Data Communication/Computer Network Overview

Introduction

A system of interconnected computers and computerized peripherals *such as printers* is called network. This interconnection among computers facilitates information sharing among them. Computers may connect to each other by wired media or wireless media.

Categories

Computer Networks are classified into many categories based on their respective attributes. These include:

- Geographical span
- Inter-connectivity
- Administration
- Architecture

Geographical Span

Geographically a network can be seen in one of the following categories:

- It may be spanned across your table, among Bluetooth enabled devices. Ranging not more than few meters.
- It may be spanned across a whole building, including intermediate devices to connect all floors.
- It may be spanned across a whole city.
- It may be spanned across multiple cities or provinces.
- It may be one network covering whole world.

Inter-connectivity

Components of a network can be connected to each other differently in some fashion. By connectedness we mean either logically or physically or both ways.

- Every single device can be connected to every other device on network, making the network mesh.
- All devices can be connected to a single medium but geographically disconnected, created bus like structure.
- Each device is connected to its left and right peers only, creating linear structure.
- All devices connected together with a single device, creating star like structure.

- All devices connected arbitrarily using all previous ways to connect each other, resulting in a hybrid structure.

Administration

From an administrator's point of view, a network can be private network which belongs a single autonomous system and cannot access outside its physical or logical domain. Or a network can be a public network, which can be accessed by all.

Network Architecture

- There can be one or more systems acting as Server. Other being Client, request the Server to serve requests. Servers take and process request on behalf of Clients.
- Two systems can be connected Point-to-Point, or in other words back-to-back fashion. They both reside on same level and called peers.
- There can be hybrid network which involves network architecture of both the above types.

Network Applications

Computer systems and peripherals are connected to form a network provides bunch of advantages:

- Resource sharing such as printers and storage devices.
- Exchange of Information by means of emails and FTP.
- Information sharing by using Web or Internet.
- Interaction with other users using dynamic web pages.
- IP phones
- Video Conferences
- Parallel computing
- Instant Messaging

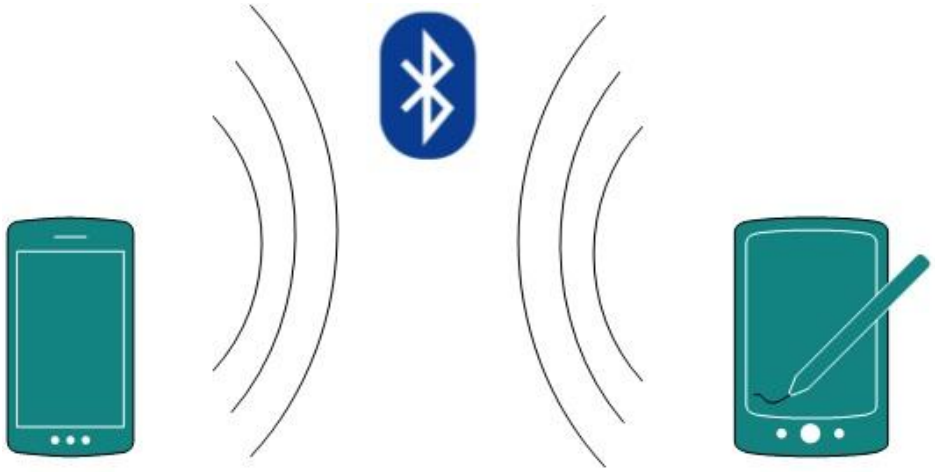
Computer Network Types

Generally, networks are distinguished based on their geographical span. A network can be as small as distance between your mobile phone and its Bluetooth headphone and as large as the Internet itself, covering the whole geographical world, i.e. the Earth.

Personal Area Network

A Personal Area Network or simply PAN, is smallest network which is very personal to a user. This may include Bluetooth enabled devices or infra-red enabled devices. PAN has connectivity

range up to 10 meters. PAN may include wireless computer keyboard and mouse, Bluetooth enabled headphones, wireless printers and TV remotes for example.



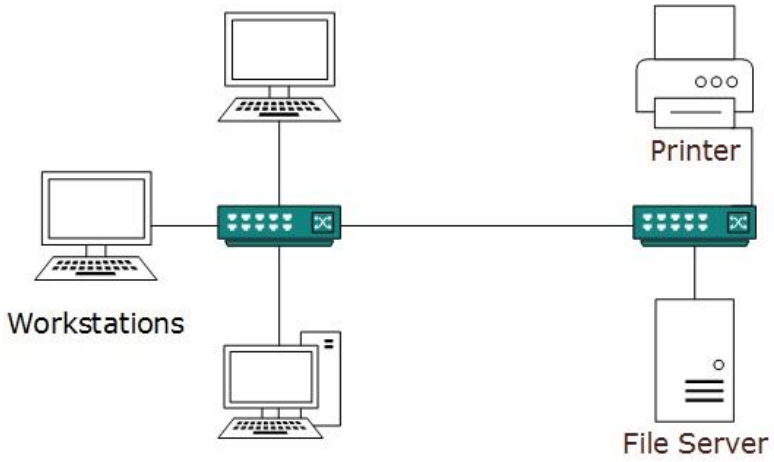
[*Image: Personal Area Network | Bluetooth*]

Pico net is an example Bluetooth enabled Personal Area Network which may contain up to 8 devices connected together in a master-slave fashion.

Local Area Network

A computer network spanned inside a building and operated under single administrative system is generally termed as Local Area Network. Usually, Local Area Network covers an organization's offices, schools, college/universities etc. Number of systems may vary from as least as two to as much as 16 million

LAN provides a useful way of sharing resources between end users. Resources like Printers, File Servers, Scanners and internet is easy sharable among computers.



