5...

Network Connectivity Devices

Objectives...

- To learn about categories of network connectivity devices.
- To study about Hubs, Repeaters, Bridges, Switches, Routers and Gateways.

5.1 NETWORK CONNECTIVITY DEVICES

- Networking Connecting Devices include all computers, peripherals, interface cards and other equipments needed to perform data-processing and communications within the network.
- **Examples:** Network Interface Card (NIC), Hub, Switch, Bridge, Router, Gateway.

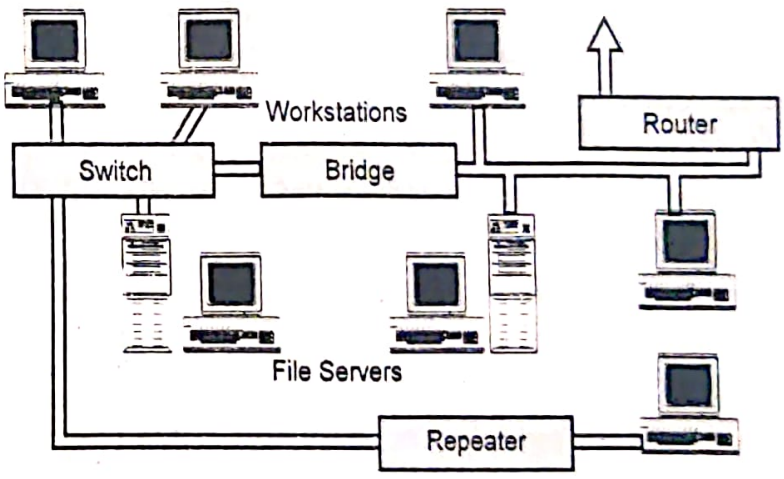


Fig. 5.1: Networking Hardware with Network connectivity devices

- A file server stands at the heart of most networks. It is a very fast computer with a large amount of RAM and storage space, along with a fast network interface card.
- The network operating system software resides on this computer, along with any software applications and data files that need to be shared.

- All user computers connected to a network is called workstations.
- A typical workstation is a computer that is configured with a network interface card, networking software and the appropriate cables. Workstations do not necessarily need floppy disk drives because files can be saved on the file server.
- Almost any computer can serve as a network workstation.

5.2 ACTIVE AND PASSIVE HUBS (S-18, S-19, S-23)

5.2.1 What is Hub?

- As the name suggests, the meaning of hub is a center of activities. A hub is a medium used to collect signals from the input line(s) and redistribute them in various available wirings around a topology (Topologies such as: Arcnet, 10base-T, 10base-F etc.).
- Hubs operate at the Physical layer of the Open Systems Interconnection (OSI) model.

Physical Structure:

- A hub is a small rectangular box, often constructed mainly of plastic that receives its power from an ordinary wall outlet. A hub joins multiple computers or other network devices together to form a single network segment.
- On this network segment, all computers can communicate directly with each other. Ethernet hubs are by far the most common type, but hubs for other types of networks (such as USB) also exist.
- Hubs come in a variety of shapes and sizes.
- A hub includes a series of ports that each accepts a network cable. Small hubs network four computers. They contain four or sometimes five ports (the fifth port being reserved for "uplink" connections to another hub or similar device). Larger hubs contain 8, 12, 16, and even 24 ports.
- Even the most basic hubs can provide satisfactory file sharing and Internet connection sharing for a LAN.
- They will work with traditional dial-up, cable modem, and DSL service. For high-performance networking such as online gaming, net workers will want a more expensive 10/100 Fast Ethernet-capable hub.
- Future high-speed Internet services like VDSL will almost certainly require Fast Ethernet performance as well.
- Hubs differ in the features they support as well as in performance, making direct comparisons difficult.
- Hubs are used in Ethernet (IEEE 802.3) networks. The electronics in hubs need to be more sophisticated however, because a signal received at any port must be "instantly" retransmitted on all other ports for the CSMA/CD access method to work.

- Network segments that employ hubs are often described as having a Star-Bus network topology, in which the hub forms the wiring centre of the "star".

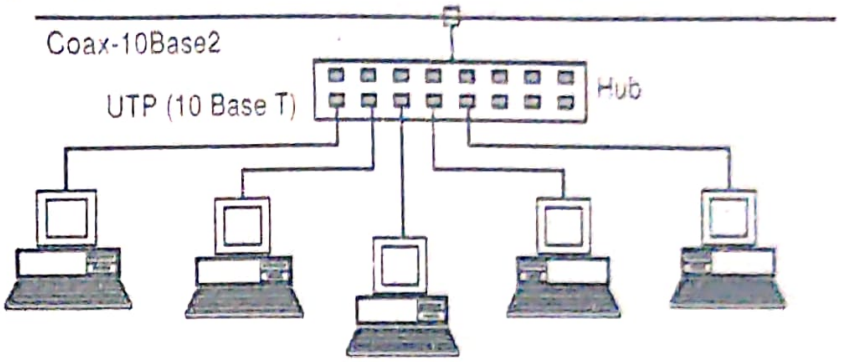


Fig. 5.2: Typical hub is used to connect the Different Nodes

Advantages:

- Hubs offer a convenient, affordable way to build a home or small business network.
- It provides a degree of fault tolerance, because each node has its own connection to the hub, and if the connection fails, only that node is affected.
- It also simplifies the task of expanding the network, as many additional nodes can be added to the network using a single hub, which is normally connected to the network backbone.

Disadvantages:

- In early computer networks, nodes were connected together in daisy-chain fashion. Once, all the nodes were connected, each end of the cable would be closed with a terminator.
- The main problem with this design was that a break anywhere in the cable meant that the network would not function, and one of the major overheads was the time spent in locating the problem.

Need of Hub:

- Generally, when we build a network using two or more computers, we need a hub. However, it is possible to connect two computers to each other directly without the need of hub but when we add a third computer in the network, we need a hub to allow a proper data communication within the network.
- There are many types of hubs with various features/specifications, which provide the type of functionality you need in building network.

Types of Hubs:

- Hubs can be either active or passive.
- Small hubs with five or eight connection ports are commonly referred to as workgroup hubs. Others can accommodate larger numbers of devices (normally up to 32).
- These are referred to as high-density devices. Because hubs do not perform any processing, they do little except enable communication between connected devices.

5.2.2 Active Hub (S-18, S-19, S-22)

- Active hub is a type of hub that takes active participation in data communication within the network/LAN.
- An active hub is basically a multiport repeater of the Class II type, although it is still a physical layer device - it buffers incoming frames and regenerates them, sending the regenerated signal out on all of its ports.
- In order to do this, active hubs require their own power supply. Because the signal is regenerated at the hub, each output port can take full advantage of the maximum cable length. Since the medium used is Unshielded Twisted Pair (UTP), maximum length will be 100 meters.

Features:

- Active hubs come with various features, such as,
  - Receiving the signal (data) from the input port and storing it for some time before forwarding it. This feature allows the hub to monitor the data that is forwarding.
  - Some hubs come with a feature that helps in transmitting data that has high priority before the data that has lower priority (this feature is very important for some applications and some type of networks).
  - Some hubs help in synchronizing data communication (by retransmitting the packets, which are not properly received at the receiving computer or by adjusting re-transmission of the data packets to compensate timing).
  - Some active hubs come with a feature that rectifies the data/signal before forwarding it in the network/LAN.
  - Active hubs also help in troubleshooting at certain level. If there is a bottleneck within the network/LAN, active hubs can be used to find out the problem at certain extent.
- Active hubs have some benefits over the use of passive hubs; however, active hubs are more expensive than passive hubs as they provide additional features.

5.2.3 Passive Hub (S-18, S-19, S-22)

- As its name suggests, passive hubs which does not provide any additional feature except for working just as an interface between the topology.
- A passive hub simply receives signal(s) on input port(s) and broadcasts it (them) on the output port(s) without even rectifying it (them).
- Managed hubs offer some control over the nodes connected to them.
- For example, each port can be individually enabled or disabled by the network administrator and some intelligent hubs can track network activities such as the number of packets transferred and the occurrence of errors within those packets.
- A hub does not perform any processing on the data that it forwards, nor does it perform any error checking.

5.3 REPEATERS (S-18, S-19, S-22)

- A repeater is primarily a non-intelligent network device that receives a signal on one of its connections and passes that signal on to all of its other connections after regenerating it.

