Experiment No : 01

Aim : Study of different network components

Theory :

1. **Bridges**

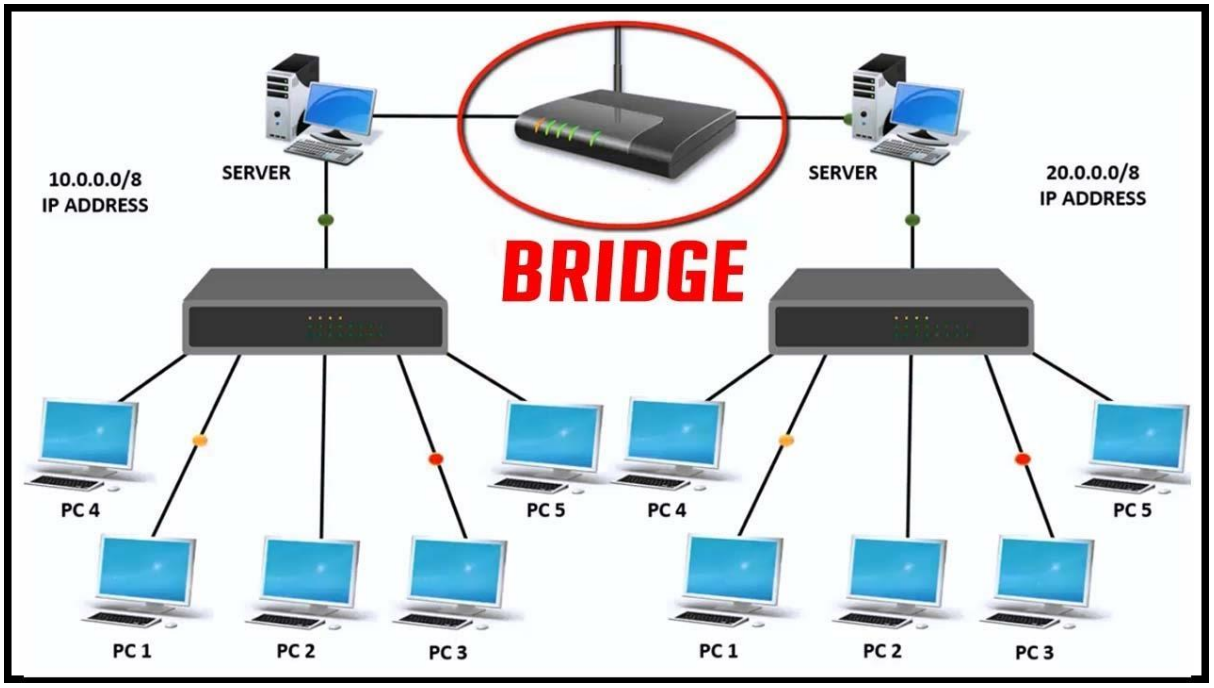
   A bridge is a network device that connects multiple LANs (local area networks) together to form a larger LAN. A bridge connects the different components so that they appear as parts of a single network. Bridges operate at the data link layer of the OSI model and hence are also referred to as Layer 2 switches. 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. A bridge functions by blocking or forwarding data, based on the destination MAC address written into each frame of data.

Uses of Bridge

● Bridges connect two or more different LANs that have a similar protocol and provide communication between the devices (nodes) in them.

● By joining multiple LANs, bridges help in multiplying the network capacity of a single LAN.



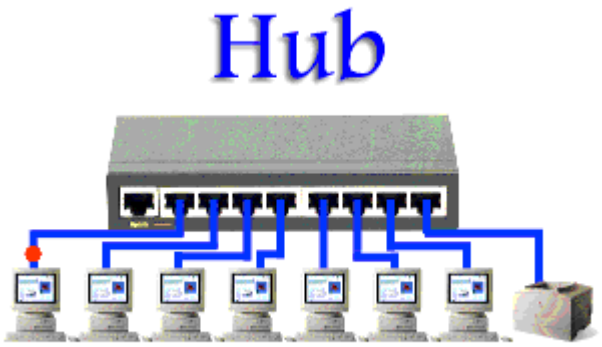
2. Hub

There are three types of network hubs: passive, active, and intelligent. network. They do not improve the performance of local area networks (LANs), and may limit maximum media distances. Typically, passive hubs are connected to other devices in a star configuration. In general, a hub refers to a hardware device that enables multiple devices or connections to connect to a computer. An example is a USB hub, which allows multiple USB devices to connect to one computer, even though that computer may only have a few USB connections Hub is commonly

