Expt.No. 1 **Date:**

Study of Networking & Internetworking Devices

AIM: To study various networking and internetworking devices.

Theory:

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. Various devices are used to connect the nodes/networks to form a network. Some of the widely used networking & internetworking devices are:

- Hubs
- Switches
- Routers
- Gateways
- Bridge
- Firewall
- Repeater
- Network Interface Cards
- Modem
- RJ45 Connector

Hubs

- The basic function of a hub is to take data from one of the connected devices and forward it to all the other ports regardless of the intended recipient. This is called broadcasting.
- This method of operation is inefficient because, in most cases, the data is intended for only one of the connected devices and not for all other connected devices.
- On busy networks, broadcast communications can significantly reduce overall network performance by consuming the bandwidth unnecessarily.
- Most hubs are referred to as either **Active or Passive**.
    - ***Active Hubs*** regenerate a signal before forwarding it to all the ports on the device and requires a power supply. Built-in power supply or an external power adapter can be used to supply the power.

- ***Passive* Hubs**, which today are seen only on older networks, do not need power and they don't regenerate the data signal.

- Due to the inefficiencies of the hub system and the constantly increasing demand for more bandwidth, hubs are slowly but surely being replaced with switches. As you will see in the next section, switches offer distinct advantages over hubs.

FIGURE 3.2 A high-capacity, or high-density, hub.

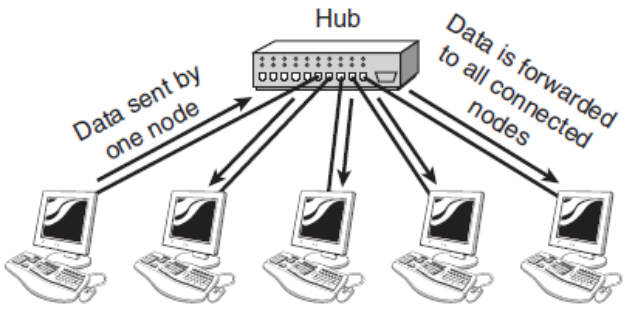

FIGURE 3.3 How a hub works.

Switches

Figure: 32-Port Ethernet Switch

- On the surface, a *switch* looks much like a hub. Despite their similar appearance, switches are far more efficient than hubs and are far more desirable for today's network environments.
- As with a hub, computers connect to a switch via a length of twisted-pair cable.
- Despite their similarity in appearance and their identical physical connections to computers, switches offer significant operational advantages over hubs.

- As discussed earlier, a hub forwards data to all ports, regardless of whether the data is intended for the system connected to the port. This arrangement is inefficient; however, it requires little intelligence on the part of the hub, which is why hubs are inexpensive.

- Rather than forwarding data to all the connected ports, a switch forwards data only to the port on which the destination system is connected.

- It looks at the Media Access Control (MAC) addresses of the devices connected to it to determine the correct port. A *MAC address* is a unique number that is stamped into every NIC.

- By forwarding data only to the system to which the data is addressed, the switch decreases the amount of traffic on each network link dramatically. In effect, the switch literally channels (or *switches*, if you prefer) data between the ports. Figure 3.5 illustrates how a switch works.

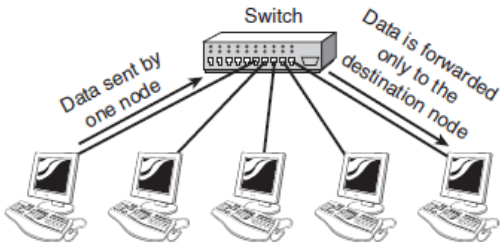

FIGURE 3.5 How a switch works.

- **Collisions** occur on the network when two devices attempt to transmit at the same time. Such collisions cause the performance of the network to degrade. By channeling data only to the connections that should receive it, switches reduce the number of

collisions that occur on the network. As a result, switches provide significant performance improvements over hubs.

- Switches can also further improve performance over the performance of hubs by using a mechanism called ***full-duplex***. On a standard network connection, the communication between the system and the switch or hub is said to be ***half-duplex***. In a half-duplex connection, data can be either sent or received on the wire but not at the same time. Because switches manage the data flow on the connection, a switch can operate in full-duplex mode—it can send and receive data on the connection at the same time.

Half-Duplex It's important to remember that a full-duplex connection has a maximum data rate of double the standard speed, and a half-duplex connection *is* the standard speed. The term *half-duplex* can sometimes lead people to believe that the connection speed is half of the standard, which is not the case. To remember this, think of the half-duplex figure as half the full-duplex figure, not half the standard figure.

