# Computer Networks

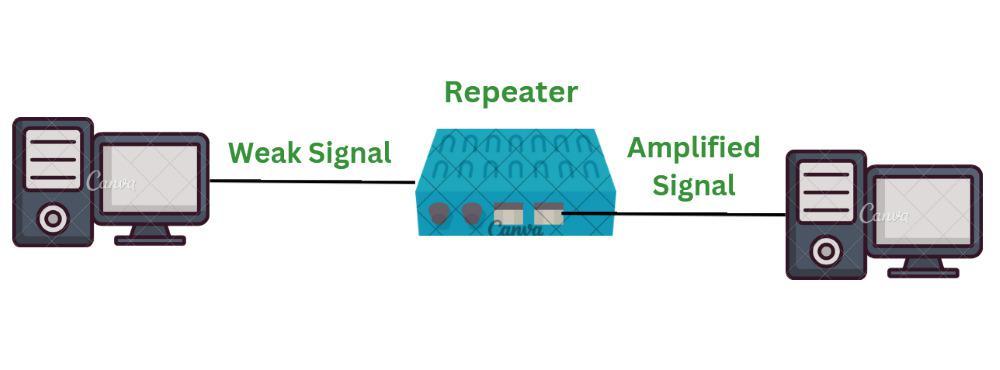
**Expt-1: Study of Networking Devices & Transmission Media**

# Networking Devices

Repeater

Source: https://www.geeksforgeeks.org/repeaters-in-computer-network/

Repeaters are defined as a networking device that is used to amplify and generate the incoming signal. Repeaters work at the physical layer of the OSI model. The main aim of using a repeater is to increase the networking distance by increasing the strength and quality of signals. The performance of Local Area Networks (LANs) and Wide Area Networks (WANs) repeaters are used. Using repeaters helps to reduce error, and loss of data and provides with delivery of data at specified locations only. The major advantage of using a repeater is that it provides with transfer of data with more security and over a long distance.



**Working of Repeaters**

* Initially the source system transmits the signals. This source systems can be a [mobile phone](https://www.geeksforgeeks.org/advanced-mobile-phone-system/), laptop or radio.
* This transmitted signal from the source system travels in air if it’s wireless network or through the cable if it is wired network. As the signal goes away from the source it’s strength gets weak.
* The signal received to the repeater is not the actual signal sent by source system but a weak signal. Therefore repeater amplifies this weak signal to get it strengthen.
* The strengthen signal is now being sent from the repeater to its destination. This signal is more stronger and can travel at longer distance. In short, it extends the network without losing the quality of signal.
* Repeaters are therefore used in various [wireless technologies](https://www.geeksforgeeks.org/wireless-mobile-computing-technologies/) such as [Wi-Fi](https://www.geeksforgeeks.org/what-is-wi-fiwireless-fidelity/)and wired technologies such as [ethernet](https://www.geeksforgeeks.org/what-is-ethernet/).

**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.

**Advantages of Repeater**

* **Better Performance of Network:**Repeaters provide with better performance of network because they do not always depend on processing overheads at the time.
* **Cost Effective:**Repeaters are more cost effective as compared to other network devices therefore they are cost effective.
* **Extends the network:** Repeaters provides with an advantage to extend the available network for transmission of data.
* **No Physical barriers:**Using physical devices can led to some barrier while transmission of signals. With the help of wireless repeaters such issues are resolved.
* **Enhanced Signals:** When computer devices and [routers](https://www.geeksforgeeks.org/introduction-of-a-router/)are connected in a network over long distance it weakens the strength of signals. While using repeaters it improves the strength of signals even over long distances.

**Disadvantages of Repeater**

* **Network Traffic:** Repeaters do not have features to segment the network traffic. Therefore repeaters do lack with the property to congestion.
* **Network Segmentation:**As repeaters do not have feature to segment the network traffic repeaters cannot create a separate traffic from one cable to another.
* **Limited number of repeaters:** Use of limited number of repeaters is supported by the network. If more number of repeaters are used that the specified one, it can even create collision of packets and increase the noise.
* **Collision Domain:** The information is passed from various domains repeater is not able to separate the devices.

