CN EXPERIMENT 1

AIM: To study different networking devices

**What are network devices?**

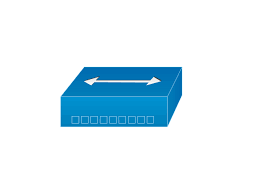
Hardware devices that are used to connect computers, printers, fax machines and other electronic devices to a network are called network devices. These devices transfer data in a fast, secure and correct way over same or different networks. Network devices may be inter-network or intra-network. Some devices are installed on the device, like NIC card or RJ45 connector, whereas some are part of the network, like router, switch, etc. Let us explore some of these devices in greater detail.

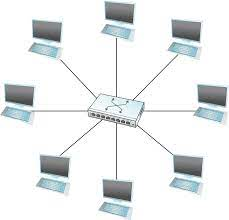
**Types of network devices:**

**Here is a list of commonly used network devices.**

* **Hub**
* **Switch**
* **Router**
* **Bridge**
* **Gateway**
* **Modem**
* **Repeater**
* **Access Point**

# HUB:





Hubs connect multiple computer networking devices together. A hub also acts as a repeater in that it amplifies signals that deteriorate after traveling long distances over connecting cables. A hub is the simplest in the family of network connecting devices because it connects LAN components with identical protocols.

A hub can be used with both digital and analog data, provided its settings have been configured to prepare for the formatting of the incoming data.

Hubs operate at the Physical layer of the [Open Systems Interconnection (OSI) model](https://www.netwrix.com/network_security_best_practices.html).

**Types of Hub**

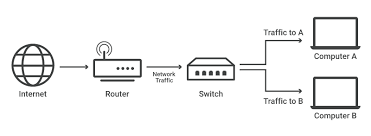
* **Active Hub:-** These are the hubs which have their own power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as wiring centre. These are used to extend the maximum distance between nodes.
* **Passive Hub :-** These are the hubs which collect wiring from nodes and power supply from 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 work like active hubs and include 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.

APPLICATIONS:

* Hubs are used to create small Home Networks.
* Hubs are used for monitoring the networks.
* Hubs are used in Organizations and Computer Labs for connectivity.
* It Makes one device or peripheral available throughout the whole network.

# SWITCH:

# 



switches generally have a more intelligent role than hubs. A switch is a multiport device that improves network efficiency. The switch maintains limited routing information about nodes in the internal network, and it allows connections to systems like hubs or routers. Strands of LANs are usually connected using switches. Generally, switches can read the hardware addresses of incoming packets to transmit them to the appropriate destination.

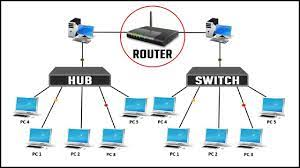
A switch generally can work on the Data Link layer but a multilayer switch is one that can operate at Data Link layer or the Network layer of the OSI model, which means that it can operate as both a switch and a router.

APPLICATIONS

* Switch increases the bandwidth of the network.
* To reduce the workload on individual PCs as it sends the information to only that device which has been addressed.
* To increase the overall performance of the network by reducing the traffic on the network.
* To reduce frame collision as switch creates the collision domain for each connection.

# ROUTER:



A router is a network layer hardware device that transmits data from one LAN to another if both networks support the same set of protocols. So a router is typically connected to at least two LANs and the internet service provider (ISP). It receives its data in the form of packets, which are data frames with their destination address added. Router also strengthens the signals before transmitting them. That is why it is also called repeater.

### Types of Routers

**Ⅰ. Edge Routers**

This type of router is placed at the edge of the ISP network, that is normally configured to external protocol like BGP (Border gateway protocol) to another BGP of other ISP or large organization.

**Ⅱ. Subscriber Edge Routers**

This type of router belongs to an end user (enterprise) organization. It’s configured to broadcast external BGP to its provider’s AS(s)

**Ⅲ. Inter-provider Border Routers**

This type of router is for Interconnecting ISPs. This is a BGP speaking router that maintains BGP sessions with other BGP speaking routers in other providers' ASes.

