Internetworking

Internetworking refers to the practice of connecting different networks together to create a larger, interconnected network. This enables devices and systems from different locations and networks to communicate and share resources. It's a fundamental concept in modern networking and the foundation of the internet.

Devices play a crucial role in internetworking, as they are the endpoints that send and receive data over the interconnected networks. These devices can vary widely in terms of their capabilities and functions. Some common types of devices involved in internetworking include:

1. **Hubs:** Hubs are basic devices that connect multiple devices in a network, but they lack the intelligence of switches. Data sent to a hub is broadcast to all connected devices.

   In computer networking, a hub is a basic networking device that connects multiple devices within a local area network (LAN). Hubs operate at the physical layer of the OSI (Open Systems Interconnection) model and are designed to receive data packets from one device and broadcast those packets to all other devices connected to the hub. They are considered legacy devices and have largely been replaced by more advanced networking equipment like switches.

   Here are some key characteristics and limitations of hubs:

1. **Broadcasting**: When a hub receives data from one device, it broadcasts that data to all other devices connected to the hub, regardless of whether the data is intended for a specific device. This creates a significant amount of unnecessary traffic and reduces the overall efficiency of the network.
2. **Collision Domain**: Hubs create a single collision domain, which means that if two devices transmit data simultaneously, a collision occurs and the data becomes corrupted. This limits the overall bandwidth and performance of the network.
3. **Bandwidth Sharing**: Since all devices connected to a hub share the same bandwidth, the available bandwidth is divided among all devices. This can lead to slow network performance, especially when multiple devices are actively transmitting data.
4. **No Intelligence**: Hubs lack intelligence and do not have the ability to learn MAC addresses or make decisions about how to forward data. This lack of intelligence contrasts with more advanced devices like switches.
5. **Limited Network Management**: Hubs offer very limited network management and monitoring capabilities. They do not provide features for managing traffic, segmenting the network, or implementing security measures.
6. **Obsolete Technology**: Hubs have largely been replaced by switches, which provide better performance, enhanced features, and improved network management capabilities.

2. **Switches:** Switches operate at the data link layer and are used to connect devices within the same network. They forward data only to the specific device it's intended for, improving efficiency compared to traditional hubs.

   In computer networking, a switch is a network device that operates at the data link layer (Layer 2) of the OSI model. Switches are designed to connect devices within a local area network (LAN) and intelligently forward data packets only to the specific device for which the data is intended. This makes switches more efficient and capable than the older networking device known as a hub.

Here's how a switch works and some of its key features:

1. **MAC Address Learning**: Switches learn the MAC addresses of devices connected to their ports. When a device sends a data packet to the switch, the switch examines the source MAC address of the packet and associates it with the port from which the packet arrived. This allows the switch to build a MAC address table that maps MAC addresses to specific ports.
2. **MAC Address Forwarding**: When the switch receives a data packet with a destination MAC address, it consults its MAC address table to determine which port the destination device is connected to. It then forwards the packet only to that specific port, reducing unnecessary network traffic and improving efficiency.
3. **Broadcast and Multicast Filtering**: While switches avoid unnecessary broadcasts by forwarding data only to the relevant port, they do broadcast multicast traffic (such as when one device sends data to multiple recipients). However, they filter out multicast traffic from ports that don't need the data.
4. **Collision Domain Isolation**: Switches create separate collision domains for each port, which eliminates the collision issues that hubs create in shared networks. This increases network performance and stability.
5. **Bandwidth Allocation**: Each port on a switch operates at its own dedicated bandwidth, meaning that devices connected to different ports can transmit and receive data simultaneously without causing collisions.
6. **VLAN Support**: Switches often support Virtual LANs (VLANs), which allow network administrators to logically segment a single physical switch into multiple virtual networks. This enhances security, network management, and organization.
7. **Port Security**: Some switches provide port security features that allow administrators to control which devices are allowed to connect to specific ports. This helps prevent unauthorized access to the network.
8. **Managed vs. Unmanaged**: Switches can be either managed or unmanaged. Managed switches offer more advanced features like VLAN configuration, QoS (Quality of Service) settings, and remote management capabilities. Unmanaged switches are simpler and do not offer the same level of configurability.
9. **Link Aggregation**: Managed switches often support link aggregation, allowing multiple physical links to be combined into a single logical link for increased bandwidth and redundancy.

3. **Routers:** Routers are devices that connect different networks together and forward data packets between them. They make decisions about the best path for data to travel from source to destination.

   In computer networking, a router is a networking device that connects different networks together and directs data packets between them. Routers operate at the network layer (Layer 3) of the OSI model and are essential for the functioning of the internet and other large-scale networks. They play a crucial role in determining the best path for data to travel from the source to the destination across interconnected networks.

Here's how routers work and some of their key features:

1. **Packet Forwarding**: Routers receive data packets from various sources and use routing algorithms to determine the most efficient path to forward these packets toward their destination. This involves examining the destination IP address of the packet and consulting the router's routing table to find the appropriate next hop.

2. **Routing Tables**: Routers maintain routing tables that contain information about the network topology, including routes to different destinations. These tables are updated dynamically using routing protocols to adapt to changes in the network.
3. **Network Address Translation (NAT)**: Routers often perform NAT, which allows multiple devices within a local network to share a single public IP address for communication with the wider internet. This helps conserve IP addresses and provides a level of security by hiding internal IP addresses from external networks.
4. **Gateway**: Routers can act as gateways between different types of networks, such as connecting a local Ethernet LAN to the global internet, or connecting a wired network to a wireless network.
5. **Firewall and Security**: Many routers include built-in firewall capabilities to filter incoming and outgoing network traffic based on predefined security rules. This helps protect the network from unauthorized access and potential threats.
6. **Quality of Service (QoS)**: Routers can prioritize certain types of network traffic over others, ensuring that critical applications like voice and video calls receive sufficient bandwidth and low latency.
7. **Dynamic Routing Protocols**: Routers use dynamic routing protocols, such as RIP (Routing Information Protocol), OSPF (Open Shortest Path First), and BGP (Border Gateway Protocol), to exchange routing information and adapt to changes in the network topology.
8. **Subnetting and Network Segmentation**: Routers allow for the creation of subnets, which are smaller network segments within a larger network. Subnets help manage and organize network resources while also enhancing security.
9. **IPv6 Transition**: Routers play a role in the transition from IPv4 to IPv6, allowing devices using the newer IPv6 protocol to communicate with devices still using IPv4.
10. **VPN (Virtual Private Network) Support**: Some routers offer VPN capabilities, allowing remote users to securely connect to the local network over the internet.

4. **Gateways:** Gateways are devices or software that translate between different communication protocols or network architectures. They enable communication between networks that use different technologies.

   In computer networking, a gateway is a device or software component that acts as an intermediary between different networks, enabling communication and data transfer between them. Gateways operate at the network layer (Layer 3) of the OSI model and are responsible for routing data between networks that may use different communication protocols, addressing schemes, or technologies.

   Here's how gateways work and some key features:

1. **Protocol Translation**: Gateways are capable of translating data between different network protocols. For example, a gateway can translate data from an IP-based network to a completely different protocol used by another network, allowing them to communicate despite the protocol differences.
2. **Address Translation**: Gateways can also perform address translation to allow devices in one network to communicate with devices in another network using different addressing schemes. This is especially common in cases where private internal IP addresses need to communicate with public external IP addresses on the internet.
3. **Network Interconnection**: Gateways connect networks with different architectures, such as connecting a local Ethernet network to the internet. In this scenario, the gateway performs

tasks like IP address translation, routing, and potentially providing firewall and security functions.

4. **Network Segmentation**: Gateways can help segment networks by acting as the point of entry and exit between different segments. This helps with network management, security, and resource allocation.
5. **Security and Filtering**: Gateways can function as security checkpoints, filtering traffic based on predefined rules and policies. This enhances network security by preventing unauthorized access and blocking potentially harmful traffic.
6. **Firewall Functionality**: Some gateways include firewall features to protect internal networks from external threats and unauthorized access. They can block certain types of traffic, perform intrusion detection, and prevent malicious activities.
7. **Routing**: Gateways use routing algorithms to determine the best path for data to travel from the source network to the destination network. They maintain routing tables that specify how to reach different networks.
8. **Network Address Translation (NAT)**: Many gateways perform NAT to allow multiple devices within a local network to share a single public IP address. This conserves IP addresses and enhances security by hiding internal addresses from external networks.
9. **Proxy Services**: Gateways can provide proxy services, allowing devices in one network to request resources from another network through the gateway. This can help improve security, caching, and performance.
10. **Virtual Private Networks (VPNs)**: Gateways can facilitate VPN connections, allowing remote users or branch offices to securely connect to a main network over the internet.

5. **Bridge:**

In computer networking, a bridge is a network device that connects and filters traffic between two or more network segments at the data link layer (Layer 2) of the OSI model. Bridges are used to extend the size of a network, improve network performance, and segment networks for better organization and management. They operate based on the MAC addresses of devices and are designed to selectively forward data based on these addresses.

Here's how bridges work and some of their key features:

1. **Segmentation and Collision Domains**: Bridges create separate collision domains for each connected network segment. This means that collisions that occur on one segment do not affect the devices on other segments, improving overall network performance and stability.
2. **MAC Address Learning**: Similar to switches, bridges learn the MAC addresses of devices connected to each network segment. They build a MAC address table that maps MAC addresses to specific segments.
3. **Selective Forwarding**: When a bridge receives a data frame, it checks its MAC address table to determine which segment the destination MAC address belongs to. The bridge then forwards the frame only to the appropriate segment, reducing unnecessary network traffic.
4. **Filtering and Isolation**: Bridges can be used to filter out unwanted network traffic. For example, they can prevent broadcast storms from affecting the entire network by containing them within a single segment. They also provide isolation between network segments, enhancing security and privacy.
5. **Network Expansion**: Bridges allow networks to expand by connecting multiple segments. This is particularly useful when the physical distance between devices is too great for a single network segment or when the number of devices on a single segment becomes too large to manage efficiently.