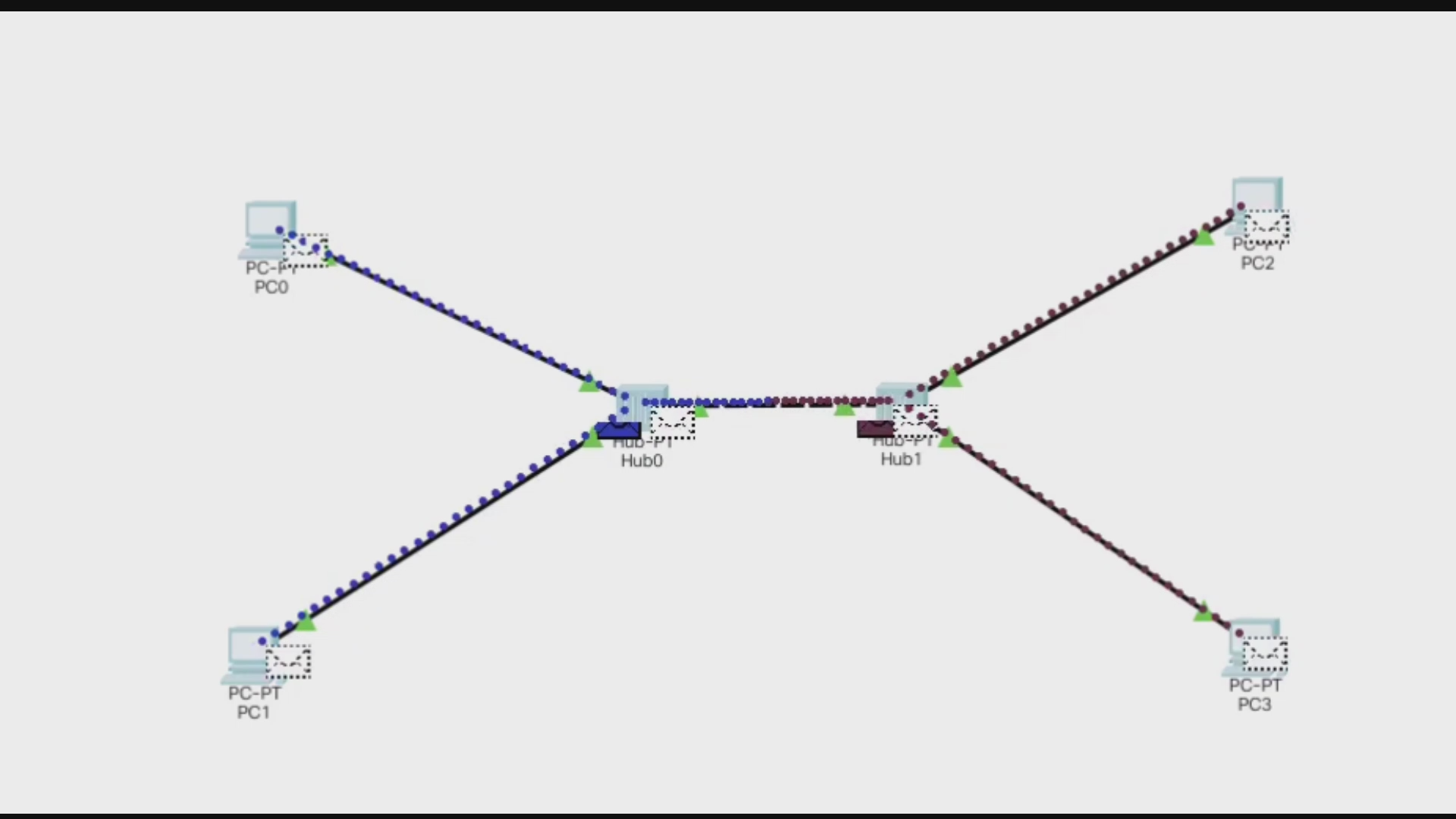
HUB

Source: https://www.geeksforgeeks.org/what-is-network-hub-and-how-it-works/

A hub is a 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 of all hosts connected through hub remains one. Hub does not have any routing table to store the data of ports and map destination addresses., the routing table is used to send/broadcast information across all the ports.

**How Does a Network Hub Work?**

A hub is a multiport device, which has multiple ports in a device and shares the data to multiple ports altogether. A hub acts as a dumb switch that does not know, which data needs to be forwarded where so it broadcasts or sends the data to each port.



