Module 6

Internetworking

Lesson 1

Internetworking Devices

Specific Instructional Objectives

At the end of this lesson, the students will be able to:

- Specify the need for internetworking
- State various issues related to internetworking
- Explain the operation of various internetworking devices:
    - Hubs
    - Bridges
        - Bridge forwarding and learning
        - Transparent and source routing bridges
    - Switches
    - Routers
    - Gateways

6.1.1 Introduction

HILI subcommittee (IEEE802.1) of the IEEE identified the following possible internetworking scenarios.

- A single LAN
- Two LANs connected together (LAN-LAN)
- A LAN connected to a WAN (LAN-WAN)
- Two LANs connected through a WAN (LAN-WAN-LAN)

Various internetworking devices such as hubs, bridges, switches, routers and gateways are required to link them together. These internetworking devices are introduced in this lesson.

6.1.2 Repeaters

A single Ethernet segment can have a maximum length of 500 meters with a maximum of 100 stations (in a cheapernet segment it is 185m). To extend the length of the network, a *repeater* may be used as shown in Fig. 6.1.1. Functionally, a repeater can be considered as two transceivers joined together and connected to two different segments of coaxial cable. The repeater passes the digital signal bit-by-bit in both directions between the two segments. As the signal passes through a repeater, it is amplified and regenerated at the other end. The repeater does not isolate one segment from the other, if there is a collision on one segment, it is regenerated on the other segment. Therefore, the two segments form a single LAN and it is transparent to rest of the system. Ethernet allows five segments to be used in cascade to have a maximum network span of 2.5 km. With reference of the ISO model, a repeater is considered as a *level-1 relay* as depicted in Fig. 6.1.2. It simply repeats, retimes and amplifies the bits it receives. The repeater is merely used to extend the span of a single LAN. Important features of a repeater are as follows:

- A repeater connects different segments of a LAN
- A repeater forwards every frame it receives
- A repeater is a regenerator, not an amplifier
- It can be used to create a single extended LAN

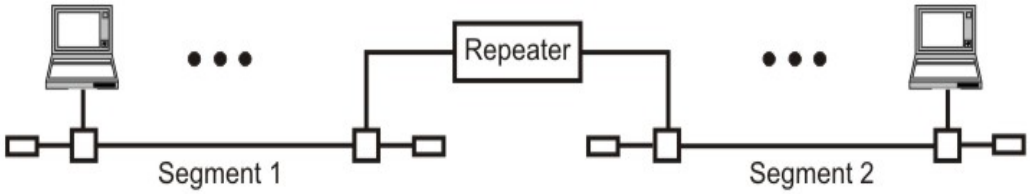


Figure 6.1.1 Repeater connecting two LAN segments

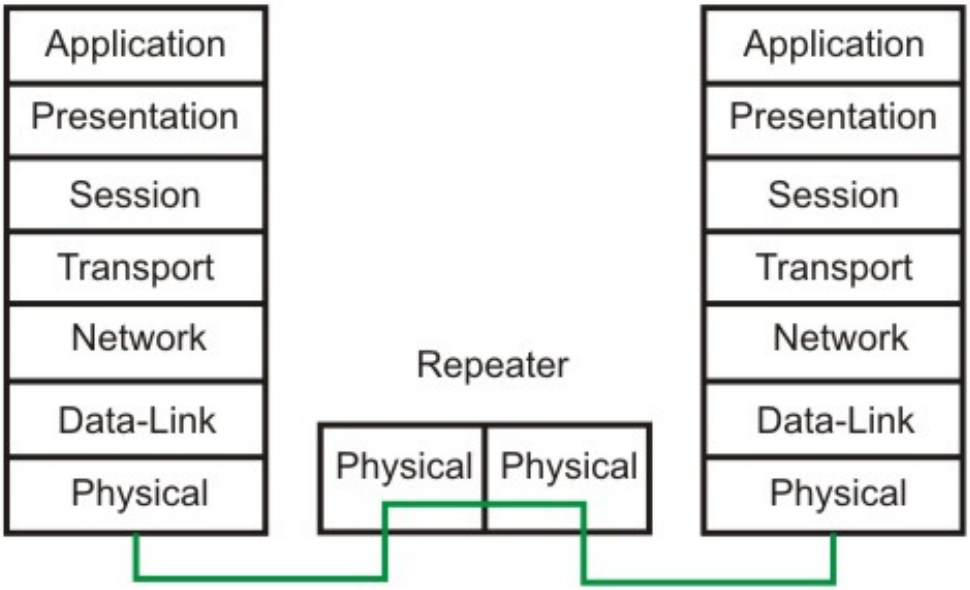


Figure 6.1.2 Operation of a repeater as a level-1 relay

6.1.3 Hubs

Hub is a generic term, but commonly refers to a multiport repeater. It can be used to create multiple levels of hierarchy of stations. The stations connect to the hub with RJ-45 connector having maximum segment length is 100 meters. This type of interconnected set of stations is easy to maintain and diagnose. Figure 6.1.3 shows how several hubs can be connected in a hierarchical manner to realize a single LAN of bigger size with a large number of nodes.

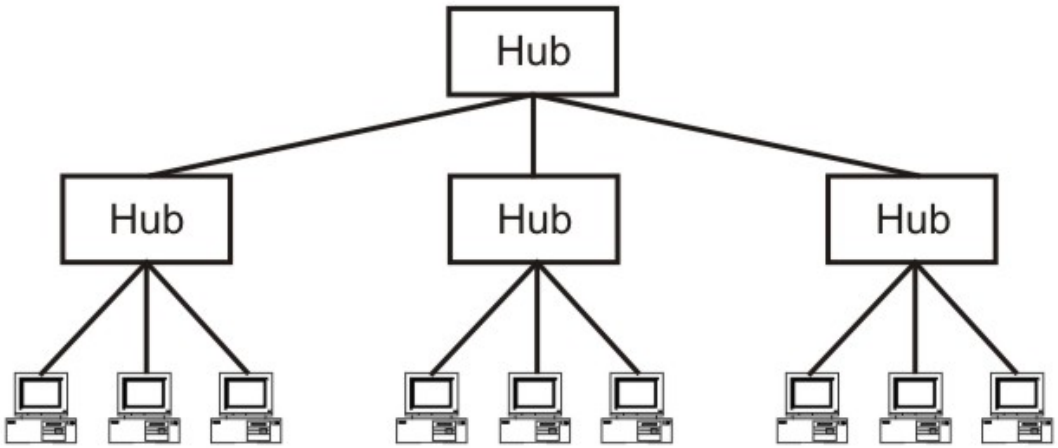


Figure 6.1.3 Hub as a multi-port repeater can be connected in a hierarchical manner to form a single LAN with many nodes

