CHAPTER-1

Review of Networking Basics:

Computer Networking is the practice of connecting computers together to enable communication and data exchange between them. In general, Computer Network is a collection of two or more computers. It helps users to communicate more easily. In this article, we are going to discuss the basics which everyone must know before going deep into Computer Networking.

How Does a Computer Network Work?

Basics building blocks of a Computer network are Nodes and Links. A Network Node can be illustrated as Equipment for Data Communication like a Modem, Router, etc., or Equipment of a Data Terminal like connecting two computers or more. Link in Computer Networks can be defined as wires or cables or free space of wireless networks.

The working of Computer Networks can be simply defined as rules or protocols which help in sending and receiving data via the links which allow Computer networks to communicate. Each device has an IP Address that helps in identifying a device.

Basic Terminologies of Computer Networks

- **Network:** A network is a collection of computers and devices that are connected together to enable communication and data exchange.
- **Nodes:** Nodes are devices that are connected to a network. These can include computers, Servers, Printers, Routers, Switches, and other devices.
- **Protocol:** A protocol is a set of rules and standards that govern how data is transmitted over a network. Examples of protocols include TCP/IP, HTTP, and FTP.
- **Topology:** Network topology refers to the physical and logical arrangement of nodes on a network. The common network topologies include bus, star, ring, mesh, and tree.
- **Service Provider Networks:** These types of Networks give permission to take Network Capacity and Functionality on lease from the Provider. Service Provider Networks include Wireless Communications, Data Carriers, etc.
- **IP Address**: An IP address is a unique numerical identifier that is assigned to every device on a network. IP addresses are used to identify devices and enable communication between them.
- **DNS:** The Domain Name System (DNS) is a protocol that is used to translate human-readable domain names (such as www.google.com) into IP addresses that computers can understand.
- **Firewall:** A firewall is a security device that is used to monitor and control incoming and outgoing network traffic. Firewalls are used to protect networks from unauthorized access and other security threats.

Types of Enterprise Computer Networks

- **LAN:** A Local Area Network (LAN) is a network that covers a small area, such as an office or a home. LANs are typically used to connect computers and other devices within a building or a campus.
- **WAN:** A Wide Area Network (WAN) is a network that covers a large geographic area, such as a city, country, or even the entire world. WANs are used to connect LANs together and are typically used for long-distance communication.
- **Cloud Networks:** Cloud Networks can be visualized with a Wide Area Network (WAN) as they can be hosted on public or private cloud service providers and cloud networks are available if there is a demand. Cloud Networks consist of Virtual Routers, Firewalls, etc.

These are just a few basic concepts of computer networking. Networking is a vast and complex field, and there are many more concepts and technologies involved in building and maintaining networks. Now we are going to discuss some more concepts on Computer Networking.

- **Open system:** A system that is connected to the network and is ready for communication.
- **Closed system:** A system that is not connected to the network and can't be communicated with.

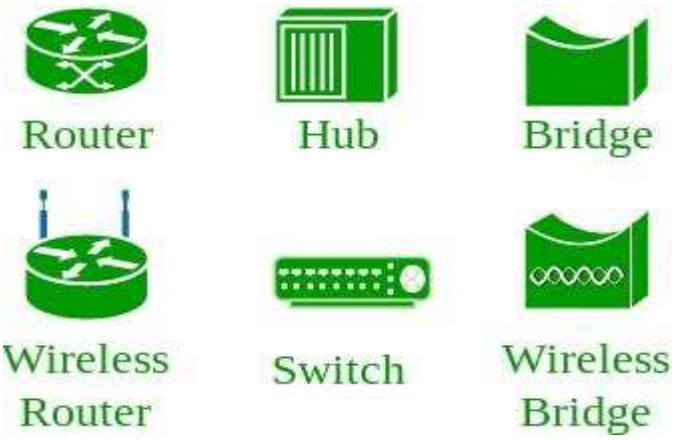
Types of Computer Network Architecture

Computer Network falls under these broad Categories:

- **Client-Server Architecture:** Client-Server Architecture is a type of Computer Network Architecture in which Nodes can be Servers or Clients. Here, the server node can manage the Client Node Behavior.
- **Peer-to-Peer Architecture:** In P2P (Peer-to-Peer) Architecture, there is not any concept of a Central Server. Each device is free for working as either client or server.

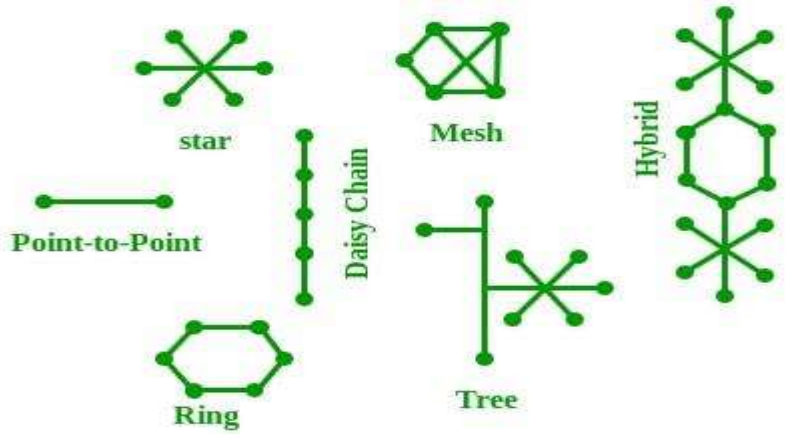
Network Devices

An interconnection of multiple devices, also known as hosts, that are connected using multiple paths for the purpose of sending/receiving data or media. Computer networks can also include multiple devices/mediums which help in the communication between two different devices; these are known as Network devices and include things such as routers, switches, hubs, and bridges.



