

Module 3: Data Communications & Computer Networks

1. Components:

- Data Communication is defined as exchange of data between two devices via some form of transmission media such as a cable, wire or it can be air or vacuum also. For occurrence of data communication, communicating devices must be a part of communication system made up of a combination of hardware or software devices and programs.
- Data communication refers to the exchange of data between devices over a transmission medium such as a wire cable. It involves the following components:

Data Communication System Components :

There are mainly five components of a data communication system:

1. Message
2. Sender
3. Receiver
4. Transmission Medium
5. Set of rules (Protocol)

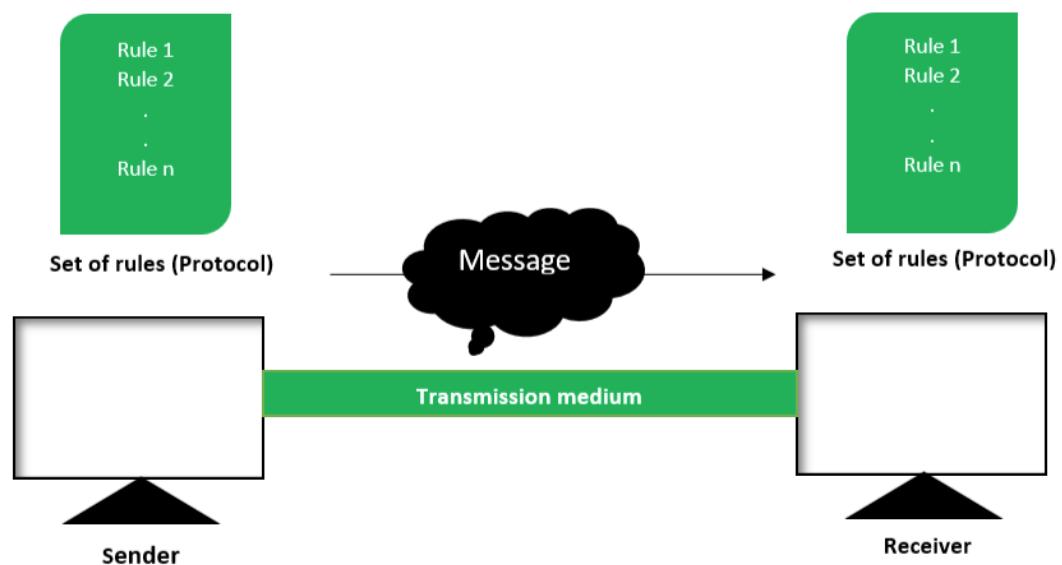


Figure – Components of Data Communication System

Key Components:

- **Message:** The information or data to be communicated.
- **Sender:** The device that sends the message (e.g., a computer or a smartphone).
- **Receiver:** The device that receives the message (e.g., another computer or smartphone).
- **Transmission Medium:** The physical path by which the message travels from sender to receiver (e.g., twisted-pair cables, fiber-optic cables, or wireless).
- **Protocol:** A set of rules that govern data communication (e.g., TCP/IP).

1. **Message :**

This is most useful asset of a data communication system. The message simply refers to data or piece of information which is to be communicated. A message could be in any form, it may be in form of a text file, an audio file, a video file, etc.

2. **Sender :**

To transfer message from source to destination, someone must be there who will play role of a source. Sender plays part of a source in data communication system. It is simple a device that sends data message. The device could be in form of a computer, mobile, telephone, laptop, video camera, or a workstation, etc.

3. **Receiver :**

It is destination where finally message sent by source has arrived. It is a device that receives message. Same as sender, receiver can also be in form of a computer, telephone mobile, workstation, etc.

4. **Transmission Medium :**

In entire process of data communication, there must be something which could act as a bridge between sender and receiver, Transmission medium plays that part. It is physical path by which data or message travels from sender to receiver. Transmission medium could be guided (with wires) or unguided (without wires), for example, twisted pair cable, fiber optic cable, radio waves, microwaves, etc.

5. **Set of rules (Protocol) :**

To govern data communications, various sets of rules had been already designed by the designers of the communication systems, which represent a kind of agreement between communicating devices. These are defined as protocol. In simple terms, the protocol is a set of rules that govern data communication. If two different devices are connected but there is

no protocol among them, there would not be any kind of communication between those two devices. Thus the protocol is necessary for data communication to take place.

Data Representation:

Information today comes in different forms such as text, numbers, images, audio, and video.