Bridges

- Bridges are networking devices that **connect networks**.
- Sometimes it is necessary to divide networks into subnets to reduce the amount of traffic on each larger subnet or for security reasons. Once divided, the bridge connects the two subnets and manages the traffic flow between them.
- A bridge functions by blocking or forwarding data, based on the destination MAC address written into each frame of data.
- If the bridge believes the destination address is on a network other than that from which the data was received, it can forward the data to the other networks to which it is connected.
- If the address is not on the other side of the bridge, the data is blocked from passing.
- Bridges "learn" the MAC addresses of devices on connected networks by "listening" to network traffic and recording the network from which the traffic originates.

Figure 3.9 shows a representation of a bridge.

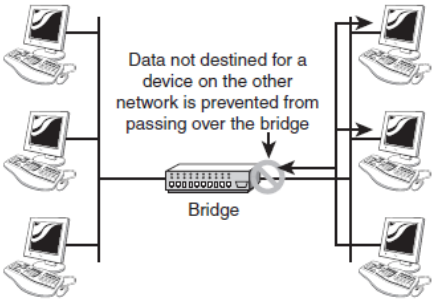

FIGURE 3.9 How a bridge works.

The advantages of bridges are simple and significant.

- By preventing unnecessary traffic from crossing onto other network segments, a bridge can dramatically reduce the amount of Bridges network traffic on a segment.
- Bridges also make it possible to isolate a busy network from a not-so-busy one, thereby preventing pollution from busy nodes.

NOTE

Manual Bridge Configuration Some early bridge implementations required you to enter the information for each device on the network manually. Fortunately, bridges are now of the learning variety, and manual configuration is no longer necessary.

Routers

- Routers are network devices that literally **route data around the network**.
- By examining data as it arrives, the router can determine the destination address for the data; then, by using tables of defined routes, the router determines the best way for the data to continue its journey.
- Unlike bridges and switches, which use the hardware-configured MAC address to determine the destination of the data, routers use the software-configured network address **(IP address)** to make decisions. This approach makes routers more functional than bridges or switches, and it also makes them more complex because they have to work harder to determine the information.

Figure 3.12 shows basically how a router functions.

Routing Protocols
Routing protocols are the means by which routers communicate with each other. This communication is necessary so that routers can learn the network topology and changes that occur in it.

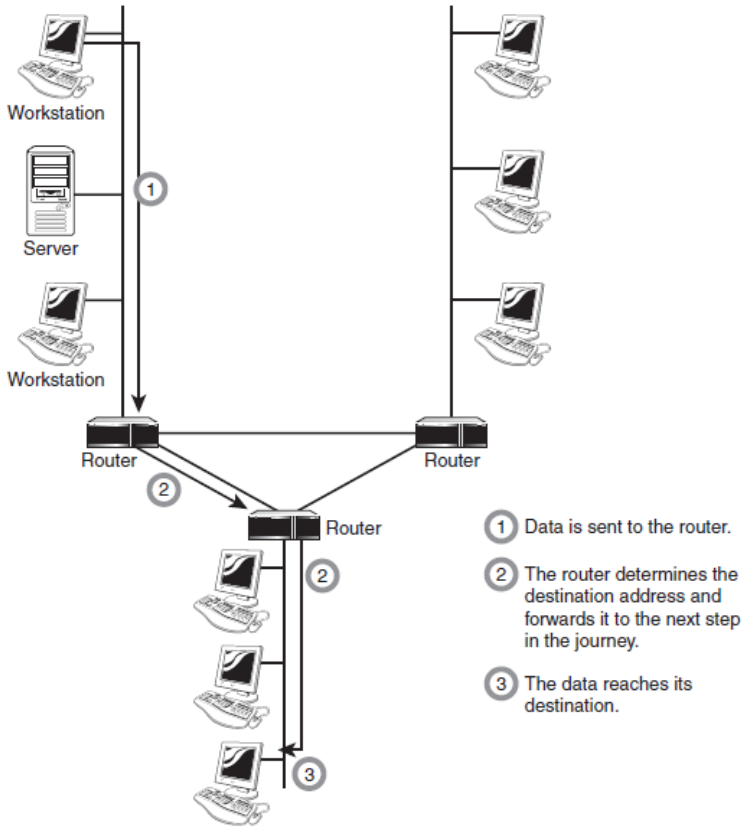

FIGURE 3.12 The basic function of a router.

