**D22IT202**

**Practical-2**

**AIM:** Study at following Network devices in details**.**

1. **NIC:**

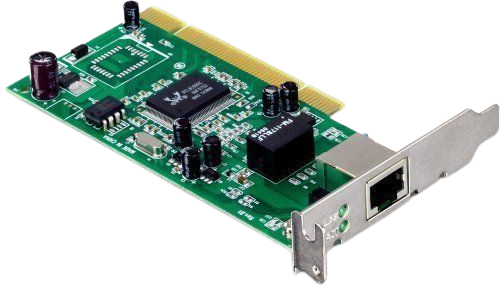
A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter.

* NIC allows both wired and wireless communications.
* NIC allows communications between computers connected via local area network (LAN) as well as communications over large-scale network through Internet Protocol (IP).
* NIC is both a physical layer and a data link layer device, it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

NIC cards are of two types:

1. Internal network cards:

In internal networks cards, motherboard has a slot for the network card where it can be inserted. It requires network cables to provide network access. Internal network cards are of two types. The first type uses Peripheral Component Interconnect (PCI) connection, while the second type uses Industry Standard Architecture (ISA).

****

1. External network cards:

In desktops and laptops that do not have an internal NIC, external NICs are used. External network cards are of two types: Wireless and USB based. Wireless network card needs to be inserted into the motherboard however no network cable is required to connect to the network. They are useful while traveling or accessing a wireless signal.

****

1. **HUB:**

A hub is a physical layer networking device which is used to connect multiple devices 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 or not.

In a network. They are generally used to connect computers in a LAN.

A hub has many ports in it. A computer which intends to be connected to the network is plugged in to 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 or not.



1. **Switch:**

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. it supports unicast, multicast as well as broadcast communications.

A switch is a device in a [computer network](https://en.wikipedia.org/wiki/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](https://en.wikipedia.org/wiki/Network_packet) only to the one or more devices for which the packet is intended. Each networked device connected to a switch can be identified by its [network address](https://en.wikipedia.org/wiki/Network_address), allowing the switch to direct the flow of traffic maximizing the security and efficiency of the network.

A switch is more intelligent than an [Ethernet hub](https://en.wikipedia.org/wiki/Ethernet_hub), which simply retransmits packets out of every port of the hub except the port on which the packet was received, unable to distinguish different recipients, and achieving an overall lower network efficiency.

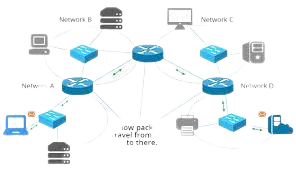
1. **Router:**

A router is a [networking device](https://en.wikipedia.org/wiki/Networking_device) that forwards [data packets](https://en.wikipedia.org/wiki/Data_packet) between [computer networks](https://en.wikipedia.org/wiki/Computer_network). Routers perform the traffic directing functions on the [Internet](https://en.wikipedia.org/wiki/Internet). Data sent through the internet, such as a [web page](https://en.wikipedia.org/wiki/Web_page) or [email](https://en.wikipedia.org/wiki/Email), is in the form of data packets. A packet is typically [forwarded](https://en.wikipedia.org/wiki/Packet_forwarding) from one router to another router through the networks that constitute an [internetwork](https://en.wikipedia.org/wiki/Internetwork) until it reaches its destination [node](https://en.wikipedia.org/wiki/Node_(networking)).

A router is connected to two or more data lines from different [IP networks](https://en.wikipedia.org/wiki/IP_network). When a data packet comes in on one of the lines, the router reads the [network address](https://en.wikipedia.org/wiki/Network_address) information in the packet header to determine the ultimate destination. Then, using information in its [routing table](https://en.wikipedia.org/wiki/Routing_table) or [routing policy](https://en.wikipedia.org/wiki/Routing_policy), it directs the packet to the next network on its journey.

When multiple routers are used in interconnected networks, the routers can exchange information about destination addresses using a [routing protocol](https://en.wikipedia.org/wiki/Routing_protocol). Each router builds up a [routing table](https://en.wikipedia.org/wiki/Routing_table), a list of routes, between two computer systems on the interconnected networks.

The software that runs the router is composed of two functional processing units that operate simultaneously, called planes:

* [Control plane](https://en.wikipedia.org/wiki/Control_plane): A router maintains a routing table that lists which route should be used to forward a data packet, and through which physical interface connection.
* [Forwarding plane](https://en.wikipedia.org/wiki/Forwarding_plane): This unit forwards the data packets between incoming and outgoing interface connections. It reads the [header](https://en.wikipedia.org/wiki/Header_(computing)) of each packet as it comes in, matches the destination to entries in the FIB supplied by the control plane, and directs the packet to the outgoing network specified in the FIB.

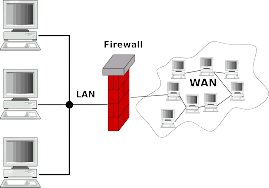
1. **Gateway:**

A gateway is a [network node](https://www.techtarget.com/searchnetworking/definition/node) used in telecommunications that connects two networks with different transmission [protocols](https://www.techtarget.com/searchnetworking/definition/protocol) together. Gateways serve as an entry and exit point for a network as all data must pass through or communicate with the gateway prior to being routed. In most [IP](https://www.techtarget.com/searchunifiedcommunications/definition/Internet-Protocol)-based networks, the only traffic that does not go through at least one gateway is traffic flowing among nodes on the same local area network ([LAN](https://www.techtarget.com/searchnetworking/definition/local-area-network-LAN)) segment. The term default gateway or network gateway may also be used to describe the same concept.