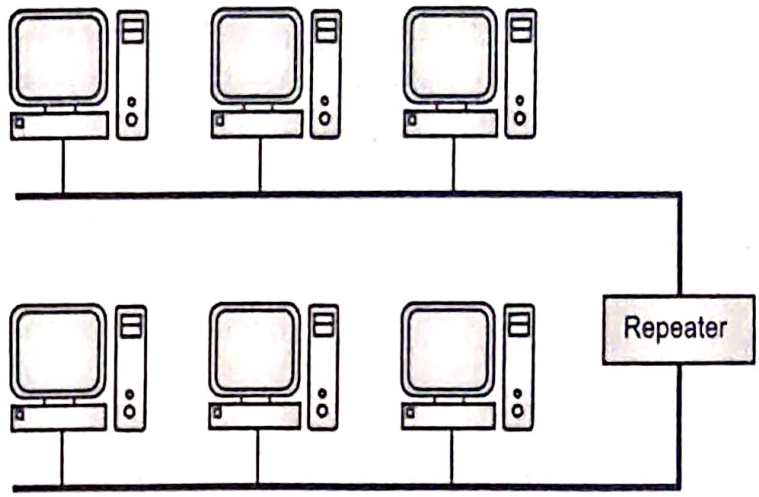


Fig. 5.3: Repeaters can be used to extend the Length of a Network

- Repeaters work at the physical layer and can be used to extend the length of a network, but not the capacity.
- As signals travel along a network cable (or any other medium of transmission), they degrade and become distorted in a process that is called attenuation.
- If a cable is long enough, the attenuation will finally make a signal unrecognizable by the receiver.
- A Repeater enables signals to travel longer distances over a network. A repeater regenerates the received signals and then retransmits the regenerated (or conditioned) signals on other segments.
- Amplifier cannot discriminate between the intended signal and noise i.e. it amplifies equally everything fed into it.
- A repeater does not amplify the signal, it regenerates the signal. When repeater receives a weakened or corrupted signal, it creates a copy, bit for bit, at the original strength.
- Hub is basically a multiport repeater.

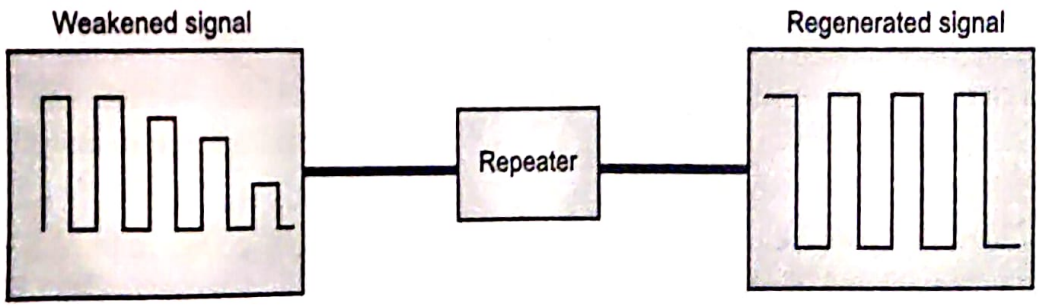
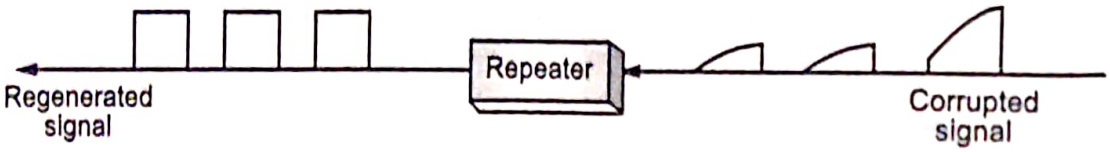
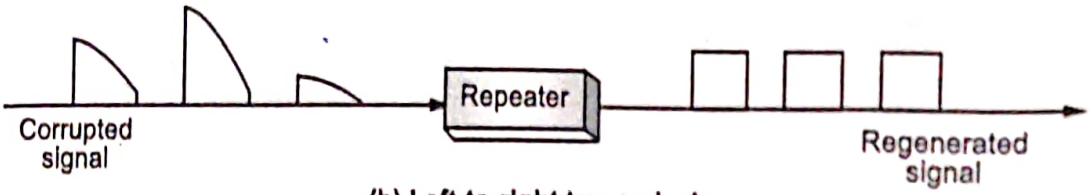


Fig. 5.4: Regenerated signal using the Repeater

- To pass data through the repeater in a usable fashion from one segment to the next, the packets and the Logical Link Control (LLC) protocols must be the same on the each segment.
- This means that a repeater will not enable communication, for example, between an 802.3 segment (Ethernet) and an 802.5 segment (Token Ring).
- That is, they cannot translate an Ethernet packet into a Token Ring packet. In other words, repeaters do not translate anything. As signals travel along a transmission medium, there will be a loss or attenuation, of signal strength.



(a) Right-to-left transmission



(b) Left-to-right transmission

Fig. 5.5: Function of a Repeater

- Repeaters are defined into 2 classes:
  1. Class I (or Type I): These are not stackable, and cannot be daisy- chained.
  2. Class II (or Type II): These are stackable, and can be daisy-chained.
- Some multiport repeaters act as multiport hubs and connect different types of media.

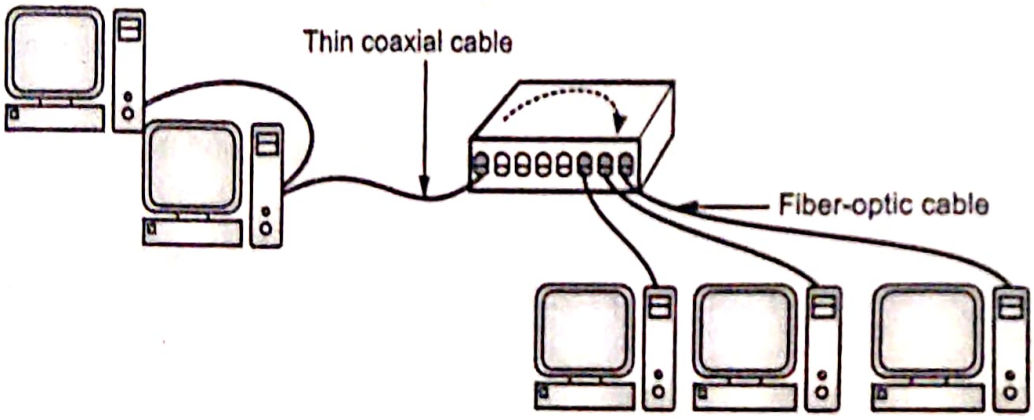


Fig. 5.6: Repeaters can connect different types of Media

- Repeaters cannot be used to enlarge a network beyond the capabilities of its underlying architecture, nor they can be used to connect network segments that rely on different access methods.
- They can, however, be used to move transmissions between different media types, such as coaxial and fiber optic cables.

5.4 BRIDGES

(W-18, S-18, S-19, W-22, S-23)

- Like a repeater, a bridge can join segments or workgroup LANs. However, a bridge can also divide a network to isolate traffic or problems.
- For example, if the volume of traffic from one or two computers or a single department is flooding the network with data and slowing down entire operation, a bridge can isolate those computers or that department.

