UNIT 4 INTERNETWORKING DEVICES

Structure **Page Nos**

4.0 INTRODUCTION

In this unit, you will learn on various internetwork devices such as NIC adapters, routers, hubs, switches, modems, gateway and other related devices. A network is consists of a larger number of the communication devices. The simplest device that is used in the communication is the NIC adapter which is attached with the every computer in a network. If you want to build a LAN, you will need to have computers, hubs, switches, network adapters, UTP/STP cables, routers, internal/external modems, connectors, cable testers and clipping tool. This unit explains some of mostly used network devices.

4.1 OBJECTIVES

After going through this unit, you should be able to know:

- Understand various network devices
- Functions of various network devices
- Merits and limitations of various network devices
- Difference between layer 2 and layer 3 switching, and
- Network gateway and its importance.

4.2 INTERNETWORKING DEVICES

Computer network can be established by using various network devices such as such as cables, Network Interface Cards (NICs), Modems, Repeaters, Hubs, Bridges, Switches, and Gateways. The following are various internetwork devices that are used in building LAN/WAN.

4.2.1 Network Interface Card

A network card or network interface controller or network adapter or simply NIC (network interface card) is a piece of computer hardware designed to allow computers to communicate over a computer network as shown in Figure 1. It access to a networking medium and often provides a low-level addressing system through the use of MAC addresses. It allows users to connect to each other, either by using cables or wirelessly.

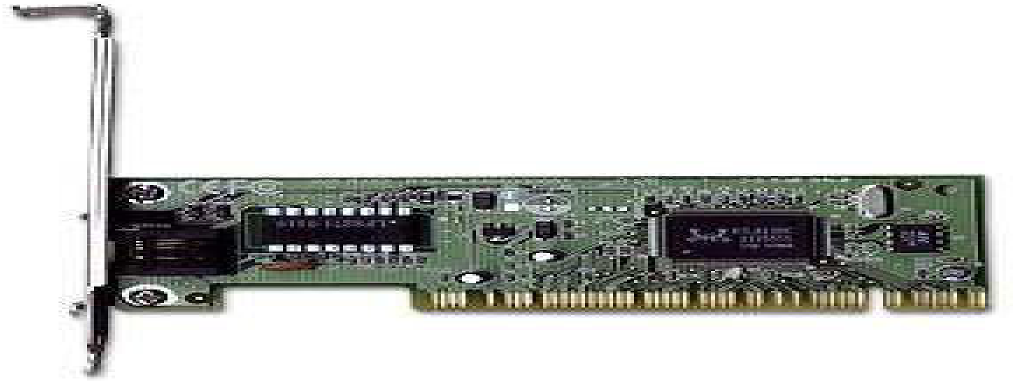

Figure 1: A Network Interface Card (NIC)

Early network interface controllers were commonly implemented on expansion cards that plugged into a computer bus; the low cost and ubiquity of the Ethernet standard means that most new computers have a network interface built into the motherboard.

The network controller implements the electronic circuitry required to communicate using a specific physical layer and data link layer standard such as Ethernet, Wi-Fi, or Token Ring. This provides a base for a full network protocol stack, allowing communication among small groups of computers on the same LAN and large-scale network communications through routable protocols, such as IP.

The NIC may use one or more of four techniques to transfer data:

- **Polling** is where the CPU examines the status of the peripheral under program control.
- **Programmed I/O** is where the microprocessor alerts the designated peripheral by applying its address to the system's address bus.
- **Interrupt-driven I/O** is where the peripheral alerts the microprocessor that it is ready to transfer data.
- **Direct memory access** is where an intelligent peripheral assumes control of the system bus to access memory directly. This removes load from the CPU but requires a separate processor on the card.

4.2.2 Modem (Modulator/Demodulator)

Modem is a device that converts digital and analog signals as shown in the Figure 2. At the source, modems convert digital signals to a form suitable for transmission over analog communication facilities (public telephone lines). At the destination, modems convert the signal back to a digital format.

