BASICS OF COMPUTER NETWORKS

Open system:
A system which is connected to the network and is ready for communication.
Closed system:
A system which is not connected to the network and can't be communicated with.
Computer Network:
An interconnection of multiple devices, also known as hosts, that are connected using multiple paths for the purpose of sending/receiving data or media. Computer networks can also include multiple devices/mediums which help in the communication between two different devices; these are known as **Network devices** and include things such as routers, switches, hubs, and bridges.
Network Topology:
The layout arrangement of the different devices in a network. Common examples include: Bus, Star, Mesh, Ring, and Daisy chain.

OSI:
OSI stands for **Open Systems Interconnection**. It is a reference model that specifies standards for communications protocols and also the functionalities of each layer.
Protocol:
A protocol is the set of rules or algorithms which define the way how two entities can communicate across the network and there exists different protocol defined at each layer of the OSI model. Few of such protocols are TCP, IP, UDP, ARP, DHCP, FTP and so on.
UNIQUE IDENTIFIERS OF NETWORK
Host name:
Each device in the network is associated with a unique device name known as Hostname.
Type "hostname" in the command prompt(Administrator Mode) and press 'Enter', this displays the hostname of your machine.
IP Address (Internet Protocol address):
Also known as the Logical Address, the IP Address is the network address of the system across the network.
To identify each device in the world-wide-web, the Internet Assigned Numbers Authority (IANA) assigns an IPV4 (Version 4) address as a unique identifier to each device on the Internet.
The length of an IPv4 address is 32-bits, hence, we have 2^{32} IP addresses available. The length of an IPv6 address is 128-bits.

Type "ipconfig" in the command prompt and press 'Enter', this gives us the IP address of the device.

MAC Address (Media Access Control address):

Also known as physical address, the MAC Address is the unique identifier of each host and is associated with its NIC (Network Interface Card).

A MAC address is assigned to the NIC at the time of manufacturing.

The length of the MAC address is : 12-nibble/ 6 bytes/ 48 bits

Type "ipconfig/all" in the command prompt and press 'Enter', this gives us the MAC address.

Port:

A port can be referred to as a logical channel through which data can be sent/received to an application. Any host may have multiple applications running, and each of these applications is identified using the port number on which they are running.

A port number is a 16-bit integer, hence, we have 2^{16} ports available which are categorized as shown below:

Port Types	Range
Well known Ports	0 – 1023
Registered Ports	1024 – 49151
Ephemeral Ports	49152 – 65535

Number of ports: 65,536

Range: 0 – 65535

*Type "**netstat -a**" in the command prompt and press 'Enter', this lists all the ports being used.*

Socket:

The unique combination of IP address and Port number together are termed as Socket.

Other related concepts

DNS Server:

DNS stands for **Domain Name system**.

DNS is basically a server which translates web addresses or URLs (ex: www.google.com) into their corresponding IP addresses. We don't have to remember all the IP addresses of each and every website.

The command '**nslookup**' gives you the IP address of the domain you are looking for. This also provides the information of our DNS Server.
ARP:
ARP stands for **Address Resolution Protocol**.
It is used to convert an IP address to its corresponding physical address(i.e., MAC Address).
ARP is used by the Data Link Layer to identify the MAC address of the Receiver's machine.
RARP:
RARP stands for **Reverse Address Resolution Protocol**.
As the name suggests, it provides the IP address of the device given a physical address as input. But RARP has become obsolete since the time DHCP has come into the picture.
This article is contributed by **Kundana Thiyari**. If you like GeeksforGeeks and would like to contribute, you can also write an article using contribute.geeksforgeeks.org or mail your article to contribute@geeksforgeeks.org. See your article appearing on the GeeksforGeeks main page and help other Geeks.
Please write comments if you find anything incorrect, or you want to share more information about the topic discussed above.

Goals of Networks

Computer Network means an interconnection of autonomous (standalone) computers for information exchange. The connecting media could be a copper wire, optical fiber, microwave, or satellite.