Text:

In data communications, text is represented as a bit pattern, a sequence of bits (0s or 1s). Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding. Today, the prevalent coding system is called Unicode, which uses 32 bits to represent a symbol or character used in any language in the world. The American Standard Code for Information Interchange (ASCII), developed some decades ago in the United States, now constitutes the first 127 characters in Unicode and is also referred to as Basic Latin.

Numbers:

Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations. Appendix B discusses several different numbering systems.

Images:

Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot

Audio:

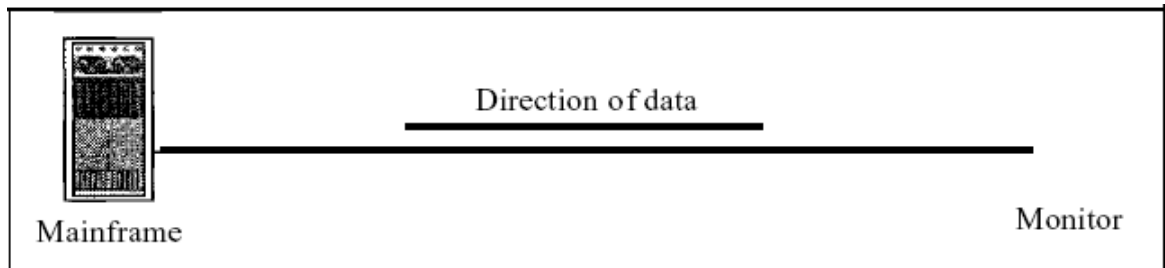
Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continuous, not discrete

Video:

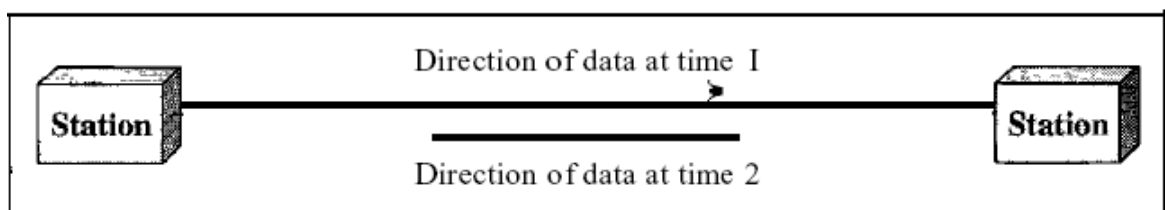
Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion. Again we can change video to a digital or an analog signal.

Data Flow:

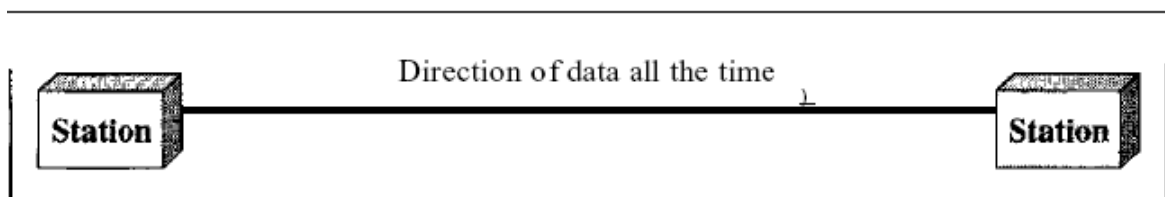
Communication between two devices can be simplex, half-duplex, or full-duplex as shown in Figure



a. Simplex



b. Half-duplex



c. Full-duplex

Simplex:

In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive (see Figure a). Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

Half-Duplex:

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is like a one-lane road with traffic allowed in both directions.

When cars are traveling in one direction, cars going the other way must wait. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems.

The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

Full-Duplex:

In full-duplex both stations can transmit and receive simultaneously. One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.

NETWORKS: Network Criteria, Physical Structures

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.

- **Distributed Processing**

Most networks use distributed processing, in which a task is divided among multiple computers. Instead of one single large machine being responsible for all aspects of a process, separate computers (usually a personal computer or workstation) handle a subset.

Network Criteria

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

Performance:

Performance can be measured in many ways, including transit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software. Performance is often evaluated by two networking metrics:

throughput and delay. We often need more throughput and less delay. However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

Reliability:

In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

Security:

Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

Physical Structures:

Type of Connection

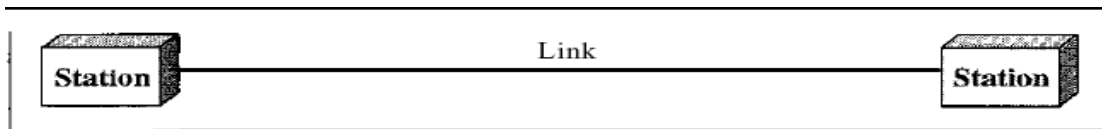
A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For visualization purposes, it is simplest to imagine any link as a line drawn between two points. For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections: point-to-point and multipoint.

