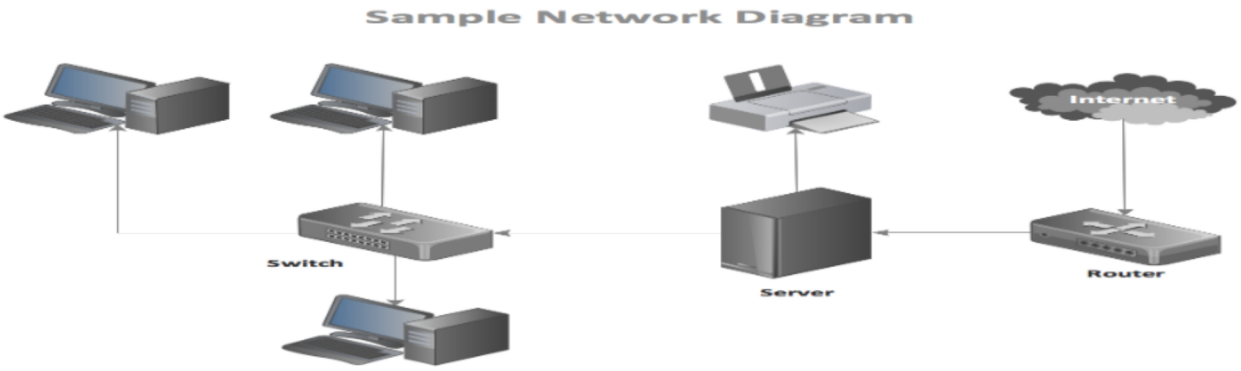
Unit 1

Basics of Network

Network concepts

- **What is network ?**



- A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to help to communication and resource-sharing .
- The shared resource can be data, a printer,a fax modem, or a service such as a database or an email system.
- All systems on the pathway must follow a set of common communication rules for data to arrive at its intended destination and for the sending and receiving systems to understand each other. The rules governing computer communication are called ***protocols*.**

communication

all networks must have the following:

. A resource to share **(resource**)
. A pathway to transfer data (**transmission medium**)
. A set of rules governing how to communicate (**protocols**)

Use of network

- **Communication :** Using a network, different people can communicate with each other all over the world. People can communicate at very low cost via e-mail, chatting, telephone, video telephone, video conferencing, groupware, and SMS services etc.
- **Sharing Resources :** In a computer network, resources such as, printers, scanners, fax machines and modems can be shared among different users. Suppose several personals computers and a laser printer are connected to a network. Each users can access the printer.
- **Sharing Software :** In a computer network, usually application programs and other software are stored on the central computer. Users connected to a network can access these programs or software.
- **Data Sharing :** In a network environment, any authorized user can access data stored on other computers on the network. For example, on the Internet, a large number of Internet users can access same database.

Unit 1

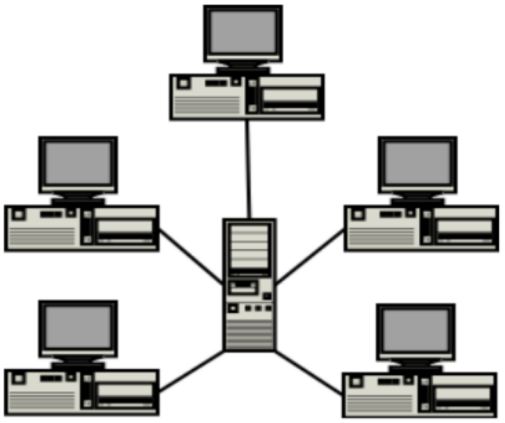
Basics of Network

Network Model

- Networks generally fall into one of two broad network categories:
  - . Peer-to-peer networks
  - . Client/server networks

  It is important to remember that one type of networking configuration is not necessarily better than another. Each type of networking model has its own strengths and weaknesses.

➢ **Client/server networks**



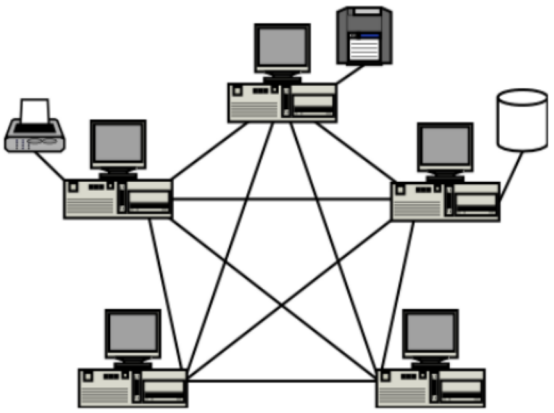
- A client/server network consists of a group of user-oriented PCs (called *clients*) that issue requests to a server.
- The client PC is responsible for issuing requests server's content or service function. Clients therefore initiate communication sessions with servers which await incoming requests.
- The server's function on the network is to service these requests. Servers generally are higher-performance systems that are optimized to provide network services to other PCs. The server machine often has a faster CPU, more memory, and more disk space than a typical client machine.
- Some examples of client/server-based networks are Novell NetWare, Windows NT Server, and Banyan Vines.
- Some common server types include file servers, mail servers, print servers, fax servers, and application servers.
- Eating at a restaurant is analogous to a client/server model. You, the customer, are a client. You issue requests for meals, drinks, anddessert. The waiter is the server. It is the waiter's job to service those requests.
- In summary, the client/server model is a network in which the role of the client is to issue requests and the role of the server is to service requests.]
- Security is relatively easy to implement with this type of network model, since you can setup a single server computer to handle all information requests or login requests for the entire network, thus you only need one username and password for each user on the network.
- Information control is also fundamentally easier with this type of network model because you can have individual server computers store all the important documents of you company on a single store.
- With the Client-Server network model, each workstation only really needs to have one theoretical connection on the network, and that connection is to the main server as illustrated in the image. Because of this, the maintenance cost for the network drops.
- The cost of this type of network is relatively high up front, not only must you purchase the server hardware, but most server software is very expensive, especially for larger networks since some software companies charge more for each client computer that will connect to the main server
- Another downside to consider is the possibility of the main server having problems. How fast must you have the network working again? If you need 24x7 operability, you should allow in your budget a second "redundant" server, so if the main server goes down, the redundant server will step in and provide services until the primary server is back up again.

