**Computer Network:**

Computer network refers to the interconneted computing devices which can exchange the data & share resources with each other .

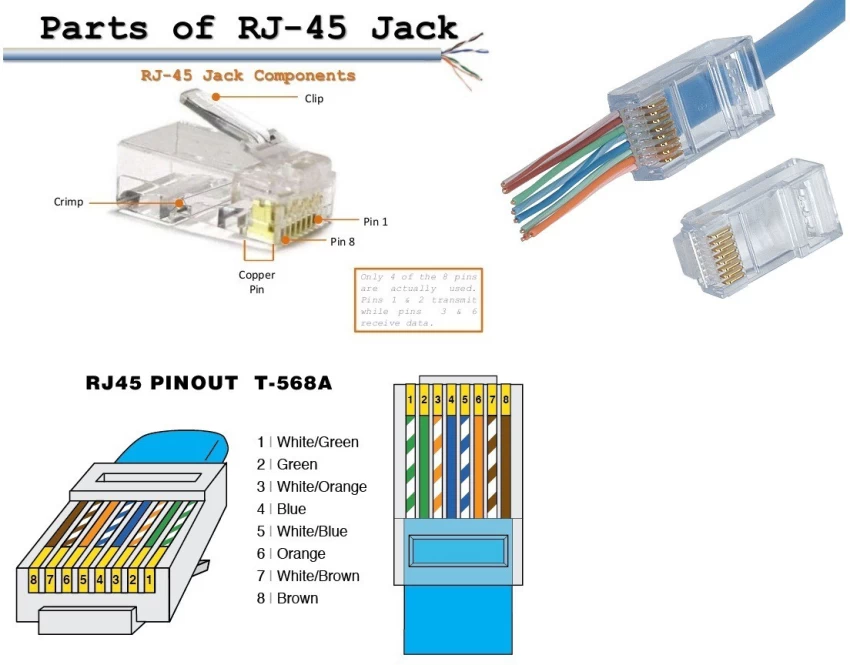
**LAN Card:**

A LAN Card is the network interface card that is used by the device to communicate with the network.



**RJ 45 Connector:**

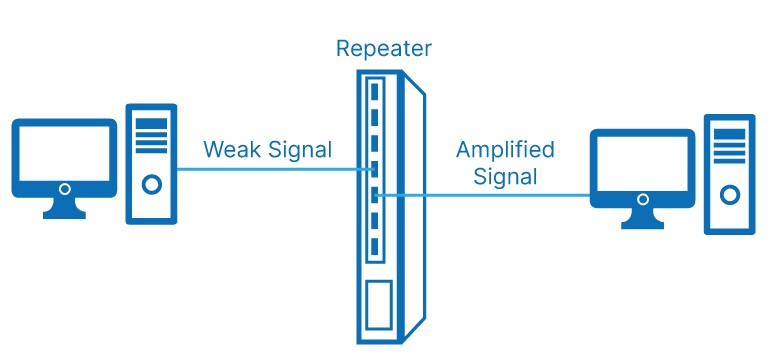
The eight-pin RJ45 connector is a standardized interface which often connects a computer to a Local Area Network (LAN).



**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.



**2. 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.

**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:**

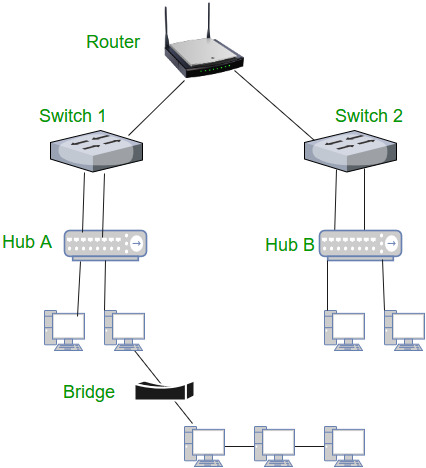
* **Transparent Bridges:-** These are the bridge in which the stations are completely unaware of the bridge’s existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and 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.