6.1.4 Bridges

The device that can be used to interconnect two separate LANs is known as a *bridge*. It is commonly used to connect two similar or dissimilar LANs as shown in Fig. 6.1.4. The bridge operates in layer 2, that is data-link layer and that is why it is called *level-2 relay* with reference to the OSI model. It links similar or dissimilar LANs, designed to store and forward frames, it is protocol independent and transparent to the end stations. The flow of information through a bridge is shown in Fig. 6.1.5. Use of bridges offer a number of advantages, such as higher reliability, performance, security, convenience and larger geographic coverage. But, it is desirable that the quality of service (QOS) offered by a bridge should match that of a single LAN. The parameters that define the QOS include *availability, frame mishaps, transit delay, frame lifetime, undetected bit errors, frame size* and *priority*. Key features of a bridge are mentioned below:

- A bridge operates both in physical and data-link layer
- A bridge uses a table for filtering/routing
- A bridge does not change the physical (MAC) addresses in a frame
- Types of bridges:
    - Transparent Bridges
    - Source routing bridges

A bridge must contain addressing and routing capability. Two routing algorithms have been proposed for a bridged LAN environment. The first, produced as an extension of IEEE 802.1 and applicable to all IEEE 802 LANs, is known as *transparent bridge*. And the other, developed for the IEEE 802.5 token rings, is based on *source routing approach*. It applies to many types of LAN including token ring, token bus and CSMA/CD bus.

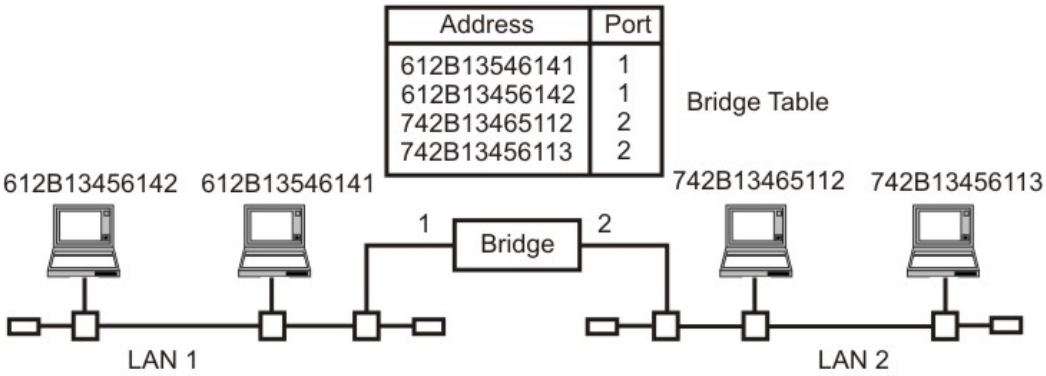


Figure 6.1.4 A bridge connecting two separate LANs

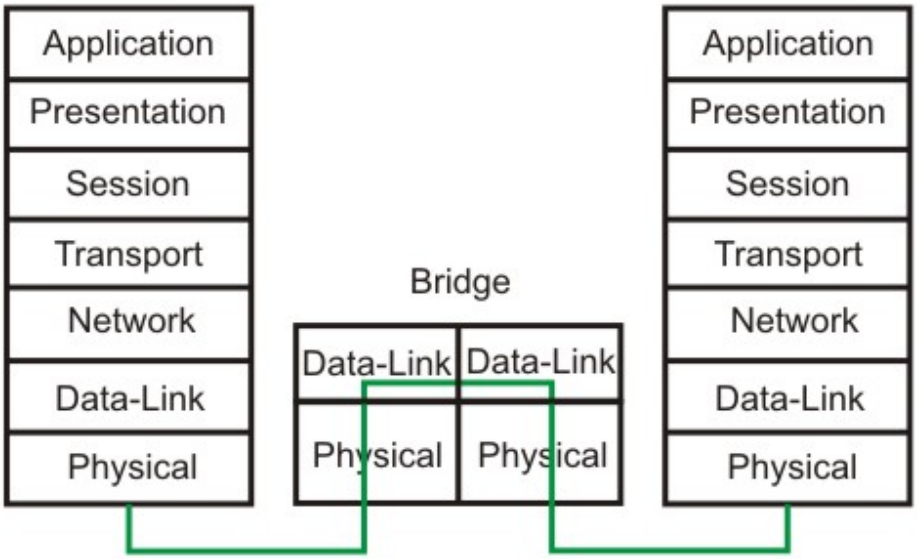


Figure 6.1.5 Information flow through a bridge

6.1.5 Transparent Bridges

The transparent bridge uses two processes known as **bridge forwarding** and **bridge learning**. If the destination address is present in the forwarding database already created, the packet is forwarded to the port number to which the destination host is attached. If it is not present, forwarding is done on all parts (flooding). This process is known as *bridge forwarding*. Moreover, as each frame arrives, its source address indicates where a particular host is situated, so that the bridge learns which way to forward frames to that address. This process is known as *bridge learning*. Key features of a transparent bridge are:

- The stations are unaware of the presence of a transparent bridge
- Reconfiguration of the bridge is not necessary; it can be added/removed without being noticed

- It performs two functions:
  - Forwarding of frames
  - Learning to create the forwarding table

6.1.5.1 Bridge Forwarding

Bridge forwarding operation is explained with the help of a flowchart in Fig. 6.1.6. Basic functions of the bridge forwarding are mentioned below:

- Discard the frame if source and destination addresses are same
- Forward the frame if the source and destination addresses are different and destination address is present in the table
- Use flooding if destination address is not present in the table