**Ⅳ. Core Routers**

A router that resides within the middle or backbone of the LAN network rather than at its periphery. In some instances, a core router provides a stepdown backbone, interconnecting the distribution routers from multiple building of a campus (LAN), or Large Enterprise Location (WAN). They tend to be optimized for a high bandwidth.

**Ⅴ. Wired and Wireless Routers**

Home and small office networking is becoming popular by day by the use of IP wired and wireless router. Wired and wireless router are able to maintain routing and configuration information in their routing table. They also provide the service of filtering traffic of incoming and outgoing packets based on IP addresses.

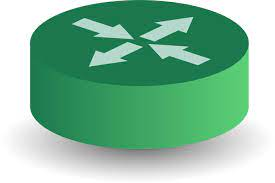
Some wireless routers can be combined the functions of router with those of a network switch and that of a firewall in one.

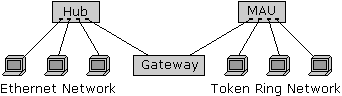
## Applications of Routers

There are various areas where a router is used:

* Routers are used to connect hardware equipment with remote location networks like **BSC, MGW, IN, SGSN**, and other servers.
* It provides support for a fast rate of data transmission because it uses high STM links for connectivity; that's why it is used in both wired or wireless communication.
* Internet service providers widely use routers to send the data from source to destination in the form of e-mail, a web page, image, voice, or a video file. Furthermore, it can send data all over the world with the help of an IP address of the destination.
* Routers offer access restrictions. It can be configured in a way that allows for few users to access the overall data and allows others to access the few data only, which is defined for them.
* Routers are also used by software testers for WAN communications. For example, the software manager of an organization is located in Agra, and its executive is located at a different place like Pune or Bangalore. Then the router provides the executive the method to share his software tools and other applications with the manager with the help of routers by connecting their PCs to the router using WAN architecture.
* In wireless networks, by configuring VPN in routers, it can be used in the client-server model, which allows sharing the internet, video, data, voice, and hardware resources.

# GATEWAY:





Gateways normally work at the Transport and Session layers of the OSI model. At the Transport layer and above, there are numerous protocols and standards from different vendors; gateways are used to deal with them. Gateways provide translation between networking technologies such as Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP). Because of this, gateways connect two or more autonomous networks, each with its own routing algorithms, protocols, topology, domain name service, and network administration procedures and policies.

Gateways perform all of the functions of routers and more. In fact, a router with added translation functionality is a gateway.

### **Types of gateways**

Gateways can take several forms and perform a variety of tasks. Examples of this include:

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

APPLICATIONS of Gateway:

**1.** The gateways work as the software sometimes performs as the hardware and sometimes it can be both. The voice and data communication are the techniques which are being used as the data types.

**2.** It provides complete security to a local network and also connects a local network to a public network gateway.

**3.** The gateways are also an important aspect or we can utter that is the important technique for any of the telephony signaling process.

**4.** It provides a way of communication between the telephone network and the internet.

**5.** It implements the significant interface between the wide-area and local protocols such as TCP/IP on the major intranet/internet.

# REPEATER:



A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

## **Types of Repeaters**

According to the types of signals that they regenerate, repeaters can be classified into two categories −

* **Analog Repeaters** − They can only amplify the analog signal.
* **Digital Repeaters** − They can reconstruct a distorted signal.

According to the types of networks that they connect, repeaters can be categorized into two types −

* **Wired Repeaters** − They are used in wired LANs.
* **Wireless Repeaters** − They are used in wireless LANs and cellular networks.

According to the domain of LANs they connect, repeaters can be divided into two categories −

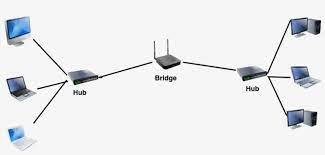
* **Local Repeaters** − They connect LAN segments separated by small distance.
* **Remote Repeaters** − They connect LANs that are far from each other.

APPLICATION of repeater

* To retransmit the data and strengthen the weak signals as the Signals get weaker as it travels to the longer distances.

# BRIDGE:

# 



A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of 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.

Bridges have mostly fallen out of favor in recent years and have been replaced by switches, which offer more functionality. In fact, switches are sometimes referred to as “multiport bridges” because of how they operate.