Network Topology

The Network Topology is the layout arrangement of the different devices in a network. Common examples include Bus, Star, Mesh, Ring, and Daisy chain.



OSI Model

OSI stands for Open Systems Interconnection. It is a reference model that specifies standards for communications protocols and also the functionalities of each layer. The OSI has been developed by the International Organization for Standardization and it is 7 layer architecture. Each layer of OSI has different functions and each layer has to follow different protocols. The 7 layers are as follows:

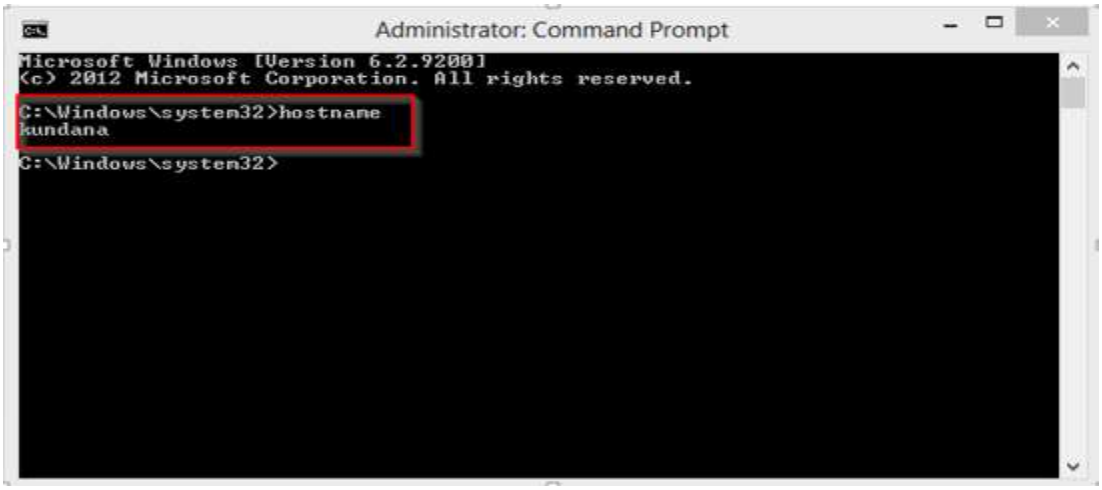
- Physical Layer
- Data link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

Protocol

A protocol is a set of rules or algorithms which define the way how two entities can communicate across the network and there exists a different protocol defined at each layer of the OSI model. A few such protocols are TCP, IP, UDP, ARP, DHCP, FTP, and so on.

Unique Identifiers of Network

Hostname: Each device in the network is associated with a unique device name known as Hostname. Type "hostname" in the command prompt (Administrator Mode) and press 'Enter', this displays the hostname of your machine.



IP Address (Internet Protocol address): Also known as the Logical Address, the IP Address is the network address of the system across the network. To identify each device in the world-wide-web, the Internet Assigned Numbers Authority (IANA) assigns an IPV4 (Version 4) address as a unique identifier to each device on the Internet. The length of an IPv4 address is 32 bits, hence, we have 2^{32} IP addresses available. The length of an IPv6 address is 128 bits. Type "ipconfig" in the command prompt and press 'Enter', this gives us the IP address of the device.

MAC Address (Media Access Control address): Also known as physical address, the MAC Address is the unique identifier of each host and is associated with its NIC (Network Interface Card). A MAC address is assigned to the NIC at the time of manufacturing. The length of the MAC address is: 12-nibble/ 6 bytes/ 48 bits Type "ipconfig/all" in the command prompt and press 'Enter', this gives us the MAC address.

DNS Server: DNS stands for **Domain Name System**. DNS is basically a server that translates web addresses or URLs (ex: www.google.com) into their corresponding IP addresses. We don't have to remember all the IP addresses of each and every website. The command '**nslookup**' gives you the IP address of the domain you are looking for. This also provides information on our DNS Server. \

ARP: ARP stands for **Address Resolution Protocol**. It is used to convert an IP address to its corresponding physical address (i.e., MAC Address). ARP is used by the Data Link Layer to identify the MAC address of the Receiver's machine.

RARP: RARP stands for **Reverse Address Resolution Protocol**. As the name suggests, it provides the IP address of the device given a physical address as input. But RARP has become obsolete since the time DHCP has come into the picture.

Subnetting:

Subnetting is a technique used in computer networking to divide a single network into multiple smaller networks, known as subnetworks or subnets. The purpose of subnetting is to partition a large network into smaller, more efficient subnets, which can improve network performance, security, and organization.

There are two parts in an IP Address. One for them is Network part and the another is Host part. With IP Subnetting, we are adding one more part. This is "Subnet Part". From the Host part, we borrow some bits and we will use this part for Subnet.

How to create a subnet

A subnet contains three main elements:

Network address (or) subnet ID: This is always the first address of the subnet.

Broadcast address: This is always the last address of the subnet. A packet forwarded to the broadcast address is broadcasted to all the addresses in a subnet.

