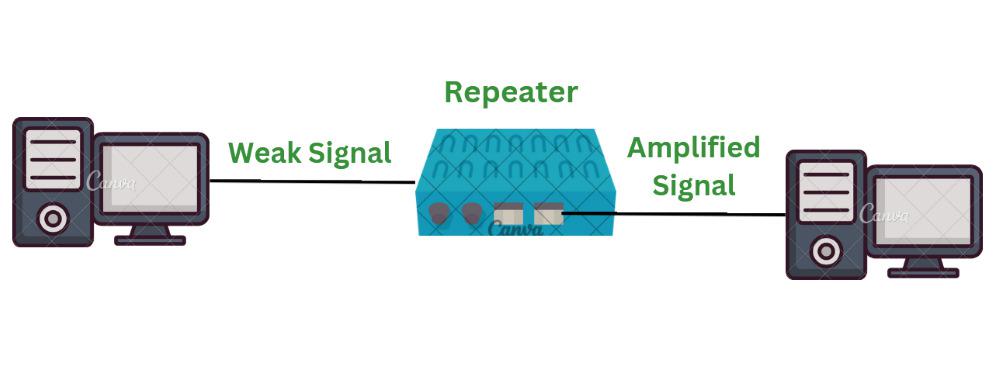
**Aim: Study of Different Network Devices in Details.**

**Network Devices:** Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example Repeater, Hub, Bridge, Switch, Routers, Gateway, Brouter, and NIC, etc.

1. **Repeater** – A repeater operates at the physical layer. Its job is to amplifies (i.e., regenerates) the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.