1.Point-to-Point:

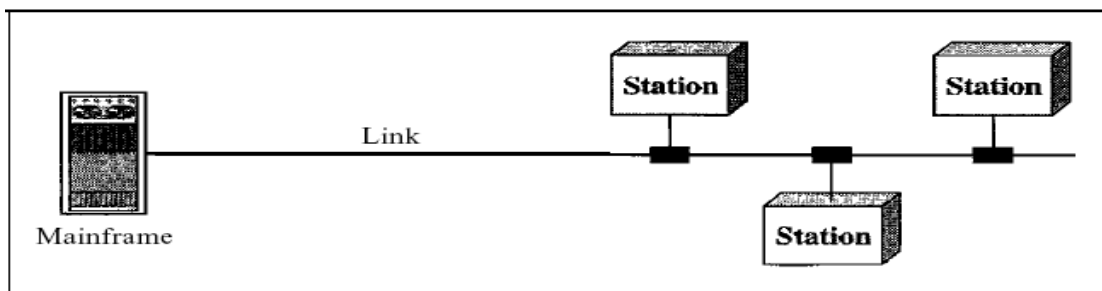
A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite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

2. Multipoint:

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



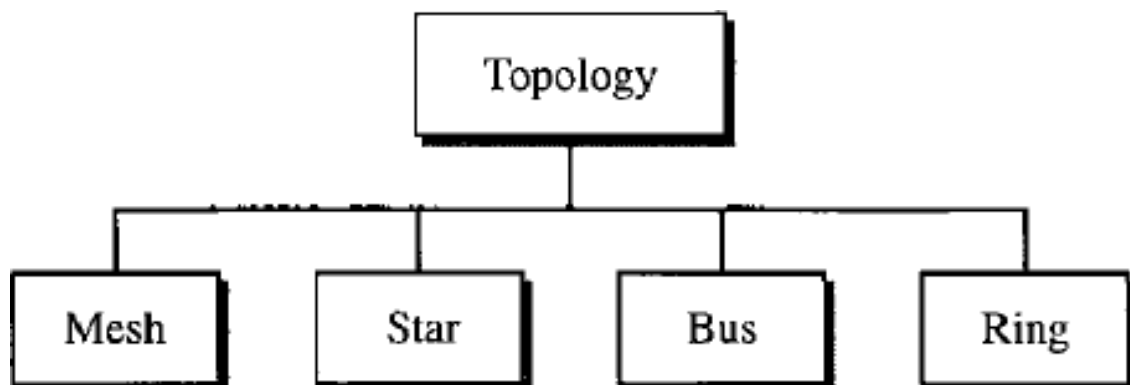
a. Point-to-point



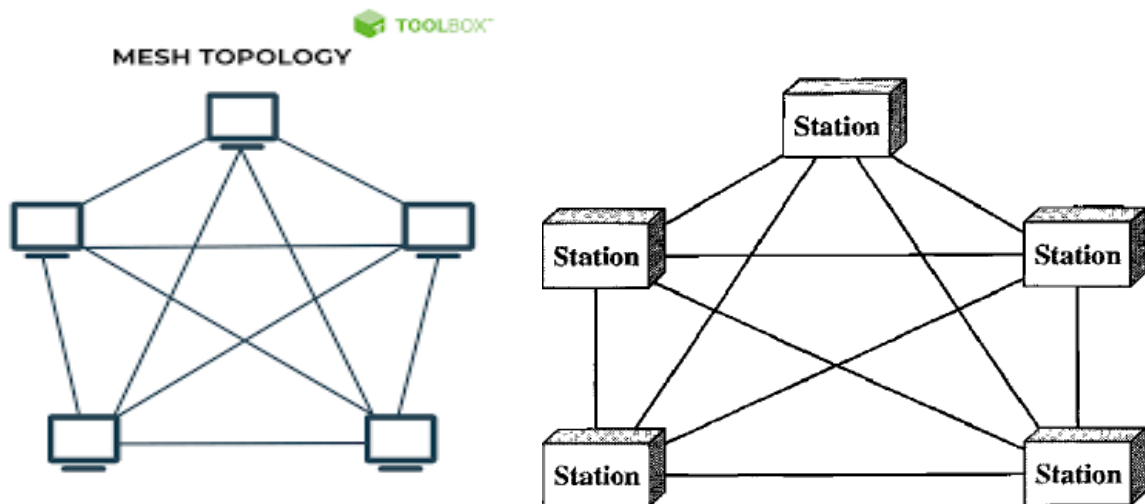
b. Multipoint

Physical Topology

The term *physical topology* refers to the way in which a network is laid out physically. One or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies possible: mesh, star, bus, and ring.