Suppose there are five ports in a hub A, B, C, D, and E. Consider A wants to send any data frame, or let’s say A is acting as a sender, so the hub will forward the data transmitted by A to B, C, D, E. Now, at the same time B also wants to send the data then data received from A and B will collide and can cause data loss. In this situation, the data gets destroyed, and the hosts send a jam signal to all the hosts informing them about the collision, and each sender needs to wait for a certain amount of time.

**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.
* It is unable to filter the data and hence transmit or broadcast it to each port.
* It cannot find the best route/ shortest path to send any data, which makes it an inefficient device.

**Advantages of Network Hubs**

* It is less expensive.
* It does not impact network performance.
* Hub support different network media.

**Disadvantages of Network Hubs**

* It cannot find the best/ shortest path of the network.
* No mechanism for traffic detection.
* No mechanism for data filtration.
* Not capable of connecting to different network topologies like token ring, ethernet, etc.

Switch

Source: https://www.geeksforgeeks.org/what-is-a-network-switch-and-how-does-it-work/

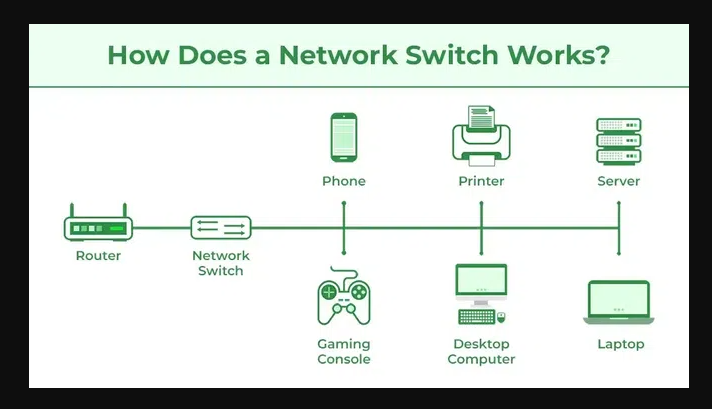
The Switch is a network device that is used to segment the networks into different subnetworks called subnets or LAN segments. It is responsible for filtering and forwarding the packets between LAN segments based on [MAC address](https://www.geeksforgeeks.org/introduction-of-mac-address-in-computer-network/).

Switches have many ports, and when data arrives at any port, the destination address is examined first and some checks are also done and then it is processed to the devices. Different types of communication are supported here like unicast, multicast, and broadcast communication.

**How Does a Network Switch Works?**

When the source wants to send the data packet to the destination, the packet first enters the switch and the switch reads its header and finds the MAC address of the destination to identify the device then it sends the packet out through the appropriate ports that lead to the destination devices.

Switch establishes a temporary connection between the source and destination for communication and terminates the connection once the conversation is done. Also, it offers full bandwidth to network traffic going to and from a device simultaneously to reduce collision.



**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.
* Switches have a more significant number of ports.

**Advantages of Switches**

* Prevents traffic overloading in a network by segmenting the network into smaller subnets.
* Increases the bandwidth of the network.
* Less frame collision as the switch creates the collision domain for each connection.

**Disadvantages of Switches**

* It can not stop traffic destined for a different LAN segment from traveling to all other LAN segments.
* Switches are more expensive.

Bridge

Source: https://www.geeksforgeeks.org/what-is-bridge-in-computer-network-types-uses-functions-differences/

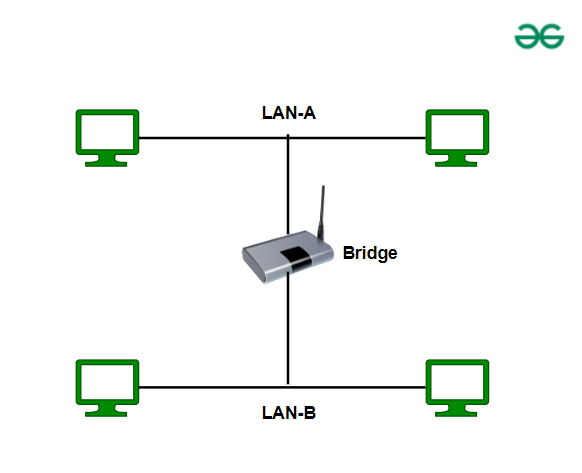
A bridge in a computer network is a device used to connect multiple LANs together with a larger Local Area Network (LAN). The mechanism of network aggregation is known as bridging. The bridge is a physical or hardware device but operates at the OSI model’s data link layer and is also known as a layer of two switches.

