum, would be connected to one another. Each IMP had to be able to communicate with other IMPs as well as with its own attached host. By 1969, ARPANET was a reality. Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the University of Utah, were connected via the IMPs to form a network. Software called the Network Control Protocol (NCP) provided communication between the hosts. In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the Internetting Projec1.

The Internet today is not a simple hierarchical structure. It is made up of many wide- and local-area networks joined by connecting devices and switching stations. It is difficult to give an accurate representation of the Internet because it is continually changing-new networks are being added, existing networks are adding addresses, and networks of defunct companies are being removed. Today

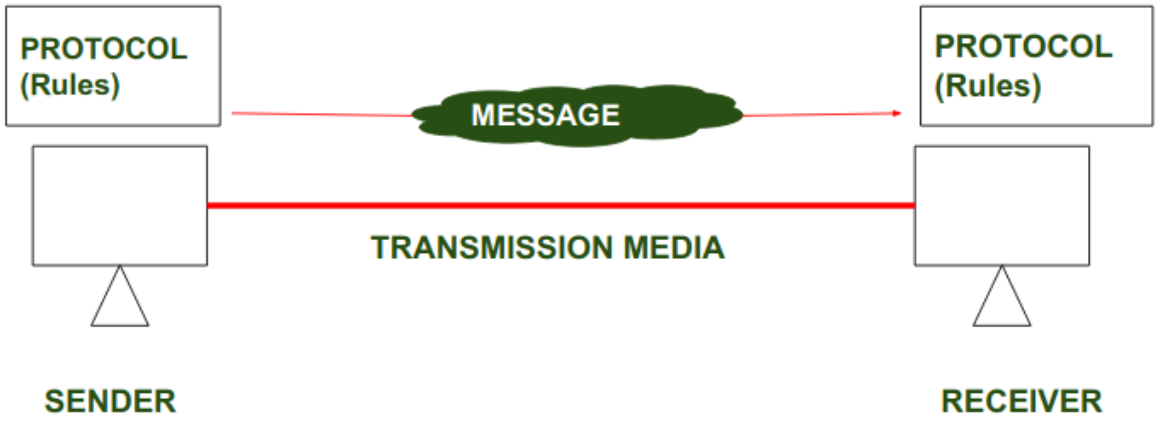
most end users who want Internet connection use the services of Internet service providers (lSPs).

There are international service providers, national service providers, regional service providers, and local service providers. The Internet today is run by private companies, not the government. Figure 1.13 shows a conceptual (not geographic) view of the Internet.

Computer networks are dependent on protocols and standards which plays a vital role, which enables communication between different devices and systems with one another and share data seamlessly. Network protocol ensures that different technologies and components of the network are compatible with one another, reliable, and able to function together.

Overview of Protocol

In Order to make communication successful between devices , some rules and procedures should be agreed upon at the sending and receiving ends of the system. Such rules and procedures are called as Protocols . Different types of protocols are used for different types of communication.



In above diagrams Protocols are shown as set of rules . Such that Communication between Sender and Receiver is not possible without Protocol**.**

Key Element of Protocol

- **Syntax :** syntax refers to the structure or the format of the data that gets exchanged between the devices. Syntax of message includes the type of data, composition of message and sequencing of message. The starting 8 bits of data is considered as the address of the sender. The next 8 bits is considered to be the address of the receiver. The remaining bits are considered as the message itself.

- **Semantics :** Semantics defines data transmitted between devices. It provides rules and norms for understanding message or data element values and actions.
- **Timing :** Timing refers to the synchronization and coordination between devices while transferring the data. Timing ensures at what time data should be sent and how fast data can be sent. For example, If a sender sends 100 Mbps but the receiver can only handle 1 Mbps, the receiver will overflow and lose data. Timing ensures preventing data loss, collisions and other timing related issues.
- **Sequence control :** Sequence control ensures the proper ordering of data packets. The main responsibility of sequence control is to acknowledge the data while it get received, and the retransmission of lost data. Through this mechanism the data is delivered in correct order.
- **Flow Control :** Flow control regulates device data delivery. It limits the sender's data or asks the receiver if it's ready for more. Flow control prevents data congestion and loss.
- **Error Control :** Error control mechanisms detect and fix data transmission faults. They include error detection codes, data resend, and error recovery. Error control detects and corrects noise, interference, and other problems to maintain data integrity.
- **Security :** Network security safeguards data confidentiality, integrity, and authenticity. which includes encryption, authentication, access control, and other security procedures. Network communication's privacy and trustworthiness are protected by security standards.

