**MINOR PROJECT REPORT**

**ON**

**SIMPLE NETWORKING TOPOLOGIES**



**BACHELOR OF ENGINEERING**

**In**

**Computer Science and Engineering**

**SUBMITTED BY**

**Group no.- (G8)**

ARYAN SHARMA (2020a1r194)

ABHAY SOLAN (2020a1l006)

ARYAN SHARMA (2020a1r183)

**Model Institute of Engineering and Technology**

**Kot Bhalwal, Jammu - 181122**

**www.mietjammu.in**

**Contents**

|  |  |
| --- | --- |
| S.NO. | TOPICS |
| 1. | Tech stack |
| 2. | What is Network topologies? |
| 3. | Types of Network Topologies |
| 4. | Bus topology |
| 5. | Star Topology |
| 6. | Ring Topology |
| 7. | Mesh Topology |
| 8. | Hubs |
| 9. | Switches |
| 10. | End Devices |
| 11. | Demonstration |
| 12. | References |

## **TECH STACK**

1. Cisco Packet Tracer



## **Cisco packet tracer**

**Cisco Packet Tracer** as the name suggests, is a tool built by Cisco. This tool provides a network simulation to practice simple and complex networks.

The main purpose of Cisco Packet Tracer is to help students learn the principles of networking with hands-on experience as well as develop Cisco technology specific skills. Since the protocols are implemented in software only method, this tool cannot replace the hardware Routers or Switches. Interestingly, this tool does not only include Cisco products but also many more networking devices.

Using this tool is widely encouraged as it is part of the curriculum like CCNA, CCENT where Faculties use Packet Trace to demonstrate technical concepts and networking systems. Students complete assignments using this tool, working on their own or in teams.

Engineers prefer to test any protocols on Cisco Packet Tracer before implementing them. Also, Engineers who would like to deploy any change in the production network prefer to use Cisco Packet Tracer to first test the required changes and proceed to deploy if and only if everything is working as expected.

This makes the job easier for Engineers allowing them to add or remove simulated network devices, with a Command line interface and a drag and drop user interface.

**Workspace :**

1. **Logical –**  
   Logical workspace shows the logical network topology of the network the user has built. It represents the placing, connecting and clustering virtual network devices.
2. **Physical –**  
   Physical workspace shows the graphical physical dimension of the logical network. It depicts the scale and placement in how network devices such as routers, switches and hosts would look in a real environment. It also provides geographical representation of networks, including multiple buildings, cities and wiring closets.

**Key Features:**

* Unlimited devices
* E-learning
* Customize single/multi user activities
* Interactive Environment
* Visualizing Networks
* Real-time mode and Simulation mode
* Self-paced

**What is network topology?**

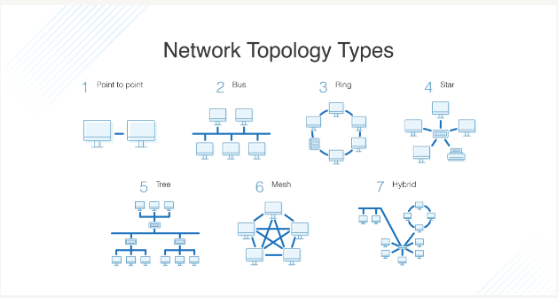
## What is network topologies?

A network topology is the physical and logical arrangement of nodes and connections in a network. Nodes usually include devices such as switches, routers and software with switch and router features. Network topologies are often represented as a graph.

Network topologies describe the arrangement of networks and the relative location of traffic flows. Administrators can use network topology diagrams to determine the best placements for each [node](https://www.techtarget.com/searchnetworking/definition/node) and the optimal path for traffic flow. With a well-defined and planned-out network topology, an organization can more easily locate faults and fix issues, improving its data transfer efficiency.

Network geometry can be defined as the physical topology and the logical topology. Network topology diagrams are shown with devices depicted as network nodes and the connections between them as lines. The type of network topology differs depending on how the network needs to be arranged.

.

.

## **Types of Network Topologies**

## *Bus Topology*

Bus topologies have the simplest layout. In a bus topology, there is a main cable (also known as the bus) that connects to each of the network’s devices. Network users utilize the main cable to relay data information from one end of the bus to the other.