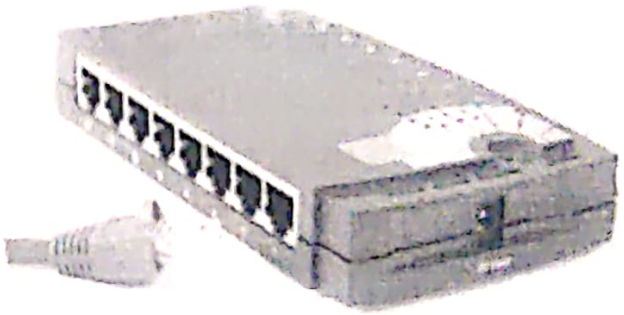


Fig. 5.7 (a): Bridge

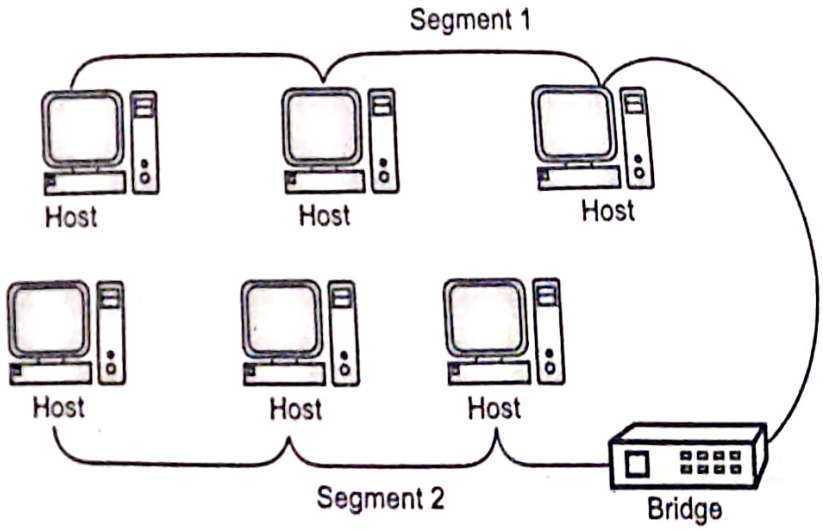


Fig. 5.7 (b): Use of Bridge

- In Fig. 5.7(b), a bridge is used to connect two segments, Segment 1 and Segment 2.
- Bridges operate at the Data Link Layer of the OSI Reference Model. A bridge both filters and passes packets between network segments.
- While true bridges connect only LANs that have an identical network architecture (i.e. 802.3 - 802.3, 802.5 - 802.5), certain types of bridge (bridge-routers or brouters) can also join LANs based on different network architectures.
- For example, they can join an Ethernet segment to a Token Ring segment and transfer packets between the two despite the difference in protocols used.
- Thus bridges can both extend the length of a network and increase its capacity.

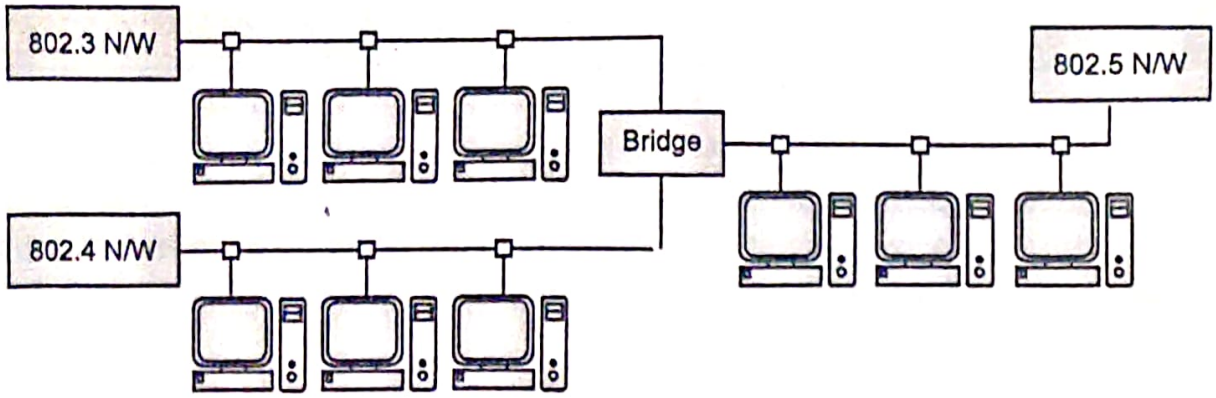


Fig. 5.8: Bridge used to connect Multiple Segments

- Unless the sender and the recipient are on different network segments, there is no need for the bridge to transfer the packet to another network segment. If the sender and the recipient are on different segments, the bridge needs to be able to determine where the recipient is.
- Bridges can be used to:
  - Expand the distance of a segment.
  - Provide for an increased number of computers on the network.
- Network bridges can be used to connect LAN segments or to isolate heavily trafficked segments from the rest of the network.

Working principle:

- A bridge works on the principle that each network node has its own address.
- A bridge forwards the packets based on the address of the particular destination node. As traffic passes through the bridge, information about the computer addresses is then stored in the bridge's RAM.
- The bridge will then use this RAM to build a routing table based on source addresses.

5.4.1 Types of Bridges

- Three types of bridges are used in networks:
  1. Transparent Bridge
  2. Source Route Bridge
  3. Spanning Tree Bridge

1. Transparent Bridge:

- A transparent bridge is a type of Network Bridge. It interconnects several computers in a network by forwarding packets to hosts.
- A transparent bridge is a bridge whose presence and operation is invisible to hosts on the network.
- A transparent bridge does nothing except block or forward data based on the MAC address.

- Physically, a transparent bridge looks like a box with two or more holes (ports) where network cables are plugged. The other extreme of each cable is usually connected to the network port of a computer, or to another network device, which is further connected to one or more computers.
- While a network bridge simply enables local networks (or segments) to communicate with each other, but forwards the traffic to all ports, a transparent bridge is capable of redirecting the packets to the proper port, hence it can isolate the networks from broadcast traffic.
- A transparent bridge directs the outgoing data traffic using a forwarding table that associates addresses to ports.
- The table can be static or built by learning the network topology from the analysis of the incoming traffic. For example, learning happens by the device inspecting the source Media Access Control (MAC) address of all incoming data frames. The device will send frames out of all its ports.
- This method uses a forwarding database to send frames across network segments.
- The forwarding database is initially empty and entries in the database are built as the bridge receives frames.
- If an address entry is not found in the forwarding database, the frame is rebroadcast to all ports of the bridge, forwarding the frame to all segments except the source address.
- By means of these broadcast frames, the destination network will respond and a route will be created. Along with recording the network segment to which a particular frame is to be sent, bridges may also record a bandwidth metric to avoid looping when multiple paths are available.
- Devices that have this transparent bridging functionality are also known as *adaptive bridges*. They are primarily found in Ethernet networks.

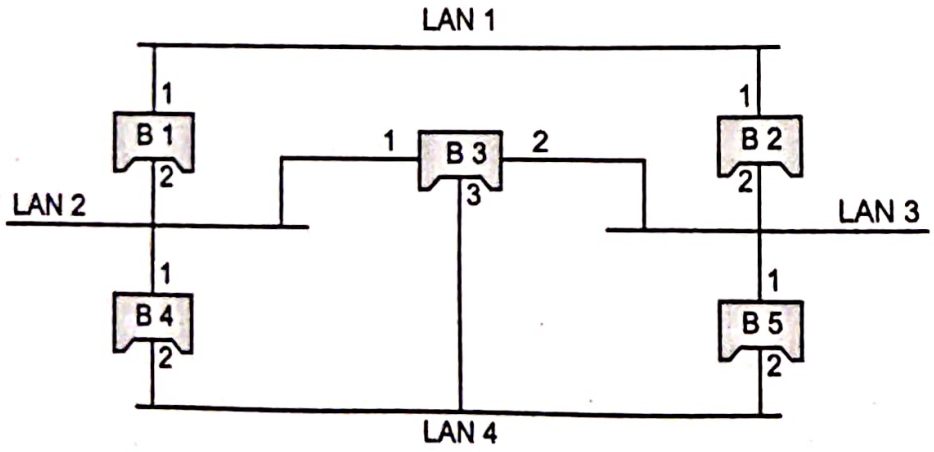
2. Source Route Bridge:

- The source route bridge derives its name from the fact that the entire path that the packet is to take through the network is embedded within the packet. Used in Token Ring networks.
- With source route bridging two frame types are used in order to find the route to the destination network segment: Single-Route (SR) frames and All-Route (AR) frames.
- Single-Route (SR) frames make up most of the network traffic and have set destinations, while All-Route (AR) frames are used to find routes.
- Bridges send AR frames by broadcasting on all network branches; each step of the followed route is registered by the bridge performing it.
- Each frame has a maximum hop count, which is determined to be greater than the diameter of the network graph, and is decremented by each bridge. Frames are dropped when this hop count reaches zero, to avoid indefinite looping of AR frames.