**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 source station and the frame specifies which route to follow. The host can discover frame by sending a special frame called discovery frame, which spreads through the entire network using all possible paths to destination.

APPLICATIONS OF BRIDGE:

* Bridges connects two or more different LANs that has a similar protocol and provides communication between the devices (nodes) in them.
* By joining multiple LANs, bridges help in multiplying the network capacity of a single LAN.
* Since they operate at data link layer, they transmit data as data frames. On receiving a data frame, the bridge consults a database to decide whether to pass, transmit or discard the frame.
  + If the frame has a destination MAC (media access control) address in the same network, the bridge passes the frame to that node and then discards it.
  + If the frame has a destination MAC address in a connected network, it will forward the frame toward it.
* By deciding whether to forward or discard a frame, it prevents a single faulty node from bringing down the entire network.
* In cases where the destination MAC address is not available, bridges can broadcast data frames to each node. To discover new segments, they maintain the MAC address table.
* In order to provide full functional support, bridges ideally need to be transparent. No major hardware, software or architectural changes should be required for their installation.
* Bridges can switch any kind of packets, be it IP packets or AppleTalk packets, from the network layer above. This is because bridges do not examine the payload field of the data frame that arrives, but simply looks at the MAC address for switching.
* Bridges also connect virtual LANs (VLANs) to make a larger VLAN.
* A wireless bridge is used to connect wireless networks or networks having a wireless segment.

# CONCLUSION:

EXP 2

AIM: To study different network topologies

## 

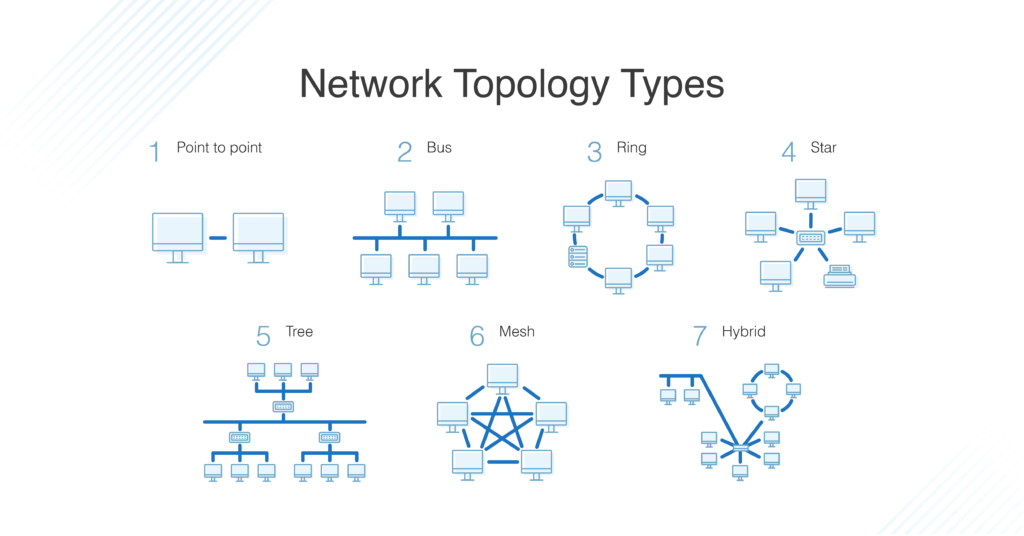
## What is Network Topology?

Network topology refers to the manner in which the links and nodes of a network are arranged to relate to each other. Topologies are categorized as either physical network topology, which is the physical signal transmission medium, or logical network topology, which refers to the manner in which data travels through the network between devices, independent of physical connection of the devices. Logical network topology examples include twisted pair Ethernet, which is categorized as a logical bus topology, and token ring, which is categorized as a logical ring topology.

Physical network topology examples include star, mesh, tree, ring, point-to-point, circular, hybrid, and bus topology networks, each consisting of different configurations of nodes and links. The ideal network topology depends on each business’s size, scale, goals, and budget. A network topology diagram helps visualize the communicating devices, which are modeled as nodes, and the connections between the devices, which are modeled as links between the nodes.