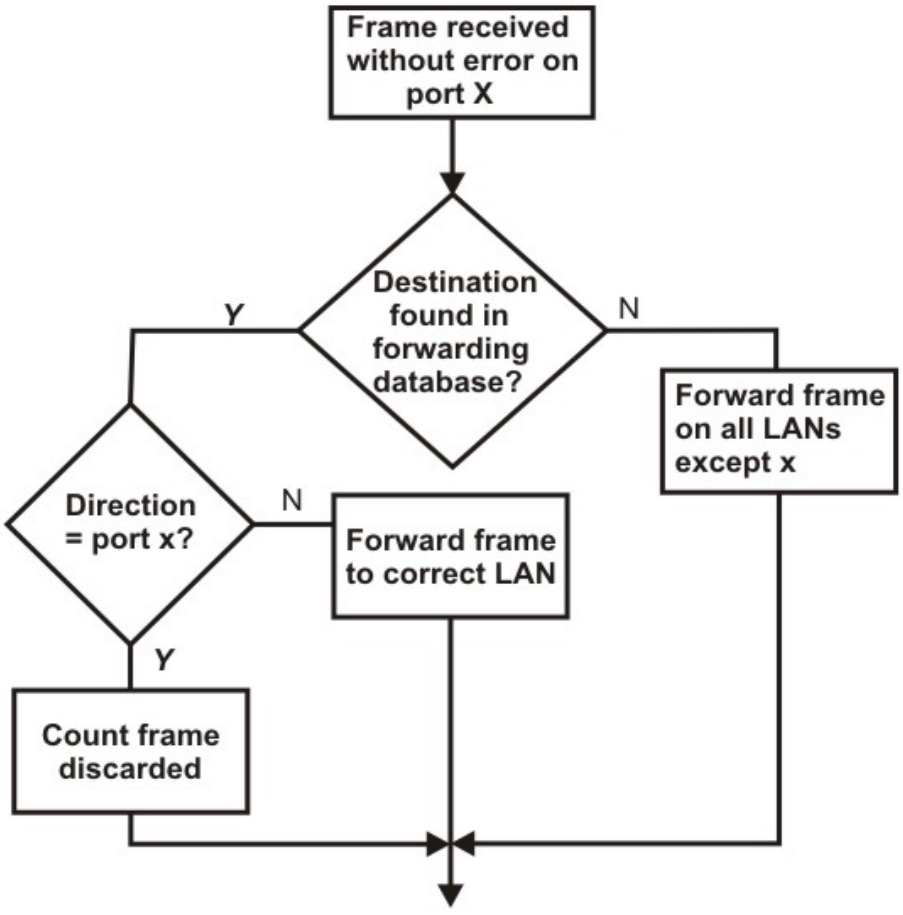


Figure 6.1.6 Bridge forwarding

6.5.1.2 Bridge Learning

At the time of installation of a transparent bridge, the database, in the form of a table, is empty. As a packet is encountered, the bridge checks its source address and build up a table by associating a source address with a port address to which it is connected. The flowchart of Fig.6.1.7 explains the learning process. The table building up operation is illustrated in Fig. 6.1.8.