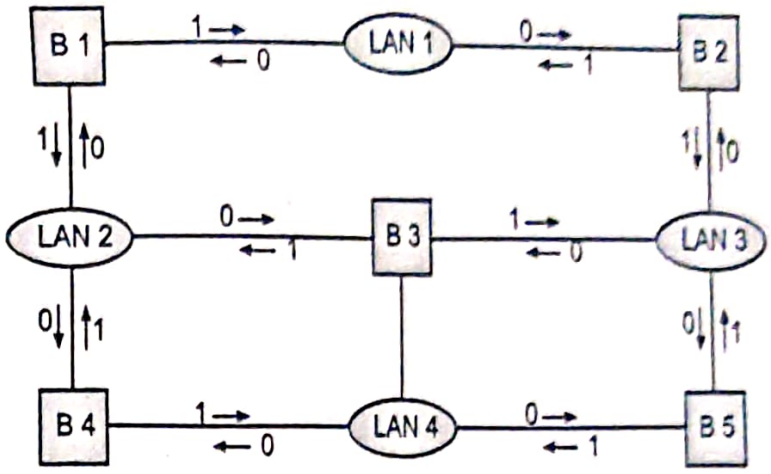
- The first AR frame which reaches its destination is considered to have followed the best route, and the route can be used for subsequent SR frames; the other AR frames are discarded. This method of locating a destination network can allow for indirect load balancing among multiple bridges connecting two networks.
- The more a bridge is loaded, the less likely it is to take part in the route finding process for a new destination as it will be slow to forward packets.
- A new AR packet will find a different route over a less busy path if one exists. This method is very different from transparent bridge usage, where redundant bridges will be inactivated; however, more overhead is introduced to find routes, and space is wasted to store them in frames.
- A switch with a faster backplane can be just as good for performance, if not for fault tolerance. They are primarily found in Token Ring networks.

3. Spanning Tree Bridge:

- A spanning tree is a graph in which there is no loop. In a bridged LAN, this means creating a topology in which each and every LAN can be reached from any other LAN through one path only i.e. no loop.
- You cannot change the physical topology of the system because of physical connections between cables and bridges, but you can create a logical topology which overlays the physical one.
- Fig. 5.9 shows a system with four LANs and five bridges. You have shown the physical system and its representation in graph theory.
- The connecting arcs show the connection of a LAN to a bridge and vice versa. To find the spanning tree, you need to assign a cost to each arc.
- The interpretation of the cost is left up to the systems administrator. It may be the path with minimum nodes, the path with minimum delay or the path with maximum bandwidth.



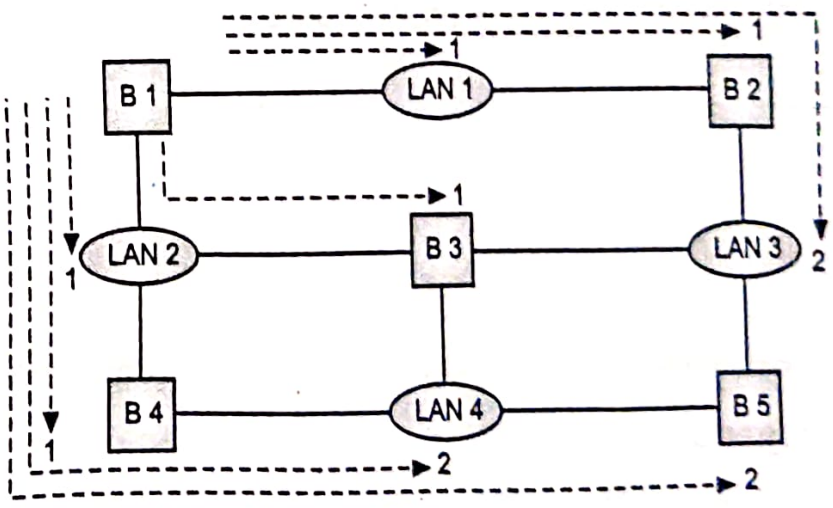
(a)



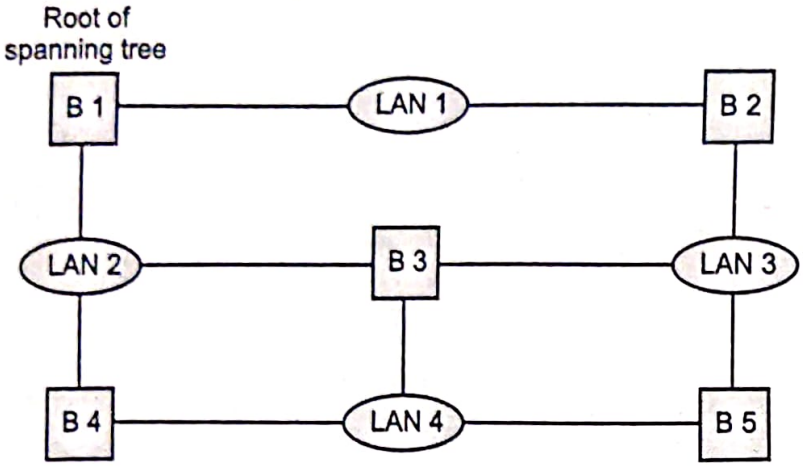
(b)

Fig. 5.9: A system of connected LANs and show its graph representation

- If two ports have the same shortest value, the systems administrator just chooses one. You have chosen the minimum nodes.
- The process to find the spanning tree involves three steps given below:
  1. Every bridge has a built-in ID. Each and every bridge broadcasts this ID so that all bridges know which one has the smallest ID. The bridge with the smallest ID is selected as the root bridge. You assume that bridge B1 has the smallest ID, for this reason B1 selected as the root bridge.
  2. The algorithm tries to find the shortest path from the root bridge to every other bridge. The shortest path can be found by examining the total cost from the root bridge to the destination. Fig. 5.10 shows the shortest paths.
  3. The combination of the shortest paths creates the shortest tree, which is also shown in Fig. 5.10.



(a) Shortest paths



(b) Spanning tree

Fig. 5.10: Determining the shortest paths and the spanning tree in a system of bridge

- Based on the spanning tree, you mark the ports that are part of the spanning tree, the forwarding ports, which forward a frame that the bridge receives. You also mark those ports that are not part of the spanning tree, the blocking ports, which block the frames received by the bridge. Fig. 5.11 illustrates the physical systems of LANs with forwarding points (solid lines) and blocking ports (broken lines).
- Note there is only one single path from any LAN to any other LAN in the spanning tree system. No loops are created. You can prove to yourself that there is only one path from LAN 1 to LAN 2, LAN 3 or LAN 4. Similarly, there is only one path from LAN 2 to LAN 1, LAN 3, and LAN 4. The same is true for LAN 3 and LAN 4.

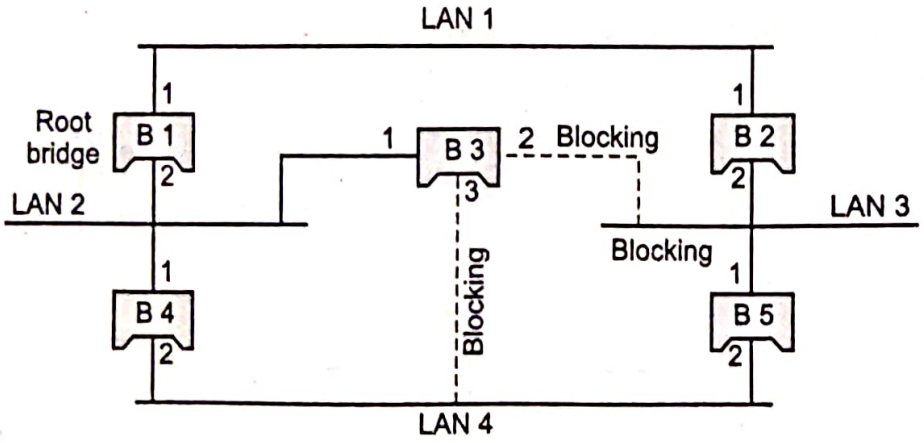


Fig. 5.11: The physical systems of LANs with forwarding points and blocking ports

5.4.2 Advantages of Bridges

- Advantages of bridges are given below:
  1. Self configuring.
  2. Primitive bridges are often inexpensive.

3. Reduce the size of collision domain by micro segmentation in non-switched networks.
4. Transparent to protocols above the MAC layer.
5. Allows the introduction of management/performance information and access control.
6. LANs interconnected are separate and physical constraints such as number of stations, repeaters and segment length do not apply.
7. Helps minimize bandwidth usage.
8. Used to interconnect two LANs.

