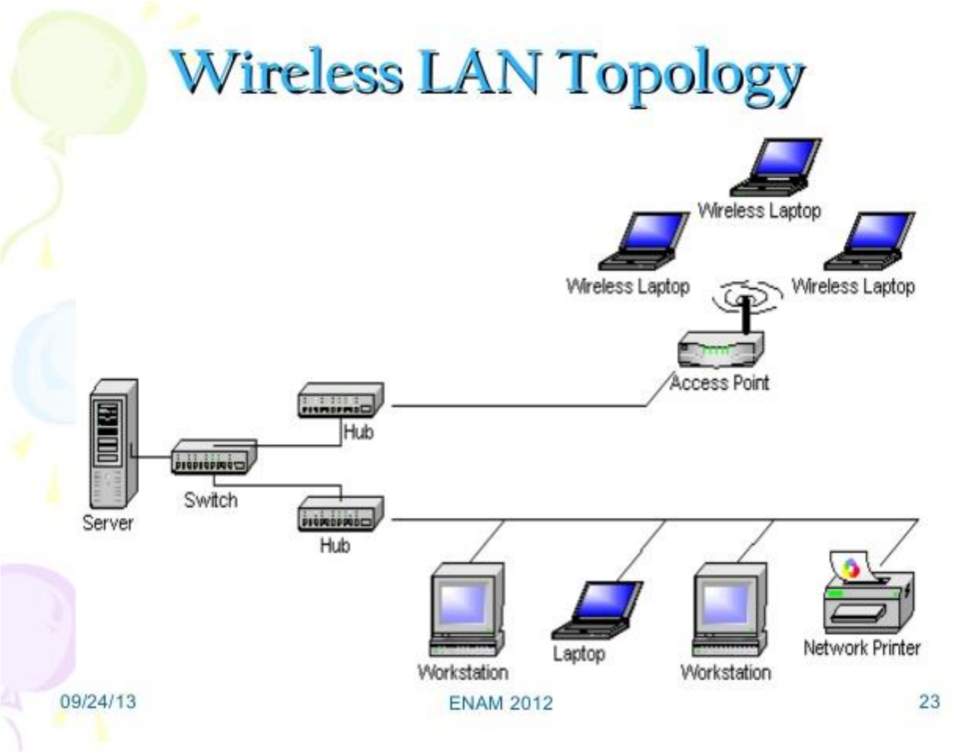
# Unit 4:

# LAN and WAN Network

## LAN Topologies

LAN physical topology defines the geographical arrangement of networking devices. Topologies are driven fundamentally by two network connection types:

A point-to-point connection is a direct link between two devices. For example, when you attach your computer to a printer, you have created a point-to-point link. In networking terms, most of the today’s point-to-point connections are associated with modems and PSTN (Public Switched Telephone Network) communications because only two devices share point-to-point connections, it defeats the purpose of a shared network.



Wireless LAN Topology

09/24/13 ENAM 2012 23

Source: www.slideshare.com

A multipoint connection, on the other hand, is a link between three or more devices. Historically, multipoint connections were used to attach central CPUs to distributed dumb terminals.

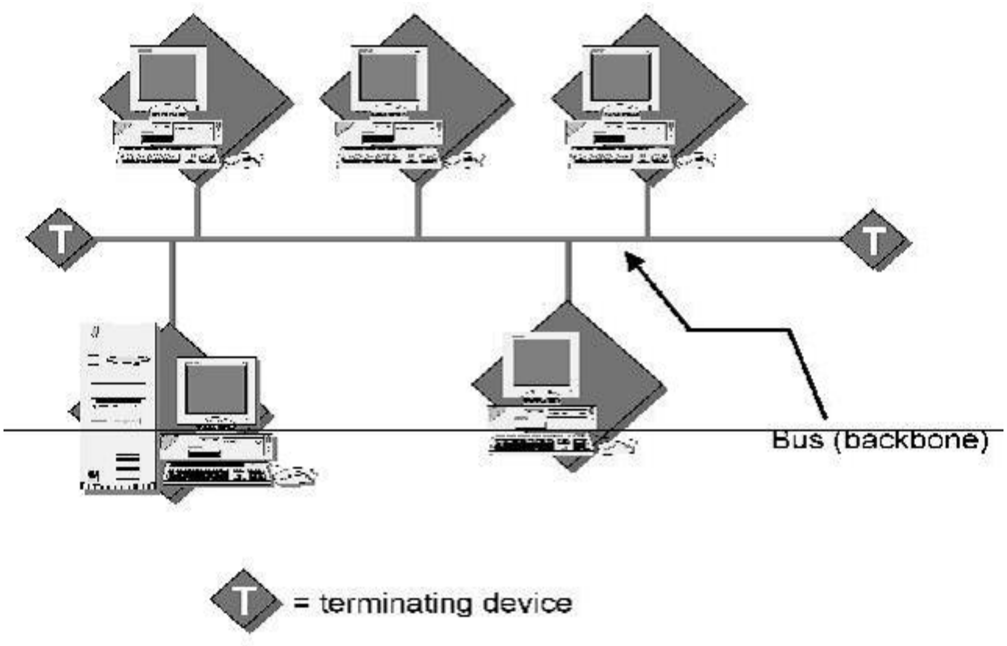
In today's LAN environments, multipoint connections link many network devices in various configurations.

**The major topologies of LAN are:**

1. Bus Topology
2. Ring Topology
3. Star Topology
4. Mesh Topology
5. Cellular Topology
6. Hybrid Topology

*Bus Topology*

The physical bus topology is the simplest and most widely used of the network designs. It consists of one continuous length of cabling (trunk) and a terminating resistor (terminator) at each end. The data communications message travels along the bus in both directions until it is picked up by a workstation or server NIC.



Source:networkingelearnsite.blogspot.com

If the message is missed or not recognized, it reaches the end of the cabling and dissipates at the terminator. All nodes in the bus topology have equal access to the trunk – no discriminating here. This is accomplished using short drop cables or direct T-connectors.

This design is easy to install because the backbone trunk traverses the LAN as one cable segment. This minimizes the amount of transmission media required. Also, the number of devices and length of the trunk can be easily expanded.

### Advantages of Bus Topology:

1. It uses established standards and it is relatively easy to install.
2. Requires fewer media than other topologies.

### Disadvantages of Bus Topology:

1. The bus networks are difficult to reconfigure, especially when the acceptable number of connections or maximum distances have been reached.
2. They are also difficult to troubleshoot because everything happens on a single media segment. This can have dangerous consequences because any break in the cabling brings the network to its knees.

*Ring Topology*

As its name implies, the physical ring topology is a circular loop of point-to-point links. Each device connects directly or indirectly to the ring through an interface device or drop cable. Messages travel around the ring from node to node in very organized manner. Each workstation checks the messages for a matching destination address.

If the address doesn't match, the node simply regenerates the message and sends it on its way. If the address matches, the node accepts the message and sends a reply to the originating sender. Initially, ring topologies are moderately simple to install; however, they require more media than bus systems because the loop must be closed.

Once your ring has been installed, it's a bit more difficult to reconfigure. Ring segments must be divided or replaced every time they're changed. Moreover, any break in the loop can affect all devices on the network.