Subnet mask (or) netmask: This is the bitmask used to identify the subnet of an IP address by applying bitwise AND operation with the netmask and the IP address. All the IP addresses in a subnet contain an identical most-significant bit group. This is how a router identifies the subnet of an IP address since data packets only contain the destination IP address.

Consider the following example:

Say we have a network with IP addresses ranging from 192.168.255.0 to 192.168. 255.255 and want to create two subnets.

In general, each IP address consists of two parts: network identifier and host identifier. All the host addresses in the same network will have an identical network identifier but a unique host identifier.

In this case, the first 24 bits (i.e., 192.168.255) represent the network identifier, and the remaining 8 bits represent the host identifier.

Considering x is the number of 1 bits needed in the host identifier part of the subnet mask, 2x is the number of subnets. As we need 2 subnets, x is 1.

192.168.255.0 is also the common network identifier for the whole network, and its subnet mask is 255.255.255.0

Let's convert these two addresses into binary:

192.168.255.0 = 11000000.10101000.11111111.00000000

255.255.255.0 = 11111111.11111111.11111111.00000000

As we need 2 subnets, one 1 bit is required in the host identifier part of the subnet mask. Hence, the subnet mask required is:

11111111.11111111.11111111.10000000 = 255.255.255.128

Accordingly, the subnet ID of the first subnet is 192.168.255.0, and the broadcast address is 192.168.255.127. Similarly, the subnet ID of the second subnet is 192.168.255.128, and the broadcast address is 192.168.255.255.

Except for the subnet ID and broadcast address, we can use all the remaining IP addresses in a subnet as host addresses.

Calculating a subnet mask can be time-consuming and confusing. Instead, we can use a subnet mask calculator to calculate a subnet mask accurately.

Benefits of subnetting:

Subnetting offers three common benefits:

- **Improved Network Performance:** When a device broadcasts a packet, it'll reach all the network devices, burdening the network. Without proper context, broadcast packets can also spam devices within the network. This can lead to degraded network performance. By creating subnets, you can limit the scope of intra network broadcast messages to a specific subnet. This also enables efficient communication between devices in a subnet and sends a packet for routing outside the subnet if a destination address isn't part of the subnet, leading to minimum network congestion.
- **Enhanced Network Security:** If an attacker gains unauthorized access to your network, all your network devices may be compromised. With subnets, you can limit a network breach by isolating the compromised subnetwork.
- **Simplified Network Management:** IPv4 host addresses are classified into three classes: Class A, Class B, and Class C.

a. Each Class A block contains 16,777,214 addresses.

b. Each Class B block contains 65,534 addresses.

c. Each Class C block contains 254 addresses.

If your organization requires more than 254 host addresses, then a Class B allocation would be necessary. Without subnetting, this may waste huge amounts of addresses.

Limitations of subnetting

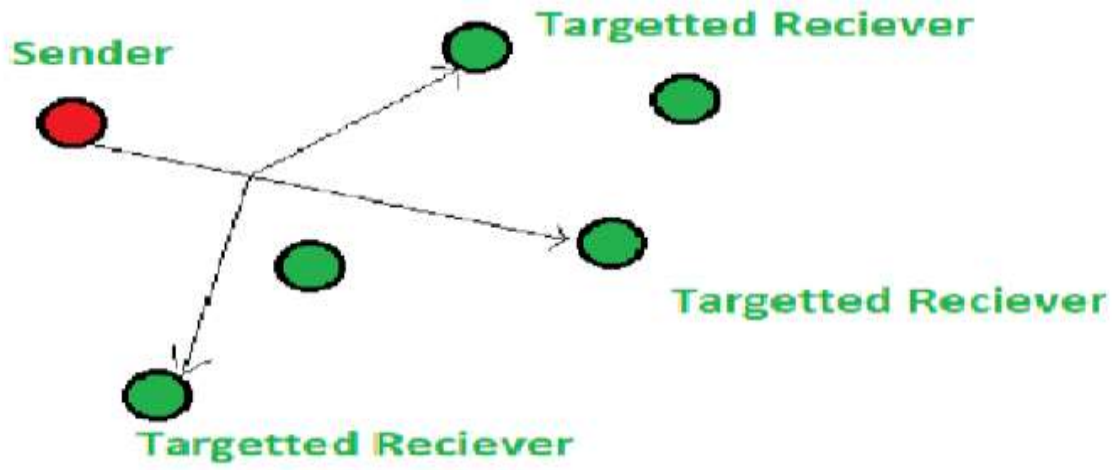
While subnetting offers many advantages, it can also result in some disadvantages:

- Communication between one subnet to another subnet requires a router. A poorly configured or fatally failed router can significantly impact your organization's network.
- Since each subnet requires dedicated IP addresses as subnet ID and broadcast address, it wastes IP addresses.
- Creating too many subnets can create unnecessary complexity and impact the effectiveness of network administration.

Multicasting:

Multicast is a method of group communication where the sender sends data to multiple receivers or nodes present in the network simultaneously. Multicasting is a type of one-to-many and many-to-many communication as it allows sender or senders to send data packets to multiple receivers at once across LANs or WANs. This process helps in minimizing the data frame of the network because at once the data can be received by multiple nodes.