5.4.3 Disadvantages of Bridges

- Disadvantages of bridges are given below:
  1. Does not limit the scope of broadcasts.
  2. Does not scale to extremely large networks.
  3. Buffering introduces store and forward delays; on average traffic destined for bridge will be related to the number of stations on the rest of the LAN.
  4. Bridging of different MAC protocols introduces errors.
  5. Because bridges do more than repeaters by viewing MAC addresses, the extra processing makes them slower than repeaters.

5.5 SWITCHES (S-18, S-19, S-22, S-23)

- A network switch is a computer networking device that connects network segments. The term commonly refers to a Network bridge that processes and routes data at the Data link layer (layer 2) of the OSI model.
- Switches that additionally process data at the Network layer (layer 3) are often referred to as Layer 3 switches or Multilayer switches.

Fig. 5.12: Switch

- The term network switch does not generally encompass unintelligent or passive network devices such as hubs and repeaters.
- The switch is a relatively new network device which is beginning to be used in Local Area Networks either in place of or in combination with Hubs.

- Unlike hubs, which broadcast messages to all ports regardless of the destination address, switches use internal address tables to route frames to only the port associated with the recipient node.
- Switches can be used to connect single network nodes or entire network segments and in this respect they superficially resemble a cross between a hub and a Bridge.
- Technically, switches work at the Data Link Layer of the OSI Reference Model, and use the MAC address (48 bit Hardware Address) within the frame to determine which node to send the frame to.

Difference between Hub and Switch:

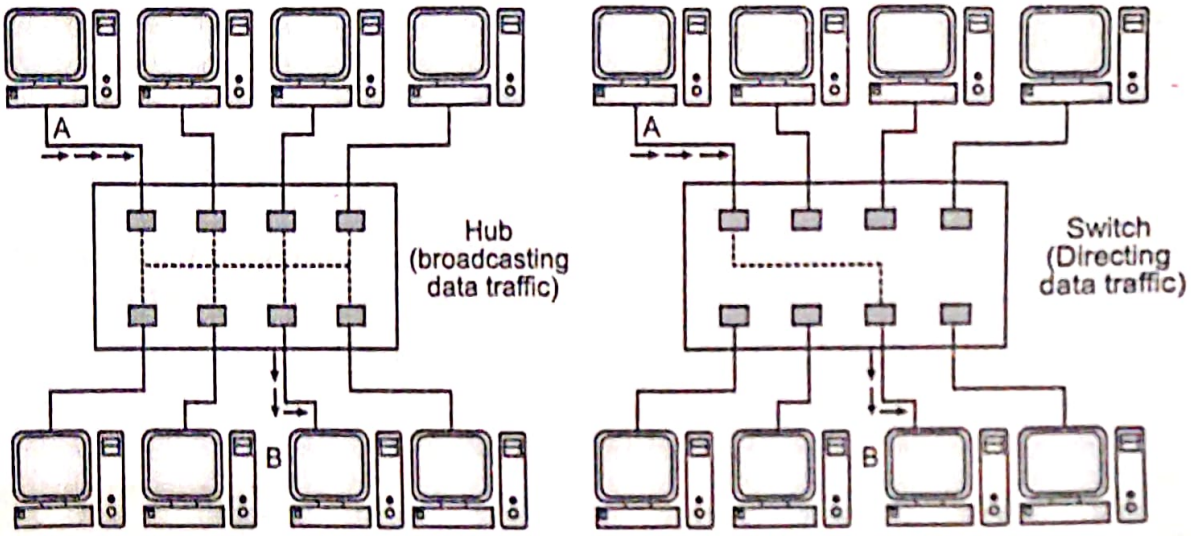


Fig. 5.13: The difference between a Hub and a Switch

- One major difference between a hub and a switch is that all the nodes connected to a hub share the available bandwidth, whereas a device connected to a switch port has the full bandwidth to itself.
- For example, if 8 nodes are connected using a hub on a 10 Mbps network, then each node may only get a portion of the 10 Mbps if other nodes on the hub want to communicate at the same time. With a switch, each node can communicate at 10 Mbps.
- The Fig. 5.13 illustrates the difference between a hub and a switch in a situation where node A transmits data to node B.
- With the hub, the data is transmitted to all nodes because the incoming frame from node A is broadcast to all ports. If other nodes are transmitting at the same time, collisions will occur.
- With the switch, the incoming frame is sent only to the port to which node B is attached via a "data pipe", avoiding possible collisions.

Types of Switches:

- There are two kinds of switches - the workgroup switch and the enterprise switch.

1. **The Workgroup Switch:**

- This is the direct replacement for the hub and works as described above, where the switch gives each port its own dedicated "data pipe" as opposed to the shared bandwidth of the traditional hub.
- This is like having a multi-port bridge with dedicated port-to-port connections, with one major difference. Hubs and bridges are connected to, and therefore rely on the backbone, whereas the workgroup switch has pre-assigned logical channels to avoid collisions.
- The transfer of data between ports uses specific channels for any possible bi-directional combinations on the device, so that for any given pair of ports there is a distinct and separate channel.

2. **The Enterprise Switch:**

- This is connected to the backbone, with no user connections directly attached to it (although this is possible).
- This allows the network management to connect the enterprise switch to hubs, bridges and Routers (the diagram below illustrates this concept).
- The bandwidth of the Enterprise Switch should be greater than the combined bandwidth of the entire network to which it is connected.

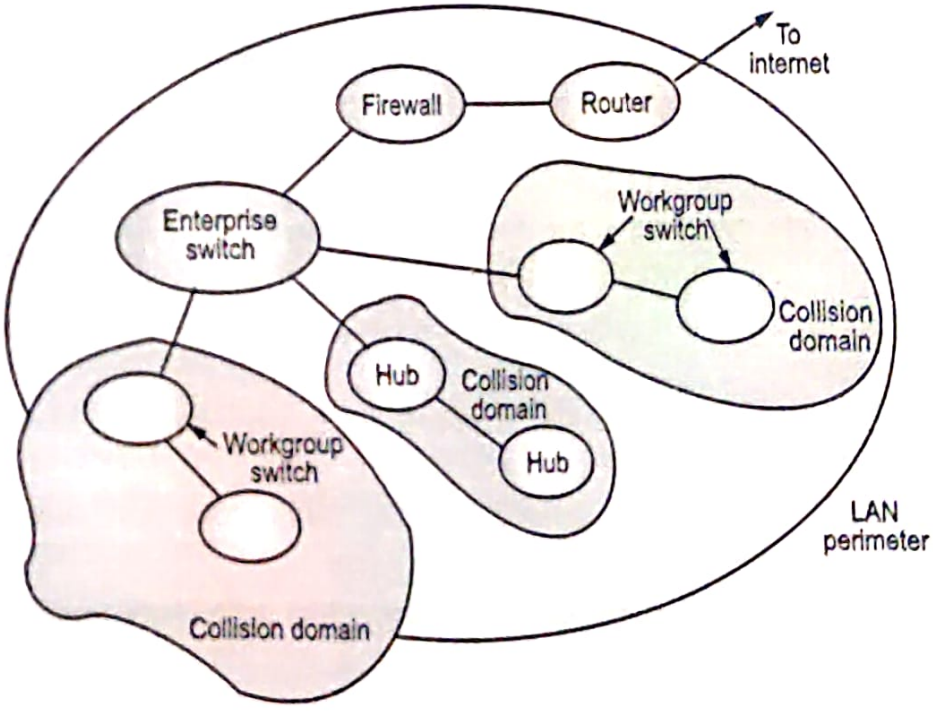


Fig. 5.14: Switch Architecture

Role of Switches in Network:

- Switches may operate at one or more OSI layers, including physical, data link, network, or transport (i.e., end-to-end).
- A device that operates simultaneously at more than one of these layers is called a Multilayer Switch, although use of the term is diminishing.

- In switches intended for commercial use, built-in or modular interfaces make it possible to connect different types of networks, including Ethernet, Fiber Channel, ATM, ITU-T G.hn and 802.11.
- This connectivity can be at any of the layers mentioned. While Layer 2 functionality is adequate for speed-shifting within one technology, interconnecting technologies such as Ethernet and token ring are easier at Layer 3.
- Interconnection of different Layer 3 networks is done by routers. If there are any features that characterize "Layer-3 switches" as opposed to general-purpose routers, it tends to be that they are optimized, in larger switches, for high-density Ethernet connectivity.
- In some service provider and other environments where there is a need for a great deal of analysis of network performance and security, switches may be connected between WAN routers as places for analytic modules.
- Some vendors provide firewall, network intrusion detection, and performance analysis modules that can plug into switch ports. Some of these functions may be on combined modules.
- In other cases, the switch is used to create a mirror image of data that can go to an external device.
- Since most switch port mirroring provides only one mirrored stream, network hubs can be useful for fanning out data to several read-only analyzers, such as intrusion detection systems and packet sniffers.

