Unit 5 Network Connectivity Devices

Hub:-

1) **Hub Constructions:-**
   a) A hub is a small rectangular box, often made of plastic that receives its power from an ordinary wall outlet.
   b) A hub joins multiple computers (or other network devices) together to form a single network segment.
   c) On this network segment, all computers can communicate directly with each other.
   d) Ethernet hubs are by far the most common type, but hubs for other types of networks such as USB also exist.
   e) A hub includes a series of ports that each accepts a network cable.
   f) 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 eight, 12, 16, and even 24 ports.

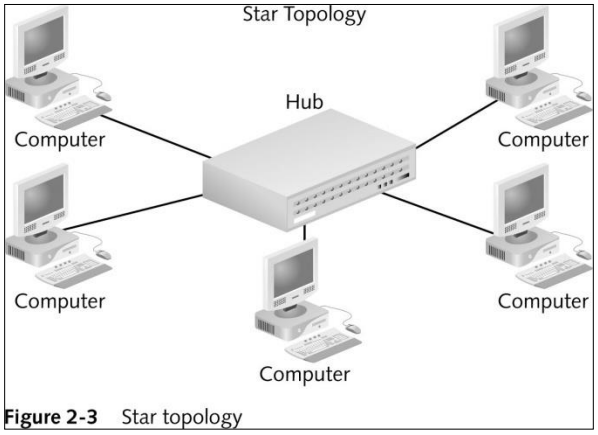


Figure 2-3 Star topology

2) **Key Features of Hubs**
   a) Hubs classify as Layer 1 devices in the OSI model.
   b) At the physical layer, hubs can support little in the way of sophisticated networking.
   c) Hubs do not read any of the data passing through them and are not aware of their source or destination.
   d) Essentially, a hub simply receives incoming packets, possibly amplifies the electrical signal, and broadcasts these packets out to all devices on the network - including the one that originally sent the packet!
   e) A computer's network interface card sends out packets to the network.
   f) The hub receives this information and passes it through all the ports on the hubs that have attached cables.
   g) This means that the computer that sent the data also gets it back.
   h) The networking protocols have ways of determining which computer on the network needs to process the information

3) Need of Hub:-
   a) 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 with the network.

b) There are many types of hubs with various features/specifications, which provide the types of functionality you need in building network.

4) **Types of HUB:-**

Technically speaking, three different types of hubs exist:

a) passive
b) active
c) intelligent

a) Passive Hub:-

i. Passive hubs do not amplify the electrical signal of incoming packets before broadcasting them out to the network.
ii. Passive hubs are the ones, which does not provide any additional feature except for working just as an interface between the topology.
iii. In passive hub there is very hard to get any help from the passive hubs while troubleshooting in case if there is any fault in the hardware or the network.
iv. Passive hub simply receiving signals on input ports and broadcasts it(them) on the output ports without even rectifying it(them).

b) Active Hubs

i. An active hub works more than just a connector but also regenerates the data bits to ensure the signals are strong.
ii. It provides an active participation in the network aside from acting as an interface.
iii. It participates in the data communication, such as storing signals received through the input ports, before forwarding them.
iv. It can monitor the data it is forwarding and sometimes help improve signals before forwarding them to other connections.
v. Such a feature makes troubleshooting network problems easier intelligent hubs add extra features to an active hub that are of particular importance to businesses.

c) An intelligent hub

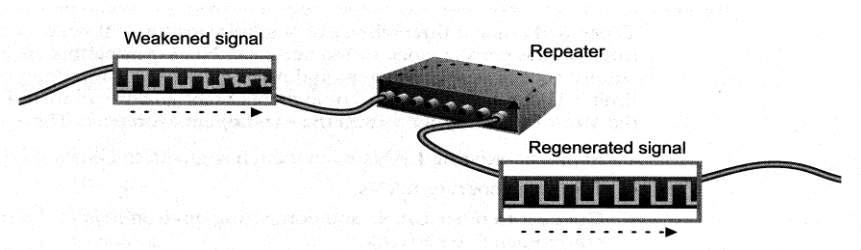
i. An intelligent hub can perform everything that the passive hub and active hub do, and help manage network resources effectively to ensure that the performance of the network is highly efficient.
ii. An intelligent hub can also help in troubleshooting by pinpointing the actual location of the problem.
iii. An intelligent hub typically is stackable (built in such a way that multiple units can be placed one on top of the other to conserve space).

Repeater:-

1. 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.
2. A Repeater enables signals to travel longer distances over a network. Repeaters work at the OSI's Physical layer. A repeater regenerates the received signals and then retransmits the regenerated (or conditioned) signals on other segments
3. 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.