Because only one cable is responsible for transmitting messages, all of the network’s devices may hear a sent message, but only the intended receiver accepts it. This topology can get noisy, so it’s best for smaller network setups with fewer devices.

## *Star Topology*

In star topology, you use a central hub or switch as a sort of middleman for data transmission. Each network device enlists the central hub when requesting or providing communication.

Star topologies are easy to troubleshoot and scale and have the advantage of one failed node not impacting the others. The centralized device must always remain in quality condition for this topology to work effectively.

## *Ring Topology*

Ring topology gets its name from the ring shape that’s formed as a result of each device connecting to two other devices in the network. Devices in this type of topology send messages in a unified direction.

One downside to this topology type is that if one device fails, the rest of the network suffers, too. On the flipside, this makes troubleshooting easier, as IT can quickly locate which node stopped the message from completing its circular cycle.

## *Mesh Topology*

The two different types of mesh topology are full mesh and partial mesh.

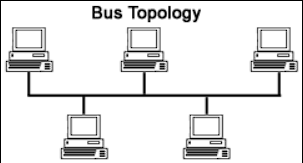
With full mesh, every device is connected to every other device within the network. In partial mesh topologies, some computer systems aren’t hooked up to every other device.

Various connections within mesh topology allow direct, uninterrupted, and secure communication between nodes. However, this topology type does require the most cabling and can get quite complex the larger you scale it.

## **Bus Topology**

Bus topology is a specific kind of network topology in which all of the various devices in the network are connected to a single cable or line. In general, the term refers to how various devices are set up in a network.

One way to think about a bus topology is that the line connected to all of the devices or nodes in the network is like an aisle along which a signal travels in order to find the node to which it is to be delivered. Typically, the cable in the bus topology has two end terminals that dampen the signal so that it does not keep moving from one end of the network to the other. Different types of bus topology can be referred to as linear or distributed bus topology. A linear bus topology implies that there is just one line associated with two distinct endpoints. In a distributed bus topology, there may be more than one linear pattern connected to the network. Bus topologies are often valued for their simplicity and lower cost of implementation. However, one drawback is that if the central line is compromised, the entire network will go down. Also, it can be difficult to troubleshoot these kinds of systems, and problems like data signal loss can occur with a longer linear cable.



## **Star Topology**

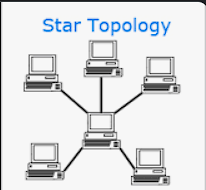
Star topology is a [network topology](https://www.techopedia.com/definition/5538/network-topology) in which each network component is physically connected to a central node such as a router, hub or switch.

In a star topology, the central hub acts like a server and the connecting nodes act like clients. When the central node receives a [packet](https://www.techopedia.com/definition/5380/packet) from a connecting node, it can pass the packet on to other nodes in the network. A star topology is also known as a star network.

Star networks require a [point-to-point connection](https://computernetworktopology.com/point-to-point-topology/) between the central node and connecting devices. To improve communication between the devices on the network, the central node can provide signal reconditioning and amplification services.

Star topologies are often used in home networks. The benefits of a star network topology include the following:

* Limits the impact of a single point of failure. In star networks, each connecting node is isolated from other connecting nodes. If one connecting node goes down, it will not impact the performance of other connecting nodes in the network.
* Facilitates adding or removing individual components to and from a network. Star networks are usually kept small because network performance can suffer when too many devices compete for access to the central node.



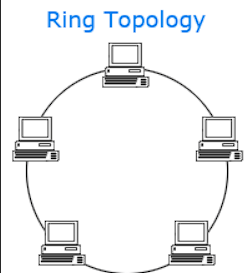
## **Ring Topology**

A **ring topology** is a [network](https://www.computerhope.com/jargon/n/network.htm) configuration where device connections create a circular [data](https://www.computerhope.com/jargon/d/data.htm) path. Each networked device is connected to two others, like points on a circle. Together, devices in a ring topology are referred to as a **ring network**.

In a ring network, [packets](https://www.computerhope.com/jargon/p/packet.htm) of data travel from one device to the next until they reach their destination. Most ring topologies allow packets to travel only in one direction, called a **unidirectional** ring network. Others permit data to move in either direction, called **bidirectional**.

The major disadvantage of a ring topology is that if any individual connection in the ring is broken, the entire network is affected.