# TYPES OF NETWORK TOPOLOGIES

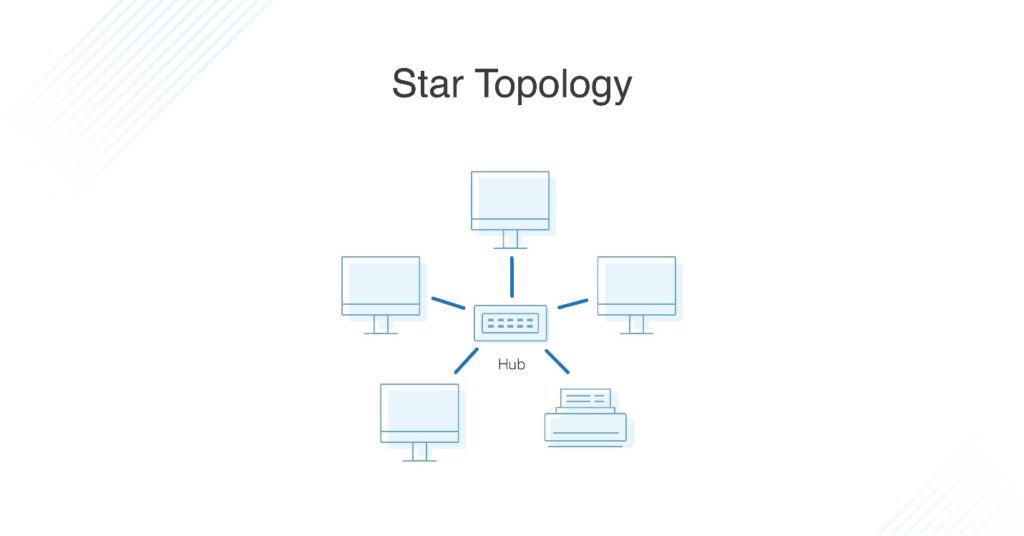
Building a local area network (LAN) topology can be make-or-break for your business, as you want to set up a resilient, secure, and easy-to-maintain topology. There are several different types of network topology and all are suitable for different purposes, depending on the overall network size and your objectives.



As with most things, there’s no “right” or one-size-fits-all option. With this in mind, I’ll walk you through the most common network topology definitions to give you a feel for the advantages and disadvantages of each.

## What Is Star Topology?

A star topology, the most common network topology, is laid out so every node in the network is directly connected to one central hub via coaxial, twisted-pair, or fiber-optic cable. Acting as a server, this central node manages data transmission—as information sent from any node on the network has to pass through the central one to reach its destination—and functions as a repeater, which helps [prevent data loss](https://www.dnsstuff.com/data-loss-prevention-software).



### Advantages of Star Topology

Star topologies are common since they allow you to conveniently manage your entire network from a single location. Because each of the nodes is independently connected to the central hub, should one go down, the rest of the network will continue functioning unaffected, making the star topology a stable and secure network layout.

Additionally, devices can be added, removed, and modified without taking the entire network offline.

On the physical side of things, the structure of the star topology uses relatively little cabling to fully connect the network, which allows for both straightforward setup and management over time as the network expands or contracts. The simplicity of the network design makes life easier for administrators, too, because it’s easy to identify where errors or performance issues are occurring.