4. A repeater is the simplest facility used for network interconnection, whose major function is to receive a network signal from one LAN terminal cable segment and to regenerate and retransmit the signal as it is in its original strength over a one or more other cable segment.



5. Basically repeater regenerates the strength of the signal before transmitting it
6. Repeaters operate in the OSI model Physical layer and are transparent to all the protocols operating in the layers above the Physical layer.
7. A specific LAN implementation usually places a limit on the physical size of a single cable segment.
8. The limit is based on the physical medium and transmission techniques used
9. Repeaters allow a network to be constructed to exceed the size limit of a single, physical, cable segment.
10. The number of repeaters that can be used intended is generally limited by a particular LAN implementation.
11. Using a repeater between two or more LAN cables segment requires that the same physical layer protocol be used to send signal over all the cable segments

12. Example of how this work

   a. Two LAN cable segment in an Ethernet LAN that both use baseband transmission could be connected with a repeater.
   b. Different types of physical transmission medium can be connected using a properly designed repeater as long as they handle similar type of signal, as explained below:
   c. Ethernet repeaters are available that allows all the various types of baseband Ethernet transmission medium, including 10baseT, Coaxial cable, 10base2 and twisted pair cable segment to be interconnected in the same LAN

13. Repeaters defines as two classes

   a. Class I: These are not stackable, and cannot be daisy chained.
   b. Class II: These are stackable, and can be daisy chained.

14. Advantages of a repeater

   a. Simple to connect
   b. Cost effective
   c. Ability to strengthen signal

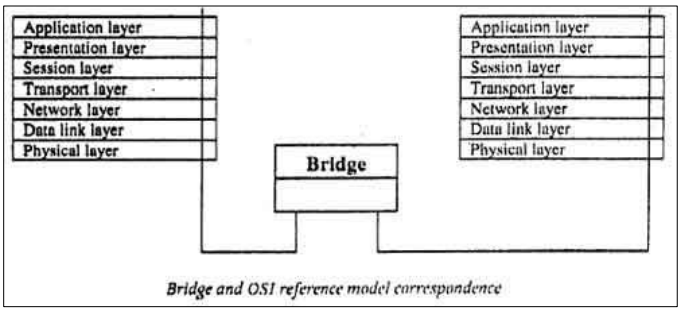
15. Disadvantages of a repeater

   a. Repeaters provide no method for isolating traffic generated on one cable segment from traffic generated by the other cable segment

b. When network uses a repeater to connect cable segment A to segment B whether or not there is a station in segment B that is the destination of the signal

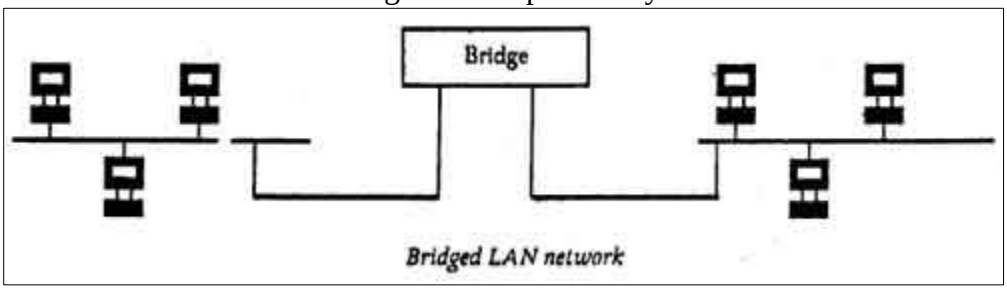
Bridge:-

1. Like repeaters, bridges are used to connect similar LANs together, for example, Ethernet-to-Ethernet and operate at the bottom two layers of the OSI model, i.e. physical layer and data link layer.
2. As it operates on second layer of the OSI model,' it relays only necessary data to other signals. MAC addresses (physical addresses) are used to determine whether data is necessary or not.
3. It passes information from one LAN segment to another based on the destination address of the packet. In other words, when a bridge receives data through one of its ports, it checks the data for a MAC address.
4. If this address matches that of the node connected to other port, the bridge sends this data through this port. This action is called forwarding. If the address does not match with any node connected to other port, the bridge discards it.
5. This action is called filtering. Unlike repeaters, bridges have buffers to store and forward packets in the event that the destination link is congested with traffic.
6. The main advantage of bridge over repeater is that it has filtering action.
7. If any noise on Ethernet occurs because of collision or disturbance in electrical signal, the bridge will consider it as an incorrectly formed frame and win not forward to the segment connected to other port of the bridge. Note that bridge can relay broadcast packets and packets with unknown destination.