[*Image: Local Area Network*]

Local Area Networks are composed of inexpensive networking and routing equipment. It may contains local servers serving file storage and other locally shared applications. It mostly operates on private IP addresses and generally do not involve heavy routing. LAN works under its own local domain and controlled centrally.

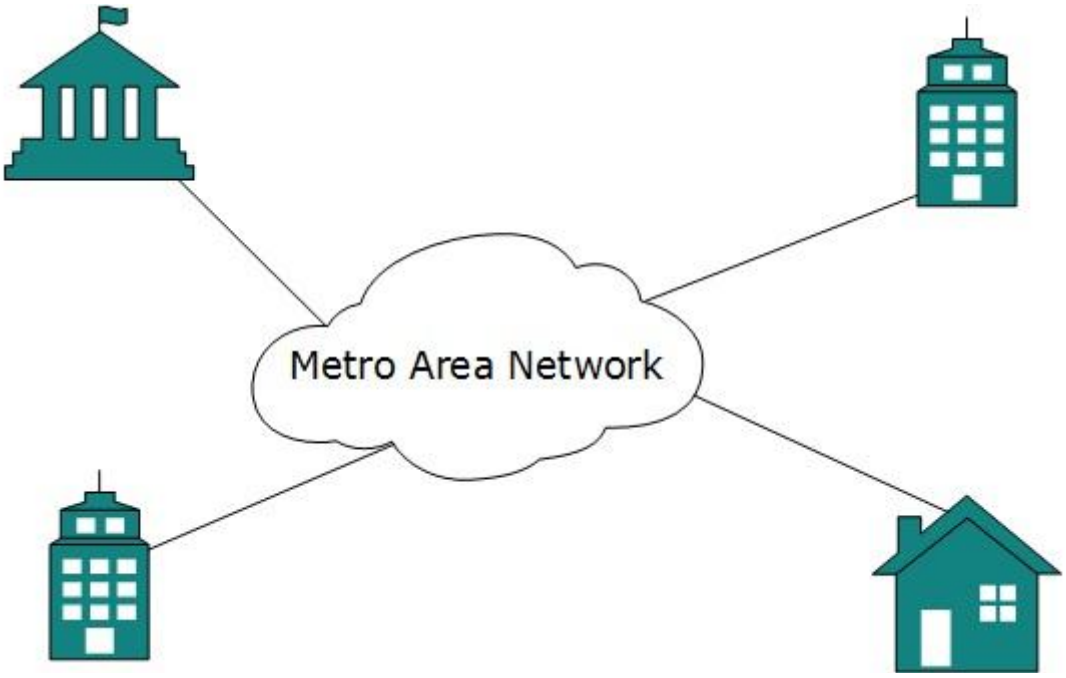
LAN uses either Ethernet or Token-ring technology. Ethernet is most widely employed LAN technology and uses Star topology while Token-ring is rarely seen.

LAN can be wired or wireless or in both forms at once.

Metropolitan Area Network

MAN, generally expands throughout a city such as cable TV network. It can be in form of Ethernet, Token-ring, ATM or FDDI.

Metro Ethernet is a service which is provided by ISPs. This service enables its users to expand their Local Area Networks. For example, MAN can help an organization to connect all of its offices in a City.

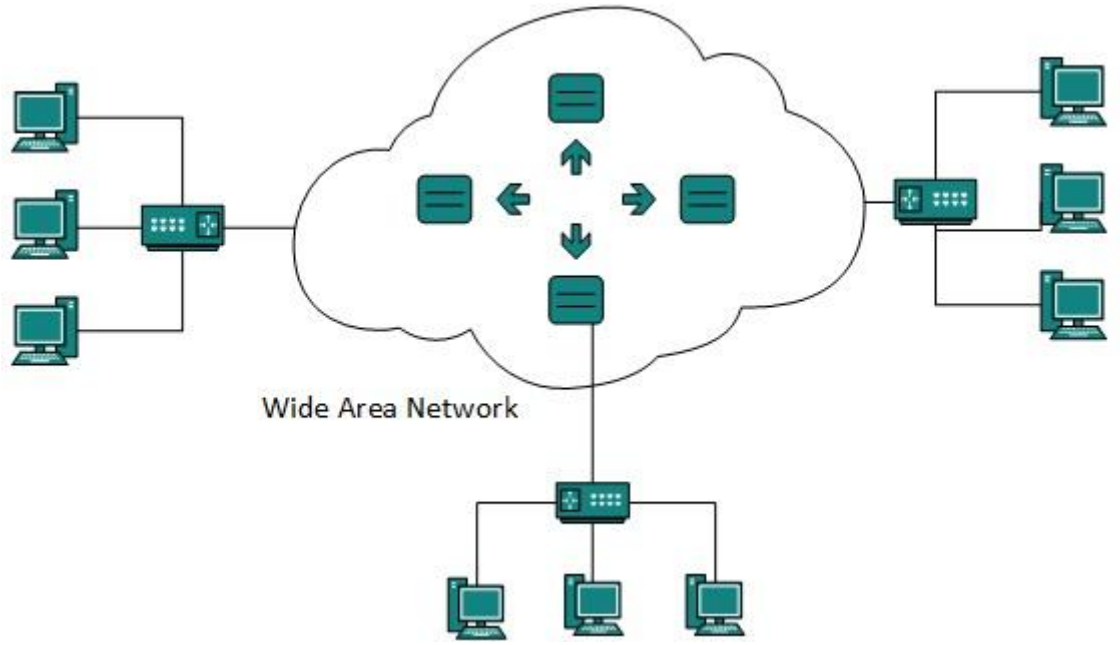


[*Image: Metropolitan Area Network*]

Backbone of MAN is high-capacity and high-speed fiber optics. MAN is works in between Local Area Network and Wide Area Network. MAN provides uplink for LANs to WANs or Internet.

