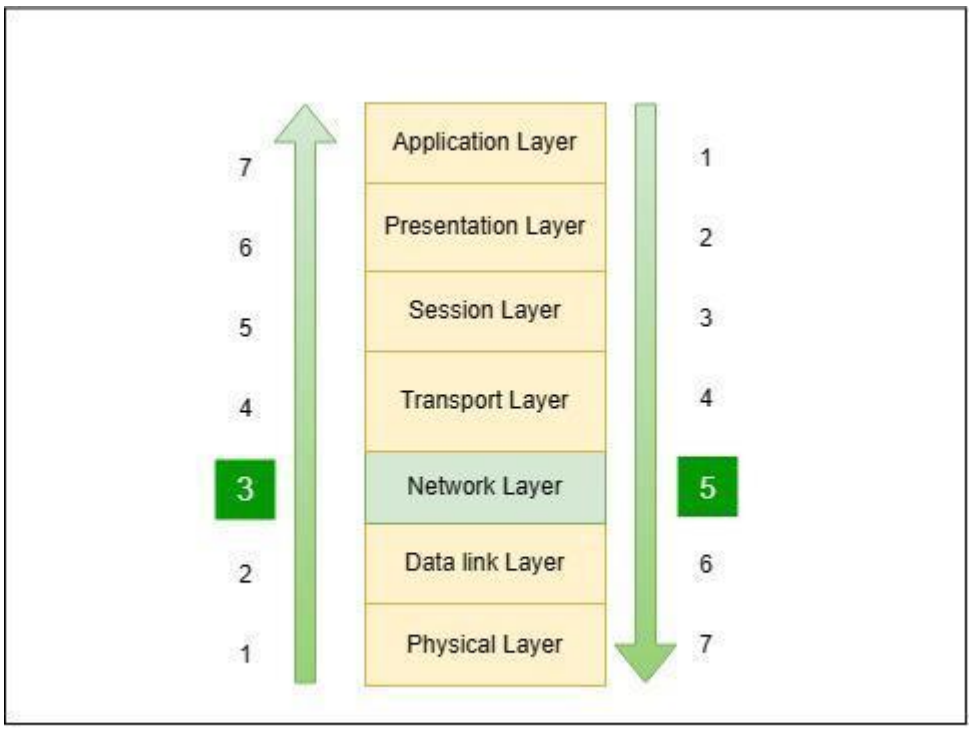
Unit-3

Network Layer in OSI Model

OSI stands for Open Systems Interconnection. It was developed by the ISO – 'International Organization for Standardization', in the year 1984. It is a 7-layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.

What is a Network Layer?

The Network Layer is the 5th Layer from the top and the 3rd layer from the Bottom of the OSI Model. It is one of the most important layers which plays a key role in data transmission. The main job of this layer is to maintain the quality of the data and pass and transmit it from its source to its destination. It also handles routing, which means that it chooses the best path to transmit the data from the source to its destination, not just transmitting the packet. There are several important protocols that work in this layer.



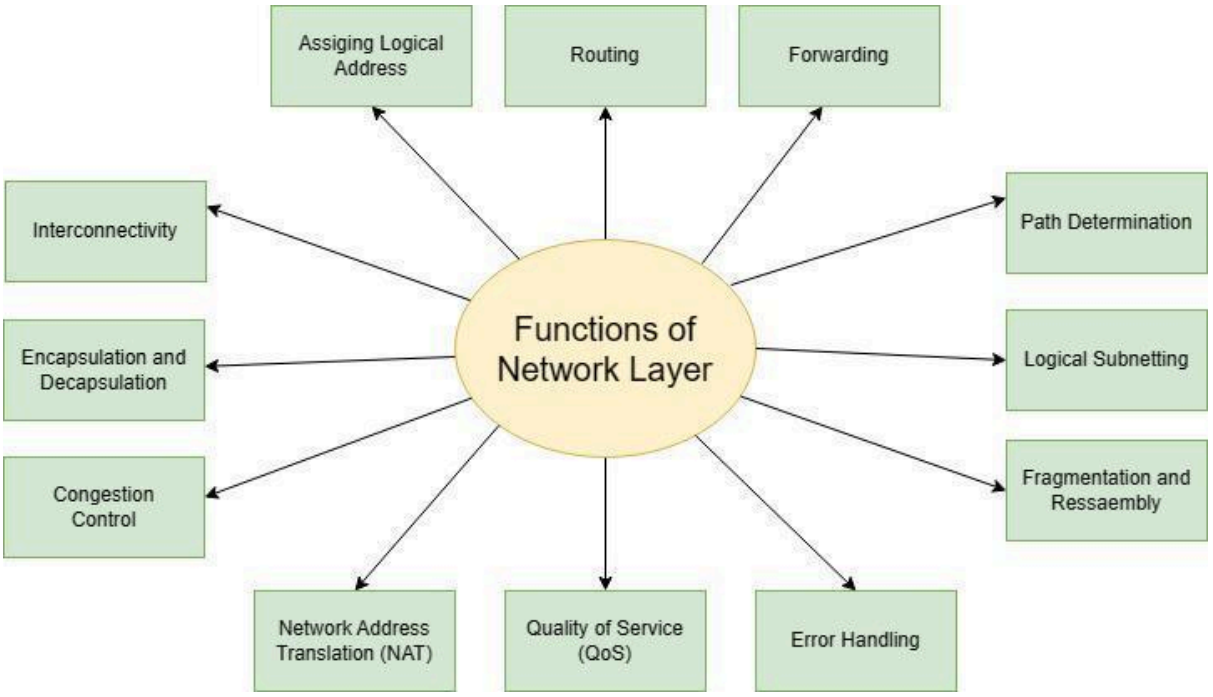
Entire OSI Model and the Location of Network Layer

Data is transmitted in the form of packets via various logical network pathways between various devices. In the seven-layer open system interconnection paradigm, the network layer is the third layer. It offers routes for data packet transfers across the network. The network layer is also responsible for organising and controlling the available paths for data transfer.

Functions of Network Layer

Unit-3

Network Layer serves various important functions in the data transport mechanism. It is also responsible for the routing mechanism in which it selects the best path to transfer the data from source to it's destination. It divides the entire data into smaller packets which eases the transfer procedure. It is also responsible for attaching the logical address to the devices between which the data transmission is happening, so that the packets reach correct destination and the destination can confirm that it is the same packet it was looking for. Some of the most important functions of the network layer is given below.



1. Assigning Logical Address

Network layer is solely responsible for assigning logical addresses to devices which are either sending or receiving data packets. It is useful to uniquely identify each devices in a certain network. The data packets sent or received consists the IP address of both the sender device and the receiver device. It is useful to confirm that the packets are sent or received by the desired parties. There are two part in an IP address, a Host ID and Network ID, using the Host ID it can be confirmed that the packets were sent by the authorized sender and it has successfully reached the desired receiver.

2. Routing

Routing is the process of identifying the best path to transmit the packets, Network Layer not only just sends packets from sender to receiver, but also determines the best route to send them. Numerous routers are used to find out the best and safest route to transmit the data packets. Various routing algorithms are used to determine the best path, like link state routing, Distance Vector Routing, Flooding, Random Walk etc. The header of each data packet holds the information regarding the path they need to follow to reach their destination via different routers. Usually there are multiple routers between the sender and the receiver, so the data packets are routed by using all these available routers.

Unit-3

3. Host-to-Host delivery

Host-to-Host delivery also known as Forwarding is the process in which the network layer transmits or forwards the data packets via routers, after determining the best path/route. In some cases it takes more than one router to reach the destination, Network Layer takes care of those too, it forwards packets from each router to the another router until it reaches the destination securely.

4. Logical Subnetting

Network Layer also allows a bigger network to be divided into smaller chunks of network known as Logical Subnetting. It helps the IP addresses to be used more efficiently and less amount of IP address will be wasted. It is also helpful to manage a larger network more efficiently. Due to smaller networks, it would be easier to find the device if any troubleshooting is needed.

5. Fragmentation and Reassembly

Each device / node has a maximum capacity to receive data (it may differ from Node to Node), which is called Maximum Transmission Unit (MTU). If the total size of data packets exceedes that size limit, then those data packets are fragmented into more smaller packets / fragmented so that they can fit the MTU. After fragmentation those packets are being send to the receiver, and at the receiving end all those fragmented packets are rearranged to create the actual data in order. The fragmentation is taken care by the routers.

6. Error Handling

Network Layer also check for errors and handles them. Network Layer uses various error detection techniques like Cylic Redundancy Check (CRC) , Checksums etc. Apart from just detecting, it also handle those errors using different approaches like Forward Error Correction (FEC), Hamming Code etc. It also re-transmit the packets which are either erroneous or didn't reach the receiver. It uses the ACK messages to determine whether a packet has been successfully reached the receiver or not, if there is a Negative ACK, then it means that there is some error with the packet, and the receiver will ask the sender to resend that packet.

7. Quality of Service (QoS)

Network layer also keep track of the important data or the particular quality of data which is needed to be send first. Based on the QoS settings, it determines and prioritize the important data types which needed to be send first. It ensures that there is no delay in receiving the important data in any condition.

8. Network Address Translation (NAT)

Network Layer also takes care of the Network Address Translation (NAT), means that it converts any private IP address into a public IP address which is required to communicate between the sender and the receiver.

9. Congestion Control

Unit-3

Just like MTU, if there is an excessive load on the network which it can't handle, the network become congested. Due to which the entire process of sending and receiving data comes to a pause. Congestion can be allocated with using different algorithms like Leaky Bucket Algorithm and Token Bucket Algorithm. In case of the leaky bucket algorithm, whatever might be the speed or amount of data flow into the bucket, the data leaks at a constant rate, which reduces the congestion in the network. In case of the Token Bucket Algorithm, tokens are being added into the bucket one by one, until it has reached the maximum capacity, then one by one according the token sequence each data packet is transmitted.

10. Encapsulation and Decapsulation

Network Layer encapsulates the data coming from the Transport Layer, and also adds important header parts to the packets, which consists of the necessary information like source IP address and destination IP address. After receiving the data packets on the destination side it decapsulates those and make them of original size.

Working of Network Layer

The network layer will initially receive data from the OSI model's transport layer as part of the data flow between that layer and other OSI levels. These data packets are handled by the network layer by include their source and destination addresses. Additionally, it incorporates the network protocols for proper transfer to the data-link layer over the network channel.

Responsibilities of the Network Layer

In the network channel and communication channel, the network layer is in charge of the responsibilities listed below:

- It is in charge of managing the network channel's quickest routing path for the data packet.
- The network layer packages the data that has been received for transmission.
- maintains the network traffic in the channel by handling the network layer protocols.

Problems with the Network layer design

- The decision of how to direct packets is a key aspect of network layer design. It holds great significance as it sets the groundwork for the protocol governing the transmission of packets between nodes in a network.
- In the nodes, data transmission can be facilitated through either static tables or dynamic tables. These tables serve as the routes for the transmission of information. The paths may be pre-established or subject to frequent alteration.
- The smooth flow of data in the network can be disrupted unexpectedly if there is an overwhelming abundance of packets being transmitted or present on the network. Consequently, the network might encounter bottlenecks causing a decline in its performance.

- Separate protocols are needed to enable communication between the two networks.

Advantages of Network Layer

- The network layer takes the data and breaks it down into packets, which makes transmitting the data over the network easier. This process also eliminates any weak points in the transmission, ensuring that the packet successfully reaches its intended destination.
- Router is the important component of the network layer . Its role is to reduce network congestion by facilitating collisions and broadcasting the domains within the network layer.
- Used to send data packets across the network nodes, the forwarding method is various.