used to connect segments of a LAN (Local Area Network). When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets. Hub acts as a common connection point for devices in a network. A hub has many ports in it. A computer which intends to be connected to the network is plugged into one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination device or not.

Features of Hubs

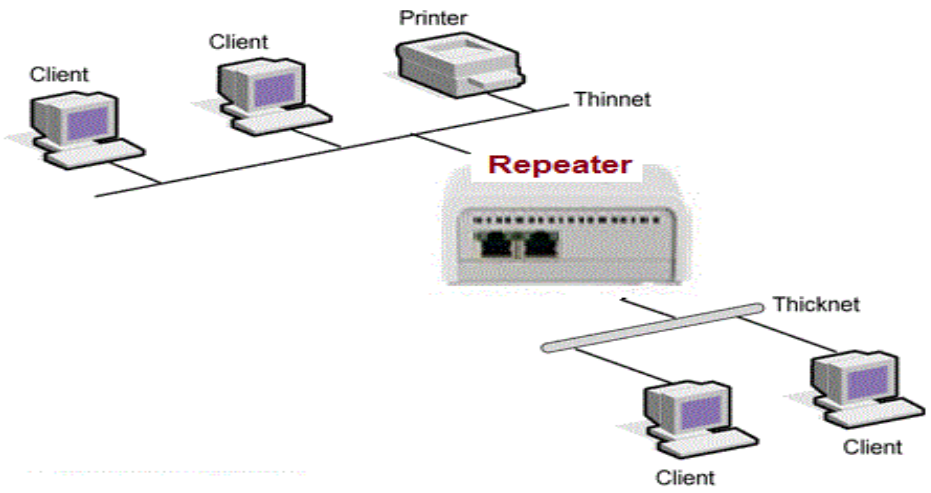
- A hub operates in the physical layer of the OSI model.
- A hub cannot filter data. It is a non-intelligent network device that sends messages to all ports.
- It primarily broadcasts messages. So, the collision domain of all nodes connected through the hub stays one.
- Transmission mode is half duplex.



3. **Repeaters**

A repeater is an electronic device that receives a signal and retransmits it. Repeaters are used to extend transmissions so that the signal can cover longer distances or be received on the other side of an obstruction. A repeater is implemented in computer networks to expand the coverage area of the network, repropagate a weak or broken signal and or service remote nodes. Repeaters amplify the received/input signal to a higher frequency domain so that it is reusable, scalable and available.Repeaters were introduced in wired data communication networks due to the limitation of a signal in propagating over a longer distance and now are a

common installation in wireless networks for expanding cell size. Repeaters are network devices operating at the physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters. 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 amplify 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.



4. **Routers**

An example of a router is a woodworking tool. An example of a router is computer hardware that transfers Internet messages to a laptop in another room; a wireless router. An intelligent switch capable of deciding where to forward packets based on a view of the network as a whole. Routers, acting as the police of network traffic, are responsible for directing different types of networks to maintain the best transmission routes on their own roads. They are wired routers, wireless routers, core routers, edge routers and VPN routers. A router is a computer whose software and hardware are designed to move data between computer networks. Routers

make sure traffic between computers goes where it needs to go. This is the first router your computer will connect to in order to get to the internet.

Features of Routers

● A router is a layer 3 or network layer device.
● It connects different networks together and sends data packets from one network to another.
● A router can be used both in LANs (Local Area Networks) and WANs (Wide Area Networks).
● It transfers data in the form of IP packets. In order to transmit data, it uses the IP address mentioned in the destination field of the IP packet.
● Routers have a routing table in it that is refreshed periodically according to the changes in the network. In order to transmit data packets, it consults the table and uses a routing protocol.
● In order to prepare or refresh the routing table, routers share information among each other.