6. **Reducing Broadcast Domain**: Bridges help reduce the size of broadcast domains. In a large network, broadcast messages can consume significant bandwidth and lead to network congestion. By segmenting the network, bridges limit the scope of broadcast messages.
7. **Transparent Operation**: Bridges operate transparently to devices connected to them. Devices are unaware that they are on different segments, as the bridge makes them appear as a single logical network.
8. **Bridge vs. Switch**: While bridges and switches both operate at Layer 2 and perform similar functions, the term "bridge" is often used to refer to a simpler device that connects two network segments, while "switch" typically refers to a more advanced device that connects multiple devices within a single segment.
9. **Spanning Tree Protocol (STP)**: Some bridges implement STP, a protocol that prevents loops in bridged networks. Loops can cause broadcast storms and network instability, and STP helps ensure a loop-free topology.

6. **Modems:** Modems are used to modulate and demodulate digital data for transmission over analog communication channels, such as telephone lines or cable systems. They're commonly used for connecting to the internet via DSL or cable connections.
7. **Access Points (APs):** APs provide wireless connectivity to a wired network. They allow Wi-Fi-enabled devices to connect to a local area network (LAN) without requiring physical cables.
8. **Network Interface Cards (NICs):** NICs are hardware components that enable computers to connect to a network. They provide the physical interface for devices to send and receive data over a network.
9. **Servers and Clients:** Servers are powerful computers that provide services, resources, or data to other devices on the network (clients). Clients make requests to servers for things like web pages, files, or email services.
10. **IoT Devices:** Internet of Things (IoT) devices are everyday objects embedded with sensors, software, and network connectivity to exchange data. Examples include smart thermostats, wearable devices, and connected appliances.
11. **Load Balancers:** Load balancers distribute incoming network traffic across multiple servers to ensure efficient resource utilization, improved performance, and high availability.
12. **Proxy Servers:** Proxy servers act as intermediaries between clients and servers, forwarding requests and responses. They can enhance security, cache data, and provide anonymity.

Differences between hubs and switches

Hubs and switches are both network devices used to connect multiple devices within a local area network (LAN), but they differ significantly in terms of functionality, performance, and efficiency. **Here are the key differences between hubs and switches:**

1. **Functionality and Data Handling**:
    - **Hub**: A hub operates at the physical layer (Layer 1) of the OSI model. It simply receives incoming data packets on one port and broadcasts them to all other ports, regardless of whether the data is intended for a specific device or not. This results in a lot of unnecessary network traffic, as all devices connected to the hub receive all data packets.
    - **Switch**: A switch operates at the data link layer (Layer 2) of the OSI model. It intelligently examines the MAC addresses of incoming data packets and forwards them only to the specific port where the intended recipient device is connected. This

selective forwarding reduces unnecessary network congestion and improves overall network efficiency.

2. **Collision Handling**:
    - **Hub**: Hubs create a single collision domain. This means that if two devices connected to the hub transmit data simultaneously, a collision occurs, and both sets of data become corrupted. Collisions reduce network efficiency and can lead to performance issues.
    - **Switch**: Switches create separate collision domains for each port. This means that collisions are limited to the devices connected to a particular port, increasing network performance and stability.
3. **Broadcasting**:
    - **Hub**: Hubs broadcast data to all connected devices. This results in more broadcast traffic, which can consume bandwidth and lead to inefficiencies.
    - **Switch**: Switches forward data only to the specific port where the recipient device is located. This reduces broadcast traffic and minimizes unnecessary data consumption.
4. **Network Efficiency**:
    - **Hub**: Hubs are less efficient due to their broadcasting nature. They cause more network congestion and reduce overall network performance.
    - **Switch**: Switches are more efficient because they forward data only to the intended device, reducing unnecessary traffic and improving network performance.
5. **MAC Address Learning and Filtering**:
    - **Hub**: Hubs do not have the ability to learn MAC addresses or make decisions based on MAC addresses. They simply forward data to all ports.
    - **Switch**: Switches learn MAC addresses and build MAC address tables to intelligently forward data to the correct port based on the destination MAC address. This eliminates unnecessary data transmission and improves efficiency.
6. **Security and Segmentation**:
    - **Hub**: Hubs do not provide any security or segmentation features. All devices connected to a hub are part of the same network segment.
    - **Switch**: Switches support features like VLANs (Virtual LANs), which allow network segmentation and enhanced security by isolating groups of devices from each other.

Network Address

A **computer network** is a group of some interconnected computers that are sharing a common or different resources provided on or by network nodes. These sharing or communication between the machines is governed by some set of rules or network protocols. These computers or machines are identified by network addresses, and may have hostnames.

A Network Address is a logical or physical address that uniquely identifies a host or a machine in a telecommunication network. A network may also not be unique and can contain some structural and hierarchical information of the node in the network. Internet protocol (IP) address, media access control (MAC) address and telephone numbers are some basic examples of network addresses. It can be of numeric type or symbolic or both in some cases.

- Network Addressing is one of the major responsibilities of the network layer.
- Network addresses are always logical, i.e., software-based addresses.

- A host is also known as end system that has one link to the network. The boundary between the host and link is known as an interface. Therefore, the host can have only one interface.
- A router is different from the host in that it has two or more links that connect to it. When a router forwards the datagram, then it forwards the packet to one of the links. The boundary between the router and link is known as an interface, and the router can have multiple interfaces, one for each of its links. Each interface is capable of sending and receiving the IP packets, so IP requires each interface to have an address.
- Each IP address is 32 bits long, and they are represented in the form of "dot-decimal notation" where each byte is written in the decimal form, and they are separated by the period. An IP address would look like 193.32.216.9 where 193 represents the decimal notation of first 8 bits of an address, 32 represents the decimal notation of second 8 bits of an address.

Types of IP Address

IP Address is of two types:

1. IPv4: Internet Protocol version 4. It consists of 4 numbers separated by the dots. Each number can be from 0-255 in decimal numbers. But computers do not understand decimal numbers, they instead change them to binary numbers which are only 0 and 1. Therefore, in binary, this (0-255) range can be written as (00000000 – 11111111). Since each number N can be represented by a group of 8-digit binary digits. So, a whole IPv4 binary address can be represented by 32-bits of binary digits. In IPv4, a unique sequence of bits is assigned to a computer, so a total of (2^32) devices approximately = 4,294,967,296 can be assigned with IPv4.

IPv4 can be written as:

189.123.123.90

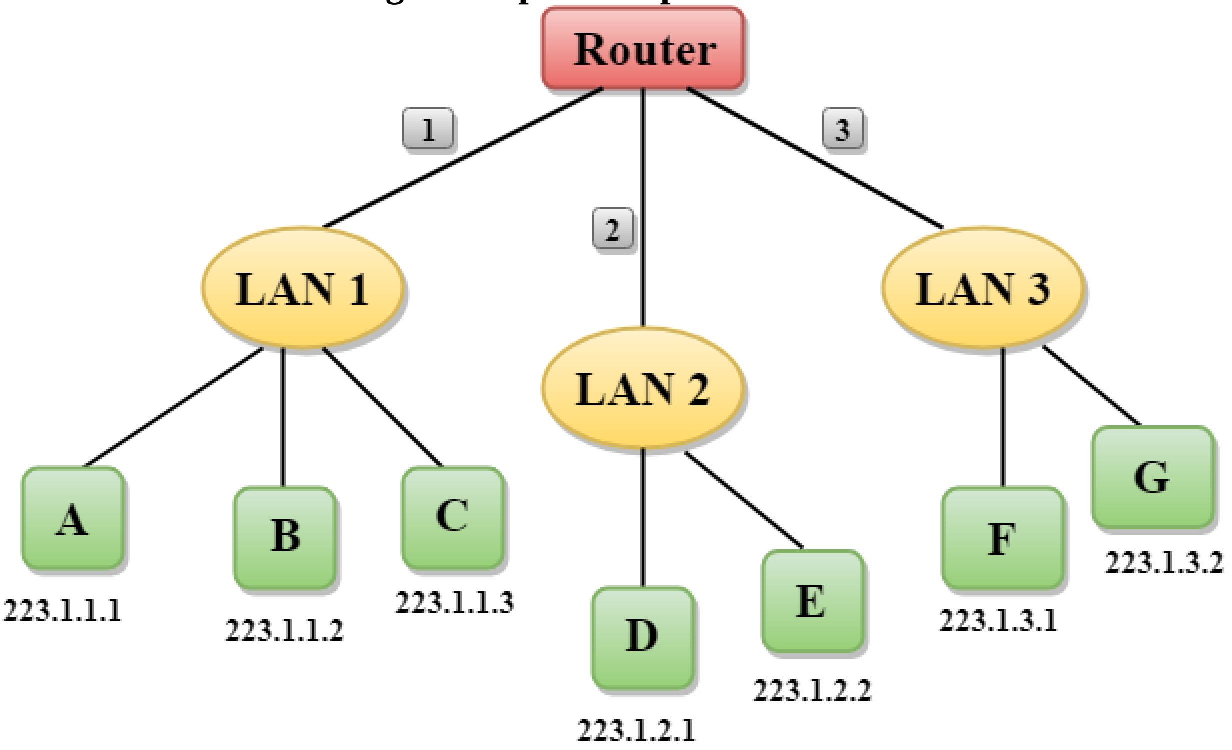
Classes of IPv4 Address: There are around 4.3 billion IPv4 addresses and managing all those addresses without any scheme is next to impossible. Let’s understand it with a simple example. If you have to find a word from a language dictionary, how long will it take? Usually, you will take less than 5 minutes to find that word. You are able to do this because words in the dictionary are organized in alphabetical order. If you have to find out the same word from a dictionary that doesn’t use any sequence or order to organize the words, it will take an eternity to find the word. If a dictionary with one billion words without order can be so disastrous, then you can imagine the pain behind finding an address from 4.3 billion addresses. For easier management and assignment IP addresses are organized in numeric order and divided into the following 5 classes :

IP Class	Address Range	Maximum number of networks
Class A	0-126	127 (2^7-1)
Class B	128-191	16384
Class C	192-223	2097152
Class D	224-239	Reserve for multitasking

IP Class	Address Range	Maximum number of networks
Class E	240-254	Reserved for Research and development

A loopback address is a distinct reserved IP address range that starts from 127.0.0.0 ends at 127.255.255.255 though 127.255.255.255 is the broadcast address for 127.0.0.0/8. The loopback addresses are built into the IP domain system, enabling devices to transmit and receive the data packets. The loopback address 127.0.0.1 is generally known as localhost.

