UNIT 1 NETWORK DEVICES-I

Structure **Page Nos.**

1.0 INTRODUCTION

As corporations grow, network designers need to extend the area of a network, the number of users on a particular network, and the bandwidth available to the network users. To solve these problems, network designer break a network into smaller portions and connect them with networking devices such as bridges, switches and gateways etc. Depending on the complexities of each of the networks being connected, a choice is made between these different network devices.

In this unit and the next unit we will examine features of several network devices.

1.1 OBJECTIVES

After going through this unit you should be able to define and differentiate between the following:

- Repeaters
- Bridges
- Switches
- Hubs

1.2 NETWORK DEVICES

Most common features of network devices are to interconnect networks, boost signals etc. The basic difference between them is that they operate at different layers. Now let us examine each device separately.

1.2.1 Repeaters

When a signal is sent over a long network cable, signal gets weakened due to attenuation. This results in ever data getting lost in the way. In order to boost the data signal Repeaters are needed to amplify the weakened signal. They are known as signal boosters or amplifiers. They are physical layer devices. They are like a small box that connects two segments of networks, refines and regenerate the digital signals on the cable and sends them on their way.

It helps in increasing the geographical coverage of network i.e. LAN for example IEEE 802.3 standard allow for upto four repeaters connecting five cables segments to a maximum of 3000 meters distance.

Repeaters use different physical media as: Ethernet cable and fibre optic cable: Token ring networks translate between electrical signals on shielded or unshielded twisted pair wiring and light pulse on fibre-optic cabling.

In modern installations repeaters are housed in the central wiring hubs of 10 Base-T and fibre optic cable systems.

Repeaters send every bit of data appearing on either cable segment through to the other side, even if data consist of malformed packets from a malfunctioning Ethernet adapter or packets not destined for use of the local LAN segment.

Figure 1 : Repeater Action

1.2.2. Bridges

Segmenting a large network with a network device has numerous benefits. Among these are reduced collisions (in an Ethernet network), contained bandwidth utilisation, and the ability to filter out unwanted packets. However, if the addition of the interconnect device required extensive reconfiguration of stations, the benefits of the device would be outweighed by the administrative overhead required to keep the network running. Bridges were created to allow network administrators to segment their networks transparently. This means that individual stations need not know whether there is a bridge separating them or not. It is up to the bridge to make sure that packets get properly forwarded to their destinations. This is the fundamental principle underlying all of the bridging behaviours.

Bridges work at the Data Link layer of the OSI model. Since bridges work in the Data Link layer they do not examine the network layer addresses. They just look at the MAC addresses for Ethernet and Token Ring, token bus and determine whether or not to forward or ignore a packet.

Purpose of a Bridge

The purposes of a Bridge are the following:

1. Isolates networks by MAC addresses
2. Manages network traffic by filtering packets
3. Translates from one MAC protocol to another.

Now let us examine the functionality of a bridge in detail.

1. **Isolates networks by MAC addresses**

A bridge divides a network into separate collision domains *(Figure 2)*. This reduces congestion as only frames that need to be forwarded are sent across interfaces. All transmissions between nodes connected to same segment are not forwarded and therefore do not load the rest of the network.

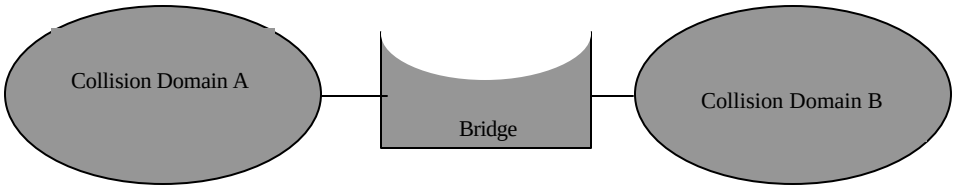

Figure 2: Bridge (Connecting two Ethernet LANs)

Thus bridges effectively improve the bandwidth of the network by reducing the unnecessary traffic in the network.