**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.
5. **Layer 3 switches:** These switches operate at the Network layer of the OSI model and can route data between different network segments. They are more advanced than Layer 2 switches and are often used in larger, more complex networks.
6. **PoE switches:** These switches have Power over Ethernet capabilities, which allows them to supply power to network devices over the same cable that carries data.
7. **Gigabit switches:** These switches support Gigabit Ethernet speeds, which are faster than traditional Ethernet speeds.
8. **Rack-mounted switches:** These switches are designed to be mounted in a server rack and are suitable for use in data centers or other large networks.
9. **Desktop switches:** These switches are designed for use on a desktop or in a small office environment and are typically smaller in size than rack-mounted switches.
10. **Modular switches:** These switches have modular design, which allows for easy expansion or customization. They are suitable for large networks and data centers.

**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.



**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.

**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.

## **Crimping:**

Crimping is a way of joining pieces of metal or other ductile material by deforming one or both of the pieces to hold the other, and this deformity is known as the "crimp". A crimping tool is the tool used to deform the material and create the connection.



## What types of crimping tool are there?

There are many different types of crimping tools, all with different uses.

Here are the main types:

### Bootlace crimping tool

Designed to crimp bootlace ferrules/crimps, which are metal tubes attached to a colour-coded insulation collar.

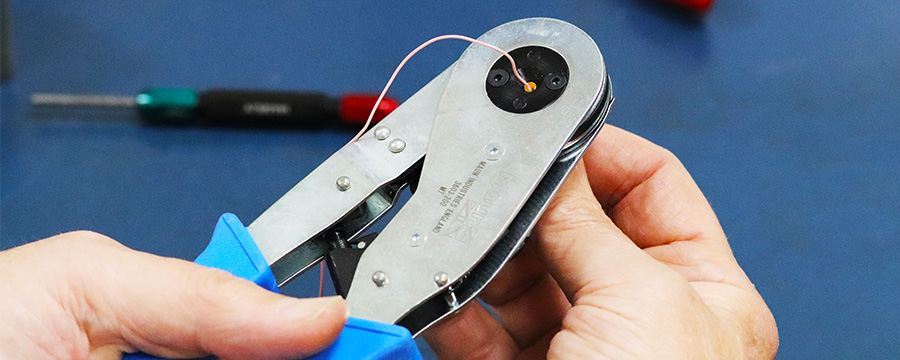
They're often used in screw terminals to stop multiple core wires from splitting and can handle a range of popular wire sizes.

Choose a high leverage one, such as the [Maun Bootlace Ferrule Crimper](https://www.maunindustries.com/bootlace-ferrule-crimper-0-5-mm2-to-16-mm2/), to get a good crimp without tiring out your hand. You can also choose the [plier version](https://www.maunindustries.com/bootlace-ferrule-crimping-plier-0-5-mm2-to-16-mm2/) to crimp a wider range of sizes.

### Thin cable precision crimping tool

When you're working with thin cables, you don't have much margin for error, which is why traditional hand crimping tools can create problems.

The solution to this is to use a crimping tool with a ratchet feature, [such as this one](https://www.maunindustries.com/crimping-tool-8-indent-26-to-16-awg/), that helps to control the crimp to remove human error from the process, ensuring a good crimp every time, even with smaller cables.



### Crimping tool for QM & IP68 connectors

These tools are designed to crimp QM connectors and IP68 connectors, which are ideal for mains control lead connections, as well as small transmission systems.

[This tool](https://www.maunindustries.com/multipole-crimping-tool-for-qm-connectors-220-mm/) can handle QM connectors up to 24 AWG wire size and IP68 connectors up to 28 AWG wire size, making it a versatile choice.



### Crimping tool for splice connectors

If you're looking to crimp splices, either gel-filled or butt splice connectors, then you need a proper tool for it, as opposed to a generic crimping tool.