Bridge and OSI reference model correspondence

8. So far, we have seen that at the maximum four repeaters can be used to connect multiple Ethernet segments. However, if a bridge is provided between repeaters, this limit of four is increased. The maximum number of bridges is not specifically limited.



Bridged LAN network

9. From architecture point of view bridges are protocol independent devices and are very simple. They do not perform complex processes on the data packets traveling through them such as the evaluation of the network as a whole in order to make end-to-end routing decisions.

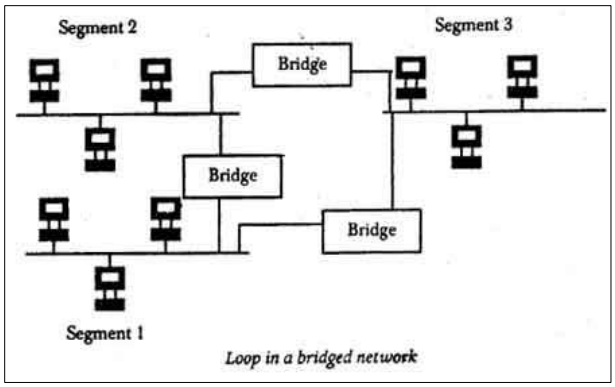
10. They simply read the destination address of the incoming data packet and forward it along its way to the next link.
11. Therefore, bridges are Inexpensive and fast. There are bridges called cascading bridges, and are used to support multiple LANs connected by multiple media.
12. Dissimilar LANs such as Ethernet-to-token ring can also be connected with the help of bridge known as encapsulating bridge.
13. The function of encapsulating bridge is also very simple. It encapsulates the originating LAN data along with control information of the end user LAN. Bridges with routing function between LANs are also available.
14. Bridge Protocols: - Bridge protocols include spanning tree, source routing protocol, and source routing transparent.

a.Transparent Bridge:-

- The bridge is called transparent because is activity is transparent to the network hosts.
- A transparent bridge is a type of Network Bridge. It interconnects several computers in a network by forwarding packets to hosts.
- A transparent bridge whose presence and operation is invisible to hosts on the network.
- Derives its name from the fact that the devices on the network are unaware of its existence.
- 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 networks of computers (a layer 2 device in the OSI model)
- While a network bridge simply enables local network (or segments) to communicate with each other, but forwards the traffic to all ports, a transport 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 is use a forwarding database to send frames across network segment.

b. Spanning Tree Protocol (STP) Bridge

- This is also known as adaptive or self-learning bridges and is defined in IEEE 802.1 standards ideally, in bridged network, the network tree of the bridge provides only one span (link) for each LAN-to-LAN connection and therefore, no network with bridges can form a loop. Sometimes, looping can occur.



- A broadcast data packet sent by the computer attached on segment 1can reach to all computers attached on segment 2 and 3 without a connection between segment 1 and 3 .Sometimes, the bridge connection between segment 1and 3 or like is provided to give the network more redundancy. Now, in this case the same broadcast packet sent by the segment 1 will reach to segment 3 by two routes i.e. from segment 1 to 2 to 3 and another by segment 1 to 3. In this manner the computers on segment 3 will receive duplicate packets. In case of large networks some segments may receive many packets and thus cause looping.

c. IBM Source Routing Protocol (SRP) Bridge

- These are programmed with specific routes for each packet based on considerations such as the physical location of the nodes, and the number of bridges involved.
- Source Routing Transparent (SRT)
- It is defined in theIEEE802.1 standard. It is effectively a combination of STP and SRP. The SRT router can connect LANs by either method, as programmed.

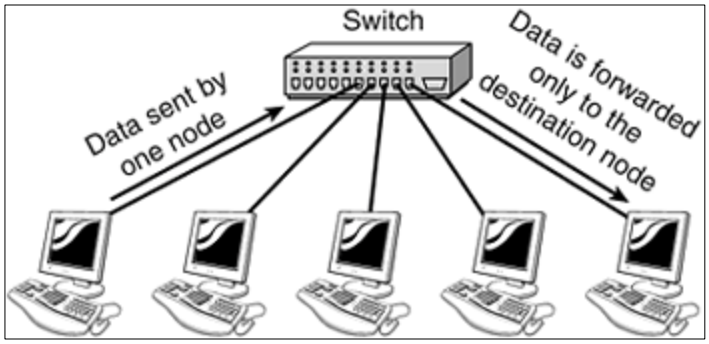
Classification of Bridges

These are classified into local and remote bridges:

1. Local bridges are ordinary bridges
2. Remote bridges are used to connect networks that are far from each other. A WAN is generally provided between two bridges.