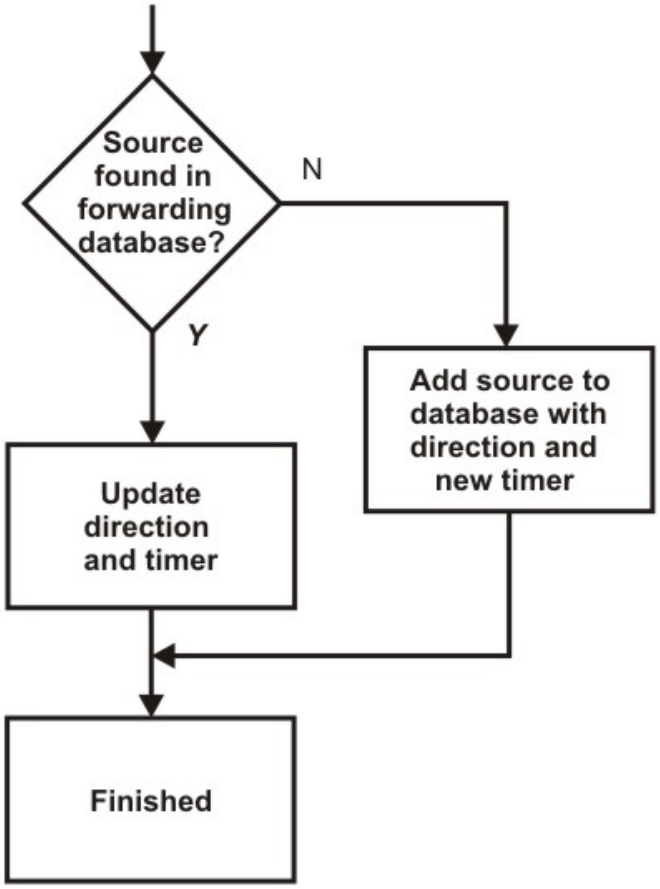


Figure 6.1.7 Bridge learning

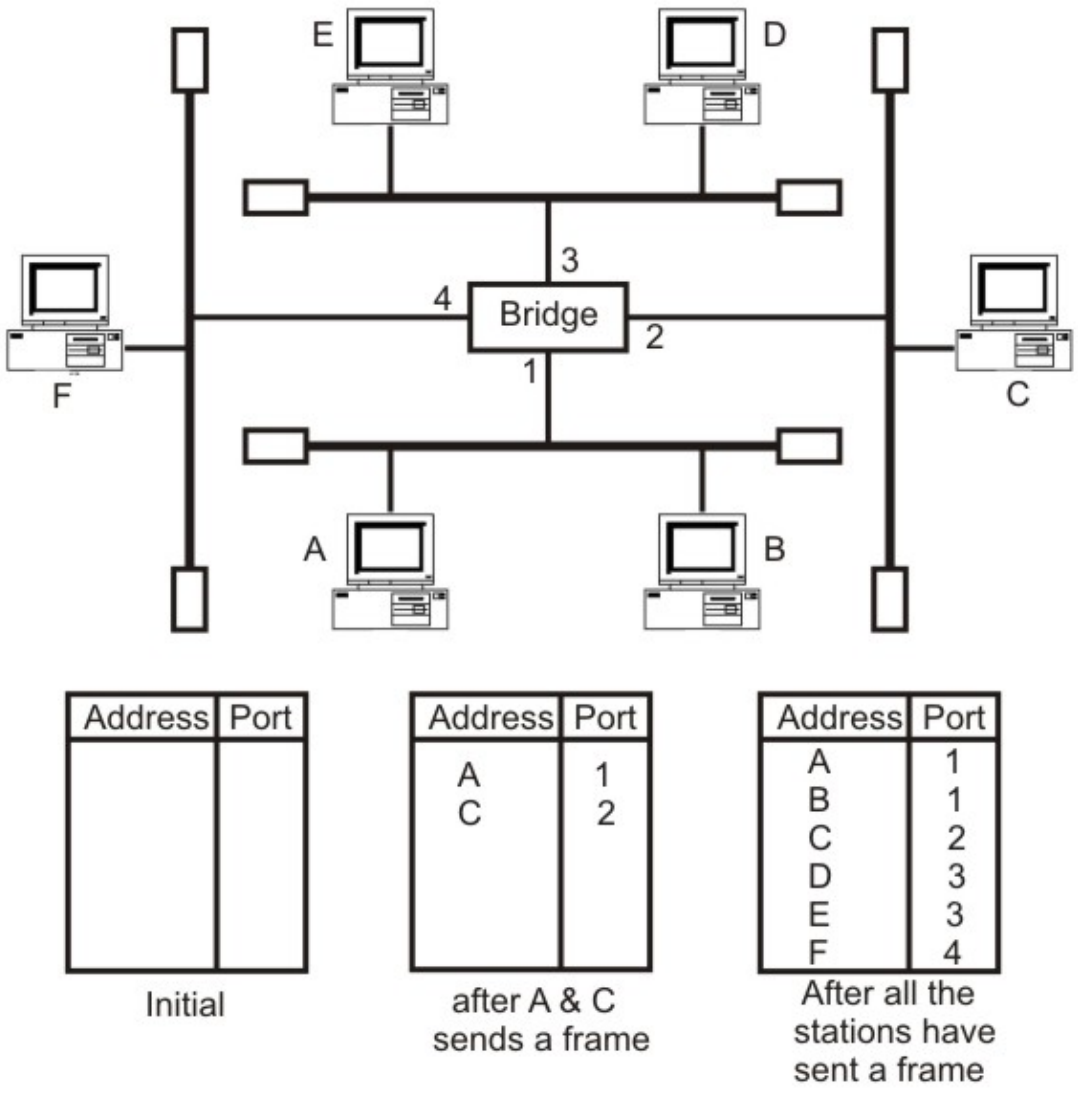


Figure 6.1.8 Creation of a bridge-forwarding table

Loop Problem

Forwarding and learning processes work without any problem as long as there is no redundant bridge in the system. On the other hand, redundancy is desirable from the viewpoint of reliability, so that the function of a failed bridge is taken over by a redundant bridge. The existence of redundant bridges creates the so-called *loop problem* as illustrated with the help of Fig. 6.1.9. Assuming that after initialization tables in both the bridges are empty let us consider the following steps:

Step 1. Station-A sends a frame to Station-B. Both the bridges forward the frame to LAN Y and update the table with the source address of A.

Step 2. Now there are two copies of the frame on LAN-Y. The copy sent by Bridge-a is received by Bridge-b and vice versa. As both the bridges have no information about Station B, both will forward the frames to LAN-X.

Step 3. Again both the bridges will forward the frames to LAN-Y because of the lack of information of the Station B in their database and again Step-2 will be repeated, and so on.

So, the frame will continue to loop around the two LANs indefinitely.

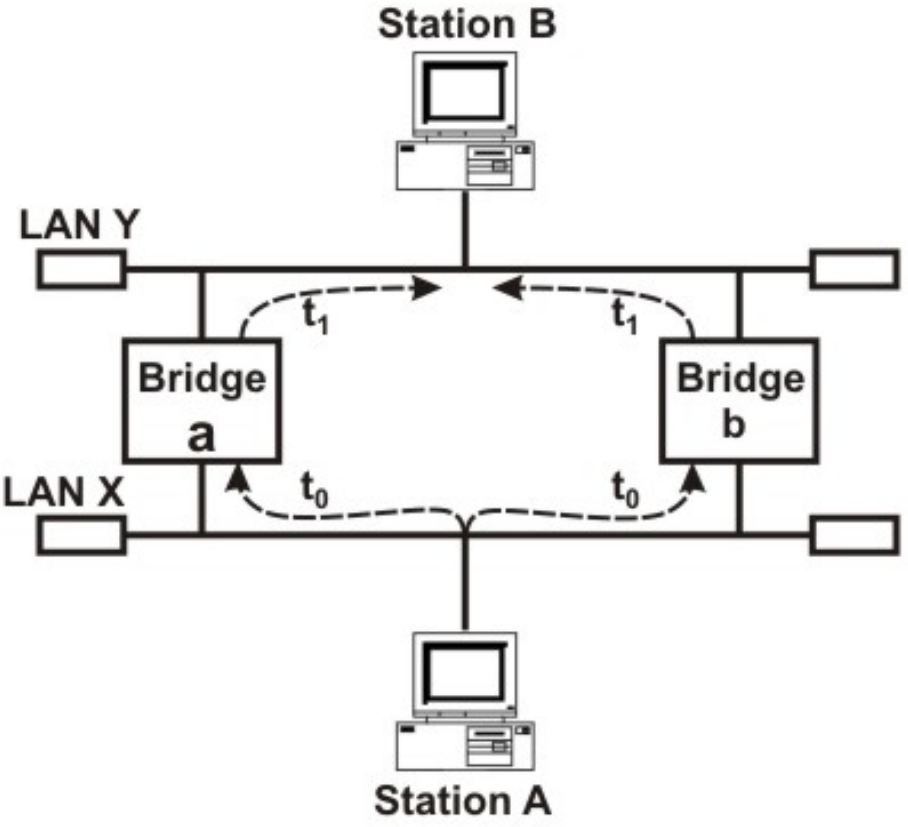


Figure 6.1.9 Loop problem in a network using bridges

Spanning Tree

As redundancy creates loop problem in the system, it is very undesirable. To prevent loop problem and proper working of the forwarding and learning processes, there must be only one path between any pair of bridges and LANs between any two segments in the entire bridged LAN. The IEEE specification requires that the bridges use a special topology. Such a topology is known as *spanning tree* (a graph where there is no loop) topology. The methodology for setting up a spanning tree is known as spanning tree algorithm, which creates a tree out of a graph. Without changing the physical topology, a logical topology is created that overlay on the physical one by using the following steps:

- Select a bridge as *Root-bridge*, which has the smallest ID.
- Select *Root ports* for all the bridges, except for the root bridge, which has least-cost path (say minimum number of hops) to the root bridge.
- Choose a *Designated bridge*, which has least-cost path to the Root-bridge, in each LAN.

- Select a port as *Designated port* that gives least-cost path from the Designated bridge to the Root bridge.
- Mark the designated port and the root ports as *Forwarding ports* and the remaining ones as *Blocking ports.*

The spanning tree of a network of bridges is shown in Fig.6.1.10. The forwarding ports are shown as solid lines, whereas the blocked ports are shown as dotted lines.