Wide Area Network

As name suggests, this network covers a wide area which may span across provinces and even a whole country. Generally, telecommunication networks are Wide Area Network. These networks provide connectivity to MANs and LANs. Equipped with very high speed backbone, WAN uses very expensive network equipment.



[*Image: Wide Area Network*]

WAN may use advanced technologies like Asynchronous Transfer Mode *ATM*, Frame Relay and SONET. WAN may be managed under by more than one administration.

Internetwork

A network of networks is called internetwork, or simply Internet. It is the largest network in existence on this planet. Internet hugely connects all WANs and it can have connection to LANs and Home networks. Internet uses TCP/IP protocol suite and uses IP as its addressing protocol. Present day, Internet is widely implemented using IPv4. Because of shortage of address spaces, it is gradually migrating from IPv4 to IPv6.

Internet enables its users to share and access enormous amount of information worldwide. It uses www, ftp, email services, audio and video streaming etc. At huge level, internet works on Client-Server model.

Internet uses very high speed backbone of fiber optics. To inter-connect various continents, fibers are laid under sea known to us as submarine communication cable.

Internet is widely deployed on World Wide Web services using HTML linked pages and is accessible by some client software known as Web Browsers. When a user requests a page using some web browser located on some Web Server anywhere in the world, the Web Server responds with the proper HTML page. The communication delay is very low.

Internet is serving many proposes and is involved in many aspects of life. Some of them are:

- Web sites
- E-mail
- Instant Messaging
- Blogging
- Social Media
- Marketing
- Networking
- Resource Sharing
- Audio and Video Streaming

Network LAN Technologies

Ethernet

Ethernet is a Local Area Network implementation technology which is widely deployed. This technology was invented by Bob Metcalfe and D.R. Boggs in early 70s. It was standardized in IEEE 802.3 in 1980. Ethernet is network technology which shares media. Network which uses shared media has high probability of data collision. Ethernet uses CSMA/CD technology to detect collisions. CSMA/CD stands for Carrier Sense Multi Access/Collision Detection. When a collision happens in Ethernet, all its host rolls back and waits for some random amount of time and then re-transmit data.

Ethernet connector, i.e. Network Interface cards is equipped with 48-bits MAC address. This helps other Ethernet devices to identify and communicate with remote devices in Ethernet.

Traditional Ethernet uses 10BASE-T specifications. 10 is for 10mpbs speed, BASE stands for using baseband and T stands for Thick net or Thick Ethernet. 10BASE-T Ethernet provides transmission speed up to 10mbps and uses Coaxial cable or Cat-5 Twisted Pair cable with RJ-5 connector. Ethernet follows Star Topology with segment length up to 100 meters. All devices are connected to a Hub/Switch in a Star Fashion.

Fast-Ethernet

To encompass need of fast emerging software and hardware technologies, Ethernet extends itself as Fast-Ethernet. It can run on UTP, Optical Fiber and can be wireless too. It can provide speed up to 100 mbps. This standard is named as 100BASE-T in IEEE 803.2 using Cat-5 Twisted pair cable. It uses CSMA/CD technique for wired media sharing among Ethernet hosts and CSMA/CA *Collision Avoidance* technique for wireless Ethernet LAN.

Fast Ethernet on fiber is defined under 100BASE-FX standard which provides speed up to 100mbps on fiber. Ethernet over Fiber can be extended up to 100 meters in half-duplex mode and can reach maximum of 2000 meters in full-duplex over multimode fibers.

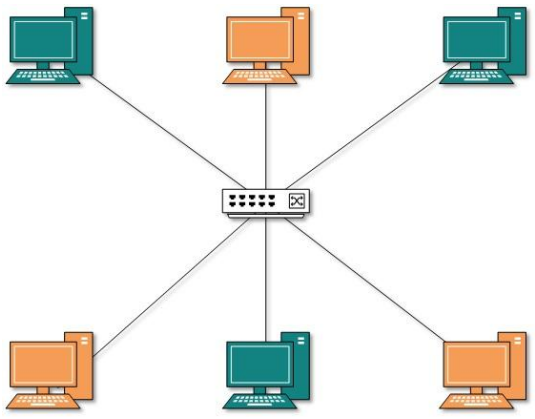
Giga-Ethernet

After being introduced in 1995, Fast-Ethernet could enjoy its high speed status only for 3 years till Giga-Ethernet introduced. Giga-Ethernet provides speed up to 1000 mbits/seconds. IEEE802.3ab standardizes Giga-Ethernet over UTP using Cat-5, Cat-5e and Cat-6 cables. IEEE802.3ah defines Giga-Ethernet over Fiber.

Virtual LAN

LAN uses Ethernet which in turn works on shared media. Shared media in Ethernet create one single Broadcast domain and one single Collision domain. Introduction of switches to Ethernet has removed single collision domain issue and each device connected to switch works in its separate collision domain. But even Switches cannot divide a network into separate Broadcast domain.

Virtual LAN is a method to divide a single Broadcast domain into more than one Broadcast domains. Host in one VLAN cannot speak to a host in another. By default, all hosts are placed into same VLAN.