Unit 1

Basics of Network

➢ Peer-to-peer networks

- Peer-to-peer networks are more commonly implemented where less then ten computers are involved and where strict security is not necessary.
- Each computer is called a *peer.* The peers share resources (such as files and printers) just like in a server-based network, although no specialized or dedicated server machines exist.
  In short, each PC can act as a client or a server.
- Small networks—usually with fewer than 10 machines—can work well in this configuration.
- Peer-to-peer networks are very cheap to implement because more than likely the Operating System software you have installed on your computers should have the ability to share items with other computers on the network, even though the feature may be limited.



- Nearly all of the most popular desktop Operating Systems have this feature, including Microsoft Windows and Apple's Mac OS, as well as Unix like OS es, such as Linux and the BSD s. So the only cost will be the networking hardware (cards, wiring, hubs or switches), and the labor to configure the workstations for this type of network sharing.
- Without a central server, it is very difficult, or nearly impossible to secure this type of network in any way.
- On a peer-to-peer network, it is also very difficult to implement a good backup system because important documents tend to be stored on different hard disks on different computers. If you do manage to implement a good backup policy, chances are great that after a while some very important documents will not get archived because someone "accidentally" saved them to the wrong location on the network.
- Peer-to-peer networks can be implemented with very little investment costs, but in order for the network to work properly, the users must be very experienced with computers, and strict guidelines must be implemented and followed in order for the data to remain secure and archived properly. In my experience, peer-to-peer networks tend to become more of a headache instead of a help after about 6 computers

Peer-to-Peer Networks vs Client/Server Networks	
Peer-to-Peer Networks	Client/Server Networks
➢ Easy to set up	➢ More difficult to set up
➢ Less expensive to install	➢ More expensive to install
➢ Can be implemented on a wide range of operating systems	➢ A variety of operating systems can be supported on the client computers, but the server needs to run an operating system that supports networking
➢ More time consuming to maintain the software being used (as computers must be managed individually)	➢ Less time consuming to maintain the software being used (as most of the maintenance is managed from the server)
➢ Very low levels of security supported or none at all. These can be very	➢ High levels of security are supported, all of which are controlled

cumbersome to set up, depending on the operating system being used	from the server. Such measures prevent the deletion of essential system files or the changing of settings
➢ Ideal for networks with less than 10 computers	➢ No limit to the number of computers that can be supported by the network
➢ Does not require a server	➢ Requires a server running a server operating system
➢ Demands a moderate level of skill to administer the network	➢ Demands that the network administrator has a high level of IT skills with a good working knowledge of a server operating system

Network services

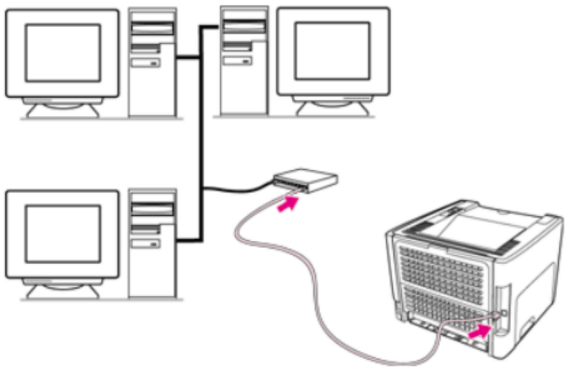
Network services are the basic reason we connect computers. Services are what a company wants to have performed or provided. Based on the services a company wants to utilize, the company purchases a specific program and operating system.

- **File service**
  - *File services* enable networked computers to share files with each other. This capability was one of the primary reasons networking of personal computers initially came about.
  - File services include all network functions dealing with the storage, retrieval, or movement of data files.
  - File services enable users to read, write, and manage files and data. This includes moving files between computers and archiving files and data.
  - File services are an important part of client/server and peer-to-peer networks. Computers providing files services are referred to as file servers
  - Two types of servers exist:
    - Dedicated : *Dedicated servers* do nothing but fulfill requests to network clients. These servers commonly are found in client/server environments
    - Non-dedicated. : *Non-dedicated servers* do double duty. They enable a user to go onto the machine acting as a file server and request the use of files from other machines; at the same time, they give files to users who request them from other computers on the network. Non-dedicated file servers often are found in peer-topeer networks.

File Transfer Services :

Most networks have some form of centralized file storage. For many years, companies have used the online storage approach to file storage. In the online storage scenario, data is stored on hard disks that are accessible on demand.

Another common approach to file storage is offline storage, which consists of removable media that are managed manually. After data is written to a tape or an optical disk, the storage medium can be removed from the server



- **Print service**:

advantages of network print services:

1. Many users can share the same printers. This capability is especially useful with expensive devices such as color printers and plotters.
2. Printers can be located anywhere, not just next to a user's PC.
3. Queue-based network printing is more efficient than direct printing because the workstation can begin to work again as soon as a job is queued to the network.
4. Modern printing services enable users to send facsimile (fax) transmissions through the network to a fax server

- Comm. service,

- Data base service :

Database servers are the most common type of application servers. Because database services enable applications to be designed in separate client and server components, such applications frequently are called client/server databases.