Networking Elements – The computer network includes the following networking elements:
1. At least two computers
2. Transmission medium either wired or wireless
3. Protocols or rules that govern the communication
4. Network software such as Network Operating System

Network Criteria:
The criteria that have to be met by a computer network are:
1. Performance – It is measured in terms of transit time and response time.
- Transit time is the time for a message to travel from one device to another

- Response time is the elapsed time between an inquiry and a response.

Performance is dependent on the following factors:

- The number of users
- Type of transmission medium
- Capability of connected network
- Efficiency of software

2. Reliability – It is measured in terms of

- Frequency of failure
- Recovery from failures
- Robustness during catastrophe

3. Security – It means protecting data from unauthorized access.

Goals of Computer Networks: The following are some important goals of computer networks:

1. **Resource Sharing –**
   Many organization has a substantial number of computers in operations, which are located apart. Ex. A group of office workers can share a common printer, fax, modem, scanner, etc.

2. **High Reliability –**
   If there are alternate sources of supply, all files could be replicated on two or more machines. If one of them is not available, due to hardware failure, the other copies could be used.

3. **Inter-process Communication –**
   Network users, located geographically apart, may converse in an interactive session through the network. In order to permit this, the network must provide almost error-free communications.

4. **Flexible access –**
   Files can be accessed from any computer in the network. The project can be begun on one computer and finished on another. Other goals include Distribution of processing functions, Centralized management, and allocation of network resources, Compatibility of dissimilar equipment and software, Good network performance, Scalability, Saving money, Access to remote information, Person to person communication, etc.

Types of Network Topology

The arrangement of a network which comprises of nodes and connecting lines via sender and receiver is referred as network topology. The various network topologies are :

a) Mesh Topology :
In mesh topology, every device is connected to another device via particular channel.

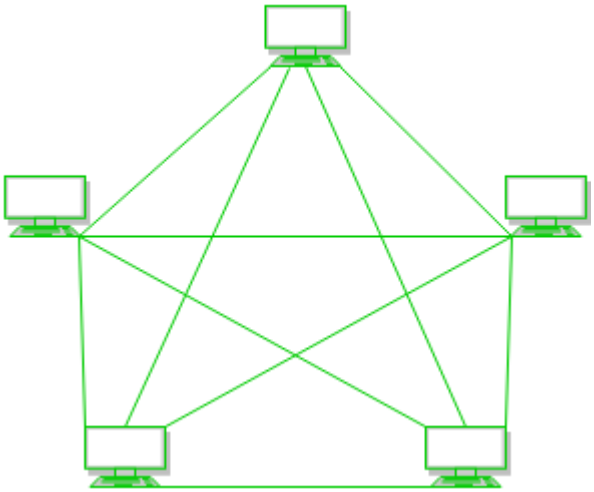

Figure 1 : Every device is connected with another via dedicated channels. These channels are known as links.

- If suppose, N number of devices are connected with each other in mesh topology, then total number of ports that is required by each device is ? N-1. In the Figure 1, there are 5 devices connected to each other, hence total number of ports required is 4.
- If suppose, N number of devices are connected with each other in mesh topology, then total number of dedicated links required to connect them is ${}^{N}C_{2}$ i.e. N(N-1)/2. In the Figure 1, there are 5 devices connected to each other, hence total number of links required is 5*4/2 = 10.

Advantages of this topology :
- It is robust.
- Fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

Problems with this topology :
- Installation and configuration is difficult.

- Cost of cables are high as bulk wiring is required, hence suitable for less number of devices.
- Cost of maintenance is high.

b) Star Topology :

? In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node. The hub can be passive ?in nature i.e. not intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as active ?hubs. Active hubs have repeaters in them.