The primary responsibility of a switch is to examine the incoming traffic and determine whether to filter or forward it. Basically, a bridge in computer networks is used to divide network connections into sections, now each section has a separate [bandwidth](https://www.geeksforgeeks.org/what-is-bandwidth-definition-working-importance-uses/)and a separate collision domain. Here bridge is used to improve network performance.

**Working of Bridges**

Let’s see the step-by-step working of the bridge in computer networks:

* **Receiving Data:**The bridge gets data packets (or frames) from both network segments A and B.
* **Building a Table**: It creates a table of MAC addresses by looking at where the data is coming from to know which device is on which segment.
* **Filtering Data:** If the data from network A is meant for a device also on network A, the bridge stops it from going further.
* **Forwarding Data:** If the data from network A is meant for a device on network B, the bridge sends it to the correct place on network B.
* **Repeating for Both Sides:** The bridge does the same thing for data coming from network B.



**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.

**Advantages**

* Bridges can be used as a network extension like they can connect two network topologies together.
* It has a separate collision domain, which results in increased bandwidth.
* It can create a buffer when different[MAC protocols](https://www.geeksforgeeks.org/mac-protocol-used-in-wireless-sensor-networks/)are there for different segments.
* Highly reliable and maintainable. The network can be divided into multiple [LAN](https://www.geeksforgeeks.org/virtual-lan-vlan/) segments.
* Simple installation, no requirement of any extra hardware or software except the bridge itself.
* Protocol transparency is higher as compared to other protocols.

**Disadvantages**

* Expensive as compared to [hubs](https://www.geeksforgeeks.org/what-is-network-hub-and-how-it-works/)and [repeaters](https://www.geeksforgeeks.org/repeaters-in-computer-network/).
* Slow in speed.
* Poor performance as additional processing is required to view the MAC address of the device on the network.
* As the traffic received is in bulk or is broadcasted traffic, individual filtering of data is not possible.
* During the broadcasting of data, the network has high broadcast traffic and broadcast storms can be formed.

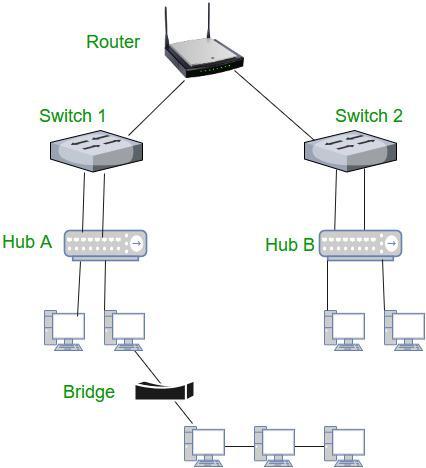
Router

Source: https://www.geeksforgeeks.org/introduction-of-a-router/

**What is a Router?**

A Router is a networking device that forwards data packets between computer networks. One or more [packet-switched networks](https://www.geeksforgeeks.org/packet-switched-network-psn-in-networking/) or subnetworks can be connected using a router. By sending data packets to their intended [IP addresses](https://www.geeksforgeeks.org/what-is-an-ip-address/), it manages traffic between different networks and permits several devices to share an [Internet connection](https://www.geeksforgeeks.org/types-of-internet-connection/).

Let us understand this by a very general example, suppose you search for *www.google.com* in your web browser then this will be a request that will be sent from your system to Google`s server to serve that webpage, now your request which is nothing but a stream of packets don`t just go to the google`s server straightaway they go through a series of networking devices known as a router which accepts this packets and forwards them to correct path and hence it reaches to the destination server. A router has several interfaces by which it can connect to several host systems. Routers are the devices that are operated on the Network Layer of the OSI Model, these are the most common devices used in networking.