### Advantages of Ring Topology:

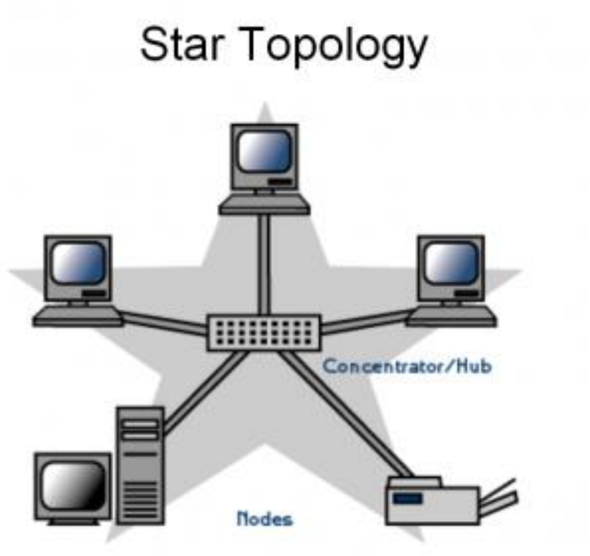
1. They are very easy to troubleshoot because each device incorporates a repeater.
2. A special internal feature called becoming, allows the troubled workstation to identify themselves quickly.

### Disadvantages of Ring Topology:

1. It is considerably difficult to install and reconfigure ring topology.
2. Media failure on unidirectional or single loop causes complete network failure.

*Star Topology*

The Physical star topology uses a central controlling hub with dedicated legs pointing in all directions – like points of a star. Each network devices has a dedicated point-to-point link to the central hub. This strategy prevents troublesome collisions and keeps the line of communication open and free of traffic.



Star topologies are somewhat difficult to install because each device gets its own dedicated segment. Obviously, they require a great deal of cabling. This design provides an excellent platform for reconfiguration and troubleshooting.

Changes to the network are as simple as plugging another segment into the hub. In addition, a break in the LAN is easy to isolate and doesn't affect the rest of the network.

**Advantages of Star Topology:**

1. Relatively easy to configure.
2. Easy to troubleshoot.
3. Media faults are automatically isolated to the failed segment.

**Disadvantages of Star Topology:**

1. Requires more cable than most topologies.
2. Moderately difficult to install.'

*Mesh Topology*

The mesh topology is the only true point-to-point design. It uses a dedicated link between every device on the network. This design is not very practical because of its excessive waste of transmission media. This topology is difficult to install and reconfigure.

Moreover, as the number of devices increases geometrically, the speed of communication also become slow. ATM (Asynchronous Transfer Mode) and switched Hubs are the example of high-speed Mesh implementation.

### Advantages of Mesh Topology:

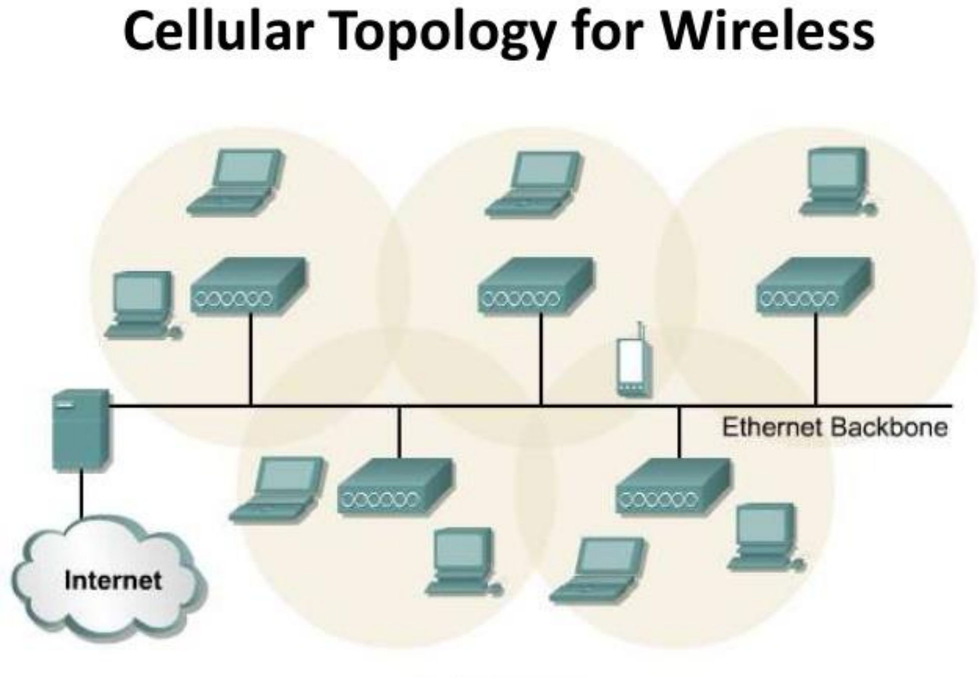
1. Easy to troubleshoot because each link is independent of all others.
2. You can easily identify faults and isolate the affected links. Because of the high number of redundant paths, multiple links can fail before the failure affects any network device.

### Disadvantages of Mesh Topology:

1. It is difficult to install and reconfigure especially as the number of devices increases.

*Cellular Topology*

A cellular topology combines wireless point-to-point and multipoint designs to divide a geographic area into cells. Each cell represents the portion of the total network area in which a specific connection operates. Devices within the cell communicate with a central station or hub. Hubs are then interconnected to route data between cells.



Source: www.slideshare.com

The cellular topology relies on the location of wireless media hubs. Cellular networks exhibit interesting characteristics since this topology do not depend on cables. Troubleshooting is easy because each hub interacts independently with each device. A cellular installation depends on the accessibility hub locations.

## Advantages of Cellular Topology:

1. It is relatively easy to install.
2. It does not require media reconfiguration when adding or removing users.
3. Fault isolation and troubleshooting is fairly simple.

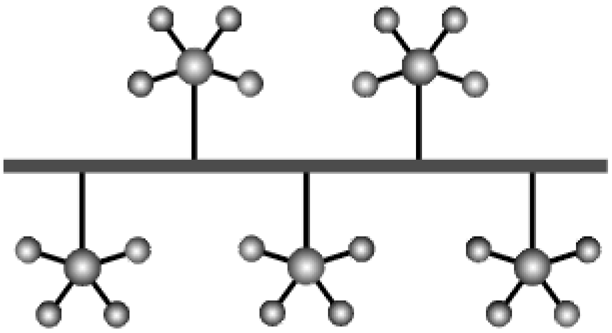
## Disadvantages of Cellular Topology:

1. All devices using a particular hub are affected by a hub failure.

*Hybrid Topology*

By modifying or combining some of the characteristics of the ‘pure’ network topologies, a more useful result may be obtained. These combinations are called hybrid topologies. Some of the hybrid topologies are:

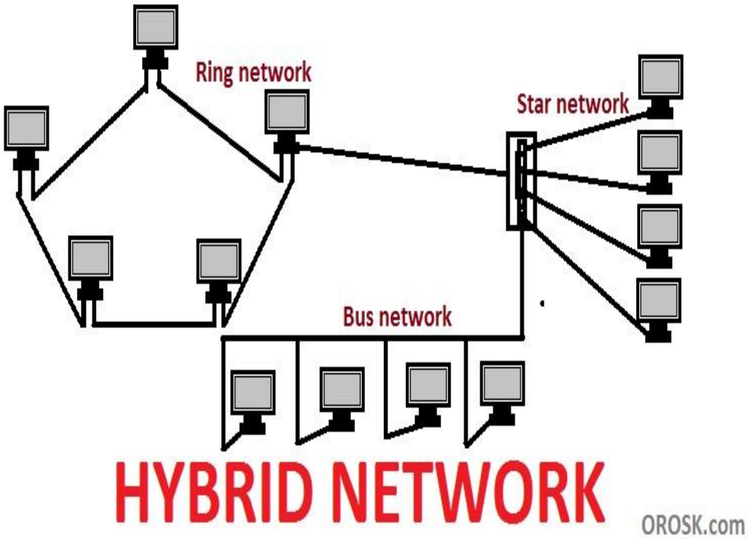
1. **Tree network**



Tree network

Source:searchnetworking.techtarget.com

2. **Star-Ring or interconnected**



# LAN Protocols

LAN protocols are distinguished by their capability to efficiently deliver data over shorter distances, such as a few hundred feet, through various mediums, such as copper cabling. Different protocols exist for different purposes and exist in different "layers" of the "Open Systems Interconnect," or OSI, model. Typically when using the word "LAN" to describe a protocol, the intent is to describe lower level, or physical, layers. Some of the most common LAN protocols are "Ethernet," "Token Ring" and "Fiber Distributed Data Interface," or "FDDI."