Multicasting is considered as the special case of broadcasting as.it works in similar to Broadcasting, but in Multicasting, the information is sent to the targeted or specific members of the network. This task can be accomplished by transmitting individual copies to each user or node present in the network, but sending individual copies to each user is inefficient and might increase the network latency. To overcome these shortcomings, multicasting allows a single transmission that can be split up among the multiple users, consequently, this reduces the bandwidth of the signal.



Applications : Multicasting is used in many areas like:

- Internet protocol (IP)
- Streaming Media
- It also supports video conferencing applications and webcasts.

– Multicasting use classful addressing of IP address of class – D which ranges from 224.0.0.0 to 239.255.255.255

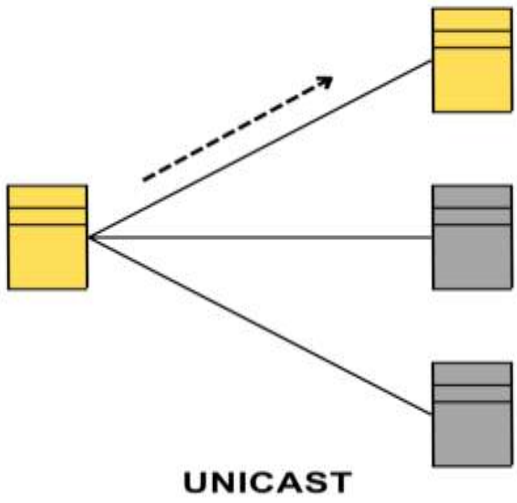
IP Multicast

Multicasting that takes place over the Internet is known as IP Multicasting. These multicast follow the internet protocol(IP) to transmit data. IP multicasting uses a mechanism known as 'Multicast trees' to transmit to information among the users of the network. Multicast trees; allows a single transmission to branch out to the desired receivers. The branches are created at the Internet routers, the branches are created such that the length of the transmission will be minimum.

Transmission of the **packet** can be done in three ways, namely-

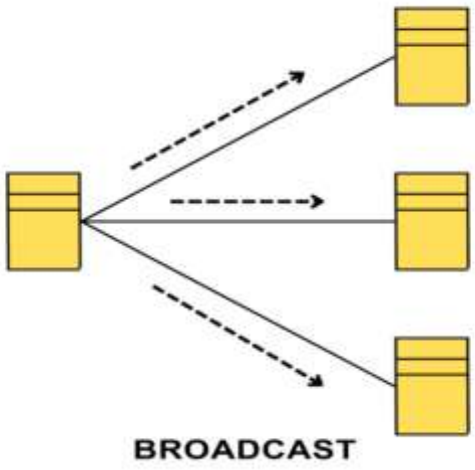
- **Unicast**

In the case of unicast, the packet is sent from one sender to one receiver, i.e., it is one-to-one communication.



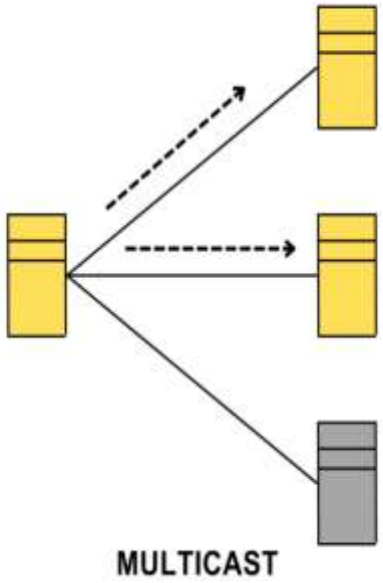
- **Broadcast**

In the case of broadcast, the message is sent from one sender to all the connected and possible receivers, i.e., it is one to all communication.



- **Multicast**

In the case of multicast, the message is sent from one sender to all the receivers who are interested to receive that particular traffic, i.e., it is one-to-many communication.



So generally, when a router receives a packet, it looks for the destination address, finds the best path of the destination by looking into the routing table, and then transmits the packet using the best path. This is a case of unicast routing, but what happens when a router receives a multicast packet? What happens when it receives a packet with a multicast address?

Multicast Routing Protocol:

Multicasting is a form of group communication where a sender simultaneously sends data to several receivers or network nodes. One or more senders can send data packets to numerous receivers simultaneously over LANs or WANs using multicasting, which is a type of one-to-many and many-to-many communication.

Multicasting is particularly useful for applications such as streaming video, online gaming, content distribution, and various forms of group communication.

Where is Multicast Routing used?

Multicast routing is used in the following technologies: –

- Video on demand
- Voice over IP
- Video streaming
- IP television (IPTV)

When using multicast routing, the sender creates a multicast group and sends data packets to a particular multicast IP address. The network's routers then use multicast routing protocols to choose the most efficient route for transmitting the packets to each recipient who has subscribed to the multicast group.

