Introduction To Networking Concept

Unit 3

What is a computer network?

- A computer network is a group of computer systems and other hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users.

Why computer networks?

- Computer networks offers a number of advantages to individuals and organizations. Some of these are :
  - Communication medium : It offers a powerful communication medium among a group of people widely spread on the earth.
  - Resource sharing : resources like files, printers, hard drives, or CPU can be shared through a computer network.
  - Higher reliability : If one computer is down, its workload can be taken over by the other computer. So it offers higher reliability than a centralized computing environment.
  - Higher flexibility : A heterogeneous system can be connected in a computer network, by which users get better flexibility.
  - Scalable : Computers and other equipments can be gradually added to satisfy the need of an organization at different points of time, without changing the original network.

Applications of computer networks

- Electronic Mail (e-mail or Email) : It is the most widely used network application is E-mail, which is forwarding of electronic files to an electronic post office for the recipient to pick up.
- Scheduling programs allow people across the network to schedule appointments directly by calling up their fellow worker's schedule and selecting a time.
- Videotext is the capability of having a two-way transmission of pictures and sounds. Distance education lectures use videotext.
- Groupware is the latest network application. It allows user groups to share documents, schedules databases.
- Teleconferencing allows people in different regions to attend meetings using telephone lines.
- Automated Banking Machines allow banking transactions to be performed everywhere : at grocery stores, drive-in machines etc..

- Information Service Providers provide connections to the Internet and other information services.
- Telecommuting allows employees to perform office work at home by “Remote Access” to the network.
- Value Added Networks are common carriers such as ERNET, Satyam, VSNL etc.. (they can be private or public companies) who provide additional leased line connections to their customers. These can be Frame Relay, ATM (Asynchronous Transfer Mode), X.25, etc..
- Marketing and sales Marketing professionals use computer network to collect, exchange and analyse data relating to customer needs.

The Topologies

- The topology is the geometric arrangement (either physically or logically) of the linking devices (usually called nodes) and the links, connecting the individual computers or nodes together.
- Five basic topologies:

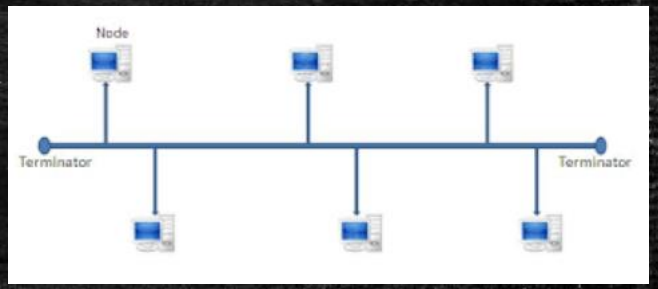
1. Bus topology
2. Ring topology
3. Star topology
4. Mesh topology
5. Combined topologies

1. Bus topology :

- The physical Bus **Network Topology** is the simplest and **most widely used** of the network designs.
- In bus topology, there is a single bus that carries all the data to the entire network.
- A bus is a single continuous communication cable to which all the computers are connected. A cable or bus runs throughout the office to which all the workstations are connected.
- Bus topology is also known as linear bus or line bus.
- When one workstation wants to talk to another, the message or signal travels down the bus in both directions. Each one reads the message to see if it matches its address.
- Bus topology is a passive topology. It means that the computers connected to the bus amplify the signal on the bus.

Advantages :

- Easy to set up.
- Any workstation can be easily moved to another location as bus runs throughout the office.
- If one computer on the bus fails, it does not affect the rest of the traffic on the bus. The entire network can be down only if the bus has a break.
- It requires less cable length than a star topology.
- It is cheaper than the other network options.
- Cost is less as only one main cable is required and least amount of cable is required to connect computers.
- Expansion is easier. New node can be easily added by using a connector.



Disadvantages :

- Difficult reconfiguration
- Fault isolation : It can be difficult to identify the problems if the whole network goes down.
- Bus topology is not great for large networks as all the traffic is on a single bus.
- Terminators are required for both ends of the main cable : The open ends of bus must be terminated to prevent signal bounce. If one or both ends of the bus are not terminated, the whole network can be down.
- Entire network shuts down if there is a break in the main cable.
- Since the cable is one, fault finding and troubleshooting becomes very difficult.
- As more workstations are added, the performance of the network will decrease because of data collisions.
- Network speed slows down as the number of computer increases in bus topology.

2. Ring Topology

- In ring topology, all the workstations are connected in the shape of a ring. The ring does not have an end.
- It is made up of short segments that connect one PC to the next and so on, until all the computers are joined in a circle.
- The signals travel only in one direction and from one PC to the next until it reaches the appropriate node.
- It is difficult to move a workstation or to add more computers to an existing ring.
- The ring topology is an active topology. Each computer boosts the signal (like a repeater) and passes to the next computer till it reaches the destination computer.

Disadvantages :

- If one computer fails, the entire network is down. However, now some ring networks are so designed that a faulty workstation is automatically bypassed.
- Traffic is in only one direction.
- It is not used for a large number of nodes.