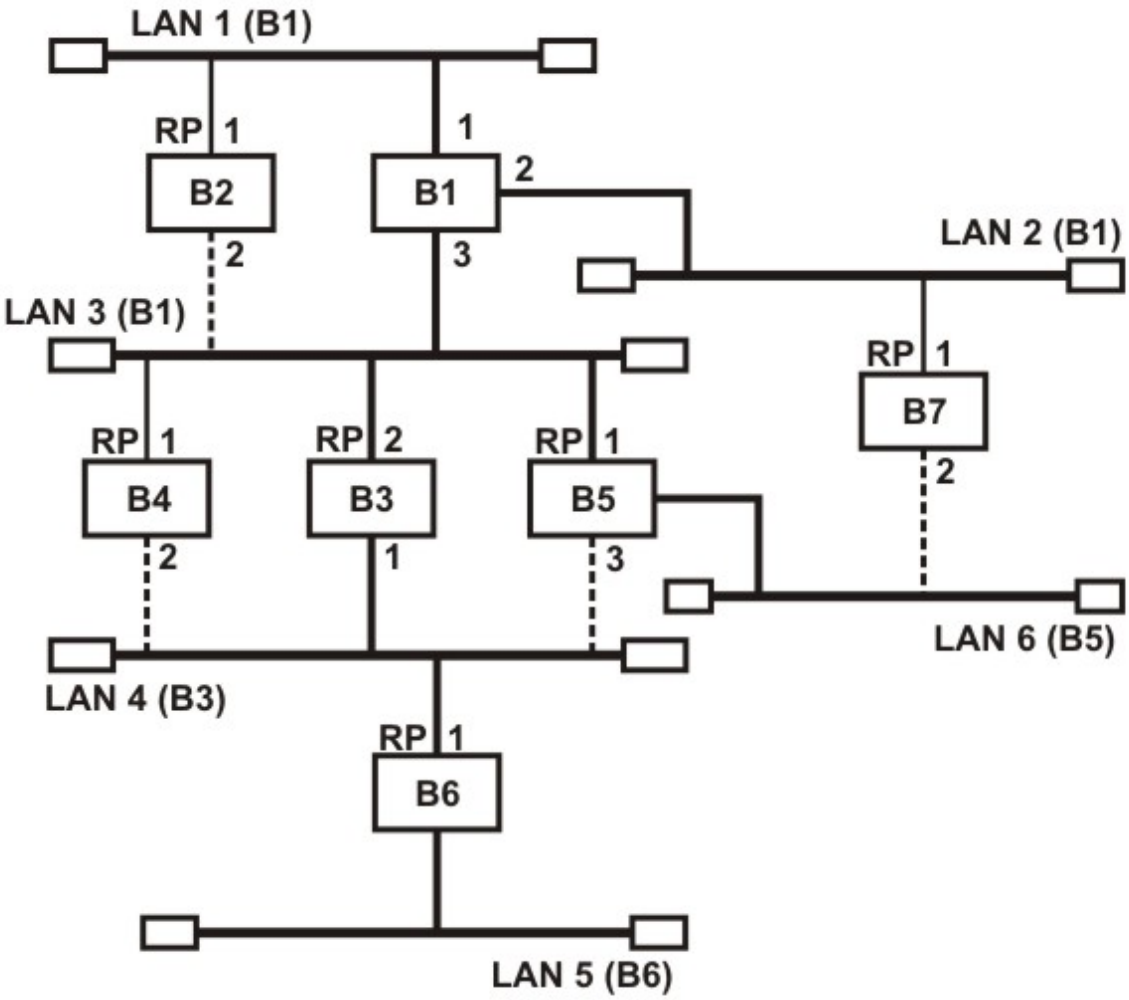


Figure 6.1.10 Spanning tree of a network of bridges

6.1.6 Source Routing Bridges

The second approach, known as *source routing*, where the routing operation is performed by the source host and the frame specifies which route the frame is to follow. A host can discover a route by sending a *discovery frame***,** which spreads through the entire network using all possible paths to the destination. Each frame gradually gathers addresses as it goes. The destination responds to each frame and the source host chooses an appropriate route from these responses. For example, a route with minimum hop-count can be

chosen. Whereas transparent bridges do not modify a frame, a source routing bridge adds a routing information field to the frame. Source routing approach provides a shortest path at the cost of the proliferation of discovery frames, which can put a serious extra burden on the network. Figure 6.1.11 shows the frame format of a source routing bridge.

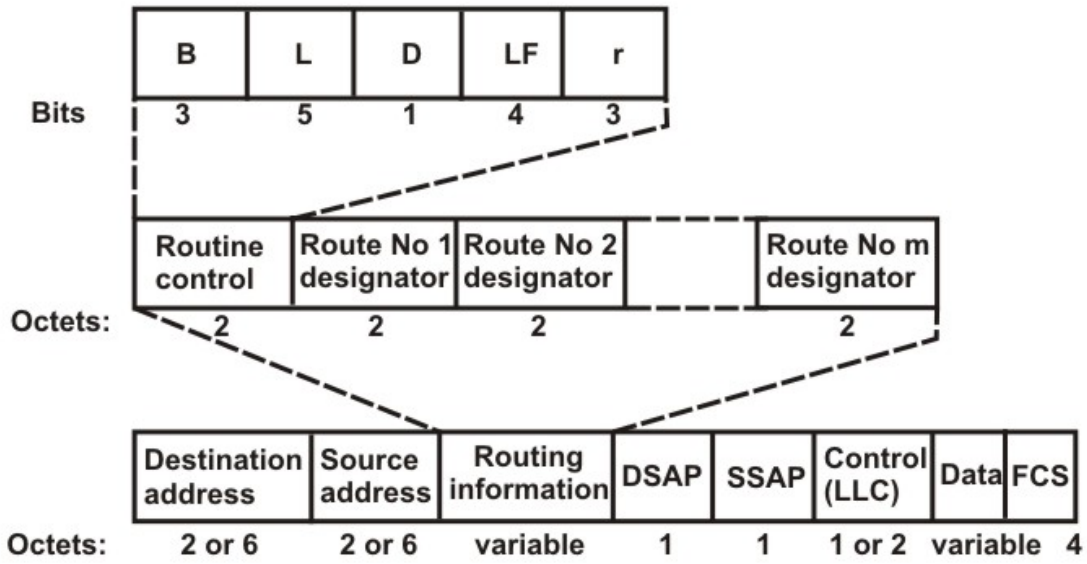


Figure 6.1.11 Source routing frame

6.1.7 Switches

A switch is essentially a fast bridge having additional sophistication that allows faster processing of frames. Some of important functionalities are:

- Ports are provided with buffer
- Switch maintains a directory: #address - port#
- Each frame is forwarded after examining the #address and forwarded to the proper port#
- Three possible forwarding approaches: Cut-through, Collision-free and Fully-buffered as briefly explained below.

Cut-through: A switch forwards a frame immediately after receiving the destination address. As a consequence, the switch forwards the frame without collision and error detection.

Collision-free: In this case, the switch forwards the frame after receiving 64 bytes, which allows detection of collision. However, error detection is not possible because switch is yet to receive the entire frame.