Ring topologies may be used in either [LANs](https://www.computerhope.com/jargon/l/lan.htm) (local area networks) or [WANs](https://www.computerhope.com/jargon/w/wan.htm) (wide area networks). Depending on the [network card](https://www.computerhope.com/jargon/n/nic.htm) used in each computer of the ring topology, a [coaxial cable](https://www.computerhope.com/jargon/c/coaxialc.htm) or an [RJ-45](https://www.computerhope.com/jargon/r/rj45.htm) network cable is used to connect computers together.



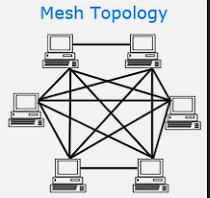
## **Mesh Topology**

Mesh topology is a type of networking in which all the computers are inter-connected to each other. In Mesh Topology, the connections between devices take place randomly. The connected nodes can be computers, switches, hubs, or any other devices. In this topology setup, even if one of the connections goes down, it allows other nodes to be distributed. This type of topology is very expensive and does not have any hierarchy, interdependency, and uniform pattern between nodes. The connections of the mesh topology are not easier to establish.

All computers, in a mesh topology, not only responsible for sending their own signals but also relays for other nodes. Usually, it is used for wireless networks, and its connections can be wired or wireless. Also, there is a point-to-point connection between all nodes in the mesh topology setup. The below picture is an instance of a mesh topology network.

The full mesh and partially-connected mesh are two forms of the mesh topology, which are discussed below:

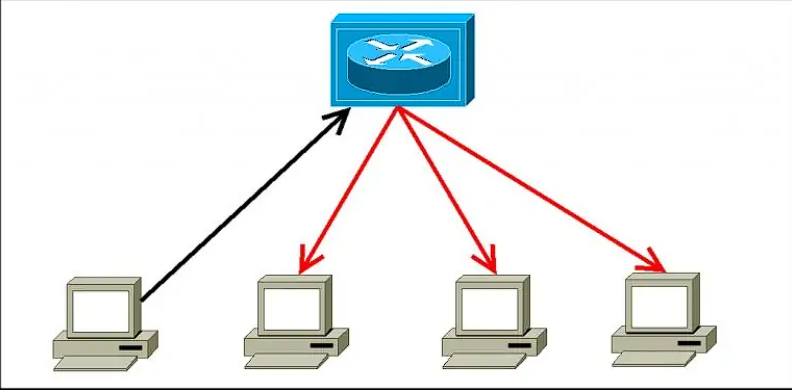
1. **Full Mesh Topology:** In a full mesh topology, all the devices are connected with all other devices. Full Mesh is a network where every node will have an n-1 number of connections if there are n number of nodes available in the network. A full mesh topology is usually reserved for network backbones, which offers a great deal of redundancy. However, it can be excessively costly to implement. Although it can be expensive to implement, it provides a benefit that if one of the nodes goes down, the traffic load of the network is redistributed to other nodes.
2. **Partial Mesh Topology:** Only a few nodes, in the partial mesh topology, are attached with all the other nodes. It means that in this network, it is not necessary to connect all the devices are attached with other. As compared to full mesh topology, it is less costly, and it provides basic redundancy to control the failure of any nodes. The partial mesh topology is used in peripheral networks through which they work with a full-mesh backbone in tandem.



## **Hubs**

A **hub** serves as a central point to which all of the hosts in a network connect to. It is an OSI Layer 1 device and has no concept of Ethernet frames or addressing – it simply receives the signal from one port and sends it out to all other ports.

hubs have no way of distinguishing out which port a signal should be sent to; instead, an electrical signal is sent out each port. All nodes on the network will receive data, and the data will eventually reach the correct destination, but with a lot of unnecessary network traffic:



In the example above you can see that the hub has sent out the receiving signal out all other ports, except the incoming port. Hubs are therefore considered obsolete and switches are commonly used instead in modern LANs. Hubs have numerous disadvantages over switches, such as:

* they are not aware of the traffic that passes through them
* they create only one large collision domain
* a hub typically operates in half duplex
* there is also a security issue with hubs since the traffic is forwarded to all ports (except the source port), which makes it possible to capture all traffic on a network with a network sniffer!