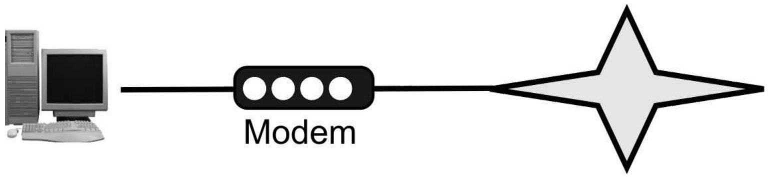

Figure 2: Modem

CSU / DSU

CSU/DSU (Channel Service Unit/Data Service Unit) is a hardware device about the size of an external modem that converts digital data frames from the communications technology used on a local area network (LAN) into frames appropriate to a wide-area network (WAN) and vice versa. A common type of device is also shown in the Figure 3. For example, if you have a Web business from your own home and have leased a digital line (perhaps a T-1 or fractional T-1 line) to a phone company or a gateway at an Internet service provider, you have a CSU/DSU at your end and the phone company or gateway host has a CSU/DSU at its end.

The Channel Service Unit (CSU) receives and transmits signals from and to the WAN line and provides a barrier for electrical interference from either side of the unit. The CSU can also echo loop back signals from the phone company for testing purposes. The Data Service Unit (DSU) manages line control, and converts input and output between RS-232C, RS-449, or V.35 frames from the LAN and the time-division multiplexed (TDM) DSX frames on the T-1 line. The DSU manages timing errors and signal regeneration. The DSU provides a modem-like interface between the computer as Data Terminal Equipment (DTE) and the CSU.

Channel service unit/data service unit (CSU/DSU) is a piece of data communications equipment that performs the following functions:

- Acts as a transceiver
- Connects data terminating equipment to dedicated circuits such as T1 and T3.
- A CSU/DSU performs multiplexing and de-multiplexing on T1 and T3 circuits.
- May have the ability to add and drop channels from a T1 or T3.
- Modern CSU/DSU's split the arriving data stream into multiple voice channels and/or multiple data channels.
- Here is a picture of the back of an external, stand-alone CSU/DSU for a T1

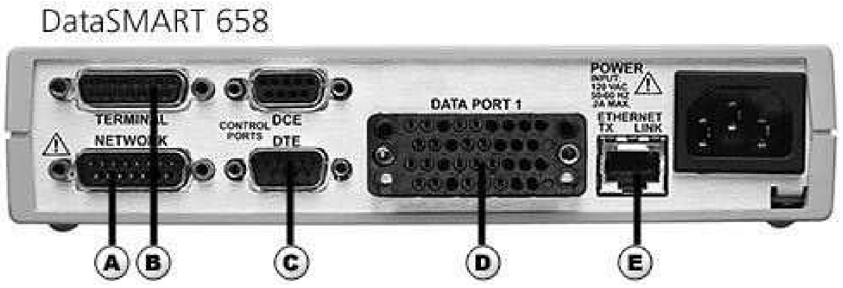

Figure 3: A CSU/DSU Device

4.2.3 Repeaters

A **repeater** is an electronic device that receives a signal and retransmits it at a higher level or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances without degradation, an example is shown in the Figure.4. Because repeaters work with the actual physical signal, and do not attempt to interpret the data being transmitted, they operate on the Physical layer, the first layer of the OSI model.

Figure 4: Repeater

In telecommunication, the term **repeater** has the following standardized meanings: An analog device that amplifies an input signal regardless of its nature (analog or digital).

A digital device that amplifies, reshapes, retimes, or performs a combination of any of these functions on a digital input signal for retransmission.

4.2.4 Hubs

A hub (concentrator) contains multiple ports as shown in Figure 5, which is used to connect devices in a star topology. When a packet arrives at one port, it is copied to all the ports of the hub. But when the packets are copied, the destination address in the frame does not change to a broadcast address. It does this in a rudimentary way; it simply copies the data to all of the Nodes connected to the hub (broadcast).