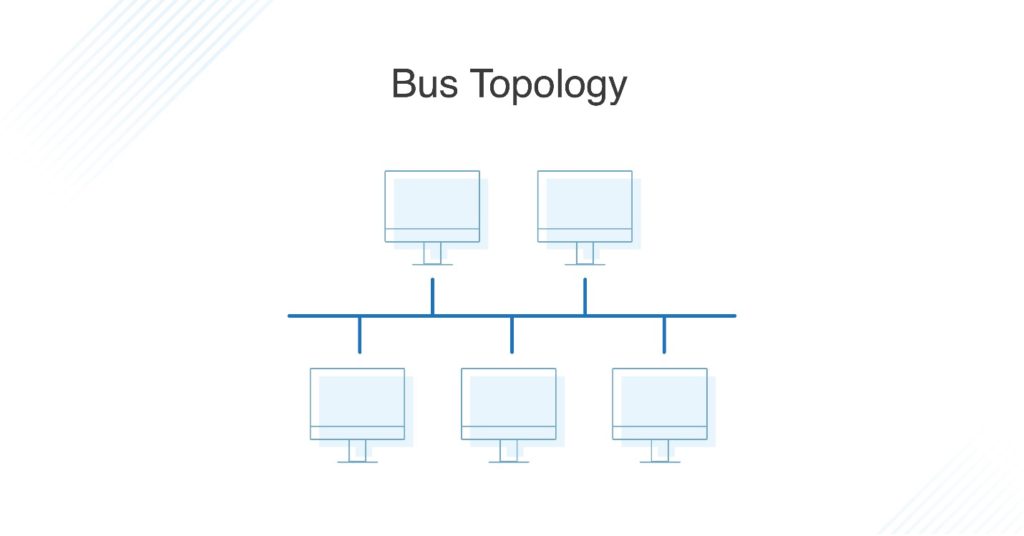
### Disadvantages of Star Topology

On the flipside, if the central hub goes down, the rest of the network can’t function. But if the central hub is properly managed and kept in good health, administrators shouldn’t have too many issues.

The overall bandwidth and performance of the network are also limited by the central node’s configurations and technical specifications, making star topologies expensive to set up and operate.

## What Is Bus Topology?

A bus topology orients all the devices on a network along a single cable running in a single direction from one end of the network to the other—which is why it’s sometimes called a “line topology” or “backbone topology.” Data flow on the network also follows the route of the cable, moving in one direction.



### Advantages of Bus Topology

Bus topologies are a good, cost-effective choice for smaller networks because the layout is simple, allowing all devices to be connected via a single coaxial or RJ45 cable. If needed, more nodes can be easily added to the network by joining additional cables.

### Disadvantages of Bus Topology

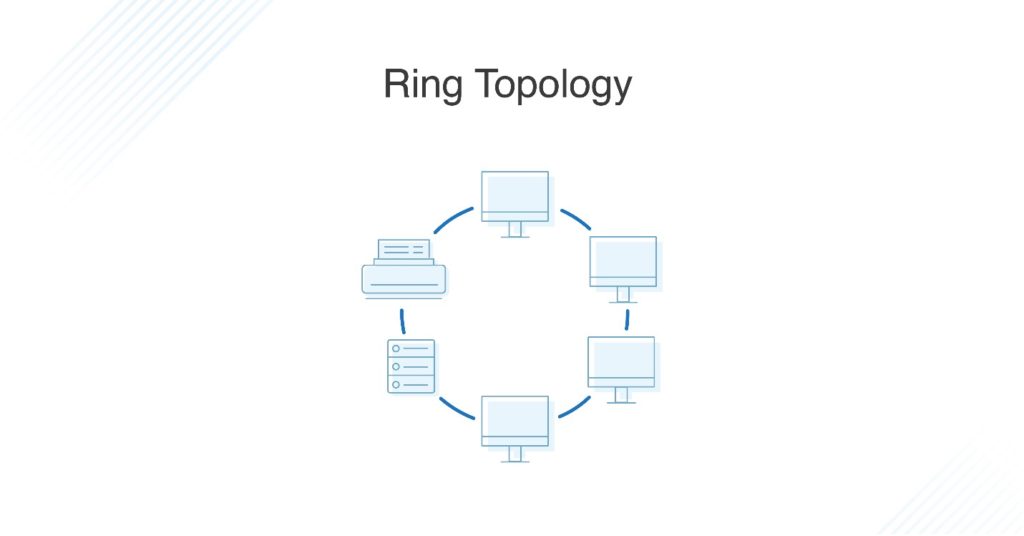
However, because bus topologies use a single cable to transmit data, they’re somewhat vulnerable. If the cable experiences a failure, the whole network goes down, which can be time-consuming and expensive to restore, which can be less of an issue with smaller networks.

Bus topologies are best suited for small networks because there’s only so much bandwidth, and every additional node will slow transmission speeds.

Furthermore, data is “half-duplex,” which means it can’t be sent in two opposite directions at the same time, so this layout is not the ideal choice for networks with huge amounts of traffic.