Let's understand through a simple example.



- In the above figure, a router has three interfaces labeled as 1, 2 & 3 and each router interface contains its own IP address.
- Each host contains its own interface and IP address.
- All the interfaces attached to the LAN 1 is having an IP address in the form of 223.1.1.xxx, and the interfaces attached to the LAN 2 and LAN 3 have an IP address in the form of 223.1.2.xxx and 223.1.3.xxx respectively.
- Each IP address consists of two parts. The first part (first three bytes in IP address) specifies the network and second part (last byte of an IP address) specifies the host in the network.

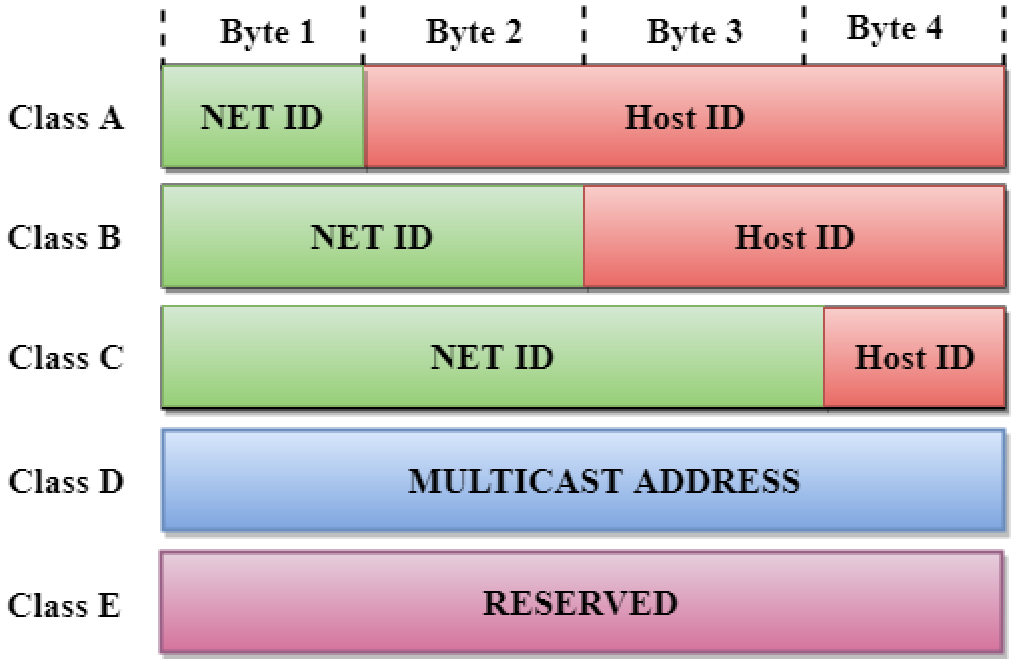
Classful Addressing

An IP address is 32-bit long. An IP address is divided into sub-classes:

- Class A
- Class B
- Class C
- Class D
- Class E

An ip address is divided into two parts:

- **Network ID:** It represents the number of networks.
- **Host ID:** It represents the number of hosts.



In the above diagram, we observe that each class have a specific range of IP addresses. The class of IP address is used to determine the number of bits used in a class and number of networks and hosts available in the class.

Class A

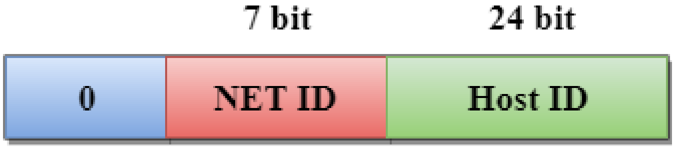
In Class A, an IP address is assigned to those networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.

The total number of networks in Class A = 2^7 = 128 network address

The total number of hosts in Class A = 2^{24} - 2 = 16,777,214 host address



Class B

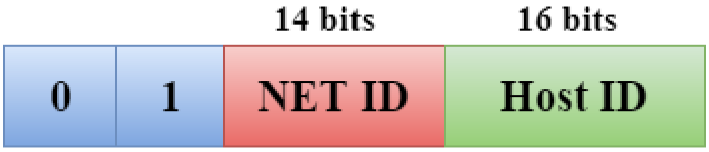
In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks.

- The Network ID is 16 bits long.
- The Host ID is 16 bits long.

In Class B, the higher order bits of the first octet is always set to 10, and the remaining14 bits determine the network ID. The other 16 bits determine the Host ID.

The total number of networks in Class B = 2^{14} = 16384 network address

The total number of hosts in Class B = 2^{16} - 2 = 65534 host address



Class C

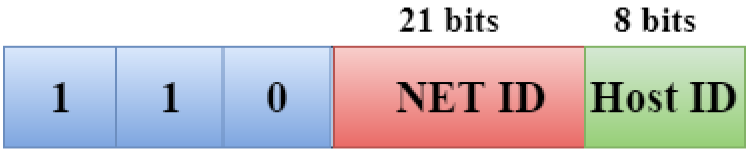
In Class C, an IP address is assigned to only small-sized networks.

- The Network ID is 24 bits long.
- The host ID is 8 bits long.

In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID. The 8 bits of the host ID determine the host in a network.

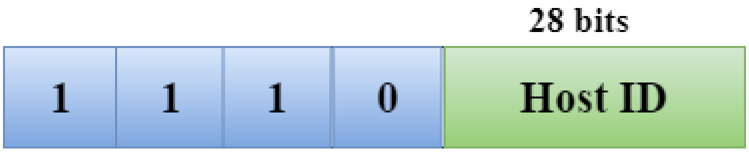
The total number of networks = 2^{21} = 2097152 network address

The total number of hosts = 2^{8} - 2 = 254 host address



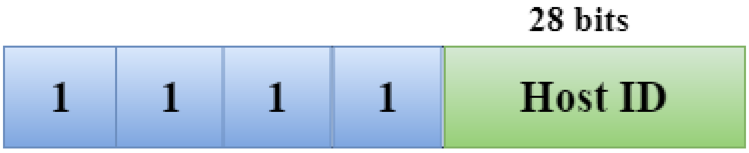
Class D

In Class D, an IP address is reserved for multicast addresses. It does not possess subnetting. The higher order bits of the first octet is always set to 1110, and the remaining bits determines the host ID in any network.



Class E

In Class E, an IP address is used for the future use or for the research and development purposes. It does not possess any subnetting. The higher order bits of the first octet is always set to 1111, and the remaining bits determines the host ID in any network.



Rules for assigning Host ID:

The Host ID is used to determine the host within any network. The Host ID is assigned based on the following rules:

- The Host ID must be unique within any network.
- The Host ID in which all the bits are set to 0 cannot be assigned as it is used to represent the network ID of the IP address.
- The Host ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

Rules for assigning Network ID:

If the hosts are located within the same local network, then they are assigned with the same network ID. The following are the rules for assigning Network ID:

- The network ID cannot start with 127 as 127 is used by Class A.
- The Network ID in which all the bits are set to 0 cannot be assigned as it is used to specify a particular host on the local network.
- The Network ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

Classful Network Architecture

Class	**Higher bits**	**NET ID bits**	**HOST ID bits**	**No.of networks**	**No.of hosts per network**	**Range**
A	0	8	24	2^{7}	2^{24}	0.0.0.0 to 127.255.255.255
B	10	16	16	2^{14}	2^{16}	128.0.0.0 to 191.255.255.255
C	110	24	8	2^{21}	2^{8}	192.0.0.0 to 223.255.255.255
D	1110	Not Defined	Not Defined	Not Defined	Not Defined	224.0.0.0 to 239.255.255.255
E	1111	Not Defined	Not Defined	Not Defined	Not Defined	240.0.0.0 to 255.255.255.255

2. IPv6: But, there is a problem with the IPv4 address. With IPv4, we can connect only the above number of 4 billion devices uniquely, and apparently, there are much more devices in the world to be connected to the internet. So, gradually we are making our way to **IPv6 Address** which is a 128-bit IP address. In human-friendly form, IPv6 is written as a group of 8 hexadecimal numbers separated with colons(:). But in the computer-friendly form, it can be written as 128 bits of 0s and 1s. Since, a unique sequence of binary digits is given to computers, smartphones, and other devices to be connected to the internet. So, via IPv6 a total of (2^128) devices can be assigned with unique addresses which are actually more than enough for upcoming future generations.

IPv6 can be written as:

2011:0bd9:75c5:0000:0000:6b3e:0170:8394

Classification of IP Address

An IP address is classified into the following types:

1. Public IP Address: This address is available publicly and it is assigned by your network provider to your router, which further divides it to your devices. Public IP Addresses are of two types,

- **Dynamic IP Address:** When you connect a smartphone or computer to the internet, your Internet Service Provider provides you an IP Address from the range of available IP Addresses. Now, your device has an IP Address and you can simply connect your device to the Internet and send and receive data to and from your device. The very next time when you try to connect to the internet with the same device, your provider provides you with different IP Addresses to the same device and also from the same available range. Since IP Address keeps on changing every time when you connect to the internet, it is called a Dynamic IP Address.
- **Static IP Address:** Static address never changes. They serve as a permanent internet address. These are used by DNS servers. What are DNS servers? Actually, these are computers that help you to open a website on your computer. Static IP Address provides information such as device is located on which continent, which country, which city, and which Internet Service Provider provides internet connection to that particular device. Once, we know who is the ISP, we can trace the location of the device connected to the internet. Static IP Addresses provide less security than Dynamic IP Addresses because they are easier to track.

2. Private IP Address: This is an internal address of your device which are not routed to the internet and no exchange of data can take place between a private address and the internet.