Figure 5: Hub

Advantages and Disadvantages of Hub

Following are some advantages and disadvantages of Hubs:

Advantages:

- Improves performance, especially for bursty traffic and large file transfers
- Enables optimum performance of PCI computers
- Offers ease of use: Fast Ethernet hubs require no hardware or software settings; just plug them in
- Leverages your knowledge of Ethernet and investment in management tools and applications

Disadvantages:

- Total bandwidth remains fixed; as network traffic grows, performance suffers

- The network manager cannot manage network load—for example, by segmenting the network into multiple collision domains or restricting certain types of traffic to certain ports
- Does not reduce collisions
- Requires Category 5 UTP cabling for each 100BaseTX connection

4.2.5 Bridges

The main network device found at the data link layer is a bridge. This device works at a higher layer than the repeater and therefore is a more complex device. It has some understanding of the data it receives and can make a decision based on the frames it receives as to whether it needs to let the information pass, or can remove the information from the network. This means that the amount of traffic on the medium can be reduced and therefore, the usable bandwidth can be increased.

Bridges are store and forward devices to provide error detection; a common type of bridge is shown in the Figure 6. They capture an entire frame before deciding whether to filter or forward the frame, which provides a high level of error detection because a frame's CRC checksum can be calculated by the bridge. Bridges are highly susceptible to broadcast storms. A broadcast storm occurs when several broadcasts are transmitted at the same time. It can take up huge bandwidth.

Figure 6: Bridge

Advantages and Disadvantages of Bridges

Following are some advantages and disadvantages of Bridges:

Advantages:

- Reliability
- Manageability
- Scalability

Disadvantages:

- A bridge cannot filter out broadcast traffic.
- It introduces 20 to 30 % latency.
- Only 2 networks can be linked with a bridge

☞ Check Your Progress 1

1. Explain the meaning of repeaters in analog and digital system

……………………………………………………………………………………
……………………………………………………………………………………

2. What are the advantages and disadvantages of bridges?

   ………………………………………………………………………………………

   ………………………………………………………………………………………

   ………………………………………………………………………………………

4.2.6 Switch

A switch is a data-link layer network device that forwards frames using MAC addresses in the header of frames. Common types of switches are shown in the Figure 7. It is used to improve network performance by: -

- Segmenting the network and creating separate collision domains.
- Reducing competition for bandwidth.

In a switch frame, forwarding is handled by specialized hardware called "Application Specific Integrated Circuit" (ASIC). ASIC technology allows a silicon chip to be programmed to perform specific functions much faster than that of a chip programmed by software.

Figure 7: Switch

Following are the Steps of Switch Functioning

1. **Learning**

   When switch starts, the MAC address table has no entry. When a node transmits data on its wire the MAC address of the node is learned by Switch Port connected to that node. In this way all the MAC addresses are learned by respective ports and these entries remain in the cache for a specific time. If during this specific time no new frame arrives from a node MAC address entry for that node is dropped from cache.

2. **Forwarding & Filtering**

   When a MAC address for a port is learnt, packets addressed to that MAC address are forwarded only to the port associated with it, using one of the Switching Methods.

3. **Loop Avoidance**

   Switches and Bridges use Spanning Tree Protocol (STP), specified by IEEE 802.1d, to prevent loops.

Switching Methods

- **Store & Forward:** in this method the switch receives complete frame. CRC (Cyclic Redundancy Check), source address and destination address are checked.

- **Cut Through:** In this method forwarding starts as soon as destination address of the frame is received in header. Also known as WIRE SPEED.
- **Fragment Free (Modified Cut Through):** In this method forwarding starts as soon as first 64 bytes of the frame are received as fragmentation occurs usually in first 64 bytes.

Advantages and Disadvantages of Switch

Following are some advantages and disadvantages of switches:

Advantages:

- Reduces the number of Broadcast domains
- Supports VLAN's (virtual local area network (VLAN) is a logical grouping of hosts on one or more LANs that allows communication to occur between hosts as if they were on the same physical LAN.) that can help in Logical segmentation of ports [physical ports]. Splitting up the broadcast domain.
- Intelligent device [compared to Hub's] which can make use of CAM table for Port to MAC mapping
- Compared to Bridges, Switches are more H/w oriented therefore operations are less CPU intense [Basic operations]
- The cost to number of ports ratio is best i.e. for a cheaper cost you get switches with more number of ports available than Routers.