For example, if you have one segment called Segment 100: it has 50 users (in several departments) using this network segment. The Engineering Department is CAD (Computer Aided Design) - oriented, while the Accounting Department is into heavy number crunching (year end reports, month end statements, etc.). On this network, any traffic between Clients of Accounting Department and the Accounting File Server (in the Accounting Department) will be heard across the Segment 100. Likewise, any traffic between the Engineering Dept clients (to the CAD File Server) will be heard throughout the Network Segment. The result is that "Other" Department accesses to the Generic File Server are incredibly slow: this is because of the unnecessary traffic that's being generated from other departments (Engineering and Accounting).

The solution is to use one Bridge to isolate the Accounting Department, and another bridge to isolate the Engineering Department. The Bridges will only allow packets to pass through that are not on the local segment. The bridge will first check its "routing" table to see if the packet is on the local segment. If it is, it will ignore the packet, and not forward it to the remote segment. If Client of Accounting Department sends a packet to the Accounting File Server then Bridge #1 will check its routing table (to see if the Accounting File Server is on the local port). If it is on the local port, then Bridge #1 will not forward the packet to the other segments. If a Client of Accounting Department sends a packet to the Generic File Server, Bridge #1 will again check its routing table to see if the Generic File Server is on the local port. If it is not, then Bridge #1 will forward the packet to the remote port.

2. **Manages network traffic by filtering packets**

Bridges listen to the network traffic, and build an image of the network on each side of the bridge. This image of the network indicates the location of each node (and the bridge's port that accesses it). With this information, a bridge can make a decision whether to forward the packet across the bridge - if the destination address is not on the same port - or, it can decide not to forward the packet (if the destination is on the same port).

This process of deciding whether or not to forward a packet is termed "filtering packets." Network traffic is managed by deciding which packets can pass through the bridge; the bridge filters packets.

3. **Translates from one protocol to another**

The MAC layer also contains the bus arbitration method used by the network. This can be CSMA/CD, as used in Ethernet, or Token Passing, as used in Token Ring. Bridges are aware of the Bus Arbitration and special translation bridges can be used to translate between Ethernet and Token Ring LANs.

Bridges physically separate a network segment by managing the traffic (that's based on the MAC address). Bridges are store and forward devices. They receive a packet on the local segment, store it, and wait for the remote segments to be clear before forwarding the packet. The two physical types of bridges are Local and Remote Bridges.

4. **Local Bridges**

Local Bridges are used (as in the previous examples) where the network is being locally (talking physical location now) segmented. The 2 segments are physically close together: same building, same floor, etc. Only one bridge is required.

5. **Remote Bridges**

Remote Bridges are used in pairs, and also used where the network is remotely segmented (again, talking physical locations). The two segments are physically far apart: different buildings, different floors, etc. 2 x Half Bridges are required: one at each segment. The Remote bridges are 1/2 of a normal bridge, and may use several different communications media in between.

6. **Bridging Methodologies**

Transparent Bridges examine the MAC address of the frames to determine whether the packet is on the local Segment or on the distant Segment. Early bridges required the system administrator to manually build the routing table to tell a bridge which addresses were on which side of the bridge. Manually building a routing table is called fixed or static routing. Modern bridges are self-learning: they listen to the network in **promiscuous mode**, meaning that they accept all packets, regardless of the packets' addressing. The bridge then looks up each packet's Destination DLC Address in its internal tables to find out which port the Destination NIC is attached to. Finally, it forwards the packet onto only the necessary port. In the case of a broadcast message, the bridge forwards the packet onto every port except the port that the packet came in. **Promiscuous listening** is the key to the bridge's transparent operation. Since the bridge effectively "hears" all packets that are transmitted, it can decide whether forwarding is necessary without any special behaviour from the individual stations.

Consider a situation where there are two Bridges, Bridge A and Bridge B. As frames flow on Bridge A's local port, Bridge A examines the source address of each frame. Any frames with a destination address (other than the nodes on the local port) are forwarded to the remote port. As far as Bridge A is concerned, nodes on Bridge B's local port appear as if they were on Bridge A's remote port and therefore are mapped in the table accordingly. Similarly Bridge B also develops its routing table for various nodes.

