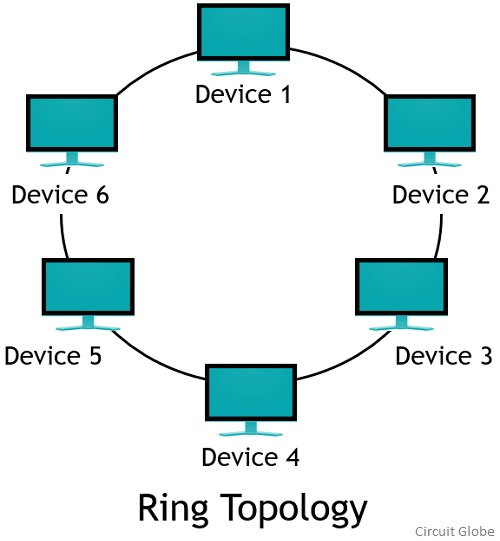
**CNL Assignment 1**

**RING TOPOLOGY**

By Roll nos. 31136, 31138, 31139, 31140



## ***Introduction*:**

Ring topology, also known as Ring network, is a type of network topology where each node is exactly connected to two other nodes, forward and backward, thus forming a single continuous path for signal transmission.

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.

Ring topology was most common, when IBM introduced its first local-area network (LAN Token Ring). Today, the need for high speed Local area networks has made this topology less popular.

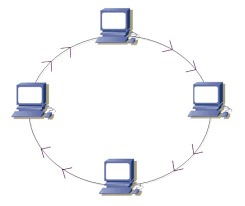
## ***Types:***

There are two types of the Ring Topology based on the data flow:

* Unidirectional
* Bidirectional

## ***Unidirectional Flow*:**

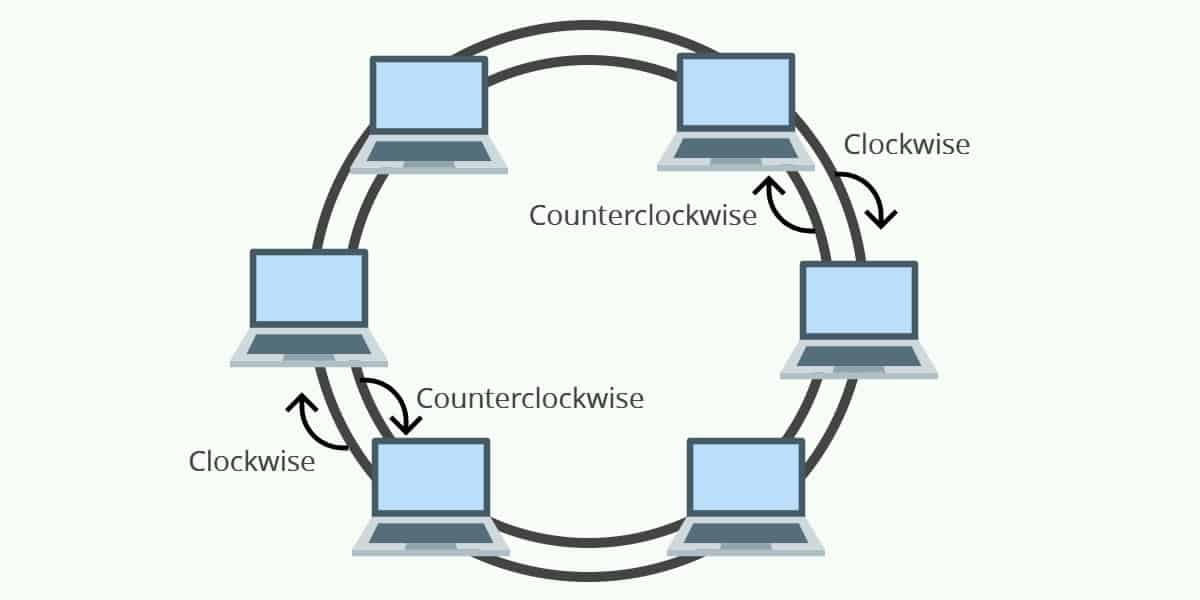
A Unidirectional ring topology handles data traffic in either clockwise or anticlockwise direction. This data network, thus, can also be called a half-duplex network. A Unidirectional ring topology is thus easy to maintain compared to the bidirectional ring topology.