Disadvantages:

- Not as good as a router in limiting Broadcasts
- Communication between VLAN's need inter VLAN routing [Router], but these days there are a number of Multilayer switches available in the market.
- Handling Multicast packets needs quite a bit of configuration and proper designing.

Layer 2 Switch

Layer 2 switching uses the media access control address (MAC address) from the host's network interface cards (NICs) to decide where to forward frames. Layer 2 switching is hardware based, which means switches use application-specific integrated circuit (ASICs) to build and maintain filter tables (also known as MAC address tables). One way to think of a layer 2 switch is as a multi-port bridge.

- Layer 2 switching provides the following:Hardware-based bridging (MAC)
- Wire speed
- High speed
- Low latency
- Low cost

Layer 2 switching is highly efficient because there is no modification to the data packet, only to the frame encapsulation of the packet, and only when the data packet is passing through dissimilar media (such as from Ethernet to FDDI). Layer 2 switching is used for workgroup connectivity and network segmentation (breaking up collision domains). This allows a flatter network design with more network segments than traditional 10BaseT shared networks. Layer 2 switching has helped develop new components in the network infrastructure.

- Server farms — Servers are no longer distributed to physical locations because virtual LANs can be created to create broadcast domains in a switched internetwork. This means that all servers can be placed in a central location, yet a certain server can still be part of a workgroup in a remote branch.

- Intranets — Allows organization-wide client/server communications based on a Web technology.

These new technologies allow more data to flow off from local subnets and onto a routed network, where a router's performance can become the bottleneck.

Limitations

Layer 2 switches have the same limitations as bridge networks.
Bridged networks break up collision domains, but the network remains one large broadcast domain. Similarly, layer 2 switches (bridges) cannot break up broadcast domains, which can cause performance issues and limits the size of your network. Broadcast and multicasts, along with the slow convergence of spanning tree, can cause major problems as the network grows. Because of these problems, layer 2 switches cannot completely replace routers in the internetwork.

Layer 3 Switch

A Layer 3 switch is a high-performance device for network routing. Layer 3 switches actually differ very little from routers. A Layer 3 switch can support the same routing protocols as network routers do. Both inspect incoming packets and make dynamic routing decisions based on the source and destination addresses inside. Both types of boxes share a similar appearance.

Layer 3 switches were conceived as a technology to improve on the performance of routers used in large local area networks (LANs) like corporate intranets. The key difference between Layer 3 switches and routers lies in the hardware technology used to build the unit. The hardware inside a Layer 3 switch merges that of traditional switches and routers, replacing some of a router's software logic with hardware to offer better performance in some situations.

Layer 3 switches often cost less than traditional routers. Designed for use within local networks, a Layer 3 switch will typically not possess the WAN ports and wide area network features a traditional router will always have.
Layer 3 switches can be placed anywhere in the network because they handle high-performance LAN traffic and can cost-effectively replace routers. Layer 3 switching is all hardware-based packet forwarding, and all packet forwarding is handled by hardware ASICs.

Functions of Layer 3 switch

1. Determine paths based on logical addressing

2. Run layer 3 checksums (on header only)

3. Use Time to Live (TTL)

4. Process and respond to any option information

5. Update Simple Network Management Protocol (SNMP) managers with Management Information Base (MIB) information

6. Provide Security

The benefits of layer 3 switching include the following

- Hardware-based packet forwarding
- High-performance packet switching
- High-speed scalability
- Low latency
- Lower per-port cost
- Flow accounting
- Security
- Quality of service (QoS)

ATM Switch

ATM Switches as shown in Figure 8 provide high-speed transfer between both LANs and WANs. Asynchronous Transfer Mode (ATM) is a network technology adopted by the telecommunication sector. It is a high-performance, cell-oriented switching and multiplexing technology that utilises fixed-length packets to carry different types of traffic. The data transfer takes place in the form of cells or packets of a fixed size (53 bytes).

The cell used with ATM is relatively small compared to units used with older technologies. The small constant cell size allows ATM equipment to transmit video, audio, and computer data over the same network, and assures that no single type of data hogs the line.