Standards

Standards are the set of rules for data communication that are needed for exchange of information among devices. It is important to follow Standards which are created by various Standard Organization like IEEE , ISO , ANSI etc.

Types of Standards

Standards are of two types :

- De Facto Standard.
- De Jure Standard.

De Facto Standard : The meaning of the work *" De Facto "* is " By Fact " or "By Convention".These are the standard s that have not been approved by any Organization , but have been adopted as Standards because of it's widespread use. Also , sometimes these standards are often established by Manufacturers.

For example : Apple and Google are two companies which established their own rules on their products which are different . Also they use some same standard rules for manufacturing for their products.

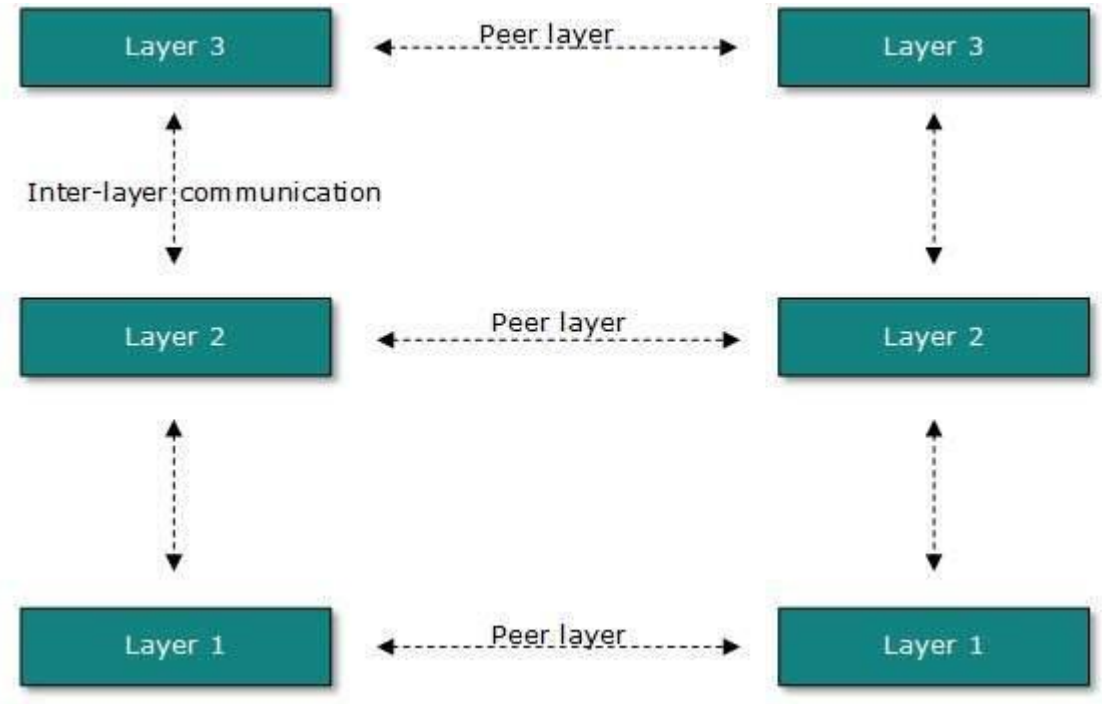
De Jure Standard : The meaning of the word *"De Jure"* is "By Law" or "By Regulations".Thus , these are the standards that have been approved by officially recognized body like ANSI , ISO , IEEE etc. These are the standard which are important to follow if it is required or needed.
For example : All the data communication standard protocols like SMTP , TCP , IP , UDP etc. are important to follow the same when we needed them.
Types of Protocol