3. Star topology

- All the stations are connected to a central computer or hub creating a star configuration.
- The devices are not directly linked to each other.
- Messages pass from the nodes to the hub, where they are processed or passed along to another node.
- The hub controls the traffic on the network.
- If hub fails, connectivity of all hosts to all other hosts fails.
- If a node fails it does not affect the rest of the traffic on the network.
- All client/server networks use this topology.

- cable from each node must be connected to a central hub, the length of total wiring required increases very much.
- A hub can be active or passive hub. A passive hub simply organizes the wiring and works just like a wiring panel for various connections. It does not need any power connection. An active hub does what a passive hub does, but besides this it regenerate and retransmits the signals the way a repeater does. An active hub needs a power connection.

Advantages :

- 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.
- Less cost of installation as each device is connected to only Hub.
- Fault Identification is easy.
- It is easier to add new node or modify any existing node without disturbing network *i.e.* expansion is easier.

- If any local computer or link fails, the entire system does not collapse. Only that link or computer is affected.

Disadvantages :

- If the central controller or hub fails, entire system collapses.
- Cabling cost is more as each node is connected individually to the hub.
- Requires more cable than most topologies
- Moderately difficult to install

4. Mesh topology

- In mesh topology, every node has a dedicated point-to point link to every other node. dedicated means that the links carry traffic only between the two nodes.
- So mesh topology does not have traffic congestion problems. Every node has n-1 link, for a fully connected mesh topology having n nodes. So the total number of links will be n(n-1).This also means that every node has (n-1) I/O ports.

Advantages :

1. Use of dedicated links guarantees that each connection can carry its own data load. Thus eliminates the traffic problem.
2. If one link fails, it does not affect the rest of network. This means it is robust.
3. Point to point links make fault identification and fault isolation easy.

4. Privacy or security is high, since the other link cannot gain access to the dedicated link where the message is travelling.

Disadvantages :

1. More cabling and Ito ports are required, because every node must be connected to every other node.

2. Cost is very high, because more number of node and cabling required.

3. Installation and reconfiguration is difficult.

5. Combined topologies

- A network may have two-or more topologies.
- Any two topologies or all the topologies can be used in a network.
- For example, a hub may be connected to other hubs using a bus and the workstations may be connected by a star.
- Two main hybrid topologies are:

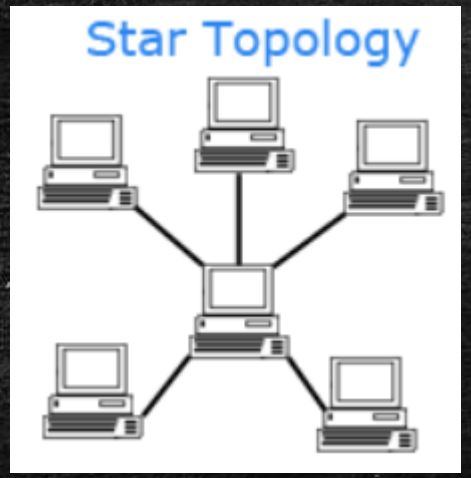
1) The Star Bus Topology

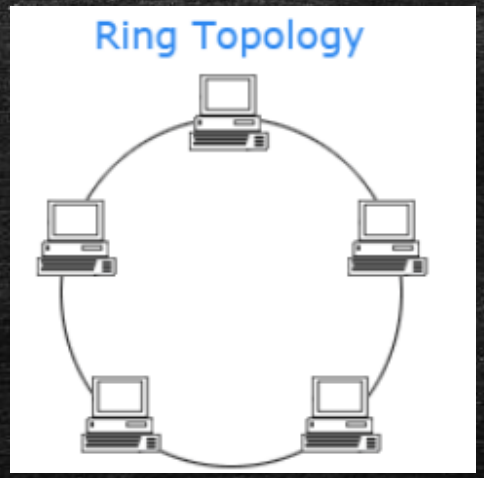
- The star bus topology is a combination of bus and star topologies. In this topology the hubs of many star topology networks are linked together with a linear bus or trunk.

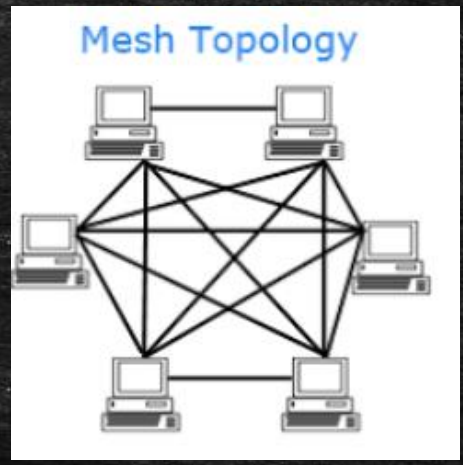
- For example, we want to link three star topology networks together. In each network, the nodes are connected to its own hub. Thus we have three hubs. These three hubs are connected by a bus topology.