Ex: SDH (Synchronous digital hierarchy) network etc.

## ***Bidirectional Flow:***

A bidirectional ring topology handles data traffic in both the direction and can be a full-duplex network.



If ring topologies are configured to be bidirectional then they are referred to as dual ring topologies.

Dual ring topologies provide each node with two connections, one in each direction. Thus, data can flow in a clockwise or counterclockwise direction as shown in the above figure.

Dual rings provide alternate paths to reach any node in case of failure in any of the intermediate nodes while sending data in one direction.

One of the prime examples for Bidirectional Ring topologies is SONET (Synchronous Optical Network).

## ***Data Flow Mechanism in Ring Topology:***

## ***Token Passing:***

Token passing in a Ring Topology is often a term which is talked about.

So, a token contains a piece of information which is sent along with data by the source computer. In easier terms, a token is like a permission packet which allows a particular node the permission to release information over the network.

The data flow in the ring topology is based on the Token Passing principle. The token is passed from one computer to the next, only the computer with the token can transmit. The receiving computer takes the data from the token and sends the token back to the sending computer with an acknowledgment signal. After verification, the token is regenerated.

Only those computers will transmit the data which have the token. Other computers have to wait for an empty token to reach them.

A token is regularly passed from one node to another. And if a node has some information to pass on the network, the node releases the information. If the node does not have any data to release on the network, then it transfers the token to the next node.

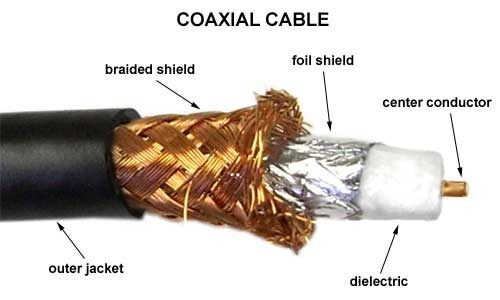
The nodes with a token are the ones only allowed to send data. Other nodes have to wait for an empty token to reach them.