## What Is Ring Topology? Single vs. Dual

Ring topology is where nodes are arranged in a circle (or ring). The data can travel through the ring network in either one direction or both directions, with each device having exactly two neighbors.



### Pros of Ring Topology

Since each device is only connected to the ones on either side, when data is transmitted, the packets also travel along the circle, moving through each of the intermediate nodes until they arrive at their destination. If a large network is arranged in a ring topology, repeaters can be used to ensure packets arrive correctly and without data loss.

Only one station on the network is permitted to send data at a time, which greatly reduces the risk of packet collisions, making ring topologies efficient at transmitting data without errors.

By and large, ring topologies are cost-effective and inexpensive to install, and the intricate point-to-point connectivity of the nodes makes it relatively easy to identify issues or misconfigurations on the network.

### Cons of Ring Topology

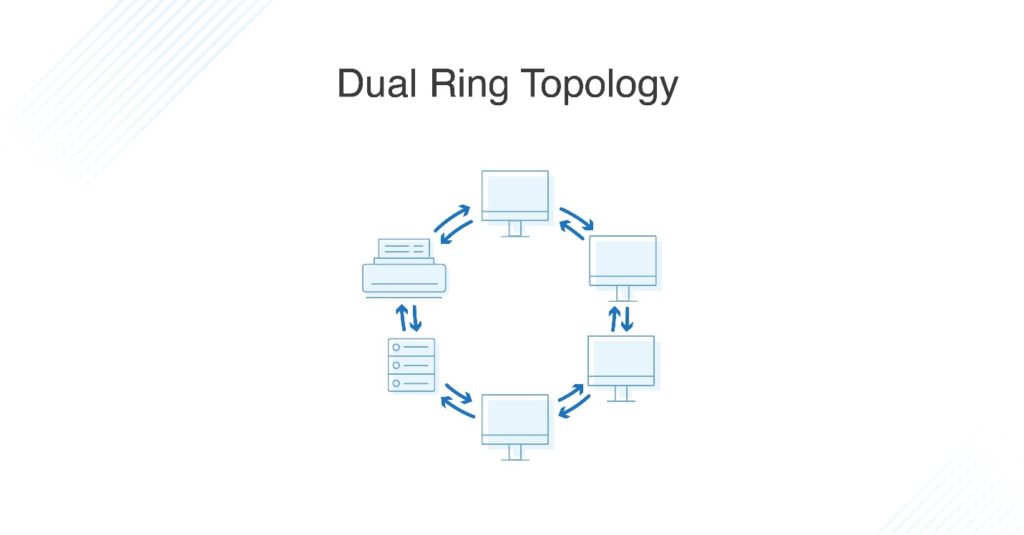
Even though it’s popular, a ring topology is still vulnerable to failure without proper network management. Since the flow of data transmission moves unidirectionally between nodes along each ring, if one node goes down, it can take the entire network with it. That’s why it’s imperative for each of the nodes to be monitored and kept in good health. Nevertheless, even if you’re vigilant and attentive to node performance, your network can still be taken down by a transmission line failure.

The question of scalability should also be taken into consideration. In a ring topology, all the devices on the network share bandwidth, so the addition of more devices can contribute to overall communication delays. Network administrators need to be mindful of the devices added to the topology to avoid overburdening the network’s resources and capacity.

Additionally, the entire network must be taken offline to reconfigure, add, or remove nodes. And while that’s not the end of the world, scheduling downtime for the network can be inconvenient and costly.

## What Is Dual-Ring Topology?

A network with ring topology is half-duplex, meaning data can only move in one direction at a time. Ring topologies can be made full-duplex by adding a second connection between network nodes, creating a dual ring topology.