Disadvantages of Network Layer

- There is no flow control mechanism provided by the network layer design.
- There may be times when there are too many datagrams in transit over the network, causing congestion. This could put further strain on the network routers. In some circumstances, the router may lose some data packets if there are too many datagrams. Important data may be lost in the process of transmission as a result of this.
- Indirect control cannot be implemented at the network layer since the data packets are broken up before being sent. Additionally, this layer lacks effective error control systems.

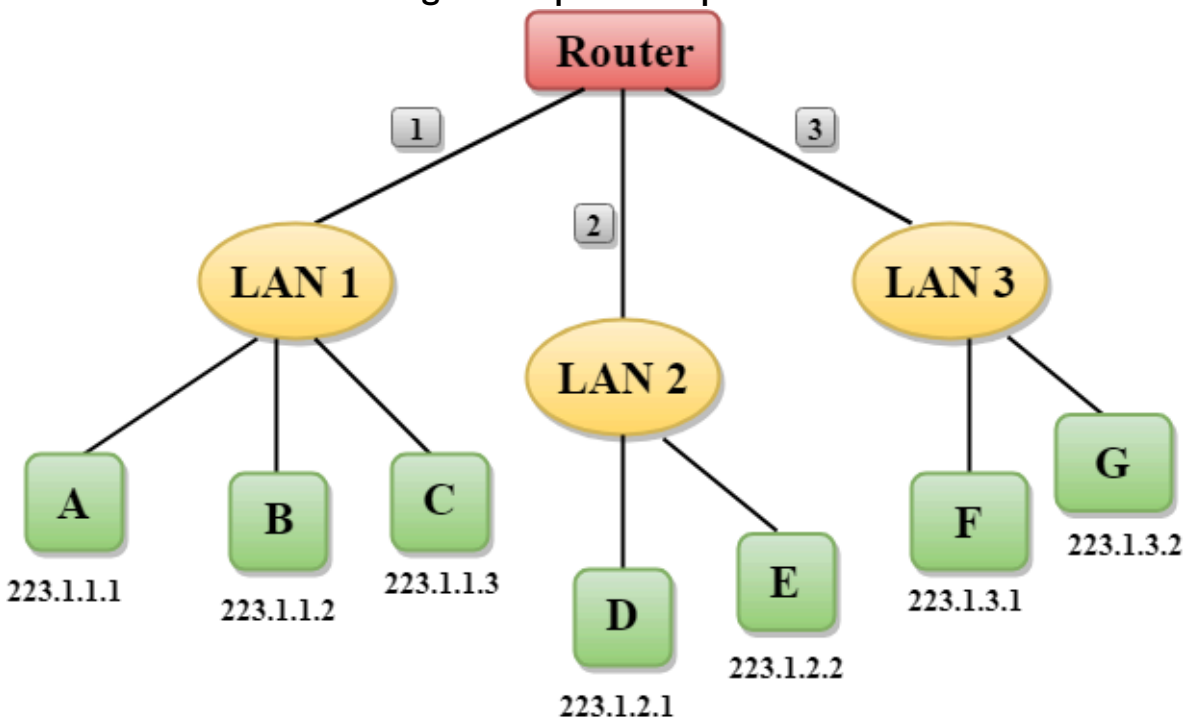
Unit-3

Network Addressing

- 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.

Unit-3

- **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

The 32-bit IP address is divided into five sub-classes. These are given below:

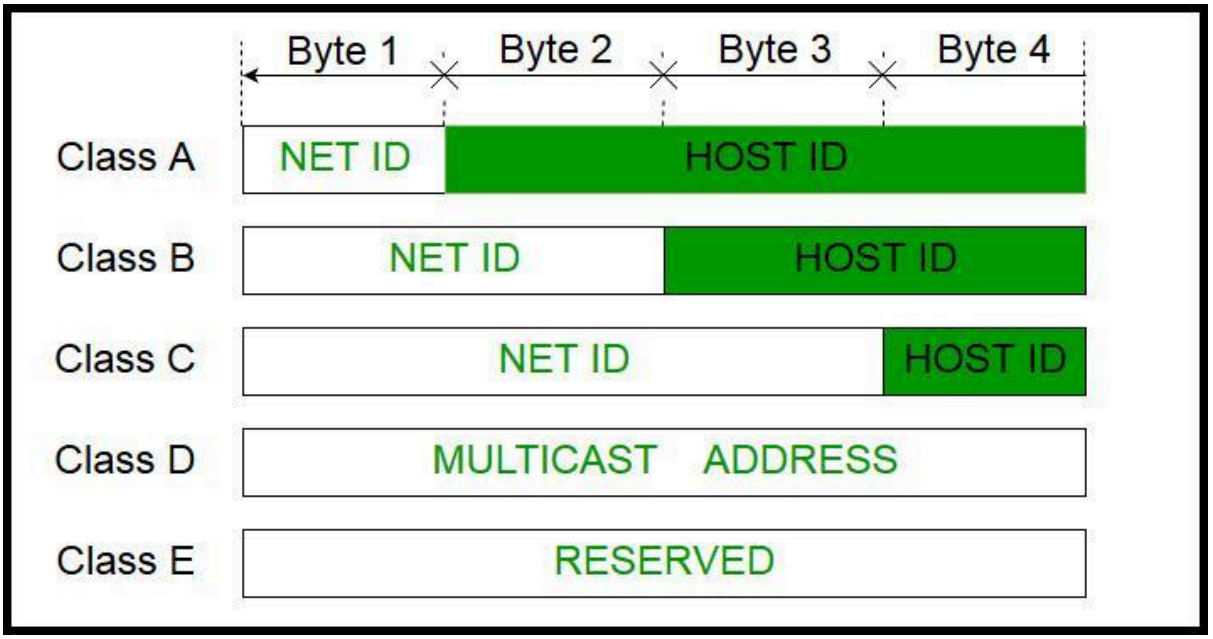
- Class A
- Class B
- Class C
- Class D
- Class E

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet (8 bits) determines the classes of the IP address. The IPv4 address is divided into two parts:

Unit-3

- Network ID
- Host ID

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP (Internet service provider) or network administrator assigns an IP address to each device that is connected to its network.



Classful Addressing

Note:

1. IP addresses are globally managed by Internet Assigned Numbers Authority(IANA) and regional Internet registries(RIR).
2. While finding the total number of host IP addresses, 2 IP addresses are not counted and are therefore, decreased from the total count because the first IP address of any network is the network number and whereas the last IP address is reserved for broadcast IP.

Class A

IP addresses belonging to class A are assigned to the networks that contain a large number of hosts.

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

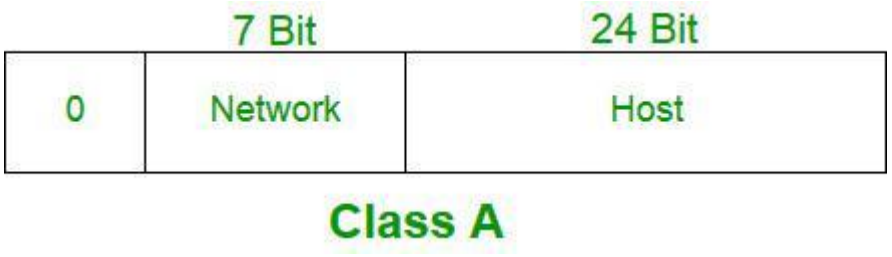
The higher-order bit of the first octet in class A is always set to 0. The remaining 7 bits in the first octet are used to determine network ID. The 24 bits of host ID are used to determine

the host in any network. The default subnet mask for Class A is 255.x.x.x. Therefore, class A has a total of:

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

IP addresses belonging to class A ranges from 0.0.0.0 – 127.255.255.255.



Class A

Class B

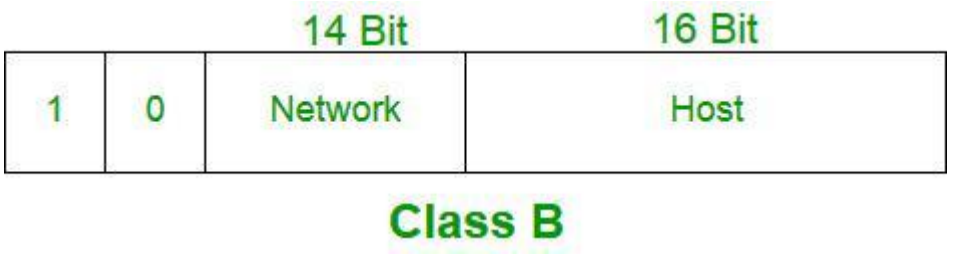
IP address belonging to class B is assigned to networks that range from medium-sized to large-sized networks.

- The network ID is 16 bits long.
- The host ID is 16 bits long.

The higher-order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine the network ID. The 16 bits of host ID are used to determine the host in any network. The default subnet mask for class B is 255.255.x.x. Class B has a total of:

- 2^14 = 16384 network address
- 2^16 – 2 = 65534 host address

IP addresses belonging to class B ranges from 128.0.0.0 – 191.255.255.255.



Class B

Class C

IP addresses belonging to class C are assigned to small-sized networks.

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

The higher-order bits of the first octet of IP addresses of class C is always set to 110. The remaining 21 bits are used to determine the network ID. The 8 bits of host ID are used to determine the host in any network. The default subnet mask for class C is 255.255.255.x. Class C has a total of:

- 2^21 = 2097152 network address
- 2^8 – 2 = 254 host address

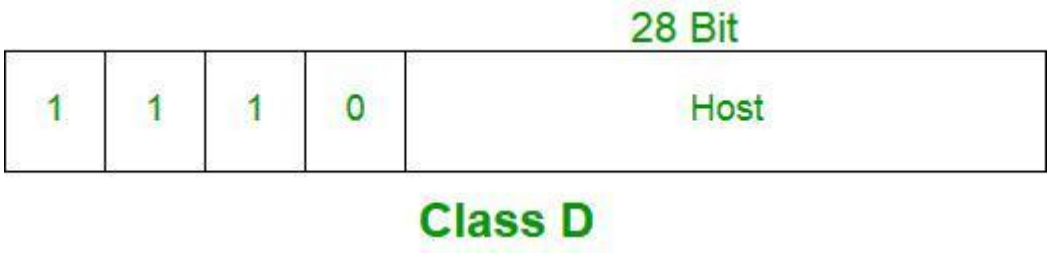
IP addresses belonging to class C range from 192.0.0.0 – 223.255.255.255.

Class C

Class D

IP address belonging to class D is reserved for multi-casting. The higher-order bits of the first octet of IP addresses belonging to class D is always set to 1110. The remaining bits are for the address that interested hosts recognize.

Class D does not possess any subnet mask. IP addresses belonging to class D range from 224.0.0.0 – 239.255.255.255.

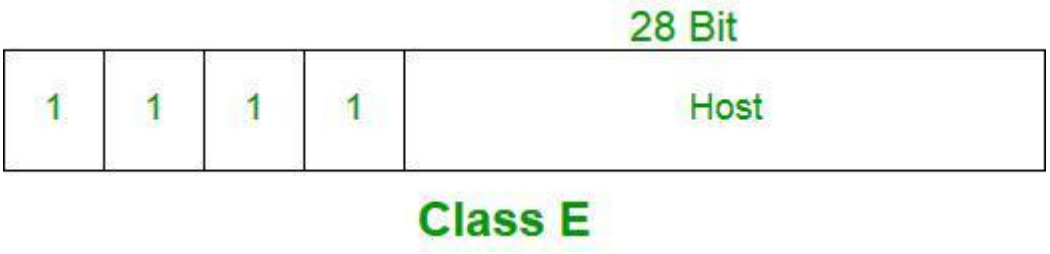


Class D

Class E

IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E range from 240.0.0.0 – 255.255.255.254. This class doesn't have any subnet mask. The higher-order bits of the first octet of class E are always set to 1111.