Types Of Routers :

● Wireless Router − They provide WiFi connection WiFi devices like laptops, smartphones etc. They can also provide standard Ethernet routing. For indoor connections, the range is 150 feet while it's 300 feet for outdoor connections.
● Broadband Routers − They are used to connect to the Internet through telephone and to use voice over Internet Protocol (VoIP) technology for providing high-speed Internet access. They are configured and provided by the Internet Service Provider (ISP).
● Core Routers − They can route data packets within a given network, but

cannot route the packets between the networks. They help to link all devices within a network thus forming the backbone of the network. It is used by ISP and communication interfaces.

● Edge Routers − They are low-capacity routers placed at the periphery of the networks. They connect the internal network to the external networks, and are suitable for transferring data packets across networks. They use Border Gateway Protocol (BGP) for connectivity. There are two types of edge routers, subscriber edge routers and label edge routers.

● Brouters − Brouters are specialised routers that can provide the functionalities of bridges as well. Like a bridge, routers help to transfer data between networks. And like a router, they route the data within the devices of a network.

5. **Switches**

Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network. A switch has many ports, to which computers are plugged in. When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s).It supports unicast, multicast as well as broadcast communications.

Features of Switches

● A switch operates in the layer 2, i.e. data link layer of the OSI model.
● It is an intelligent network device that can be conceived as a multiport network bridge.
● It uses MAC addresses (addresses of medium access control sublayer) to send data packets to selected destination ports.
● It uses packet switching technique to receive and forward data packets from the source to the destination device.
● It supports unicast (one-to-one), multicast (one-to-many) and broadcast (one-to-all) communications.
● Transmission mode is full duplex, i.e. communication in the channel occurs in both the directions at the same time. Due to this, collisions do not occur.
● Switches are active devices, equipped with network software and network management capabilities.
● Switches can perform some error checking before forwarding data to the destined port.
● The number of ports is higher – 24/48.
● Unmanaged Switch − These are inexpensive switches commonly used in home networks and small businesses. They can be set up by simply plugging in to the network, after which they instantly start operating. When more devices need to be added, more switches are simply added by this plug and play method. They are referred to as u managed since they do not require to be configured or monitored.
● Managed Switch − These are costly switches that are used in organisations with large and complex networks, since they can be customised to augment the functionalities of a standard switch. The augmented features may be QoS (Quality of Service) like higher security levels, better precision control and complete network management. Despite their cost, they are preferred in growing organisations due to their scalability and flexibility. Simple Network Management Protocol (SNMP) is used for configuring managed switches.
● LAN Switch − Local Area Network (LAN) switches connect devices in the internal LAN of an organisation. They are also referred to as Ethernet

switches or data switches. These switches are particularly helpful in reducing network congestion or bottlenecks. They allocate bandwidth in a manner so that there is no overlapping of data packets in a network.

● PoE Switch − Power over Ethernet (PoE) switches are used in PoE Gigabit Ethernets. PoE technology combines data and power transmission over the same cable so that devices connected to it can receive both electricity as well as data over the same line. PoE switches offer greater flexibility and simplifies the cabling connections.

6. **Server**

A network server, today, is a powerful computer that provides various shared resources to workstations and other servers on a network. A given application in a computer may function as a client with requests for services from other programs and also as a server of requests from other programs. Servers are computers that run services to serve the needs of other computers. There are, for example, home media servers, web servers, and print servers. One company employee, for example, may log

in to the client computer to access the files and applications that the server runs. A server is a computer connected to a network of other workstations called 'clients'. Client computers request information from the server over the network. Servers tend to have more storage, memory and processing power than a normal workstation. In computing, a server is a computer program or a device that provides functionality for called clients which are other programs or devices. This architecture is called the client–server model. A single overall computation is distributed across multiple processes or devices. Servers can provide various functionalities called services. These services include sharing data or resources among multiple clients, or performing computation for a client. Multiple clients can be served by a single server, and a single client can use multiple servers. A client process may run on the same device. It can also connect over a network to a server to run on a different device. Examples of servers may include database servers, mail servers, print servers, file servers, web servers, application servers, and game servers.