The algorithm used by transparent bridges is backward learning. As mentioned above the bridges operate in **promiscuous mode** and track the source addresses of different frames. Because it knows what ports different addresses come from, it also knows

onto what port to send packets going to those addresses. The backward learning algorithm can be written in Pseudo Code as follows:

If the address is in the tables then

Forward the packet onto the necessary port.

If the address is not in the tables, then

> *Forward the packet onto every port except for the port that the packet was received on, just to make sure the destination gets the message. Add an entry in your internal tables linking the Source Address of the packet to whatever port the packet was received from.*

Take, for example, a simple network consisting of a four-port transparent bridge with five stations attached to it. The ports on the bridge shall be numbered one through four, with Station A and Station B on port 1, no station on port 2, Station C on port 3, and Station D and Station E on port 4. The bridge has just been brought on-line, and its tables are empty.

Station B transmits a packet destined for Station C. Since the bridge doesn't know what port station B is on yet, it puts the packet out onto every port except Port 1 (the packet came from Port 1, so the bridge knows that the packet has already been seen by stations on Port 1). This behavior is known as flooding. The bridge also examines the Source Address in the packet and determines that Station B is attached to Port 1. It updates its tables to reflect this.

Now that the bridge knows where Station B is, it will forward packets destined for Station B only onto Port 1. As stations transmit packets, the bridge will learn the location of more and more stations until, finally, it knows the location of every station that is attached to its ports. The beauty of the system is that even if the bridge doesn't know the location of a station, packets still get sent to their destination, just with a tiny bit of wasted bandwidth.

Finally, the bridge ages each entry in its internal tables and deletes the entry if, after a period of time known as the aging time, the bridge has not received any traffic from that station. This is just an extra safeguard to keep the bridge's tables up-to-date.

7. Advantages of Transparent Bridges

- Self learning: Requires no manual configuration, considered plug and work.
- Independent of higher level protocols (TCP/IP, IPX/SPX, Netbeui, etc.).
- No hardware changes required, no software changes required.

8. Disadvantages of Transparent Bridges

Can only work with one path between segments: loops are not allowed. A loop would confuse the bridge as to which side of the bridge a node was really on (i.e., local or remote) ? Transparent Bridges are not suitable for use on MANs or WANs, because many paths can be taken to reach a destination. In a LAN, it is simple to determine that a loop occurs, but in a large corporate network (with several hundred bridges), it may be next to impossible to determine. As such, Bridges are most commonly used in LAN to LAN connectivity (and not in MANs or WANs).

9. Spanning Tree Bridges

The Spanning Tree Protocol was developed to address the problems of loops in Transparent Bridging. The IEEE 802.1D committee standardized the Spanning Tree Protocol.
The Spanning Tree Protocol (STP) converts a loop into a tree topology by disabling a bridge link. This action ensures that there is a unique path from any node to every other node (in a MAN or WAN). Disabled bridges are kept in a stand-by mode of operation until a network failure occurs. At that time, the Spanning Tree Protocol will attempt to construct a new tree, using any of the previously disabled links.

The Spanning Tree Protocol is a Bridge-to-Bridge communication where all bridges cooperate to form the overall bridge topology. The Spanning Tree algorithm is dynamic, and periodically checks every one to four seconds to see if the bridge topology has changed.

Each bridge is assigned an arbitrary number that assigns priority to the bridge in the Internetwork. The number is concatenated with the bridge MAC address. If 2 bridges have the same priority, the MAC address is used as a tie breaker mechanism. The lower the assigned number, the higher the bridge priority.

During initial power-up, a Bridge Protocol Data Unit (BPDU) floods each network port of the bridge. The BPDU contains the following: the current spanning tree root, the distance to the root (measured in hops through other bridges), the bridge address information, and the age of the information in the BPDU. Bridge priorities are usually controlled manually so as to configure the traffic flow - over the Internetwork - on a preferred path.

Problems can arise where, for example, the Spanning Tree Algorithm may select a path from Los Angeles to New York City and back to San Francisco rather than the preferred route of Los Angeles to San Francisco.