Unit-3



Class E

Range of Special IP Addresses

169.254.0.0 – 169.254.0.16 : Link-local addresses
127.0.0.0 – 127.255.255.255 : Loop-back addresses
0.0.0.0 – 0.0.0.8: used to communicate within the current network.

Rules for Assigning Host ID

Host IDs are used to identify a host within a network. The host ID is assigned based on the following rules:

- Within any network, the host ID must be unique to that network.
- A host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address.
- Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast address to send packets to all the hosts present on that particular network.

Rules for Assigning Network ID

Hosts that are located on the same physical network are identified by the network ID, as all host on the same physical network is assigned the same network ID. The network ID is assigned based on the following rules:

- The network ID cannot start with 127 because 127 belongs to the class A address and is reserved for internal loopback functions.
- All bits of network ID set to 1 are reserved for use as an IP broadcast address and therefore, cannot be used.
- All bits of network ID set to 0 are used to denote a specific host on the local network and are not routed and therefore, aren't used.

Summary of Classful Addressing

Unit-3

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

In the above table No. of networks for class A should be 127. (Network ID with all 0 s is not considered)

Unit-3

Internet Protocols

Internet Protocols are a set of rules that directs the communication and exchange of data over the internet. Both the sender and receiver should follow the same protocols in order to communicate the data. In order to understand it better, let's take an example of a language.

Any language has its own set of vocabulary and grammar which we need to know if we want to communicate in that language. Similarly, over the internet whenever we access a website or exchange some data with another device then these processes are governed by a set of rules called the internet protocols.

Working of Internet Protocol

The internet and many other data networks work by organizing data into small pieces called packets. Each large data sent between two network devices is divided into smaller packets by the basic hardware and software. Each network protocol defines the rules for how its data packets must be organized in specific ways according to the protocols the network supports.

Need of Protocols

It may be that the sender and receiver of data are parts of different networks, located in different parts of the world having different data transfer rates. So, we need protocols to manage the flow control of data, and access control of the link being shared in the communication channel.

Suppose there is a sender X who has a data transmission rate of 10 Mbps. And, there is a receiver Y who has a data receiving rate of 5Mbps. Since the rate of receiving the data is slow so some data will be lost during transmission. In order to avoid this, receiver Y needs to inform sender X about the speed mismatch so that sender X can adjust its transmission rate.

Similarly, the access control decides the node which will access the link shared in the communication channel at a particular instant in time. If not the transmitted data will collide if many computers send data simultaneously through the same link resulting in the corruption or loss of data.

What is IP Addressing?

An IP address represents an Internet Protocol address. A unique address that identifies the device over the network. It is almost like a set of rules governing the structure of data sent over the Internet or through a local network. An IP address helps the Internet to distinguish between different routers, computers, and websites. It serves as a specific machine identifier in a specific network and helps to

Types of Internet Protocol

Internet Protocols are of different types having different uses. These are mentioned below:

Unit-3

1. TCP/IP(Transmission Control Protocol/ Internet Protocol)
2. SMTP(Simple Mail Transfer Protocol)
3. PPP(Point-to-Point Protocol)
4. FTP (File Transfer Protocol)
5. SFTP(Secure File Transfer Protocol)
6. HTTP(Hyper Text Transfer Protocol)
7. HTTPS(HyperText Transfer Protocol Secure)
8. TELNET(Terminal Network)
9. POP3(Post Office Protocol 3)
10. IPv4
11. IPv6
12. ICMP
13. UDP
14. IMAP
15. SSH
16. Gopher

1. TCP/IP(Transmission Control Protocol/ Internet Protocol)

These are a set of standard rules that allows different types of computers to communicate with each other. The IP protocol ensures that each computer that is connected to the Internet is having a specific serial number called the IP address. TCP specifies how data is exchanged over the internet and how it should be broken into IP packets. It also makes sure that the packets have information about the source of the message data, the destination of the message data, the sequence in which the message data should be re-assembled, and checks if the message has been sent correctly to the specific destination. The TCP is also known as a connection-oriented protocol.

For more details, please refer TCP/IP Model article.

2. SMTP(Simple Mail Transfer Protocol)

These protocols are important for sending and distributing outgoing emails. This protocol uses the header of the mail to get the email id of the receiver and enters the mail into the queue of outgoing mail. And as soon as it delivers the mail to the receiving email id, it removes the email from the outgoing list.

The message or the electronic mail may consider the text, video, image, etc. It helps in setting up some communication server rules.

Unit-3

3. PPP(Point-to-Point Protocol)

It is a communication protocol that is used to create a direct connection between two communicating devices. This protocol defines the rules using which two devices will authenticate with each other and exchange information with each other. For example, A user connects his PC to the server of an Internet Service Provider and also uses PPP. Similarly, for connecting two routers for direct communication it uses PPP.

4. FTP (File Transfer Protocol)

This protocol is used for transferring files from one system to the other. This works on a client-server model. When a machine requests for file transfer from another machine, the FTP sets up a connection between the two and authenticates each other using their ID and Password. And, the desired file transfer takes place between the machines.

5. SFTP(Secure File Transfer Protocol)

SFTP which is also known as SSH FTP refers to File Transfer Protocol (FTP) over Secure Shell (SSH) as it encrypts both commands and data while in transmission. SFTP acts as an extension to SSH and encrypts files and data then sends them over a secure shell data stream. This protocol is used to remotely connect to other systems while executing commands from the command line.

6. HTTP(Hyper Text Transfer Protocol)

This protocol is used to transfer hypertexts over the internet and it is defined by the www(world wide web) for information transfer. This protocol defines how the information needs to be formatted and transmitted. And, it also defines the various actions the web browsers should take in response to the calls made to access a particular web page. Whenever a user opens their web browser, the user will indirectly use HTTP as this is the protocol that is being used to share text, images, and other multimedia files on the World Wide Web.

Note: *Hypertext refers to the special format of the text that can contain links to other texts.*

7. HTTPS(HyperText Transfer Protocol Secure)

HTTPS is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network with the SSL/TLS (Secure Socket Layer & Transport Layer Securities) protocol for encryption and authentication. So, generally, a website has an HTTP protocol but if the website is such that it receives some sensitive information such as credit card details, debit card details, OTP, etc then it requires an SSL certificate installed to make the website more secure. So, before entering any sensitive information on a website, we should check if the link is HTTPS or not. If it is not HTTPS then it may not be secure enough to enter sensitive information.

8. TELNET(Terminal Network)

TELNET is a standard TCP/IP protocol used for virtual terminal service given by ISO. This enables one local machine to connect with another. The computer which is being connected

is called a remote computer and which is connecting is called the local computer. TELNET operation lets us display anything being performed on the remote computer in the local computer. This operates on the client/server principle. The local computer uses the telnet client program whereas the remote computer uses the telnet server program.

9. POP3(Post Office Protocol 3)

POP3 stands for Post Office Protocol version 3. It has two Message Access Agents (MAAs) where one is client MAA (Message Access Agent) and another is server MAA(Message Access Agent) for accessing the messages from the mailbox. This protocol helps us to retrieve and manage emails from the mailbox on the receiver mail server to the receiver's computer. This is implied between the receiver and the receiver mail server. It can also be called a one-way client-server protocol. The POP3 WORKS ON THE 2 PORTS I.E. PORT 110 AND PORT 995.

10. IPv4

The fourth and initially widely used version of the Internet Protocol is called IPv4 (Internet Protocol version 4). It is the most popular version of the Internet Protocol and is in charge of distributing data packets throughout the network. Maximum unique addresses for IPv4 are 4,294,967,296 (232), which are possible due to the use of 32-bit addresses. The network address and the host address are the two components of each address. The host address identifies a particular device within the network, whereas the network address identifies the network to which the host belongs. In the "dotted decimal" notation, which is the standard for IPv4 addresses, each octet (8 bits) of the address is represented by its decimal value and separated by a dot (e.g. 192.168.1.1).

11. IPv6

The most recent version of the Internet Protocol, IPv6, was created to address the IPv4 protocol's drawbacks. A maximum of 4.3 billion unique addresses are possible with IPv4's 32-bit addresses. Contrarily, IPv6 uses 128-bit addresses, which enable a significantly greater number of unique addresses. This is significant because IPv4 addresses were running out and there are an increasing number of devices that require internet access. Additionally, IPv6 offers enhanced security features like integrated authentication and encryption as well as better support for mobile devices. IPv6 support has spread among websites and internet service providers, and it is anticipated to gradually

dislocate IPv4 as the main internet protocol.

For more details, please refer Differences between IPv4 and IPv6 article.

12. ICMP

ICMP (Internet Control Message Protocol) is a network protocol that is used to send error messages and operational information about network conditions. It is an integral part of the Internet Protocol (IP) suite and is used to help diagnose and troubleshoot issues with network connectivity. ICMP messages are typically generated by network devices, such as

routers, in response to errors or exceptional conditions encountered in forwarding a datagram. Some examples of ICMP messages include:

- Echo Request and Echo Reply (ping)
- Destination Unreachable
- Time Exceeded
- Redirect

ICMP can also be used by network management tools to test the reachability of a host and measure the round-trip time for packets to travel from the source to the destination and back.

It should be noted that ICMP is not a secure protocol, it can be used in some types of network attacks like DDoS extension.

13. UDP

UDP (User Datagram Protocol) is a connectionless, unreliable transport layer protocol. Unlike TCP,

it does not establish a reliable connection between devices before transmitting data, and it does not guarantee that data packets will be received in the order they were sent or that they will be received at all.

Instead, UDP simply sends packets of data to a destination without any error checking or flow control.

UDP is typically used for real-time applications such as streaming video and audio, online gaming, and VoIP (Voice over Internet Protocol) where a small amount of lost data is acceptable and low latency is important.

UDP is faster than TCP because it has less overhead. It doesn't need to establish a connection, so it can send data packets immediately.

It also doesn't need to wait for confirmation that the data was received before sending more, so it can transmit data at a higher rate.

14. IMAP

IMAP (Internet Message Access Protocol) is a protocol used for retrieving emails from a mail server. It allows users to access and manage their emails on the server, rather than downloading them to a local device. This means that the user can access their emails from multiple devices and the emails will be synced across all devices.

IMAP is more flexible than POP3 (Post Office Protocol version 3) as it allows users to access and organize their emails on the server, and also allows multiple users to access the same mailbox.

Unit-3

15. SSH

SSH (Secure Shell) is a protocol used for secure remote login and other secure network services. It provides a secure and encrypted way to remotely access and manage servers, network devices, and other computer systems. SSH uses public-key cryptography to authenticate the user and encrypt the data being transmitted, making it much more secure than traditional remote login protocols such as Telnet. SSH also allows for secure file transfers using the SCP (Secure Copy) and SFTP (Secure File Transfer Protocol) protocols.

16. Gopher

Gopher is a type of file retrieval protocol that provides downloadable files with some description for easy management, retrieving, and searching of files. All the files are arranged on a remote computer in a stratified manner. It is an old protocol and it is not much used nowadays.

Unit-3

Differences between IPv4 and IPv6

e address through which any computer communicates with our computer is simply called an Internet Protocol Address or IP address. For example, If we want to load a web page or we want to download something, we require the address for delivery of that particular file or webpage. That address is called an IP Address.