Mesh: In a mesh topology, every device has a dedicated point-to-point link to every other device. The term *dedicated* means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to $n - 1$ nodes, node 2 must be connected to $n - 1$ nodes, and finally node n must be connected to $n - 1$ nodes. We need $n(n - 1)$ physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need $n(n - 1) / 2$ duplex-mode links. To accommodate that many links, every device on the network must have $n - 1$ input/output (VO) ports to be connected to the other $n - 1$ stations.



Advantages:

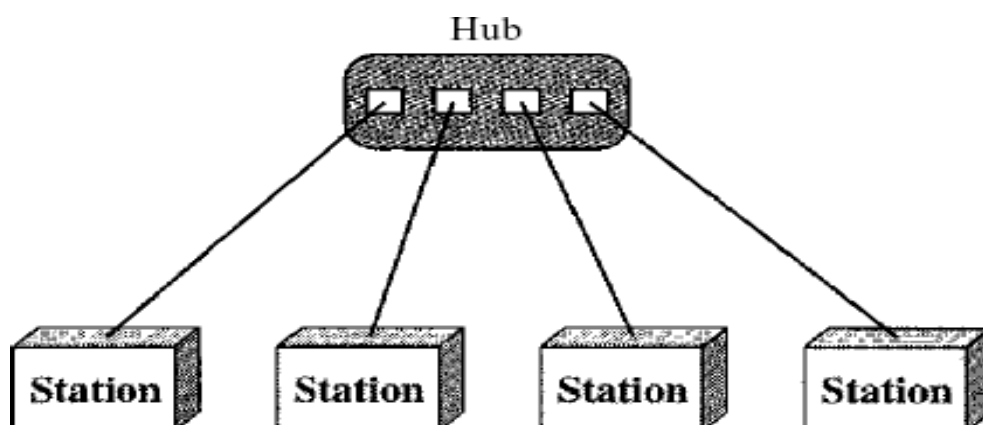
- The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
- A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system. Third, there is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages. Finally, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

Disadvantages:

- Disadvantage of a mesh are related to the amount of cabling because every device must be connected to every other device, installation and reconnection are difficult.
- Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate. Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

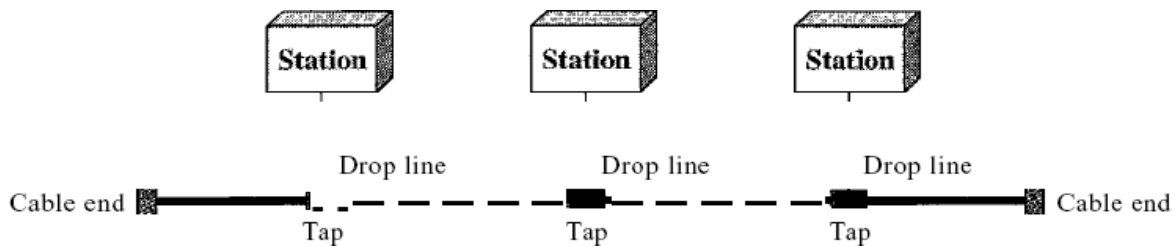
Star Topology:

- In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device .
- A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure.
- Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.
- One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead. Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).



Bus Topology:

The preceding examples all describe point-to-point connections. A **bus topology**, on the other hand, is multipoint. One long cable acts as a **backbone** to link all the devices in a network



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

Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies. In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. In a bus, this redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

Disadvantages include difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. Adding new devices may therefore require modification or replacement of the backbone.