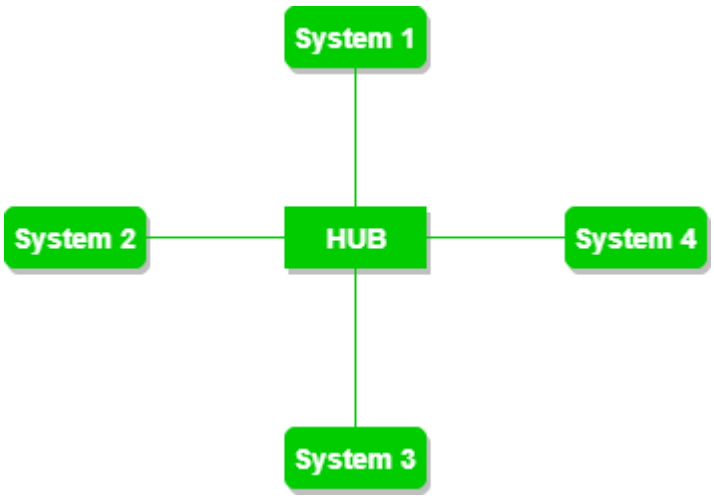

Figure 2 : A star topology having four systems connected to single point of connection i.e. hub.

Advantages of this topology :

- If N devices are connected to each other in star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device require only 1 port i.e. to connect to the hub.

Problems with this topology :

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- Cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

c) Bus Topology :

? Bus topology is a network type in which every computer and network device is connected to single cable. It transmits the data from one end to another in single direction. No bi-directional feature is in bus topology. It is multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

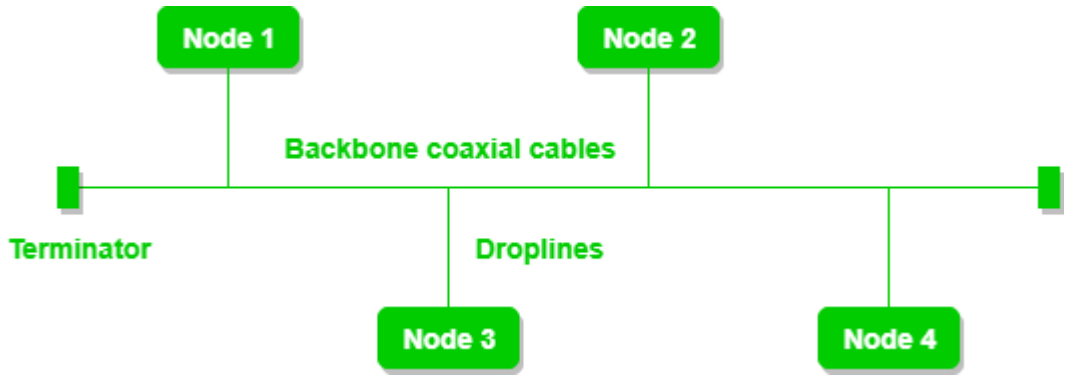

Figure 3 : A bus topology with shared backbone cable. The nodes are connected to the channel via drop lines.

Advantages of this topology :

- If N devices are connected to each other in bus topology, then the number of cables required to connect them is 1 ?which is known as backbone cable and N drop lines are required.
- Cost of the cable is less as compared to other topology, but it is used to built small networks.

Problems with this topology :

- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD etc.

d) Ring Topology :

In this topology, it forms a ring connecting devices with its exactly two neighboring devices.

A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.