Types of IP Addresses

1. IPv4 (Internet Protocol Version 4)
2. IPv6 (Internet Protocol Version 6)

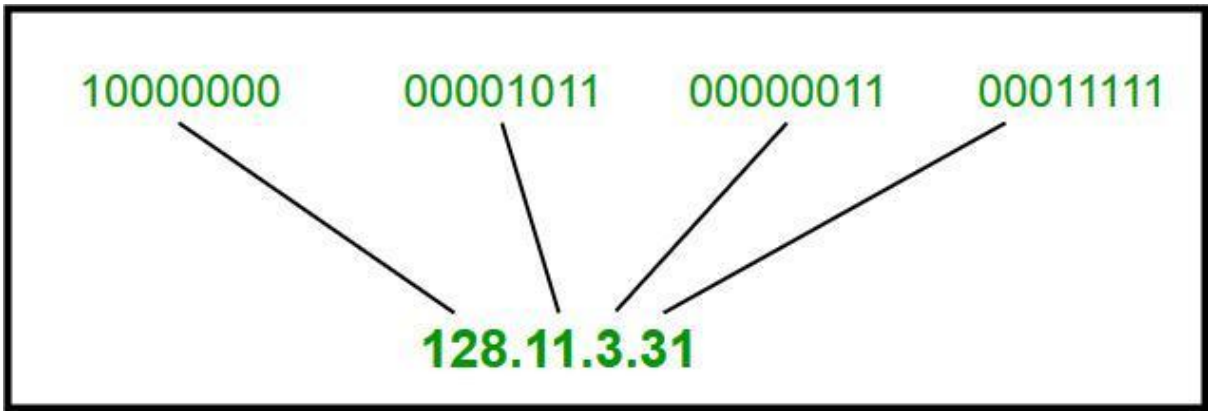
IPv4

IPv4 address consists of two things that are the network address and the host address. It stands for **Internet Protocol version four.** It was introduced in 1981 by DARPA (Defense Advanced Research Projects Agency) and was the first deployed version in 1982 for production on SATNET and on the ARPANET in January 1983.

IPv4 addresses are 32-bit integers that have to be expressed in Decimal Notation. It is represented by 4 numbers separated by dots in the range of 0-255, which have to be converted to 0 and 1, to be understood by Computers. For Example, An IPv4 Address can be written as **189.123.123.90.**

IPv4 Address Format

IPv4 Address Format is a 32-bit Address that comprises binary digits separated by a dot (.).



IPv4 Address Format

Unit-3

IPv6

IPv6 is based on IPv4 and stands for Internet Protocol version 6. It was first introduced in December 1995 by Internet Engineering Task Force. IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency. IPv6 is written as a group of 8 hexadecimal(16-base) numbers separated by colon (:). It can be written as 128 bits of 0s and 1s.

IPv6 Address Format

IPv6 Address Format is a 128-bit IP Address, which is written in a group of 8 hexadecimal numbers separated by colon (:).

IPv6 Address Format

Benefits of IPv6

The recent Version of IP IPv6 has a greater advantage over IPv4. Here are some of the mentioned benefits:

- **Larger Address Space:** IPv6 has a greater address space than IPv4, which is required for expanding the IP Connected Devices. IPv6 has 128 bit IP Address rather and IPv4 has a 32-bit Address.
- **Improved Security:** IPv6 has some improved security which is built in with it. IPv6 offers security like Data Authentication, Data Encryption, etc. Here, an Internet Connection is more Secure.

- **Simplified Header Format:** As compared to IPv4, IPv6 has a simpler and more effective header Structure, which is more cost-effective and also increases the speed of Internet Connection.
- **Prioritize:** IPv6 contains stronger and more reliable support for QoS features, which helps in increasing traffic over websites and increases audio and video quality on pages.
- **Improved Support for Mobile Devices:** IPv6 has increased and better support for Mobile Devices. It helps in making quick connections over other Mobile Devices and in a safer way than IPv4.

For more, you can refer to, the Advantages of IPv6.

Difference Between IPv4 and IPv6

IPv4	IPv6
IPv4 has a 32-bit address length	IPv6 has a 128-bit address length
It Supports Manual and DHCP(Dynamic Host Configuration Protocol) address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end, connection integrity is Unachievable	In IPv6 end-to-end, connection integrity is Achievable

Unit-3

IPv4	IPv6
It can generate 4.29×109 address space	The address space of IPv6 is quite large it can produce 3.4×1038 address space
The Security feature is dependent on the application	IPSEC is an inbuilt security feature in the IPv6 protocol
Address representation of IPv4 is in decimal	Address Representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation is performed only by the sender
In IPv4 Packet flow identification is not available	In IPv6 packet flow identification are Available and uses the flow label field in the header
In IPv4 checksum field is available	In IPv6 checksum field is not available
It has a broadcast Message	In IPv6 multicast and anycast message transmission scheme is available

Unit-3

IPv4	IPv6
Transmission Scheme	
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
IPv4 has a header of 20-60 bytes.	IPv6 has a header of 40 bytes fixed
IPv4 can be converted to IPv6	Not all IPv6 can be converted to IPv4
IPv4 consists of 4 fields which are separated by addresses dot (.)	IPv6 consists of 8 fields, which are separated by a colon (:)
IPv4's IP addresses are divided into five different classes. Class A , Class B, Class C, Class D , Class E.	IPv6 does not have any classes of the IP address.
IPv4 supports VLSM(Variable	IPv6 does not support VLSM.

Unit-3

IPv4	IPv6
Length subnet mask).	
Example of IPv4: 66.94.29.13	Example of IPv6: 2001:0000:3238:DFE1:0063:0000:0000:FEFB

Unit-3

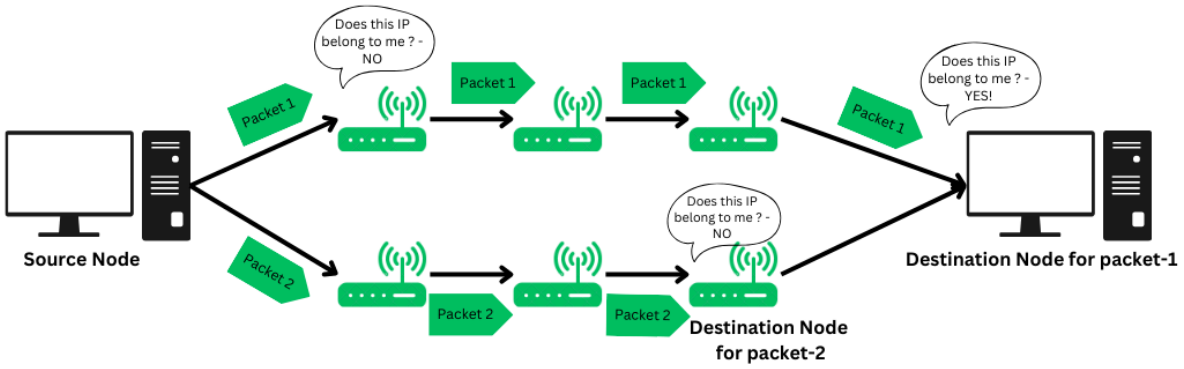
Routing

The process of choosing a path across one or more networks is known as network routing. Any kind of network, including public transit and phone networks, can use the routing principles. Routing chooses the routes along which Internet Protocol (IP) packets get from their source to their destination in packet-switching networks, such as the Internet. Routers are specialized pieces of network hardware that make these judgments about Internet routing.

What is Routing?

Routing refers to the process of directing a data packet from one node to another. It is an autonomous process handled by the network devices to direct a data packet to its intended destination. Note that, the node here refers to a network device called – 'Router'. Routing is a crucial mechanism that transmits data from one location to another across a network (Network type could be any like LAN, WAN, or MAN). The process of routing involves making various routing decisions to ensure reliable & efficient delivery of the data packet by finding the shortest path using various routing metrics which we will be discussing in this article.

Routing of a data packet is done by analyzing the destination IP Address of the packet. Look at the below image:



Routing of packets

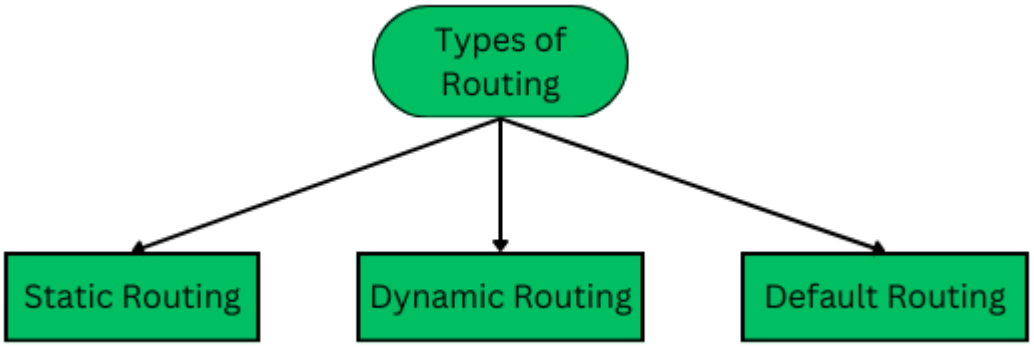
- Source Node (Sender) sends the data packet on the network, embedding the IP in the header of data packet.
- The nearest router receives the data packet, and based on some metrics, further routes the data packet to other routers.
- Step-2 occurs recursively till the data packet reaches its intended destination.

Note: There are limits to how many hop counts a packet can do if its exceeded, the packet is considered to be lost.

Types of Routing

Routing is typically of 3 types, each serving their own purpose and offering different functionalities.

Unit-3



Types of Routing

1. Static Routing

Static routing is also called as "non-adaptive routing"(not able to change). In this, routing configuration is done manually by the network administrator. Let's say for example, we have 5 different routes to transmit data from one node to another, so the network administrator will have to manually enter the routing information by assessing all the routes.

- Network administrator has full control over the network, routing the data packets to their concerned destinations
- Routers will route packets to the destination configured manually the network administrator.
- Although this type of routing gives a fine-grained control over the routes, it may not be suitable for large scale enterprise networks.

2. Dynamic Routing

Dynamic Routing is another type of routing in which routing is an autonomous procedure without any human intervention. Packets are transmitted over a network using various shortest path algorithms and pre-determined metrics. This type of routing is majorly preferred in modern networks as it offers more flexibility and adaptable functionality.

- It is also known as adaptive routing.
- In this, the router adds a new routes to the routing table based on any changes made in the topology of the network.
- The autonomous procedure of routing helps in automating every routing operation from adding to removing a route upon updates or any changes made to the network.

3. Default Routing

Default Routing is a routing technique in which a router is configured to transmit packets to a default route that is, a gateway or next hop device if no specific path is defined or found. It is commonly used when the network has single exit point. The IP Router has the following address as the default route : 0.0.0.0/0.

Unit-3

Working Principle of Routing

Routing works by finding a shortest path from the source node to the destination node across a network. Here's step-by-step working of routing:

Step1: Communication initiation

The first step that typically happens is, one node (client or server) initiates a communication across a network using HTTP protocols.

Step2: Data Packets

The source device now breaks a big portion of information into small data packets for reliable and efficient transmission. This process is called is called de-assembling and encapsulating the data payload. And then each data packet is labelled with the destination node's IP address.

Step3: Routing Table

Routing table is a logical data structure used to store the IP addresses and relevant information regarding the nearest routers. The source node then looks up for the IP addresses of all the nodes that can transmit the packet to its destination and selects the shortest path using the shortest path algorithm and then routes accordingly.

Routing Table is stored in a router, a network device that determines the shortest path and routes the data packet.

Step4: Hopping procedure

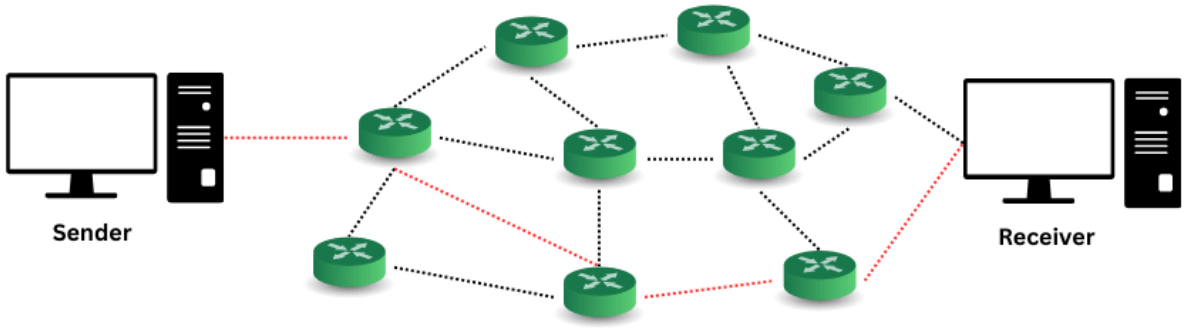
In the procedure or routing, the data packet will undergo many hops across various different nodes in a network till it reaches its final destination node. Hop-count is defined as the number of nodes required to traverse through to finally reach the intended destination node. This hopping procedure has a certain criteria defined for every data packet, there's a limited number of hops a packet can take if the packet exceeds that, then its considered to be lost and it is retransmitted.