**How Does Router Work?**

* A router determines a packet’s future path by examining the destination IP address of the header and comparing it to the routing [database](https://www.geeksforgeeks.org/what-is-database/). The list of [routing tables](https://www.geeksforgeeks.org/routing-tables-in-computer-network/) outlines how to send the data to a specific network location. They use a set of rules to determine the most effective way to transmit the[data](https://www.geeksforgeeks.org/what-is-data/) to the specified IP address.
* To enable communication between other devices and the internet, routers utilize a modem, such as a cable, fiber, or [DSL modem](https://www.geeksforgeeks.org/digital-subscriber-line-dsl/). Most routers include many ports that can connect a variety of devices to the [internet](https://www.geeksforgeeks.org/internet-and-its-services/) simultaneously. In order to decide where to deliver data and where traffic is coming from, it needs routing tables.
* A routing table primarily specifies the router’s default path. As a result, it might not determine the optimum path to forward the data for a particular packet. For instance, the office router directs all networks to its internet service provider through a single default channel.
* Static and dynamic tables come in two varieties in the router. The [dynamic routing](https://www.geeksforgeeks.org/what-is-dynamic-routing-in-computer-network/) tables are automatically updated by dynamic routers based on network activity, whereas the [static routing tables](https://www.geeksforgeeks.org/difference-between-static-and-dynamic-routing/) are configured manually.

**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.
5. **Quality of Service (QoS):**Routers can prioritize network traffic based on the type of data being transmitted. This ensures that critical applications and services receive adequate bandwidth and are not affected by lower-priority traffic.
6. **Virtual Private Network (VPN) connectivity:** Routers can be configured to allow remote users to connect securely to the network using a [VPN](https://www.geeksforgeeks.org/vpn-virtual-private-network/).
7. **Bandwidth management:** Routers can be used to manage network[bandwidth](https://www.geeksforgeeks.org/introduction-to-bandwidth/)by controlling the amount of data that is allowed to flow through the network. This can prevent network congestion and ensure that critical applications and services receive adequate bandwidth.
8. **Monitoring and diagnostics**: Routers can be configured to monitor network traffic and provide diagnostics information in the event of network failures or other issues. This allows network administrators to quickly identify and resolve problems.

**Advantages of Router**

* **Easier Connection:**Sharing a single network connection among numerous machines is the main advantage of router. This enables numerous people to connect to the internet, boosting total productivity. In addition, routers have connections between various media and network designs.
* **Security:**Undoubtedly, installing a router is the first step in securing a network connection. Because using a modem to connect directly to the internet exposes your computer to several security risks. So that the environment is somewhat secure, routers can be utilized as an intermediary between two networks. While not a [firewall or antivirus](https://www.geeksforgeeks.org/difference-between-firewall-and-antivirus/) replacement.
* **NAT Usage:**Routers use [Network Address Translation (NAT)](https://www.geeksforgeeks.org/network-address-translation-nat/) to map multiple private IP addresses into one [public IP address](https://www.geeksforgeeks.org/what-is-public-ip-address/). This allows for a better Internet connection and information flow between all devices connected to the network.
* **Supports Dynamic Routing:**The router employs dynamic routing strategies to aid in network communication. The internet work’s optimum path is chosen through [dynamic routing](https://www.geeksforgeeks.org/what-is-dynamic-routing-in-computer-network/). Additionally, it creates collision and broadcast domains. Overall, this can lessen network traffic.
* **Filtering of Packets:**Switching between packets and filtering packets are two more router services. A collection of filtering rules are used by routers to filter the network. The packets are either allowed or passed through.

**Disadvantages of Router**

* **Slower:**Routers analyze multiple layers of information, from the [physical layer](https://www.geeksforgeeks.org/physical-layer-in-osi-model/)to the [network layer](https://www.geeksforgeeks.org/network-layer-services-packetizing-routing-and-forwarding/), which slows down connections. The same issue can also be encountered when multiple devices are connected to these network devices, causing “connection waiting”.
* **High Cost:**They are more expensive than some other tools for systems administration. This includes security, extension, and the focal point. As a result, routers are typically not the greatest option for issues.
* **Need for configuration:**The router must be properly configured to work properly. In general, the more complex the intended use, the more configuration is required. This requires professional installation, which can add to the cost of buying a router.
* **Quality Issues:**The time transitions are not always accurate. Even yet, some modern devices use the 2.4GHz band, which is frequently deactivated. These kinds of separations are frequently possible for those who live in apartments and condominiums.
* **Bandwidth shortages:**[Dynamic routing](https://www.geeksforgeeks.org/what-is-dynamic-routing-in-computer-network/) techniques used by routers to support connections tend to cause network overhead, consuming a lot of bandwidth. This leads to a bandwidth shortage that significantly slows down the internet connection between connected devices.