Types of Servers and their applications:

1. Application server –

These servers host web apps (computer programs that run inside a web browser) allowing users in the network to run and use them, preventing the installation of a copy on their own computers. These servers need not be part of the World Wide Web. Their clients are computers with a web browser.

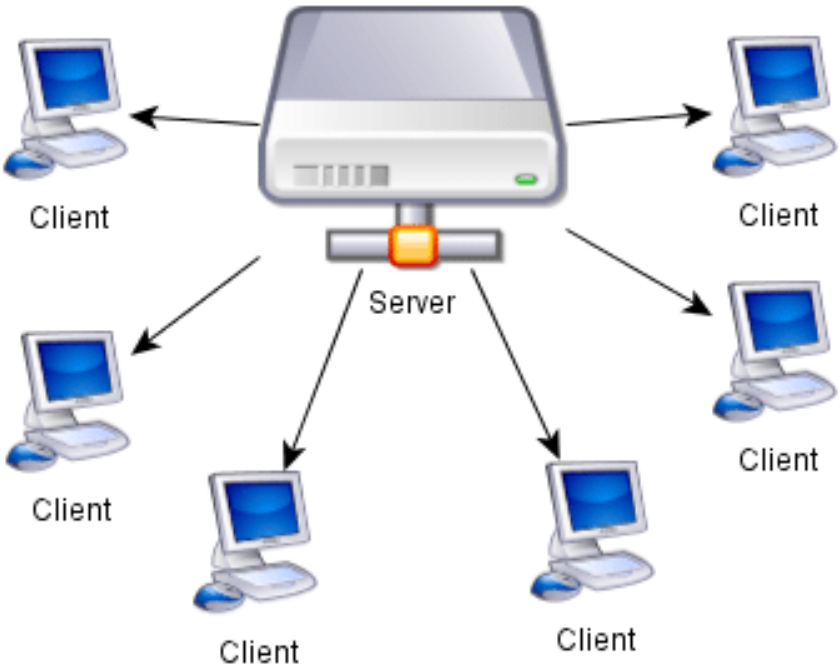
2. **Catalogue server –**

These servers maintain an index or table of contents of information that can be found across a large distributed network. Distributed networks may include computers, users, files shared on file servers, and web apps. Examples of catalogue servers are Directory servers and name servers. Their clients are any computer program that needs to find something on the network. Example can be a Domain member attempting to log in, an email client looking for an email address, or a user looking for a file

3. **Communications server –**

These servers maintain an environment needed for one

communication endpoint to find other endpoints and then communicate with them. These servers may or may not include a directory of communication endpoints and a presence detection service, depending on the openness and security parameters of the network. Their clients are communication endpoints.



7. **Gateway**

The definition of a gateway is an opening or entrance. An example of a gateway is the doorway of a barn. A gateway is a network node that forms a passage between two networks operating with different transmission protocols. The most common type of gateways, the network gateway operates at layer 3, i.e. network layer of the OSI (open systems interconnection) model. However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model. It acts as the entry – exit point for a network since all traffic that flows across the

networks should pass through the gateway. Only the internal traffic between the nodes of a LAN does not pass through the gateway.

Features of Gateways

● Gateway is located at the boundary of a network and manages all data that inflows or outflows from that network.

● It forms a passage between two different networks operating with different transmission protocols.

● A gateway operates as a protocol converter, providing compatibility between the different protocols used in the two different networks.

● The feature that differentiates a gateway from other network devices is that it can operate at any layer of the OSI model.

● It also stores information about the routing paths of the communicating networks.

● When used in enterprise scenarios, a gateway node may be supplemented as a proxy server or firewall.

● A gateway is generally implemented as a node with multiple NICs (network interface cards) connected to different networks. However, it can also be configured using software.