[*Image: Virtual LAN*]

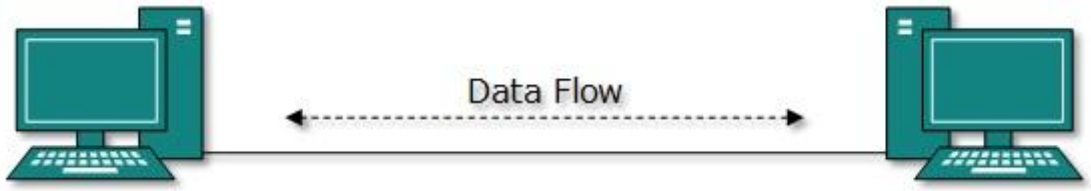
In above pictures, different VLANs are depicted in different color codes. Hosts in one VLAN, even if connected on the same Switch cannot see or speak to other hosts in different VLANs. VLAN is Layer-2 technology which works closely on Ethernet. To route packets between two different VLANs a Layer-3 device *such as Router* is required.

Computer Network Topologies

A Network Topology is the way computer systems or network equipment connected to each other. Topologies may define both physical and logical aspect of the network. Both logical and physical topologies could be same or different in a same network.

Point-to-point

Point-to-point networks contains exactly two hosts *computer or switches or routers or servers* connected back to back using a single piece of cable. Often, the receiving end of one host is connected to sending end of the other end and vice-versa.

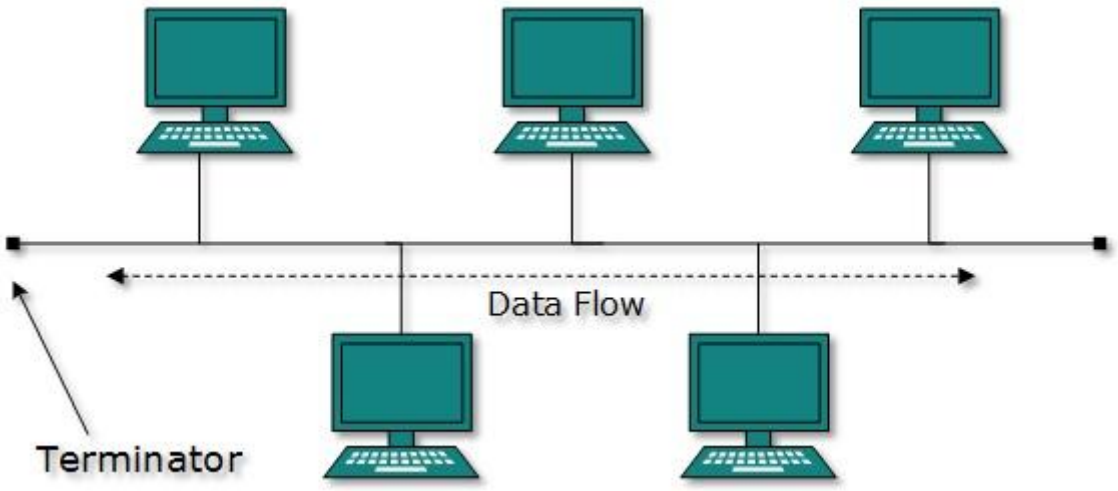


[*Image: Point-to-point Topology*]

If the hosts are connected point-to-point logically, then may have multiple intermediate devices. But the end hosts are unaware of underlying network and see each other as if they are connected directly.

Bus Topology

In contrast to point-to-point, in bus topology all device share single communication line or cable. All devices are connected to this shared line. Bus topology may have problem while more than one hosts sending data at the same time. Therefore, the bus topology either uses CSMA/CD technology or recognizes one host has Bus Master to solve the issue. It is one of the simple forms of networking where a failure of a device does not affect the others. But failure of the shared communication line make all other devices fail.

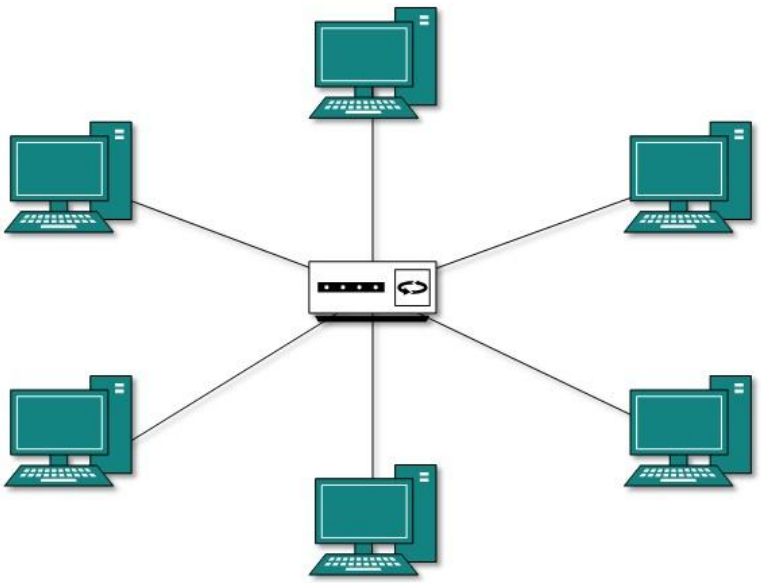


[*Image: Bus Topology*]

Both ends of the shared channel have line terminator. The data is sent in only one direction and as soon as it reaches the extreme end, the terminator removes the data from the line.

Star Topology

All hosts in star topology are connected to a central device, known as Hub device, using a point-to-point connection. That is, there exists a point to point connection between hosts and Hub. The hub device can be Layer-1 device *Hub*/*repeater* or Layer-2 device *Switch*/*Bridge* or Layer-3 device *Router*/*Gateway*.