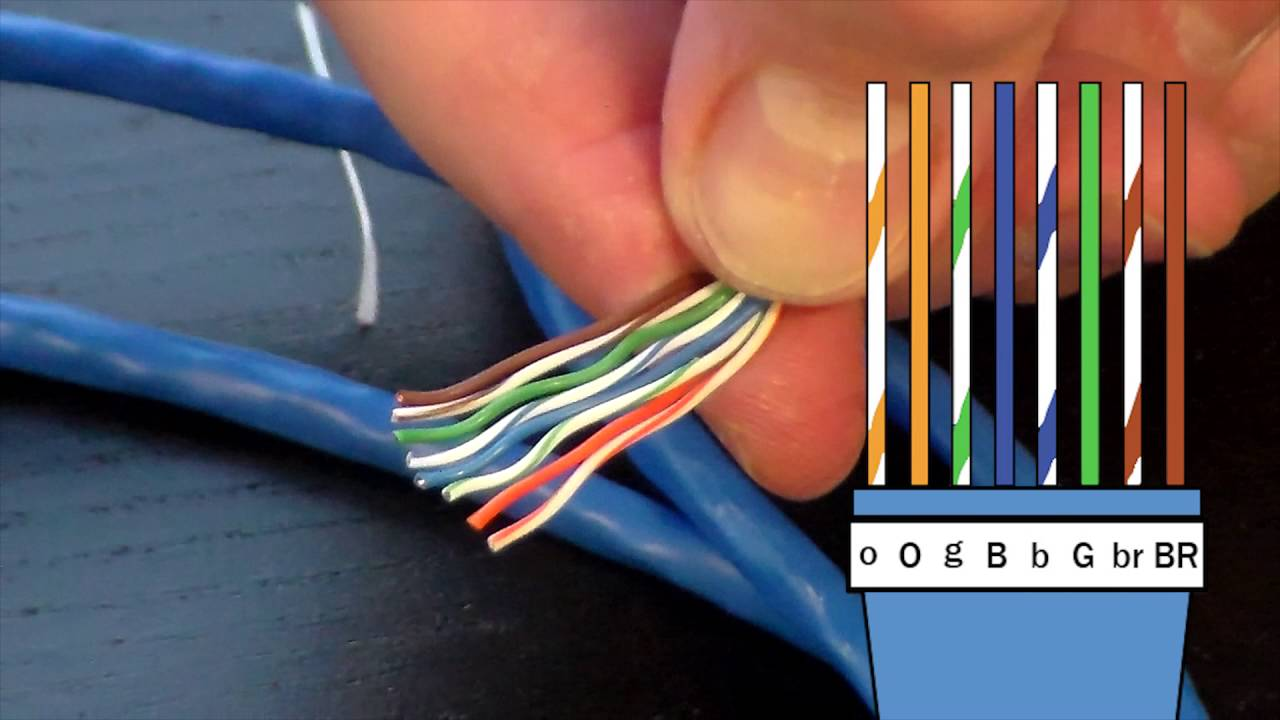
## ***Cable:***

Depending on the network card used in each computer of the ring topology, a coaxial cable or an RJ-45 network cable is used to connect computers together.

(RJ-45: RJ stands for ‘Registered Jack’ and 45 is the number of the interface standard)

SONET is a Fiber Optic Cable Ring Topology.

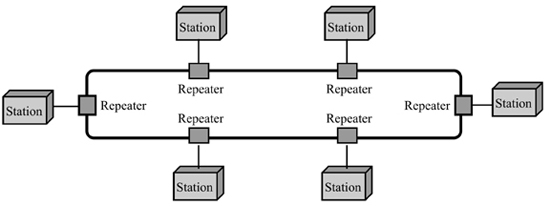


RJ45 Patch Cable Color Code

## ***Networking device:***

A number of repeaters are used for Ring topology with a large number of nodes.



This is 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.

## ***Advantages and Disadvantages of Ring Topology:***

## ***Advantages of Ring Topology:***

1. All data flows in one direction, reducing the chance of packet collisions.
2. A network server is not needed to control network connectivity between each workstation.
3. Data can transfer between workstations at high speeds.
4. Additional workstations can be added without impacting performance of the network.
5. Cheap to install and expand

## ***Disadvantages of Ring Topology:***

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.
4. The hardware needed to connect each workstation to the network is more expensive than Ethernet cards and hubs/switches.