Step5: Reaching the destination node

Once all the data packets reach their intended destination node, they re-assemble and transform into complete information that was sent by the sender (source node). The receiver will perform various error checking mechanism to verify the authenticity of the data packets.

Overall, the data packet will be transmitted over least hop-count path as well as the path on which there is less traffic to prevent packet loss.

Unit-3



Routing Working Example

Working of Routing

In the above image, we have 3 major components

- Sender
- Receiver
- Routers

The shortest path is highlighted in red, the path with least hop-count. As we can see, there are multiple paths from source to node but if all the appropriate metrics are satisfied, the data packets will be transmitted through the shortest path (highlighted in red).

Routing Metrics and Protocols

The purpose of routing protocols is to learn about all the available paths to route data packets, build routing table and take routing decisions based on some specified metrics. There are two primary types of routing protocols rest of them ideate from these two only.

1. Distance Vector Routing

In this type of routing protocol, all the nodes that are a part of the network advertise their routing table to their adjacent nodes (nodes that are directly connected to each other) at regular intervals. With each router getting updated at regular intervals, it may take time for all the nodes to have the same accurate network view.

- Uses fixed length sub-net, not suitable for scaling.
- Algorithm used: Bellman Ford Algorithm to find the shortest path.

2. Link State Routing

Link State Routing is another type of dynamic routing protocol in which routes advertise their updated routing tables only when some new updates are added. This results in effective use of bandwidth. All the routers keep exchanging the information dynamically regarding different links such as cost and hop count to find the best possible path.

Unit-3

- Uses variable length sub-net mask, which is scalable and uses addressing more effectively.
- Algorithm used: Djikstra's Algorithm to find the shortest path.

Let's look at the metrics used to measure the cost to travel one node to another :-

1. Hop Count: Hop count refers to the number of nodes a data packet has to traverse to reach its intended destination. Transmitting from one node to another node counts as 1 – hop count. The goal is to minimize the hop count and find the shortest path.

2. Bandwidth Consumption: Bandwidth is the ability of a network to transmit data typically measured in (Kilobits per second)kbps, mbps(Megabits per second) or Gbps (Gigabits per second). The bandwidth depends on a number of factors such as – the volume of data, traffic on a network, network speed etc. Routing decision is made in a way to ensure efficient bandwidth consumption.

3. Delay: Delay is the time it takes for a data packet to travel from source node to its destination node. There are different types of delay such as – propagation delay, transmission delay, queing delay.

4. Load: Load refers to the network traffic on a certain path in the context of routing. A data packet will be routed to the path with lesser load so that it reaches its destination in the specified time.

5. Reliability: Reliability refers to the assured delivery of the data packet to its intended destination although there are certain other factors, the data packet is routed in such a way so that it reaches its destination. The stability and availability of the link in the network is looked over before routing the data packet from a specific path.

Advantages of Routing

- Overall routing can be done in various ways its important to know requirements and use the one that fits right for our specific needs, hence the automated routing is typically preferred as the routing of packets is done by the algorithms defined and moreover the manually configurable routing can give us a fine grained control over the network.
- Routing is a high scalable operation for transmitting data that is, in a large scale enterprise networks it becomes crucial to manage information related to all the nodes that may be sharing sensitive and confidential information regarding the organization.
- Load Balancing is also one of the crucial aspects taken care of by routing data packets off the routes that are generally busy as sending data through those routes will only put our data at risk of getting lost.

Disadvantages of Routing

Unit-3

Every type of routing comes with some pros and cons here are some of the disadvantages for specific types of routing :

- Static Routing: This type of routing is appropriate only for smaller network where the network administrator has an accurate view of the network & good knowledge of topology else it might raise some security concerns and complex configuration issues.
- Dynamic Routing: Everything is done automatically by the algorithms, providing less control over the network that may not be suitable for every kind of network. It is also computationally expensive and consumes more bandwidth.
- Default Routing: The path on which the packets are to be transmitted by default is configurable but can be a complex procedure if not defined clearly.

Unit-3

Shortest Path Algorithm in Computer Network

In between sending and receiving data packets from the sender to the receiver, it will go through many routers and subnets. So as a part of increasing the efficiency in routing the data packets and decreasing the traffic, we must find the shortest path. In this article, we are discussing the shortest path algorithms.

What is Shortest Path Routing?

It refers to the algorithms that help to find the shortest path between a sender and receiver for routing the data packets through the network in terms of shortest distance, minimum cost, and minimum time.

- It is mainly for building a graph or subnet containing routers as nodes and edges as communication lines connecting the nodes.
- Hop count is one of the parameters that is used to measure the distance.
- **Hop count**: It is the number that indicates how many routers are covered. If the hop count is 6, there are 6 routers/nodes and the edges connecting them.
- Another metric is a geographic distance like kilometers.
- We can find the label on the arc as the function of bandwidth, average traffic, distance, communication cost, measured delay, mean queue length, etc.

Common Shortest Path Algorithms

- Dijkstra's Algorithm
- Bellman Ford's Algorithm

Dijkstra's Algorithm

The Dijkstra's Algorithm is a greedy algorithm that is used to find the minimum distance between a node and all other nodes in a given graph. Here we can consider node as a router and graph as a network. It uses weight of edge .ie, distance between the nodes to find a minimum distance route.

Algorithm for Dijkstra's Algorithm:

1. **Mark the source node with a current distance of 0 and the rest with infinity.**
2. **Set the non-visited node with the smallest current distance as the current node.**
3. **For each neighbor, N of the current node adds the current distance of the adjacent node with the weight of the edge connecting 0->1. If it is smaller than the current distance of Node, set it as the new current distance of N.**
4. **Mark the current node 1 as visited.**
5. **Go to step 2 if there are any nodes are unvisited.**

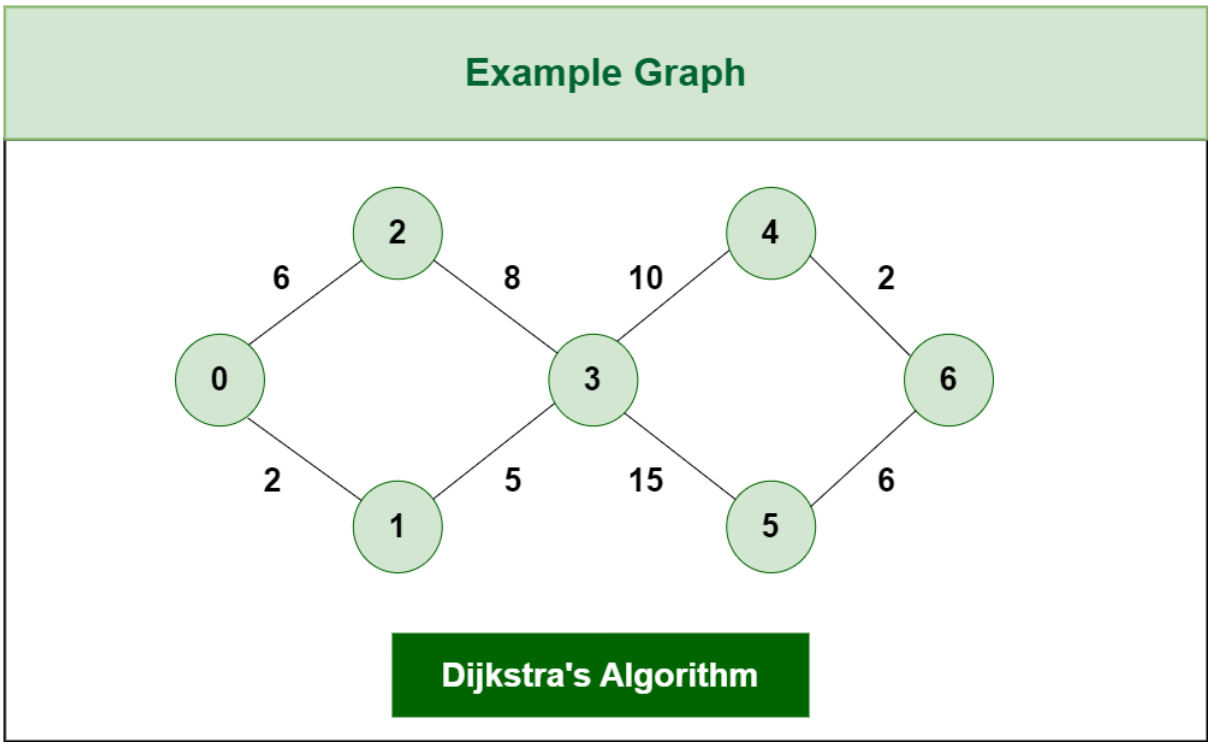
Unit-3

How does Dijkstra's Algorithm works?

Let's see how Dijkstra's Algorithm works with an example given below:

Dijkstra's Algorithm will generate the shortest path from Node 0 to all other Nodes in the graph.

Consider the below graph:



Dijkstra's Algorithm

The algorithm will generate the shortest path from node 0 to all the other nodes in the graph.

For this graph, we will assume that the weight of the edges represents the distance between two nodes.

As, we can see we have the shortest path from,
Node 0 to Node 1, from
Node 0 to Node 2, from
Node 0 to Node 3, from
Node 0 to Node 4, from
Node 0 to Node 6.

Initially we have a set of resources given below :

- ***The Distance from the source node to itself is 0. In this example the source node is 0.***

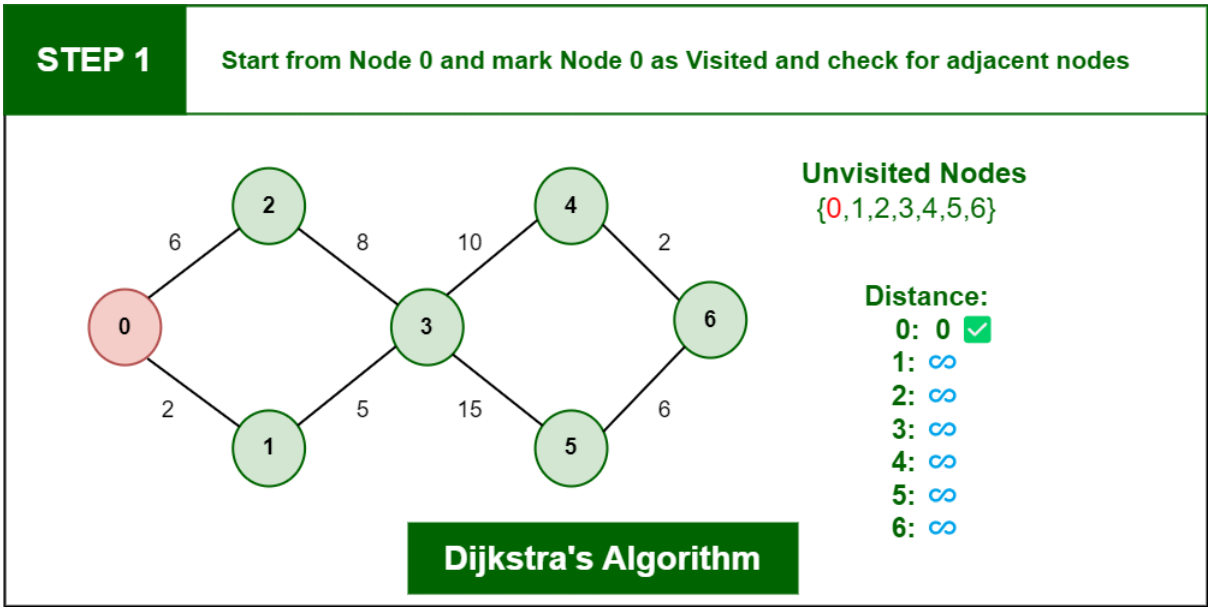
Unit-3

- *The distance from the source node to all other node is unknown so we mark all of them as infinity.*

Example: 0 -> 0, 1-> ∞,2-> ∞,3-> ∞,4-> ∞,5-> ∞,6-> ∞.