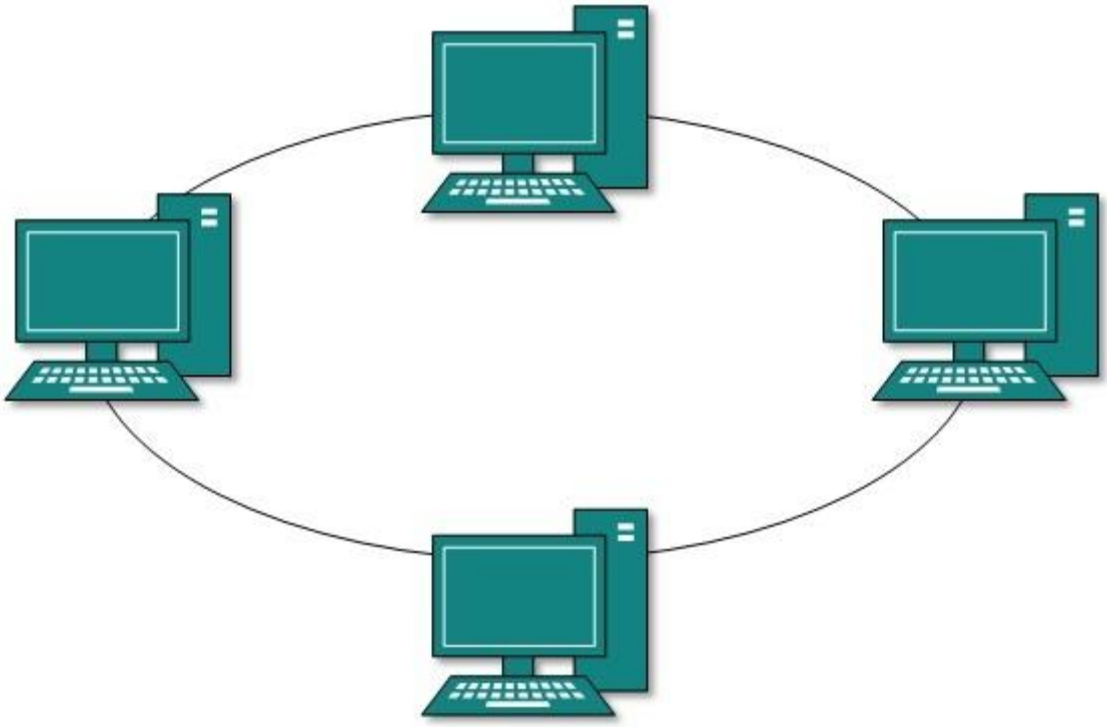


[*Image: Star Topology*]

As in bus topology, hub acts as single point of failure. If hub fails, connectivity of all hosts to all other hosts fails. Every communication happens between hosts, goes through Hub only. Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.

Ring Topology

In ring topology, each host machine connects to exactly two other machines, creating a circular network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts. To connect one more host in the existing structure administrator may need only one more extra cable.

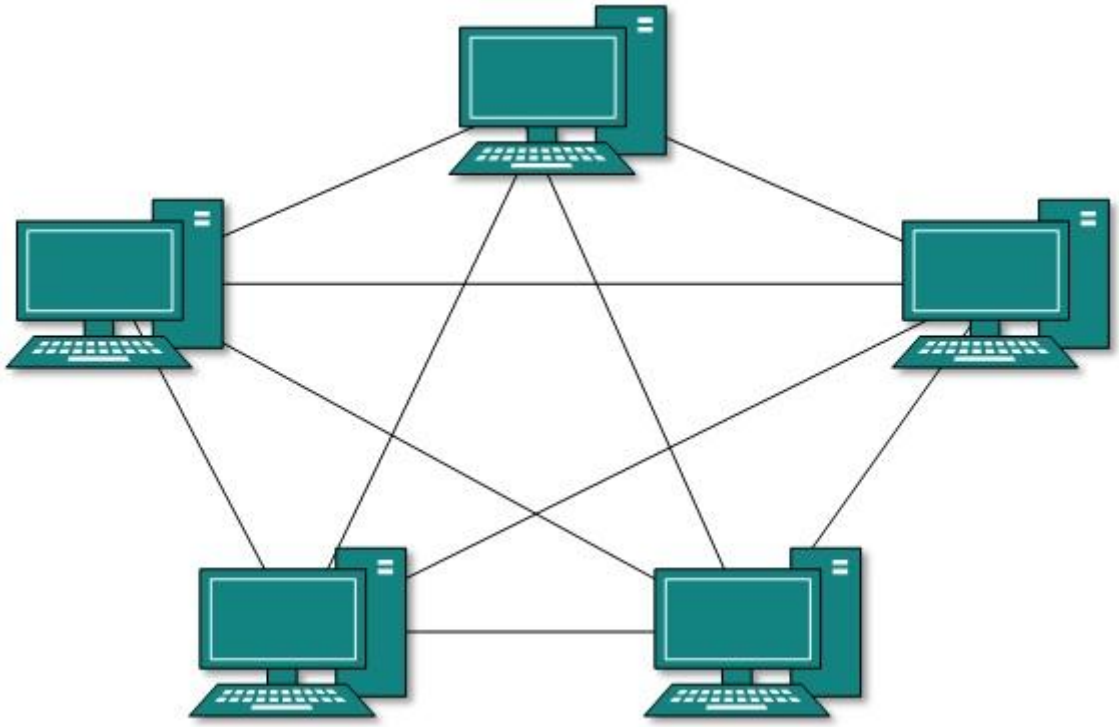


[*Image: Ring Topology*]

Failure of any host results in failure of the whole ring. Thus every connection in the ring is point of failure. There exist methods which employs one more backup ring.