## **Switches**

A switch is a hardware component in network infrastructure that performs the switching process. The switch connects network devices, such as computers and servers, to one another.

A switch enables multiple devices to share a network while preventing each device's traffic from interfering with other devices' traffic. The switch acts as a traffic cop at a busy intersection. When a data packet arrives at one of its ports, the switch determines which direction the packet is headed. It then forwards the packet through the correct port for its destination.

Some data packets might come to the switch from devices, like computers or voice-over-IP (VoIP) phones, that are attached directly to it. Other data packets might come to the switch from indirectly connected devices, through a network element such as a hub or router.

The switch knows which of the network's devices are connected to it, and it can transfer data packets between those devices directly. In other cases, data packets may be going to more-distant destinations, on other networks. A switch in such a scenario forwards the packets to a router, which then forwards them to their destinations on the network. 

Before there were switches, there were network hubs. Hubs enable many devices to plug into a network through a single shared port on a router. The disadvantage of hubs is that when a hub receives a packet, it sends copies of the packet to every other device connected to it. This can cause problems with traffic congestion and data security.

Switches solve this problem by keeping tables of the MAC addresses of all devices sending packets to them and forwarding packets only to their destinations, instead of flooding all connected devices with the packets.

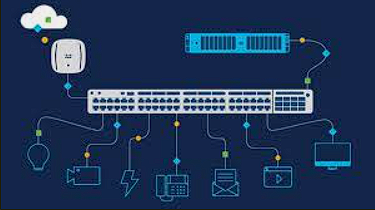
A switch connects devices within a LAN (local-area network) by using MAC addresses to identify where to send data packets. A router connects LANs to other area networks or to the internet. A router uses IP addresses to route data packets.

Switches are still at the core of network infrastructure, but today's advanced switches can do much more than just connect devices in a network or IT environment. Most important, advanced switches can act as both switches and routers.

Modern [Ethernet switches](https://www.cisco.com/c/en/us/products/switches/what-is-an-ethernet-switch.html) incorporate features and functions that eliminate the need for some types of additional hardware. For example, switches now include security capabilities that were once handled by dedicated firewalls.

Also, multigigabit switches can provide variable speeds to match the throughput needs of wireless access points, which provide Wi-Fi access to devices such as laptops and mobile phones. And advancements in Power over Ethernet (PoE) switches can supply devices over copper Ethernet cable with up to 90 watts of power per switch port.

Some switches now incorporate machine learning, so they can act as network sensors, collecting data about the network to help network engineers make informed decisions. Modern switches are also programmable and can include [network monitoring](https://www.cisco.com/c/en/us/solutions/automation/what-is-network-monitoring.html) applications and [network analytics](https://www.cisco.com/c/en/us/solutions/analytics/what-is-network-analytics.html) tools.



## **End Devices**

**The network devices that people are most familiar with** are called end devices, or hosts. These devices form the interface between users and the underlying communication network. A host device is either the source or destination of a message transmitted over the network.

End devices are the **non-networking devices that connect to the network, such as IP phones, personal computers, wireless access points, printers, and IP cameras**. The Ethernet interfaces that connect to end devices are referred to as access interfaces.