With a client/server database, the client and server applications are designed to take advantage of the specialized capabilities of client and database systems, as described here:

- The client application manages data input from the user, generation of screen displays, some of the reporting, and data retrieval requests sent to the database server.
- The database server manages the database files; adds, deletes, and modifies records in the database; queries the database and generates the results required by the client; and transmits results back to the client. The database server can service requests for multiple clients at the same time.

A modern database server is a sophisticated piece of software that can perform the following functions:

- Provide database security
- Optimize the performance of database operations
- Determine optimum locations for storing data without requiring clients to know where the data is located.
- Service large numbers of clients by reducing the amount of time any one client spends accessing the database.
- Distribute data across multiple database servers

Unit 1

Basics of Network

- Security service:

Another service provided by networks is security. Security is one of the most important elements involved in a network. When users share resources and data on a network, they should be able to control who can access the data or resource and what the user can do with it.

Another service provided by networks is security. Security is one of the most important elements involved in a network. When users share resources and data on a network, they should be able to control who can access the data or resource and what the user can do with it.

- Application service

Business applications, for example, often must perform complex statistical calculations beyond the scope of most desktop PCs. Statistical software with the required capabilities might need to run on a mainframe computer or on a minicomputer. The statistical package, however, can make its capabilities available to applications on users' PCs by providing an application service.

The client PC sends the calculation request to the statistics server. When the results become available, they are returned to the client. This way, only one computer in an organization needs to have the expensive software license and processing power required to calculate the statistics, but all client PCs can benefit. Application services enable organizations to install servers that are specialized for specific functions (see Figure 1.10).

Some of the more common application servers are database servers, messaging/communication servers, groupware servers, and directory servers. Application servers are an effective strategy for making a network more scalable. Additional application servers can be added as new application needs emerge

Network access methods

Random access: CSMA, CSMA/CD, CSMA/CA

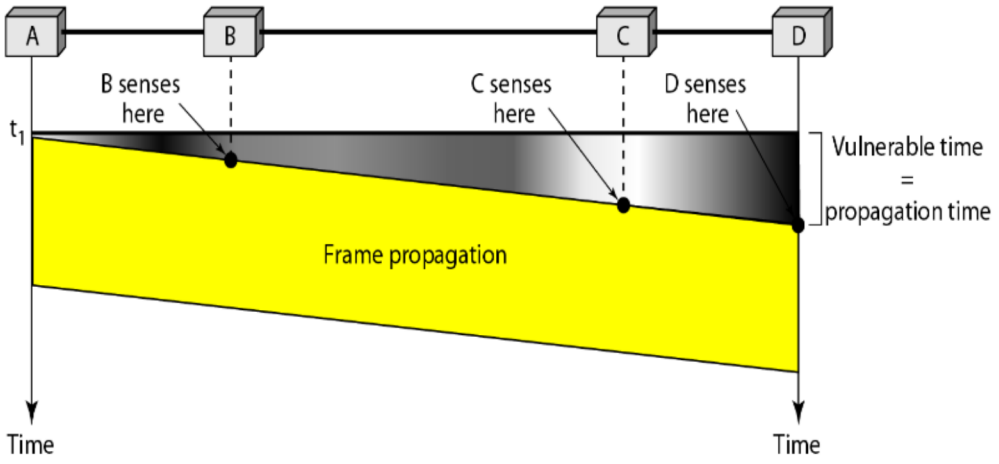
In random access or contention methods, no station is superior to another station and none is assigned the control over another. No station permits, or does not permit, another station to send. At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send. This decision depends on the state of the medium (idle or busy).
Two features give this method its name. First, there is no scheduled time for a station to transmit. Transmission is random among the stations. That is why these methods are called *random access.* Second, no rules specify which station should send next. Stations compete with one another to access the medium.

Carrier Sense Multiple Access (CSMA)

To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed. The chance of collision can be reduced if a station senses the medium before trying to use it. Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the

state of the medium) before sending. In other words, CSMA is based on the principle "sense before transmit" or "listen before talk."

CSMA can reduce the possibility of collision, but it cannot eliminate it.
The vulnerable time for CSMA is the propagation time T_p. This is the time needed for a signal to propagate from one end of the medium to the other.



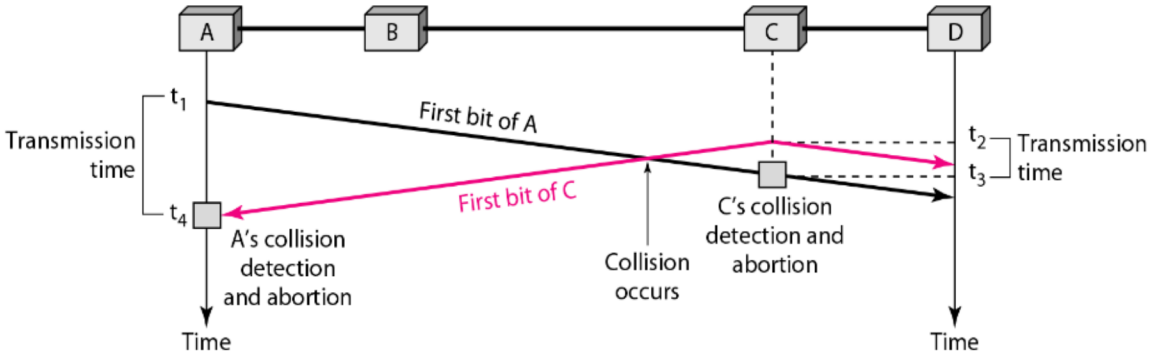
When a station sends a frame, and any other station tries to send a frame during this time, a collision will result. But if the first bit of the frame reaches the end of the medium, every station will already have heard the bit and will refrain from sending.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

The CSMA method does not specify the procedure following a collision. Carrier senses multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.

