**Data Communication/Computer Network**

****

## 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.

## 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 e-mails and FTP.
* Information sharing by using Web or Internet.
* Interaction with other users using dynamic web pages.
* Video Conferences
* Parallel computing
* Instant Messaging

**Advantages of a Network**

* Simultaneous Access
* Shared Peripheral Devices
* Personal Communication
* Easier Data Backup

**Types of Teleconference**

* Videoconferencing
* Audio-conferencing
* Data-conferencing

**Videoconferencing :**

* Videoconferencing enables real-time communication over a distance by allowing people at two or more sites to communicate with each other by seeing a video picture of the people at the other sites. Each site has one or more cameras, microphones, loudspeakers, and monitors.

**Audio-conferencing :**

* Audio conferencing provides an audio link similar to that of conventional telephone, except that it offers much higher quality audio and enables more than two sites to be linked together.

**Data-conferencing:**

* Data –conferencing enables participants at two or more sites to have a shared workspace on their computer desktops. Data conferencing is often used in conjunction with video or audio-conferencing and can be useful when users at different sites want to work together on documents.

**VoIP (Voice over Internet Protocol):**

* VoIP systems bypass the need for the cost of regular telephone service by using the company’s internal network to send and receive phone calls.
* VoIP transmits the sound of your voice over a computer network using the IP rather than sending the signal over traditional phone wires

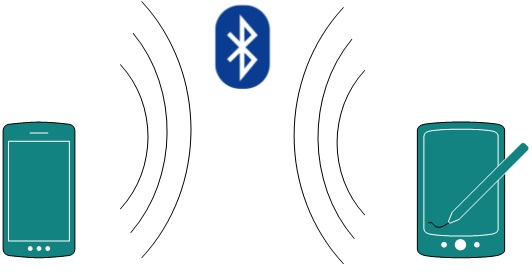
# Computer Network Types

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(PAN)

A Personal Area Network or simply PAN

the 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.



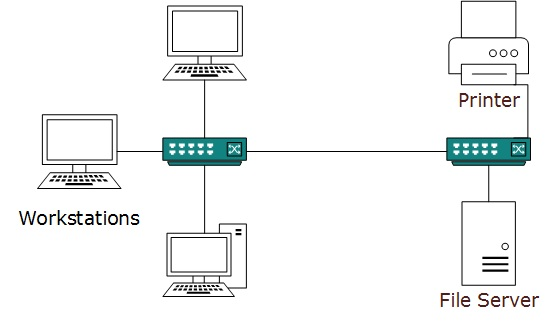
[*Image: Personal Area Network | Bluetooth*]

Piconet 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.

A local area network (LAN) is a computer network that connects computers and devices in a limited geographical area (less than a few KM).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*]

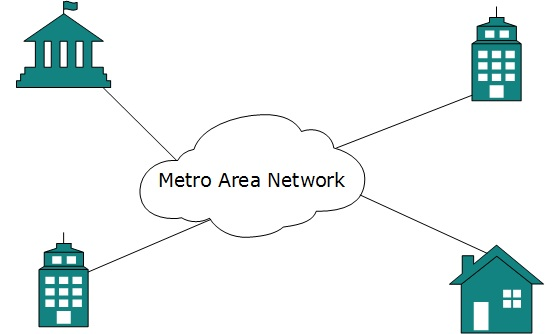
Local Area Networks are composed of inexpensive networking and routing equipment. It may contains local servers serving file storage and other locally shared applications. It mostly operates on private IP addresses and generally do not involve heavy routing. LAN works under its own local domain and controlled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

## Metropolitan Area Network

MAN, generally expands throughout a city such as cable TV network.

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.

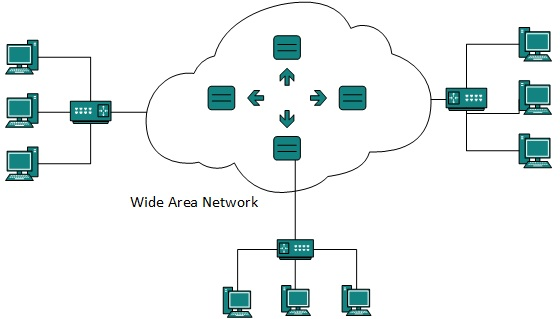


[*Image: Metropolitan Area Network*]

Backbone of MAN is high-capacity and high-speed fiber optics. MAN 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 provides 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:

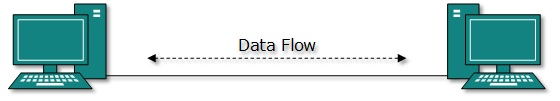
* Web sites
* E-mail
* Instant Messaging
* Blogging
* Social Media
* Marketing
* Networking
* Resource Sharing
* Audio and Video Streaming

# 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.

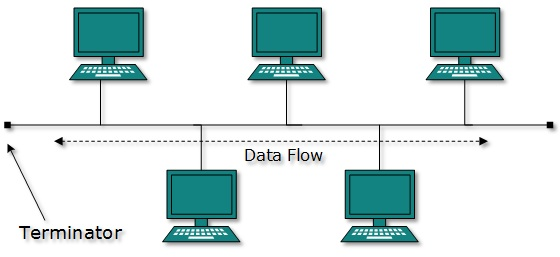


[*Image: Point-to-point Topology*]

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. 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.