This [Scotchlok™ Crimping Plier](https://www.maunindustries.com/scotchlok-8a-8b-crimping-plier-150-mm/) handles both Scotchlok™ 8A and 8B splice connectors, and has a return spring to make it easier to handle.



### Crimping tool for coaxial cable

Coaxial cable is a type of transmission line used to carry high-frequency signals, such as broadband internet, and has an inner conductor cable surrounded by a conducting shield, making it difficult to crimp.

Crimping tools for this type of cable tend to come in different categories depending on the coaxial cable impedance (calculated in Ohms Ω), so make sure to get one that matches your cable type.

Here are some suggestions:

* For 75 Ω connectors, choose [this tool](https://www.maunindustries.com/crimping-tool-bnc-tnc-uhf-75-connectors/).
* For 50 Ω connectors, choose [this tool](https://www.maunindustries.com/crimping-tool-bnc-tnc-uhf-50-connectors/).



**Cat 5 cable:**

A cat 5—or category 5 (5e, or 6)—is an Ethernet cable, or cabling used to support computer networks. It can transmit video and telephony signals in addition to standard computer data. The cat 5 is usually the bare minimum required for Hosted VoIP.



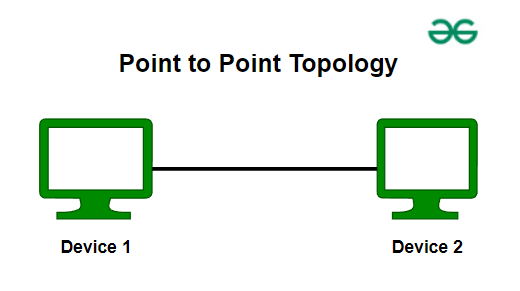
## Types of Network Topology

The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as **Network Topology**. The various network topologies are:

* [Point to Point Topology](https://www.geeksforgeeks.org/differences-between-point-to-point-and-multi-point-communication/)
* [Mesh Topology](https://www.geeksforgeeks.org/advantage-and-disadvantage-of-mesh-topology/)
* [Star Topology](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-star-topology/)
* [Bus Topology](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-bus-topology/)
* [Ring Topology](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-ring-topology/)
* [Tree Topology](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-tree-topology/)
* [Hybrid Topology](https://www.geeksforgeeks.org/what-is-hybrid-topology/)

## Point to Point Topology

Point-to-point topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point-to-Point provides high bandwidth.



Point to Point Topology

## Mesh Topology

In a mesh topology, every device is connected to another device via a particular channel. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), [DHCP](https://www.geeksforgeeks.org/dynamic-host-configuration-protocol-dhcp/) (Dynamic Host Configuration Protocol), etc.



Mesh Topology

**Figure 1**: Every device is connected to another via dedicated channels. These channels are known as links.

* Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure 1, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. The total number of ports required = N \* (N-1).
* Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is NC2 i.e. N(N-1)/2. In Figure 1, there are 5 devices connected to each other, hence the total number of links required is 5\*4/2 = 10.

**Advantages of Mesh Topology**

* Communication is very fast between the nodes.
* Mesh Topology is robust.
* The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
* Provides security and privacy.

**Disadvantages of Mesh Topology**

* Installation and configuration are difficult.
* The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
* The cost of maintenance is high.

A common example of mesh topology is the internet backbone, where various internet service providers are connected to each other via dedicated channels. This topology is also used in military communication systems and aircraft navigation systems.

For more, refer to the [Advantages and Disadvantages of Mesh Topology](https://www.geeksforgeeks.org/advantage-and-disadvantage-of-mesh-topology).

## Star Topology

In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them. Coaxial cables or RJ-45 cables are used to connect the computers. In Star Topology, many popular [Ethernet](https://www.geeksforgeeks.org/what-is-ethernet/) LAN protocols are used as CD(Collision Detection), [CSMA](https://www.geeksforgeeks.org/carrier-sense-multiple-access-csma/) (Carrier Sense Multiple Access), etc.