- **Network Layer Protocols :** Network layer protocols operate in the network layer which is also known as the Layer 3 of the network architecture. Network layer protocols are responsible for packet routing, forwarding and addressing of data packets throughout the network . IP and ICMP are the network layer protocols.
- **Transport layer Protocols** : Transport layer protocols works in transport layer which provides end-to-end service ensuring data transfer across apps on different devices. TCP and UDP are the most popular transport layer protocols.
- **Application Layer Protocol :** Application layer protocol working in the application layer of the network architecture provides communication between applications running on different devices. The application layer protocols enable cross-device communication. They format, exchange, and interpret application data. HTTP, FTP, and SMTP are examples.
- **Wireless Protocols :** Wireless protocols basically used in wireless communication which enables data transfer through wireless networks. Bluetooth, Wi-Fi, and LTE protocols are examples.
- **Routing Protocols :** Routing protocol establishes the best/optimal network pathways throughout the network for fastest data transmission. Routers share information to develop and maintain routing tables. RIP, OSPF, and BGP are examples.
- **Security Protocols :** security protocol protects data confidentiality, integrity, and authenticity while transmission of data over the network. They include SSL and TLS, encryption methods, and authentication protocols for providing data security.
- **Internet Protocols :** IP identifies devices uniquely. Internet protocol provides data communication through routing and forwarding data packets from one device to another by unique addressing scheme.

Layered Tasks

In layered architecture of Network Model, one whole network process is divided into small tasks. Each small task is then assigned to a particular layer which works dedicatedly to process the task only. Every layer does only specific work.

In layered communication system, one layer of a host deals with the task done by or to be done by its peer layer at the same level on the remote host. The task is either initiated by layer at the lowest level or at the top most level. If the task is initiated by the-top most layer, it is passed on to the layer below it for further processing. The lower layer does the same thing, it processes the task and passes on to lower layer. If the task is initiated by lower most layer, then the reverse path is taken.



Every layer clubs together all procedures, protocols, and methods which it requires to execute its piece of task. All layers identify their counterparts by means of encapsulation header and tail.

OSI Model

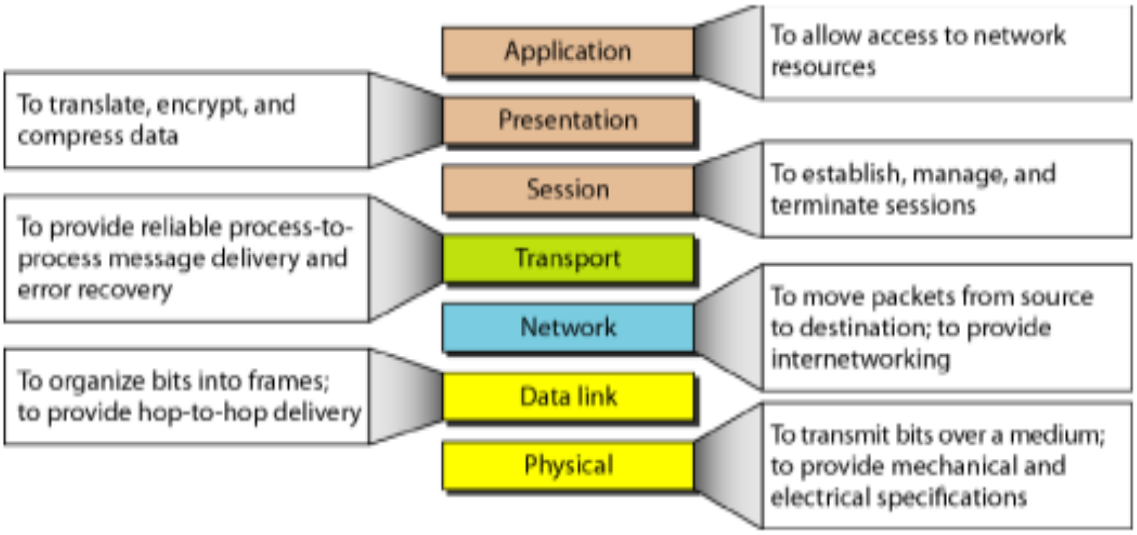
Open System Interconnect is an open standard for all communication systems. OSI model is established by International Standard Organization (ISO).

