

LAB - 1(Study of Network Devices)

A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams. Computer networks components comprise both Hardware parts as well as the software parts required for installing computer networks, both at organizations and at home. The hardware components are the server, client, peer, transmission medium, and connecting devices.

The hardware components are as follows:

- 1) Servers: -Servers are high-configuration computers that manage the resources of the network. The network operating system is typically installed in the server and so they give user accesses to the network resources.
- 2) Clients: - Clients are computers that request and receive service from the servers to access and use the network resources.
- 3) Peers: - Peers are computers that provide as well as receive services from other peers in a work group network.
- 4) Transmission Media: - Transmission media are the channels through which data is transferred from one device to another in a network.
- 5) Networking Devices: - Connecting devices act as middleware between networks or computers, by binding the network media together.

The Software Components are as follows:

Operating System - Network Operating Systems is typically installed in the server and facilitate workstations in a network to share files, database, applications, printers etc.

Protocol Suite - A protocol is a rule or guideline followed by each computer for data communication. Protocol suite is a set of related protocols that are laid down for computer networks.

Following are some networking devices:

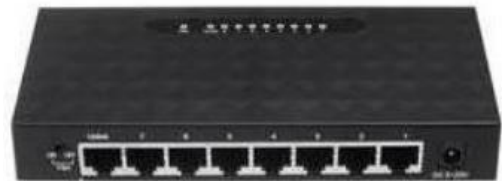
- 1) Router:** Routers are networking devices operating at layer 3 or a network layer of the OSI model. They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.

Working of Router:

A router examines a packet header's destination IP address and compares it against a routing table to determine the packet's best next hop. Routing tables list directions for forwarding data to particular network destinations, sometimes in the context of other variables, like cost. They amount to an algorithmic set of rules that calculate the best way to transmit traffic toward any given IP address. A routing table often specifies a default route, which the router uses whenever it fails to find a better forwarding option for a given packet. For example, the typical home office router directs all outbound traffic along a single default route to its internet service provider (ISP). Routing tables can be static i.e., manually configured or dynamic. Dynamic routers automatically updated their routing tables based on network activity, exchanging information with other devices via routing protocols.



2) Hub: A Network Hub is one of the most commonly used networking devices can be easily found on any small networks such as home or office. Hub operates at the physical layer of OSI model. It is the simplest networking device hence has low cost. Basically, a hub is a repeater with multiple ports. The function of a hub in networking is similar to the repeater. It transfers data in the form of binary bits and uses for broadcasting data.



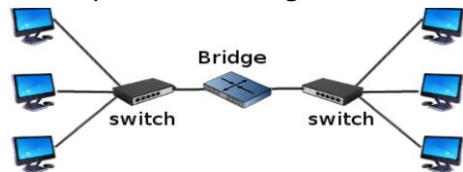
Working of Hubs: When a host sends frames, the hub forwards the frames in all the ports. Hubs do not separate the type of the frame, for example, whether the frame unicast should be either multicast or broadcast. Hubs forward all the frames into all the ports. Although a hub sends the frames to all the ports, a computer accepts the ones, whose MAC match matches the destination MAC address field. The rest of the frames are discarded after receiving the required information.

3) Switch: A switch is a Networking device in a computer network that connects other devices together. Multiple data cables are plugged into a switch to enable communication between different networked devices. Switches manage the flow of data across a network by transmitting a received network packet only to the one or more devices for which the packet is intended.



Working of Switch: Whenever a host sends a frame to any other host, then the source host is stored with the port in the address table of the MAC address switch. A switch always stores the address of the source in the table. Unless a host does send some data, its MAC address and port number will not be stored in the table of the switch. Unless a host does send some data, its MAC address and port number will not be stored in the table of the switch. When you initialize the switch, the switch does not contain any information about any host and its address. In such a situation, when a host frame sends, its MAC address is stored in the table but due to no destination information, the switch sends the frame to all the hosts. When you initialize the switch, the switch does not contain any information about any host and its address. In such a situation, when a host frame sends, its MAC address is stored in the table but due to no destination information, the switch sends the frame to all the hosts. As soon as the second host sends some data, its address also gets stored in the table. As soon as the second host sends some data, its address also gets stored in the table. Whenever a host sends the frames, the switch stores it if its address is not already present in the table. Thus, a switch creates its table. When all the hosts addresses and port numbers come in the switch, the switch delivers the frame to all hosts only, delivering the same host to the host for which the data has been sent.

4) Bridge: Bridge is termed as a network device which is helpful in filtering the data load of the traffic by dividing it into segments or packets. They are used to lower the load of traffic on the LAN and other networks. Bridges are passive devices, because there is no interaction between bridged and the paths of bridging. Bridges operate on the second layer of the OSI model that is the data link layer.



Working of Bridge: When various network segments are established at the data link layer of the OSI model, we refer to it as bridge. However, when the packets of data are transferred along a network, without locating the network addresses this process is termed as bridging. The process of bridging is helpful in locating the addresses of unknown addresses to which it is viable to send data. In bridging the data packets contain a header or a packet header which holds the address to the intended device. Bridge can remember and recall the address of the devices for further transmission. There are two kinds of bridging modes, the transparent bridging and the source routing bridging. When the process of bridging occurs, it makes a bridging table alongside where it stores the MAC addresses of the various terminals. This table helps the bridges to send the data packet to the exact location next time. However, when a specific address does not meet the contents of the bridging table, the data packet is forwarded further ahead to every attached terminal in LAN except from the computer it is connected to. This type of bridging is called transparent bridging. When the

source computer presents pathway information within the packet, this type of bridging is known as source route bridging. It is most commonly used in used on Token Ring networks.

5) Repeater: A repeater is a network device that retransmits a received signal with more power and to an extended geographical or topological network boundary than what would be capable with the original signal repeater is implemented in computer networks to expand the coverage area of the network, re propagate a weak or broken signal and or service remote nodes.



Working of Repeater: When an electrical signal is transmitted via a channel, it gets attenuated depending upon the nature of the channel or the technology. This poses a limitation upon the length of the LAN or coverage area of cellular networks. This problem is alleviated by installing repeaters at certain intervals. Repeaters amplifies the attenuated signal and then retransmits it. Digital repeaters can even reconstruct signals distorted by transmission loss. So, repeaters are popularly incorporated to connect between two LANs thus forming a large single LAN.

6) Gateway: The link between two computers to connect to internet or another network is called gateway. The gateway works like a portal among two programs by means of communications between protocol and permit them to share data on same computers or among different computers. Gateways are also known as protocol converter that can perform at any OSI model layer.



Working of Gateway: A gateway is a network point that works as an access to another network. Generally, in intranet a node can be either a gateway node or the nodes that join the network are gateways. In large organization where the computers control the traffic between organization networks are gateway nodes. Like that the computers used by ISP to connect different user with each other at a time to the internet are gateway nodes. In a project of any business company computer server work as a gateway node and it may be proxy server or firewall some time. A gateway may connect to a router because a router exactly known where to through a given packet of data that appears at the gateway then a switch finalizes the actual in and out path of the gateway for the specified packet. A gateway is a compulsory features of routes even though other devices can perform as a gateway. The operating system mostly used this term and internet connection sharing act as a gateway and creating a connection among internal network.