10. Source Routing Bridges

Source-Routing is mostly used to interconnect token ring LANs. In Source-Routing, the source station must determine, in advance, the route to the LAN of the destination station, and include this route in the header of each frame. To determine the routing information, the source station first issues a search frame which is generally an LLC *TEST* command, on its ring. If a response is received from the desired destination station, it indicates that both source and destination stations are on the same ring and that no routing information is required. However, if no response is received, the source station issues a route discovery frame, which fans-out on every ring in the LAN segment. As the frame is forwarded from one ring to another, each bridge updates the routing information in the search frame. When the search frame reaches the destination, it contains the route between the source and destination stations. The destination station then sends a response frame to the source station, with the routing information. Both stations then use the routing information in each subsequent frame sent to each other.

Source-Routing uses two key parameters to identify a route between a source station and a destination station. These parameters are ring numbers and bridge numbers. Each ring is assigned a unique number. These numbers generally range between 1 and FFF (hex). Each bridge is assigned a bridge number, ranging between 0 and F (hex). The only restriction when assigning bridge numbers is that parallel bridges, connecting identical rings, must have different bridge numbers. The route between the source and the destination stations consists of LAN numbers and bridge numbers. The route is obtained by that each bridge which receives the route discovery frame adds to the existing route, its number and the ring number that it forwards this frame to.

- *The host uses its known path to the destination if it has one that is not old.*
- *Else, the host sends a probe message.*
- *The probe will be forwarded by every bridge that sees it, on every LAN to which the bridge is attached (except the one the probe came in on).*
- *If the bridge sees its own ID already in the path the probe is accumulating, it will drop the probe without forwarding (preventing a loop).*
- *The probe will eventually get to the destination by every possible path, including the shortest.*
- *The destination will return the probe to the sender, using the best discovered route as its source routing path.*
- *The source will then send its "real" message using the newly discovered route.*

1.2.3 Switches

A switch is a device that incorporates bridge functions as well as point-to-point 'dedicated connections'. They connect devices or networks, filter, forward and flood frames based on the MAC destination address of each frame. Switch operates at data-link layer of the OSI model. They are technically called bridges. They move data without contention. Ethernet switches provide a combinations of shared/dedicated 10/100/1000 Mbps connections. Some E-net switches support cut-through switching: frame forwarded immediately to destination without awaiting for assembly of the entire frame in the switch buffer. They significantly increases throughput. They provide express lane for traffic.

Figure 3: Switch

1.2.4 Hubs

If multiple incoming connections need to be connected with multiple outgoing connections, then a hub *(Figure 4)* is required. In data communications, a hub is a place of convergence where data arrives from one or more directions and is forwarded out in one or more other directions. Hubs are multi-port repeaters, and as such they obey the same rules as repeaters. They operate at the OSI Model Physical Layer.

Hubs are used to provide a Physical Star Topology. At the center of the star is the Hub, with the network nodes located on the tips of the star.

Figure 4: Hub

Star Topology

The Hub is installed in a central wiring closet, with all the cables extending out to the network nodes. The advantage of having a central wiring location is that it's easier to maintain and troubleshoot large networks. All of the network cables come to the central hub. This way, it is especially easy to detect and fix cable problems. You can easily move a workstation in - a star topology - by changing the connection to the hub at the central wiring closet.

The disadvantages to a star topology are given below:

- Failure of the Hub can disable a major section of the network.
- The Star Topology requires more cabling than does the ring or the bus topology because all stations must be connected to the hub, not to the next station.

Hub's Segment-to-Segment Characteristics

To understand the Ethernet segment-to-segment characteristics of a hub, let us first determine how the Ethernet Hubs operate. Logically, they appear as a Bus Topology, and physically as a Star Topology. Looking inside an Ethernet Hub, we can see that it consists of a electronic printed circuit board. Understanding that inside the Hub is only more repeaters, we can draw the conclusion that all connections attached to a Hub are on the same Segment (and have the same Segment Number). A single repeater is said to exist from any port to any port, even though it is indicated as a path of 2 repeaters.