3. Shared IP addresses: Many websites use shared IP addresses where the traffic is not huge and very much controllable, they decide to rent it to other similar websites so to make it cost-friendly. Several companies and email sending servers use the same IP address (within a single mail server) to cut down the cost so that they could save for the time the server is idle.

4. Dedicated IP addresses: A dedicated IP Address is an address used by a single company or an individual which gives them certain benefits using a private Secure Sockets Layer (SSL) certificate which is not in the case of a shared IP address. It allows to access the website or log in via File Transfer Protocol (FTP) by IP address instead of its domain name. It increases the performance of the website when the traffic is high. It also protects from a shared IP address that is black-listed due to spam.

What is Subnetting in Computer Networks?

Subnetting in computer networks is an important technique that allows network administrators to divide a larger network into smaller subnetworks. Subnetting in computer networks is a technique that allows a single network to be divided into multiple smaller networks, known as subnets.

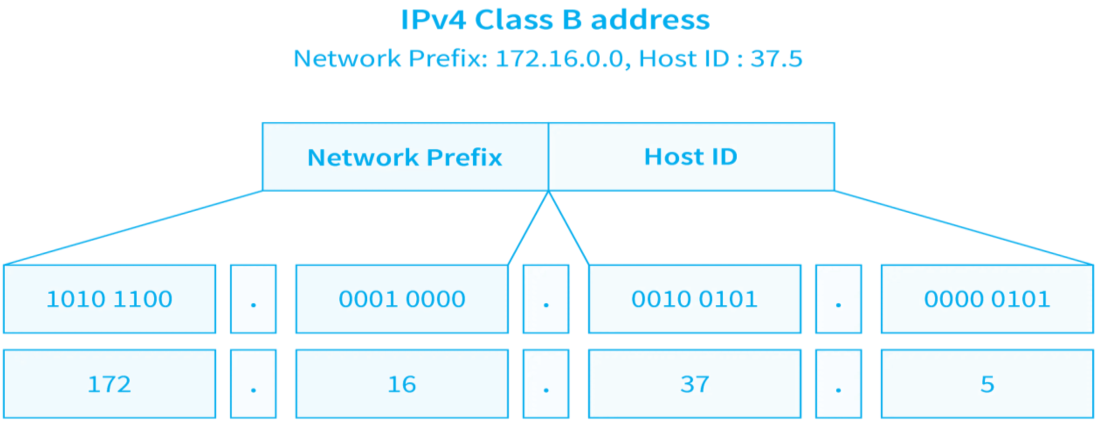
Overall, subnetting in computer networks is a technique used to better organize, allocate resources, and improve security.

How does Subnetting in Computer Networks Work?

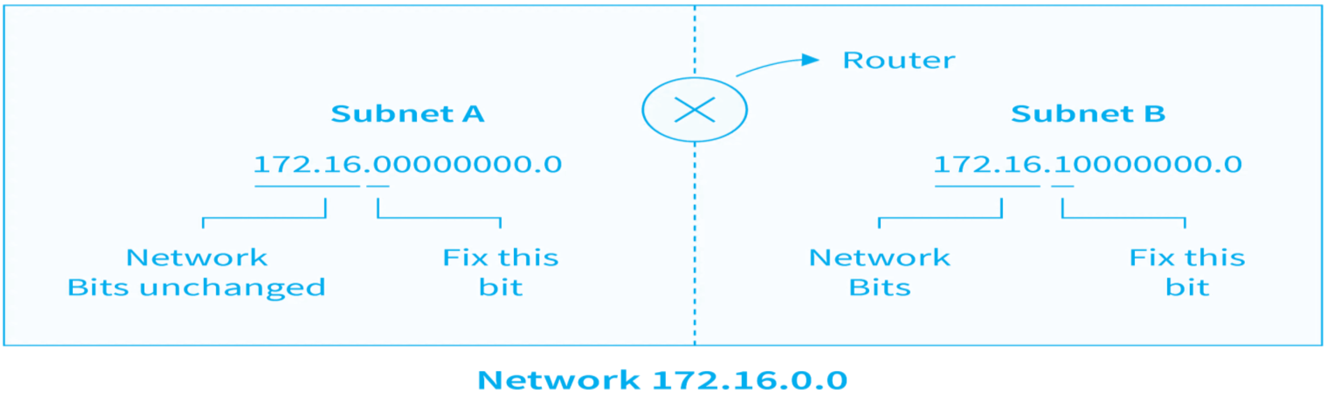
Subnetting, as we now know, divides a network into small subnets. Routers are used to communicate between subnets, and each subnet allows its connected devices to communicate with one another. The size of a subnet is decided by the network technology used and the number of connections required. Each organization is responsible for determining the number and size of subnets it generates within the constraints of the address space available for its use.

Let’s look at how subnetting divides a network into subnets.

An IP address is made up of two fields: a Network Prefix (also known as the Network ID) and a Host ID. The way the Network Prefix and the Host ID are separated depends on whether the address belongs to Class A, B, or C. The picture shown below illustrates an IPv4 Class B address with a value of 172.16.37.5. The first two octets (172.16) represent the network prefix, while the last two octets (37.5) represent the host ID.



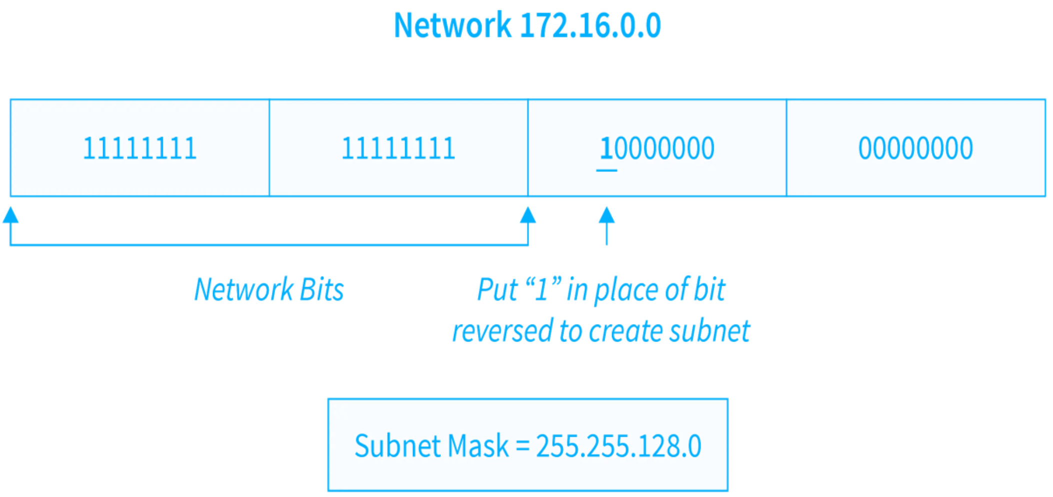
To generate subnets, we commonly fix the MSB (Most Significant Bit) bits of the Host ID. The image below illustrates how we can create two network subnets by fixing one of the host’s Most Significant Bit (MSB) bits. We cannot modify network bits because doing so changes the entire network.



A subnet mask is needed to identify a subnet, which is calculated by substituting ‘1’ for all Network ID bits and the number of bits reserved in Host ID to generate the subnet. The subnet mask is responsible for routing data packets from the internet to the desired subnet network. A subnet mask also determines which part of an address will be used as the Subnet ID. To apply the subnet mask to the entire network address, a binary AND operation is performed. AND operations work by assuming that output is "true" if both inputs are "true." If not, "false" is returned.

This generates the Subnet ID. Routers use the Subnet ID to figure out the most efficient route between different subnetworks.

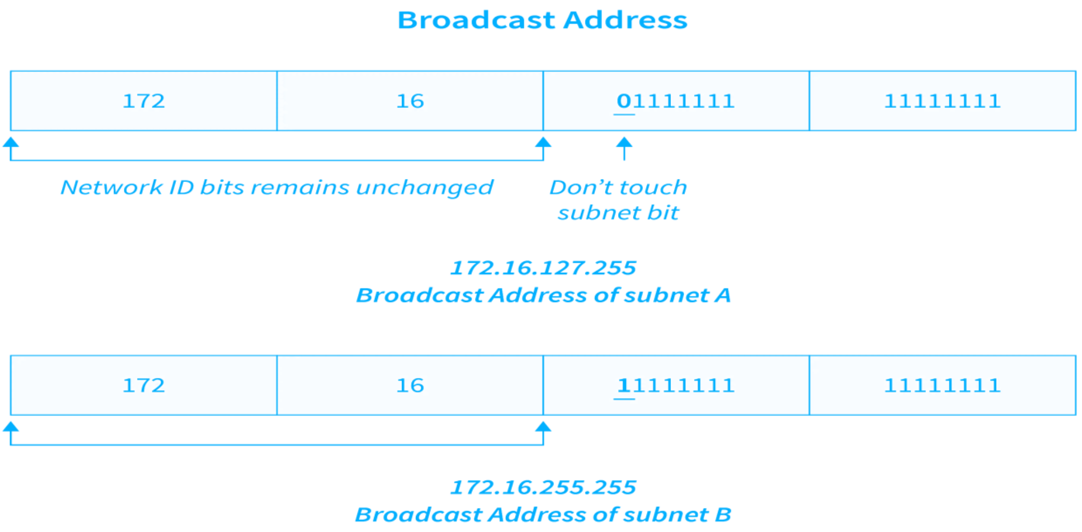
Refer to the illustration of generating a subnet mask for further information.



To build variable-length subnets, we use permutations on the number of bits reserved for subnet creation. This is referred to as Variable Length Subnet Masking (VLSM).