In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again.

To better understand CSMA/CD, let us look at the first bits transmitted by the two stations involved in the collision. Although each station continues to send bits in the frame until it detects the collision, we show what happens as the first bits collide. In Figure, stations A and C are involved in the collision.



At time t_1, station A has executed its procedure and starts sending the bits of its frame. At time t_2, station C has not yet sensed the first bit sent by A.
Station C executes its procedure and starts sending the bits in its frame, which propagate both to the left and to the right. The collision occurs sometime after time t_2. Station C detects a collision at time t_3 when it receives the first bit of A's frame.
Station C immediately

(or after a short time, but we assume immediately) aborts transmission. Station A detects collision at time *t4* when it receives the first bit of C's frame; it also immediately aborts transmission.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

Carrier sense multiple access with collision avoidance *(CSMAICA)* was invented for this network.
prior to transmitting, a node first listens to the shared medium (such as listening for wireless signals in a wireless network) to determine whether another node is transmitting or not.
if another node was heard, we wait for a period of time for the node to stop transmitting before listening again for a free communications channel.

In this case, the sender transmits first a short RTS (request to send) control packet, indicating the total time required to transmit the data and the acknowledgment packet. When the access point receives the RTS packet, it responds by sending a CTS (Clear to send) packet including again the required time for the complete transmission

The RTS/CTS mechanism informs all stations in the range of the sender and the access point (receiver) about the planned transmission and instructs them not to send for the reserved duration. Thus it serves two purposes:

- Since the RTS and CTS packets are short, a collision will only last for the duration of the short packet. The following data and ACK packets are transmitted without collision
- The hidden station problem can be avoided, since all stations in the range of the receiver are informed about the transmission and wait until it is finished

CONTROLLED ACCESS

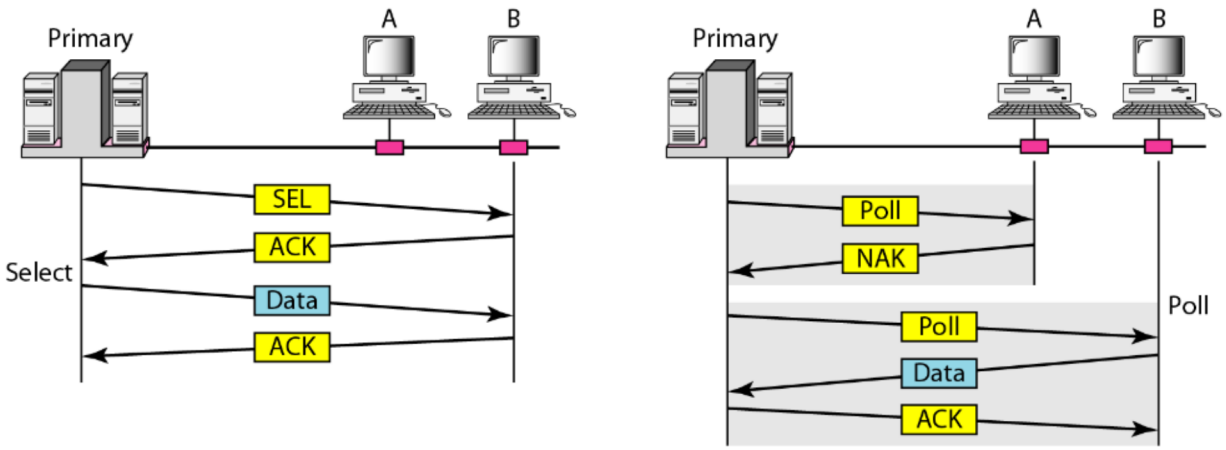
In controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations.

Polling

Polling works with topologies in which one device is designated as a primary station and the other devices are secondary stations.

All data exchanges must be made through the primary device even when the ultimate destination is a secondary device. It is up to the primary device to determine which device is allowed to use the channel at a given time. The primary device, therefore, is always the initiator of a session .

If the primary wants to receive data, it asks the secondaries if they have anything to send; this is called poll function. If the primary wants to send data, it tells the secondary to get ready to receive; this is called select function.



Select

The *select* function is used whenever the primary device has something to send. Remember that the primary controls the link. If the primary is neither sending nor receiving data, it knows the link is available.

If it has something to send, the primary device sends it. What it does not know, however, is whether the target device is prepared to receive. So the primary must alert the secondary to the upcoming transmission and wait for an acknowledgment of the secondary's ready status. Before sending data, the primary creates and transmits a select (SEL) frame, one field of which includes the address of the intended secondary.

Poll

The *poll* function is used by the primary device to solicit transmissions from the secondary devices. When the primary is ready to receive data, it must ask (poll) each device in turn if it has anything to send. When the first secondary is approached, it responds either with a NAK frame if it has nothing to send or with data (in the form of a data frame) if it does. If the response is negative (a NAK frame), then the primary polls the next secondary in the same manner until it finds one with data to send. When the response is positive (a data frame), the primary reads the frame and returns an acknowledgment (ACK frame), verifying its receipt.

Token Passing

In the token-passing method, the stations in a network are organized in a logical ring. In other words, for each station, there is a *predecessor* and a *successor.*

The predecessor is the station which is logically before the station in the ring; the successor is the station which is after the station in the ring.

The current station is the one that is accessing the channel now. The right to this access has been passed from the predecessor to the current station. The right will be passed to the successor when the current station has no more data to send.

But how is the right to access the channel passed from one station to another? In this method, a special packet called a token circulates through the ring. The possession of the token gives the station the right to access the channel and send its data. When a station has some data to send, it waits until it receives the token from its predecessor.