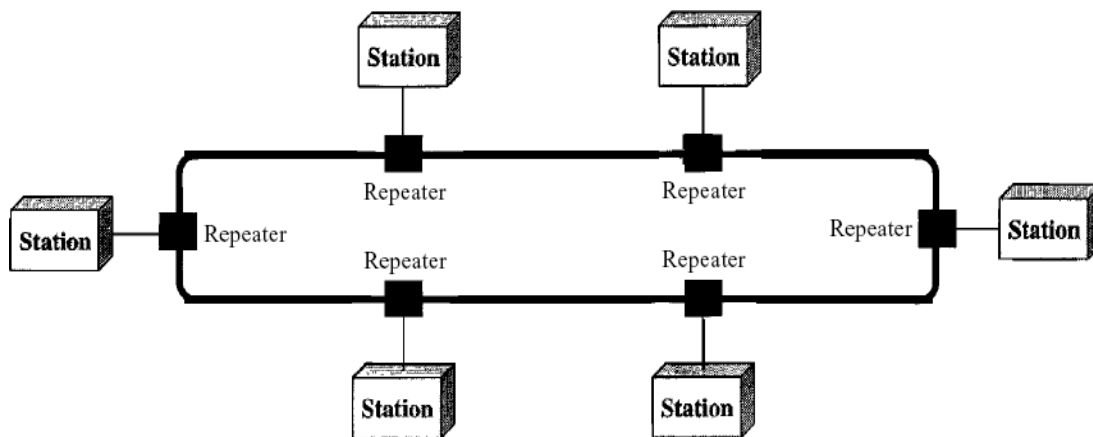
In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in

the direction of origin, creating noise in both directions.

Bus topology was the one of the first topologies used in the design of early local area networks. Ethernet LANs can use a bus topology, but they are less popular.

Ring Topology

In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

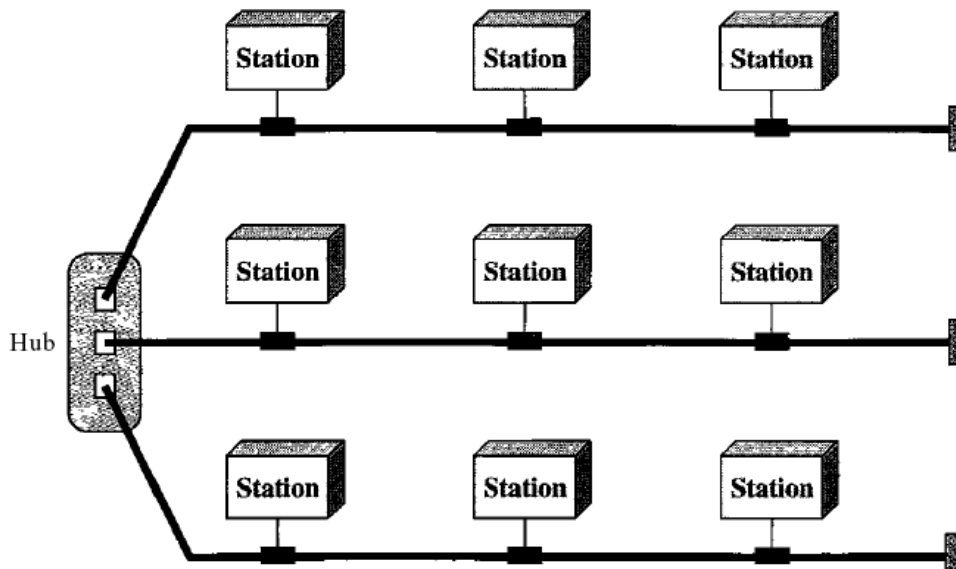


A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break. Ring topology was prevalent when IBM introduced its local-area network Token Ring. Today, the need for higher-speed LANs has made this topology less popular.

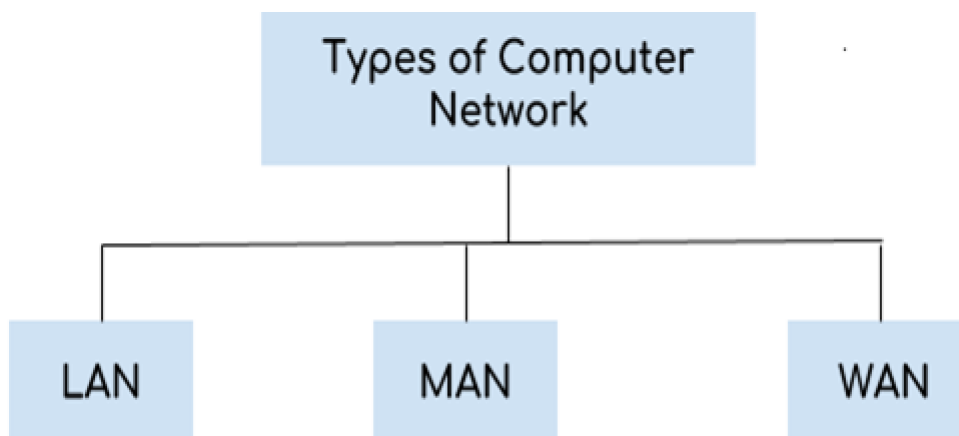
Hybrid Topology:

A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown in Figure



NETWORK TYPES / Categories of Networks

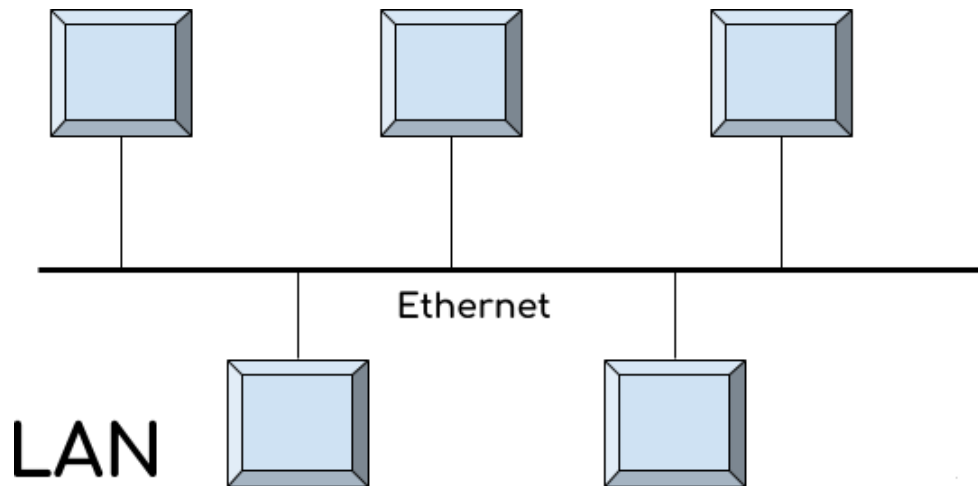
Types of Computer Network



There are mainly three types of computer networks based on their size:

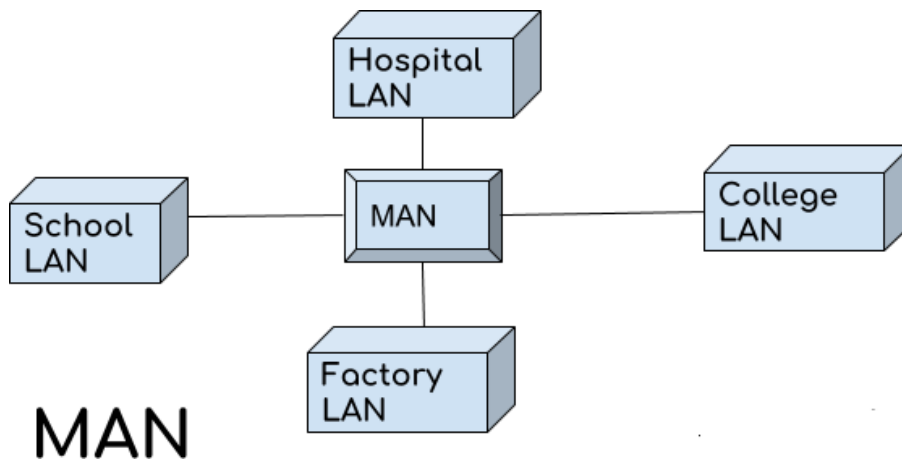
1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide area network (WAN)