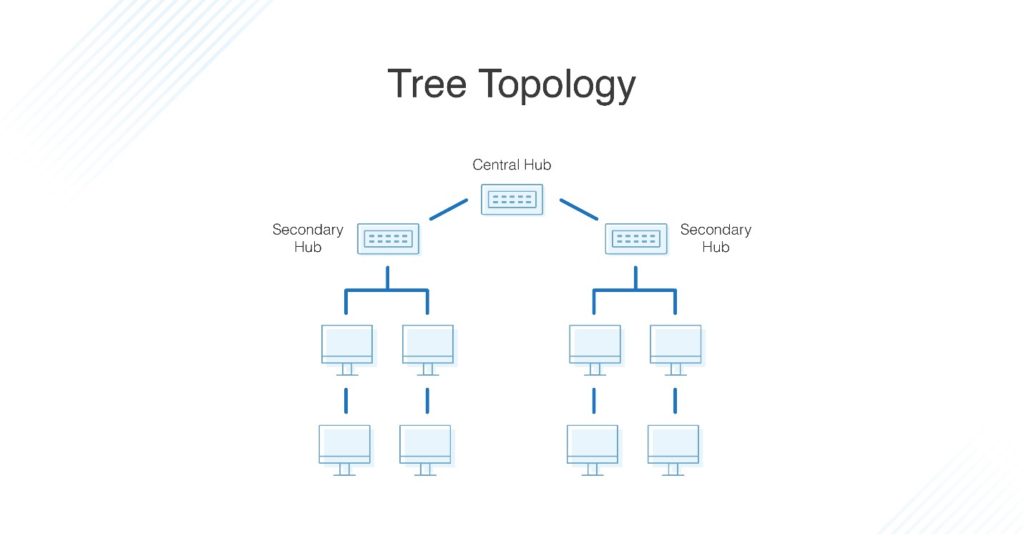


### Advantages of Dual-Ring Topology

The primary advantage of dual ring topology is its efficiency: because each node has two connections on either side, information can be sent both clockwise and counterclockwise along the network. The secondary ring included in a dual-ring topology setup can act as a redundant layer and backup, which helps solve for many of the disadvantages of traditional ring topology. Dual ring topologies offer a little extra security, too: if one ring fails within a node, the other ring is still able to send data.

## What Is Tree Topology?

The tree topology structure gets its name from how the central node functions as a sort of trunk for the network, with nodes extending outward in a branch-like fashion. However, where each node in a star topology is directly connected to the central hub, a tree topology has a parent-child hierarchy to how the nodes are connected. Those connected to the central hub are connected linearly to other nodes, so two connected nodes only share one mutual connection. Because the tree topology structure is both extremely flexible and scalable, it’s often used for wide area networks to support many spread-out devices.



### Pros of Tree Topology

Combining elements of the star and bus topologies allows for the easy addition of nodes and network expansion. Troubleshooting errors on the network is also a straightforward process, as each of the branches can be individually assessed for performance issues.

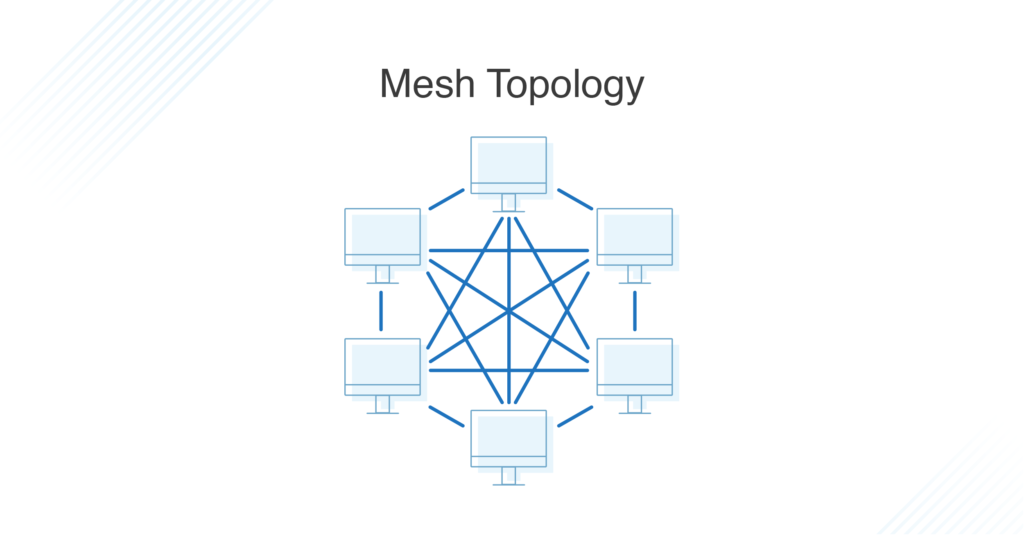
### Cons of Tree Topology

As with the star topology, the entire network depends on the health of the root node in a tree topology structure. Should the central hub fail, the various node branches will become disconnected, though connectivity within—but not between—branch systems will remain.