Fully buffered: In this case, the switch forwards the frame only after receiving the entire frame. So, the switch can detect both collision and error free frames are forwarded.

Comparison between a switch and a hub

Although a hub and a switch apparently look similar, they have significant differences. As shown in Fig. 6.1.12, both can be used to realize physical star topology, the hubs works like a logical bus, because the same signal is repeated on all the ports. On the other hand, a switch functions like a logical star with the possibility of the communication of separate signals between any pair of port lines. As a consequence, all the ports of a hub belong to the same collision domain, and in case of a switch each port operates on separate collision domain. Moreover, in case of a hub, the bandwidth is shared by all the stations connected to all the ports. On the other hand, in case of a switch, each port has dedicated bandwidth. Therefore, switches can be used to increase the bandwidth of a hub-based network by replacing the hubs by switches.

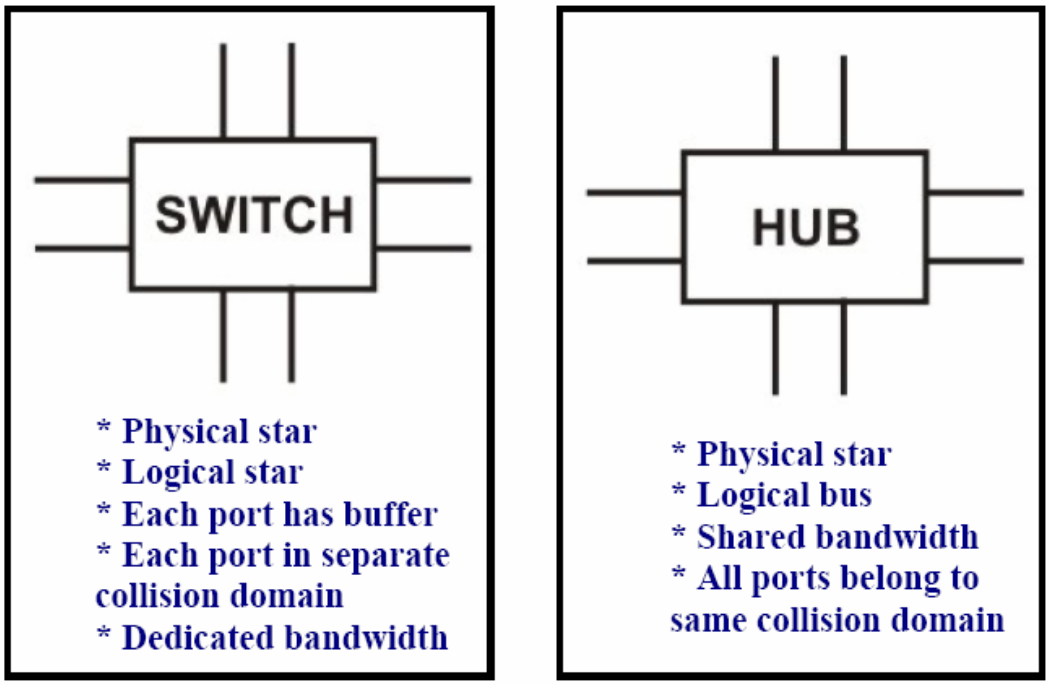


Figure 6.1.12 Difference between a switch and a bridge

6.1.8 Routers

A router is considered as a layer-3 relay that operates in the network layer, that is it acts on network layer frames**.** It can be used to link two dissimilar LANs**.** A router isolates LANs in to subnets to manage and control network traffic. However, unlike bridges it is not transparent to end stations. A schematic diagram of the router is shown on Fig. 6.1.13. A router has four basic components: Input ports, output ports, the routing processor and the switching fabric. The functions of the four components are briefly mentioned below.

- *Input port* performs physical and data-link layer functions of the router. As shown in Fig. 6.1.14 (a), the ports are also provided with buffer to hold the packet before forwarding to the switching fabric.

- *Output ports*, as shown in Fig. 6.1.14(b), perform the same functions as the input ports, but in the reverse order.
- The *routing processor* performs the function of the network layer. The process involves table lookup.
- The *switching fabric*, shown in Fig. 6.1.15, moves the packet from the input queue to the output queue by using specialized mechanisms. The switching fabric is realized with the help of multistage interconnection networks.
- Communication of a frame through a router is shown in Fig. 6.1.16.

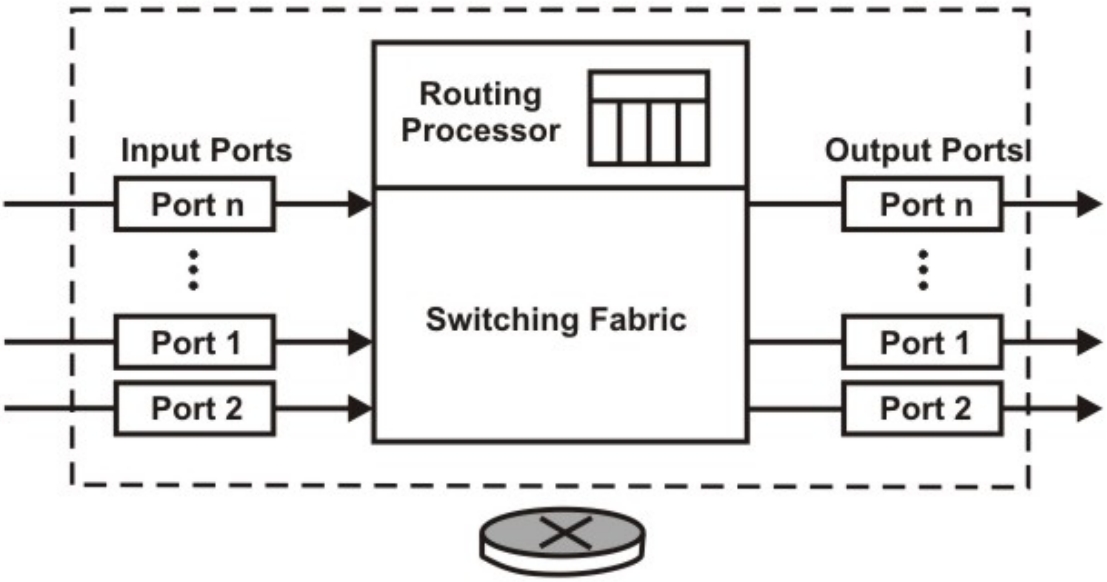
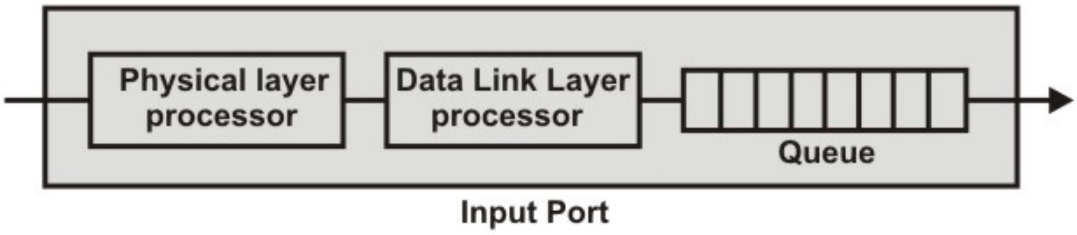
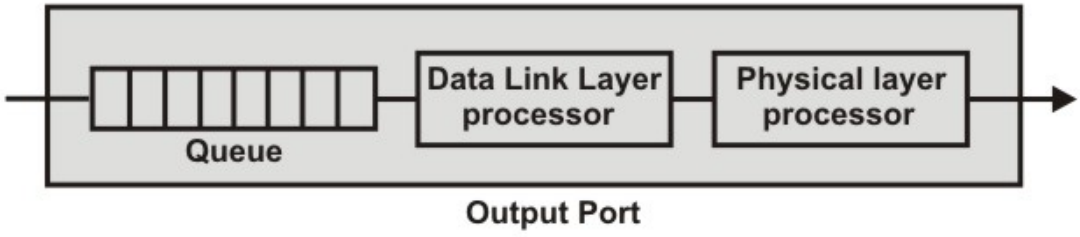