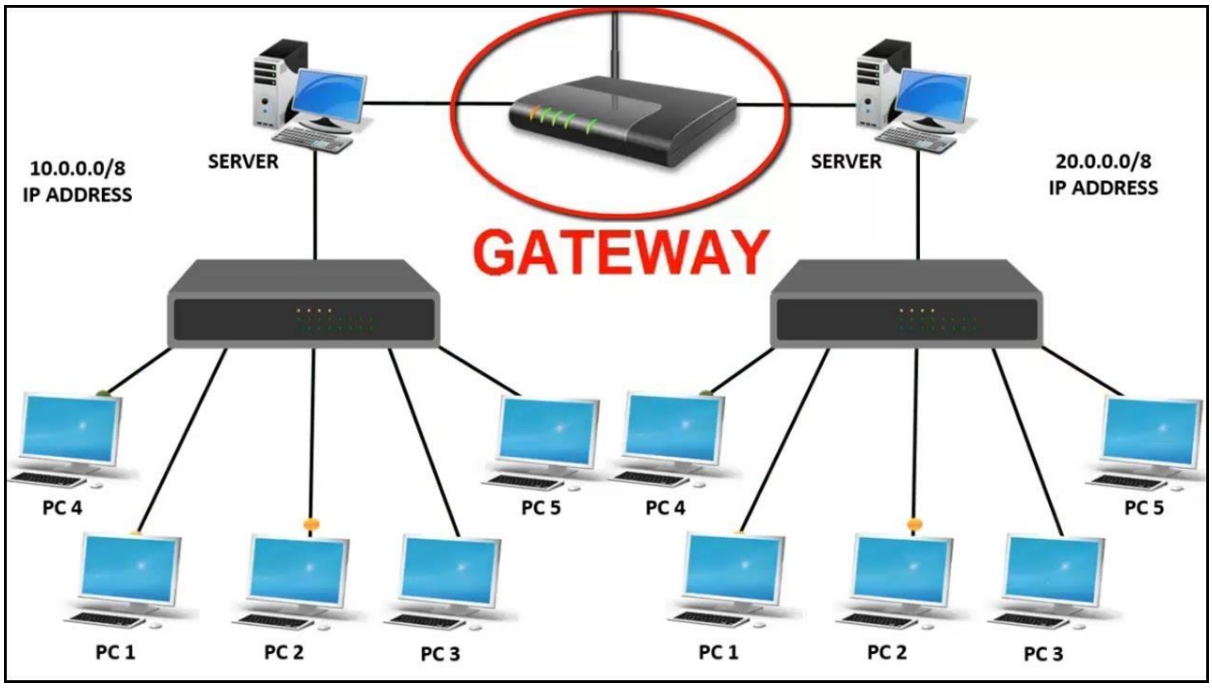
● It uses packet switching techniques to transmit data across the networks.

Types of Gateways

On basis of direction of data flow, gateways are broadly divided into two categories −

● Unidirectional Gateways − They allow data to flow in only one direction. Changes made in the source node are replicated in the destination node, but not vice versa. They can be used as archiving tools.

● Bidirectional Gateways − They allow data to flow in both directions. They can be used as synchronisation tools.



8. Modem

A modem is a device that connects your home, usually through a coax cable connection, to your Internet service provider (ISP), like Xfinity. The modem takes signals from your ISP and translates them into signals your local devices can use, and vice versa.There are three types of modems: cable, digital subscriber line (DSL) and dial-up. This type of modem delivers high speed internet to your device. DSL and dial-up modems use