ATM technology is used for both local and wide area networks (LANs and WANs) that support real-time voice and video as well as data. ATM is widely used as a backbone technology in carrier networks and large enterprises, but never became popular as a local network (LAN) topology. ATM is highly scalable and supports transmission speeds of 1.5, 25, 100, 155, 622, 2488 and 9953 Mbps.

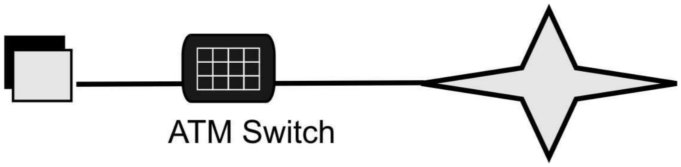

Figure 8: ATM Switch in the middle

Router

Router is a networking device which forwards data packets along networks by using headers and forwarding/routing tables to determine the best path to forward the packets. Common types of modern routers are shown here in Figure 9. Routers work at the Internet layer of the TCP/IP model or layer 3 of the OSI model. Routers also provide interconnectivity between like and unlike media. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Some DSL and cable modems, for home use, have been integrated with routers to allow multiple home computers to access the Internet.

Figure 9: Two Modern Routers

Introducing Routing

Once we create an internetwork by connecting your WANs and LANs to a router, we shall need to configure logical network addresses, such as IP addresses, to all hosts on the internetwork so that they can communicate across that internetwork.

The term ***routing*** is used for taking a packet from one device and sending it through the network to another device on a different network. Routers don’t really care about hosts—they only care about networks and the best path to each network. The logical network address of the destination host is used to get packets to a network through a routed network, and then the hardware address of the host is used to deliver the packet from a router to the correct destination host.

If your network has no routers, then it should be apparent that you are not routing. Routers route traffic to all the networks in your internetwork. To be able to route packets, a router must know, at a minimum, the following:

- Destination address
- Neighbor routers from which it can learn about remote networks
- Possible routes to all remote networks
- The best route to each remote network
- How to maintain and verify routing information
- The router learns about remote networks from neighbor routers or from an administrator

As it is already discussed that IP routing is basically of three types: static routing, default routing and dynamic routing.

Static 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.

Default Route

A default route is often called the 'route of last resort'. It is the last route tried by a router when all other routes fail because it has the fewest number of network bits matching and is therefore less specific. We use *default routing* to send packets with a remote destination network not in the routing table to the next-hop router. You should only use default routing on stub networks—those with only one exit path out of the network. To configure a default route, you use wildcards in the network address and mask locations of a static route. In fact, you can just think of a default route as a static route that uses wildcards instead of network and mask information.
The syntax for Default routing is : *ip route 0.0.0.0 0.0.0.0 <next hop or exit interface*

Dynamic Routing

Dynamic routing is when protocols (Routing Protocols) are used to find networks and update routing tables on routers. This is easier than using static or default routing, but it'll cost in terms of router CPU processes and bandwidth on the network links. The chief advantages of dynamic routing over static routing are scalability and adaptability. A dynamically routed network can grow more quickly and larger, and is able to adapt to changes in the network topology brought about by this growth or by the failure of one or more network components. Chief among the disadvantages is an increase in complexity.

4.2.7 Gateway

In a communications network, gateway is a network node equipped for interfacing with another network that uses different protocols.

A gateway may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability. It also requires the establishment of mutually acceptable administrative procedures between both networks. A protocol translation/mapping gateway interconnects networks with different network protocol technologies by performing the required protocol conversions.

A gateway is a network point that acts as an entrance to another network. On the Internet, gateway is a node or stopping point node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes, while the nodes that connect the networks in between are gateways. For example, the computers that control traffic between company networks or the computers used by internet service providers (ISPs) to connect users to the internet are gateway nodes.

In the network for an enterprise, a computer server acting as a gateway node is often simultaneously acting as a proxy server and a firewall server. A gateway is often associated with both a router, which knows where to direct a given packet of data that arrives at the gateway, and a switch, which furnishes the actual path in and out of the gateway for a given packet.