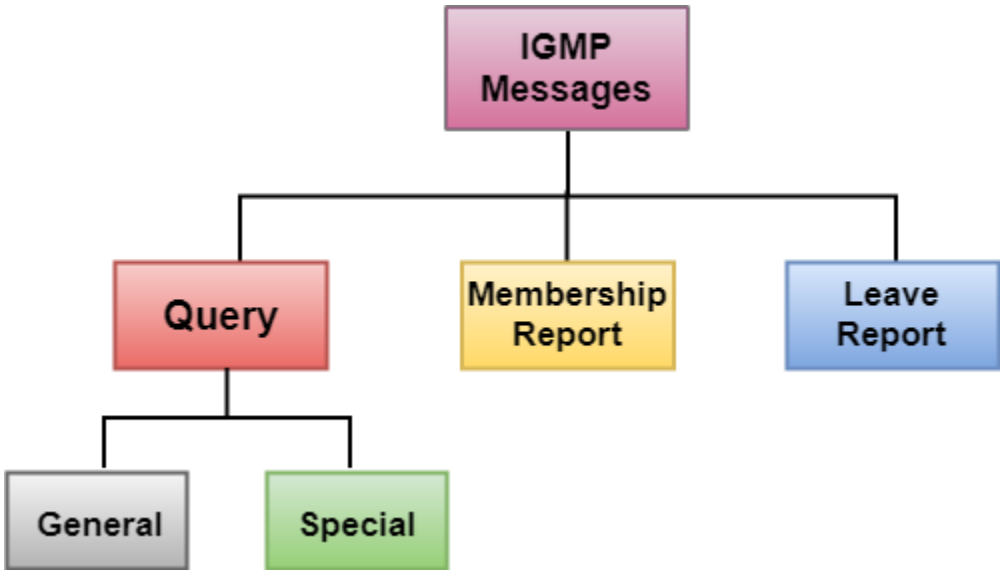
Which Multicast Routing Protocols are used?

In the case of multicast routing, the following multicast routing protocol is used: –

- Protocol Independent Multicast (PIM)
- Distance Vector Multicast Routing Protocol (DVMRP): –
- Multicast Open Shortest Path First (MOSPF)
- IGMP(Internet group Message Protocol)

IGMP

- IGMP stands for **Internet Group Message Protocol**.
- The IP protocol supports two types of communication:
    - **Unicasting:** It is a communication between one sender and one receiver. Therefore, we can say that it is one-to-one communication.
    - **Multicasting:** Sometimes the sender wants to send the same message to a large number of receivers simultaneously. This process is known as multicasting which has one-to-many communication.
- The IGMP protocol is used by the hosts and router to support multicasting.
- The IGMP protocol is used by the hosts and router to identify the hosts in a LAN that are the members of a group.



Membership Query message

This message is sent by a router to all hosts on a local area network to determine the set of all the multicast groups that have been joined by the host.

Membership Report message

The host responds to the membership query message with a membership report message.

Membership report messages can also be generated by the host when a host wants to join the multicast group without waiting for a membership query message from the router.

Leave Report
When the host does not send the "Membership Report message", it means that the host has left the group. The host knows that there are no members in the group, so even when it receives the next query, it would not report the group.

Protocol Independent Multicast (PIM)

PIM forwards multicast packets to recipients using a shared or source-specific tree.

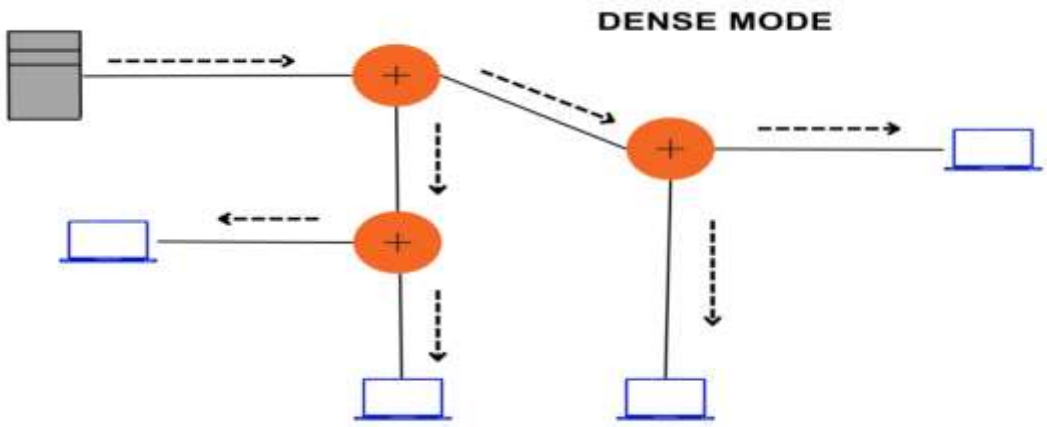
A family of multicast routing systems called PIM is made to operate with any unicast routing mechanism. PIM allows routers to dynamically create multicast distribution trees, which establish the route for multicast traffic to be forwarded from a sender to numerous receivers.

There have two modes of communication in PIM.

- **PIM Dense Mode (PIM-DM)**

It is designed for the network where there are many receivers interested in a multicast group. In dense Mode, it is assumed that most devices in the network are interested to receive the multicast packet hence, the router floods the multicast packet to ensure that it can reach every part of the network and then prunes it back to avoid sending data to a device that is not interested in receiving the packet.