Mesh Topology

In this type of topology, a host is connected to one or two or more than two hosts. This topology may have hosts having point-to-point connection to every other host or may also have hosts which are having point to point connection to few hosts only.



[*Image: Full Mesh Topology*]

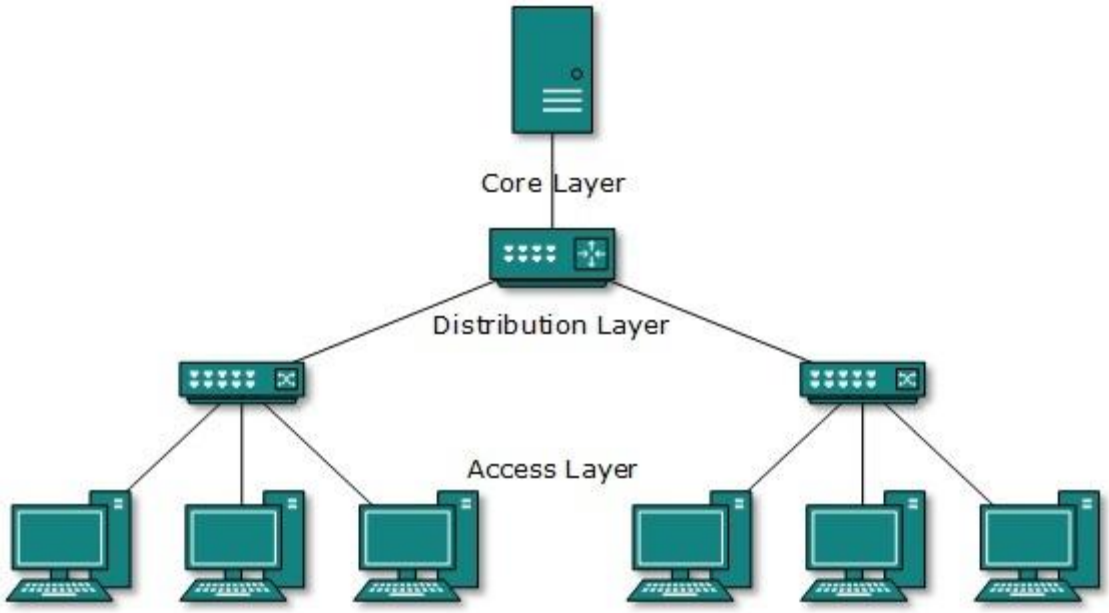
Hosts in Mesh topology also work as relay for other hosts which do not have direct point-to-point links. Mesh technology comes into two flavors:

- **Full Mesh**: All hosts have a point-to-point connection to every other host in the network. Thus for every new host n$n-1/2$ cables *connection* are required. It provides the most reliable network structure among all network topologies.
- **Partially Mesh**: Not all hosts have point-to-point connection to every other host. Hosts connect to each other in some arbitrarily fashion. This topology exists where we need to provide reliability to some host whereas others are not as such necessary.

Tree Topology

Also known as Hierarchical Topology is the most common form of network topology in use present day. This topology imitates as extended Star Topology and inherits properties of Bus topology.

This topology divides the network in to multiple levels/layers of network. Mainly in LANs, a network is bifurcated into three types of network devices. The lowest most is access-layer where user's computer is attached. The middle layer is known as distribution layer, which works as mediator between upper layer and lower layer. The highest most layers is known as Core layer, and is central point of the network, i.e. root of the tree from which all nodes fork.



[*Image: Tree Topology*]

All neighboring hosts have point-to-point connection between them. Like bus topology, if the root goes down, the entire network suffers. Though it is not the single point of failure. Every connection serves as point of failure, failing of which divides the network into unreachable segment and so on.

Daisy Chain

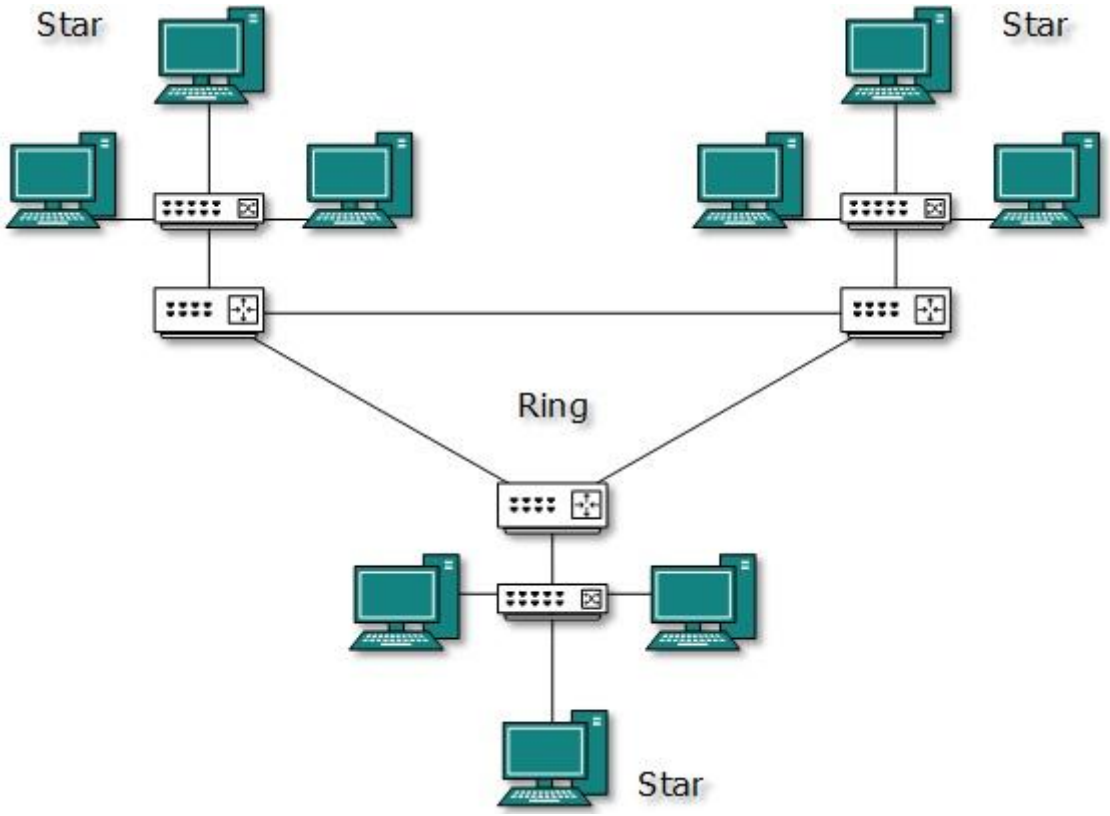
This topology connects all its hosts in a linear fashion. Similar to Ring topology, all hosts in this topology are connected to two hosts only, except the end hosts. That is if the end hosts in Daisy Chain are connected then it represents Ring topology.