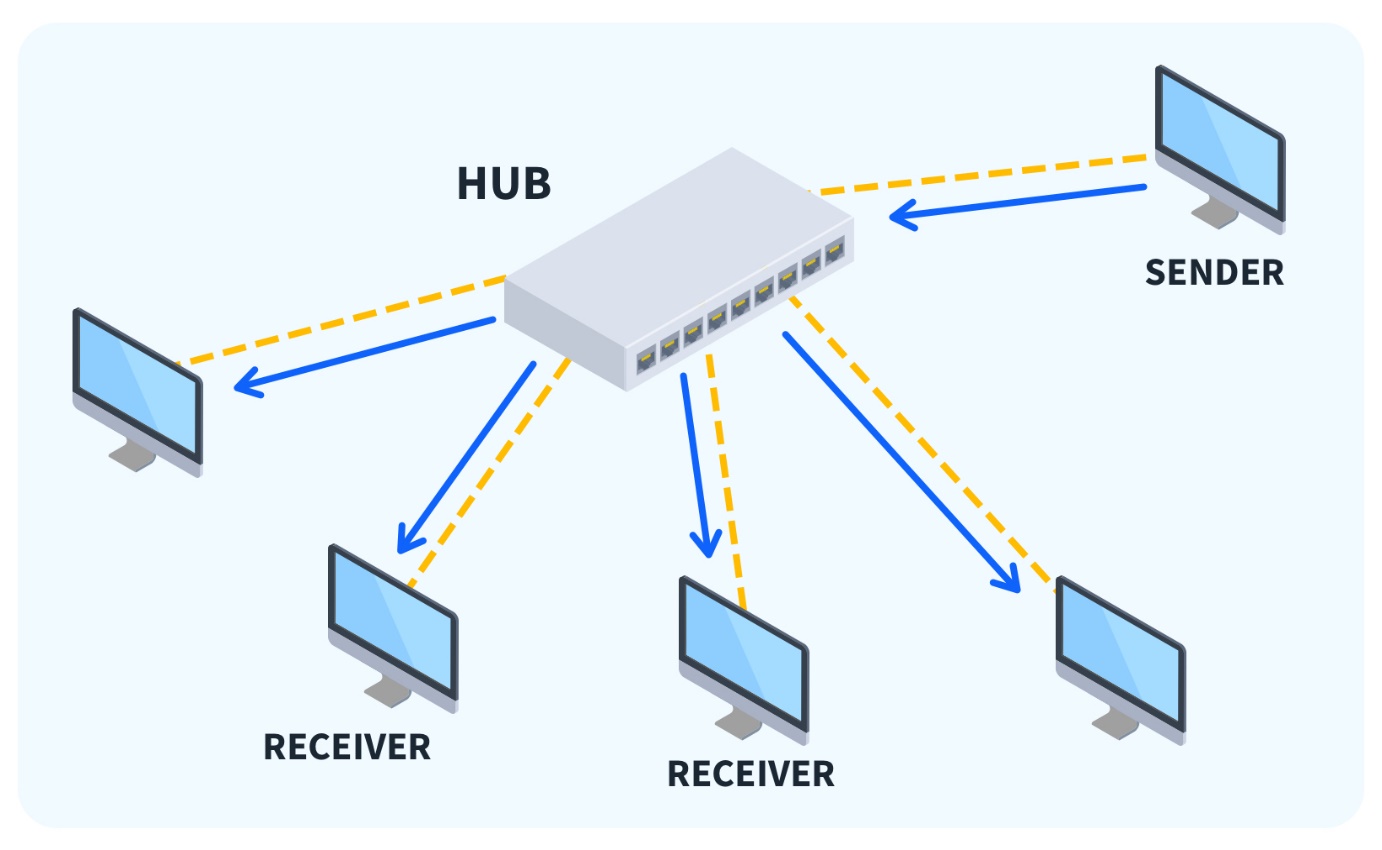
**Features of Repeaters**

* Repeater can regenerate the signal without modifying it.
* Repeaters can be used in [analog signals](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-analog-signals/) and [digital signals](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-digital-signals/).
* Repeaters can extend the range of networks.
* Dynamic networking is supported by repeater.
* Use of Repeaters reduces error and loss of data.
* Power is required for working of repeaters.
* Using repeater can add complexity in the network.

1. **Hub** – A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices.  In other words, the [collision domain](https://en.wikipedia.org/wiki/Collision_domain) of all hosts connected through Hub remains one.  Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

**Types of Hub**

* **Active Hub:-**These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.
* **Passive Hub:-**These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can’t be used to extend the distance between nodes.
* **Intelligent Hub:-**It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.



**Features of Hubs**

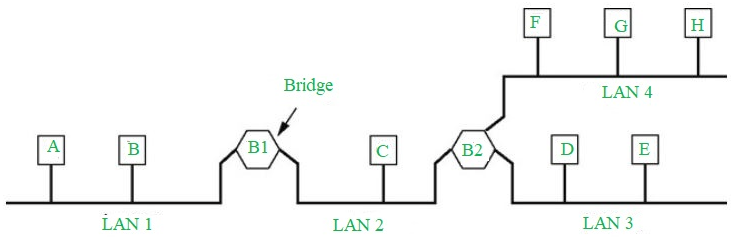
Hubs are the hardware device that operates in the physical layer of the OSI model.

* It supports[half-duplex transmission](https://www.geeksforgeeks.org/transmission-modes-computer-networks/)
* It works with shared bandwidth and broadcasting.
* The hub can provide a high data transmission rate to different devices.
* It can detect collisions in the network and send the jamming signal to each port.
* Hub does not support [Virtual LAN(VLAN)](https://www.geeksforgeeks.org/virtual-lan-vlan/) and spanning tree protocol.

**3. Bridge** – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

**Types of Bridges**

* **Transparent Bridges:-**These are the bridge in which the stations are completely unaware of the bridge’s existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
* **Source Routing Bridges:-**In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.



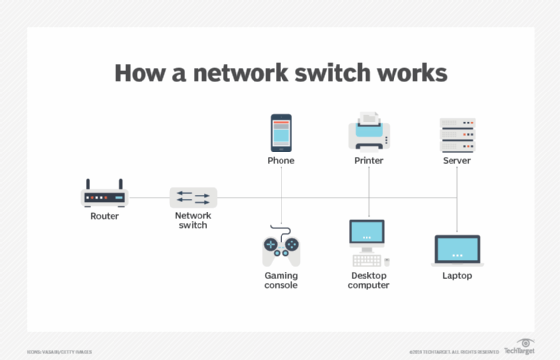
**Functions of Bridges in the Network**

* The bridge is used to divide LANs into multiple segments.
* To control the traffic in the network.
* It can interconnect two LANs with a similar protocols.
* It can filter the data based on destination/MAC address.

**4. Switch** – A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only.  In other words, the switch divides the collision domain of hosts, but the [broadcast domain](https://en.wikipedia.org/wiki/Broadcast_domain) remains the same.

#### **Types of  Switch**

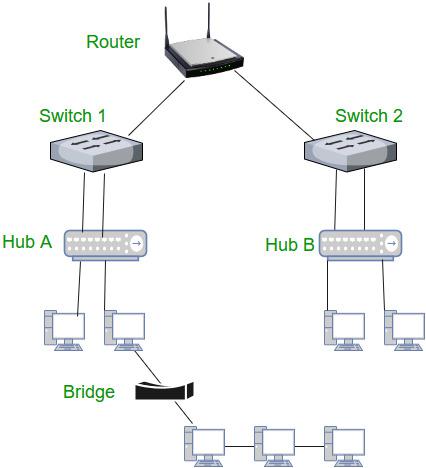
1. Unmanaged switches: These switches have a simple plug-and-play design and do not offer advanced configuration options. They are suitable for small networks or for use as an expansion to a larger network.
2. Managed switches: These switches offer advanced configuration options such as VLANs, QoS, and link aggregation. They are suitable for larger, more complex networks and allow for centralized management.
3. Smart switches: These switches have features similar to managed switches but are typically easier to set up and manage. They are suitable for small- to medium-sized networks.
4. Layer 2 switches: These switches operate at the Data Link layer of the OSI model and are responsible for forwarding data between devices on the same network segment.