"Ethernet" is by far the most common type of LAN protocol. It is found in homes and offices throughout the world and is recognizable by its common "CAT5" copper cable medium. It uses a switch or hub to which all systems connect to exchange data.

"Token Ring" is an older LAN technology that is not prevalent anymore. The basic premise of "Token Ring" is a single "token" is passed from system to system, or through a hub, and only the intended recipient reads the token.

"FDDI" defines how LAN traffic is transmitted over fiber cabling. Fiber cabling is used when longer distances, usually between floors or buildings, are required, or where heightened security is required.

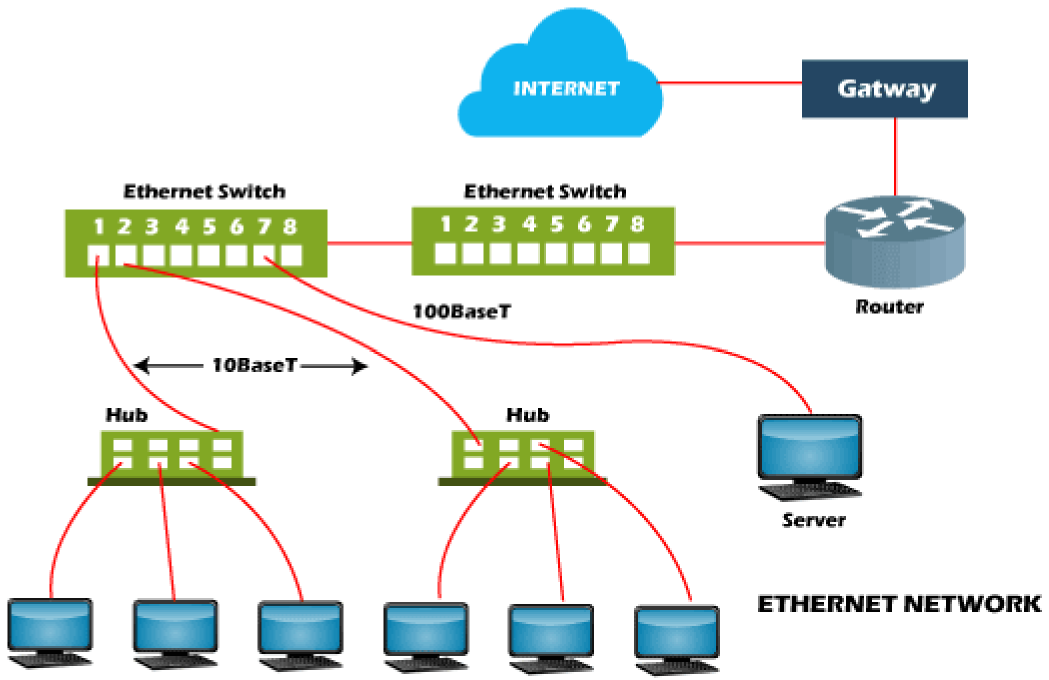
# What is Ethernet?

Ethernet is a type of communication protocol that is created at Xerox PARC in 1973 by Robert Metcalfe and others, which connects computers on a network over a wired connection. It is a widely used LAN protocol, which is also known as Alto Aloha Network. It connects computers within the local area network and wide area network. Numerous devices like printers and laptops can be connected by LAN and WAN within buildings, homes, and even small neighborhoods.

It offers a simple user interface that helps to connect various devices easily, such as switches, routers, and computers. A local area network (LAN) can be created with the help of a single router and a few Ethernet cables, which enable communication between all linked devices. This is because an Ethernet port is included in your laptop in which one end of a cable is plugged in and connect the other to a router. Ethernet ports are slightly wider, and they look similar to telephone jacks.

With lower-speed Ethernet cables and devices, most of the Ethernet devices are backward compatible. However, the speed of the connection will be as fast as the lowest common denominator. For instance, the computer will only have the potential to forward and receive data at 10 Mbps if you attach a computer with a 10BASE-T NIC to a 100BASE-T network. Also, the maximum data transfer rate will be 100 Mbps if you have a Gigabit Ethernet router and use it to connect the device.

The wireless networks replaced Ethernet in many areas; however, Ethernet is still more common for wired networking. Wi-Fi reduces the need for cabling as it allows the users to connect smartphones or laptops to a network without the required cable. While comparing with Gigabit Ethernet, the faster maximum data transfer rates are provided by the 802.11ac Wi-Fi standard. Still, as compared to a wireless network, wired connections are more secure and are less prone to interference. This is the main reason to still use Ethernet by many businesses and organizations.



## Different Types of Ethernet Networks

An Ethernet device with CAT5/CAT6 copper cables is connected to a fiber optic cable through fiber optic media converters. The distance covered by the network is significantly increased by this extension for fiber optic cable. There are some kinds of Ethernet networks, which are discussed below:

- Fast Ethernet: This type of Ethernet is usually supported by a twisted pair or CAT5 cable, which has the potential to transfer or receive data at around100 Mbps. They function at 100Base and 10/100Base Ethernet on the fiber side of the link if any device such as a camera, laptop, or other is connected to a network. The fiber optic cable and twisted pair cable are used by fast Ethernet to create communication. The 100BASE-TX, 100BASE-FX, and 100BASE-T4 are the three categories of Fast Ethernet.
- Gigabit Ethernet: This type of Ethernet network is an upgrade from Fast Ethernet, which uses fiber optic cable and twisted pair cable to create communication. It can transfer data at a rate of 1000 Mbps or 1Gbps. In modern times, gigabit Ethernet is more common. This network type also uses CAT5e or other advanced cables, which can transfer data at a rate of 10 Gbps.

The primary intention of developing the gigabit Ethernet was to full fill the user's requirements, such as faster transfer of data, faster communication network, and more.

- 10-Gigabit Ethernet: This type of network can transmit data at a rate of 10 Gigabit/second, considered a more advanced and high-speed network. It makes use of CAT6a or CAT7 twisted-pair cables and fiber optic cables as well. This network can be expended up to nearly 10,000 meters with the help of using a fiber optic cable.

- Switch Ethernet: This type of network involves adding switches or hubs, which helps to improve network throughput as each workstation in this network can have its own dedicated 10 Mbps connection instead of sharing the medium. Instead of using a crossover cable, a regular network cable is used when a switch is used in a network. For the latest Ethernet, it supports 1000Mbps to 10 Gbps and 10Mbps to 100Mbps for fast Ethernet.

## Advantages of Ethernet

- It is not much costly to form an Ethernet network. As compared to other systems of connecting computers, it is relatively inexpensive.
- Ethernet network provides high security for data as it uses firewalls in terms of data security.
- Also, the Gigabit network allows the users to transmit data at a speed of 1-100Gbps.
- In this network, the quality of the data transfer does maintain.
- In this network, administration and maintenance are easier.
- The latest version of gigabit ethernet and wireless ethernet have the potential to transmit data at the speed of 1-100Gbps.

## Disadvantages of Ethernet

- It needs deterministic service; therefore, it is not considered the best for real-time applications.
- The wired Ethernet network restricts you in terms of distances, and it is best for using in short distances.
- If you create a wired ethernet network that needs cables, hubs, switches, routers, they increase the cost of installation.
- Data needs quick transfer in an interactive application, as well as data is very small.
- In ethernet network, any acknowledge is not sent by receiver after accepting a packet.