[*Image: Daisy Chain Topology*]

Each link in Daisy chain topology represents single point of failure. Every link failure splits the network into two segments. Every intermediate host works as relay for its immediate hosts.

Hybrid Topology

A network structure whose design contains more than one topology is said to be Hybrid Topology. Hybrid topology inherits merits and demerits of all the incorporating topologies.



[*Image: Hybrid Topology*]

The above picture represents an arbitrarily Hybrid topology. The combining topologies may contain attributes of Star, Ring, Bus and Daisy-chain topologies. Most WANs are connected by means of dual Ring topology and networks connected to them are mostly Star topology networks. Internet is the best example of largest Hybrid topology

Computer Network Models

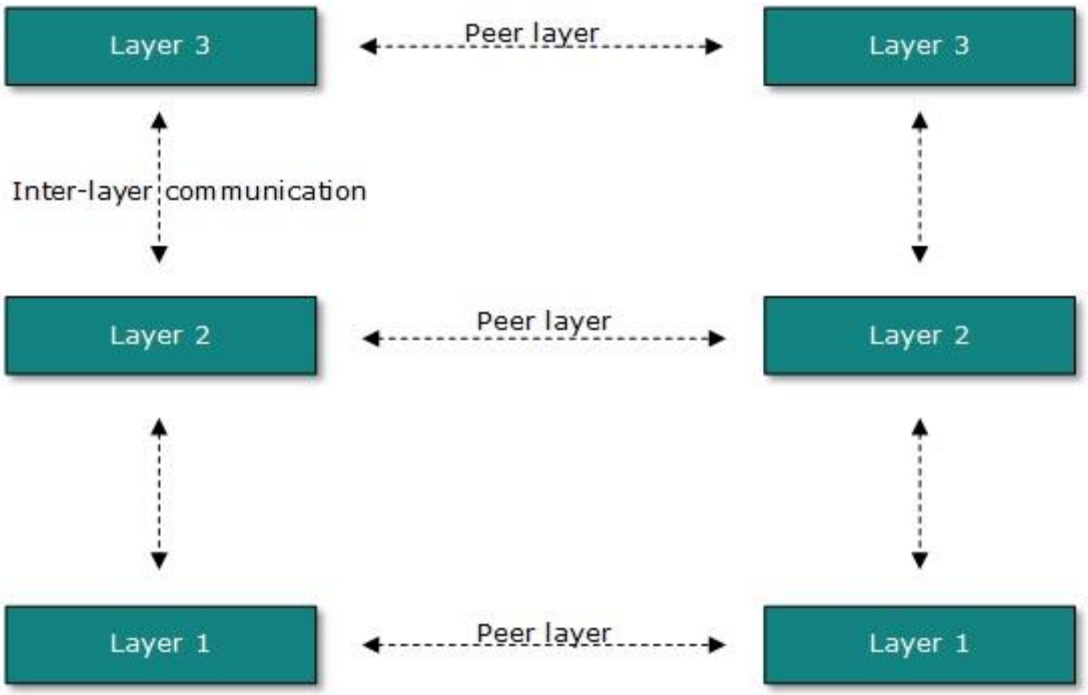
Introduction

Networking at engineering level is a complicated task. It involves software, firmware, chip level engineering, hardware and even electric pulses. To ease network engineering, the whole networking concept is divided into multiple layers. Each layer is involved in some particular task and is independent of all other layers. But as a whole the almost all networking task depends on all of these layers. Layers share data between them and they depend on each other only to take input and give output.

Layered tasks

In layered architecture of Network Models, 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 top most layer it is then passed on to the layer below it for further processing. The lower layer does the same thing, it processes the task and pass on to lower layer. If the task is initiated by lowest most layer the reverse path is taken.