**Features of Network Switches**

* It operates in Data Link Layer in [OSI Model](https://www.geeksforgeeks.org/layers-of-osi-model/).
* It performs error checking before forwarding data.
* It transfers the data only to the device that has been addressed.
* It operates in full duplex mode.
* It allocates each [LAN](https://www.geeksforgeeks.org/lan-full-form/) segment a limited bandwidth.
* It uses Unicast (one-to-one), multicast (one-to-many), and broadcast (one-to-all) transmission modes.
* Packet Switching techniques are used to transfer data packets from source to destination.

**5. Routers** – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.

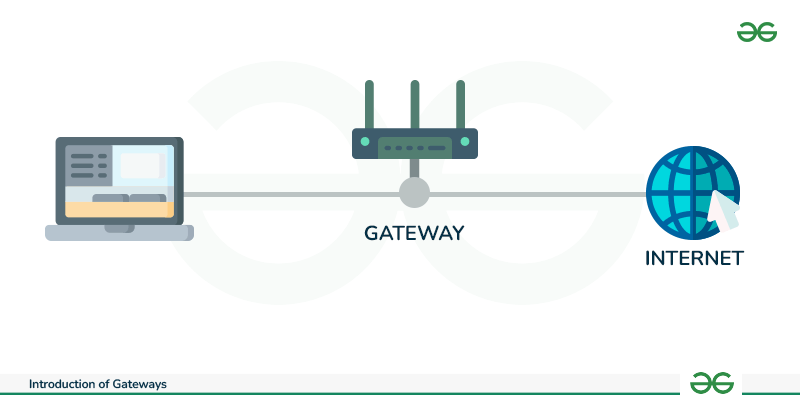


**Functions of Router**

The router performs below major functions:

1. **Forwarding:**The router receives the packets from its input ports, checks its header, performs some basic functions like checking [checksum](https://www.geeksforgeeks.org/error-detection-code-checksum/), and then looks up to the routing table to find the appropriate output port to dump the packets onto, and forwards the packets onto that output port.
2. **Routing:**Routing is the process by which the router ascertains what is the best path for the packet to reach the destination, It maintains a routing table that is made using different [algorithms](https://www.geeksforgeeks.org/introduction-to-algorithms/) by the router only.
3. **Network Address Translation (NAT):** Routers use [NAT](https://www.geeksforgeeks.org/network-address-translation-nat/) to translate between different IP address ranges. This allows devices on a private network to access the internet using a single public IP address.
4. **Security:**Routers can be configured with [firewalls](https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/) and other security features to protect the network from unauthorized access, [malware](https://www.geeksforgeeks.org/malware-and-its-types/), and other threats.

**6. Gateway** – A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. A gateway is also called a protocol converter.

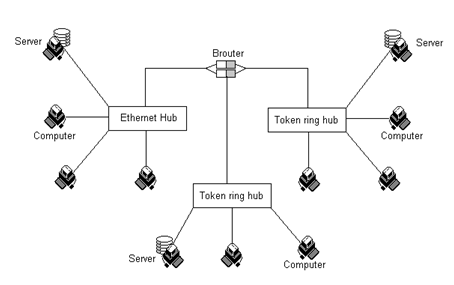


**Features of Gateways**

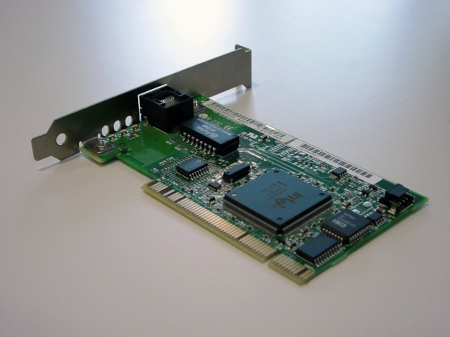
Gateways provide a wide variety of features. Some of these are:

* A gateway is situated at a network’s edge and manages all data that enters or exits the network.
* A gateway is distinct from other network devices in that it can operate at any layer of the [OSI model](https://www.geeksforgeeks.org/open-systems-interconnection-model-osi/).
* Gateways made the transmission more feasible as it queued up all the data and divided it into small packets of data rather than sending it bulk.
* Gateways provide security within the network.

**7. Brouter** – It is also known as the bridging router is a device that combines features of both bridge and router. It can work either at the data link layer or a network layer. Working as a router, it is capable of routing packets across networks and working as the bridge, it is capable of filtering local area network traffic.