Star Topology

**Figure 2**: A star topology having four systems connected to a single point of connection i.e. hub.

**Advantages of Star Topology**

* If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
* Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.
* It is Robust. If one link fails only that link will affect and not other than that.
* Easy to fault identification and fault isolation.
* Star topology is cost-effective as it uses inexpensive coaxial cable.

**Disadvantages of Star Topology**

* If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
* The cost of installation is high.
* Performance is based on the single concentrator i.e. hub.

A common example of star topology is a local area network (LAN) in an office where all computers are connected to a central hub. This topology is also used in wireless networks where all devices are connected to a wireless access point.

For more, refer to the [Advantages and Disadvantages of Star Topology.](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-star-topology)

## Bus Topology

Bus Topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes. In Bus Topology, various [MAC](https://www.geeksforgeeks.org/mac-address-in-computer-network/) (Media Access Control) protocols are followed by LAN ethernet connections like [TDMA](https://www.geeksforgeeks.org/difference-between-fdma-tdma-and-cdma/), [Pure Aloha](https://www.geeksforgeeks.org/what-is-pure-aloha/), CDMA, [Slotted Aloha](https://www.geeksforgeeks.org/what-is-slotted-aloha/), etc.



Bus Topology

**Figure 3**: A bus topology with shared backbone cable. The nodes are connected to the channel via drop lines.

**Advantages of Bus Topology**

* If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, known as backbone cable, and N drop lines are required.
* Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.
* The cost of the cable is less compared to other topologies, but it is used to build small networks.
* Bus topology is familiar technology as installation and troubleshooting techniques are well known.
* [CSMA](https://www.geeksforgeeks.org/carrier-sense-multiple-access-csma) is the most common method for this type of topology.

**Disadvantages of  Bus Topology**

* A bus topology is quite simpler, but still, it requires a lot of cabling.
* If the common cable fails, then the whole system will crash down.
* If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.
* Adding new devices to the network would slow down networks.
* Security is very low.

A common example of bus topology is the Ethernet LAN, where all devices are connected to a single coaxial cable or twisted pair cable. This topology is also used in cable television networks. For more, refer to the [Advantages and Disadvantages of Bus Topology](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-bus-topology).

## Ring Topology

In a Ring Topology, it forms a ring connecting devices with exactly two neighboring devices. A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The data flows in one direction, i.e. it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.



Ring Topology

**Figure 4**: A ring topology comprises 4 stations connected with each forming a ring.

The most common access method of ring topology is token passing.

* **Token passing:** It is a network access method in which a token is passed from one node to another node.
* **Token:** It is a frame that circulates around the network.

**Operations of Ring Topology**

1. One station is known as a **monitor** station which takes all the responsibility for performing the operations.
2. To transmit the data, the station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
3. When no station is transmitting the data, then the token will circulate in the ring.
4. There are two types of token release techniques: **Early token release** releases the token just after transmitting the data and **Delayed token release** releases the token after the acknowledgment is received from the receiver.

**Advantages of Ring Topology**

* The data transmission is high-speed.
* The possibility of collision is minimum in this type of topology.
* Cheap to install and expand.
* It is less costly than a star topology.

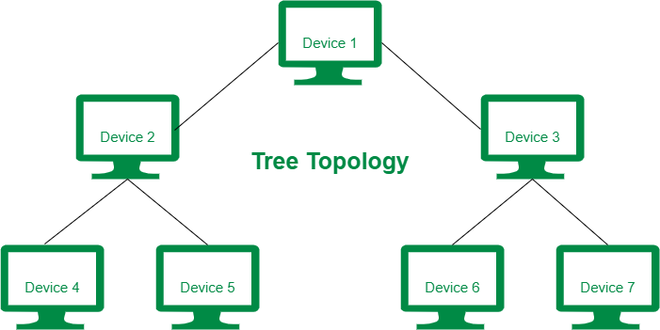
**Disadvantages of Ring Topology**

* The failure of a single node in the network can cause the entire network to fail.
* Troubleshooting is difficult in this topology.
* The addition of stations in between or the removal of stations can disturb the whole topology.
* Less secure.