Gateways

- The term *gateway* is applied to any device, system, or software application that can perform the function of **translating data from one format to another**.
- The key feature of a gateway is that it converts the format of the data, not the data itself.
- You can use gateway functionality in many ways. For example, a router that can route data from an IPX network to an IP network is, technically, a gateway. The same can be said of a translational bridge that, as described earlier in this chapter, converts from an Ethernet network to a Token Ring network and back again.
- Software gateways can be found everywhere. Many companies use an email system such as Microsoft Exchange or Novell GroupWise. These systems transmit mail internally in a certain format. When email needs to be sent across the Internet to users using a different email system, the email must be converted to another format, usually to Simple Mail Transfer Protocol (SMTP). This conversion process is performed by a software gateway.

Modems

Modem is a contraction of the terms modulator and demodulator.

The main function of the modem is to convert digital signal into analog and vice versa. Modem is a combination of two devices − modulator and demodulator. The modulator converts digital data into analog data when the data is being sent by the computer. The demodulator converts analog data signals into digital data when it is being received by the computer.

Modems are available as internal devices that plug into expansion slots in a system; external devices that plug into serial or USB ports; PCMCIA cards designed for use in laptops; and specialized devices designed for use in systems such as handheld computers. In addition, many Laptops now come with integrated modems. Figure 3.17 shows an internal modem and a PCMCIA modem.

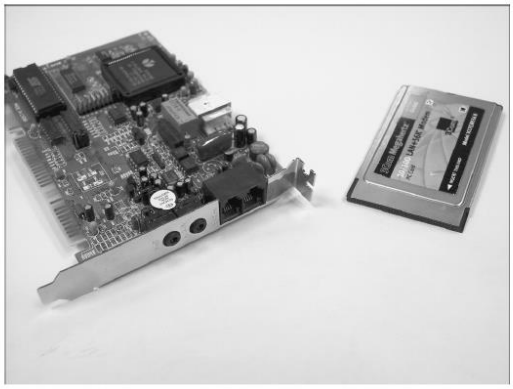

FIGURE 3.17 An internal modem (left) and a PCMCIA modem (right).

Firewalls

- A *firewall* is a networking device, either hardware or software based, that controls access to your organization's network. This controlled access is designed to protect data and resources from outside threat.
- To do this, firewalls are typically placed at entry/exit points of a network. For example, a firewall might be placed between an internal network and the Internet.
- After the firewall is in place, it can control access in and out of that point.
- Although firewalls typically protect internal networks from public networks, they are also used to control access between specific network segments within a network. For example, you might place a firewall between the Accounts Department and the Sales Department of your company.
- As mentioned, firewalls can be implemented through software or through a dedicated hardware device.

- Organizations implement software firewalls through network operating systems (NOS) such as Linux/Unix, Windows servers, and Mac OS servers. The firewall is configured on the server to allow or permit certain types of network traffic.
- Hardware firewalls are often dedicated network devices and can be implemented with very little configuration and protect all system behind it from outside sources. Hardware firewalls are readily available and often combined with other devices today. For example, many broadband routers and wireless access points have firewall functionality built in.

Network Interface Cards (NICs)

- NICs—sometimes called network cards—are the mechanisms by which computers connect to a network. On a network, each NIC is identified by a unique MAC address. MAC addresses are assigned by the manufacturers that produce the devices,

TIP

A MAC Address Is the Physical Address A MAC address is sometimes referred to as a *physical address* because it is physically embedded in the interface. Sometimes it is also referred to as a *network address*, which is incorrect. A *network address* is the logical protocol address assigned to the network to which the interface is connected.

A MAC address is a 6-byte hexadecimal address that allows a NIC to be uniquely identified on the network. The MAC address forms the basis of network communication, regardless of the protocol used to achieve network connection. Because the MAC address is so fundamental to network communication, mechanisms are in place to ensure that there is no possibility of duplicate addresses being used.

RJ45 Connector

- RJ45 is the acronym for **Registered Jack 45. RJ45 connector** is an 8-pin jack used by devices to physically connect to Ethernet based local area networks (LANs). Ethernet is a technology that defines protocols for establishing a LAN. The cable used for Ethernet LANs are twisted pair ones and have RJ45 connector pins at both ends. These pins go into the corresponding socket on devices and connect the device to the network.

Conclusion: Various networking and internetworking devices were studied successfully.