It then holds the token and sends its data. When the station has no more data to send, it releases the token, passing it to the next logical station in the ring. The station cannot send data until it receives the token again in the next round. In this process, when a station receives the token and has no data to send, it just passes the data to the next station.

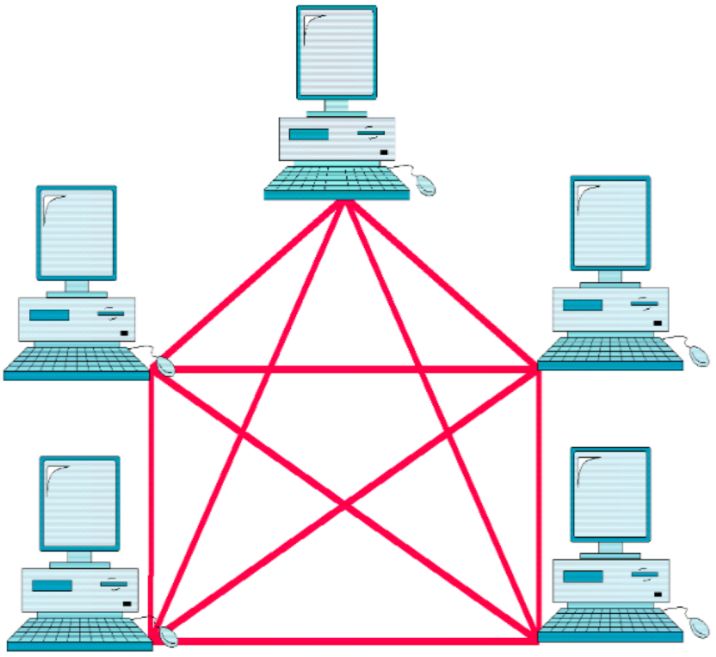
Token management is needed for this access method. Stations must be limited in the time they can have possession of the token. The token must be monitored to ensure it has not been lost or destroyed. For example, if a station that is holding the token fails, the token will disappear from the network. Another function of token management is to assign priorities to the stations and to the types of data being transmitted. And finally, token management is needed to make low-priority stations release the token to highpriority stations.

Network Topology

Mesh

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.

A mesh offers several advantages over other network topologies.



First, 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.

Second, 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.

The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required. First, 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.

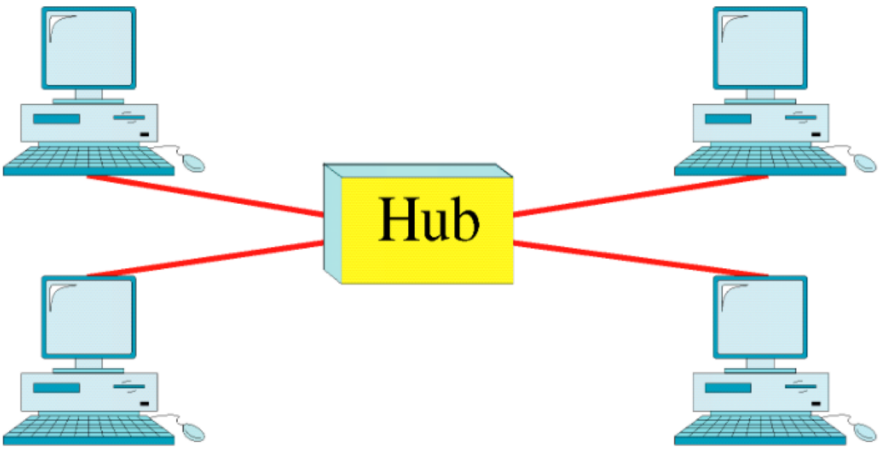
One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

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.



Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.

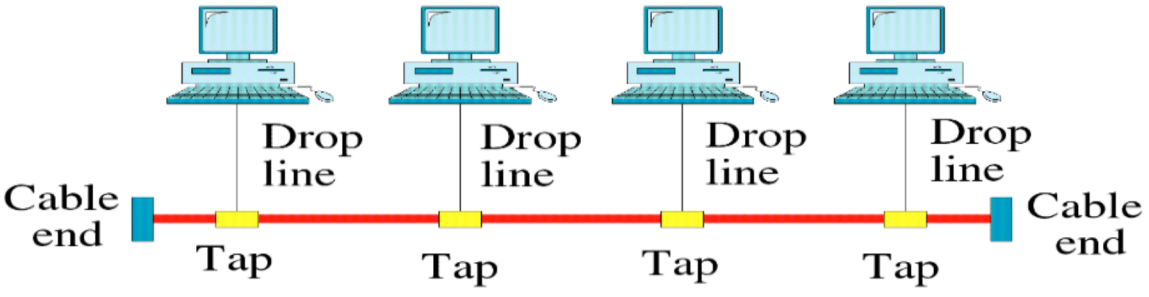
Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

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.

Bus

A **bus topology** 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.

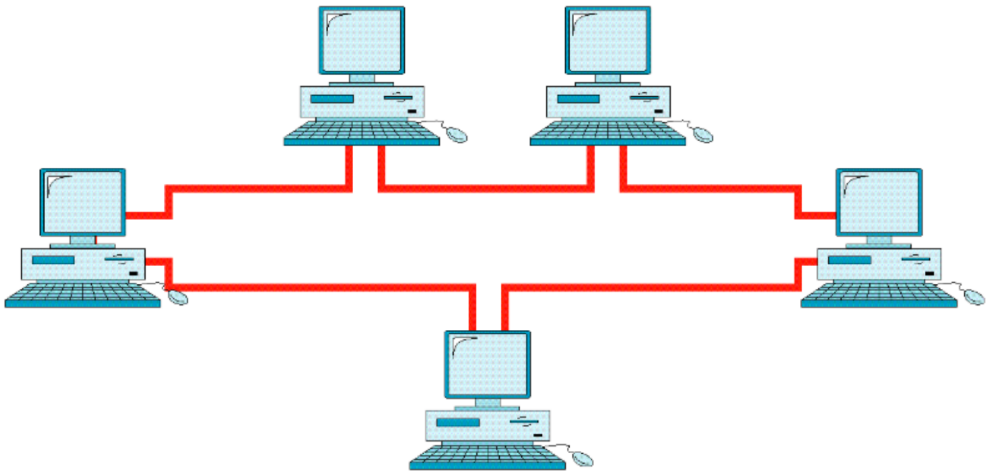
Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In a bus, this redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has 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.