Switches

1. Like hubs, switches are the connectivity points of an Ethernet network. Devices connect to switches via twisted-pair cabling, one cable for each device.
2. The difference between hubs and switches is in how the devices deal with the data that they receive.
3. Whereas a hub forwards the data it receives to all of the ports on the device, a switch forwards it only to the port that connects to the destination device.
4. It does this by learning the MAC address of the devices attached to it, and then by matching the destination MAC address in the data it receives. Figure 1 shows how a switch works.

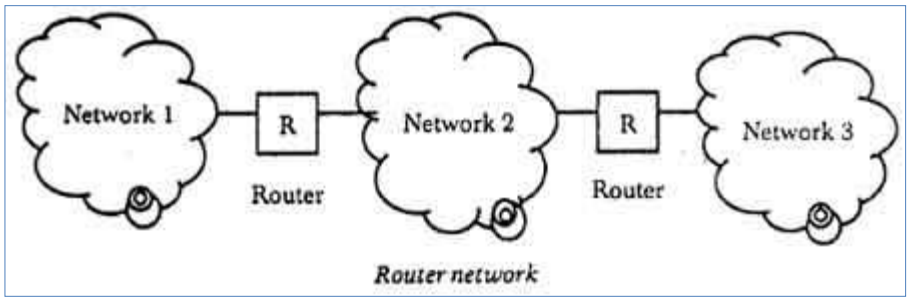


5. By forwarding data only to the connection that should receive it, the switch can improve network performance in two ways.
6. First, by creating a direct path between two devices and controlling their communication, it can greatly reduce the number of collisions on the network.
7. As you might recall, collisions occur on Ethernet networks when two devices attempt to transmit at exactly the same time.
8. In addition, the lack of collisions enables switches to communicate with devices in full-duplex mode. In a full-duplex configuration, devices can send and receive data from the switch at the same time.
9. Contrast this with half-duplex communication, in which communication can occur in only one direction at a time. Full-duplex transmissions speeds are double that of a standard, half-duplex, connection. So, a 10Mbps connection becomes 20Mbps, and a 100Mbps connection becomes 200Mbps.
10. The net result of these measures is that switches can offer significant performance improvements over hub-based networks, particularly when network use is high.
11. Irrespective of whether a connection is at full or half duplex, the method of switching dictates how the switch deals with the data it receives. The following is a brief explanation of each method:
    - Cut-through in a cut-through switching environment, the packet begins to be forwarded as soon as it is received. This method is very fast, but creates the possibility of errors being propagated through the network, as there is no error checking.
    - Store-and-forward unlike cut-through, in a store-and-forward switching environment, the entire packet is received and error checked before being forwarded. The upside of this method is that errors are not propagated through the network. The downside is that the error checking process takes a relatively long time, and store-and-forward switching is considerably slower as a result.
    - Fragment Free to take advantage of the error checking of store-and-forward switching, but still offer performance levels nearing that of cut-through switching, Fragment Free switching can be used. In a Fragment Free-switching environment, enough of the packet is read so that the switch can determine whether the packet has been involved in a collision. As soon as the collision status has been determined, the packet is forwarded.
    - Adaptive Switching method of automatically switching between the other three modes.

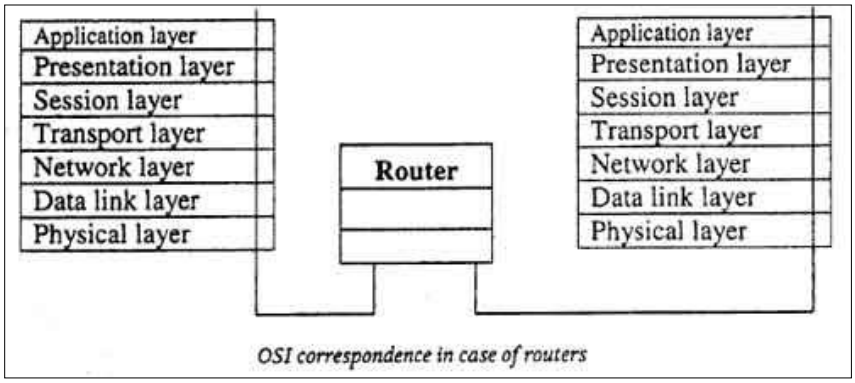
Routers:-

1. **Routers** are used to connect both similar and dissimilar LANs. Router operates on the network layer of OSI model using the physical layer, data link layer and network layer to provide connectivity, addressing and switching.
2. These are highly intelligent devices. In case *of TCP/IP* network, Internet Protocol (IP) is used as addresses for network; this is the router which interprets the IP address and delivers the packet reliably.
3. Now, we may say that router transmits the network layer data and therefore, provides transmission of data between LANs that use different data link protocols but using the same network layer protocol.