Figure 6.1.13 Schematic diagram of a router



(a)



(b)

Figure 6.1.14 Schematic diagram of a router

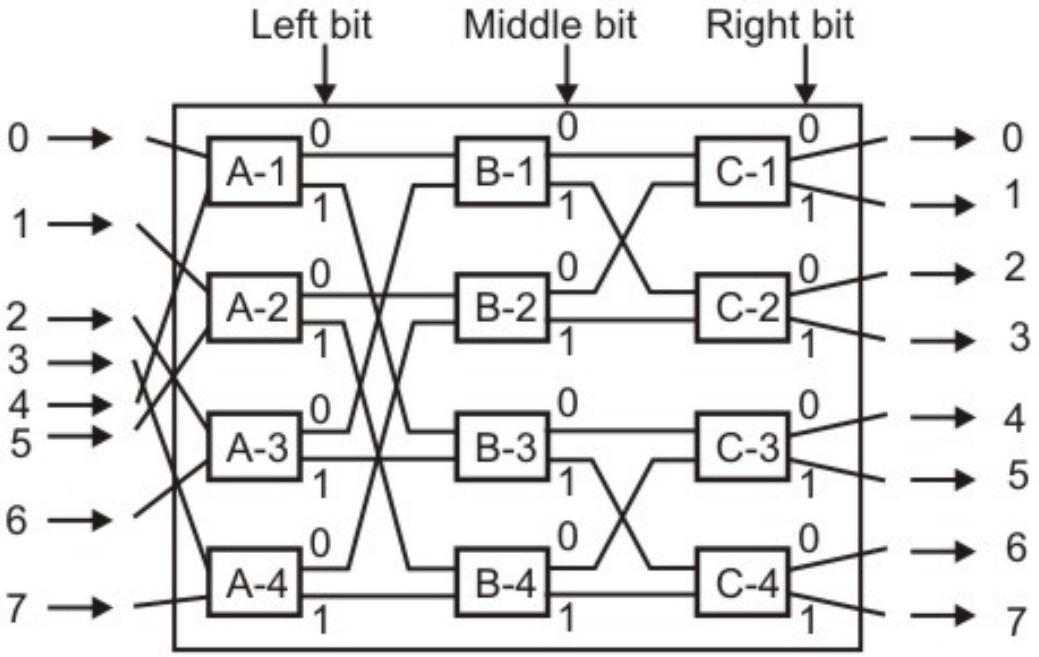


Figure 6.1.15 Switching fabric of a router

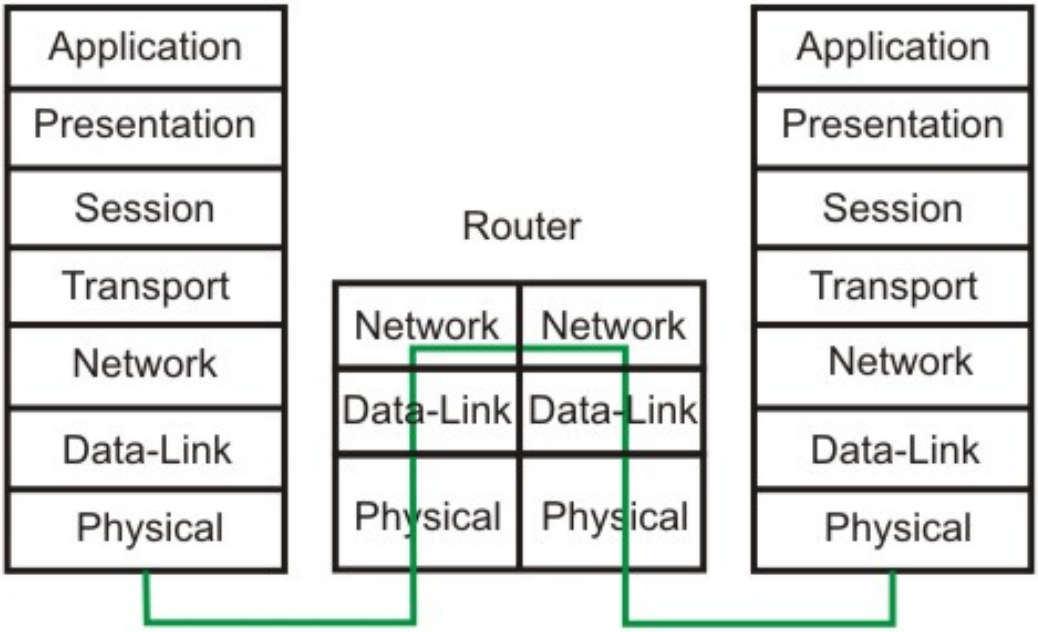


Figure 6.1.16 Communication through a router

6.1.9 Gateways

A gateway works above the network layer, such as application layer as shown in Fig. 6.1.17. As a consequence, it is known as a Layer-7 relay. The application level gateways can look into the content application layer packets such as email before forwarding it to the other side. This property has made it suitable for use in Firewalls discussed in the next module.