Cascaded Hub Network

Connecting Hubs together through ports creates Cascading Hubs. One Master Hub (Level 1) is connected to many Level 2 (Slave) Hubs, who are masters to Level 3 (Slave) Hubs in a hierarchical tree (or clustered star). The maximum number of stations in a Cascaded Hub Network is limited to 128.

Backbone Networks

In a Backbone Network, there is no Master Hub. The Level 1 Hubs are connected through their AUI port to a Coax Backbone. For Thin Coax, up to 30 Hubs can be

connected together. For Thick Coax, up to 100 Hubs can be connected to the backbone. The Backbone is considered to be a populated segment.

Level 2 Hubs are allowed to be connected to the Level 1 Hubs' 10BaseT ports. This connection between the 2 Hubs is considered an un populated segment, or link segment. Up to 1024 stations (or nodes) can be attached to the Level 2 Hubs' 10 BaseT ports.

All stations and segments would appear as one logical segment, with one network Number. In the real world, 1024 stations are never attached to one segment; as the resulting traffic would slow the network to a crawl.

Hub's Addressing

Because a Hub is just many repeaters in the same box, any network traffic between nodes is heard over the complete network. As far as the stations are concerned, they are connected on one long logical bus (wire).

Half-Duplex and Full-Duplex Ethernet Hubs

Normal Ethernet operation is Half-Duplex: only 1 station or node is talking at a time. The stations take turns talking on the bus (CSMA/CD -bus arbitration).

Full-Duplex Ethernet Hubs are Hubs which allow two-way communication, thus doubling the available bandwidth from 10 Mbps to 20 Mbps. Full duplex Hubs are proprietary products, and normally only work within their own manufacturer's line.

For example, if A wanted to talk to C, a direct 10 Mbps line would be connected through the 2 switching hubs. Simultaneously, if D wanted to talk to B, another direct 10 Mbps line (in the opposite direction) would be connected through the two switching Hubs (doubling the available bandwidth to 20 Mbps).

There are no official standards for Full-Duplex Ethernet although proprietary standards do exist.

Switching Hubs

Switching hubs are hubs that will directly switch ports to each other. They are similar to full duplex hubs, except that they allow dedicated 10 Mbps channels between ports.

If A wanted to communicate with B, a dedicated 10 Mbps connection would be established between the two. If C wanted to communicate with D, another dedicated 10 Mbps connection would be established.

1.2.5 Comparison of Switches and Hubs

	HUBS	**SWITCHES**
1.	Collision Domain	Broadcast Domain
2.	All of the parts on a hub are part of the same Ethernet	Each part on a switches may be regarded as a separate Ethernet (but all are part of the same local area network)
3.	All parts on a hub share the same 10Mb (100 Mb) bandwidth	Each part on a switch has its own 10Mb (100 Mb) bandwidth
4	Any frame appearing on one port of a hub is repeated to all other ports on the hub	A directed frame appearing on one part of a switch is forwarded only to the destination port.

5.	A sniffer on any hub port can see all of the traffic on the network	Switched networks are difficult to sniff
6.	A hub will repeat defective frames	

☞ **Check Your Progress 1**

1) Which of the following network device is used at the physical layer?

(a) Routers (b) Bridge (c) Repeaters (d) Switches

2) List the major functionalities of a Bridge are

……

……

……

3) Compare Switches and Hubs.

……

……

……

4) What are Switching Hubs?

……

……

……

1.3 SUMMARY

In this unit we have studied about features of different network devices namely **repeaters, bridge, hubs and switches.**

Repeaters are used in long distance network cable to enhance the signals that get wakened due to attenuation.
Bridges are used to interconnect multiple LANs two devices at the data link layers of the OSI model.
Switches are used for performing bridges functions as well as point-to-point dedicated connections.
Hubs are used to interconnect various incoming connections with different outgoing connections at the Physical layer of the OSI model.

In the next unit we will examine another set of network devices.

1.4 SOLUTIONS/ANSWERS

1) Repeater
2) The major functionalities of a bridge are:
   - Connect multiple LANs
   - Manage network traffic by filtering packets
   - Translate from one MAC address to another

3) Refer to Section 1.2.5
4) Refer to Section 1.2.4.