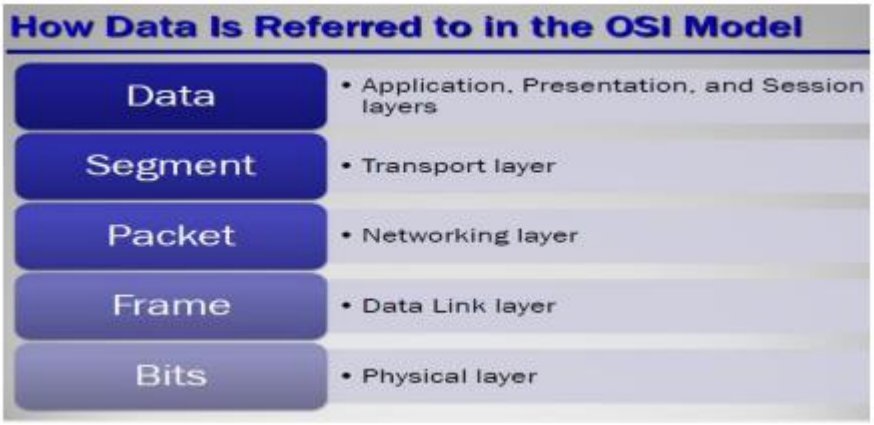
- It is not a standard that networking protocols must follow
- Each layer has specific functions it is responsible for
- All layers work together in the correct order to move data around a network

This model has seven layers:


Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

1


Application
To allow access to network resources
To translate, encrypt, and compress data
Presentation
Session
To establish, manage, and terminate sessions
To provide reliable process-to-process message delivery and error recovery
Transport
Network
To move packets from source to destination; to provide internetworking
To organize bits into frames; to provide hop-to-hop delivery
Data link
Physical
To transmit bits over a medium; to provide mechanical and electrical specifications



1)Physical Layer

- Deals with all aspects of physically moving data from one computer to the next
- Converts data from the upper layers into 1s and 0s for transmission over media
- Defines how data is encoded onto the media to transmit the data
- Defined on this layer: Cable standards, wireless standards, and fiber optic standards. Copper wiring, fiber optic cable, radio frequencies, anything that can be used to transmit data is defined on the Physical layer of the OSI Model
- Device example: Hub
- Used to transmit data

2) Data Link Layer

- Is responsible for moving frames from node to node or computer to computer
- Can move frames from one adjacent computer to another, cannot move frames across routers
- Encapsulation = frame
- Requires MAC address or physical address
- Protocols defined include Ethernet Protocol and Point-to-Point Protocol (PPP
- Device example: Switch
- Two sublayers: Logical Link Control (LLC) and the Media Access Control (MAC) o Logical Link Control (LLC)

♣ –Data Link layer addressing, flow control, address notification, error control

o Media Access Control (MAC)

♣ –Determines which computer has access to the network media at any given time

♣ –Determines where one frame ends and the next one starts, called frame synchronization

3) Network Layer

- Responsible for moving packets (data) from one end of the network to the other, called end-to-end communications
- Requires logical addresses such as IP addresses
- Device example: Router
- –Routing is the ability of various network devices and their related software to move data packets from source to destination

4) Transport Layer

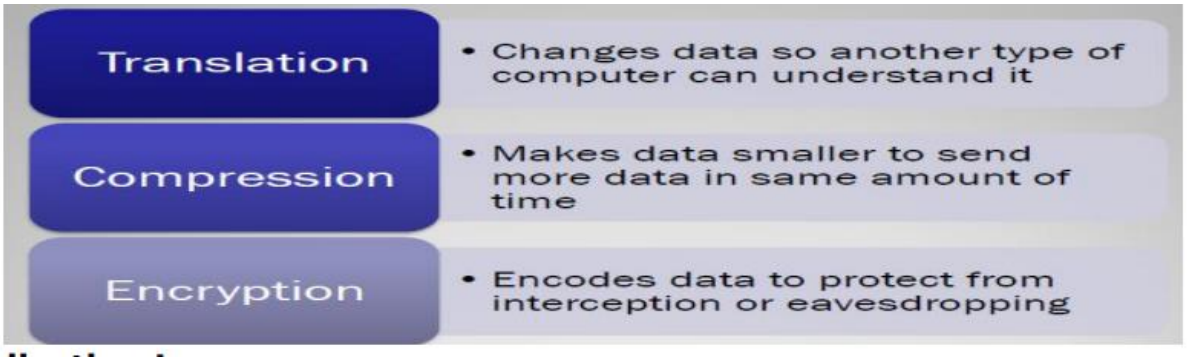
- Takes data from higher levels of OSI Model and breaks it into segments that can be sent to lower-level layers for data transmission
- Conversely, reassembles data segments into data that higher-level protocols and applications can use
- Also puts segments in correct order (called sequencing) so they can be reassembled in correct order at destination
- Concerned with the reliability of the transport of sent data
- May use a connection-oriented protocol such as TCP to ensure destination received segments
- May use a connectionless protocol such as UDP to send segments without assurance of delivery
- Uses port addressing