[*Image: Layered Tasks*]

Every layer clubs together all procedures, protocols, 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. This model has seven layers:

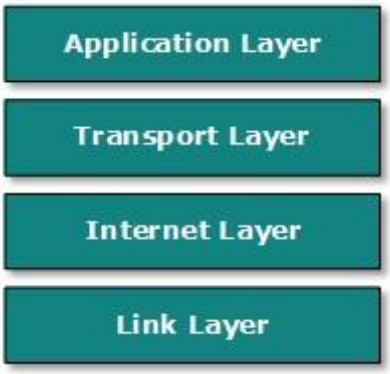
[*Image: OSI Model*]

- **Application Layer**: This layer is responsible for providing interface to the application user. This layer encompasses protocols which directly interact with the user.
- **Presentation Layer**: This layer defines how data in the native format of remote host should be presented in the native format of host.
- **Session Layer**: This layer maintains sessions between remote hosts. For example, once user/password authentication is done, the remote host maintains this session for a while and does not ask for authentication again in that time span.
- **Transport Layer**: This layer is responsible for end-to-end delivery between hosts.
- **Network Layer**: This layer is responsible for address assignment and uniquely addressing hosts in a network.
- **Data Link Layer**: This layer is responsible for reading and writing data from and onto the line. Link errors are detected at this layer.
- **Physical Layer**: This layer defines the hardware, cabling and wiring, power output, pulse rate etc.

Internet Model

Internet uses TCP/IP protocol suite, also known as Internet suite. This defines Internet Model which contains four layered architecture. OSI Model is general communication model but

Internet Model is what Internet uses for all its communication. Internet is independent of its underlying network architecture so is its Model. This model has the following layers:



[*Image: Internet Model*]

- **Application Layer**: This layer defines the protocol which enables user to internet with the network such as FTP, HTTP etc.
- **Transport Layer**: This layer defines how data should flow between hosts. Major protocol at this layer is Transmission Control Protocol. This layer ensures data delivered between hosts is in-order and is responsible for end to end delivery.
- **Internet Layer**: IP works on this layer. This layer facilitates host addressing and recognition. This layer defines routing.
- **Link Layer**: This layer provides mechanism of sending and receiving actual data. But unlike its OSI Model's counterpart, this layer is independent of underlying network architecture and hardware.

Computer Network - Security

Introduction

When first networking was used, it was limited to Military and Universities for Research and development purposes. Later when all networks merge together and formed Internet, user's data use to travel through public transit network, where users are not scientists or computer science scholars. Their data can be highly sensitive as bank's credentials, username and passwords, personal documents, online shopping or secret official documents.

All security threats are intentional i.e. they occur only if intentionally triggered. Security threats can be divided into the below mentioned categories:

- **Interruption:**

  Interruption is a security threat in which availability of resources is attacked. For example, a user is unable to access its web-server or the web-server is hijacked.

- **Privacy-breach:**

  In this threat, the privacy of a user is compromised. Someone, who is not the authorized person is accessing or intercepting data sent or received by the original authenticated user.

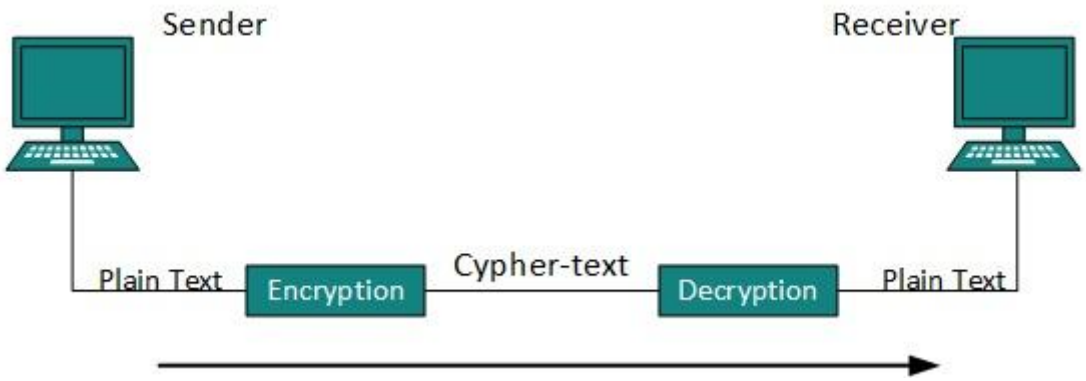
- **Integrity:**

  This type of threat includes any alteration or modification in the original context of communication. The attacker intercepts and receives the data sent by the Sender and the attacker then either modifies or generates false data and sends to the receiver. The receiver receives data assuming that it is being sent by the original Sender.

- **Authenticity:**

  When an attacker or security breather, represents himself as if he is the authentic person and access resources or communicate with other authentic users.

No technique in the present world can provide 100% security. But steps can be taken to secure data while it travels in unsecured network or internet. The most widely used technique is Cryptography.



[*Image: Cryptography*]

Cryptography is a technique to encrypt the plain-text data which makes it difficult to understand and interpret. There are several cryptographic algorithm available present day as described below:

- Secret Key
- Public Key
- Message Digest

Secret Key Encryption

Both sender and receiver have one secret key. This secret key is used to encrypt the data at sender's end. After encrypting the data, it is then sent on the public domain to the receiver. Because the receiver knows and has the Secret Key, the encrypted data packets can easily be decrypted.

Example of secret key encryption is DES. In Secret Key encryption it is required to have a separate key for each host on the network making it difficult to manage.

Public Key Encryption

In this encryption system, every user has its own Secret Key and it is not in the shared domain. The secret key is never revealed on public domain. Along with secret key, every user has its own but public key. Public key is always made public and is used by Senders to encrypt the data. When the user receives the encrypted data, he can easily decrypt it by using its own Secret Key.

Example of public key encryption is RSA.

Message Digest

In this method, the actual data is not sent instead a hash value is calculated and sent. The other end user, computes its own hash value and compares with the one just received. The both hash values matches, it is accepted otherwise rejected.

Example of Message Digest is MD5 hashing. It is mostly used in authentication where user's password is cross checked with the one saved at Server.