1. Local Area Network (LAN)



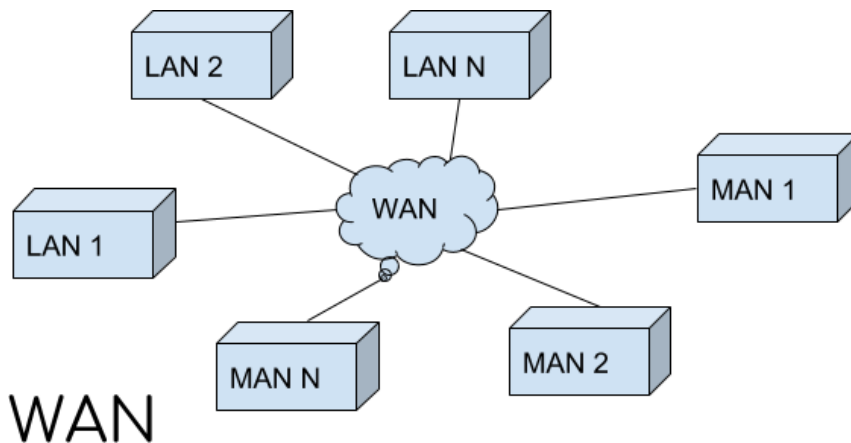
1. Local area network is a group of computers connected with each other in a small places such as school, hospital, apartment etc.
2. LAN is secure because there is no outside connection with the local area network thus the data which is shared is safe on the local area network and can't be accessed outside.
3. LAN due to their small size are considerably faster, their speed can range anywhere from 100 to 100Mbps.
4. LANs are not limited to wire connection, there is a new evolution to the LANs that allows local area network to work on a wireless connection.

2. Metropolitan Area Network (MAN)



MAN network covers larger area by connections LANs to a larger network of computers. In Metropolitan area network various Local area networks are connected with each other through telephone lines. The size of the Metropolitan area network is larger than LANs and smaller than WANs(wide area networks), a MANs covers the larger area of a city or town.

3. Wide area network (WAN)



Wide area network provides long distance transmission of data. The size of the WAN is larger than LAN and MAN. A WAN can cover country, continent or even a whole world. Internet connection is an example of WAN. Other examples of WAN are mobile broadband connections such as 3G, 4G etc.

Advantages of WAN:

- Centralized infrastructure: One of the main advantage of WAN is the that we do not need to maintain the backup and store data on local system as everything is stored online on a data centre, from where we can access the data through WAN.
- Privacy: We can setup the WAN in such a way that it encrypts the data that we share online that way the data is secure and minimises the risk of unauthorized access.
- Increased Bandwidth: With the WAN we get to choose the bandwidth based on the need, a large organization can have larger bandwidth that can carry large amount of data faster and efficiently.
- Area: A WAN can cover a large area or even a whole world through internet connection thus we can connect with the person in another country through WAN which is not possible in other type of computer networks.

Disadvantages of WAN:

- Antivirus: Since our systems are connected with the large amount of systems, there is possibility that we may unknowingly download the virus that can affect our system and become threat to our privacy and may lead to data loss.
- Expensive: Cost of installation is very high.
- Issue resolution: Issue resolution takes time as the WAN covers large area, it is really difficult to pin point the exact location where the issues raised and causing the problem.

Difference between LAN, MAN, and WAN

The following table highlights all the key differences between LAN, MAN, and WAN

| Basis of Comparison | LAN | MAN | WAN |
|-------------------------|--|--|--|
| Full Form | LAN stands for Local Area Network. | MAN stands for Metropolitan Area Network. | WAN stands for Wide Area Network. |
| Definition | It is the type of networking system in which systems are very near to each other. This system is generally in a single office, building or home. | It is a type of networking system in which two or more LANs are communicated. It is located in a vast geographical area. | This networking system has many connections, and these are associated with various companies or organizations at an equivalent time. |
| Ownership of Network | LAN is under the complete control of the owner, i.e., Private. | The ownership of the network can be private or public. | The ownership of the network can be private or public. |
| Speed | Data transmission speed is high. | Data transmission speed is average. | Data transmission speed is low. |
| Maintenance and Design | It can be easy to design and maintain. | It is tough to maintain. | It is tough to maintain. |
| Operational Speed | Its operational speed usually is 10,100 and 1000 Mbps. | Its operational speed usually is 1.5 Mbps, and it may be very at the wireless network. | Its operation is speed usually is 100 Mbps. |
| Fault Tolerance | There is higher fault tolerance in LAN. | There is smaller fault tolerance. | There is smaller fault tolerance. |
| Communication Allotment | LAN allows a small number of computers to establish a communication. | MAN allows simultaneous communication of a large number of computers. | WAN allows a very large number of computers to interact simultaneously with each other |

| | | | |
|-------------------|--|--|---|
| Congestion | In LANs, the network congestion is very low due to less number of computers | In MANs, the network congestion is high. | In WANs, the network is very high. |
| Propagation Delay | In LANs, the propagation delay is very less. | In MANs, the propagation delay is moderate. | In WANs, the propagation delay is very high. |
| Examples | Computer networks of schools, homes, offices, hospitals, etc. are the common examples of LANs. | Computer networks that spread over a small city, or town are the examples of MANs. | Computer networks that cover an entire city, or globe like internet are the examples of WANs. |

Internet History

The internet has evolved significantly since its inception:

1960s: Development of ARPANET, the precursor to the internet, funded by the U.S. Department of Defense.