- *we'll also have an array of unvisited elements that will keep track of unvisited or unmarked Nodes.*
- *Algorithm will complete when all the nodes marked as visited and the distance between them added to the path. Unvisited Nodes:- 0 1 2 3 4 5 6.*

Step 1: Start from Node 0 and mark Node as visited as you can check in below image visited Node is marked red.

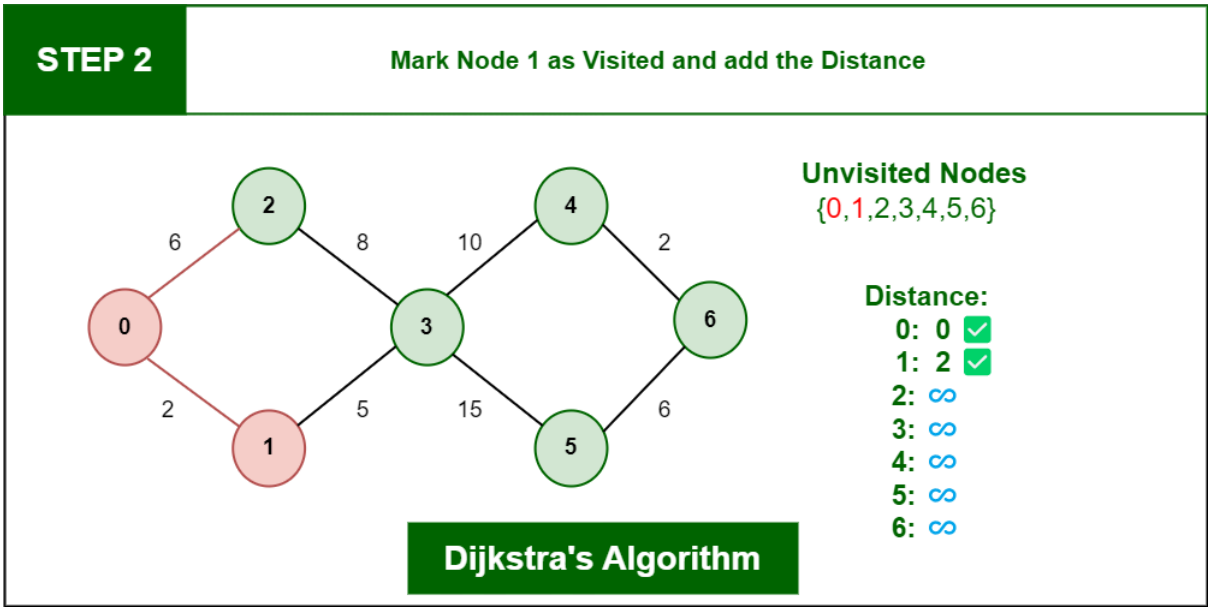


Dijkstra's Algorithm

Step 2: Check for adjacent Nodes, Now we have to choices (Either choose Node1 with distance 2 or either choose Node 2 with distance 6) and choose Node with minimum distance. In this step Node 1 is Minimum distance adjacent Node, so marked it as visited and add up the distance.

Distance: Node 0 -> Node 1 = 2

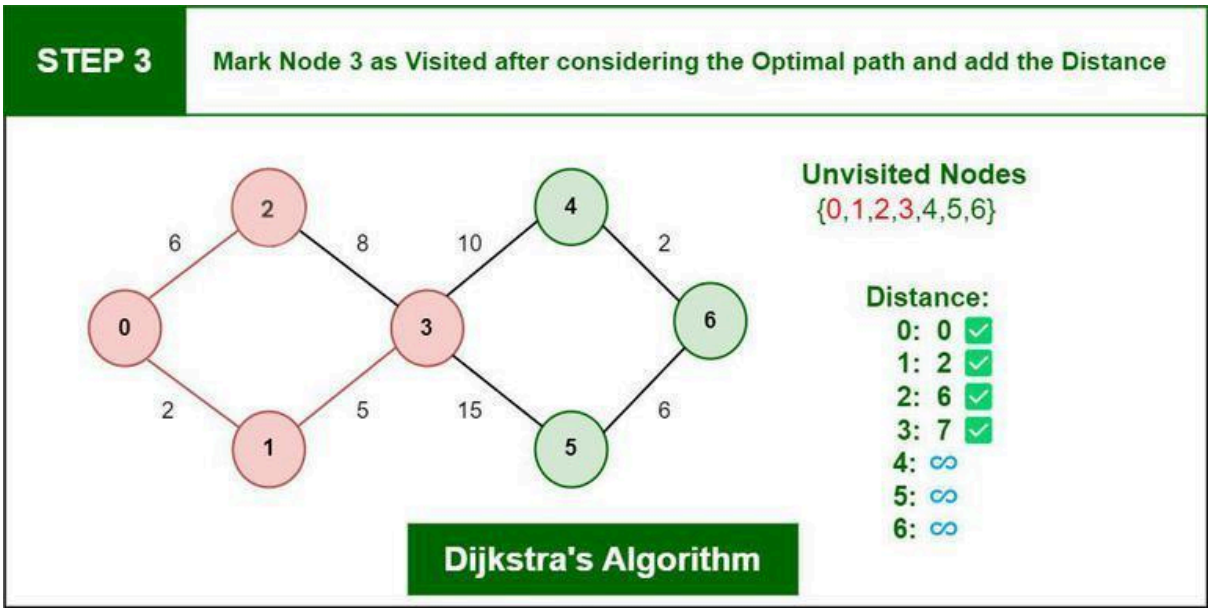
Unit-3



Dijkstra's Algorithm

Step 3: Then Move Forward and check for adjacent Node which is Node 3, so marked it as visited and add up the distance, Now the distance will be:

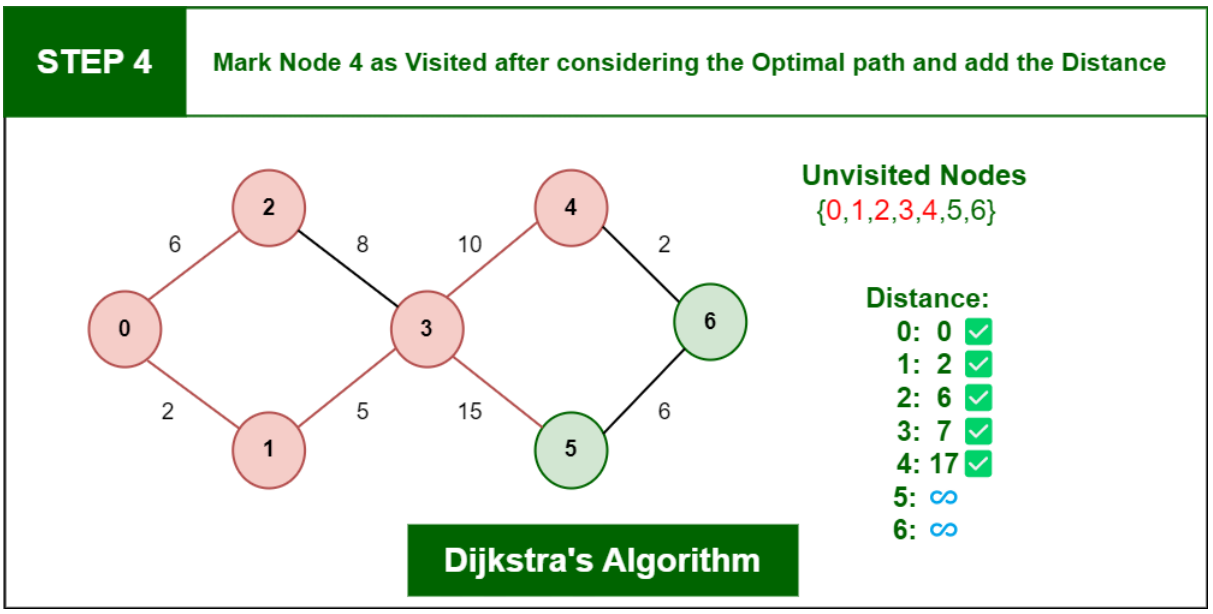
Distance: Node 0 -> Node 1 -> Node 3 = 2 + 5 = 7



Dijkstra's Algorithm

Step 4: Again we have two choices for adjacent Nodes (Either we can choose Node 4 with distance 10 or either we can choose Node 5 with distance 15) so choose Node with minimum distance. In this step Node 4 is Minimum distance adjacent Node, so marked it as visited and add up the distance.

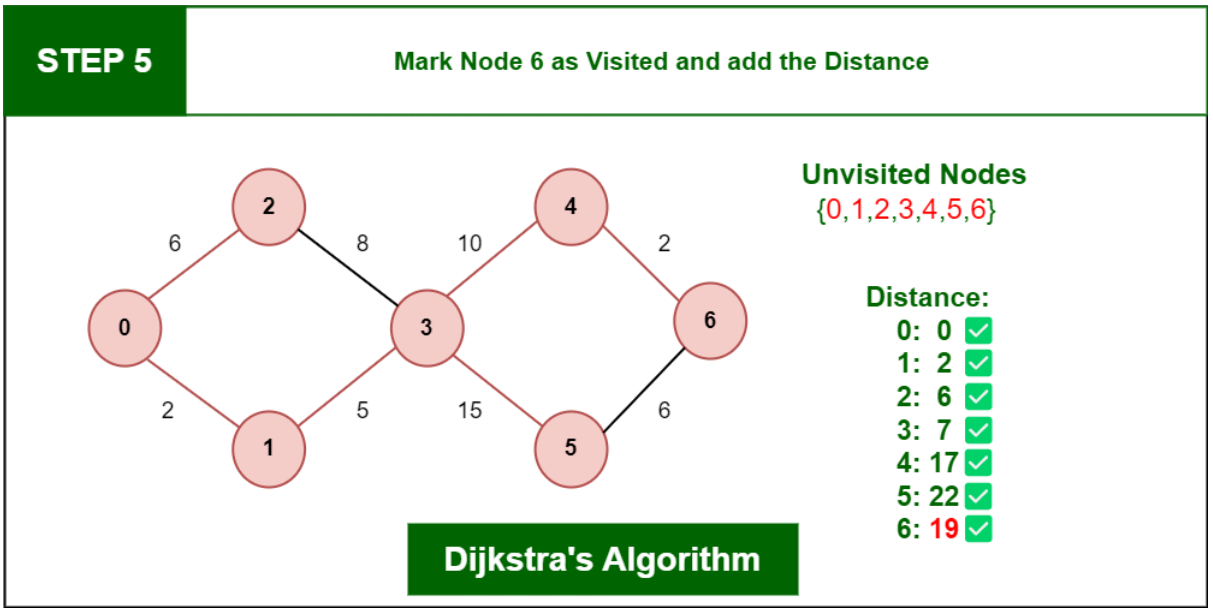
Distance: Node 0 -> Node 1 -> Node 3 -> Node 4 = 2 + 5 + 10 = 17



Dijkstra's Algorithm

Step 5: Again, Move Forward and check for adjacent Node which is Node 6, so marked it as visited and add up the distance, Now the distance will be:

Distance: Node 0 -> Node 1 -> Node 3 -> Node 4 -> Node 6 = 2 + 5 + 10 + 2 = 19



Dijkstra's Algorithm

So, the Shortest Distance from the Source Vertex is 19 which is optimal one

Unit-3

Hierarchical Routing

Hierarchical routing protocols consist of a hierarchical topology to organize the network and routing information. Multiple layers and levels are introduced in a network. Each layer may be assigned a different responsibility like forwarding packets, maintaining routing tables, etc. HRPs are valuable for large networks, as they provide the capability of organizing network information and reducing the amount of routing information that should be exchanged between nodes. Hence, HRPs demonstrate significant scalability and fault tolerance. This is attributed to their hierarchical structure, which provides redundancy and facilitates the efficient distribution of routing data throughout the network.