5)Session Layer

- Responsible for managing the dialog between networked devices
- Establishes, manages, and terminates connections
- Provides duplex, half-duplex, or simplex communications between devices
- Provides procedures for establishing checkpoints, adjournment, termination, and restart or recovery procedures.

6)Presentation Layer

- Concerned with how data is presented to the network
- Handles three primary tasks: –Translation , –Compression , –Encryption



7) Application Layer

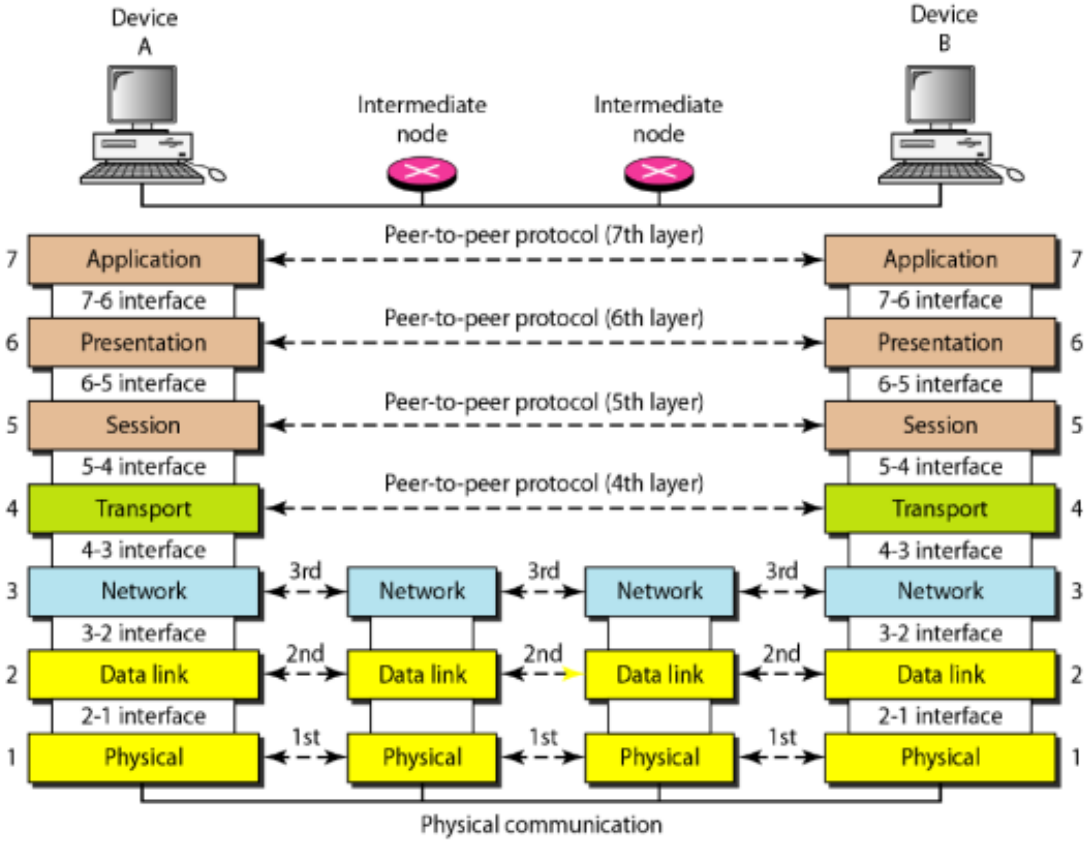
• Contains all services or protocols needed by application software or operating system to communicate on the network

• Examples :

o –Firefox web browser uses HTTP (Hyper-Text Transport Protocol)\

o –E-mail program may use POP3 (Post Office Protocol version to read e-mails and SMTP (Simple Mail Transport Protocol) to send e-mails