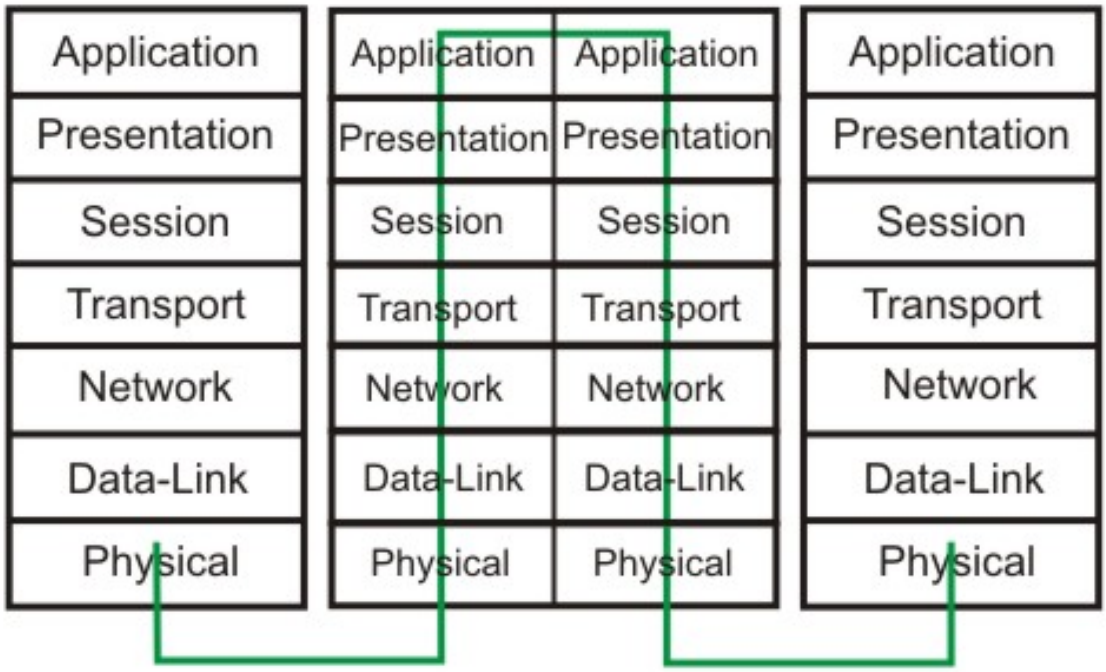


Figure 6.1.17 Communication through a gateway

6.1.10 A Simple Internet

A simple internet comprising several LANs and WANs linked with the help of routers is shown in Fig. 6.1.18.

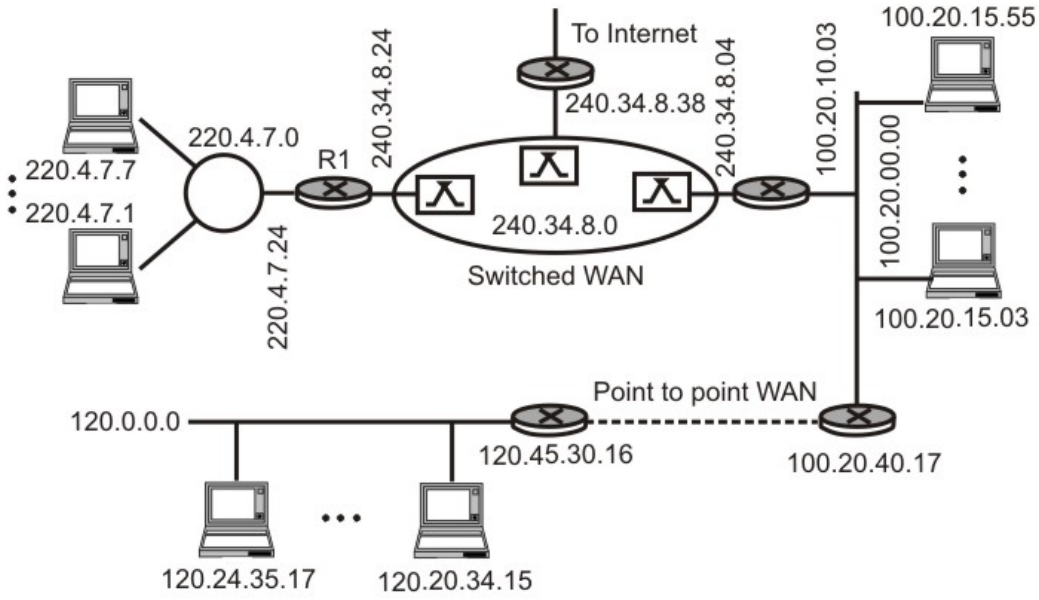


Figure 6.1.18 Simple internet showing interconnection of LANs and WANs

Review Questions

Q1.Why do you need internetworking?
Ans: As stations connected to different LANs and WANs want to communicate with each other, it is necessary to provide this facility. Internetworking creates a single virtual network over which all stations in different network can communicate seamlessly and transparently.

Q2. Why a repeater is called level-1 relay?
Ans: A repeater operates in the physical layer. Data received on one of its ports is relayed on the remaining port bit-by-bit without looking into the contents. That is why repeater is called a level-1 relay.

Q3. What is bridge? How it operates in the internetworking scenario?
Ans: A bridge operates in the Data link layer. It looks into various fields of a frame to take various actions. For example, it looks at the destination address field so that it can forward the frame to a port where destination stations is connected. It also looks at the FCS field to check error in the received frame, it any. A bridge helps to create a network having different collision domains.

Q4. Why spanning tree topology is necessary for routing using a bridge?
Ans: If there exit more than one path between two LANs through different bridges, there is a possibility of continuous looping of a frame between the LANs. To avoid the loop problem, spanning tree topology is used. It is essentially an overlay of tree topology on the physical graph topology, providing only one path between any two LANs.

Q5. What is discovery frame?
Ans: In the source routing protocol, a host can discover a route by sending a *discovery frame***,** which spreads through the entire network using all possible paths to the destination. Each frame gradually gathers addresses as it goes. The destination responds to each frame and the source host chooses an appropriate route from these responses.

Q6. What limitation of transparent bridge protocol is overcome by the source routing protocol?
Ans: Transparent bridge protocol uses spanning tree algorithm, where a unique path is used for communication between two stations. As a consequence, it does not make use of other paths leading to lesser utilization of network resources. This problem is overcome in source routing algorithm.

Q7. What limitations of a bridge are overcome by a router?
Ans: A router overcomes the following limitations of a bridge:

- Linking of two dissimilar networks
- Routing data selectively and efficiently
- Enforcement of security
- Vulnerability to broadcast storm