The primary advantage of using a gateway in personal or enterprise scenarios is simplifying internet connectivity into one device. In the enterprise, a gateway node can also act as a [proxy server](https://www.techtarget.com/whatis/definition/proxy-server) and a [firewall](https://www.techtarget.com/searchsecurity/definition/firewall). Gateways can be purchased through popular technology retailers, such as Best Buy, or rented through an internet service provider.

Types of gateways:

* [Web application firewalls](https://www.techtarget.com/searchsecurity/definition/Web-application-firewall-WAF)- This type filters traffic to and from a web server and looks at application-layer data.
* [Cloud storage gateways](https://www.techtarget.com/searchstorage/definition/cloud-storage-gateway)- This type translates storage requests with various cloud storage service API calls. It allows organizations to integrate storage from a private cloud into applications without migrating into a public cloud.
* [API](https://www.techtarget.com/searchapparchitecture/definition/application-program-interface-API), [SOA](https://www.techtarget.com/searchapparchitecture/definition/service-oriented-architecture-SOA) or XML gateways – This type manages traffic flowing into and out of a service, microservices-oriented architecture or XML-based web service.
* IoT gateways-This type aggregates sensor data from devices in an IoT environment, translates between sensor protocols and processes sensor data before sending it onward.
* [Media gateways](https://www.techtarget.com/searchunifiedcommunications/definition/media-gateway)- This type converts data from the format required for one type of network to the format required for another.
* Email security gateways- This type prevents the transmission of emails that break company policy or will transfer information with malicious intent.
* [VoIP trunk gateways](https://www.techtarget.com/searchunifiedcommunications/definition/VoIP-trunk-gateway)- This type facilitates the use of plain old telephone service equipment, such as landline phones and fax machines, with a voice over IP (VoIP)



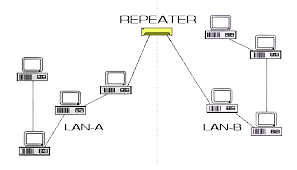
1. **Repeater:**

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.

A 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. 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.

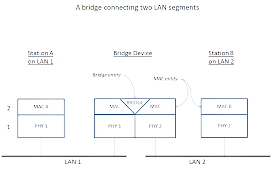
Repeaters are also known as signal boosters.



1. **Bridge:**

A network bridge is a [computer networking device](https://en.wikipedia.org/wiki/Networking_hardware) that creates a single, aggregate network from multiple [communication networks](https://en.wikipedia.org/wiki/Communication_network) or [network segments](https://en.wikipedia.org/wiki/Network_segment). This function is called network bridging. Bridging is distinct from [routing](https://en.wikipedia.org/wiki/Routing). Routing allows multiple networks to communicate independently and yet remain separate, whereas bridging connects two separate networks as if they were a single network. In the [OSI model](https://en.wikipedia.org/wiki/OSI_model), bridging is performed in the [data link layer](https://en.wikipedia.org/wiki/Data_link_layer)   If one or more segments of the bridged network are [wireless](https://en.wikipedia.org/wiki/Wireless_network), the device is known as a wireless bridge.

Transparent bridging uses a table called the [forwarding information base](https://en.wikipedia.org/wiki/Forwarding_information_base) to control the forwarding of frames between network segments. The table starts empty and entries are added as the bridge receives frames. If a destination address entry is not found in the table, the frame is flooded to all other ports of the bridge, flooding the frame to all segments except the one from which it was received. By means of these flooded frames, a [host](https://en.wikipedia.org/wiki/Host_(network)) on the destination network will respond and a forwarding database entry will be created. Both source and destination addresses are used in this process: source addresses are recorded in entries in the table, while destination addresses are looked up in the table and matched to the proper segment to send the frame to. [Digital Equipment Corporation](https://en.wikipedia.org/wiki/Digital_Equipment_Corporation) (DEC) originally developed the technology in the 1980s.



1. **B router:**

A bridge router or B router is a network device that works as a [bridge](https://en.wikipedia.org/wiki/Network_bridge) and as a [router](https://en.wikipedia.org/wiki/Router_(computing)). The b router routes packets for known [protocols](https://en.wikipedia.org/wiki/Communications_protocol) and simply forwards all other packets as a bridge would.

B routers operate at both the [network layer](https://en.wikipedia.org/wiki/Network_layer) for routable [protocols](https://en.wikipedia.org/wiki/Protocol_(computing)) and at the [data link layer](https://en.wikipedia.org/wiki/Data_link_layer) for non-routable protocols. As networks continue to become more complex, a mix of routable and non-routable protocols has led to the need for the combined features of bridges and routers. B routers handle both routable and non-routable features by acting as routers for routable protocols and bridges for non-routable protocols. Bridged protocols might propagate throughout the network, but techniques such as filtering and learning might be used to reduce potential congestion. B routers are used as connecting devices in the networking system, so it acts as a bridge in a network and as a router in an internetwork.