5.5.1 Layer 2 Switch

- A network bridge, operating at the Media Access Control (MAC) sublayer of the data link layer, may interconnect a small number of devices in a home or office.
- This is a trivial case of bridging, in which the bridge learns the MAC address of each connected device.
- Single bridges also can provide extremely high performance in specialized applications such as storage area networks.
- Bridges may also interconnect using a spanning tree protocol that allows the best path to be found within the constraint that it is a tree.
- In contrast to routers, bridges must have topologies with only one active path between two points.
- The older IEEE 802.1D spanning tree protocol could be quite slow, with forwarding stopping for 30–90 seconds while the spanning tree would re-converge.
- A Rapid Spanning Tree Protocol was introduced as IEEE 802.1w, but the newest edition of IEEE 802.1D-2004, adopts the 802.1w extensions as the base standard.
- While "layer-2 switch" remains more of a marketing term than a technical term, the products that were introduced as "switches" tended to use micro segmentation and Full duplex to prevent collisions among devices connected to Ethernets.

- By using an internal forwarding plane much faster than any interface, they give the impression of simultaneous paths among multiple devices.
- Once a bridge learns the topology through a spanning tree protocol, it forwards data link layer frames using a layer 2 forwarding method.
- There are four forwarding methods a bridge can use, of which the second through fourth method were performance-increasing methods when used on "switch" products with the same input and output port speeds:
  1. **Store and Forward:** The switch buffers and, typically, performs a checksum on each frame before forwarding it on.
  2. **Cut through:** The switch reads only up to the frame's hardware address before starting to forward it. There is no error checking with this method.
  3. **Fragment free:** A method that attempts to retain the benefits of both store and forward and cut through. Fragment free checks the first 64 bytes of the frame, where addressing information is stored. According to Ethernet specifications, collisions should be detected during the first 64 bytes of the frame, so frames that are in error because of a collision will not be forwarded. This way the frame will always reach its intended destination. Error checking of the actual data in the packet is left for the end device in Layer 3 or Layer 4 (OSI), typically a router.
  4. **Adaptive switching:** A method of automatically switching between the other three modes.
- Cut-through switches have to fall back to store and forward if the outgoing port is busy at the time the packet arrives.
- While there are specialized applications, such as storage area networks, where the input and output interfaces are the same speed, this is rarely the case in general LAN applications.
- In LANs, a switch used for end user access typically concentrates lower speed (e.g. 10/100 Mbit/s) into a higher speed (at least 1 Gbit/s). Alternatively, a switch that provides access to server ports usually connects to them at a much higher speed than used by end user devices.

5.5.2 Layer 3 Switch

- Within the confines of the Ethernet physical layer, a layer-3 switch can perform some or all of the functions normally performed by a router. A true router is able to forward traffic from one type of network connection (For example, T1, DSL) to another (For example, Ethernet, Wi-Fi).
- The most common layer-3 capability is awareness of IP multicast. With this awareness, a layer-3 switch can increase efficiency by delivering the traffic of a multicast group only to ports where the attached device has signaled that it wants to listen to that group.

- If a switch is not aware of multicasting and broadcasting, frames are also forwarded on all ports of each broadcast domain, but in the case of IP multicast this causes inefficient use of bandwidth. To work around this problem some switches implement IGMP snooping.
- The term "Layer 3 switch" often is used interchangeably with router, but switch is a general term without a rigorous technical definition. In marketing usage, it is generally optimized for Ethernet LAN interfaces and may not have other physical interface types.

5.6 ROUTERS (W-22)

- In an environment that consists of several network segments with differing protocols and architectures, a bridge might be inadequate for ensuring fast communication among all segments.
- A network this complex needs a device that not only knows the address of each segment, but can also determine the best path for sending data and filtering broadcast traffic to the local segment. Such a device is called a "router".

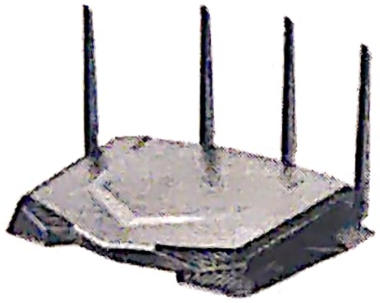


Fig. 5.15: Router

- Routers are networking devices which interconnect two different networks. For an example your home router connects your internet connection with a private local network.
- Routers work at the Network Layer of the OSI reference model. This means they can switch and route packets across multiple networks. They do this by exchanging protocol-specific information between separate networks.
- Routers read complex network addressing information in the packet and because they function at a higher layer in the OSI reference model than bridges, they have access to additional information.
- Router's software and hardware are usually tailored to the tasks of routing and forwarding information. For example, on the Internet, information is directed to various paths by routers.
- Bridges work at the Data-link layer MAC sublayer, and Routers work at the Network Layer.

- Routers connect two or more logical subnets, which do not necessarily map one-to-one to the physical interfaces of the router. In comparison, a network hub does not do any routing; instead every packet it receives on one network line gets forwarded to all the other network lines.
- Routers operate in two different planes:
  1. **Control Plane:** In which the router learns the outgoing interface that is most appropriate for forwarding specific packets to specific destinations.
  2. **Forwarding Plane**: Which is responsible for the actual process of sending a packet received on a logical interface to an outbound logical interface.

Functions:

- Routers can provide the following functions of a bridge:
  - Filtering and Isolating traffic.
  - Connecting network segments.
  - Routers have access to more of the information in packets than bridges have and use this information to improve packet deliveries.
  - Routers are used in complex networks because they provide better traffic management.

Routing Table:

- Routers maintain their own routing tables, usually consisting of network addresses; host addresses can also be kept if the network architecture calls for it.
- To determine the destination address for incoming data, the routing table includes:
  1. All known network addresses.
  2. Instructions for connection to other networks.
  3. The possible paths between routers.
  4. The costs of sending data over those paths.
- Router uses its data-routing table to select the best route for the data based on costs and available paths.
- Routing tables play a very important role in the routing process. They are the means by which the router makes its decisions. For this reason, a routing table needs to do two things. It must be up-to-date and complete.

Routing Process:

- When routers receive packets destined for a remote network, they send them to the router that manages the destination network. In some ways, this is an advantage because it means routers can:
  1. Segment large networks into smaller ones.
  2. Act as safety barriers between segments.
  3. Prohibit broadcast storms, because broadcasts are not forwarded.