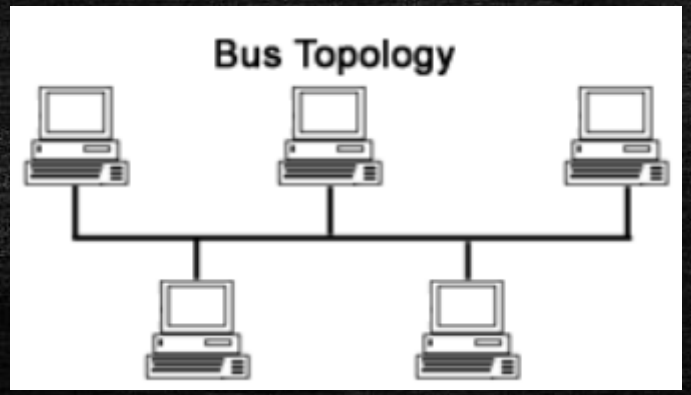
2. The Star Ring Topology

- In this topology the hubs of many star topology networks are connected to another main hub in a star pattern. Thus if we have three star topology networks, then the three hubs of the networks are connected to a fourth hub (main hub) in star pattern.









Architectural models for designing computer networks

- There are primarily two architectural models for designing computer networks. They are :

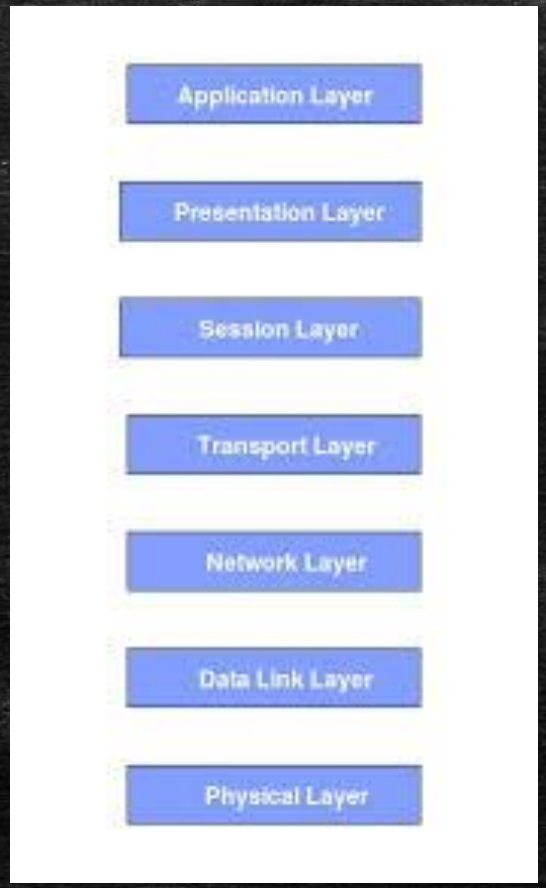
1. OSI model
2. TCP/IP model

Characteristics of OSI model

- Open System Interconnection (OSI) is an ISO standard. It is not a protocol.
- OSI reference model has seven layers. The seven layers are divided into two categories: upper layers and lower layers.
- The upper layers deal with application issues and are implemented only in software.
- The lower layers deal with data transport issues and are implemented in hardware and software.
- The seven layers of the OSI model are :

1. Physical layer
2. Data link layer
3. Network layer
4. Transport layer

5. Session layer
6. Presentation layer
7. Application layer



1. Physical layer :

- It is the lowest layer of OSI model.
- It is implemented in hardware and software.
- It is closest to the physical network medium.
- It is responsible for actually placing information on the medium.

Infrared transmission

- It is another line of sight medium.
- It uses electromagnetic radiation of wave lengths between radio waves and visible light, operation between 100GHZ and 100THZ.
- These frequencies are very high offering nice data transfer rates.
- IR technology is used in television or VCR remotes.
- IR is generally restricted to LAN within or between buildings.

Advantages :

1. Higher bandwidth means superior throughput to radio.
2. Inexpensive to produce
3. No longer limited to tight interroom line-of-sight restrictions

Disadvantages :

1. Limited in distance
2. Cannot penetrate physical barriers like walls, ceilings, floors etc..

Connecting Devices or Network Devices

- As companies grow, their networks also grow.
- We can connect two or more networks together to create larger networks.
- A LAN can be connected to another LAN. A LAN can be connected to another WAN.
- The components or devices that are employed to connect two or more networks together are called connecting devices or network devices.
- The different connecting devices or networking devices are :

1. Repeaters
2. Hubs
3. Bridges
4. Routers
5. Gateways

1. Repeaters

- Repeaters are also called as regenerators.
- They are physical hardware devices.
- They connect two network segments and broadcast packets between them, thus extending your network beyond the maximum length of your cable segment.
- They have primary function to regenerate the electrical signal (shown below) :
  - Reshaping the waveform
  - Amplifying the waveform
  - Retiming the signal, to avoid collision on the network

- As signal travels along a cable, its strength or amplitude decreases. This is called attenuation. In other words, the signal attenuates as it travels along a cable. This limits the length of a cable used to connect the computers together.
- Signal is a factor in the maximum length of a segment, repeater can regenerate (or amplify) the weak signals so that they can travel additional cable lengths.
- A repeater has intelligence , so that it takes a weak signal from one cable segment, regenerates it and passes it on to the next segment.
- Or we can simply say that, it recreates the bit pattern of the original signal.
- No more than four repeaters are used to join segments together to keep collision detection working properly.
- Amplifier uses analog signal, it cannot differentiate between original signal and noise, therefore it amplifies both original signal and noise.