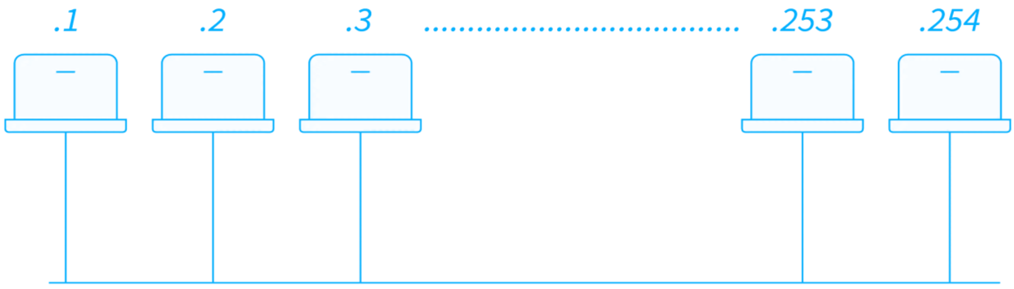
A subnet’s broadcast address is determined by setting all of the remaining bits of Host Id as’1′ after some bits are reserved to represent the subnet.

See the below image of the Broadcast Address.



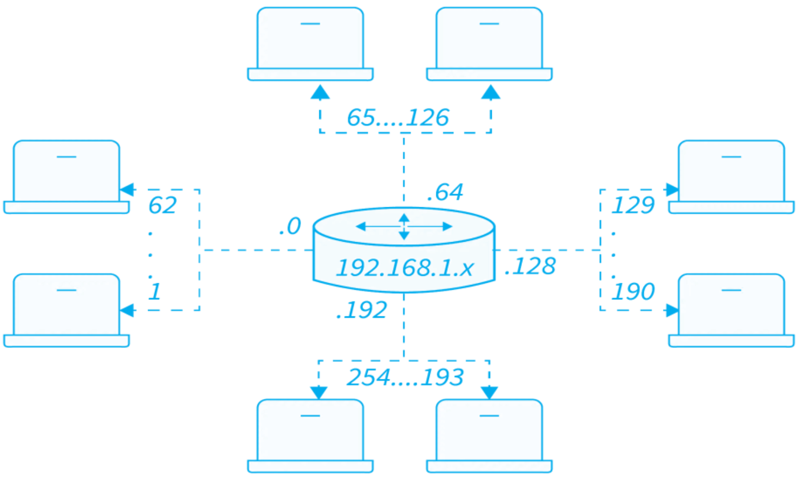
Example of Subnetting

Let’s look at a simple situation to better grasp subnetting. A small organization is divided into four departments: the technology department, the sales and marketing department, the finance department, and the HR department. Every department has 50 employees. The organizations made use of a private class C IP network (with network ID 192.168.1.0). If there is no subnetting, all computers will operate in a single large network. It becomes difficult for the network administrator to manage the task because if he broadcasts a message to the system, it will be forwarded to all departments. Subnetting is used to solve this type of difficulty.



A Single Large Class C IP Network

After subnetting, the network will look something like this:



Uses of Subnetting in Computer Networks

Subnetting in computer networks has several uses, including:

- **Efficient use of IP addresses:** Subnetting allows for the creation of smaller networks within a larger network, which helps to conserve IP addresses.
- **Improved network performance:** By creating smaller networks, subnetting can help reduce network traffic and improve overall network performance.

- **Enhanced security:** Subnetting can improve network security by separating different parts of the network into smaller subnetworks, making it harder for unauthorized access.
- **Flexibility:** Subnetting allows for the creation of networks of different sizes, depending on the specific needs of the organization.
- **Routing efficiency:** Subnetting can improve routing efficiency by allowing routers to route traffic directly to the appropriate subnet instead of broadcasting it to the entire network.
- **Improved fault tolerance:** Subnetting can help improve fault tolerance by isolating network problems to specific subnets and preventing them from affecting the entire network.

Advantages of Subnetting in Computer Networks

There are several advantages of subnetting in computer networks, including:

- **Better Organization and Management:** Subnetting allows network administrators to divide a larger network into smaller, more manageable subnets. This makes it easier to allocate resources, troubleshoot network issues, and manage network traffic.
- **Improved Network Performance:** Subnetting can improve network performance by reducing network congestion and limiting the amount of broadcast traffic on the network. With smaller subnets, broadcast traffic is limited to only the devices on that subnet, reducing the overall amount of network traffic.
- **Enhanced Security:** Subnetting improves network security by isolating traffic between subnets and restricting access to sensitive information. This makes it more difficult for unauthorized users to access sensitive data or launch attacks on the network.
- **More Efficient Use of IP Addresses:** By dividing a larger network into smaller subnets, network administrators can make more efficient use of IP addresses. This is particularly important as the number of devices connected to the network continues to grow.
- **Flexibility:** Subnetting provides network administrators with greater flexibility in how they manage their networks. They can allocate resources more efficiently, troubleshoot issues more effectively, and make changes to the network more easily.

Overall, we can confidently say subnetting in computer networks is valuable for network administrators.

Disadvantages of Subnetting in Computer Networks

Although there are several advantages of subnetting, there are also some potential disadvantages of subnetting in computer networks that network administrators should consider:

- **Increased Complexity:** Subnetting can add complexity to network design and configuration, which can make it more difficult for network administrators to manage the network.
- **Requires Additional Resources:** Subnetting requires additional resources such as routers and switches, which can increase the cost of building and maintaining the network.
- **Risk of Misconfiguration:** Subnetting requires careful planning and configuration to ensure that subnets are properly set up and configured. Misconfiguration can lead to network issues, security vulnerabilities, and other problems.
- **Reduced Broadcast Capability:** By dividing a network into smaller subnets, the overall broadcast capability of the network is reduced. This can make it more difficult to broadcast messages to all devices on the network.
- **Potential for Subnet Overlap:** If subnets are not properly designed and configured, there is a risk of subnet overlap, which can lead to network issues and security vulnerabilities.

Routing

Routing is a process that is performed by layer 3 (or network layer) devices in order to deliver the packet by choosing an optimal path from one network to another.

- 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.

Classification of Routing in Computer Networks

There are three types of Routing:

1. Static Routing
2. Default Routing
3. Dynamic Routing

Static Routing

Another name for **Static Routing** is **Nonadaptive Routing**. Static routing is the process of manually joining routes to the routing table.

Let's suppose our computer wants to connect with another computer, and there are ten different networks between them. When we want to connect both the computers, we have to give the information manually about the networks through which we want to connect to the router, then only the exchange of data can be possible. This process is said to be Static Routing.

Advantages:

- The administrator manually sets it up.
- It is safe and quick.
- There is no bandwidth usage between routers.
- Because there is no routing overhead for the router CPU, a less expensive router can be used for routing.

Disadvantages:

- Utilized in small network
- Everything has to be set up manually.

Dynamic Routing

Another name of **Dynamic Routing** is **Adaptive Routing**. Dynamic routing automatically adjusts routes based on the current state of the route in the routing table. Protocols are used in dynamic routing to discover network destinations and the routes that will take them there. The best examples of dynamic routing protocols are **RIP** and **OSPF**. If one of the network routes fails, it will make automatic adjustments to reach the network's destination.

Let's suppose our computer wants to connect with another computer. There are ten different networks between them, so the path they have to follow while connecting is chosen automatically, assuring security, collision, hacking, and many more.

Advantages:

- There is no need to understand the networks.
- Its setup is easy.
- Administrator work is less.
- It is used for big organizations.
- It is more effective at determining the best path in response to changes in the condition or topology.

Disadvantages:

- More bandwidth is consumed when interacting with other neighbours.
- Dynamic routing necessitates the use of more resources such as CPU, RAM, and bandwidth. That's why it's more expensive.
- Dynamic routing introduces more complexity to the network, especially during implementation.

Default Routing

It is the method in which the router is set up to send all packets to a single router (next hop). It makes no difference to which network the packet belongs to; it is forwarded to the router that is set to default routing. It is typically used in conjunction with stub routers. A stub router only has one route to all other networks.

It is set up for unknown locations or end locations. It is the least preferred Routing. It helps in minimizing the size of your routing table.

Advantages:

- If there are no fixed routes in the routing table, the default route can be helpful. The default route is used for all packet traffic with an unknown destination in the routing table.
- It is suitable for packet filtering, firewalling, and proxy servers as it is configured for unknown destinations.

Disadvantages:

- If the network is overly complex, the setup will also be difficult.
- The network topology determines it.

What is Routing Table in Router?

A routing table determines the path for a given packet with the help of an IP address of a device and necessary information from the table and sends the packet to the destination network. The routers have the internal memory that is known as Random Access Memory (RAM). All the information of the routing table is stored in RAM of routers.

For example:

Destination (Network ID)	Subnet mask	Interface
200.1.2.0	255.255.255.0	Eth0
200.1.2.64	255.255.255.128	Eth1
200.1.2.128	255.255.255.255	Eth2
Default		Eth3

A routing table contains the following entities:

- It contains an IP address of all routers which are required to decide the way to reach the destination network.
- It includes extrovert interface information.
- Furthermore, it is also contained IP addresses and subnet mask of the destination host.

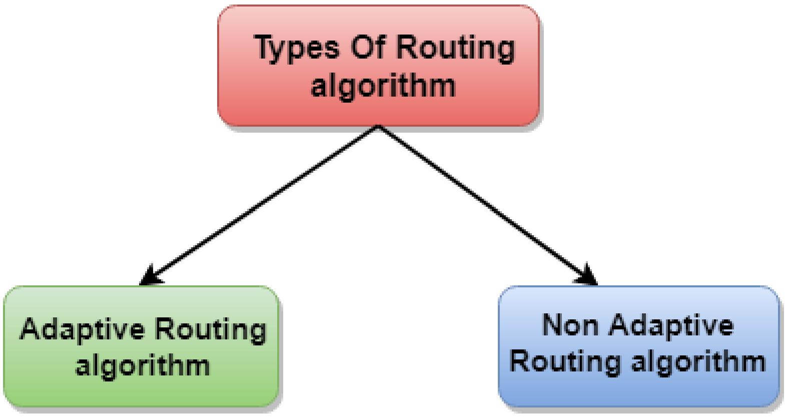
Routing algorithm

- In order to transfer the packets from source to the destination, the network layer must determine the best route through which packets can be transmitted.
- Whether the network layer provides datagram service or virtual circuit service, the main job of the network layer is to provide the best route. The routing protocol provides this job.
- The routing protocol is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the "least-cost path" from source to the destination.
- Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.