## 

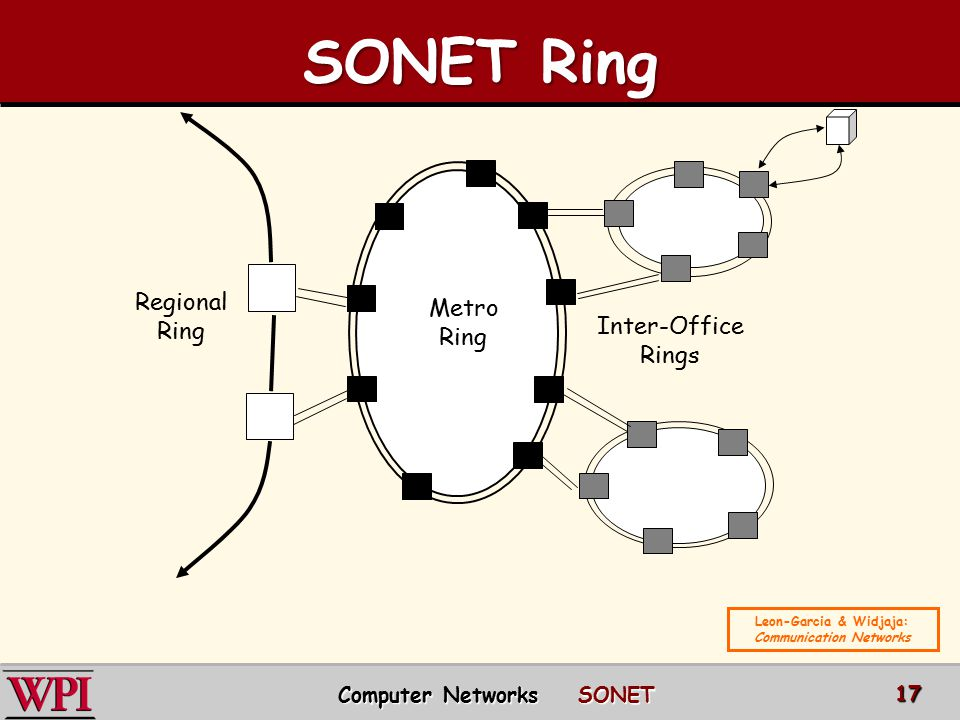
## 

## 

## ***LAN standards (IEEE):***

The IEEE 802.5 standard for SONET(Bi-Directional Ring Topology)

* Data rate for OC-1 carrier level is 50 Kbits/s
* Message is passed in the form of tokens.
* The encoding used for SONETs is PCM(Pulse-Code Modulation).
* Bit Interleaved Parity (*BIP*) -8 is used for error monitoring in different *SONET*/*SDH* layers.



## ***Real life Applications:***

Typically you will not find Ring Topology Examples in real life now-a-days because it is massively replaced by Star Network.

However, one of the common examples that still exists is SONET Rings.

SONET stands for Synchronous Optical Networking.

Also,thisnetwork topology can also be found in schools, small building, and small scale offices.

**PART B: Wireless LAN**

By Roll no. 31139

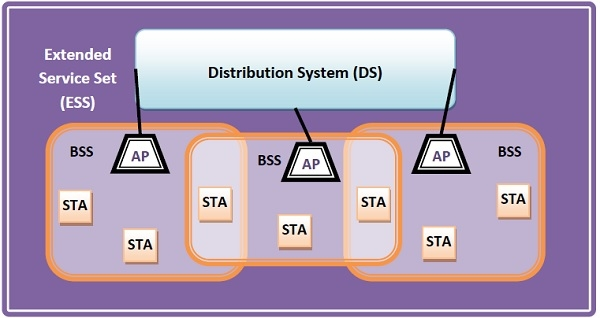
***What is a WLAN?***

* Stands for "Wireless Local Area Network." A WLAN, or wireless LAN, is a network that allows devices to connect and communicate wirelessly. Unlike a traditional wired LAN, in which devices communicate over Ethernet cables, devices on a WLAN communicate via Wi-Fi.
* While a WLAN may look different than a traditional LAN, it functions the same way. New devices are typically added and configured using DHCP. They can communicate with other devices on the network the same way they would on a wired network. The primary difference is how the data is transmitted. In a LAN, data is transmitted over physical cables in a series of Ethernet packets containing. In a WLAN, data is transmitted over the air using one of the **IEEE 802.11** protocols.