Gateway

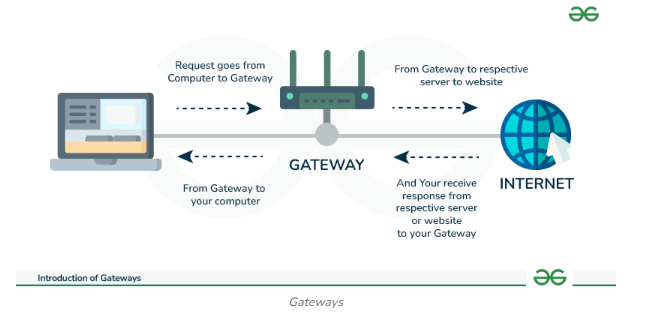
Source: https://www.geeksforgeeks.org/introduction-of-gateways/

**What are Gateways?**

A network gateway is a device that connects different networks by translating messages from one protocol into another protocol. The gateway monitors and controls all the incoming and outgoing [network traffic](https://www.geeksforgeeks.org/scraping-data-in-network-traffic-using-python/). Gateways are also known as protocol converters because they play an important role in converting protocols supported by traffic on different networks. As a result, it allows smooth communication between two networks.

**How Gateways Work?**

* The gateway receives data from devices within the network.
* After receiving data the gateway intercept and analyze data packets, which include analyzing packet header, payload etc.
* Based on the analysis of the data packets, the gateway calculate an appropriate destination address of [data packet](https://www.geeksforgeeks.org/what-is-packet-sniffing/). It then routes the data packets to their destination address.
* In some cases, the gateway might also want to transform the format of the obtained data to ensure compatibility at the receiver.
* Once the data packets have been analyzed, routed, and converted, then the gateway sends the last packets to their respective destinations address inside the network.



**Advantages of Gateways**

* Gateway helps in connecting two different network.
* Gateway is used to filters and does not allow anything that can harm to the network.
* Gateway is worked as the protocol converter.
* Gateway is the highly secure device that provides security from external attacks.

**Limitations of Gateways**

There are few limitations of gateways as well. Here are some of them:

* Gateway causes time delay since the conversion of data according to the network requires time.
* Failure of the gateway might lead to the failure of connection with other networks.
* The implementation of Gateway is very complex and it is not cost efficient.
* Gateway is hard to manage

# Transmission Media

Source: https://www.geeksforgeeks.org/types-transmission-media/

Guided Media

[Guided Media](https://www.geeksforgeeks.org/wired-communication-media/) is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.   
Features:

* High Speed
* Secure
* Used for comparatively shorter distances

There are 3 major types of Guided Media:

1. **Twisted Pair Cable**

It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. [Twisted Pair](https://www.geeksforgeeks.org/twisted-pair-cable/) is of two types:

* **Unshielded Twisted Pair (UTP):** UTP consists of two insulated copper wires twisted around one another. This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.



*Unshielded Twisted Pair*

**Advantages of Unshielded Twisted Pair**

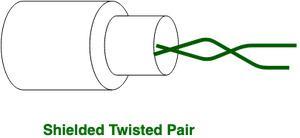
Least expensive

* Easy to install
* High-speed capacity

**Disadvantages of Unshielded Twisted Pair**

Susceptible to external interference

* Lower capacity and performance in comparison to STP
* Short distance transmission due to attenuation



*Shielded Twisted Pair*

**Shielded Twisted Pair (STP):** This type of cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.

**Advantages of Shielded Twisted Pair**

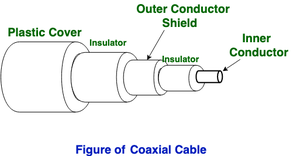
* Better performance at a higher data rate in comparison to UTP
* Eliminates crosstalk
* Comparatively faster

**Disadvantages of Shielded Twisted Pair**

* Comparatively difficult to install and manufacture
* More expensive
* Bulky

1. **Coaxial Cable**

It has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover. The [coaxial cable](https://www.geeksforgeeks.org/what-is-coaxial-cable/) transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.