On an IP network, clients should automatically send IP packets with a destination outside a given subnet mask to a network gateway. A subnet mask defines the IP range of a private network. For example, if a private network has a base IP address of 192.168.0.0 and has a subnet mask of 255.255.255.0, then any data going to an IP address outside of 192.168.0.X will be sent to that network's gateway. While forwarding an IP packet to another network, the gateway might or might not perform Network Address Translation.

Most computer operating systems use the terms described above. Microsoft Windows, however, describes this standard networking feature as Internet Connection Sharing, which acts as a gateway, offering a connection between the Internet and an internal network. Such a system might also act as a DHCP server. Dynamic Host Configuration Protocol (DHCP) is a protocol used by networked devices (clients) to obtain various parameters necessary for the clients to operate in an Internet Protocol (IP) network. By using this protocol, system administration workload greatly decreases, and devices can be added to the network with minimal or no manual configurations.

☞ Check Your Progress 1

1. Explain the advantages of using switch. Also discuss its disadvantages.

   ……………………………………………………………………………………

   ……………………………………………………………………………………

   ……………………………………………………………………………………

   ……………………………………………………………………………………

2. What is network gateway? Explain

   ……………………………………………………………………………………

   ……………………………………………………………………………………

   ……………………………………………………………………………………

   ……………………………………………………………………………………

4.3 SUMMARY

In this unit, various internetwork components used in a computer network are explained. Some of the components such as NIC, Modem, Repeater, Hub, Switch and their functions along with merits and limitations are clearly discussed. After completing this unit you can understand the importance of various internetworking devices particularly at the network layer. You have also studied the different switching and routing methods in this unit. The block of this course has presented the details of transport layer and application layer.

4.4 REFERENCES/FURTHER READINGS

1) *Computer Networks*, A. S. *Tanenbaum* 4th Edition, Practice Hall of India, New Delhi. 2003.

2) *Computer Networking*, J.F. Kurose & K.W. Ross, A Top Down Approach Featuring the Internet, Pearson Edition, 2003.

3) *Introduction to Data Communication & Networking,* Behrouz Forouzan, Tata McGraw Hill, 1999.

4) *Communications Networks*, Leon Garcia, and Widjaja, Tata McGraw Hill, 2000.

5) *Data and Computer Communications,* Willian Stallings, 6th Edition, Pearson Education, New Delhi.

6) www.wikipedia.org

4.5 SOLUTIONS/ANSWERS

☞ Check Your Progress 1

1. In telecommunication, the term **repeater** has the following standardized meanings:

   - An analog device that amplifies an input signal regardless of its nature (analog or digital).
   - A digital device that amplifies, reshapes, retimes, or performs a combination of any of these functions on a digital input signal for retransmission.

2. Following are some advantages and disadvantages of Bridges:

   Advantages:

   - Reliability
   - Manageability
   - Scalability

   Disadvantages:

   - A bridge cannot filter out broadcast traffic.
   - It introduces 20 to 30 % latency.
   - Only 2 networks can be linked with a bridge

☞ Check Your Progress 2

1. Following are some advantages and disadvantages of switches:

   Advantages:

   - Reduces the number of Broadcast domains
   - Supports VLAN's (virtual local area network (VLAN) is a logical grouping of hosts on one or more LANs that allows communication to occur between hosts as if they were on the same physical LAN.) that can help in Logical segmentation of ports [physical ports]. Splitting up the broadcast domain.
   - Intelligent device [compared to Hub's] which can make use of CAM table for Port to MAC mapping
   - Compared to Bridges, Switches are more H/w oriented therefore operations are less CPU intense [Basic operations]
   - The cost to number of ports ratio is best i.e. for a cheaper cost you get switches with more number of ports available than Routers.

   Disadvantages:

   - Not as good as a router in limiting Broadcasts
   - Communication between VLAN's need inter VLAN routing [Router], but these days there are a number of Multilayer switches available in the market.
   - Handling Multicast packets needs quite a bit of configuration & proper designing.

2. In a communications network, gateway is a network node equipped for interfacing with another network that uses different protocols.

A gateway may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability. It also requires the establishment of mutually acceptable administrative procedures between both networks. A protocol translation/mapping gateway interconnects networks with different network protocol technologies by performing the required protocol conversions.