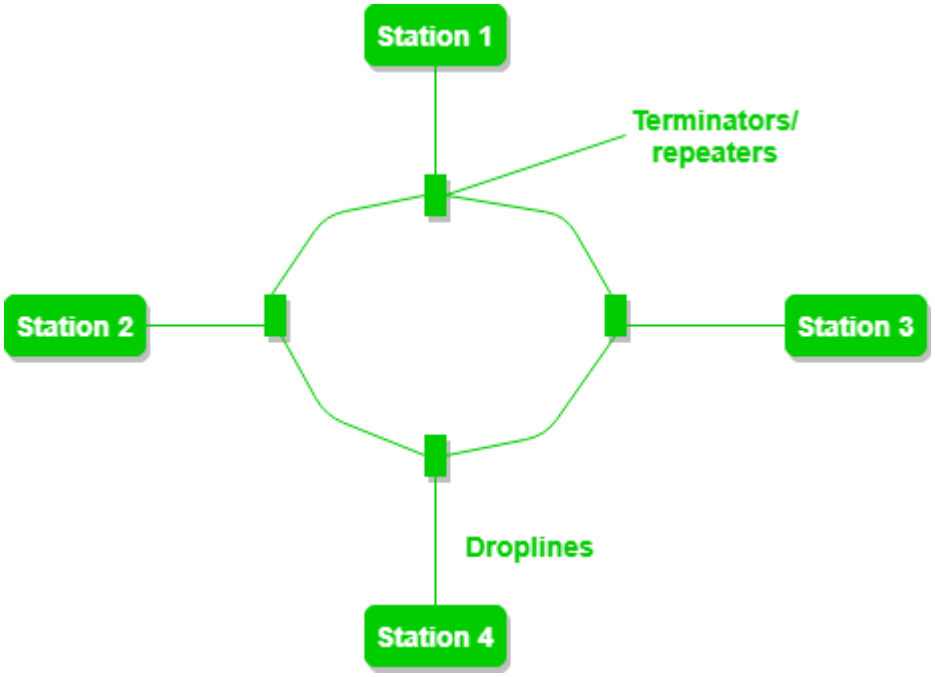

Figure 4 : A ring topology comprises of 4 stations connected with each forming a ring..
The following operations takes place in ring topology are :

1. One station is known as **monitor** station which takes all the responsibility to perform the operations.
2. To transmit the data, station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
3. When no station is transmitting the data, then the token will circulate in the ring.
4. There are two types of token release techniques : **Early token release** releases the token just after the transmitting the data and **Delay token release** releases the token after the acknowledgement is received from the receiver.

Advantages of this topology :

- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.

Problems with this topology :

- Troubleshooting is difficult in this topology.
- Addition of stations in between or removal of stations can disturb the whole topology.

e) Tree Topology :
? This topology is the variation of Star topology. This topology have hierarchical flow of data.

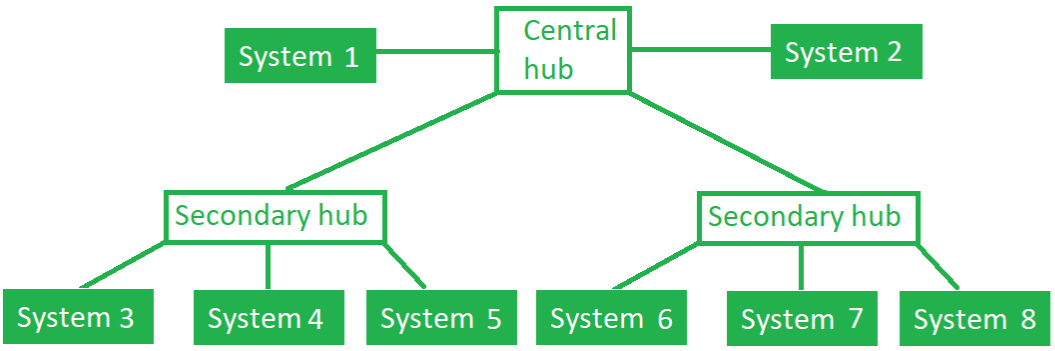

Figure 5 : In this the various secondary hubs are connected to the central hub which contains the repeater. In this data flow from top to bottom i.e from the central hub to secondary and then to the devices or from bottom to top i.e. devices to secondary hub and then to the central hub. It is multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

Advantages of this topology :

- It allows more devices to be attached to a single central hub thus it increases the distance that is travel by the signal to come to the devices.
- It allows the network to get isolate and also prioritize from different computers.