Classification of a Routing algorithm

The Routing algorithm is divided into two categories:

- Adaptive Routing algorithm
- Non-adaptive Routing algorithm


Types Of Routing algorithm
Adaptive Routing algorithm
Non Adaptive Routing algorithm

Adaptive Routing algorithm

- An adaptive routing algorithm is also known as dynamic routing algorithm.
- This algorithm makes the routing decisions based on the topology and network traffic.
- The main parameters related to this algorithm are hop count, distance and estimated transit time.

An adaptive routing algorithm can be classified into three parts:

- **Centralized algorithm:** It is also known as global routing algorithm as it computes the least-cost path between source and destination by using complete and global knowledge about the network. This algorithm takes the connectivity between the nodes and link cost as input, and this information is obtained before actually performing any calculation. **Link state algorithm** is referred to as a centralized algorithm since it is aware of the cost of each link in the network.
- **Isolation algorithm:** It is an algorithm that obtains the routing information by using local information rather than gathering information from other nodes.
- **Distributed algorithm:** It is also known as decentralized algorithm as it computes the least-cost path between source and destination in an iterative and distributed manner. In the decentralized algorithm, no node has the knowledge about the cost of all the network links. In the beginning, a node contains the information only about its own directly attached links and through an iterative process of calculation computes the least-cost path to the destination. A Distance vector algorithm is a decentralized algorithm as it never knows the complete path from source to the destination, instead it knows the direction through which the packet is to be forwarded along with the least cost path.

Non-Adaptive Routing algorithm

- Non Adaptive routing algorithm is also known as a static routing algorithm.
- When booting up the network, the routing information stores to the routers.
- Non Adaptive routing algorithms do not take the routing decision based on the network topology or network traffic.

The Non-Adaptive Routing algorithm is of two types:

Flooding: In case of flooding, every incoming packet is sent to all the outgoing links except the one from it has been reached. The disadvantage of flooding is that node may contain several copies of a particular packet.

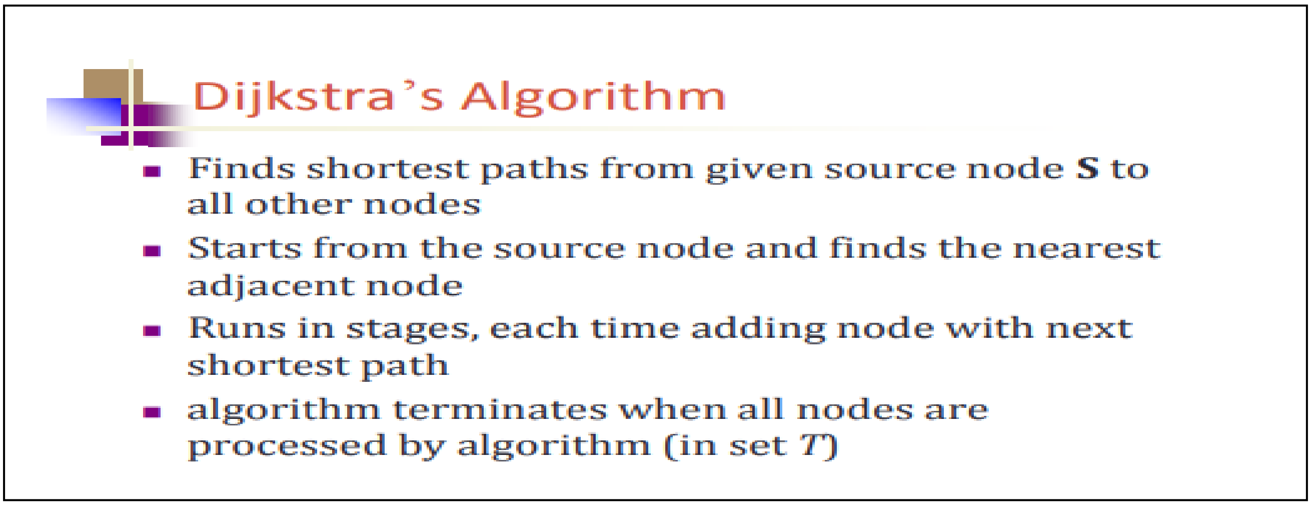
Random walks: In case of random walks, a packet sent by the node to one of its neighbors randomly. An advantage of using random walks is that it uses the alternative routes very efficiently.

Shortest Path Routing:

- Build a graph of network
- Each node represent a router
- Each arc represent a link
- Find shortest path between the two nodes

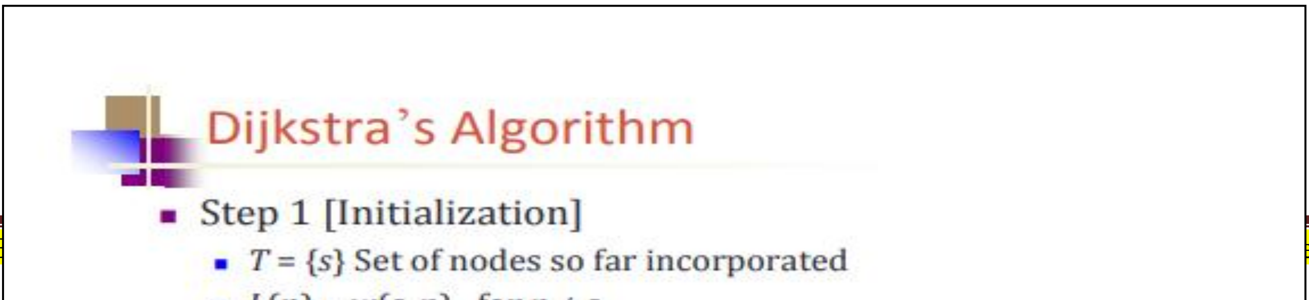
Shortest Path Routing

- For a pair of communicating hosts, there is av shortest path between them
- Shortness may be defined by:
    - number of hops
    - geographic distance
    - mean queuing/transmission delay
    - bandwidth
    - cost



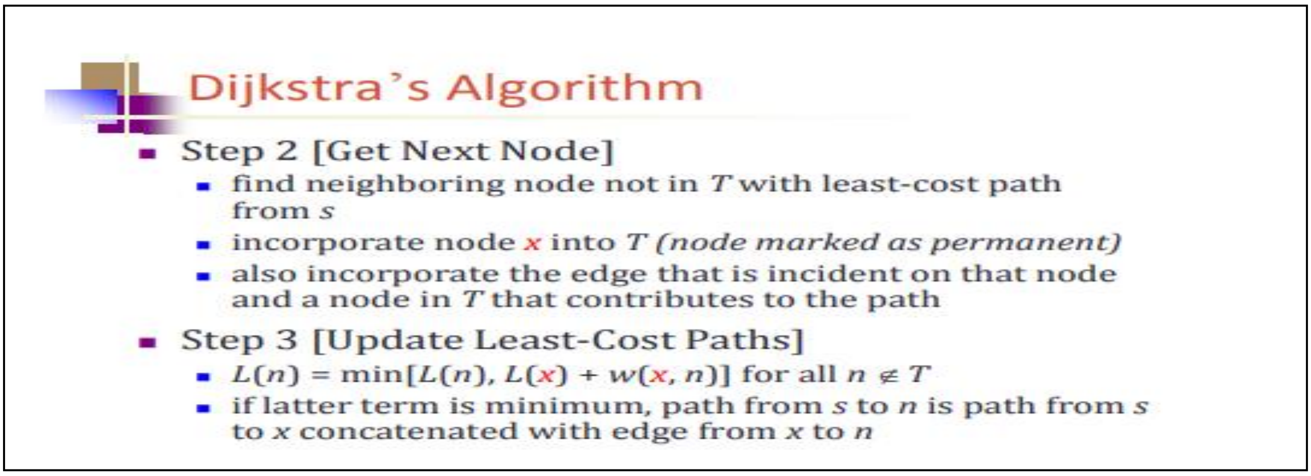
Dijkstra's Algorithm

- Finds shortest paths from given source node **S** to all other nodes
- Starts from the source node and finds the nearest adjacent node
- Runs in stages, each time adding node with next shortest path
- algorithm terminates when all nodes are processed by algorithm (in set *T*)