***Components of WLANs***

The components of WLAN architecture are as follows −

* **Stations** – All components that can connect into a wireless medium in a network are referred to as stations. Wireless stations can be laptops, smartphones, printers, etc. that are equipped with a wireless network interface.
* **Access Points(AP) –** Access Points, normally wireless routers, are base stations for the wireless network. They transmit and receive radio frequencies for wireless enabled devices to communicate with. It’s the central device in infrastructure WLAN type.
* **Basic Service Set (BSS)** − A Basic Service Set is the building block of WLAN. It is a set of stations communicating at the physical layer. Every BSS has an identification called the BSSID, which is the MAC address of the access point servicing the BSS. BSS can be of two categories −
  + Infrastructure BSS
  + Independent BSS
* **Extended Service Set (ESS)** – A set of connected BSSs that communicate with each other. APs in an ESS are connected by a distribution system.
* **Distribution System** – This system connects the APs in an ESS.



## 

## ***Types of WLANS***

WLANs, according to the IEEE 802.11 standards, has two basic modes of operation:

* **Infrastructure Mode** − Most Wi-Fi networks are deployed in infrastructure mode. In infrastructure mode, wireless clients, such as laptops and smartphones, connect to the WAP to join the network. The WAP usually has a wired network connection and may have permanent wireless connections to other WAPs.
* **Ad Hoc Mode** – Peer to peer (ad hoc) network is a network where stations communicate only peer to peer (P2P). There is no base and no one gives permission to talk. This is accomplished using the Independent Basic Service Set (IBSS).

## ***Advantages of WLANs***

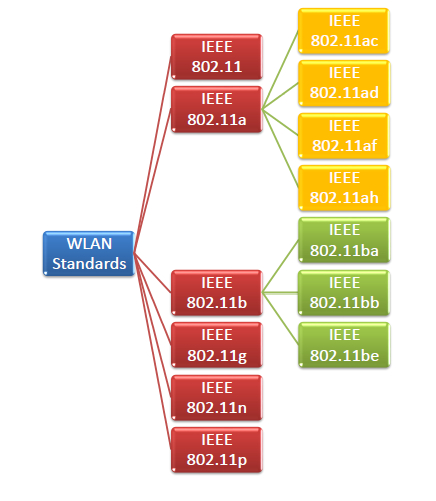
* **Mobility:** Mobility is a significant advantage of WLANs. User can access shared resources without looking for a place to plug in, anywhere in the organization. A wireless network allows users to be truly mobile if the mobile terminal is under the network coverage area.
* **Range of Coverage:** The range of a typical WLAN node is about 100 m. Coverage can be extended, and true freedom of mobility achieved via roaming. This means using access points to cover an area in such a way that their coverages overlap each other. Thereby the user can wander around and move from the coverage area of one access point to another without even knowing he has, and at the same time seamlessly maintain the connection between his node and an access point.
* **Ease of use:** WLAN is easy to use and the users need very little new information to take advantage of WLANs. Because the WLAN is transparent to a user's network operating system, applications work in the same way as they do in wired LANs.
* **Installation speed, Simplicity and Flexibility:** Installation of a WLAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings. Furthermore, wireless LAN enables networks to be set up where wires might be impossible to install.
* **Scalability:** Wireless networks can be designed to be extremely simple or complex. Wireless networks can support large numbers of nodes and large physical areas by adding access points to extend coverage.
* **Cost:** Finally, the cost of installing and maintaining a WLAN is on average lower than the cost of installing and maintaining a traditional wired LAN, for two reasons. First, WLAN eliminates the direct costs of cabling and the labor associated with installing and repairing it. Second, because WLANs simplify moving, additions, and changes, the indirect costs of user downtime and administrative overhead are reduced.