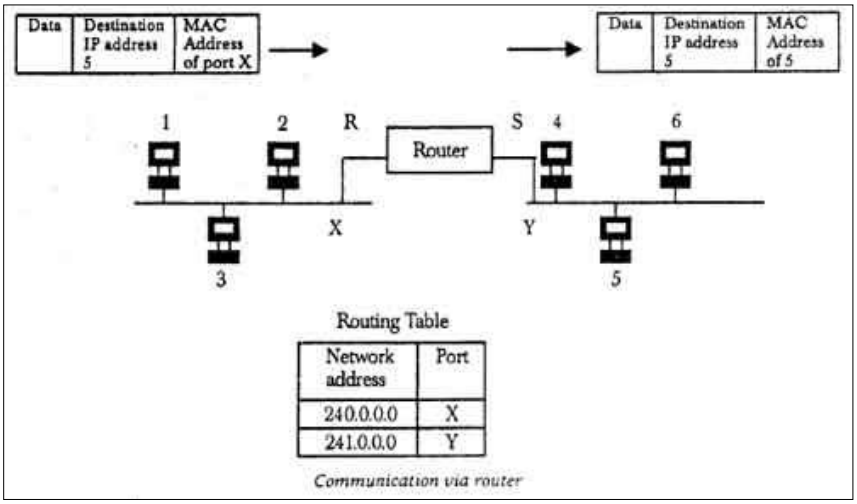
4. Because of this, Etl1ernet can be connected with token ring network using routers. Additionally, routers provide connectivity La MAN (SMDS) and WAN (X.25, Frame Relay and ATM).
5. Routers are protocol sensitive; typically supporting multiple protocols and large and varying packet sizes such as might be involved in supporting both Ethernet and Token Ring.
6. A network consisting of routers can have multiple paths unlike bridges. Normally, the shortest of all paths in the network is used to transfer packets.



Router network



OSI correspondence in case of routers



Communication via router

7. Consider a case for data transmission from computer 1 to computer 5 on the network. When computer 1 starts sending the data, it compares its IP address with computer 5, i.e. destination computer addresses to know whether computer 5 lies on its own network or not.

8. When computer 1 finds that it is not on its network, it transmits a data packet containing the MAC address R of router in this case.
9. When router receives this packet, it sets the MAC address of computer 5 and sends packet to the port which has the same IP destination address as given in data packet. In this manner computer 5 receives the data packet.
10. **Characteristics of Routers**

- Routers are multiport devices with high - speed backbones
- Routers also support filtering and encapsulation like bridges
- Like bridges routers are also self-learning, as they can communicate their existence. to other devices and can learn of the existence of new routers, nodes and LAN segments
- As explained earlier, they route traffic by considering the network as a whole. It shows that they use a high level of intelligence to accomplish this task. This characteristic makes them superior than hubs and bridges because they simply view the network on a link-by-link basis
- The packet handled by router may include destination address, packet priority level, least-cost route, minimum route delay, minimum route distance, and route congestion level
- Routers constantly monitor the condition of the network, as a whole to dynamically adapt to changes in the condition of the network
- They typically provide some level of redundancy so that they are less susceptible to catastrophic failure.

11. **Router Protocols**

Router protocols consist of both bridging and routing protocols as listed below:

- **Inter-router Protocols**

These are router-to-router protocols that can operate over dissimilar networks. This protocol routes information and stores data packets during periods of idleness.

- **Serial Line Protocols**

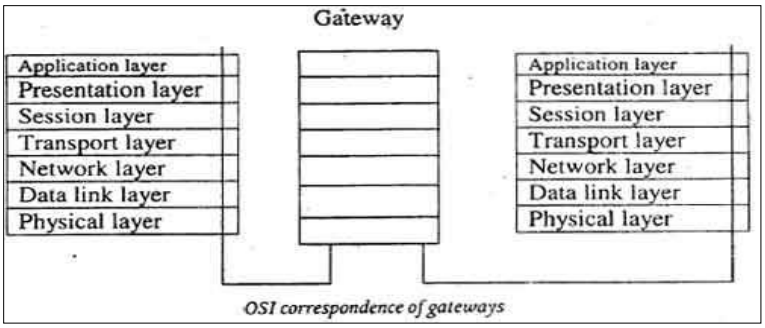
This protocol is widely used over serial or dialup links connecting unlike routers. Examples include HDLC, SLIP (Serial Line Interface Protocol), and PPP (Point-to-Point Protocol).