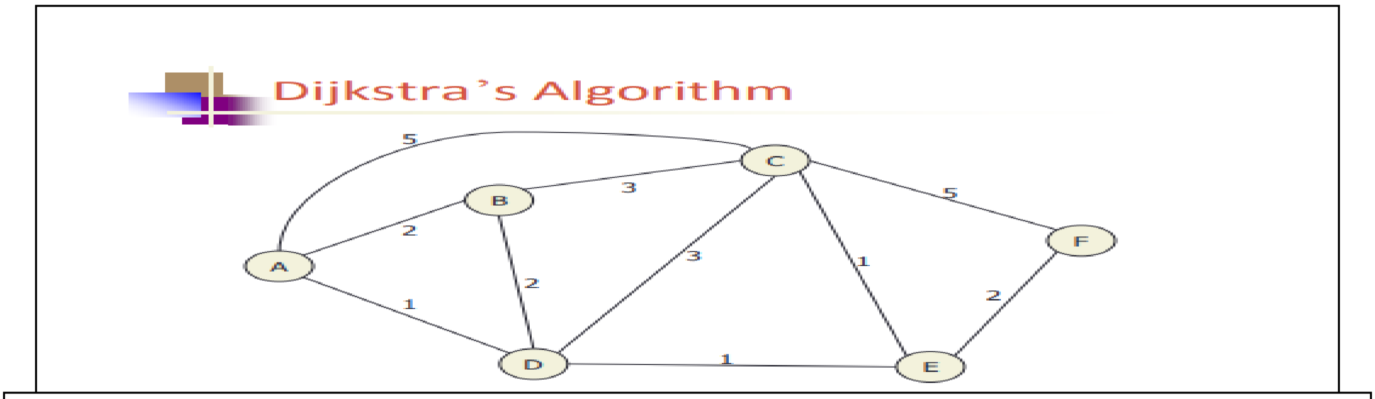
Dijkstra's Algorithm

- Step 1 [Initialization]
    - $T = \{s\}$ Set of nodes so far incorporated

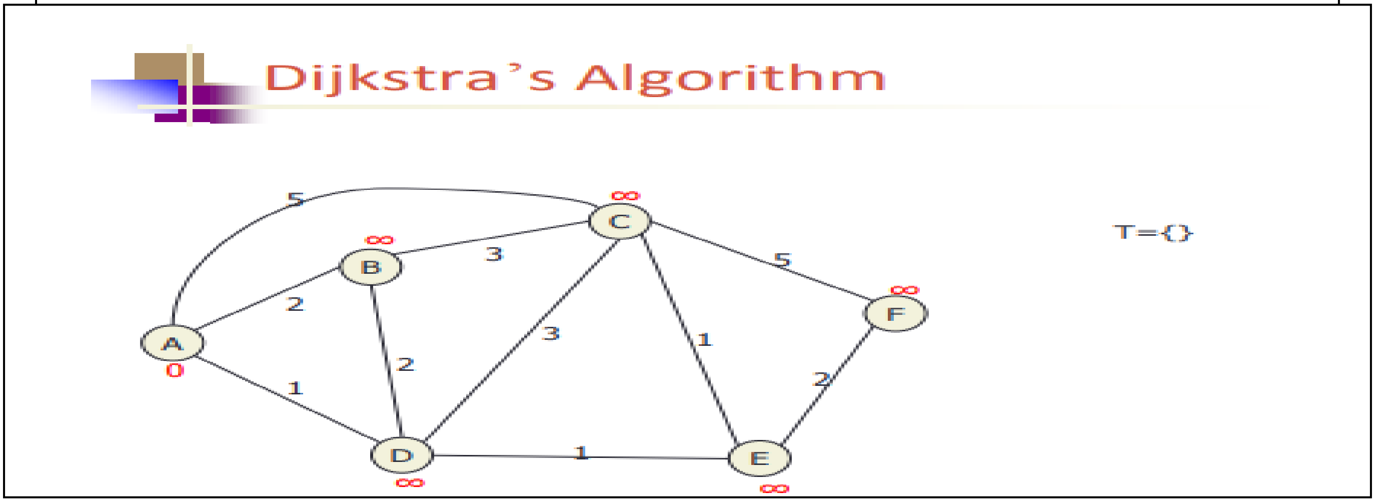


Dijkstra's Algorithm

- Step 2 [Get Next Node]
  - find neighboring node not in *T* with least-cost path from *s*
  - incorporate node *x* into *T (node marked as permanent)*
  - also incorporate the edge that is incident on that node and a node in *T* that contributes to the path
- Step 3 [Update Least-Cost Paths]
  - $L(n) = \min[L(n), L(x) + w(x, n)]$ for all $n \notin T$
  - if latter term is minimum, path from *s* to *n* is path from *s* to *x* concatenated with edge from *x* to *n*

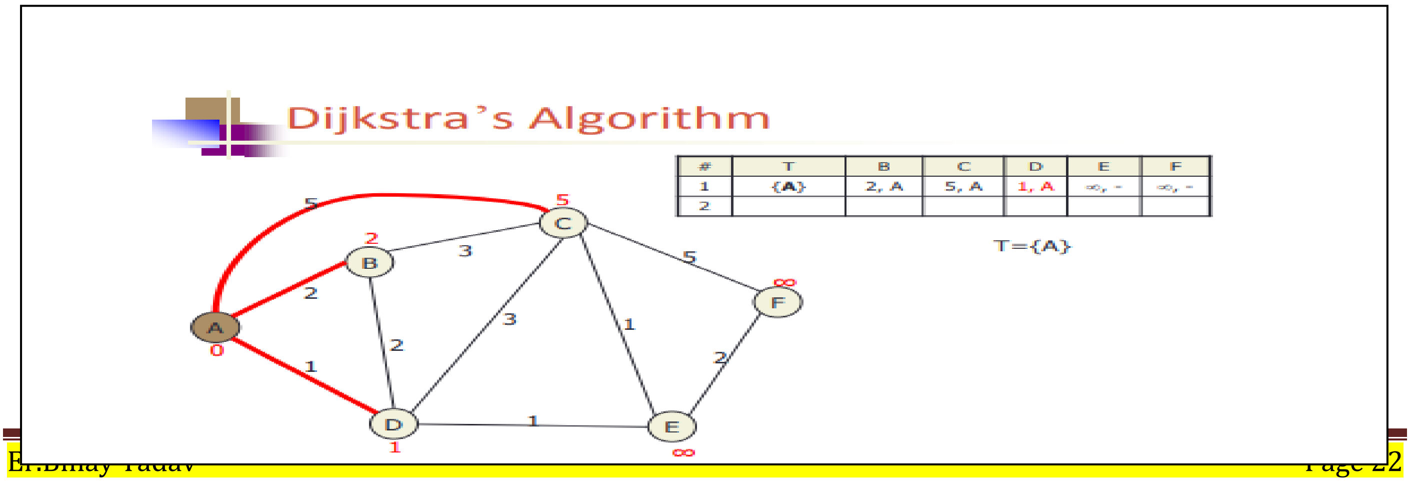


Dijkstra's Algorithm



Dijkstra's Algorithm

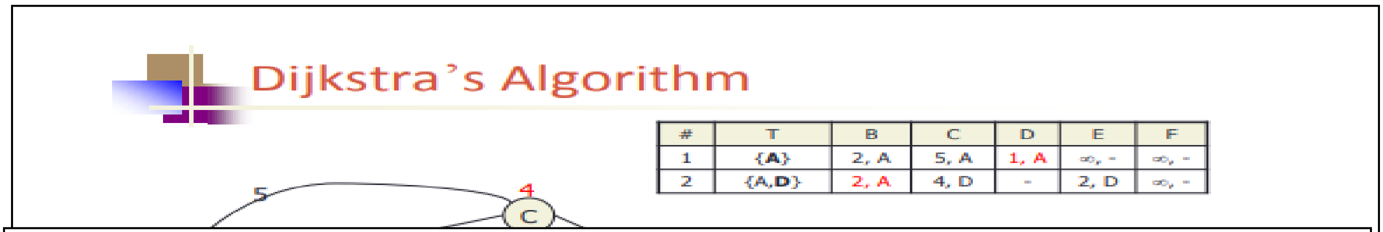
T={}



Dijkstra's Algorithm

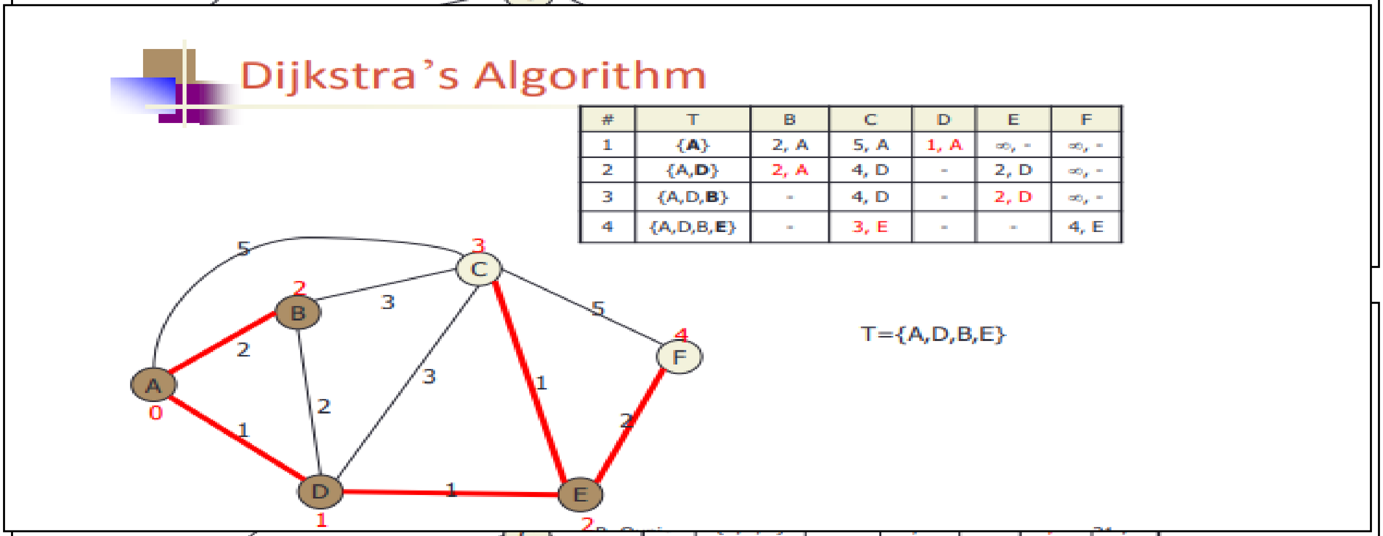
#	T	B	C	D	E	F
1	{A}	2, A	5, A	1, A	∞, -	∞, -
2						

T={A}



Dijkstra's Algorithm

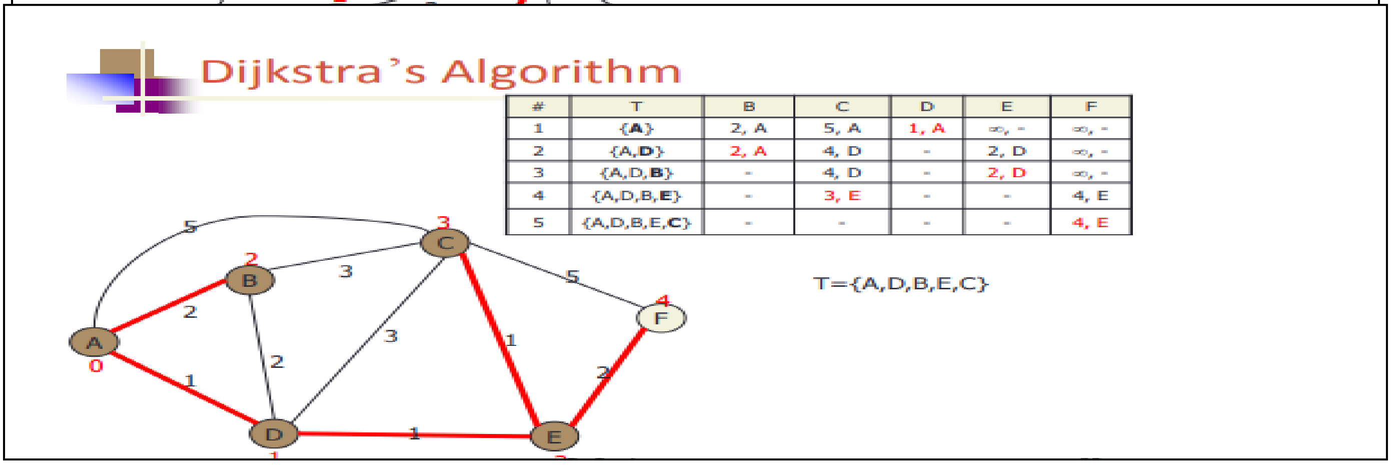
#	T	B	C	D	E	F
1	{**A**}	2, A	5, A	1, A	∞, -	∞, -
2	{A,**D**}	2, A	4, D	-	2, D	∞, -