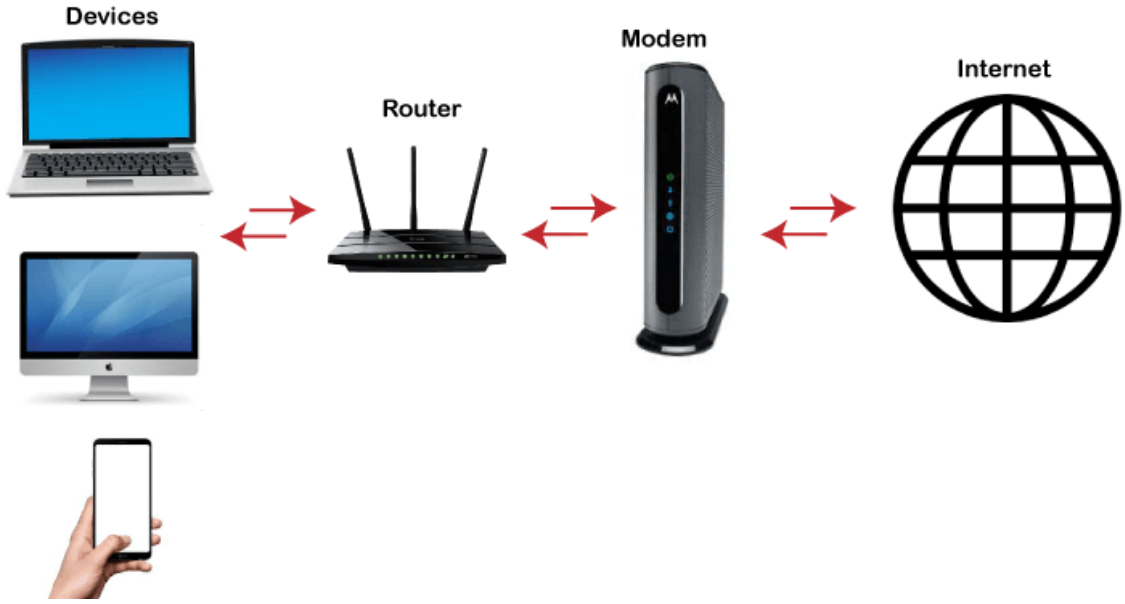
a cable that connects to your phone line. DSL, however, still allows you to use your landline telephone while connected to the internet. A modem is a small box that connects your household to the Internet using cables. It acts as a digital translator, taking an information signal (Internet data) from your cable or phone lines and making it accessible to your computer. Modulation techniques used for Modem: The basic modulation techniques used by a modem to convert digital data to analog signals are:

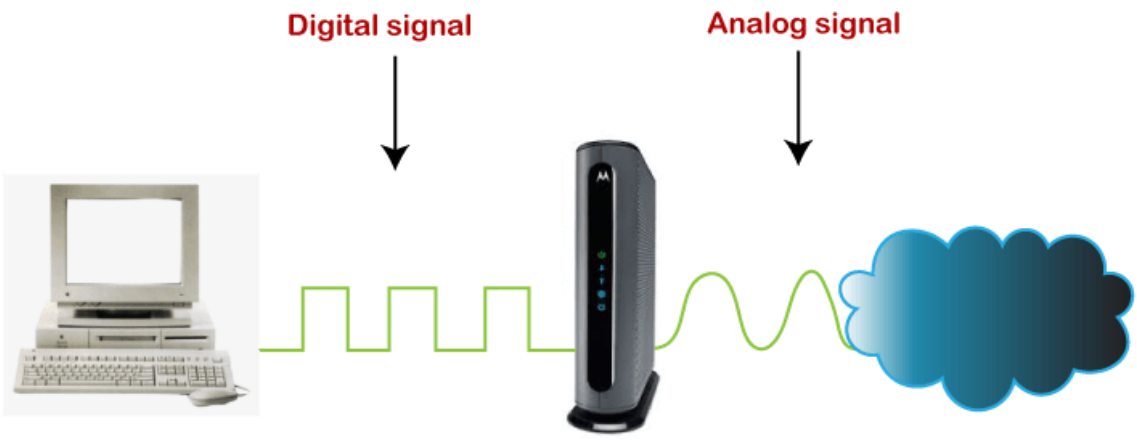
• Amplitude shift keying (ASK).
•Frequency shift keying (FSK).
• Phase shift keying (PSK).
• Differential PSK (DPSK).

These techniques are known as the binary continuous wave (CW) modulation.

•Modems are always used in pairs. Any system whether simplex, half duplex or full duplex requires a modem at the transmitting as well as the receiving end.