Differences Between Hierarchical and Flat Routing Protocol

Basis	**Hierarchical Routing Protocol**	**Flat Routing Protocol**
Topology	Hierarchical topology used	Single-level topology
Network	Suitable for large networks	Suitable for small networks
Routing Tables	Uses multiple routing tables to organize network information	The single routing table is used.
Scalability	Highly scalable, able to handle expansive networks with multiple layers	Limited scalability, can get congested and wasteful as the network grows

Unit-3

Basis	Hierarchical Routing Protocol	Flat Routing Protocol
Complexity	More complex to set up and maintain	Simpler in comparison
Optimality	Simple but non-optimal	This can be made optimal by making it more complex
Scheduling	It is a channel reservation-based scheduling	It is a contention-based scheduling
Collisions	Collisions are avoided	Collisions may occur frequently
Allocation	Ensures fair channel allocation	The allocation might not be fair most of the time
Energy	Energy dissipation is constant	Energy Dissipation depends on patterns in traffic

If one has to choose between the two, the choice might depend on the nature of the network that requires routing and its needs and characteristics

Advantages of HRP

- **Scalability:** Hierarchical routing protocols exhibit excellent scalability by partitioning the network into smaller segments or areas. This division reduces the demand for routing tables and updates on each router, enhancing network efficiency and decreasing overall network traffic.
- **Better Traffic Control:** Hierarchical routing protocols demonstrate superior traffic management compared to flat routing protocols. The hierarchical framework enables more efficient traffic control, mitigating the need for unnecessary routing updates and preventing loops in the network.
- **Easy to Manage:** The organisational framework in these protocols facilitates simplified management and maintenance. Segmentation of the network into manageable sections enhances the ease of troubleshooting and diagnosing issues.

Unit-3

Disadvantages of HRP

- **Complexity**: Hierarchical routing protocols tend to be more complicated compared to flat routing protocols. The presence of additional layers and segments necessitates more extensive configuration, posing potential challenges in implementation.
- **Latency**: Latency may be introduced into the network due to the presence of additional layers and segments. Such delays in data transmission can pose challenges, particularly for real-time applications.

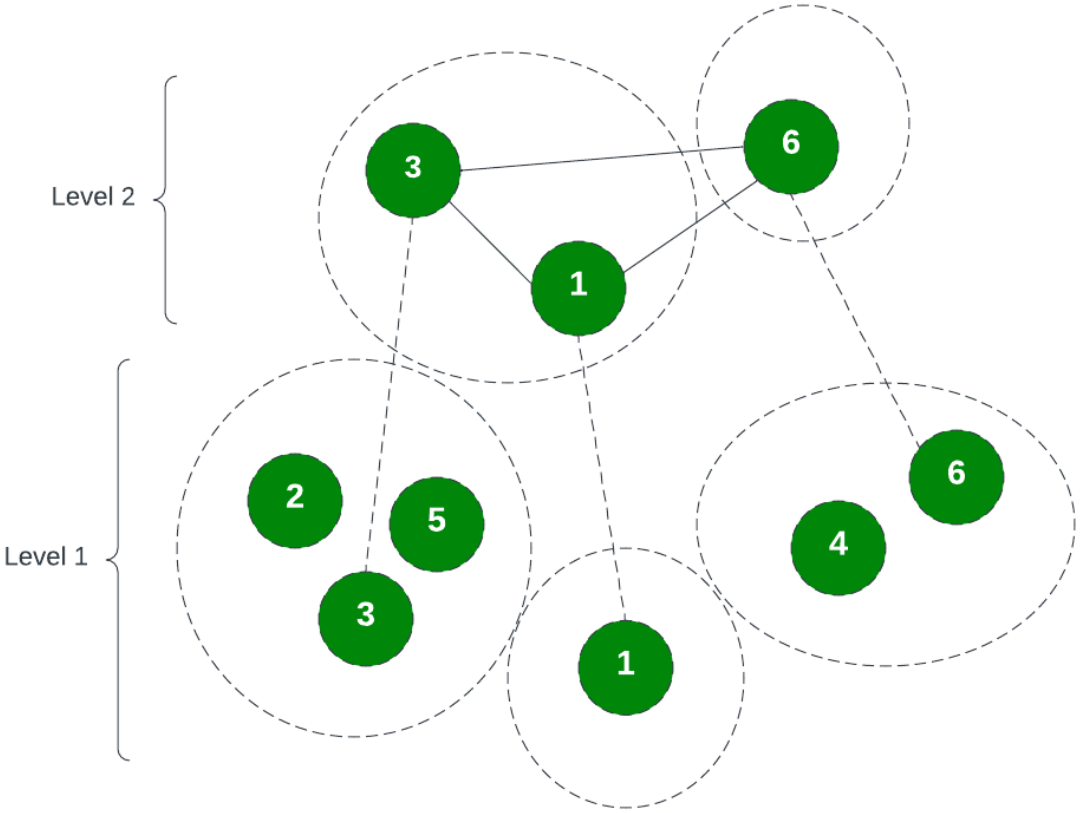
Hierarchical State Routing Protocol

The hierarchical state routing protocol (HSR) is a multi-level and distributed routing protocol. It makes use of clustering, present on different levels. Each level of cluster has the potential to manage its members efficiently. This improves resource allocation and management. Leaders are elected in each cluster, which form the members of the immediate higher level.

Various clustering algorithms are employed for electing leaders in each level. There can be two types of clustering: physical and logical. One level of physical clustering is done among nodes that are available in a single wireless hop. The other level is made among nodes that act as cluster heads of each of the first-level clusters. Logical clustering scheme of HSR is based on relationships among nodes rather than their geographical locations.

Nodes have complete details about how to route packets to destinations within its own cluster. But it does not have any information on the internal structure of other regions.

Unit-3



Multilayer Clustering in HSR Protocol

At the lowest level, there are three clusters. Nodes 1, 3 and 6 are classified as cluster leaders, or gateway nodes. A cluster leader is entrusted with responsibilities such as slot/frequency/code allocation, call admission control, scheduling of packet transmissions, exchange of routing information, and handling route breaks. The higher level nodes are further organized into clusters.

Working of HSRP

- Each node maintains information about its neighboring node and their link status
- The information regarding the cluster is broadcast in the network at regular intervals.
- The job of the cluster leader is to exchange topology and link state routing information among other cluster leaders of neighborhood clusters.
- The exchange of link state information is carried out over multiple hops that consist of gateway nodes and cluster-heads.
- The path between two cluster-heads which is formed by multiple wireless links is called virtual link.

- The link status for the virtual link(otherwise called tunnel) is obtained from the link status parameters of the wireless links that constitute the virtual link.
- After obtaining information from its peers, the cluster head floods the information to the lower levels.
- Hierarchical addressing in HSR reduces routing information compared to link-state routing. HSR's HID and node ID structure simplifies addressing and topology management.
- HSR tables update with received routing packets, maintaining accurate hierarchy information.

Kinds of Nodes in a Cluster

- **Cluster Head** – This node acts as a local coordinator of transmissions within the cluster. Cluster head performs the function of allocating slot or frequency or code, call admission control, and most importantly scheduling packet transmission.
- **Gateway Node** – These nodes are associated with more than two clusters.
- **Internal Node –** These are the members of the clusters at the most root level

Virtual Link – Information is exchanged between the gateway nodes and leader nodes through this path.

Advantages

- **Reduction in Table Size:** HSR protocol reduces the routing table size by making use of hierarchy information. The storage space required is of O(N x M) whereas in flat topology the space required is O(NM). Here, N is the average number of nodes in a cluster and m is the number of levels.

Disadvantages

- **Overhead Involved:** The overhead for exchanging packets containing information about multiple levels of hierarchy and cluster head appointment process makes the protocol expensive from the ad hoc wireless network point of view.
- **Scalability:** The number of nodes involved in an ad hoc network does not grow to the dimensions of the number of nodes in the Internet which is more suited for hierarchical routing.
- **Time Consuming:** Sharing information across all levels of the hierarchy and conducting leader elections within each cluster is a time-consuming process.
- **Regular Hello Messages:** To preserve the network's topology, nodes must regularly send hello messages to their neighboring nodes, which contributes to overhead.
- **Power Supply:** The concentration of routes through cluster leaders imposes additional strain on the power supply of these leaders.

Unit-3

Unit-3

Difference Between Broadcast and Multicast

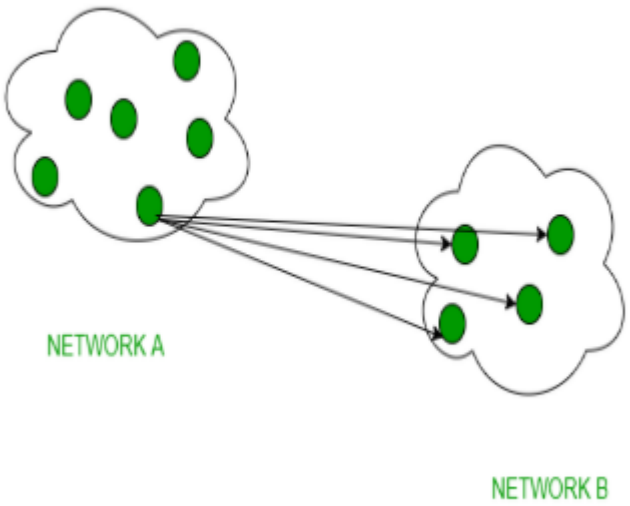
The world of computer networks has a variety of communication mechanisms and protocols that provide a set of guidelines and rules to be followed while transmitting data from one node to another. These mechanisms and protocols determine the efficiency and reliability of the inter-connected and intra-connected network systems. In this article, we'll learn about the difference between two of the most commonly used message distribution mechanisms – Broadcast and Multicast, shedding light on the unique characteristics of both.

Broadcast and a Multicast are two different communication mechanism in computer networks for transmitting data between the nodes in a network.

1. Broadcast

Broadcast transfer (one-to-all) techniques and can be classified into two types : Limited Broadcasting and direct Broadcasting. In broadcasting mode, transmission happens from one host to all the other hosts connected on the LAN. In simple words, broadcasting is a communication mechanism where data is sent to all the nodes in a network. The broadcast address is a special reserved address bits for broadcasting messages in a network, we can calculate the broadcast address given its IP address and the subnet Mask.

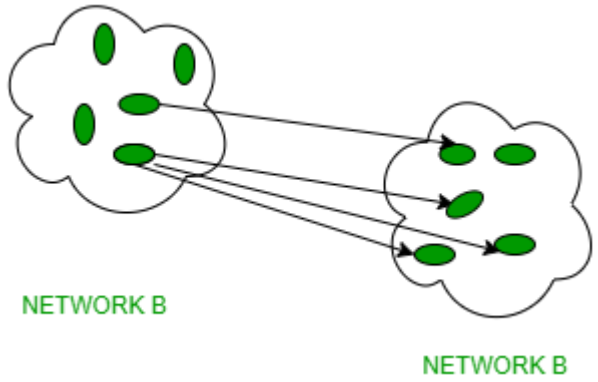
Devices such as bridge uses this. A protocol like ARP(address resolution protocols) implements this, in order to know the MAC address for the corresponding IP address of the host machine. ARP does IP address to MAC address translation. RARP does the reverse.