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.

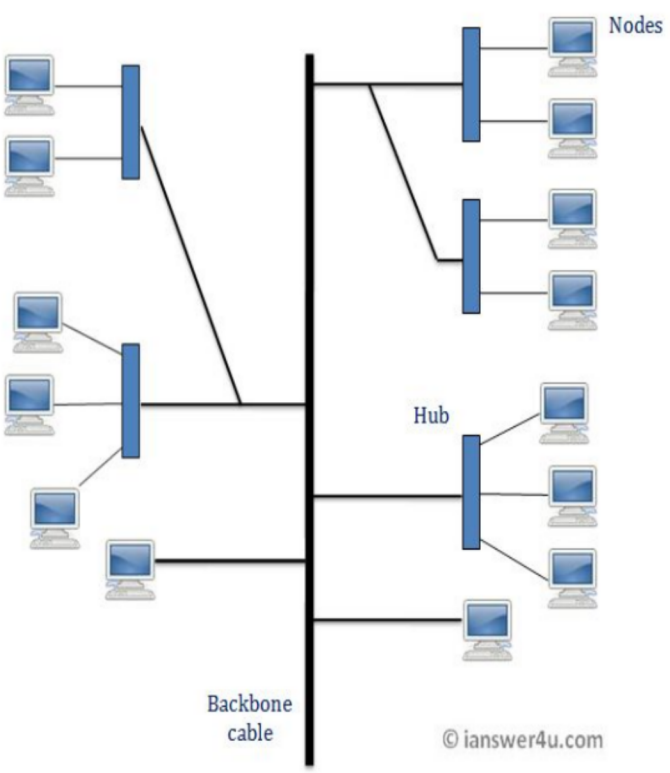
Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

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.

Tree Topology

A tree topology is essentially a combination of bus topology and star topology.

In Tree Topology, the number of Star networks are connected using Bus. This main cable seems like a main stem of a tree, and other star networks as the branches. It is also called Expanded Star Topology. Ethernet protocol is commonly used in this type of topology. The diagram below will make it clear.



Let's discuss the advantages and disadvantages of Tree Topology now

Advantages of Tree Topology

1. It is an extension of Star and bus Topologies, so in networks where these topologies can't be implemented individually for reasons related to scalability, tree topology is the best alternative.
2. Expansion of Network is possible and easy.
3. Here, we divide the whole network into segments (star networks), which can be easily managed and maintained.
4. Error detection and correction is easy.
5. Each segment is provided with dedicated point-to-point wiring to the central hub.
6. If one segment is damaged, other segments are not affected.

Disadvantages of Tree Topology

1. Because of its basic structure, tree topology, relies heavily on the main bus cable, if it breaks whole network is crippled.
2. As more and more nodes and segments are added, the maintenance becomes difficult.
3. Scalability of the network depends on the type of cable used.

Hybrid Topology

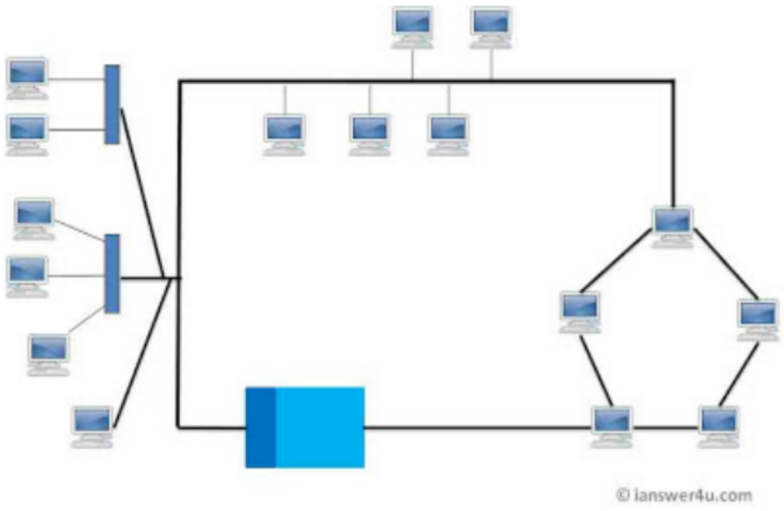
Hybrid, as the name suggests, is mixture of two different things. Similarly in this type of topology we integrate two or more different topologies to form a resultant topology which has good points(as well

as weaknesses) of all the constituent basic topologies rather than having characteristics of one specific topology. This combination of topologies is done according to the requirements of the organization.

For example, if there exists a ring topology in one office department while a bus topology in another department, connecting these two will result in Hybrid topology. Remember connecting two similar topologies cannot be termed as Hybrid topology. Star-Ring and Star-Bus networks are most common examples of hybrid network.

Advantages of Hybrid Network Topology

1) **Reliable :** Unlike other networks, fault detection and troubleshooting is easy in this type of topology. The part in which fault is detected can be isolated from the rest of network and required corrective measures can be taken, WITHOUT affecting the functioning of rest of the network.
2) **Scalable:** Its easy to increase the size of network by adding new components, without disturbing existing architecture.