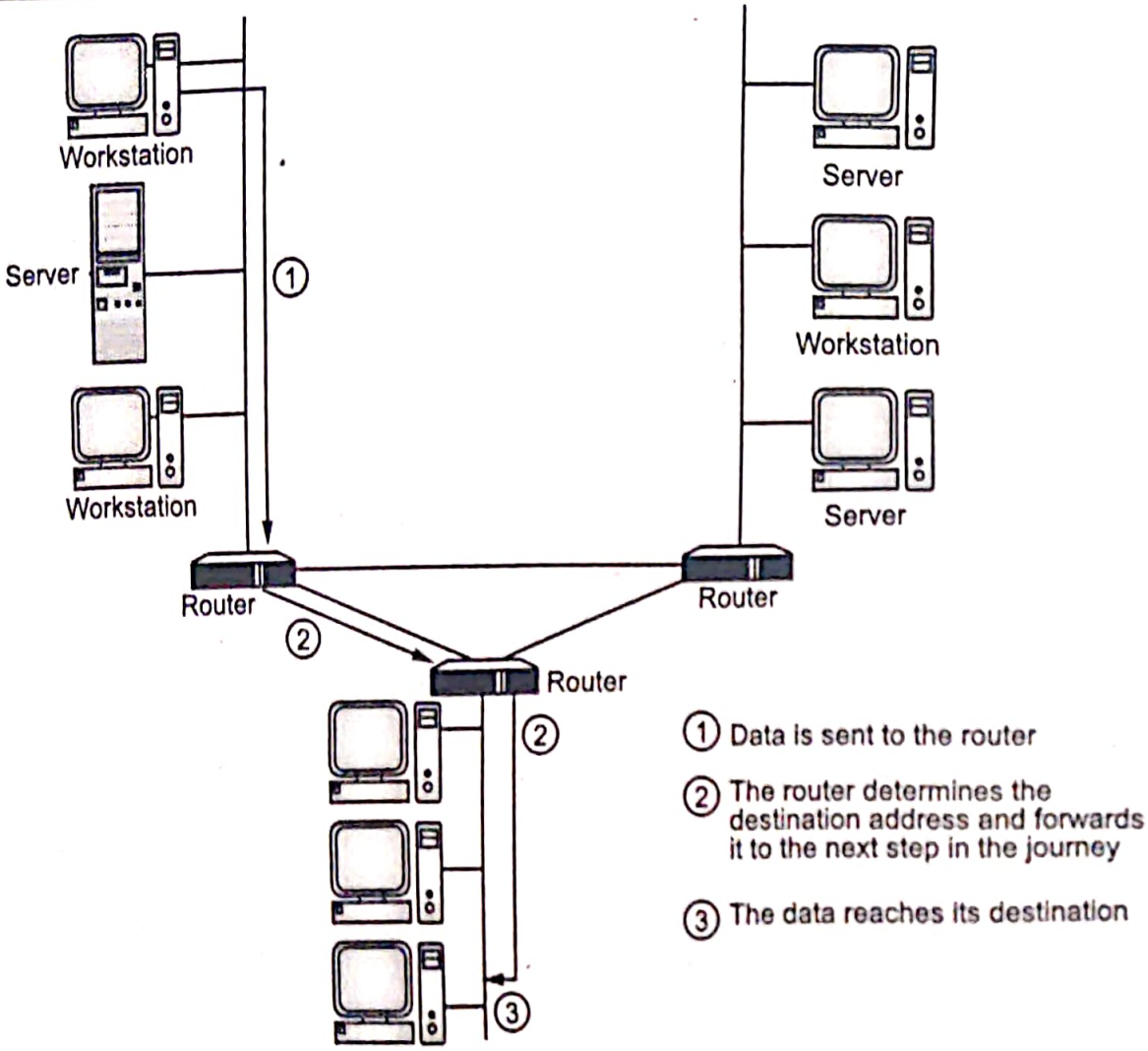


Fig. 5.16: Routing Process

- Routers do not communicate with remote hosts - it communicates only with other routers.

Routable Protocols:

Routing protocols determine how your data gets to its destination and helps to make that process as smooth as possible.

- All routing protocols can be classified into the following:
  - Distance Vector or Link State Protocols
  - Interior Gateway Protocols (IGP) or Exterior Gateway Protocols (EGP)
- **Examples of IGP:**
  - Open Shortest Path First (OSPF)
  - Routing Information Protocol (RIP)
  - Intermediate System to Intermediate System (IS-IS)
  - Enhanced Interior Gateway Routing Protocol (EIGRP)
- **Examples of EGP:**
  - Border Gateway Protocol (BGP)
  - Exterior Gateway Protocol (EGP)

- The ISO's InterDomain Routing Protocol (IDRP)

Classful or Classless Protocols:

- Classful routing protocols don't send subnet mask information during routing updates but classless routing protocols do. Examples: RIPv1 and IGRP.
- Classless routing protocols send IP subnet mask information during routing updates. Examples: RIPv2, EIGRP, OSPF, and IS-IS.

- There are two ways that the router can get the information for the routing table - through Static routing or dynamic routing.
  - **Static routing** is the process in which the system network administrator would manually configure network routers with all the information necessary for successful packet forwarding. The administrator constructs the routing table in every router by putting in the entries for every network that could be a destination.
  - **Dynamic routing** protocols allow routers to automatically add information to their routing tables from connected routers. With these protocols, routers send out topology updates whenever the topological structure of the network changes.

Routing Components: (W-22)

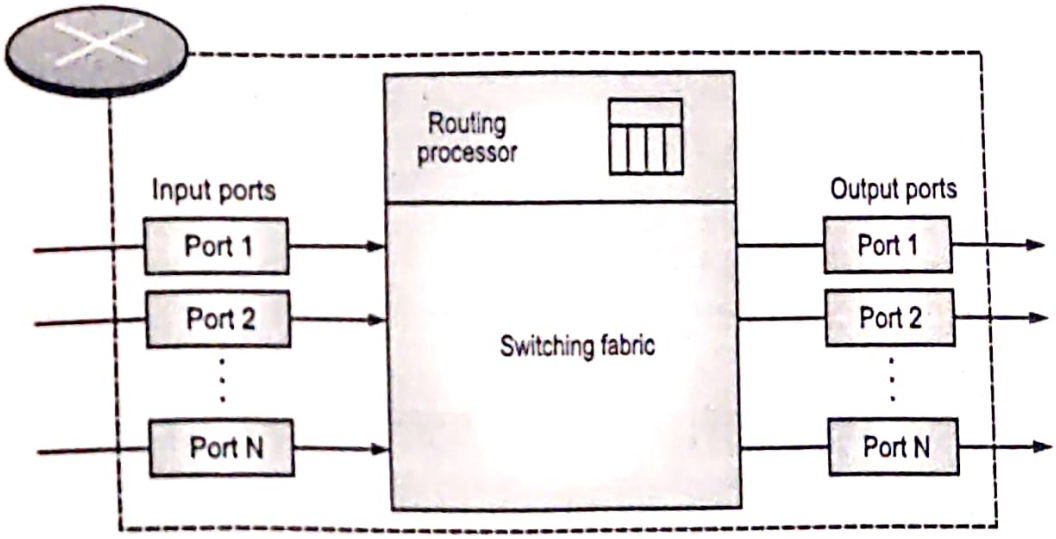


Fig. 5.17: Router Components

- Router has four components:
  1. Input ports
  2. Output ports
  3. Routing processor
  4. Switching fabric

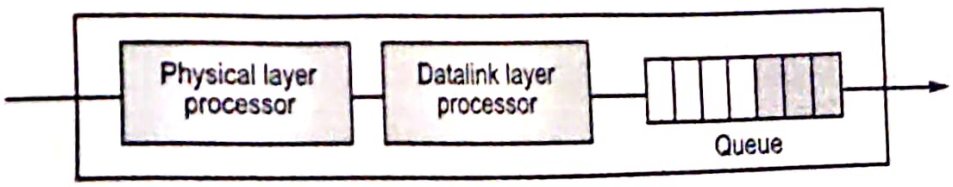


Fig. 5.18: Input Port

- **Input port** performs the physical and data link layer functions of router. The bits are constructed from the received signal.
- **Output port** performs the same functions as the input port but in the reverse order. Packet is encapsulated in a frame and physically transmitted on the line in raw bits fashion.

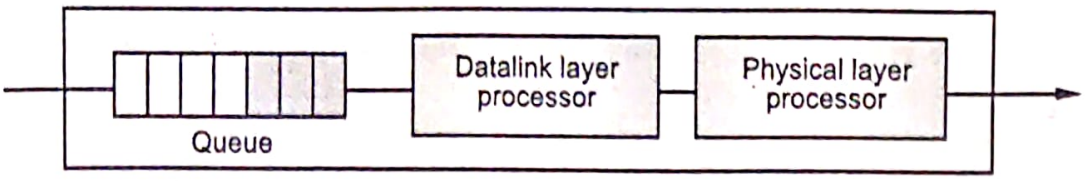


Fig. 5.19: Output Port

- **Routing processor** performs the function at network layer. The destination address is used to find the address of the next hop and at the same time the output port number from which the packet is sent out.
- **Switching fabrics** is used to move the packet from the input queue to output queue. The switching fabric is most difficult process in router. The following switching techniques are used:
  (a) Crossbar switching
  (b) Banyan switching
  (c) Batcher-Banyan switch.

Advantages of Routers:

- Following are the advantages of Routers:
  1. It shares connection between different network architectures such as Ethernet & token ring etc.
  2. It can choose best path across the internetwork using dynamic routing techniques.
  3. It can reduce network traffic by creating collision domains and also by creating broadcast domains.
  4. It provides sophisticated routing, flow control and traffic isolation.
  5. They are configurable which allows network manager to make policy based on routing decisions.

Drawbacks or disadvantages of Routers:

- Following are the drawbacks or disadvantages of Routers:
  1. Dynamic router communications can cause additional network overhead. This results into less bandwidth for user data.
  2. They are slower as they need to analyze data from physical to network layer.
  3. They require considerable amount of initial configurations.