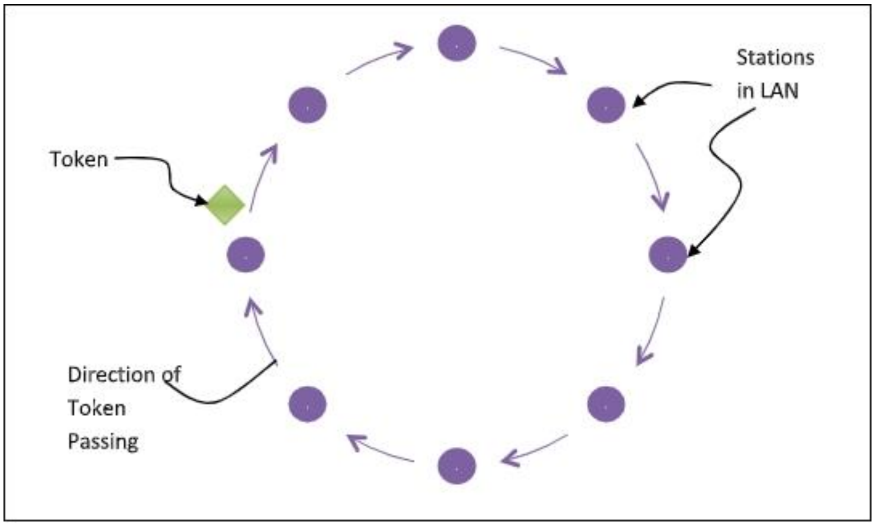
- If you are planning to set up a wireless Ethernet network, it can be difficult if you have no experience in the network field.
- Comparing with the wired Ethernet network, wireless network is not more secure.
- The full-duplex data communication mode is not supported by the 100Base-T4 version.
- Additionally, finding a problem is very difficult in an Ethernet network (if has), as it is not easy to determine which node or cable is causing the problem.

# Token Ring

Token ring (IEEE 802.5) is a communication protocol in a local area network (LAN) where all stations are connected in a ring topology and pass one or more tokens for channel acquisition. A token is a special frame of 3 bytes that circulates along the ring of stations. A station can send data frames only if it holds a token. The tokens are released on successful receipt of the data frame.

## Token Passing Mechanism in Token Ring

If a station has a frame to transmit when it receives a token, it sends the frame and then passes the token to the next station; otherwise it simply passes the token to the next station. Passing the token means receiving the token from the preceding station and transmitting to the successor station. The data flow is unidirectional in the direction of the token passing. In order that tokens are not circulated infinitely, they are removed from the network once their purpose is completed. This is shown in the following diagram −



# FDDI Full Form

**FDDI** stands for **Fiber Distributed Data Interface**. It is a set of ANSI and ISO guidelines for information transmission on fiber-optic lines in Local Area Network (LAN) that can expand in run upto 200 km (124 miles). The FDDI convention is based on the **token ring protocol.**

In expansion to being expansive geographically, an FDDI neighborhood region arranges can support thousands of clients. FDDI is habitually utilized on the spine for a Wide Area Network(WAN).

An FDDI network contains **two token rings,** one for possible backup in case the essential ring falls flat.

The primary ring offers up to 100 Mbps capacity. In case the secondary ring isn’t required for backup, it can also carry information, amplifying capacity to 200 Mbps. The single ring can amplify the most extreme remove; a double ring can expand 100 km (62 miles).

*Characteristics of FDDI*

- FDDI gives 100 Mbps of information throughput.
- FDDI incorporates two interfaces.
- It is utilized to associate the equipment to the ring over long distances.
- FDDI could be a LAN with Station Management.
- Allows all stations to have broken even with the sum of time to transmit information.
- FDDI defines two classes of traffic viz. synchronous and asynchronous.

*Advantages of FDDI*

- Fiber optic cables transmit signals over more noteworthy separations of approximately 200 km.
- It is conceivable to supply the need to the work stations associated within the chain. Consequently, based on the prerequisite a few stations are bypassed to supply speedier benefit to the rest.
- FDDI employments different tokens to make strides organize speed.
- It offers a higher transmission capacity (up to 250 Gbps). Thus, it can handle information rates up to 100 Mbps.
- It offers tall security because it is troublesome to spy on the fiber-optic link.
- Fiber optic cable does not break as effectively as other sorts of cables.

*Disadvantages of FDDI*

- FDDI is complex. Thus establishment and support require an incredible bargain of expertise.
- FDDI is expensive. Typically since fiber optic cable, connectors and concentrators are exceptionally costly.

# Introduction to Wireless LAN

Wireless LAN stands for **Wireless Local Area Network**. It is also called LAWN (**Local Area Wireless Network**). WLAN is one in which a mobile user can connect to a Local Area Network (LAN) through a wireless connection.

The IEEE 802.11 group of standards defines the technologies for wireless LANs. For path sharing, 802.11 standard uses the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance). It also uses an encryption method i.e. wired equivalent privacy algorithm.

Wireless LANs provide high speed data communication in small areas such as building or an office. WLANs allow users to move around in a confined area while they are still connected to the network.

In some instance wireless LAN technology is used to save costs and avoid laying cable, while in other cases, it is the only option for providing high-speed internet access to the public. Whatever the reason, wireless solutions are popping up everywhere.

Examples of WLANs that are available today are NCR's waveLAN and Motorola's ALTAIR.

## Advantages of WLANs

- **Flexibility:** Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.).
- **Planning:** Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans.
- **Design:** Wireless networks allow for the design of independent, small devices which can for example be put into a pocket. Cables not only restrict users but also designers of small notepads, PDAs, etc.
- **Robustness:** Wireless networks can handle disasters, e.g., earthquakes, flood etc. whereas, networks requiring a wired infrastructure will usually break down completely in disasters.
- **Cost:** The cost of installing and maintaining a wireless LAN is on average lower than the cost of installing and maintaining a traditional wired LAN, for two reasons. First, after providing wireless access to the wireless network via an access point for the first user, adding additional users to a network will not increase the cost. And second, wireless LAN

eliminates the direct costs of cabling and the labor associated with installing and repairing it.

- **Ease of Use:** Wireless LAN is easy to use and the users need very little new information to take advantage of WLANs.

## Disadvantages of WLANs

- **Quality of Services:** Quality of wireless LAN is typically lower than wired networks. The main reason for this is the lower bandwidth due to limitations is radio transmission, higher error rates due to interference and higher delay/delay variation due to extensive error correction and detection mechanisms.
- **Proprietary Solutions:** Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardization functionality plus many enhanced features. Most components today adhere to the basic standards IEEE 802.11a or 802.11b.
- **Restrictions:** Several govt. and non-govt. institutions world-wide regulate the operation and restrict frequencies to minimize interference.
- **Global operation:** Wireless LAN products are sold in all countries so, national and international frequency regulations have to be considered.
- **Low Power:** Devices communicating via a wireless LAN are typically power consuming, also wireless devices running on battery power. Whereas the LAN design should take this into account and implement special power saving modes and power management functions.
- **License free operation:** LAN operators don't want to apply for a special license to be able to use the product. The equipment must operate in a license free band, such as the 2.4 GHz ISM band.
- **Robust transmission technology:** If wireless LAN uses radio transmission, many other electrical devices can interfere with them (such as vacuum cleaner, train engines, hair dryers, etc.).Wireless LAN transceivers cannot be adjusted for perfect transmission is a standard office or production environment.

# Virtual LAN (VLAN)

*Virtual LAN (VLAN)* is a concept in which we can divide the devices logically on layer 2 (data link layer). Generally, layer 3 devices divide the broadcast domain but the broadcast domain can be divided by switches using the concept of VLAN.