1970s: Introduction of TCP/IP protocols, which became the foundation of the internet.

1980s: Expansion of the internet beyond military and academic institutions to include businesses and individuals.

1990s: The World Wide Web (WWW) was introduced, making the internet more accessible to the general public.

2000s: Rapid growth in internet usage, mobile devices, and broadband connections.

Present: The internet is an essential part of daily life, enabling communication, commerce, education, and entertainment.

1960s: ARPANET – The Birth of the Internet

- **1962:**
J.C.R. Licklider of MIT proposed the concept of an "Intergalactic Computer Network," which would later influence the creation of ARPANET.
- **1965:**
The first successful computer-to-computer communication was demonstrated between MIT and a research center in California.
- **1969:**
ARPANET (Advanced Research Projects Agency Network) was established by the U.S. Department of Defense.
 - The first message was sent from UCLA to Stanford Research Institute.
 - The system crashed after transmitting the first two letters of the word "login."

2. The Expansion and Development (1970s–1980s)

1970s: Standardization and Growth

- **1971:**
Ray Tomlinson developed the first email program, using the "@" symbol to separate the user and host names.
- **1973:**
The first international connection of ARPANET was established between the U.S. and Norway/England.
- **1974:**
TCP/IP (Transmission Control Protocol/Internet Protocol) was proposed by Vint Cerf and Bob Kahn, providing the foundation for internet communication.
- **1978:**
The first spam email was sent to ARPANET users.

1980s: From ARPANET to the Internet

- **1981:**
BITNET (Because It's Time Network) was established for academic email and file transfer.
- **1983:**
TCP/IP became the standard protocol for ARPANET, effectively creating the **Internet**.

DNS (Domain Name System) was introduced, replacing numerical IP addresses with human-readable domain names like example.com.

- **1986:**
The National Science Foundation Network (**NSFNET**) was established to connect supercomputing centers, expanding the internet beyond military and academic use.

3. The World Wide Web and Commercialization (1990s)

1990:

ARPANET was officially decommissioned.

Tim Berners-Lee developed the **World Wide Web (WWW)** while working at CERN.

He created the first web browser and web server.

1991: The World Wide Web became publicly available.

1993: Mosaic, the first widely used web browser with a graphical interface, was released. It later evolved into Netscape Navigator.

1995:

- The internet experienced rapid commercialization.
 - **Amazon** and **eBay** were launched as online marketplaces.
 - Microsoft released **Internet Explorer**.
 - **1996:**
The term "Internet of Things" (IoT) was first coined by Kevin Ashton, envisioning a future where physical objects are connected to the internet.
-

4. The Modern Internet (2000s–Present)

2000s: Rise of Social Media and Broadband

- **2004:**
Facebook was launched, followed by platforms like YouTube (2005), Twitter (2006), and Instagram (2010).
 - **2007:**
The release of the **iPhone** revolutionized mobile internet access and sparked the smartphone era.
 - **2008:**
Google launched **Chrome**, a web browser that gained significant popularity.
-

2010s: The Era of Cloud and IoT

- **Cloud Computing** emerged as a dominant technology, enabling services like Amazon Web Services (AWS), Google Cloud, and Microsoft Azure.
 - **Internet of Things (IoT)** devices like smart home appliances and wearable technology became widespread.
 - **2019:**
The rollout of **5G** technology promised faster internet speeds and lower latency, driving advancements in IoT, autonomous vehicles, and virtual reality.
-

5. The Future of the Internet

- **6G Networks:** Expected to offer even higher speeds and support advanced applications like holographic communication.
- **Quantum Internet:** Research is ongoing into creating an internet based on quantum computing principles, which could revolutionize encryption and communication.
- **Metaverse:** A fully immersive, virtual world integrating internet connectivity, VR, and AR technologies.

Key Innovations in Internet History

| Year | Innovation | Description |
|-------------|-------------------|--------------------------------|
| 1969 | ARPANET | First internet prototype |
| 1971 | Email | First email sent |
| 1983 | TCP/IP | Standardized internet protocol |
| 1990 | World Wide Web | First web browser and server |
| 1993 | Mosaic | First graphical web browser |
| 2004 | Facebook | Social media era begins |
| 2007 | iPhone | Mobile internet revolution |
| 2019 | 5G | Next-generation network |