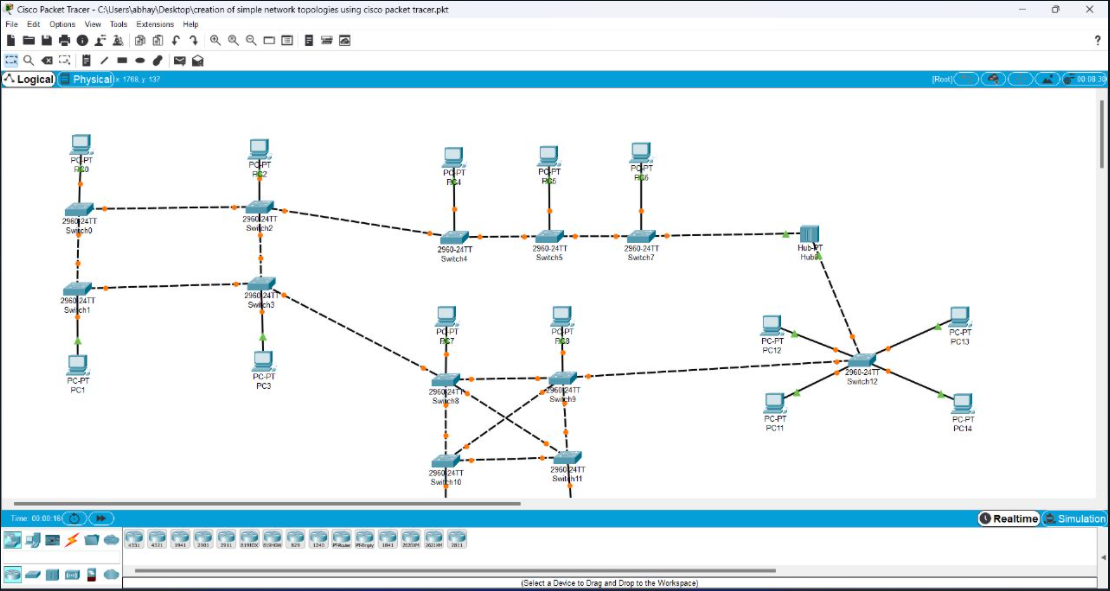
**A source or destination device in a networked system**. For example, a user's PC is an end device, and so is a server. Network switches, routers and other equipment work in between to enable messages to travel from one end device to the other.

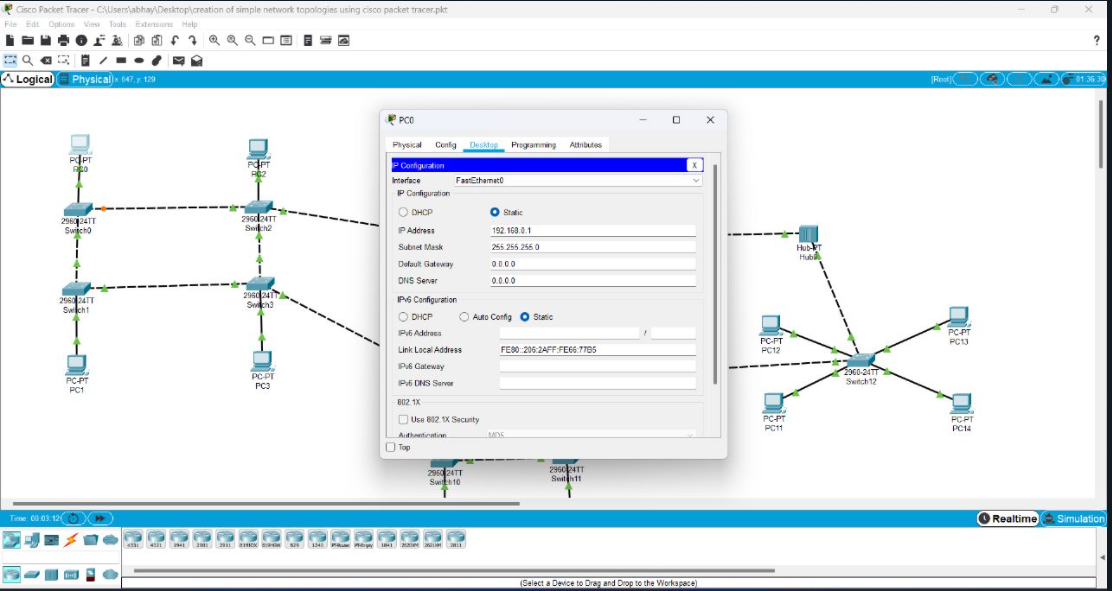
Some examples of end devices are: Computers, laptops, file servers, web servers. Network printers.

End-user device: **Any desktop or laptop computer, any tablet, smart phone, or other mobile device** is an end-user device. “End-user device” does not include removable storage like USB flash drives.



## **Demonstration**





**REFERENCES**

* [**https://www.cablewholesale.com/blog/index.php/2021/08/29/the-4-different-types-of-computer-network-topologies/**](https://www.cablewholesale.com/blog/index.php/2021/08/29/the-4-different-types-of-computer-network-topologies/)
* [**https://www.heavy.ai/technical-glossary/network-topology**](https://www.heavy.ai/technical-glossary/network-topology)
* [**https://www.geeksforgeeks.org/computer-network-tutorials/**](https://www.geeksforgeeks.org/computer-network-tutorials/)