3) **Flexible:** Hybrid Network can be designed according to the requirements of the organization and by optimizing the available resources. Special care can be given to nodes where traffic is high as well as where chances of fault are high.

Disadvantages of Hybrid Topology

1) **Complexity of Design:** One of the biggest drawback of hybrid topology is its design. Its not easy to design this type of architecture and its a tough job for designers. Configuration and installation process needs to be very efficient.
2) **Costly Hub:** The hubs used to connect two distinct networks, are very expensive. These hubs are different from usual hubs as they need to be intelligent enough to work with different architectures and should be function even if a part of network is down.
3) **Costly Infrastructure:** As hybrid architectures are usually larger in scale, they require a lot of cables, cooling systems, sophisticate network devices, etc.

Advance network topologies

Ethernet

Basics of Network

The IEEE 802.3 standard is popularly called as Ethernet. It is a bus based broadcast network with decentralized control. It can operate at **10 Mbps** or **100 Mbps** or above. Computers on an Ethernet can transmit whenever they want to do so. If two or more machines transmit simultaneously, then their packets collide. Then the transmitting computers just wait for an arbitrary time and retransmit their signal. There are various technologies available in the LAN market but the most popular one of them is Ethernet.

The **Ethernet topology** was developed at the University of Hawaii to connect computers on the various Islands. It was radio based design.
Ethernet is one of the most popular Computer Network or **LAN technologies** in use today covering more than 85% of the computer networks. Ethernet system consists of three basic elements:

1. ***The physical medium*** use to carry Ethernet signals between computers on the network

2. ***A set of rules (protocols)*** embedded in each Ethernet interface that will decide how multiple computers on the network will have access to the data on the medium.

3. ***An Ethernet frame*** that consists of a standardized set of bits used to carry data over the system.

The operation of Ethernet can be described in simple terms as follows:

Each computer on the Ethernet Network, also **known as a node,** operates independently of all other nodes. All nodes attached to an Ethernet are connected to a **shared medium** over which the **Ethernet signals travel serially**, one data bit at a time.

To send data a station first listens to the **channel** and when the channel is idle the station transmits its information in the form of an **Ethernet frame**, or **packet.** The Ethernet rules (protocol) are defined in such a way that every node gets a fair amount of frame transmission opportunity.

As each Ethernet frame is sent out on the **shared medium**, the Ethernet interfaces inside the node look at the **destination address.** The interfaces compare the destination address of the

frame with their own address. The Ethernet interface with the same address as the destination address in the frame will read the entire frame and all other network interfaces will ignore the information.

Ethernet Frame.

The heart of **Ethernet system is the Ethernet Frame**, which is used to deliver information between the computers. The **frame consists of a set of bits organized into several fields**. These **fields include address fields, a data field and an error checking field** that checks the integrity of the bits in the frame to make sure that the frame has arrived intact.

Advantages of Ethernet.

Ethernet's major advantages are:

1. It is an inexpensive way to achieve high speed LAN transmissions (10 to 100 MB/s)

2. It is a proven technology that supports various writing configurations.

3. It works well with a large number of LAN and micro-to-mainframe applications.

4. It is easy to install.

Disadvantages of Ethernet Cabling

The Ethernet cabling ahs the following disadvantages:

1. Ethernet is **not a high-level performer** in high-load environments. This protocol (CSMA/CD: Carrier Sense Multiple Access/Collision Detection) can slow down dramatically if hundreds of workstations are competing for the same cabling trunk.

2. Its linear bus cabling system can sometimes make it difficult to isolate problems.

CDDI: Copper Data Distribution Interface

CDDI uses cabling, which is unshielded twisted pair cables (UTP) made of copper. CDDI also uses the same protocols and constructs as FDDI, but uses copper wire as the medium.

The logical topology used in CDDI is a ring-based token network. CDDI does not use the IEEE 802.5 Token Ring Protocol, but derives from the IEEE 802.4 Token Bus Timed Token Protocol. This network can support thousands of users or terminals as well as cover a wide geographical area.

CDDI is not widely applied due to the decrease in the price of fiber optic installation, which has greater efficiency, a much higher bandwidth and an immunity to interference. Data transfer in CDDI has a throughput of 100 Mbps when using a redundancy architecture.

CDDI is the same networking system as FDDI, although the medium for the transmission is copper twisted-pair wire instead of fiber optic cables. Copper cables are no longer widely used because they can only stretch as far as 100 meters, compared to 1,000 meters for fiber optic cables. CDDI is commonly implemented in a wide geographical area.

FDDI

Fiber Distributed Data Interface (**FDDI**) is a standard for data transmission in a local area network. It uses optical fiber as its standard underlying physical medium.

FDDI provides a 100 Mbit/s optical standard for data transmission in local area network that can extend in range up to 200 kilometers (120 mi).

Designers normally constructed FDDI rings in a network topology such as a "dual ring of trees". A small number of devices, typically infrastructure devices such as routers and concentrators rather than host computers, were "dual-attached" to both rings.

FDDI requires this network topology because the dual ring actually passes through each connected device and requires each such device to remain continuously operational. The standard actually allows for optical bypasses, but network engineers consider these unreliable and error-prone. Devices such as workstations and minicomputers that might not come under the control of the network managers are not suitable for connection to the dual ring.