- **Protocol Stack Routing and Bridging Protocols**

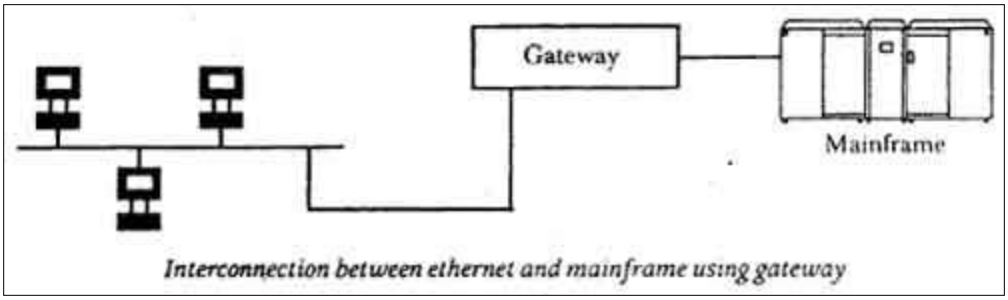
This advises the router as to which packets should be routed and which should be bridged.

Gateway:

1. This advises the routers are used to connect dissimilar LANs and perform all the functions of bridges and routers.
2. It operates at all seven layers of the OSI Reference Model.
3. These are actually predecessors of router nowadays and are technology wise more expensive and highly functional.
4. They in general consist of software which resides in a host computer, such as mid-range or mainframe.



OSI correspondence of gateways



Interconnection between ethernet and mainframe using gateway

5. 5.

5. **Characteristics of Gateways**
   a. Gateways provide full protocol conversion from one proprietary LAN technology to another, i.e. Ethernet to token ring or FDDI or any other standard or protocol rather than encapsulation
   b. It uses higher layers of the OSI model, perhaps through layer 7, the application layer. IBM SNA, DEC net, Internet TCP/IP and other protocols can be converted from network-to-network
   c. Unlike bridges and routers, gateways operate slowly because of protocol conversion. Consequently, they may create bottlenecks of congestion during periods of peak usage.

5. Default Gateway

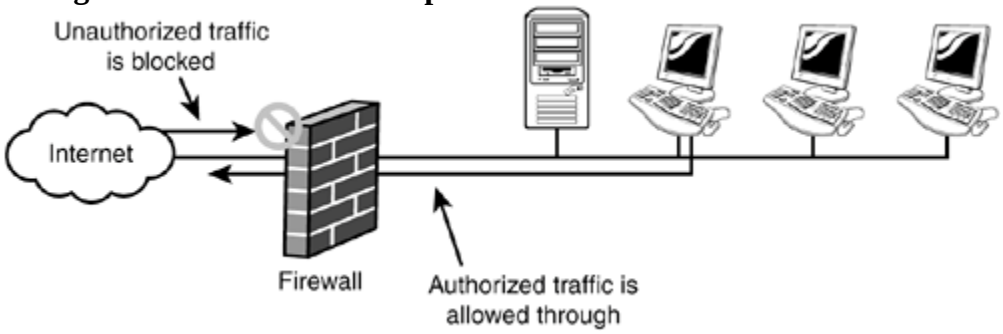
   a. Default gateway consists of manually registering router IP addresses in the host. This method is simple; and is the most frequently used. Note however, that if two or more routers are connected to the same subnet, the network administrator must determine which of these routers the message should be sent to.
   b. To solve this problem, a message called ICMP redirect is available. Default gateway checks the destination host address in the received message.
   c. If it determines that the message should be sent via other router, it will send back a redirect message that includes the IP address of the selected router, to the source host. When the source host receives this message, it stores the destination host address as well as the second router address so that it can send messages addressed to this host via the second router.

Firewall:-

1. In today's network environments, firewalls are being used to protect systems from external as well as internal threats.
2. Although firewalls initially became popular in corporate environments, many home networks with a broadband Internet connection now also implement a firewall to protect against Internet borne threats.
3. Essentially; a firewall is an application, device, system, or group of systems that controls the flow of traffic between two networks.

4. The most common use of a firewall is to protect a private network from a public network such as the Internet.
5. However, firewalls are also increasingly being used as a means to separate a sensitive area of a private network from less-sensitive areas.
6. At its most basic, a firewall is a device (it could be a computer system or a dedicated hardware device) that has more than one network interface and manages the flow of network traffic between those interfaces.
7. How it manages the flow and what it does with certain types of traffic depends on its configuration. Figure 1 shows the most basic firewall configuration.