A broadcast domain is a network segment in which if a device broadcast a packet then all the devices in the same broadcast domain will receive it. The devices in the same broadcast domain will receive all the broadcast packets but it is limited to switches only as routers don't forward out the broadcast packet. To forward out the packets to different VLAN (from one VLAN to another) or broadcast domains, inter Vlan routing is needed. Through VLAN, different small-size sub-networks are created which are comparatively easy to handle.

**VLAN ranges:**

- **VLAN 0, 4095:** These are reserved VLAN which cannot be seen or used.
- **VLAN 1:** It is the default VLAN of switches. By default, all switch ports are in VLAN. This VLAN can't be deleted or edit but can be used.
- **VLAN 2-1001:** This is a normal VLAN range. We can create, edit and delete these VLAN.
- **VLAN 1002-1005:** These are CISCO defaults for fddi and token rings. These VLAN can't be deleted.
- **Vlan 1006-4094:** This is the extended range of Vlan.

VLANs offer several features and benefits, including:

- **Improved network security:** VLANs can be used to separate network traffic and limit access to specific network resources. This improves security by preventing unauthorized access to sensitive data and network resources.
- **Better network performance:** By segregating network traffic into smaller logical networks, VLANs can reduce the amount of broadcast traffic and improve network performance.
- **Simplified network management:** VLANs allow network administrators to group devices together logically, rather than physically, which can simplify network management tasks such as configuration, troubleshooting, and maintenance.
- **Flexibility:** VLANs can be configured dynamically, allowing network administrators to quickly and easily adjust network configurations as needed.
- **Cost savings:** VLANs can help reduce hardware costs by allowing multiple virtual networks to share a single physical network infrastructure.
- **Scalability:** VLANs can be used to segment a network into smaller, more manageable groups as the network grows in size and complexity.

Some of the key features of VLANs include:

- **VLAN tagging:** VLAN tagging is a way to identify and distinguish VLAN traffic from other network traffic. This is typically done by adding a VLAN tag to the Ethernet frame header.
- **VLAN membership:** VLAN membership determines which devices are assigned to which VLANs. Devices can be assigned to VLANs based on port, MAC address, or other criteria.
- **VLAN trunking:** VLAN trunking allows multiple VLANs to be carried over a single physical link. This is typically done using a protocol such as IEEE 802.1Q.
- **VLAN management:** VLAN management involves configuring and managing VLANs, including assigning devices to VLANs, configuring VLAN tags, and configuring VLAN trunking.

**Types of connections in VLAN –**

There are three ways to connect devices on a VLAN, the type of connections are based on the connected devices i.e. whether they are VLAN-aware(A device that understands VLAN formats and VLAN membership) or VLAN-unaware(A device that doesn’t understand VLAN format and VLAN membership).

1. **Trunk Link –**
   All connected devices to a trunk link must be VLAN-aware. All frames on this should have a special header attached to it called tagged frames.
2. **Access link –**
   It connects VLAN-unaware devices to a VLAN-aware bridge. All frames on the access link must be untagged.
3. **Hybrid link –**
   It is a combination of the Trunk link and Access link. Here both VLAN-unaware and VLAN-aware devices are attached and it can have both tagged and untagged frames.

**Advantages –**

- **Performance –**
  The network traffic is full of broadcast and multicast. VLAN reduces the need to send such traffic to unnecessary destinations. e.g.-If the traffic is intended for 2 users but as 10 devices are present in the same broadcast domain, therefore, all will receive the traffic i.e. wastage of bandwidth but if we make VLANs, then the broadcast or multicast packet will go to the intended users only.
- **Formation of virtual groups –**
  As there are different departments in every organization namely sales, finance etc., VLANs can be very useful in order to group the devices logically according to their departments.

- **Security –**
  In the same network, sensitive data can be broadcast which can be accessed by the outsider but by creating VLAN, we can control broadcast domains, set up firewalls, restrict access. Also, VLANs can be used to inform the network manager of an intrusion. Hence, VLANs greatly enhance network security.
- **Flexibility –**
  VLAN provide flexibility to add, remove the number of host we want.
- **Cost reduction –**
  VLANs can be used to create broadcast domains which eliminate the need for expensive routers.
  By using Vlan, the number of small size broadcast domain can be increased which are easy to handle as compared to a bigger broadcast domain.

### Disadvantages of VLAN

1. **Complexity:** VLANs can be complex to configure and manage, particularly in large or dynamic cloud computing environments.
2. **Limited scalability:** VLANs are limited by the number of available VLAN IDs, which can be a constraint in larger cloud computing environments.
3. **Limited security**: VLANs do not provide complete security and can be compromised by malicious actors who are able to gain access to the network.
4. **Limited interoperability**: VLANs may not be fully compatible with all types of network devices and protocols, which can limit their usefulness in cloud computing environments.
5. **Limited mobility**: VLANs may not support the movement of devices or users between different network segments, which can limit their usefulness in mobile or remote cloud computing environments.
6. **Cost:** Implementing and maintaining VLANs can be costly, especially if specialized hardware or software is required.
7. **Limited visibility:** VLANs can make it more difficult to monitor and troubleshoot network issues, as traffic is isolated in different segments.

### Real-Time Applications of VLAN

Virtual LANs (VLANs) are widely used in cloud computing environments to improve network performance and security. Here are a few examples of real-time applications of VLANs:

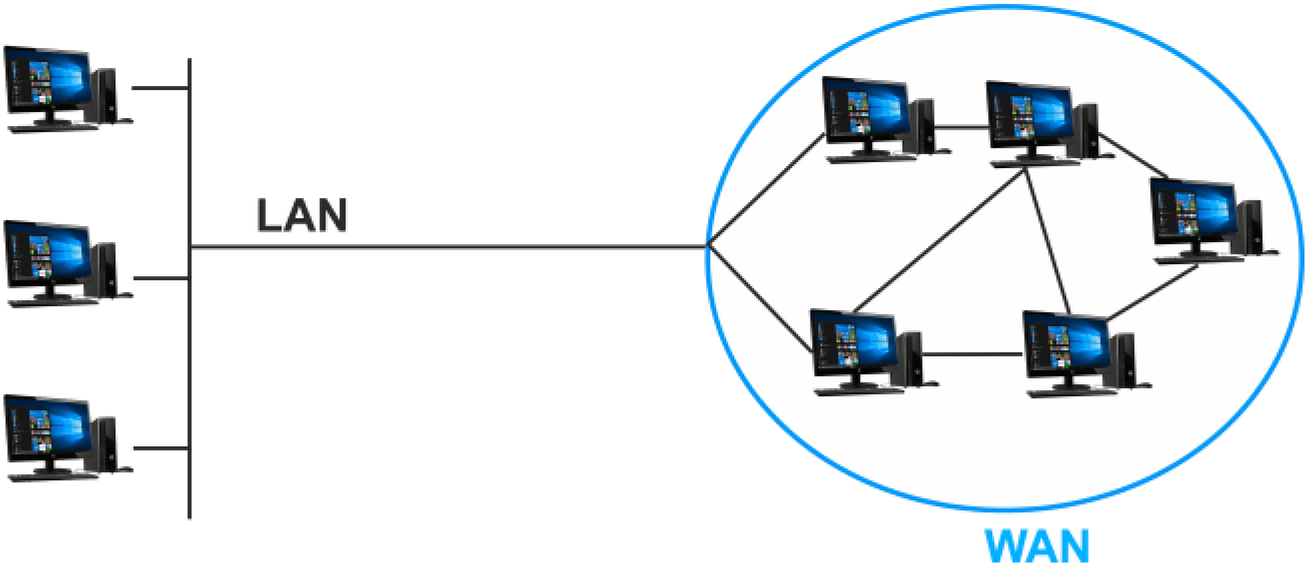
1. **Voice over IP (VoIP)** : VLANs can be used to isolate voice traffic from data traffic, which improves the quality of VoIP calls and reduces the risk of network congestion.
2. **Video Conferencing** : VLANs can be used to prioritize video traffic and ensure that it receives the bandwidth and resources it needs for high-quality video conferencing.