- The repeater does not amplify the original signal, it regenerates the original bit pattern.

Purpose of a repeater

- The purpose of a repeater is to extend the LAN segment beyond its physical limits .
- A LAN segment is a logical path, such as the logical bus used by all 802.3 Ethernet types.
- A LAN segment is given an identification number, called a segment number or network number, to differentiate it from other segments.

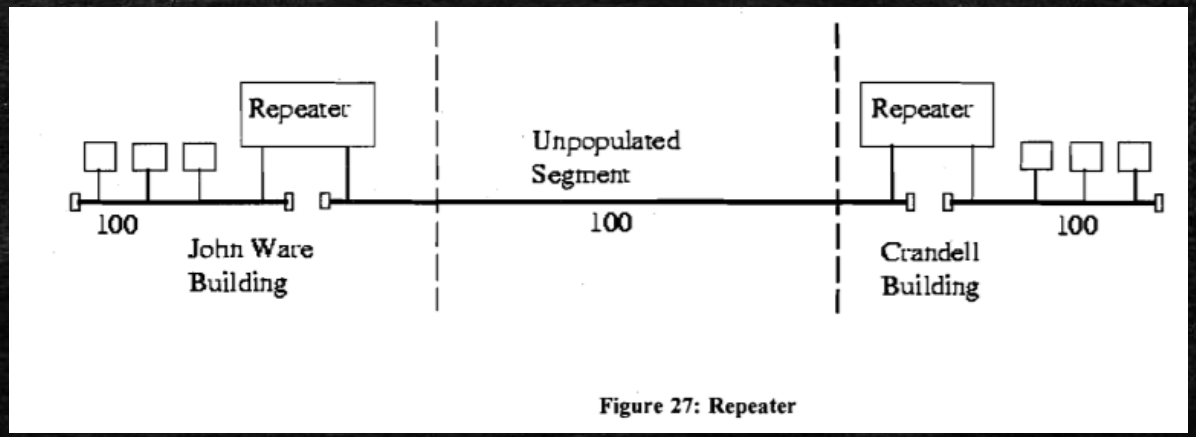


Figure 27: Repeater

- Repeaters are used to connect two physically close buildings together (when they are too far apart to just extend the segment). They can be used to connect floors of a building that would normally surpass the maximum allowable segment length.

Repeater's OSI Operating Layer

Repeaters operate at the OSI Model Physical Layer (Figure 28).

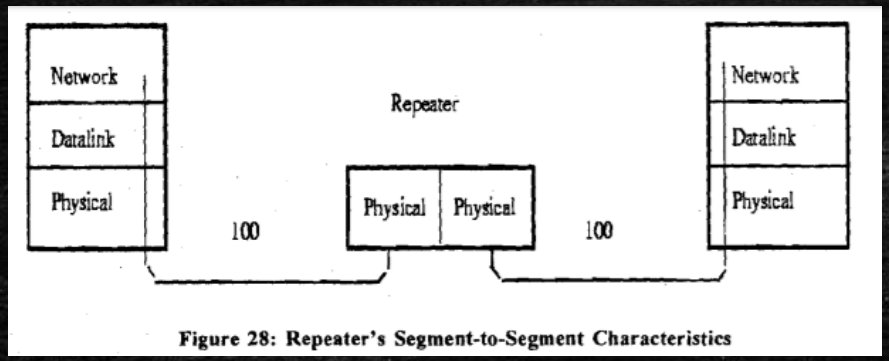


Figure 28: Repeater's Segment-to-Segment Characteristics

- A repeater cannot join two cable segments using different access methods.
- A repeater cannot be used to connect a segment using CSMA?CD access method to a segment using token passing access.
- Repeaters can join two different physical media, but they must use the same access method.
- Thus a repeater can have physical connections to join a coaxial cables segment to a fiber optic segment.
- Repeaters do not de-segment a network.
- All traffic that appears on one side of the repeater appears on both sides.
- Repeaters handle only the electrical and physical characteristics of the signal.
- Repeaters work only on the same type of physical layer : Ethernet-to-Ethernet, o Token-Ring-to-Token Ring. They cannot connect 10Base5 to 10BaseT because they both use the same 802.3 MAC layer.

- A repeater cannot connect token ring to Ethernet because the physical layer is different for each network topology.

Repeater Addressing : MAC Layer and Network segment

- The MAC layer address is used to identify the network card to the network.
- The repeater is transparent to both sides of the segment and both sides can see all the Mac Addresses (regardless of which side they are on).
- This means that any network traffic on floor 1 will also appear on floor 5, and vice versa.