4. They are protocol dependent devices which must understand the protocol they are forwarding.
5. They only do operations using routable protocols.
6. They are expensive compare to other network devices.

5.7 GATEWAYS

- Gateways make communication possible between different architectures and environments. They repackage and convert data going from one environment to another so that each environment can understand the other's environment data.
- A gateway repackages information to match the requirements of the destination system.
- Gateways can change the format of a message so that it will conform to the application program at the receiving end of the transfer. A gateway links two systems that do not use the same:
  1. Communication protocols
  2. Data formatting structures
  3. Languages
  4. Architecture.
- For example, electronic mail gateways, such as X.400 gateway, receive messages in one format, and then translate it, and forward in X.400 format used by the receiver and vice versa.
- To process the data, the gateway:
  1. Decapsulates incoming data through the networks complete protocol stack.
  2. Encapsulates the outgoing data in the complete protocol stack of the other network to allow transmission.
- Also a gateway is a device that can join together networks that use different protocols, example, Novell SPX to TCP/IP. The gateway contains two complete protocol stacks - one for each system.

Levels of Gateways:

- Data is extracted from a packet arriving at one port and is retransmitted at the other port using a different protocol. Although gateways are considered to exist at the top of the OSI Reference Model, in reality they can be found at various levels of the model:
  - **Physical Layer Gateway:** Carries out translation from one speed to another or from one medium to another, i.e. 10 Mbps Ethernet to 100 Mbps Fast Ethernet or UTP to fiber optic (this term is not generally used).
  - **MAC Gateway:** Translates one MAC protocol to another, i.e. Token Ring to Ethernet or vice versa. These are more commonly referred to as translating and tunneling bridges.

- **Architecture Gateway:** Changes the packet from one protocol stack (or architecture) to another, i.e. SNA to TCP/IP, TCP/IP to IPX/SPX or TCP/IP to Appletalk. This is achieved by replacing all the headers from the network layer up to the application layer.
- **Application Gateway:** These can translate Application Layer protocols (X.500, X.400) or actual end user applications.

- Gateways can be either dedicated standalone box, a specific installed printed circuit-board or software loaded onto an existing server.
- The term Gateway is also used to refer to a network point that acts as an entrance to another network.
- In a company network, a proxy server acts as a gateway between the internal network and the Internet and may also act as a firewall server.
- The term is also used to refer to any device that passes packets from one network to another network in their trip across the Internet.
- Fig 5.20 shows the application gateway is required for communication between two different Network Architectures.

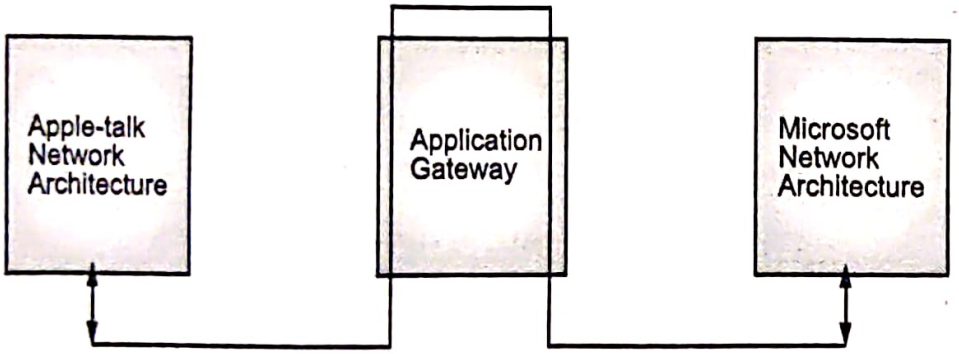


Fig. 5.20: Application Gateway

5.8 NETWORK INTERFACE CARD (NIC)

- A NIC is either an expansion card (the most popular implementation) or built in to the motherboard of the computer. In most cases, a NIC connects to the computer through expansion slots, which are special slots located on a computer's motherboard that allow peripherals to be plugged directly into it. In some notebook, NIC adapters can be connected to the printer port or through a PC card slot.
- NIC cards generally all have one or two light emitting diodes (LEDs) that help in diagnosing problems with their functionality. If there are two separate LEDs, one of them may be the Link LED, which illuminates when proper connectivity to an active network is detected. This often means that the NIC is receiving a proper signal from the hub/MAU or switch, but it could indicate connectivity to and detection of a carrier on a coax segment or connectivity with a router or other end device using a crossover

cable. The other most popular LED is the Activity LED. The Activity LED will tend to flicker, indicating the intermittent transmission or receipt of frames to or from the network.

Summary

- Networking connecting devices include all computers, peripherals, interface cards and other equipment needed to perform data-processing and communications within the network.
- A hub is a small rectangular box, often constructed mainly of plastic that receives its power from an ordinary wall outlet. A hub joins multiple computers or other network devices together to form a single network segment. Types are: Passive and Active Hub.
- Passive hub does not provide any additional feature except for working just as an interface between the topology.
- Active hub takes active participation in data communication within the network / LAN.
- A repeater is a network device that receives a signal on one of its connections and passes that signal on to all of its other connections after regenerating it.
- Network bridges can be used to connect LAN segments or to isolate heavily trafficked segments from the rest of the network. Three types of bridges are used in networks: Transparent Bridge, Source Route Bridge and Spanning tree bridge.
- A network switch is a computer networking device that connects network segments. The term commonly refers to a Network bridge that processes and routes data at the Data link layer (layer 2) of the OSI model. There are two kinds of switches - the workgroup switch and the enterprise switch.
- Routers can share status and routing information with one another and use this information to bypass slow or malfunctioning connections.
- Routers maintain their own routing tables, usually consisting of network addresses; host addresses can also be kept if the network architecture calls for it.
- Gateways make communication possible between different architectures and environments. They repackage and convert data going from one environment to another so that each environment can understand the other's environment data.

Check Your Understanding

1. _____ called Network layer Device.
   (a) Router (b) Gateway
   (c) Bridge (d) Switch
2. _____device is not amplified the signal.
   (a) Router (b) Gateway
   (c) Bridge (d) Switch

3. The device that provides a central connection point for cables is _____.
   (a) Router (b) Gateway
   (c) HUB (d) Switch
4. Which networking device connects one LAN to other LAN using same protocol standards?
   (a) Router (b) Gateway
   (c) HUB (d) Switch
5. _____ device is called intelligent device in networking
   (a) Router (b) Gateway
   (c) HUB (d) Switch

ANSWERS

1. (a)	2. (b)	3. (c)	4. (d)	5. (a)

Practice Questions

Q.I Answer the following questions in short.

1. What are network connectivity devices?
2. What is active and passive hub?
3. Which are types of bridges in networking?
4. Describe the term transparent bridge.
5. Which two frame types are used in order to find the route to the destination network segment in Source Route Bridging?

Q.II Answer the following questions.

1. What is Router? Explain its components..
2. Explain the various network connecting devices.
3. With a neat diagram explain repeaters.
4. Describe hub in brief.
5. Explain switches with suitable diagram.
6. What are repeaters? Define different types of repeaters.
7. Compare between:
   (i) Repeater and Hub
   (ii) Switches and Hub
   (iii) Bridges and Gateways
   (iv) Router and Hub.

Q.III Define the following terms:

1. Gateways
2. Source routing bridges

3. Router
4. Hub
5. Repeater

Previous Exams Questions

Summer 2018

1. Define the bridge. Explain the types of bridges. [5M]

Ans. Please refer to Section 5.4.

2. What is switch? How does it differ from HUB? [5M]

Ans. Please refer to Section 5.5 and 5.2.

3. Explain active and passive HUB. [5M]

Ans. Please refer to Section 5.2.2 and 5.2.3.

4. Write a short note on Repeater. [5M]

Ans. Please refer to Section 5.3.

Winter 2018

1. What is bridge? What are its types? Explain any one in details. [5M]

Ans. Please refer to Section 5.4.

Summer 2019

1. Define the Bridge. Explain types of Bridges. [5M]

Ans. Please refer to Section 5.4.

2. What is switch? How does it differ from HUB? [5M]

Ans. Please refer to Section 5.5 and 5.2

3. Explain active and passive HUB. [5M]

Ans. Please refer to Section 5.2.2 and 5.2.3

4. Write a short note on Repeater. [5M]

Ans. Please refer to Section 5.3