3. **Remote Access** : VLANs can be used to provide secure remote access to cloud-based applications and resources, by isolating remote users from the rest of the network.
4. **Cloud Backup and Recovery** : VLANs can be used to isolate backup and recovery traffic, which reduces the risk of network congestion and improves the performance of backup and recovery operations.
5. **Gaming** : VLANs can be used to prioritize gaming traffic, which ensures that gamers receive the bandwidth and resources they need for a smooth gaming experience.
6. **IoT** : VLANs can be used to isolate Internet of Things (IoT) devices from the rest of the network, which improves security and reduces the risk of network congestion.

## WAN: Wide Area Network

WAN stands for Wide Area Network. It is a network that made its presence globally very soon. It can be utilized to connect multiple devices all over the world. This type of network provides a better facility to communicate between devices in any part of the world. Nowadays, the internet is recognized as the world's most extensive and fastest-growing wide area network, making connectivity easier among people worldwide. WAN is very much helpful in building communication in communities, businesses and organizations.

A wide area network is a typical form of a telecommunication network that can be used through any location across the world, and that's why it is known as the most prominent computer or system network available globally today.



Simply put, a Wide Area Network is a network of multiple device connections established through Local Area Networks or other networks that can communicate with each other over large distances. WANs are essentially networks of networks, with the Internet serving as the most extensive WAN on the planet.

The wide area networks are provided with the help of service providers. For instance, the service providers in the case of SIM and cellular networks include vendors like JIO, IDEA, AIRTEL, VI, etc. They typically charge users for giving access to their networks. Customers can send or receive messages from anywhere to any location if they are within the network range of the service provider.

One of the best things about Wide Area Network is that it provides better security than other networks, providing a unique IP address to each device connected to it. An IP address is recognized as an identity of the network and is logged for every data transaction. It is typically used by a service provider to locate a specific device.

A Wide Area Network is mainly of two types. The first is based on a point-to-point connection, and the second operates by transferring data packets.

A WAN router is needed for building this network, which is also known as an edge router or border router. A WAN router is a device that is used to connect the devices that provide a path for transferring data packets between the wide area network locations and allowing access to a carrier network for a business.

## Brief History of the Wide Area Network

In the late 1950s, the Wide Area Network was first designed by the U.S. Air force. The primary roots of the huge area network are connected to the United States defence in which they developed the **ARPANET,** and with the help of it, significant researchers could communicate and share computer resources remotely. The link was made via radio waves, circuit-switched telephone lines, or optical fibres. Since then, it has evolved greatly and proved effective in the interchange of data worldwide among people. These networks are now helping to establish communication between a client and an employee, a teacher and a student, a buyer and a seller, etc. An important advantage of a Wide Area Network is that it can transmit images, audio, video and many other digital formats over long distances.

## WAN Optimization

Performance challenges in businesses are often caused by latency and bandwidth concerns in the network. Wide Area Network uses best optimization practices with the help of various techniques, including network shaping, protocol optimization, reduction, compression and local cache. With the help of these techniques, the network is improved, and packet delivery is optimized. This ultimately helps to control traffic laterally and enable dynamic network bandwidth growth or contraction as needed.

## Characteristics of a Wide Area Network

- **Broader Reach:** The reach of the wide area network is very high. WAN can cover a vast geographic area, such as a whole nation, region, or even the entire world.
- **Higher Capacity:** The capacity of the wide area network is very high compared to the local area network. Due to this, it straightforwardly connects large numbers of users over different locations worldwide, which shows its capacity to connect large numbers of devices.
- **Use of Public Carrier:** Wide area networks mainly use telephone networks, cable systems, satellites, etc., to connect and transfer data quickly because these things are readily available.
- **Resource Sharing:** Wide area network provides a facility for all users to share data and information within large areas worldwide. Computer resources can be easily managed through remote devices that quickly interchange data.

## Advantages of Wide Area Network

- The central feature of a wide area network is that it provides network coverage for a large geographical area to transfer data rapidly and easily.
- The data can be stored effectively and efficiently because WAN provides the facility of remote access to data.
- The travel expenses necessary to cover the ranges of large geographical areas can be reduced with WAN.
- One of the best advantages of a Wide Area Network is that it provides the facility to connect users and organizations all over the world quickly, thereby facilitating data interchange and allowing businesses to communicate on a global scale.

## Disadvantages of Wide Area Network

- In a wide area network, there is lots of traffic that are interpreting between the transferring of data.

- The wide area network provides less security than the LAN (local area network) or MAN (metropolitan area network).
- The setup cost of a wide area network is a little higher than other networks.
- Another drawback of a wide area network is that due to multiple connections, the noise and errors are present in a heavy amount while transferring large size of data concurrently.
- Data transfer speeds are lower in a wide area network than in a local area network because, in a WAN, multiple connections and large-distance transactions are involved within the network.

## Types of WAN Technologies

- **Packet Switching:** Packet switching is a method of transferring the data in which data is sent in several parts, which are called
- **TCP/IP:** TCP (transmission control protocol) and IP (internet protocol) are the basic-standard protocol used to communicate with the data. The Internet of today's day and specific computer/device networks employ the TCP/IP suite of fundamental communication protocols to link network devices.
- **Router:** A router is a device that is used for establishing the network between the devices. It operates as both the input and output network device.

# Routing

- A Router is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.
- A Router works at the network layer in the OSI model and internet layer in TCP/IP model
- A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.
- The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.
- The routing protocols use the metric to determine the best path for the packet delivery. The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc. used by the routing algorithm to determine the optimal path to the destination.

- The routing algorithm initializes and maintains the routing table for the process of path determination.

## Routing Metrics and Costs

Routing metrics and costs are used for determining the best route to the destination. The factors used by the protocols to determine the shortest path, these factors are known as a metric.

Metrics are the network variables used to determine the best route to the destination. For some protocols use the static metrics means that their value cannot be changed and for some other routing protocols use the dynamic metrics means that their value can be assigned by the system administrator.

**The most common metric values are given below:**

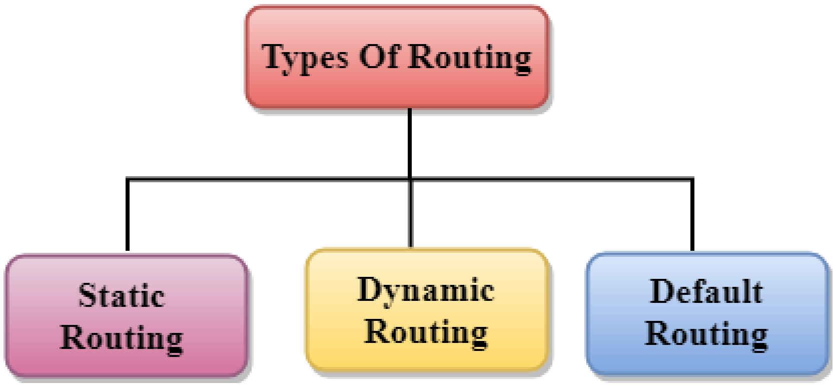
- **Hop count:** Hop count is defined as a metric that specifies the number of passes through internetworking devices such as a router, a packet must travel in a route to move from source to the destination. If the routing protocol considers the hop as a primary metric value, then the path with the least hop count will be considered as the best path to move from source to the destination.
- **Delay:** It is a time taken by the router to process, queue and transmit a datagram to an interface. The protocols use this metric to determine the delay values for all the links along the path end-to-end. The path having the lowest delay value will be considered as the best path.
- **Bandwidth:** The capacity of the link is known as a bandwidth of the link. The bandwidth is measured in terms of bits per second. The link that has a higher transfer rate like gigabit is preferred over the link that has the lower capacity like 56 kb. The protocol will determine the bandwidth capacity for all the links along the path, and the overall higher bandwidth will be considered as the best route.
- **Load:** Load refers to the degree to which the network resource such as a router or network link is busy. A Load can be calculated in a variety of ways such as CPU utilization, packets processed per second. If the traffic increases, then the load value will also be increased. The load value changes with respect to the change in the traffic.