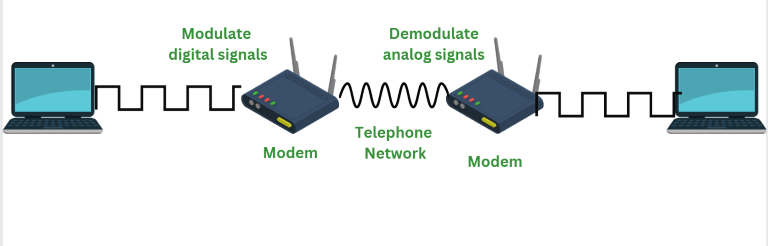


**8. NIC**– NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN.  It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC card is a layer 2 device which means that it works on both the physical and data link layers of the network model.



### **9. Access Point-** In terms of networking, an access point (AP) is a wireless network device that acts as a portal for devices to connect to a local area network. Access points can extend an existing network’s wireless coverage and increase the number of users who can connect. Wireless access points (WAPs) are devices that combine a transmitter and receiver (transceiver) to form a wireless LAN (WLAN). The access point **operates at the OSI model’s Data Link layer (Layer 2).**

**10**. **Modem**- [Modem](https://www.geeksforgeeks.org/how-to-install-a-modem/) stands for Modulator/Demodulator. The modem is defined as a [networking device](https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/) that is used to connect devices connected in the network to the[internet](https://www.geeksforgeeks.org/internet-and-its-services/). The main function of a modem is to convert the [analog signals](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-analog-signals/) that come from telephone wire into a digital form. In digital form, these converted signals are stored in the form of 0s and 1s. The modem can perform both the task of [modulation](https://www.geeksforgeeks.org/what-is-modulation/) and demodulation simultaneously. Modems are majorly used to transfer digital data in personal systems. The modem is also known as a signal translator as it translates one signal into another signal by modulating the [digital signal](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-digital-signals/)into an analog signal for transmission and then demodulates receiving analog signals into digital signals.



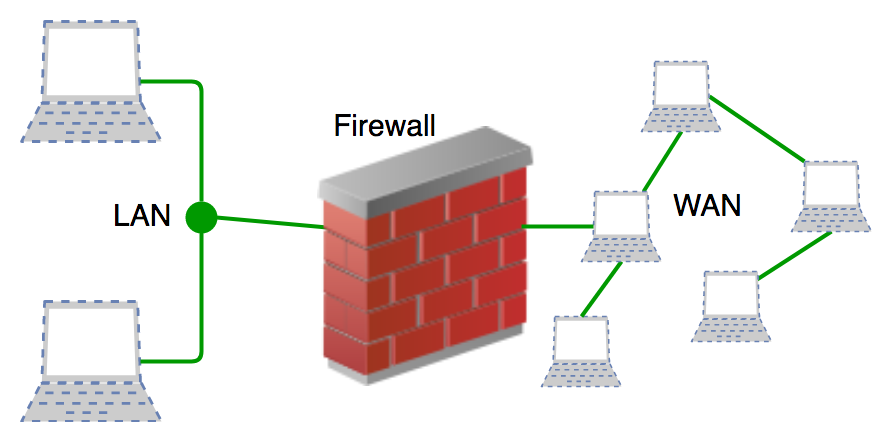
**Features of Modem**

* Modems can modulate as well as demodulate the signals simultaneously.
* Modem allows to connect only a specific number of devices to the internet.
* According to the features of modem, it’s price ranges.
* Modems can be upgraded with the help of a specific[software](https://www.geeksforgeeks.org/software-and-its-types/)patch.
* To use the devices over the internet with a modem devices need to be configured with an [Internet Service Provider(ISP)](https://www.geeksforgeeks.org/internet-service-provider-isp-hierarchy/).
* When the modem is connected to [Hub](https://www.geeksforgeeks.org/difference-between-hub-and-bridge/) it slows down its process.

**11.Firewalls**- A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules accepts, rejects, or drops that specific traffic.

* **Accept:** allow the traffic
* **Reject:** block the traffic but reply with an “unreachable error”
* **Drop:**block the traffic with no reply

A firewall is a type of network security device that filters incoming and outgoing network traffic with security policies that have previously been set up inside an organization. A firewall is essentially the wall that separates a private internal network from the open Internet at its very basic level.



**12. WiFi Extender- WiFi Extender**connects to Wired network through a wired connection may be Ethernet or coaxial cable to connect to the router. But nowadays newer WiFi Extenders don’t require these. It helps in extending the home/office network to cover more area. Once it is set up and connected then we can move it as per our requirement wherever we want a better WiFi signal. Mainly it boosts the range of existing WiFi and creates a stronger signal in the poor coverage areas. That’s why it is also called a WiFi Range Extender.