The interaction between layers in the OSI model



The advantages of the OSI model are

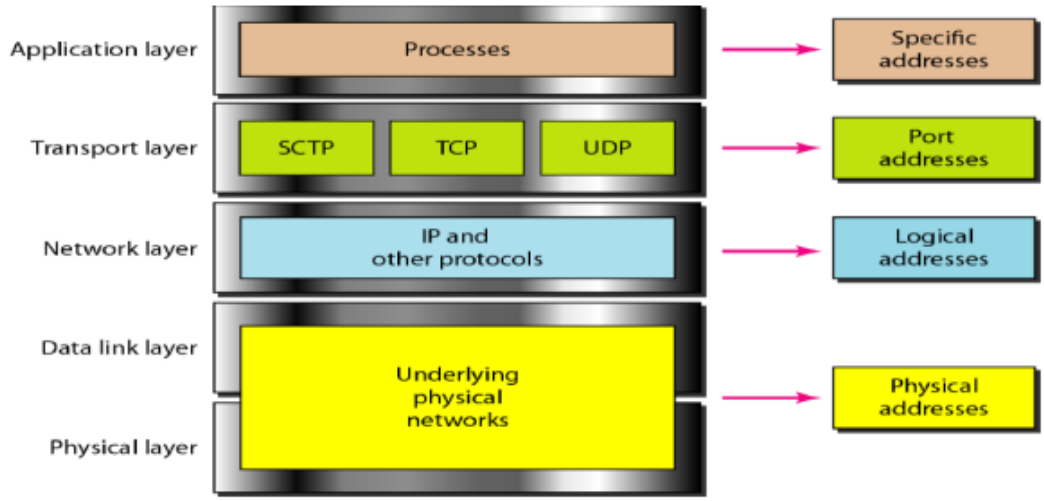
- It is a generic model and acts as a guidance tool to develop any network model.
- It is a layered model. Changes are one layer do not affect other layers, provided that the interfaces between the layers do not change drastically.
- It distinctly separates services, interfaces, and protocols. Hence, it is flexible in nature. Protocols in each layer can be replaced very conveniently depending upon the nature of the network.
- It supports both connection-oriented services and connectionless services.

The disadvantages of the OSI model are

- It is purely a theoretical model that does not consider the availability of appropriate technology. This restricts its practical implementation.
- The launching timing of this model was inappropriate. When OSI appeared, the TCP/IP protocols were already implemented. So, the companies were initially reluctant to use it.
- The OSI model is very complex. The initial implementation was cumbersome, slow and costly.
- Though there are many layers, some of the layers like the session layer and presentation layer have very little functionality when practically deployed.
- There is a duplication of services in various layers. Services like addressing, flow control and error control are offered by multiple layers.
- The standards of OSI model are theoretical and do not offer adequate solutions for practical network implementation.
- After being launched, the OSI model did not meet the practical needs as well as the TCP/IP model. So it was labeled as inferior quality.
- TCP/IP model was very much preferred by the academia. It was believed that OSI was a product of the European communities and the US government, who were trying to force an inferior model to researchers and programmers. Hence, there was considerable resistance in adopting it.

TCP/IP Model (Transmission Control Protocol/Internet Protocol)

–A *protocol suite* is a large number of related protocols that work together to allow networked computers to communicate



Relationship of layers and addresses in TCP/IP

Application Layer

- Application layer protocols define the rules when implementing specific network applications
- Rely on the underlying layers to provide accurate and efficient data delivery
- Typical protocols:
  - FTP – File Transfer Protocol
    - For file transfer
  - Telnet – Remote terminal protocol
    - For remote login on any other computer on the network
  - SMTP – Simple Mail Transfer Protocol
    - For mail transfer
  - HTTP – Hypertext Transfer Protocol
    - For Web browsing
- Encompasses same functions as these OSI Model layers Application Presentation Session