- **Reliability:** Reliability is a metric factor may be composed of a fixed value. It depends on the network links, and its value is measured dynamically. Some networks go down more often than others. After network failure, some network links repaired more easily than other network links. Any reliability factor can be considered for the assignment of reliability ratings, which are generally numeric values assigned by the system administrator.

# Types of Routing

Routing can be classified into three categories:

- Static Routing
- Default Routing
- Dynamic Routing



## Static Routing

- Static Routing is also known as Nonadaptive Routing.
- It is a technique in which the administrator manually adds the routes in a routing table.
- A Router can send the packets for the destination along the route defined by the administrator.
- In this technique, routing decisions are not made based on the condition or topology of the networks

## Advantages Of Static Routing

Following are the advantages of Static Routing:

- **No Overhead:** It has ho overhead on the CPU usage of the router. Therefore, the cheaper router can be used to obtain static routing.
- **Bandwidth:** It has not bandwidth usage between the routers.
- **Security:** It provides security as the system administrator is allowed only to have control over the routing to a particular network.

## Disadvantages of Static Routing:

Following are the disadvantages of Static Routing:

- For a large network, it becomes a very difficult task to add each route manually to the routing table.
- The system administrator should have a good knowledge of a topology as he has to add each route manually.

## Default Routing

- Default Routing is a technique in which a router is configured to send all the packets to the same hop device, and it doesn't matter whether it belongs to a particular network or not. A Packet is transmitted to the device for which it is configured in default routing.
- Default Routing is used when networks deal with the single exit point.
- It is also useful when the bulk of transmission networks have to transmit the data to the same hp device.
- When a specific route is mentioned in the routing table, the router will choose the specific route rather than the default route. The default route is chosen only when a specific route is not mentioned in the routing table.

## Dynamic Routing

- It is also known as Adaptive Routing.
- It is a technique in which a router adds a new route in the routing table for each packet in response to the changes in the condition or topology of the network.
- Dynamic protocols are used to discover the new routes to reach the destination.
- In Dynamic Routing, RIP and OSPF are the protocols used to discover the new routes.
- If any route goes down, then the automatic adjustment will be made to reach the destination.

**The Dynamic protocol should have the following features:**

- All the routers must have the same dynamic routing protocol in order to exchange the routes.
- If the router discovers any change in the condition or topology, then router broadcast this information to all other routers.

## Advantages of Dynamic Routing:

- It is easier to configure.
- It is more effective in selecting the best route in response to the changes in the condition or topology.

## Disadvantages of Dynamic Routing:

- It is more expensive in terms of CPU and bandwidth usage.
- It is less secure as compared to default and static routing.

# Distance Vector Routing (DVR) Protocol

A **distance-vector routing (DVR)** protocol requires that a router inform its neighbors of topology changes periodically. Historically known as the old ARPANET routing algorithm (or known as Bellman-Ford algorithm).

**Bellman Ford Basics –** Each router maintains a Distance Vector table containing the distance between itself and ALL possible destination nodes. Distances,based on a chosen metric, are computed using information from the neighbors' distance vectors.

Information kept by DV router -

- Each router has an ID
- Associated with each link connected to a router,
- there is a link cost (static or dynamic).
- Intermediate hops

Distance Vector Table Initialization -

- Distance to itself = 0
- Distance to ALL other routers = infinity number.

**Distance Vector Algorithm –**

1. A router transmits its distance vector to each of its neighbors in a routing packet.

2. Each router receives and saves the most recently received distance vector from each of its neighbors.
3. A router recalculates its distance vector when:
    - It receives a distance vector from a neighbor containing different information than before.
    - It discovers that a link to a neighbor has gone down.

The DV calculation is based on minimizing the cost to each destination

Dx(y) = Estimate of least cost from x to y

C(x,v) = Node x knows cost to each neighbor v

Dx = [Dx(y): y ∈ N ] = Node x maintains distance vector

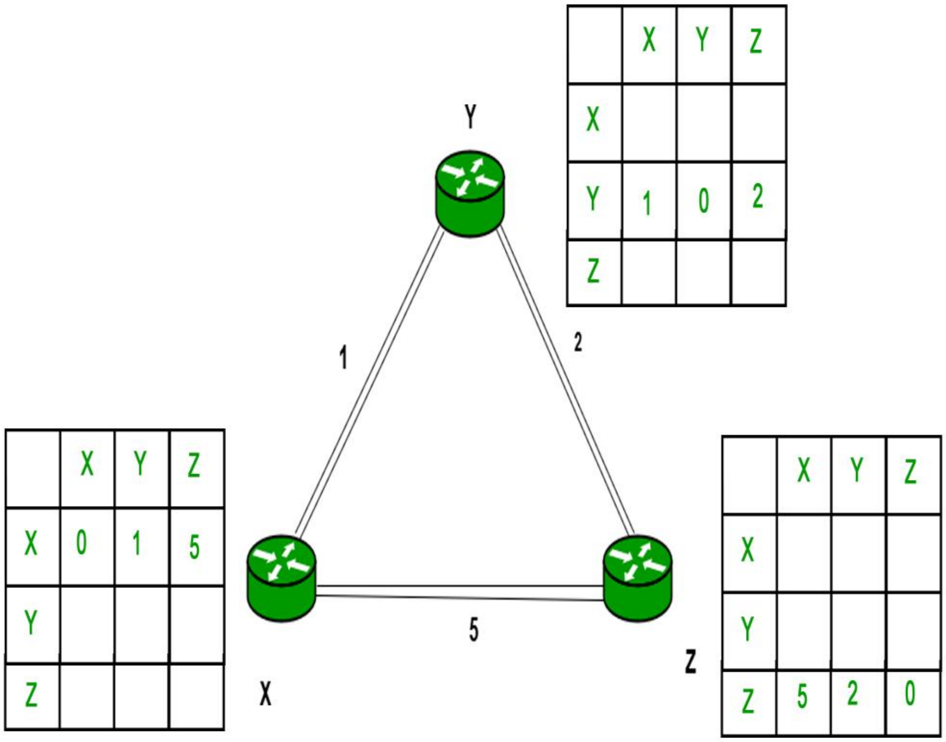
Node x also maintains its neighbors' distance vectors

– For each neighbor v, x maintains Dv = [Dv(y): y ∈ N ]

**Note –**

- From time-to-time, each node sends its own distance vector estimate to neighbors.
- When a node x receives new DV estimate from any neighbor v, it saves v’s distance vector and it updates its own DV using B-F equation:
- Dx(y) = min { C(x,v) + Dv(y), Dx(y) } for each node y ∈ N

**Example –** Consider 3-routers X, Y and Z as shown in figure. Each router have their routing table. Every routing table will contain distance to the destination nodes.