Because of the hierarchical complexity and linear structure of the network layout, adding more nodes to a tree topology can quickly make proper management an unwieldy, not to mention costly, experience. Tree topologies are expensive because of the sheer amount of cabling required to connect each device to the next within the hierarchical layout.

## What Is Mesh Topology?

A mesh topology is an intricate and elaborate structure of point-to-point connections where the nodes are interconnected. Mesh networks can be full or partial mesh. Partial mesh topologies are mostly interconnected, with a few nodes with only two or three connections, while full-mesh topologies are—surprise!—fully interconnected.



The web-like structure of mesh topologies offers two different methods of data transmission: routing and flooding. When data is routed, the nodes use logic to determine the shortest distance from the source to destination, and when data is flooded, the information is sent to all nodes within the network without the need for routing logic.

### Advantages of Mesh Topology

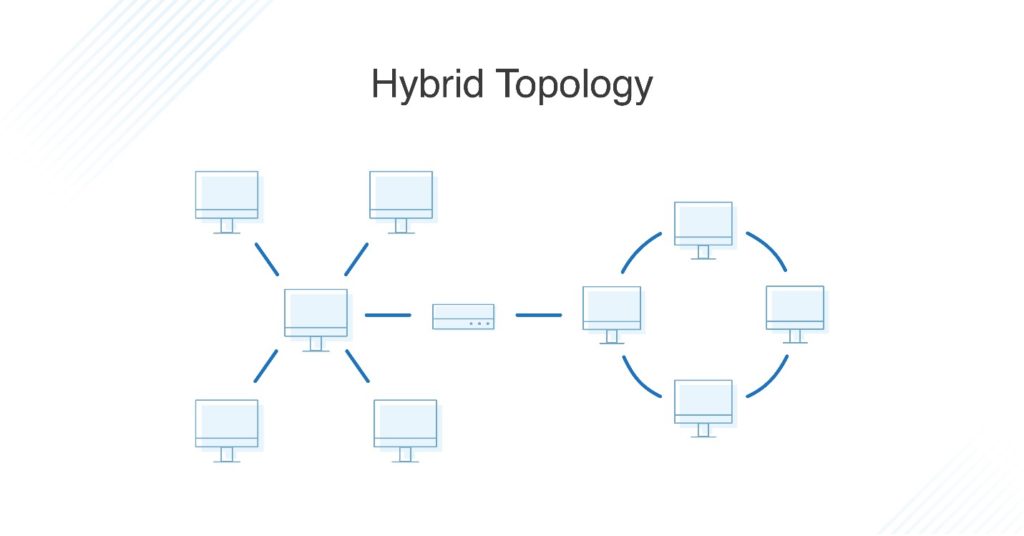
Mesh topologies are reliable and stable, and the complex degree of interconnectivity between nodes makes the network resistant to failure. For instance, no single device going down can bring the network offline.

### Disadvantages of Mesh Topology

Mesh topologies are incredibly labor-intensive. Each interconnection between nodes requires a cable and configuration once deployed, so it can also be time-consuming to set up. As with other topology structures, the cost of cabling adds up fast, and to say mesh networks require a lot of cabling is an understatement.

## What Is Hybrid Topology?

Hybrid topologies combine two or more different topology structures—the tree topology is a good example, integrating the bus and star layouts. Hybrid structures are most commonly found in larger companies where individual departments have personalized network topologies adapted to suit their needs and network usage.



### Advantages of Hybrid Topology

The main advantage of hybrid structures is the degree of flexibility they provide, as there are few limitations on the network structure itself that a hybrid setup can’t accommodate.

### Disadvantages of Hybrid Topology

However, each type of network topology comes with its own disadvantages, and as a network grows in complexity, so too does the experience and know-how required on the part of the admins to keep everything functioning optimally. There’s also the monetary cost to consider when creating a hybrid network topology.