## ***Disadvantages of WLANs***

* **Radio Signal Interference:** Radio signal interference in WLAN systems can go two ways: The WLAN can cause interference to other devices operating in or near it´s frequency band. Or conversely, other devices can interfere with WLAN operation, provided their signal is stronger. The result is a scrambled signal, which of course prevents the nodes from exchanging information between each other or access points. WLANs using infrared technology generally experience line-of-sight problems. An object blocking this line between the two WLAN units is very likely to interrupt the transmission of data.
* **Connection Problem:** TCP/IP provides reliable connection over wired LANs, but in WLAN it is susceptible to losing connections, especially when the terminal is operating within the marginal WLAN coverage. Another connection related issue is IP addressing. The wireless terminals can roam between access points in the same IP subnet, but connections are lost if the terminal moves from one IP subnet to another.
* **Network Security:** This is an important aspect in WLAN. It is difficult to restrict access to a WLAN physically because radio signals can propagate outside the intended coverage of a specific WLAN, for example an office building. Some security measures against the problem are using encryption, access control lists on the access points and network identifier codes. The technical operation of WLANs also works against the intruder: Frequency hopping and direct sequence operation makes eavesdropping impossible for everyone else than the most sophisticated.

## ***What are the IEEE 802.11 Wireless LAN Standards?***

* IEEE 802.11 standard, popularly known as WiFi, lays down the architecture and specifications of wireless LANs (WLANs). WiFi or WLAN uses high frequency radio waves for connecting the nodes.
* There are many standards of IEEE 802.11 WLANs. The well-known are 802.11, 802.11a, 802.11b, 802.11g, 802.11n and 802.11p.



**IEEE 802.11**

IEEE 802.11 was the original version released in 1997. It provided 1 Mbps or 2 Mbps data rate in the 2.4 GHz band and used either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS). It is obsolete now.

**IEEE 802.11a**

802.11a was published in 1999 as a modification to 802.11, with orthogonal frequency division multiplexing (OFDM) based air interface in physical layer instead of FHSS or DSSS of 802.11. It provides a maximum data rate of 54 Mbps operating in the 5 GHz band. Besides it provides error correcting code. As 2.4 GHz band is crowded, relatively sparsely used 5 GHz imparts additional advantage to 802.11a.

Further amendments to 802.11a are 802.11ac, 802.11ad, 802.11af, 802.11ah, 802.11ai, 802.11aj etc.

**IEEE 802.11b**

802.11b is a direct extension of the original 802.11 standard that appeared in early 2000. It uses the same modulation technique as 802.11, i.e. DSSS and operates in the 2.4 GHz band. It has a higher data rate of 11 Mbps as compared to 2 Mbps of 802.11, due to which it was rapidly adopted in wireless LANs. However, since the 2.4 GHz band is pretty crowded, 802.11b devices face interference from other devices.

Further amendments to 802.11b are 802.11ba, 802.11bb, 802.11bc, 802.11bd and 802.11be.

**IEEE 802.11g**

802.11g was endorsed in 2003. It operates in the 2.4 GHz band (as in 802.11b) and provides an average throughput of 22 Mbps. It uses OFDM technique (as in 802.11a). It is fully backward compatible with 802.11b. 802.11g devices also face interference from other devices operating in the 2.4 GHz band.

**IEEE 802.11n**

802.11n was approved and published in 2009 that operates on both the 2.4 GHz and the 5 GHz bands. It has a variable data rate ranging from 54 Mbps to 600 Mbps. It provides a marked improvement over previous standards 802.11 by incorporating multiple-input multiple-output antennas (MIMO antennas).

## ***Wireless Access Point:***

In computer networking, a wireless access point, or generally a access point (AP), is a networking hardware device that allows other Wi-Fi devices to connect to a wired network. The AP usually connects to a router as a standalone device, but it can also be an integral component of the router itself.

An AP connects directly to a wired local area network, typically Ethernet, and the AP then provides wireless connections using Wireless LAN technology, typically Wi-Fi, for other devices to use that wired connection. APs support the connection of multiple wireless devices through their one wired connection.



Cisco Aironet wireless access point

## ***Wireless Router***

A wireless router is a device that performs the functions of a router and includes the functions of a wireless access point. It is used to provide access to the Internet or a private computer network.

Depending on the manufacturer and model, it can function in a wired local area network, in a wireless-only LAN, or in a mixed wired and wireless network.