|   | X | Y | Z |
|---|---|---|---|
| X |   |   |   |
| Y | 1 | 0 | 2 |
| Z |   |   |   |

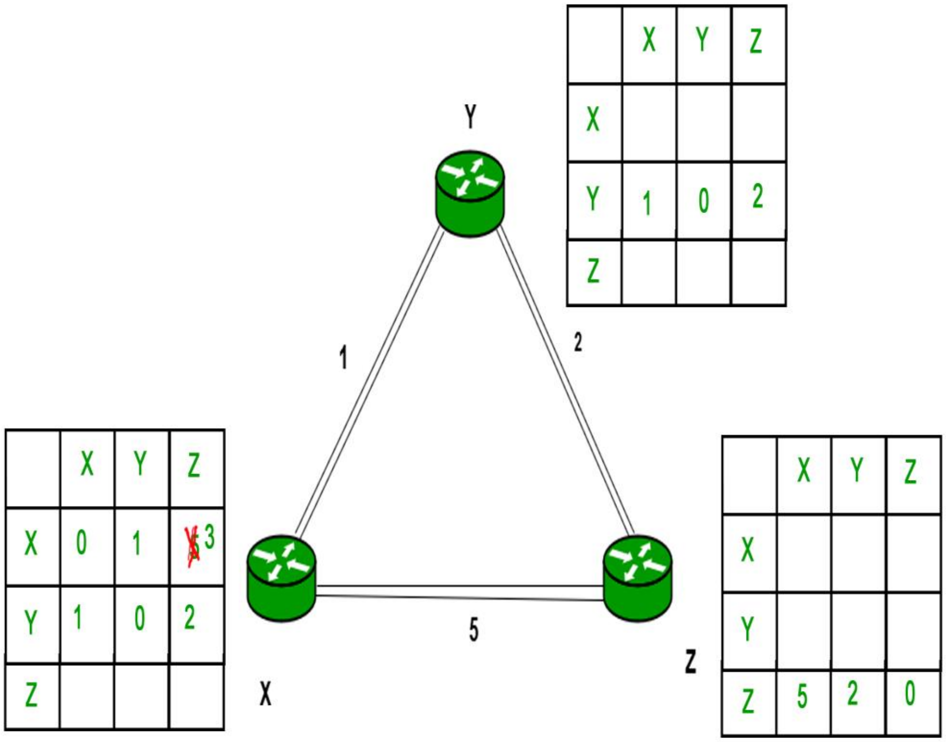
|   | X | Y | Z |
|---|---|---|---|
| X | 0 | 1 | 5 |
| Y |   |   |   |
| Z |   |   |   |

|   | X | Y | Z |
|---|---|---|---|
| X |   |   |   |
| Y |   |   |   |
| Z | 5 | 2 | 0 |

Consider router X , X will share it routing table to neighbors and neighbors will share it routing table to it to X and distance from node X to destination will be calculated using bellmen- ford equation.

Dx(y) = min { C(x,v) + Dv(y)} for each node y ∈ N

As we can see that distance will be less going from X to Z when Y is intermediate node(hop) so it will be update in routing table X.



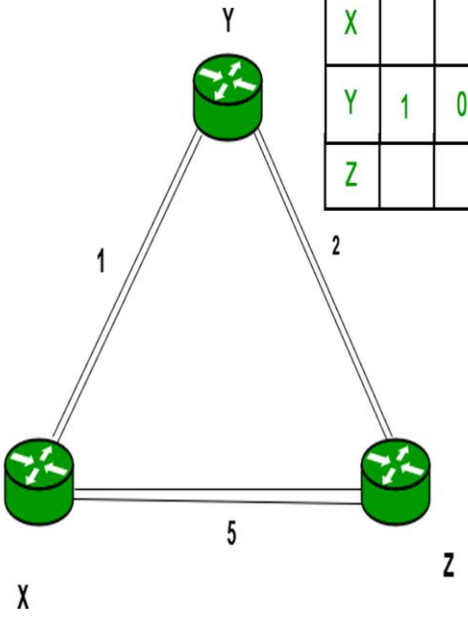
| | X | Y | Z |
|---|---|---|---|
| X | | | |
| Y | 1 | 0 | 2 |
| Z | | | |

| | X | Y | Z |
|---|---|---|---|
| X | 0 | 1 | ~~5~~ 3 |
| Y | 1 | 0 | 2 |
| Z | | | |

| | X | Y | Z |
|---|---|---|---|
| X | | | |
| Y | | | |
| Z | 5 | 2 | 0 |

Similarly for Z also –

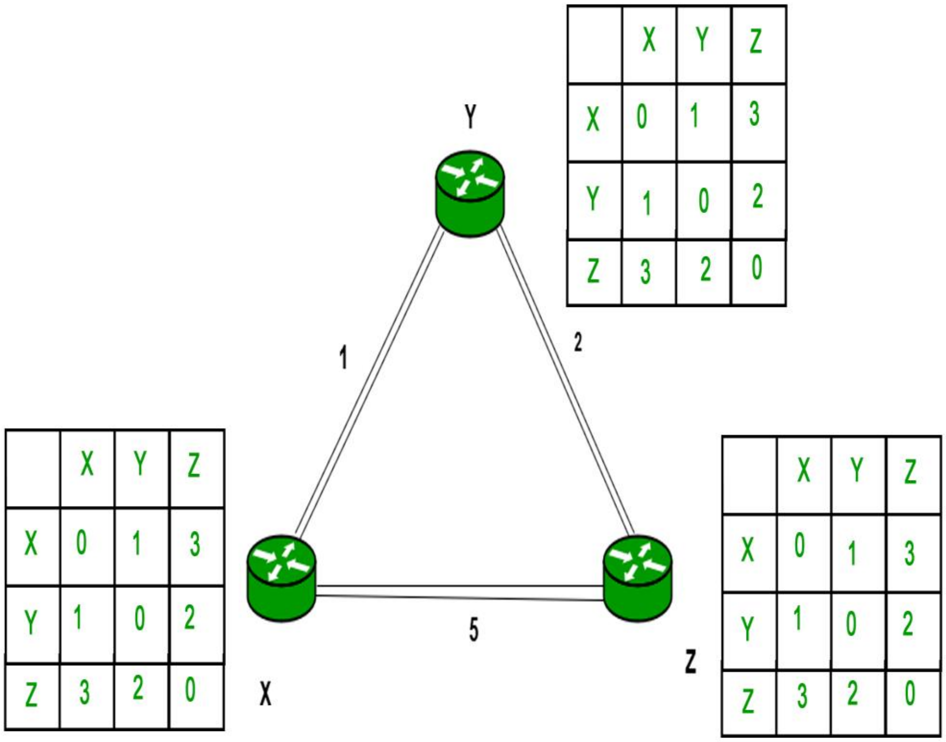
|  | X | Y | Z |
|---|---|---|---|
| X |  |  |  |
| Y | 1 | 0 | 2 |
| Z |  |  |  |



|  | X | Y | Z |
|---|---|---|---|
| X | 0 | 1 | ~~5~~ 3 |
| Y | 1 | 0 | 2 |
| Z | ~~5~~ 3 | 2 | 0 |

|  | X | Y | Z |
|---|---|---|---|
| X |  |  |  |
| Y |  |  |  |
| Z | 5 | 2 | 0 |

Finally the routing table for all –



|   | X | Y | Z |
|---|---|---|---|
| X | 0 | 1 | 3 |
| Y | 1 | 0 | 2 |
| Z | 3 | 2 | 0 |

|   | X | Y | Z |
|---|---|---|---|
| X | 0 | 1 | 3 |
| Y | 1 | 0 | 2 |
| Z | 3 | 2 | 0 |

|   | X | Y | Z |
|---|---|---|---|
| X | 0 | 1 | 3 |
| Y | 1 | 0 | 2 |
| Z | 3 | 2 | 0 |

**Advantages of Distance Vector routing –**

- It is simpler to configure and maintain than link state routing.

**Disadvantages of Distance Vector routing –**

- It is slower to converge than link state.
- It is at risk from the count-to-infinity problem.
- It creates more traffic than link state since a hop count change must be propagated to all routers and processed on each router. Hop count updates take place on a periodic basis, even if there are no changes in the network topology, so bandwidth-wasting broadcasts still occur.
- For larger networks, distance vector routing results in larger routing tables than link state since each router must know about all other routers. This can also lead to congestion on WAN links.