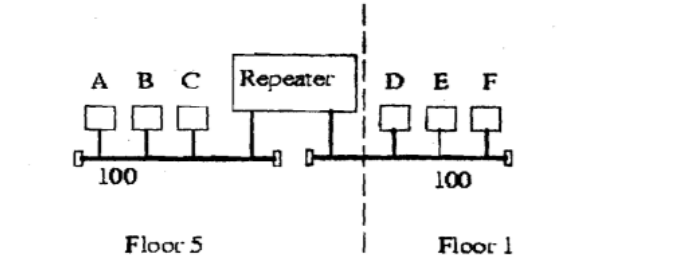


Figure 29: Repeater Addressing

- Nodes A & B could be furiously are exchanging files; this network traffic would also appear on floor I. Repeaters don't provide isolation between segments.
- Since repeaters provide no isolation between segments, and the repeater is transparent to both sides of the segment, both sides of the repeater appear as one long segment.
- The network number, or segment number, is the same on both sides of the repeater.

2. Hubs

- Hubs are also known as multi port repeaters or concentrators.
- They expand an Ethernet connection into many.
- They are physical hardware devices.
- A hub is similar to repeaters, except that it broadcasts data received by any port to all other ports on the hub.
- Some hubs are basic hubs with minimum intelligence (i.e. no microprocessors), intelligent hubs can perform basic diagnostics, and test the nodes to see if they are operating correctly. If they are not, the smart hubs (or Intelligent hubs) will remove the node from the network. Some smart hubs can be polled and managed remotely.

Purpose of hubs

- Hubs are used to provide a physical star topology (figure 30).
- The logical topology is dependent on the Medium Access Control Protocol.
- At the center of the star is the hub, with the network nodes located on the tips of the star.

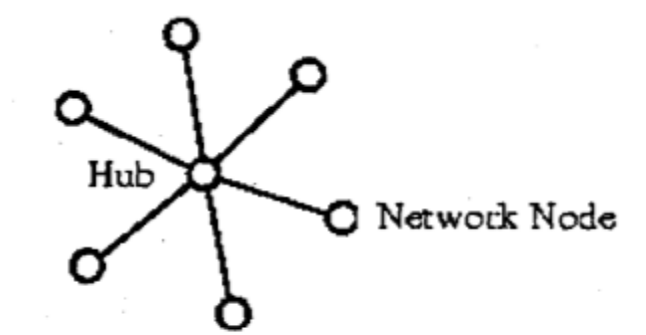


Figure 30: Position of Hub

Star topology

- The hub is installed in a central wiring closet (figure 31) with all the cables extending out to the network nodes.
- The advantage of having a central wiring location is that it is easier to maintain troubleshhot large networks. All of the network cables come to the central hub.
- This way, it is especially easy to detect and fic=x cable problems.
- You can easily move a work station in- a star topology- by changing the connection to the hub at the central wiring closet.

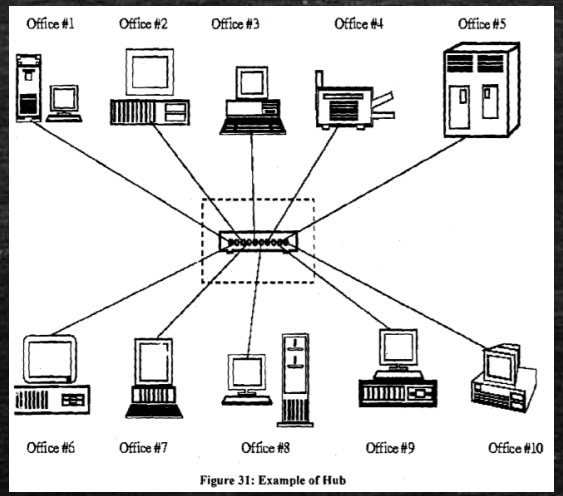


Figure 31: Example of Hub

Hub's OSI Operating Layer :

Hubs are multi port repeaters, and as such they obey the same rules as repeaters . They operate at the OSI Model Physical Layer. (See OSI operating Layer Repeaters)

Hub's segment-to-segment characteristics

- To determine Ethernet segment-to-segment characteristics of a hub, determine how the Ethernet Hubs operate. Logically , they appear as a bus topology, and physically as a star topology.
- Ethernet Hub consists of an electronic printed circuit board.