Dijkstra's Algorithm

#	T	B	C	D	E	F
1	{**A**}	2, A	5, A	1, A	∞, -	∞, -
2	{A,**D**}	2, A	4, D	-	2, D	∞, -
3	{A,D,**B**}	-	4, D	-	2, D	∞, -
4	{A,D,B,**E**}	-	3, E	-	-	4, E

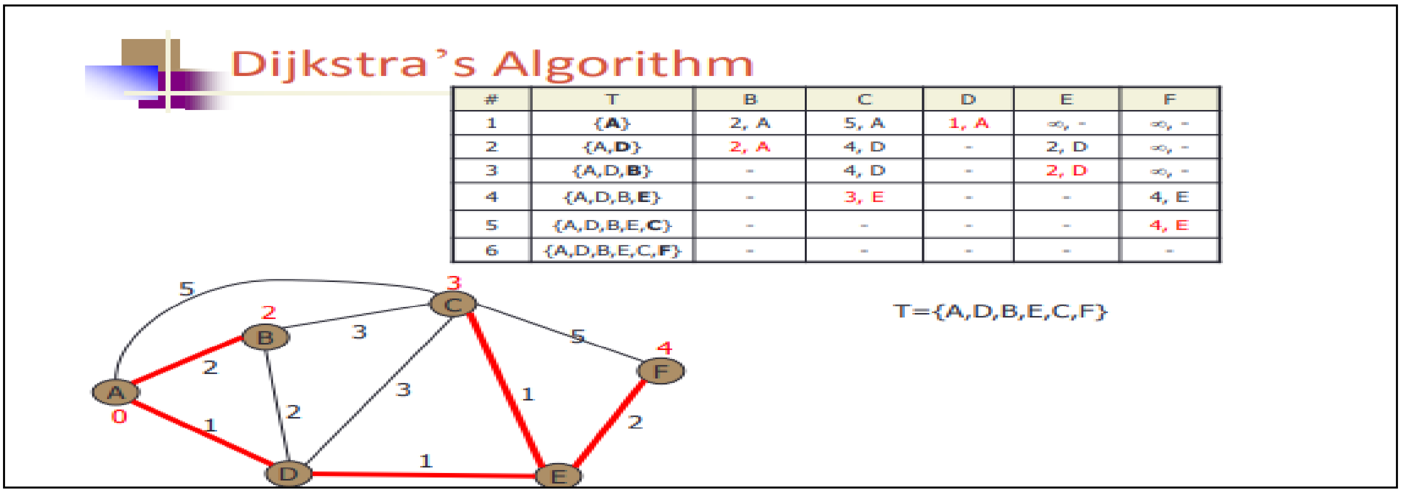
T={A,D,B,E}



Dijkstra's Algorithm

#	T	B	C	D	E	F
1	{**A**}	2, A	5, A	1, A	∞, -	∞, -
2	{A,**D**}	2, A	4, D	-	2, D	∞, -
3	{A,D,**B**}	-	4, D	-	2, D	∞, -
4	{A,D,B,**E**}	-	3, E	-	-	4, E
5	{A,D,B,E,**C**}	-	-	-	-	4, E

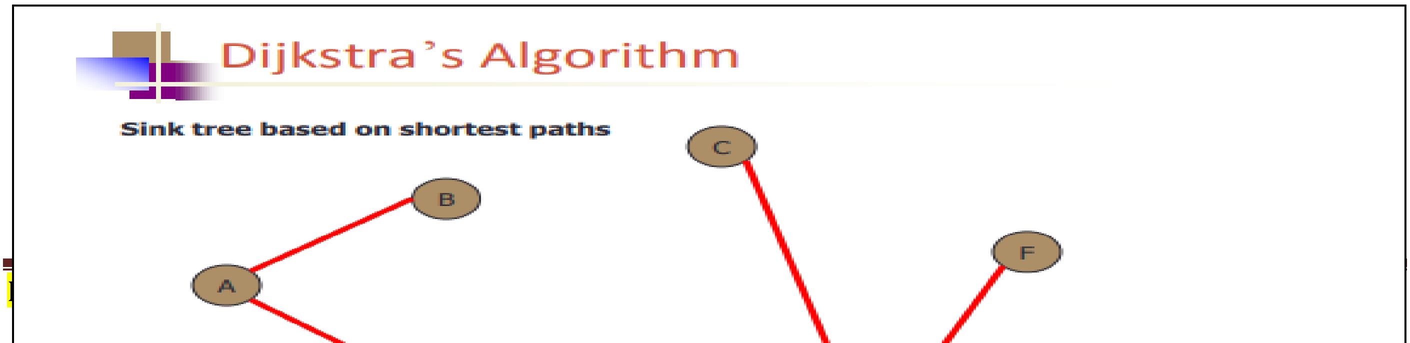
T={A,D,B,E,C}



Dijkstra's Algorithm

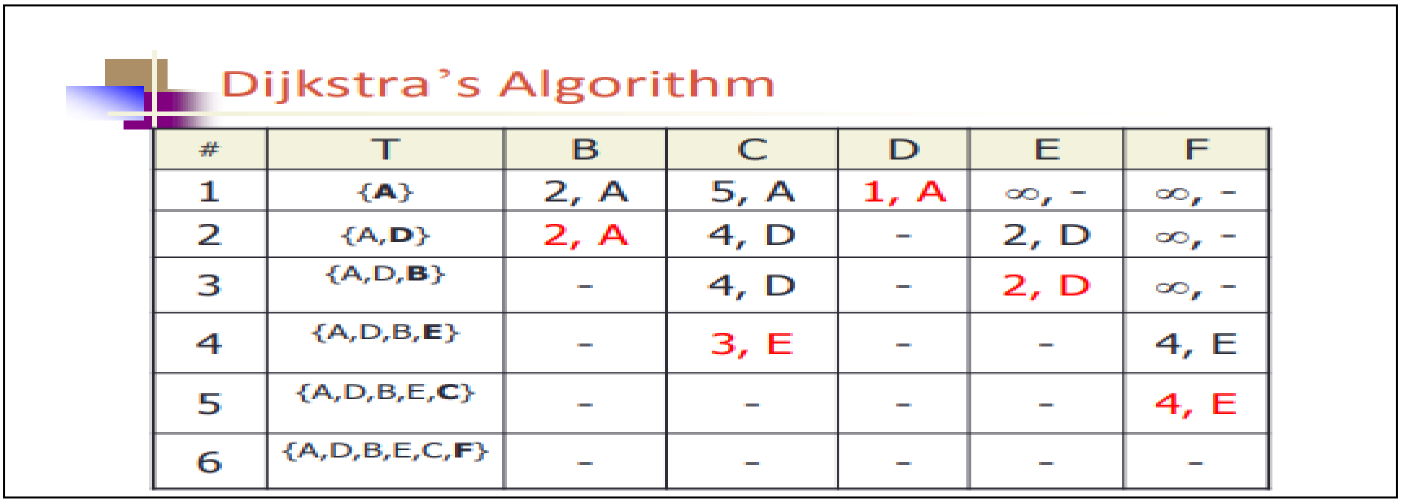
#	T	B	C	D	E	F
1	{**A**}	2, A	5, A	1, A	∞, -	∞, -
2	{A,**D**}	2, A	4, D	-	2, D	∞, -
3	{A,D,**B**}	-	4, D	-	2, D	∞, -
4	{A,D,B,**E**}	-	3, E	-	-	4, E
5	{A,D,B,E,**C**}	-	-	-	-	4, E
6	{A,D,B,E,C,**F**}	-	-	-	-	-

T={A,D,B,E,C,F}



Dijkstra's Algorithm

Sink tree based on shortest paths



Dijkstra's Algorithm

#	T	B	C	D	E	F
1	{A}	2, A	5, A	1, A	∞, -	∞, -
2	{A,D}	2, A	4, D	-	2, D	∞, -
3	{A,D,B}	-	4, D	-	2, D	∞, -
4	{A,D,B,E}	-	3, E	-	-	4, E
5	{A,D,B,E,C}	-	-	-	-	4, E
6	{A,D,B,E,C,F}	-	-	-	-	-

Differences b/w Adaptive and Non-Adaptive Routing Algorithm

Basis Of Comparison	**Adaptive Routing algorithm**	**Non-Adaptive Routing algorithm**
Define	Adaptive Routing algorithm is an algorithm that constructs the routing table based on the network conditions.	The Non-Adaptive Routing algorithm is an algorithm that constructs the static table to determine which node to send the packet.
Usage	Adaptive routing algorithm is used by dynamic routing.	The Non-Adaptive Routing algorithm is used by static routing.
Routing decision	Routing decisions are made based on topology and network traffic.	Routing decisions are the static tables.
Categorization	The types of adaptive routing algorithm, are Centralized, isolation and distributed algorithm.	The types of Non Adaptive routing algorithm are flooding and random walks.
Complexity	Adaptive Routing algorithms are more complex.	Non-Adaptive Routing algorithms are simple.