Figure 1 A basic firewall implementation.



8. Strictly speaking, a firewall performs no action on the packets it receives besides the basic functions just described.
9. However, in a real-world implementation, a firewall is likely to offer other functionality, such as Network Address Translation (*NAT*) and proxy server services. Without NAT, any host on the internal network that needs to send or receive data through the firewall needs a registered IP address.
10. Although there are such environments, most people have to settle for using a private address range on the internal network and therefore rely on the firewall system to translate the outgoing request into an acceptable public network address.
11. Although the fundamental purpose of a firewall is to protect one network from another, you need to configure the firewall to allow some traffic through. If you don't need to allow traffic to pass through a firewall, you can dispense with it entirely and completely separate your network from others.
12. A firewall can employ a variety of methods to ensure security. A firewall can use just one of these methods, or it can combine different methods to produce the most appropriate and robust configuration. The following sections discuss the various firewall methods that are commonly used: packet-filtering firewalls, circuit-level firewalls, and application gateway firewalls.
13. Of the firewall methods discussed in this chapter, packet filtering is the most commonly implemented. Packet filtering enables the firewall to examine each packet that passes through it and determine what to do with it, based on the configuration. A packet-filtering firewall deals with packets at the data-link and network layers of the Open Systems Interconnect (OSI) model. The following are some of the criteria by which packet filtering can be implemented:
    - IP address By using the IP address as a parameter, the firewall can allow or deny traffic, based on the source or destination IP address. For example, you can configure the firewall so that only certain hosts on the internal network are able to access hosts on the

Internet. Alternatively, you can configure it so that only certain hosts on the Internet are able to gain access to a system on the internal network.

- Port number, the TCP/IP suite uses port numbers to identify which service a certain packet is destined for. By configuring the firewall to allow certain types of traffic, you can control the flow. You might, for example, open port 80 on the firewall to allow Hypertext Transfer Protocol (HTTP) requests from users on the Internet to reach the corporate Web server. You might also, depending on the application, open the HTTP Secure (HTTPS) port, port 443, to allow access to a secure Web server application.
- Protocol ID because each packet transmitted with IP has a protocol identifier in it, a firewall can read this value and then determine what kind of packet it is. If you are filtering based on protocol ID, you specify which protocols you will and will not allow passing through the firewall.
- MAC address this is perhaps the least used of the packet-filtering methods discussed, but it is possible to configure a firewall to use the hardware-configured MAC address as the determining factor in whether access to the network is granted. This is not a particularly flexible method, and it is therefore suitable only in environments in which you can closely control who use which MAC address. The Internet is not such an environment.
- Circuit-level *firewalls* are similar in operation to packet-filtering firewalls, but they operate at the transport and session layers of the OSI model. The biggest difference between a packet-filtering firewall and a circuit-level firewall is that a circuit-level firewall validates TCP and UDP sessions before opening a connection, or circuit, through the firewall. When the session is established, the firewall maintains a table of valid connections and lets data pass through when session information matches an entry in the table. The table entry is removed, and the circuit is closed when the session is terminated.