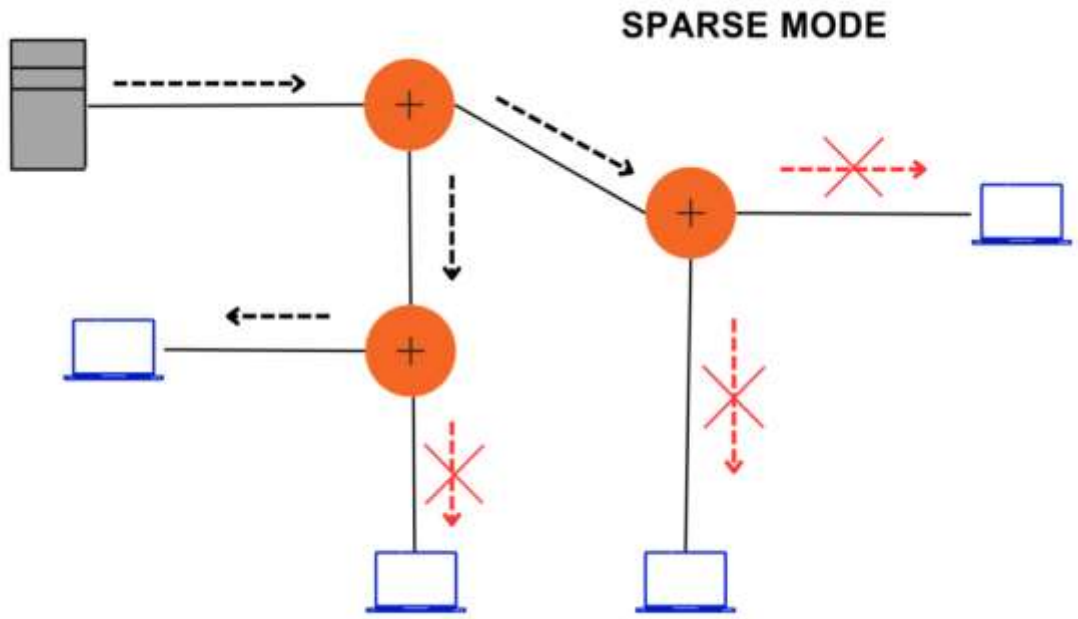
The host sends a prune message to the router to tell it that they do not need this multicast packet. PIM-DM is less commonly used as compared to PIM-SM due to its flooding behavior, which can cause unnecessary traffic in large networks.



- **PIM Sparse Mode (PIM-SM)**

It is designed for networks where multicast traffic is sparse, meaning that there are only a few receivers for a particular multicast group. This mode is used when only a few subnets of devices are interested in receiving the multicast data. Since not all connected devices want to receive the multicast data, routers do not flood the multicast packet in the network.

In Sparse Mode, the host signals the interest in receiving the multicast packet by sending the join message and hence router is capable to identify the host which is interested in receiving this multicast packet and sending it only to the active joiners. SM then builds a multicast distribution tree. It is used in the case of large networks where multicast data does not need to reach every connected device. This mode is more efficient than Dense Mode.



DVMRP (Distance Vector Multicast routing Protocol):

The distance vector multicast routing protocol is multicast routing protocol that takes the routing decision based upon the source address of the packet.

It is an older multicast routing system that determines multicast forwarding paths using a distance vector technique. While **MOSPF** is an enhancement of the OSPF unicast routing system that builds multicast distribution trees using the same link-state information.

This algorithm constructs the routing tree for a network.

- Whenever a router receives a packet, it forwards it to some of its ports based on the source address of packet.
- The rest of the routing tree is made by downstream routers.
- In this way, routing tree is created from destination to source.

Flow management in TCP:

Flow control deals with the amount of data sent to the receiver side without receiving any acknowledgment. It makes sure that the receiver will not be overwhelmed with data. It's a kind of speed synchronization process between the sender and the receiver. The data link layer in the OSI model is responsible for facilitating flow control.

One of the popular flow control mechanisms in TCP is the **sliding window protocol**. It's a byte-oriented process of variable size.

In this method, when we establish a connection between the sender and the receiver, the receiver sends the receiver window to the sender. The receiver window is the size that is currently available in the receiver's buffer.