**Advantages of Coaxial Cable**

Coaxial cables support high[bandwidth](https://www.geeksforgeeks.org/what-is-bandwidth-definition-working-importance-uses/).

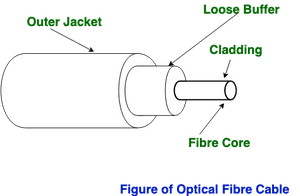
* It is easy to install coaxial cables.
* Coaxial cables have better cut-through resistance so they are more reliable and durable.
* Less affected by noise or cross-talk or electromagnetic inference.
* Coaxial cables support multiple channels

**Disadvantages of Coaxial Cable**

* Coaxial cables are expensive.
* The coaxial cable must be grounded in order to prevent any crosstalk.
* As a Coaxial cable has multiple layers it is very bulky.
* There is a chance of breaking the coaxial cable and attaching a “t-joint” by hackers, this compromises the security of the data.

1. **Optical Fiber Cable**

[Optical Fibre Cable](https://www.geeksforgeeks.org/optical-fibre-cable/) uses the concept of refraction of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for the transmission of large volumes of data. The cable can be unidirectional or bidirectional. The [WDM (Wavelength Division Multiplexer)](https://www.geeksforgeeks.org/difference-between-wdm-and-dwdm/)supports two modes, namely unidirectional and bidirectional mode.



**Advantages of Optical Fibre Cable**

* Increased capacity and bandwidth
* Lightweight
* Less signal attenuation
* Immunity to electromagnetic interference
* Resistance to corrosive materials

**Disadvantages of Optical Fibre Cable**

* Difficult to install and maintain
* High cost
* Fragile

Unguided Media

It is also referred to as Wireless or [Unbounded transmission media](https://www.geeksforgeeks.org/unguided-media/). No physical medium is required for the transmission of electromagnetic signals.

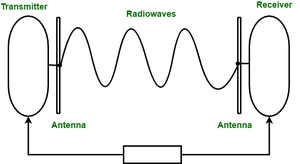
**Features of Unguided Media**

* The signal is broadcasted through air
* Less Secure
* Used for larger distances

There are 3 types of Signals transmitted through unguided media:

**Radio Waves**

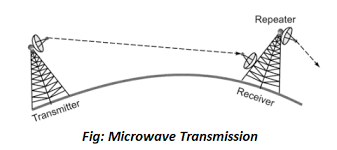
[Radio waves](https://www.geeksforgeeks.org/radio-waves/) are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radio waves for transmission.



Further Categorized as Terrestrial and Satellite.

**Microwaves**

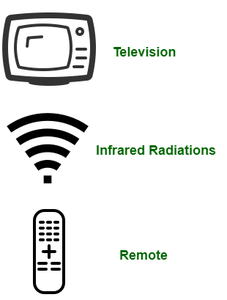
It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz.[**Micro waves**](https://www.geeksforgeeks.org/applications-of-microwaves/) are majorly used for mobile phone communication and television distribution.



*Microwave Transmission*

**Infrared**

[Infrared waves](https://www.geeksforgeeks.org/infrared-light-for-transmission/) are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.



**Difference between Radio Waves Vs Micro Waves Vs Infrared Waves**

| **Basis** | **Radiowave** | **Microwave** | **Infrared wave** |
| --- | --- | --- | --- |
| Direction | These are omni-directional in nature. | These are unidirectional in nature. | These are unidirectional in nature. |
| Penetration | At low frequency, they can penetrate through solid objects and walls but high frequency they bounce off the obstacle. | At low frequency, they can penetrate through solid objects and walls. at high frequency, they cannot penetrate. | They cannot penetrate through any solid object and walls. |
| Frequency range | Frequency range: 3 KHz to 1GHz. | Frequency range: 1 GHz to 300 GHz. | Frequency range: 300 GHz to 400 GHz. |
| Security | These offers poor security. | These offers medium security. | These offers high security. |
| Attenuation | Attenuation is high. | Attenuation is variable. | Attenuation is low. |
| Government License | Some frequencies in the radio-waves require government license to use these. | Some frequencies in the microwaves require government license to use these. | There is no need of government license to use these waves. |
| Usage Cost | Setup and usage Cost is moderate. | Setup and usage Cost is high. | Usage Cost is very less. |
| Communication | These are used in long distance communication. | These are used in long distance communication. | These are not used in long distance communication. |