**Merits & Demerits of Bus Topology**

**Merits**

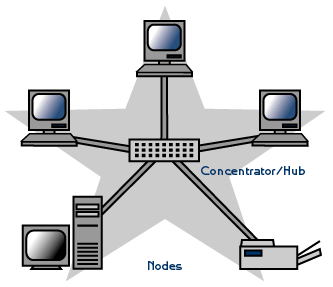
* Bus topologies are relatively easy to install
* Requires less cabling.
* Best suited for small networks.

**Demerits**

* Many devices connect to a single cable "backbone". If the backbone is broken, the entire segment fails.
* The cable length is limited. This limits the number of stations that can be connected.
* Terminators are required at both ends of the backbone cable.
* Difficult to identify the problem if the entire network shuts down

## 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.

**Merits & Demerits of Star Topology**

**Merits**

 Easy to install and wire.

 No disruptions to the network when connecting or removing devices.

 Easy to detect faults and to remove parts.

**Demerits**

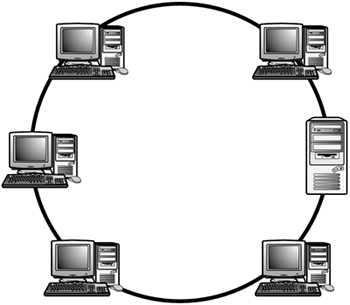
The network operation depends on the functioning of the central hub. Hence, the failure of the central hub leads to the failure of the entire network.

Requires more cable.

More expensive than bus topologies because of the cost of the hubs, etc.

## 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.

## Merits & Demerits of Ring Topology

## Merits

## Less cable required

## The data being transmitted between two nodes passes through all the intermediate nodes. A central server is not required for the management of this topology.

## Demerits

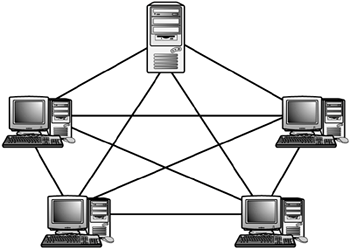
## The movement or changes made to network nodes affects the performance of the entire network.

## Messages propagate in one direction only

## The network fails if a single node fails

## 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 hosts or may also have hosts which are having point to point connection to few hosts only.



[*Image: Full Mesh Topology*]

**Merits & Demerits of Mesh Topology**

**Merits**

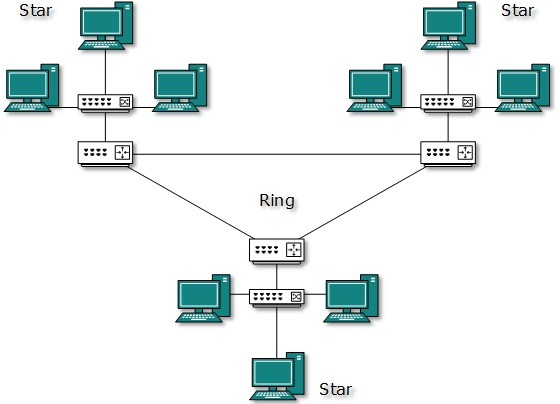
* The arrangement of the network nodes is such that it is possible to transmit data from one node to many other nodes at the same time.
* If any cable fails, there are many other ways for two nodes to communicate.

**Demerits**

* Mesh topology uses *lots* of cables to connect every node with every other node. It is very expensive to wire up.

## 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 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

# Network Linking Devices

# Hub - A hub is a connection device for networks. Allows multiple segments or computers to connect and share packets of information.

# Bridge - A bridge is a device that connects two LANs or two segments of the same LAN.

# Switches - A switch is a small hardware device that joins multiple computers together within one local area network (LAN).

# Router - A router is an electronic device that interconnects two or more computer networks, and selectively interchanges packets of data between them. It helps to select the best route to transmit the data.

# Computer Network Models

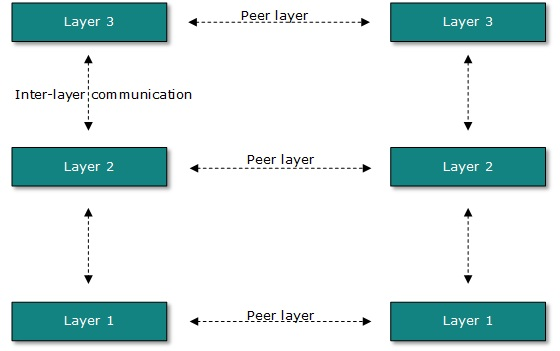
## Introduction

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.

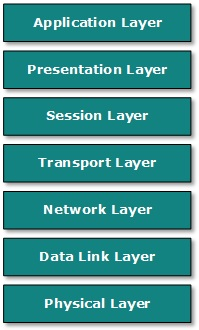


[*Image: Layered Tasks*]

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 interacts with the user. This layer defines the protocol which enables user to internet with the network such as FTP, HTTP etc.
* **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. 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.
* **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. 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.

## 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.

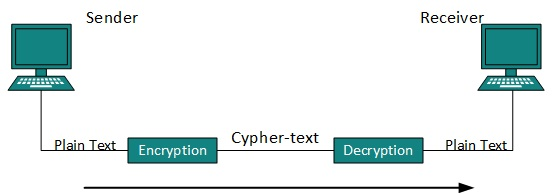
* **Integrity:**

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 generate false data and sends to the receiver. The receiver receive data assuming that it is being sent by the original Sender.

* **Authenticity:**

When an attacker or security breacher, 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.