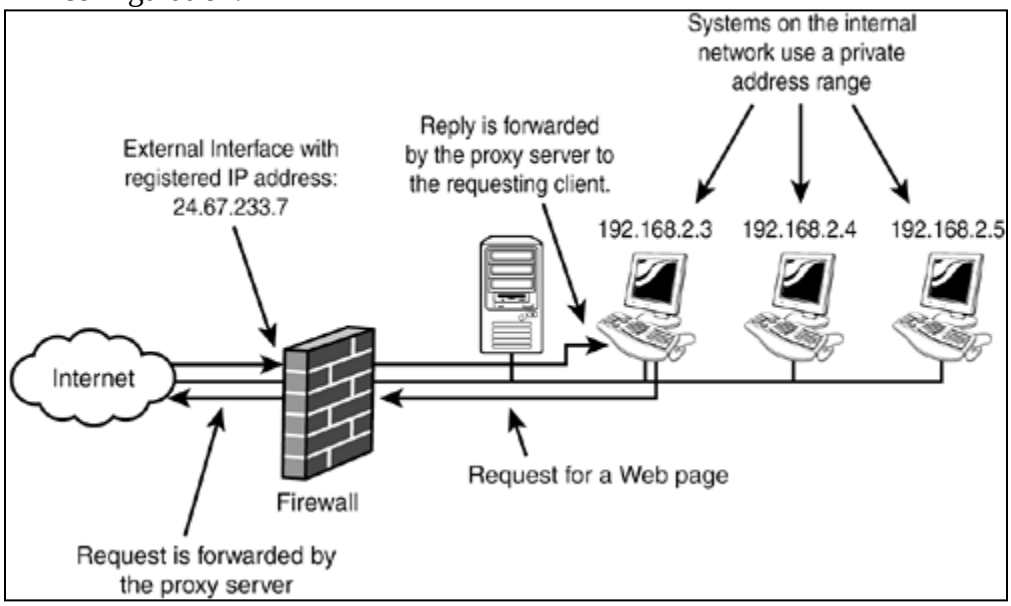
14. Application Gateway Firewalls

- The *application gateway firewall* is the most functional of all the firewall types. As its name suggests, the application gateway firewall functionality is implemented through an application. Application gateway firewall systems can implement sophisticated rules and closely control traffic that passes through. Features of these firewalls can include user authentication systems and the capability to control which systems an outside user can access on the internal network. Some also provide bandwidth control mechanisms. Because application gateway firewalls operate above the Session layer of the OSI model, they can provide protection against any software-based network traffic that attempts to pass through them.
- Firewalls are now a common sight in businesses and homes alike. As the Internet becomes an ever more hostile place, firewalls and the individuals who understand them are likely to become an essential part of the IT landscape.

Proxy Server:-

1. A proxy service provides management and control over what is now an essential feature of any modern network Internet access.
2. A proxy server, which can be a computer or dedicated hardware device running proxy service software, acts as an intermediary between a user on the internal network and a service on the external network (normally the Internet).
3. The proxy server takes requests from a user and then performs those requests on behalf of the user.

4. To the external system, the request looks as if it originated from the proxy server, not from the user on the internal network. Figure 2 shows how a proxy server fits into a network configuration.



5. There are a couple of excellent reasons to implement a proxy server:
   - To perform NAT functions a proxy server can process and execute commands on behalf of clients that have private IP addresses. This enables an organization with only one registered IP address to provide Internet access to a large number of computers. This process is known as IP proxy.
   - To allow Internet access to be controlled having a centralized point of access allows for a great deal of control over the use of the Internet.
   - By using the functionality of a proxy server application or by using an add-on feature, proxy servers can filter requests made by clients and either allow or disallow them. You can, for example, implement uniform resource locator (URL) filtering, which allows or denies users access to certain sites.
6. Although the most common function of a proxy server is to provide access to the Web for internal clients that is not its only function. A proxy server, by definition, can be used as an intermediary for anything, not just HTTP requests.
7. Other services can be supported by a proxy server, depending on the proxy server application being used and its configuration. For example, you might configure a proxy server to service HTTP requests (TCP port 80), Post Office Protocol 3 (POP3) email retrieval (TCP port 110), Simple Mail Transfer Protocol (SMTP) mail sending (TCP port 25), and HTTPS requests (TCP port 443). With an understanding of what a proxy server is designed to do, you can look at one additional feature built in to proxy server functionality, caching.
8. An additional feature offered by many proxy server applications is caching; such a server is known as a *caching proxy server*. Caching enables the proxy server to store pages that it retrieves as files on disk.
9. Consequently, if the same pages are requested again, they can be provided more quickly from the cache than if the proxy server had to continue going back to the Web server from which the pages were originally retrieved. This approach has two benefits:

- Significantly improves performance is improved particularly in environments such as a school, where there is a great likelihood that more than one user might retrieve the same page.
- Reduces demands on Internet a connection because there are fewer requests to the Internet when a caching proxy server is in use, there is a reduced demand on the Internet connection. In some cases, this results in a general speed improvement. In extreme cases, it might even be possible to adopt a less expensive Internet connectivity method because of the lower level of demand.

10. As with any technology, with caching proxy servers, there are issues to be considered. Sometimes a sizable amount of hard disk space is required to store the cached pages. With the significant decline in the cost of hard disk space over recent years, this is not likely to be much of a problem, but it still needs to be considered.
11. Another factor is that it's possible for pages held in the cache to become stale. As a result, a user might retrieve a page and believe that it is the latest version when, in fact, it has since changed, but the new page has not been updated in the proxy server cache.
12. To prevent this problem, caching proxy servers can implement measures such as aging of cached information so that it is removed from the cache after a certain amount of time.
13. Some proxy applications can also make sure that the page stored in the cache is the same as the page currently available on the Internet.
14. If the page in the cache is the same as the one on the Internet, it is served to the client from the cache. If the page is not the same, the newer page is retrieved, cached, and supplied to the client.