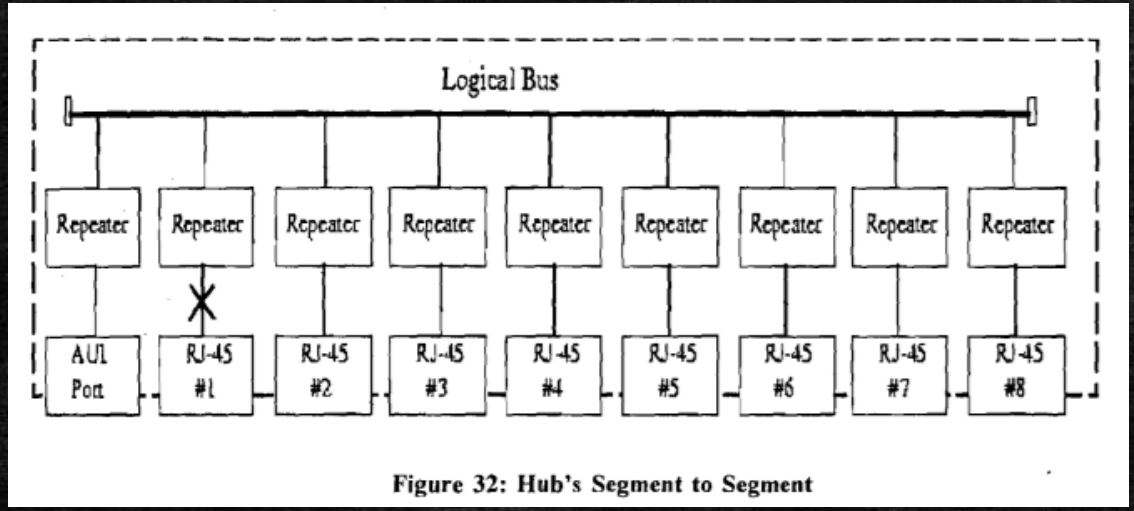


Figure 32: Hub's Segment to Segment

- Understanding that inside the hub is only more repeaters, we can draw the conclusion that all connects attached to a Hub are on the same segment (and have the same Segment Number). A single repeater is said to exist from any port to any port, even though it is indicated as a path of 2 repeaters.

Hubs addressing

- Since, a hub is just many repeaters in the same box, any network traffic between nodes is heard over the complete network. As fas as the stations are concerned, they are connected on one long logical bus (wire).

Switching hubs

- Switching hubs (figure 33) are hubs that will directly switch ports to each other.
- They are similar to full duplex hubs, except that they allow dedicated 10 Mbps channels between ports.

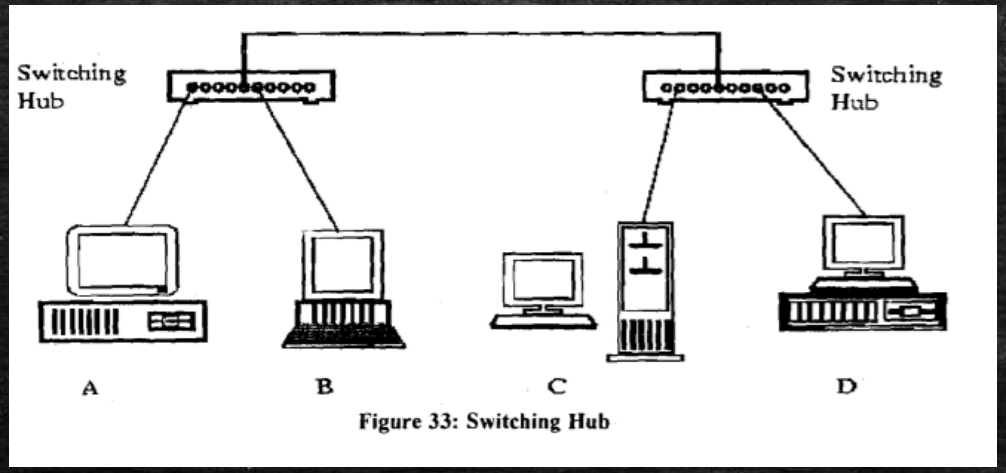


Figure 33: Switching Hub

- If A wanted to communicate with B, a dedicated 10 Mbps connection would be established between the two. If C wanted to communicate with D, another dedicated 10 Mbps connection would be established.

3. Bridges

- Bridges have all the features of the repeater.
- Besides regenerating the signals, a bridge can segment (or divide) a network to isolate traffic related problems.
- A bridge sends the data frames only to the concerned segment, thus preventing excess traffic.
- A bridge can split an overloaded network into two separate networks, reducing the amount of traffic on each segment and thus making each network more efficient.
- Just like repeaters, the bridges can be used to link different physical media.
- Brides can also be used to connect dissimilar networks like Ethernet system to a Token Ring system.

- Thus bridges can be used to join networks using CSMA/CD access and token passing access.
- Bridges are both hardware and software devices.
- They can be standalone devices- separate boxes specifically designed for bringing applications- or they can be dedicated PCs (with 2 NICs and bridging software).
- Most server software will automatically act as a bridge when a second NIC card is installed.

Bridge OSI operating layer

- Bridges operate on the OSI Model Data Link layer, while repeaters work at the physical layer.
- Since bridges work on a higher layer than repeaters, they are more complex than repeaters and cost more than repeaters.
- They look at the MAC addresses for Ethernet and Token Ring, and determine whether or not to forward- or ignore – a packet.