Transport Layer

TCP &UDP

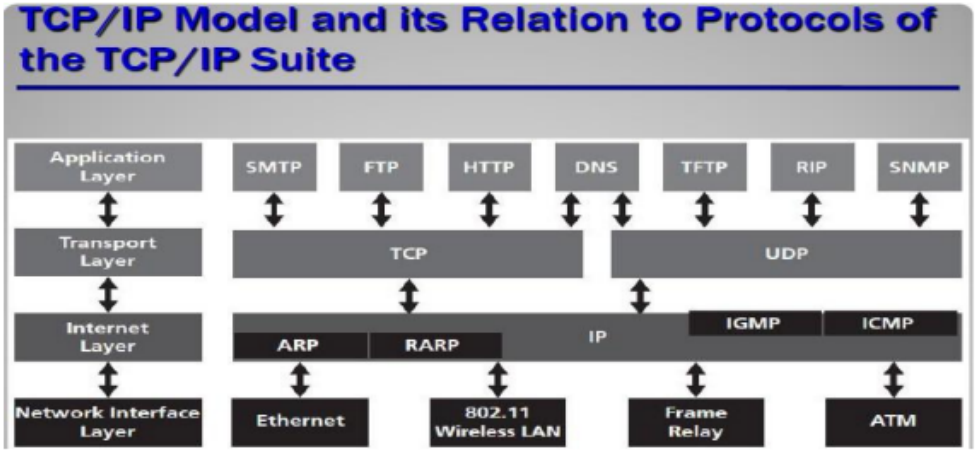
- TCP is a connection-oriented protocol
  - Does not mean it has a physical connection between sender and receiver
  - TCP provides the function to allow a connection virtually exists – also called virtual circuit
- UDP provides the functions:
  - Dividing a chunk of data into segments
  - Reassembly segments into the original chunk
  - Provide further the functions such as reordering and data resend
- Offering a reliable byte-stream delivery service
- Functions the same as the Transport layer in OSI
- Synchronize source and destination computers to set up the session between the respective computers

Internet Layer

- The network layer, also called the internet layer, deals with packets and connects independent networks to transport the packets across network boundaries. The network layer protocols are the IP and the Internet Control Message Protocol (ICMP), which is used for error reporting.

Host-to-network layer

The **Host-to-network layer** is the lowest **layer** of the **TCP/IP** reference model. It combines the link **layer** and the physical **layer** of the ISO/OSI model. At this **layer**, data is transferred between adjacent **network** nodes in a WAN or between nodes on the same LAN.



The advantages of TCP/IP protocol suite are

- It is an industry–standard model that can be effectively deployed in practical networking problems.
- It is interoperable, i.e., it allows cross-platform communications among heterogeneous networks.
- It is an open protocol suite. It is not owned by any particular institute and so can be used by any individual or organization.
- It is a scalable, client-server architecture. This allows networks to be added without disrupting the current services.

- It assigns an IP address to each computer on the network, thus making each device to be identifiable over the network. It assigns each site a domain name. It provides name and address resolution services.

The disadvantages of the TCP/IP model are

- It is not generic in nature. So, it fails to represent any protocol stack other than the TCP/IP suite. For example, it cannot describe the Bluetooth connection.
- It does not clearly separate the concepts of services, interfaces, and protocols. So, it is not suitable to describe new technologies in new networks.
- It does not distinguish between the data link and the physical layers, which has very different functionalities. The data link layer should concern with the transmission of frames. On the other hand, the physical layer should lay down the physical characteristics of transmission. A proper model should segregate the two layers.
- It was originally designed and implemented for wide area networks. It is not optimized for small networks like LAN (local area network) and PAN (personal area network).
- Among its suite of protocols, TCP and IP were carefully designed and well implemented. Some of the other protocols were developed ad hoc and so proved to be unsuitable in long run. However, due to the popularity of the model, these protocols are being used even 30–40 years after their introduction.

Difference between OSI Model and TCP/IP model

OSI Model	TCP/IP Model
OSI stands for Open System Interconnection. It is called so because it allows any two different systems to communicate regardless of their architecture	**TCP/IP stands for transmission control protocol/Internet protocol. It is named after these two protocols being part of this model.**
Developed by ISO(international standard Organization)	**Developed by DoD (Department of Defense)**
It has seven layers	**It has four layers**
Session and presentation layers are present in this model	**There if no Session and presentation layers are present in this model**

This model provides clear distinction between services, interfaces and protocols.	**It does not clearly distinguish, between services, interfaces and protocols.**
In this model, protocols do not fit well into the model	**Tcp/IP protocols fir well in this model**
OSI model supports both connectionless and connection oriented communication in network layer.	**TCP/IP model supports only connectionless communication in network layer.**