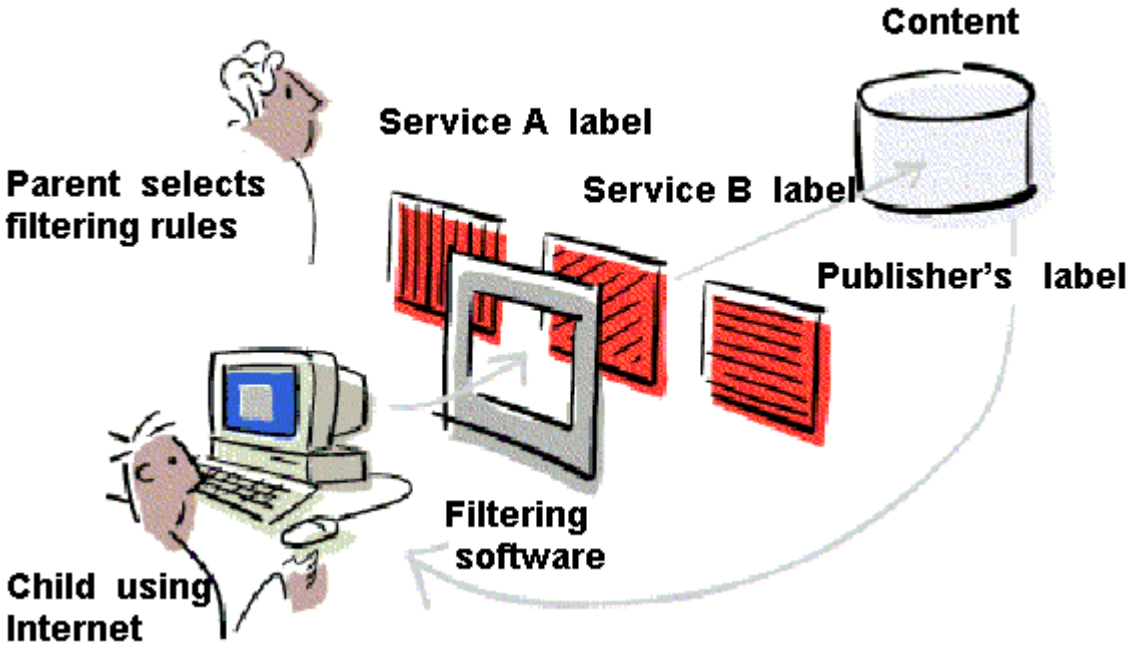
• Thus a modem acts as the electronic bridge between two worlds - the world of purely digital signals and the established analog world.


Devices
Router
Modem
Internet


Digital signal
Analog signal

9. Filters

   A filter is a network designed to pass signals having frequencies within certain bands (called pass-bands) with little attenuation, but greatly attenuates signals within other bands (called attenuation bands or stop-bands). The most common filter is a software filter that reads data in and manipulates the data to fit another output pattern or removes data that may not be needed. For example, spam filters help filter unwanted email from reaching your Inbox. 2. Hardware devices can also be filters.Filters are systems or elements used to remove substances such as dust or dirt, or electronic signals, etc., as they pass through filtering media or devices. Filters are available for filtering air or gases, fluids, as well as electrical and optical phenomena. Air filters are used for cleaning the air.During network communication, a node transmits a packet that is filtered and matched with predefined rules and policies. Once matched, a packet is either accepted or denied. Packet filtering checks source and destination IP addresses. If both IP addresses match, the packet is considered secure and verified. Because the sender may use different applications and programs, packet filtering also checks source and destination protocols, such as User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). Packet filters also verify source and destination port addresses. Some packet filters are not intelligent and unable to memorize used packets. However, other packet filters can memorize previously used packet items, such as source and destination IP addresses. Packet filtering is usually an effective defense against attacks from computers outside a local area network (LAN). As most routing devices have integrated filtering capabilities, packet filtering is considered a standard and cost-effective means of security.



Conclusion : Therefore we have successfully learned different types of network components .