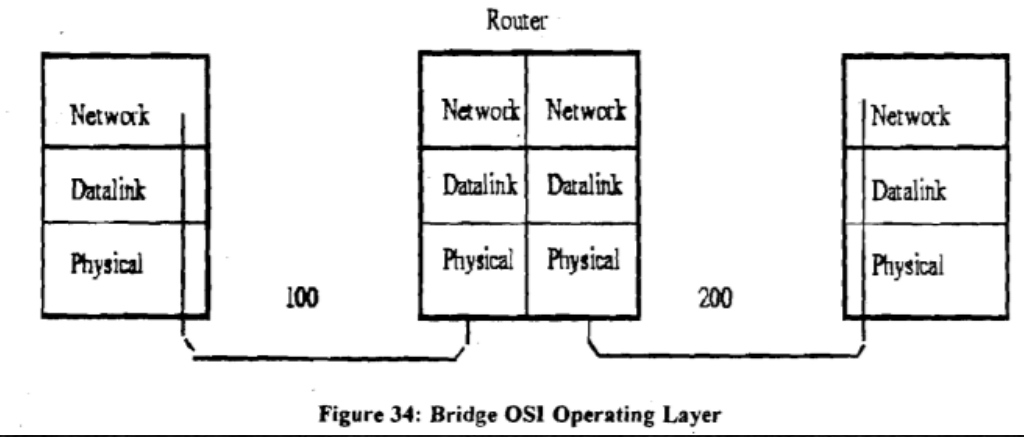


Figure 34: Bridge OSI Operating Layer

- Bridges have their own routing tables. Initially the bridge's routing table is empty. As nodes send packets, the source address is copied to the routing table.
- With this address information, the bridge learns where the computers are situated.
- When any packet is received by a bridge it reads its source and destination address.
- If the bridge knows the location of the destination node it forwards the packet to the segment on which the destination node is situated. If it does not know the destination, it forwards the packet to all the segments.

Purposes of a bridge :

The purposes of a bridge are the following :

- Isolates networks by MAC addresses
- Manages network traffic by filtering packets
- Translates from one protocol to another

Isolates networks by MAC address

Consider a segment called segment 100 that has 50 users using this network segment. Engineering department is CAD oriented and Accounting department is into heavy number crunching.

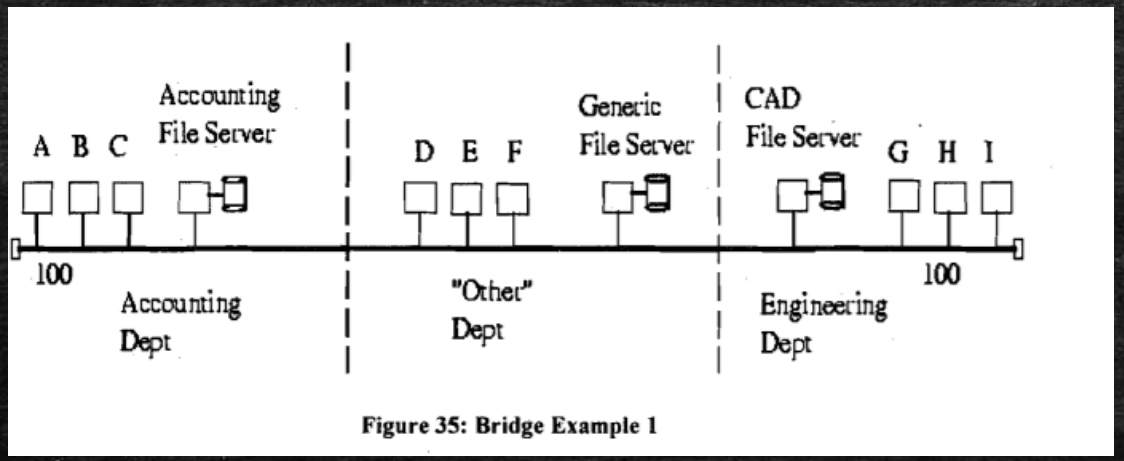


Figure 35: Bridge Example 1

- On this network, any traffic between clients A,B or C and the accounting file server will be heard across the segment 100. Similarly, any traffic between the Engineering Dept. clients G,H or I (to the CAD File Server) will be heard throughout the network segment. The result is that "Other" Department accesses to the generic file server are incredibly slow; this is because of the unnecessary traffic that is being generated from other departments.

- The solution is to use one bridge to isolate the accounting department, and another bridge to isolate the engineering department.
- The bridges will only allow packets to pass through that are not on the local segment. The bridge will first check its "routing" table to see if the packet is on the local segment. If it is, it will ignore the packet, and not forward it to the remote segment. If client A sent a packet to the Accounting File Server then Bridge #1 will check its routing table (to see if the Accounting File Server is on the local port). If it is on the local port, then Bridge #1 will not forward the packet to the other segments.

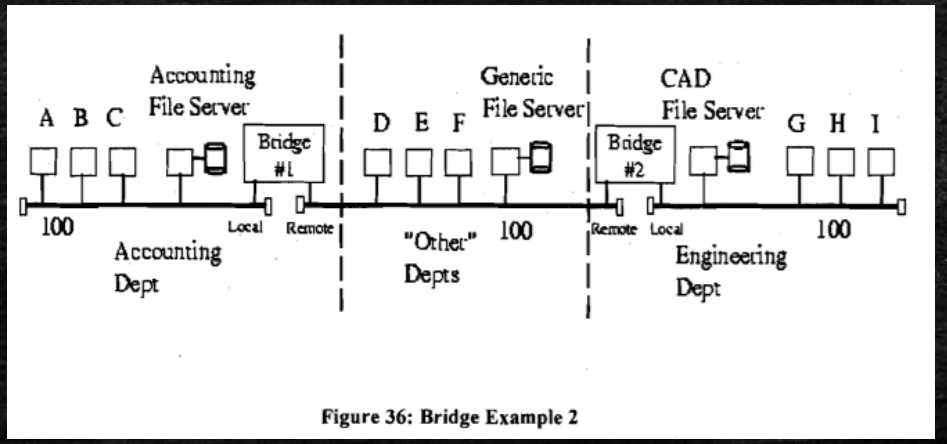


Figure 36: Bridge Example 2

- If client A sent a packet to the Generic File Server, Bridge #1 will again check its routing table to see if the Generic File Server is on the local port. If it is not, then Bridge #1 will forward the packet to the remote port.
- In this way, the network is segmented, and the local department traffic is isolated from the rest of the network.
- Overall network bandwidth increases because the Accounting Dept. does not have to fight with the Engineering Dept. (for access to the segment). Each segment has reduced the amount of traffic on it and the result is faster access. Each department still has complete access to the other segments, but only when required.