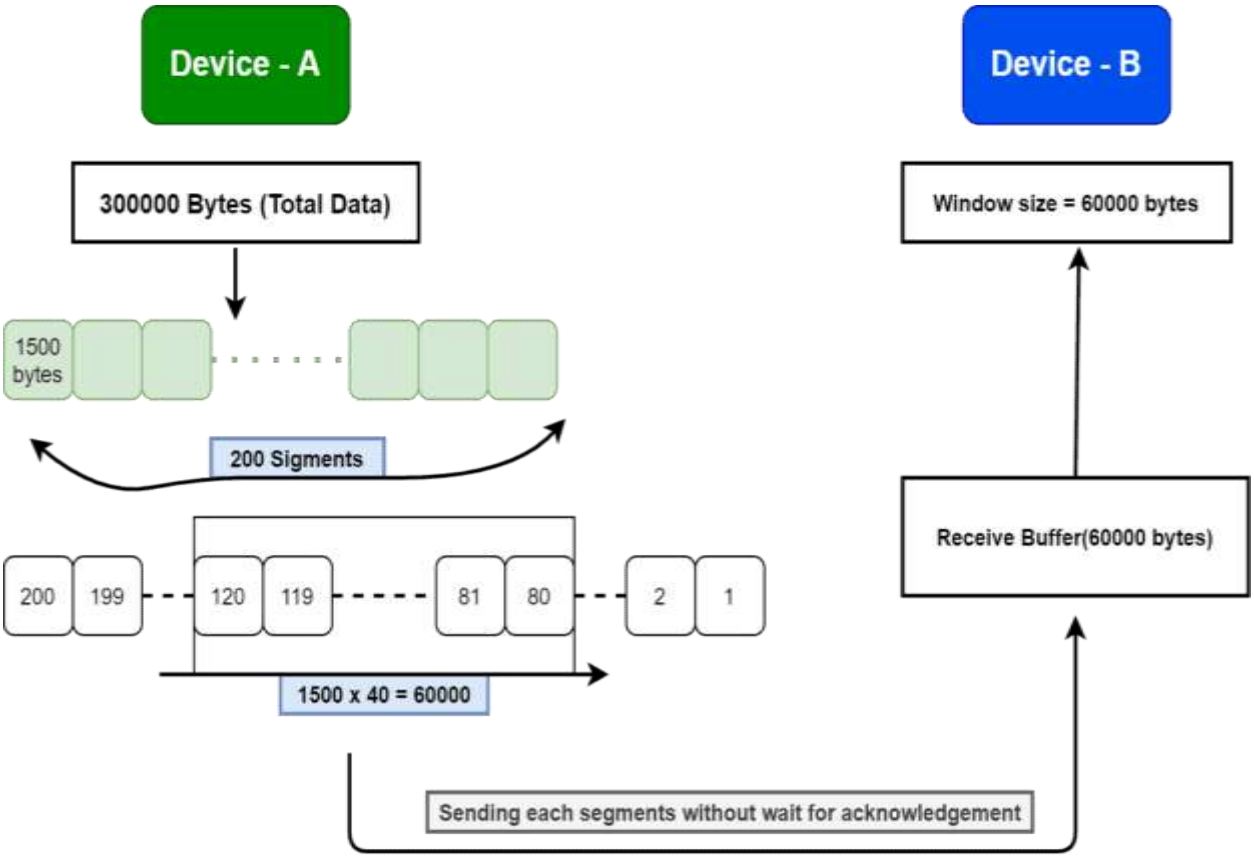
Now from the available receiver window, TCP calculates how much data can be sent further without acknowledgment. Although, if the receiver window size is zero, TCP halts the data transmission until it becomes a non-zero value.

The receiver window size is the part of the frame of TCP segments. The length of the window size is 16 bits, which means that the maximum size of the window is 65,535 bytes.

The receiver decides the size of the window. The receiver sends the currently available receiver window size with every acknowledgment message.

Suppose there are two devices: Device-A and Device-B. Device-A wants to send 300000 bytes of data to Device-B. Firstly, TCP breaks the data into small frames of size 1500 bytes each. Hence, there are 200 packets in total. In the beginning, let's assume Device-B notifies the available receiver window to Device-A, which is 60000 bytes. It means Device-A can send 60000 bytes to Device-B without receiving the acknowledgment from Device-B.

Now Device-A can send up to 40 packets (1500*40 = 60000) without waiting for an acknowledgment. Therefore, Device-A has to wait for five acknowledgment messages to complete the whole transmission**.** The number of acknowledgment messages needed is calculated and by considering the receiver buffer's capacity of Device-B:



Here, TCP is responsible for arranging the data packets and making the window size 60000 bytes. Furthermore, TCP helps in transmitting the packets which fall in the window range from Device-A to Device-B. After sending the packets, it waits for the acknowledgment. If the acknowledgment has been received, it slides the window to the next 60000 bytes and sends the packets.

We know TCP stops the transmission when the receiver sends the zero-size window. However, there is a possibility that the receiver has sent an acknowledgment but was missed by the sender.

In that situation, the receiver waits for the next packet. But on the other hand, the sender is waiting for non-zero window size. Hence, this situation would result in a deadlock**.** To handle this case, TCP starts a persist timer when it receives a zero-window size. It also sends packets periodically to the receiver.

Congestion Avoidance in TCP:

Congestion control is a mechanism that limits the flow of packets at each node of the network. Thus, it prevents any node from being overloaded with excessive packets. Congestion occurs when the rate of flow of packets towards any node is more than its handling capacity.

When congestion occurs, it slows down the network response time. As a result, the performance of the network decreases. Congestion occurs because routers and switches have a queue buffer, holding the packets for processing. After the holding process completes, they pass the packet to the next node, resulting in congestion in the network.

There are three phases that TCP uses for congestion control: slow start, congestion avoidance, and congestion detection:

congestion control phase

1. Slow Start

In the first phase of congestion control, the sender sends the packet and gradually increases the number of packets until it reaches a threshold. The window size is decided by the receiver.

In the same way, there is a window size in the congestion control mechanism. It increases gradually. In the flow control, the window size (RWND) is sent with the TCP header. Although in congestion control, the sender node or the end device stores it.

The sender starts sending packets with window size (CWND) of 1 MSS (Max Segment Size). MSS denotes the maximum amount of data that the sender can send in a single segment. Initially, the sender sends only one segment and waits for the acknowledgment for segment 1. After that, the sender increases the window size (CWND) by 1 MSS each time.

The slow start process can't continue for an indefinite time. Therefore, we generally use a threshold known as the slow start threshold (SSTHRESH) in order to terminate the slow start process. When the window size (CWND) reaches the slow-start threshold, the slow start process stops, and the next phase of congestion control starts. In most implementations, the value of the slow start threshold is 65,535 bytes.

2. Congestion Avoidance

The next phase of congestion control is congestion avoidance. In the slow start phase, window size (CWND) increases exponentially. Now, if we continue increasing window size exponentially, there'll be a time when it'll cause congestion in the network.