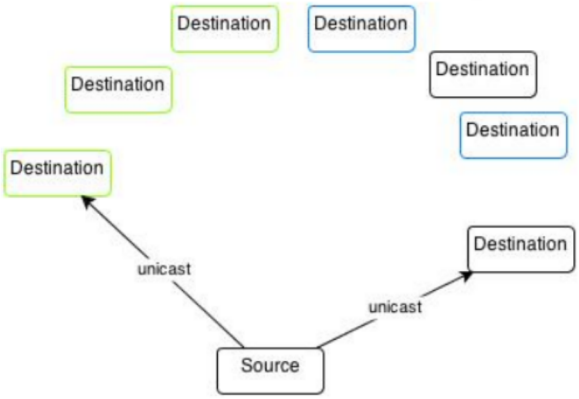
FDDI was considered an attractive campus backbone network technology in the early to mid 1990s since existing Ethernet networks only offered 10 Mbit/s data rates and token ring networks only offered 4 Mbit/s or 16 Mbit/s rates. Thus it was a relatively high-speed choice of that era.

Communication methods

Unicast

Unicast is the term used to describe communication where a piece of information is sent from one point to another point. In this case there is just one sender, and one receiver

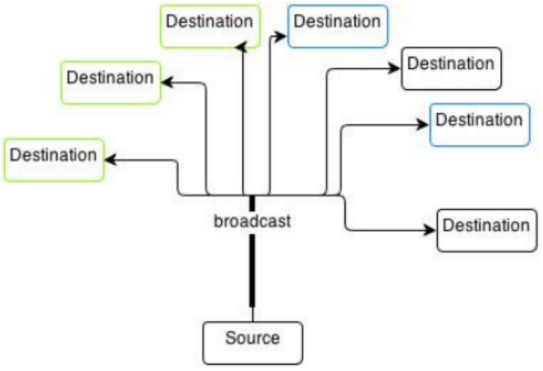
If some device needs to send a message to multiple devices, it will have to send multiple unicast messages, each message addressed to a specific device. So, the sender has to send a separate message to each destination device, and to do that it has to know the exact IP address of each destination device. Remember that in unicasting, each packet is destined for only one device.



In our example we have one source device, and multiple destination devices which belong to different groups of devices (marked with color). As we can see on the picture, unicast messages will be sent to specific devices by using the specific IP address of the device, as the destination address in the packet.

Broadcast

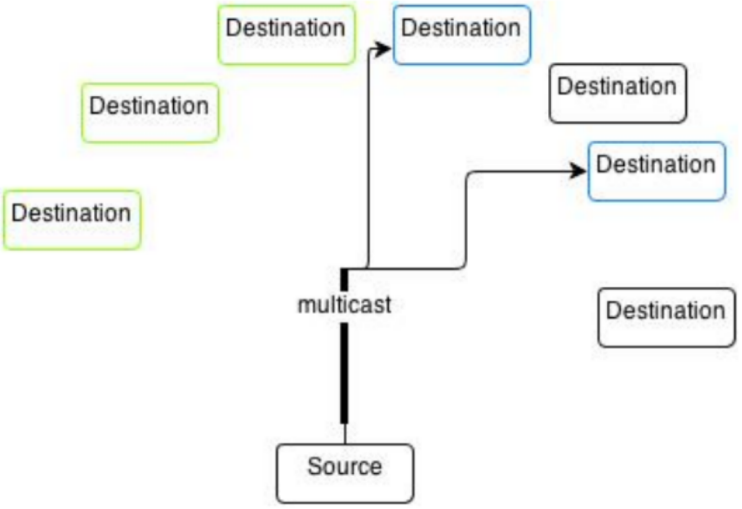
The second method of sending messages is called the broadcasting. Broadcast is a packet that's sent to all devices on specific network. The destination address in the packet is the special broadcast address. If the packet has a broadcast address, all devices that receive that message will process it. So, all devices on the same network segment will see the same message. Another thing to remember is that routers don't forward broadcast messages. The router will receive the broadcast traffic, but it will not forward it through the router.

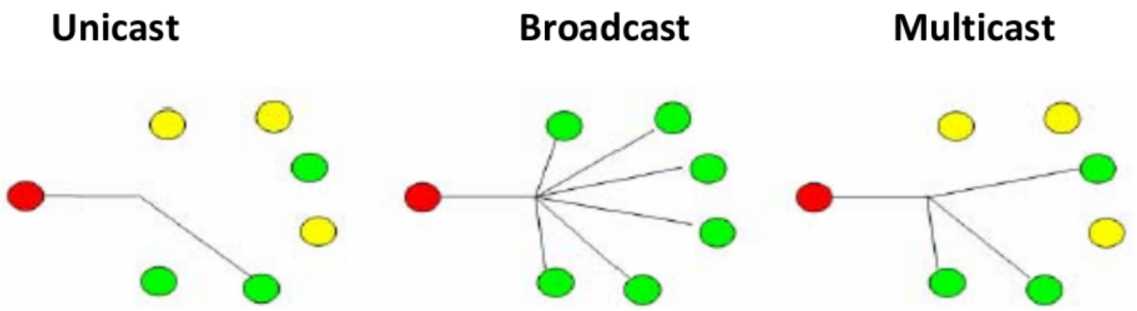


Multicast Message

Multicasting identifies logical groups of computers. A single message can then be sent to the group.

Multicast is the term used to describe communication where a piece of information is sent from one or more points to a set of other points. In this case there is may be one or more senders, and the information is distributed to a set of receivers





Broadcast

A broadcast is a packet/frame (or flows of packets/frames) that are destined for ALL devices on the network/segment. Every bit of the destination address in the packet will be binary “1”. A broadcast IP address (in Layer 3) is 255.255.255.255. A broadcast Layer2 address is ff-ff-ff-ff-ff-ff. Every host on a segment will receive such a broadcast. (Keep in mind that switches will forward a broadcast, but routers do not). Broadcast traffic is used to announce something to all hosts. For example, ARP (address resolution protocol) uses a broadcast address to propagate.