4. Routers :

- Routers are special purpose computers that has a processor (CPU) and memory like any other computer. Unlike any other computer, it has more than one I/O interface that allows it to connect to multiple computer networks.
- Routers are both hardware and software devices.
- Just like bridge, routers can connect network segments and filter and isolate traffic.
- Unlike a bridge, a router can connect networks that use different technologies, addressing methods, media types, frame formats, and speeds. Routers are used in complex networks because they provide better traffic management than bridges. Routers do not pass broadcast traffic. A router keeps track of the address of all the segment of a network and can even determine the best path for sending data.

- Like bridges, routers also maintain routing tables in their memories to store information about physical connections on the network.
- The router examines each packet of data, checks the routing table, and then forwards the packet if necessary.
- Routers are more inelegant than bridges, as routers can share status and routing information with one another and use this information to bypass slow or malfunctioning connections.
- Routers do not maintain any state information about the packets; they simply move them along the network.
- Routers are usually employed by wide area networks using dissimilar addressing schemes and different communication protocols.
- Routers do not allow bad data to get passed on to the network. Thus they save networks from broadcast storms.

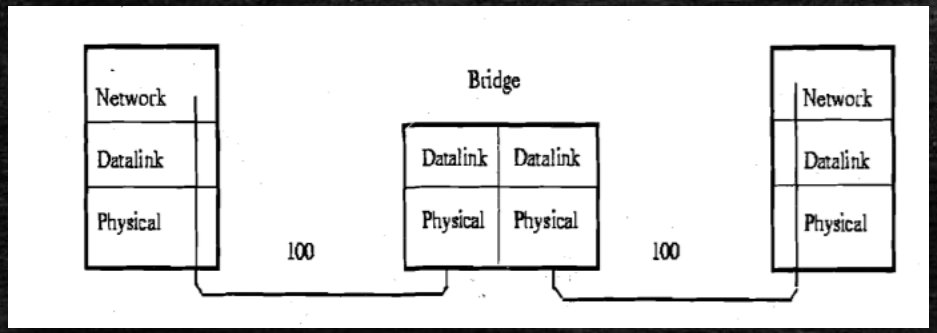
- There are two types of routers : static routers and dynamic routers

Static routers : They require an administrator to manually set up and configure the routing table and to specify each route.

Dynamic routers : They maintain a routing table automatically and require minimal set up and configuration.

Router OSI Operating layer :

- Routers operate on the OSI Model's Network Layer as shown in the below figure.



- The internet work must use the same Network Layer Protocol. Routers allow the transportation of the Network Layer PDU through the Internetwork, even though the Physical and Data Link Frame size and addressing scheme may change.
- Routers that only know Novell IPX (Internetwork Packet Exchange) will not forward nix's IP PDUs, and vice versa.
- Routers only see the network layer protocol that they have been configured for. This means that a network can have multiple protocols running on it (SPX/IPX, TCP/IP, Appletalk,XNS, etc..)

Router Addressing :

- Routers know the address of all known networks. They maintain a table of pathways between networks and can select an optimal route over which to send data.
- Routers look only at network address and not at destination node address.

- Routers talk to other routers, but not to remote computers.
- Routers combine the network number and the node address to make source and destination addresses.
- Routers have to know the name of the segment that they are on, and the segment name or number where the PDU is going.
- They also have to know the node address: MAC Address for Novell, and the IP address for TCP/IP.

5. Gateways

- It is the hardware/ software device that is used to interconnect LANs and WANs.
- Gateways are more powerful and complex than a router.
- They are slower than a router and are expensive.
- Gateway incorporates the functions of routers and bridges, but it can translate the instruction set on sending network into corresponding instruction set of the receiving network.
- Gateways make communication possible between different architectures and environments.
- Often, the router that is used to connect a LAN to the Internet will be called a gateway.
- It has the capability to direct and filter higher layer protocols to specific devices(such as web servers, ftp servers and email servers).

- A gateway links two systems that do not use the same communication protocols, data formatting structures, languages and architecture, which cannot be done by a router.
- Gateways perform protocol and data conversion.

Gateways OSI operating layer :

- Gateways operate at the transport layer and above.
- It typically translates each source layer protocol into the appropriate destination layer protocol.
- Gateways use all the seven layers of the OSI model.
- A mainframe gateway may translate all OSI model layers.
- Example, IBM's SNA (System Network Architecture) does not readily conform to the OSI model, and requires a gateway to translate between the two architectures.