To avoid that, we use a congestion avoidance algorithm. The congestion avoidance algorithm defines how to calculate window size (CWND):

\[Window Size (CWND) = Window Size (CWND) + Max Segment Size (MSS) / Window Size (CWND)\]

After each acknowledgment, TCP ensures the linear increment in window size (CWND), slower than the slow start phase.

3. Congestion Detection

The third phase is congestion detection. Now in the congestion avoidance phase, we've decreased the rate of increment in window size (CWND) in order to reduce the probability of congestion in the network. If there is still congestion in the network, we apply a congestion detection mechanism.

There're two conditions when TCP detects congestion. Firstly, when there is no acknowledgment received for a packet sent by the sender within an estimated time. The second condition occurs when the receiver gets three duplicate acknowledgments.

In the case of timeout, we start a new slow start phase. To handle the second situation, we begin a new congestion avoidance phase.

IP Spoofing:

IP spoofing, or IP address spoofing, refers to the creation of Internet Protocol (IP) packets with a false source IP address to impersonate another computer system. IP spoofing allows cybercriminals to carry out malicious actions, often without detection. This might include stealing your data, infecting your device with malware, or crashing your server.

The risks associated with IP Spoofing include:

Denial-of-service attacks: An attacker can use IP Spoofing to flood a network or system with a large number of requests, making it unavailable to legitimate users.

- Unauthorized access: An attacker can use IP Spoofing to bypass access controls and gain unauthorized access to a system or network.

- Data interception: An attacker can use IP Spoofing to intercept sensitive data, such as login credentials, financial information, or personal information.

- Reputation damage: IP Spoofing can damage the reputation of legitimate businesses and organizations, as the attack can appear to be coming from their IP address.

Different ways to Prevent IP Spoofing include :

- Do not reveal any information regarding your internal IP addresses.This helps prevent those addresses from being "spoofed".

- Monitor incoming IP packets for signs of IP spoofing using network monitoring software. One popular product is "Netlog", is along side similar products, seeks incoming packets to the external interface that have the both source and destination IP addresses in your local domain. This essentially means an incoming packet that claims to be from inside network is actually coming from outside your network. Finding one means that an attack is underway.

- Danger that IP spoofing contains is that some firewalls do not examine packets that appear to come from an internal IP address.Routing packets through filtering router is possible, if they are not configured to filter incoming packets whose source address is in local domain.

Ipv6:

IPv6 is the newest version of internet protocol formulated by the Internet Engineering Task Force (IETF), which helps identify and local endpoint systems on a computer network and route online traffic while addressing the problem of IPv4 address depletion due to prolonged internet use worldwide.

The common type of IP address (is known as IPv4, for "version 4"). Here's an example of what an IP address might look like:

25.59.209.224

An IPv4 address consists of four numbers, each of which contains one to three digits, with a single dot (.) separating each number or set of digits. This group of separated numbers creates the addresses that let you and everyone around the globe to send and retrieve data over our Internet connections. The IPv4 uses a 32-bit address scheme allowing to store 2^32 addresses which is more than 4 billion addresses. To date, it is considered the primary Internet Protocol and carries 94% of Internet traffic. Initially, it was assumed it would never run out of addresses but the present situation paves a new way to IPv6. An IPv6 address consists of eight groups of four hexadecimal digits. Here's an example IPv6 address:

3001:0da8:75a3:0000:0000:8a2e:0370:7334

This new IP address version is being deployed to fulfil the need for more Internet addresses. With 128-bit address space, it allows 340 undecillion unique address space.

Advantages of IPv6

- Faster Speeds: IPv6 supports multicast rather than broadcast in IPv4.This feature allows bandwidth-intensive packet flows (like multimedia streams) to be sent to multiple destinations all at once.
- Stronger Security: IPSecurity, which provides confidentiality, and data integrity, is embedded into IPv6.
- Routing efficiency
- Reliability
- Most importantly it's the final solution for growing nodes in Global-network.
- The device allocates addresses on its own.
- Internet protocol security is used to support security.
- Enable simple aggregation of prefixes allocated to IP networks; this saves bandwidth by enabling the simultaneous transmission of large data packages.

Disadvantages of IPv6

- Conversion: Due to widespread present usage of IPv4 it will take a long period to completely shift to IPv6.
- Communication: IPv4 and IPv6 machines cannot communicate directly with each other.
- Not going backward Compatibility: IPv6 cannot be executed on IPv4-capable computers because it is not available on IPv4 systems.
- Conversion Time: One significant drawback of IPv6 is its inability to uniquely identify each device on the network, which makes the conversion to IPV4 extremely time-consuming.
- Cross-protocol communication is forbidden since there is no way for IPv4 and IPv6 to communicate with each other.

Differenece Between IPv6 and IPv4

IPv6	IPv4
IPv6 has a 128-bit address length	IPv4 has a 32-bit address length
It supports Auto and renumbering address configuration	It Supports Manual and DHCP address configuration
The address space of IPv6 is quite large it can produce 3.4×1038 address space	It can generate 4.29×109 address space
Address Representation of IPv6 is in hexadecimal	Address representation of IPv4 is in decimal
In IPv6 checksum field is not available	In IPv4 checksum field is available
IPv6 has a header of 40 bytes fixed	IPv4 has a header of 20-60 bytes.
IPv6 does not support VLSM.	IPv4 supports VLSM(Variable Length subnet mask).