For more, refer to the [Advantages and Disadvantages of Ring Topology](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-ring-topology).

## **Tree Topology**

This topology is the variation of the Star topology. This topology has a hierarchical flow of data. In Tree Topology, protocols like DHCP and [SAC](https://www.geeksforgeeks.org/student-activity-council-sac-interview-experience/) (Standard Automatic Configuration ) are used.



Tree Topology

**Figure 5**: In this, the various secondary hubs are connected to the central hub which contains the repeater. This data flow from top to bottom i.e. from the central hub to the secondary and then to the devices or from bottom to top i.e. devices to the secondary hub and then to the central hub. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

**Advantages of Tree Topology**

* It allows more devices to be attached to a single central hub thus it decreases the distance that is traveled by the signal to come to the devices.
* It allows the network to get isolated and also prioritize from different computers.
* We can add **new devices to the existing network.**
* **Error detection** and **error correction** are very easy in a tree topology.

**Disadvantages of Tree Topology**

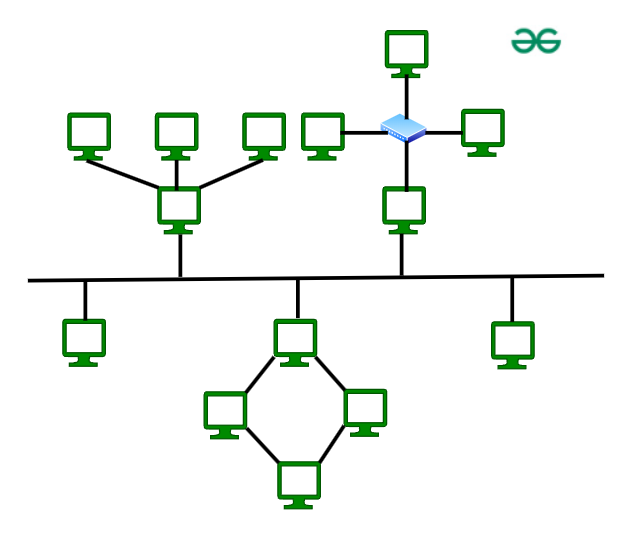
* If the central hub gets fails the entire system fails.
* The cost is high because of the cabling.
* If new devices are added, it becomes difficult to reconfigure.

A common example of a tree topology is the hierarchy in a large organization. At the top of the tree is the CEO, who is connected to the different departments or divisions (child nodes) of the company. Each department has its own hierarchy, with managers overseeing different teams (grandchild nodes). The team members (leaf nodes) are at the bottom of the hierarchy, connected to their respective managers and departments.

For more, refer to the [Advantages and Disadvantages of Tree Topology](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-tree-topology).

## Hybrid Topology

This topological technology is the combination of all the various types of topologies we have studied above. Hybrid Topology is used when the nodes are free to take any form. It means these can be individuals such as Ring or Star topology or can be a combination of various types of topologies seen above. Each individual topology uses the protocol that has been discussed earlier.



**Hybrid Topology**

The above figure shows the structure of the Hybrid topology. As seen it contains a combination of all different types of networks.

**Advantages of Hybrid Topology**

* This topology is **very flexible**.
* The size of the network can be easily expanded by **adding new devices.**

**Disadvantages of Hybrid Topology**

* It is challenging **to design the architecture** of the Hybrid Network.
* **Hubs** used in this topology are **very expensive.**
* The infrastructure cost is very high as a hybrid network **requires a lot of cabling and network devices**.

A common example of a hybrid topology is a university campus network. The network may have a backbone of a star topology, with each building connected to the backbone through a switch or router. Within each building, there may be a bus or ring topology connecting the different rooms and offices. The wireless access points also create a mesh topology for wireless devices. This hybrid topology allows for efficient communication between different buildings while providing flexibility and redundancy within each building.

For more, refer to the [Advantages and Disadvantages of Hybrid Topology](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-hybrid-topology).