Problems with this topology :

- If the central hub gets fails the entire system fails.
- The cost is high because of cabling.

Types of area networks – LAN, MAN and WAN

The **Network** allows computers to **connect and communicate** with different computers via any medium. LAN, MAN and WAN are the three major types of the network designed to operate over the area they cover. There are some similarities and dissimilarities between them. One of the major differences is the geographical area they cover, i.e. **LAN** covers the smallest area; **MAN** covers an area larger than

LAN and **WAN** comprises the largest of all.
There are other types of Computer Networks also, like :

- PAN (Personal Area Network)
- SAN (Storage Area Network)
- EPN (Enterprise Private Network)
- VPN (Virtual Private Network)

Local Area Network (LAN) –

LAN or Local Area Network connects network devices in such a way that personal computer and workstations can share data, tools and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol. Private addresses are unique in relation to other computers on the local network. Routers are found at the boundary of a LAN, connecting them to the larger WAN.
Data transmits at a very fast rate as the number of computers linked are limited. By definition, the connections must be high speed and relatively inexpensive hardware (Such as hubs, network adapters and Ethernet cables). LANs cover smaller geographical area (Size is limited to a few kilometers) and are privately owned. One can use it for an office building, home, hospital, schools, etc. LAN is easy to design and maintain. A Communication medium used for LAN has twisted pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized.

Early LAN's had data rates in the 4 to 16 Mbps range. Today, speeds are normally 100 or 1000 Mbps. Propagation delay is very short in a LAN. The smallest LAN may only use two computers, while larger LANs can accommodate thousands of computers. A LAN typically relies mostly on wired connections for increased speed and security, but wireless connections can also be part of a LAN. The fault tolerance of a LAN is more and there is less congestion in this network. For example : A bunch of students playing Counter Strike in the same room (without internet).

Metropolitan Area Network (MAN) –

MAN or Metropolitan area Network covers a larger area than that of a LAN and smaller area as compared to WAN. It connects two or more computers that are apart but resides in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). MAN is designed for customers who need a high-speed connectivity. Speeds of MAN

ranges in terms of Mbps. It’s hard to design and maintain a Metropolitan Area Network.

The fault tolerance of a MAN is less and also there is more congestion in the network. It is costly and may or may not be owned by a single organization. The data transfer rate and the propagation delay of MAN is moderate. Devices used for transmission of data through MAN are: Modem and Wire/Cable. Examples of a MAN are the part of the telephone company network that can provide a high-speed DSL line to the customer or the cable TV network in a city.

Wide Area Network (WAN) –
WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. A WAN could be a connection of LAN connecting to other LAN’s via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high speed and relatively expensive.
There are two types of WAN: Switched WAN and Point-to-Point WAN. WAN is difficult to design and maintain. Similar to a MAN, the fault tolerance of a WAN is less and there is more congestion in the network. A Communication medium used for WAN is PSTN or Satellite Link. Due to long distance transmission, the noise and error tend to be more in WAN.

WAN’s data rate is slow about a 10th LAN’s speed, since it involves increased distance and increased number of servers and terminals etc. Speeds of WAN ranges from few kilobits per second (Kbps) to megabits per second (Mbps). Propagation delay is one of the biggest problems faced here. Devices used for transmission of data through WAN are: Optic wires, Microwaves and Satellites. Example of a Switched WAN is the asynchronous transfer mode (ATM) network and Point-to-Point WAN is dial-up line that connects a home computer to the Internet.

Conclusion –
There are many advantages of LAN over MAN and WAN, such as LAN’s provide excellent reliability, high data transmission rate, they can easily be managed, and shares peripheral devices too. Local Area Network cannot cover cities or towns and for that

Metropolitan Area Network is needed, which can connect city or a group of cities together. Further, for connecting Country or a group of Countries one requires Wide Area Network.