2. Multicast

Multicasting has one/more senders and one/more recipients participate in data transfer traffic. In multicasting traffic recline between the boundaries of unicast and broadcast. It server's direct single copies of data streams and that are then simulated and routed to hosts

that request it. IP multicast requires support of some other protocols such as IGMP (Internet Group Management Protocol), Multicast routing for its working. And also in Classful IP addressing Class D is reserved for multicast groups.



Difference Between Broadcast and Multicast

Broadcast	**Multicast**
It has one sender and multiple receivers.	It has one or more senders and multiple receivers.
It sent data from one device to all the other devices in a network.	It sent data from one device to multiple devices.
It works on star and bus topology.	It works on star, mesh, tree and hybrid topology.
It scale well across large networks.	It does not scale well across large networks.
Its bandwidth is wasted.	It utilizes bandwidth efficiently.
It has one-to-all mapping.	It has one-to-many mapping.
Hub is an example of a broadcast device.	Switch is an example of a multicast device.

Unit-3

Broadcast	**Multicast**
It increases network traffic because the data packets are sent to every other node in the network	It doesn’t increase network traffic
The message to be sent should be tripled checked as some sensitive or confidential information shouldn’t be distributed to everyone in the network	No such issue, because the message is target to only selected people.

Unit-3

Classless Inter Domain Routing (CIDR)

Classless Inter-Domain Routing (CIDR) is a method of IP address allocation and IP routing that allows for more efficient use of IP addresses. CIDR is based on the idea that IP addresses can be allocated and routed based on their network prefix rather than their class, which was the traditional way of IP address allocation.

CIDR addresses are represented using a slash notation, which specifies the number of bits in the network prefix. For example, an IP address of 192.168.1.0 with a prefix length of 24 would be represented as 192.168.1.0/24. This notation indicates that the first 24 bits of the IP address are the network prefix and the remaining 8 bits are the host identifier.

Several Advantages of the Traditional Class-Based Addressing System of CIDR

- Efficient use of IP addresses: CIDR allows for more efficient use of IP addresses by allowing the allocation of IP addresses based on their network prefix rather than their class.
- Flexibility: CIDR allows for more flexible IP address allocation, as it allows for the allocation of arbitrary-sized blocks of IP addresses.
  Better routing: CIDR allows for better routing of IP traffic, as it allows routers to aggregate IP addresses based on their network prefix, reducing the size of routing tables.
- Reduced administrative overhead: CIDR reduces administrative overhead by allowing for the allocation and routing of IP addresses in a more efficient and flexible way.
- In summary, CIDR is a method of IP address allocation and routing that allows for more efficient use of IP addresses and better routing of IP traffic. It has several advantages over the traditional class-based addressing system, including greater flexibility, better routing, and reduced administrative overhead.

As with any technology or system, there are advantages and disadvantages of using CIDR:

Advantages of CIDR

- Efficient use of IP addresses: CIDR allows for more efficient use of IP addresses, which is important as the pool of available IPv4 addresses continues to shrink.
- Flexibility: CIDR allows for more flexible allocation of IP addresses, which can be important for organizations with complex network requirements.
- Better routing: CIDR allows for more efficient routing of IP traffic, which can lead to better network performance. Reduced administrative overhead: CIDR reduces administrative overhead by allowing for easier management of IP addresses and routing.

Unit-3

Disadvantages of CIDR

- Complexity: CIDR can be more complex to implement and manage than traditional class-based addressing, which can require additional training and expertise.
- Compatibility issues: Some older network devices may not be compatible with CIDR, which can make it difficult to transition to a CIDR-based network.
- Security concerns: CIDR can make it more difficult to implement security measures such as firewall rules and access control lists, which can increase security risks.
- Overall, CIDR is a useful and efficient method of IP address allocation and routing, but it may not be suitable for all organizations or networks. It is important to weigh the advantages and disadvantages of CIDR and consider the specific needs and requirements of your network before implementing CIDR.

Unit-3

Internet Control Message Protocol (ICMP)

Internet Control Message Protocol is known as ICMP. The protocol is at the network layer. It is mostly utilized on network equipment like routers and is utilized for error handling at the network layer. Since there are various kinds of network layer faults, ICMP can be utilized to report and troubleshoot these errors.

Since IP does not have an inbuilt mechanism for sending error and control messages. It depends on Internet Control Message Protocol(ICMP) to provide error control. In this article, we are going to discuss ICMP in detail along with their uses, messages, etc.

What is ICMP?

ICMP is used for reporting errors and management queries. It is a supporting protocol and is used by network devices like routers for sending error messages and operations information. For example, the requested service is not available or a host or router could not be reached.

Since the IP protocol lacks an error-reporting or error-correcting mechanism, information is communicated via a message. For instance, when a message is sent to its intended recipient, it may be intercepted along the route from the sender. The sender may believe that the communication has reached its destination if no one reports the problem. If a middleman reports the mistake,

Uses of ICMP

ICMP is used for error reporting if two devices connect over the internet and some error occurs, So, the router sends an ICMP error message to the source informing about the error. For Example, whenever a device sends any message which is large enough for the receiver, in that case, the receiver will drop the message and reply to the ICMP message to the source.

Another important use of ICMP protocol is used to perform network diagnosis by making use of traceroute and ping utility.

Traceroute: Traceroute utility is used to know the route between two devices connected over the internet. It routes the journey from one router to another, and a traceroute is performed to check network issues before data transfer.

Ping: Ping is a simple kind of traceroute known as the echo-request message, it is used to measure the time taken by data to reach the destination and return to the source, these replies are known as echo-replies messages.

Unit-3

How Does ICMP Work?

ICMP is the primary and important protocol of the IP suite, but ICMP isn't associated with any transport layer protocol (TCP or UDP) as it doesn't need to establish a connection with the destination device before sending any message as it is a connectionless protocol.

The working of ICMP is just contrasting with TCP, as TCP is a connection-oriented protocol whereas ICMP is a connectionless protocol. Whenever a connection is established before the message sending, both devices must be ready through a TCP Handshake.

ICMP packets are transmitted in the form of datagrams that contain an IP header with ICMP data. ICMP datagram is similar to a packet, which is an independent data entity.

ICMP Packet Format

ICMP header comes after IPv4 and IPv6 packet header.

<table>
<tr><td>Type(8 bit)</td><td>Code(8 bit)</td><td>CheckSum(16 bit)</td></tr>
<tr><td colspan="3">Extended Header(32 bit)</td></tr>
<tr><td colspan="3">Data/Payload(Variable Length)</td></tr>
</table>

ICMPv4 Packet Format

In the ICMP packet format, the first 32 bits of the packet contain three fields:

Type (8-bit): The initial 8-bit of the packet is for message type, it provides a brief description of the message so that receiving network would know what kind of message it is receiving and how to respond to it. Some common message types are as follows:

- Type 0 – Echo reply
- Type 3 – Destination unreachable
- Type 5 – Redirect Message
- Type 8 – Echo Request
- Type 11 – Time Exceeded
- Type 12 – Parameter problem

Code (8-bit): Code is the next 8 bits of the ICMP packet format, this field carries some additional information about the error message and type.

Unit-3

Checksum (16-bit): Last 16 bits are for the checksum field in the ICMP packet header. The checksum is used to check the number of bits of the complete message and enable the ICMP tool to ensure that complete data is delivered.

The next 32 bits of the ICMP Header are Extended Header which has the work of pointing out the problem in IP Message. Byte locations are identified by the pointer which causes the problem message and receiving device looks here for pointing to the problem.

The last part of the ICMP packet is Data or Payload of variable length. The bytes included in IPv4 are 576 bytes and in IPv6, 1280 bytes.

ICMP in DDoS Attacks

In Distributed DOS (DDoS) attacks, attackers provide so much extra traffic to the target, so that it cannot provide service to users. There are so many ways through which an attacker executes these attacks, which are described below.

Ping of Death Attack

Whenever an attacker sends a ping, whose size is greater than the maximum allowable size, oversized packets are broken into smaller parts. When the sender re-assembles it, the size exceeds the limit which causes a buffer overflow and makes the machine freeze. This is simply called a Ping of Death Attack. Newer devices have protection from this attack, but older devices did not have protection from this attack.

ICMP Flood Attack

Whenever the sender sends so many pings that the device on whom the target is done is unable to handle the echo request. This type of attack is called an ICMP Flood Attack. This attack is also called a ping flood attack. It stops the target computer's resources and causes a denial of service for the target computer.

Smurf Attack

Smurf Attack is a type of attack in which the attacker sends an ICMP packet with a spoofed source IP address. These type of attacks generally works on older devices like the ping of death attack.

Types of ICMP Messages

Type	Code	Description
0 – Echo Reply	0	Echo reply
3 – Destination Unreachable	0	Destination network unreachable

Unit-3

Type	Code	Description
	1	Destination host unreachable
	2	Destination protocol unreachable
	3	Destination port unreachable
	4	Fragmentation is needed and the DF flag set
	5	Source route failed
5 – Redirect Message	0	Redirect the datagram for the network
	1	Redirect datagram for the host
	2	Redirect the datagram for the Type of Service and Network
	3	Redirect datagram for the Service and Host
8 – Echo Request	0	Echo request

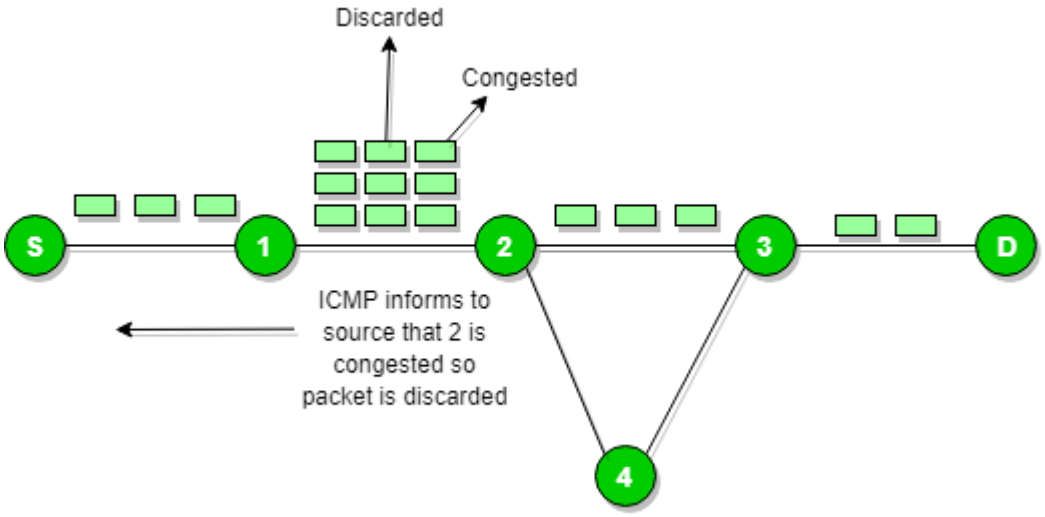
Unit-3

Type	Code	Description
9 – Router Advertisement	0	Use to discover the addresses of operational routers
10 – Router Solicitation	0	
11 – Time Exceeded	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded.
12 – Parameter Problem	0	The pointer indicates an error.
	1	Missing required option
	2	Bad length
13 – Timestamp	0	Used for time synchronization
14 – Timestamp Reply	0	Reply to Timestamp message

Source Quench Message

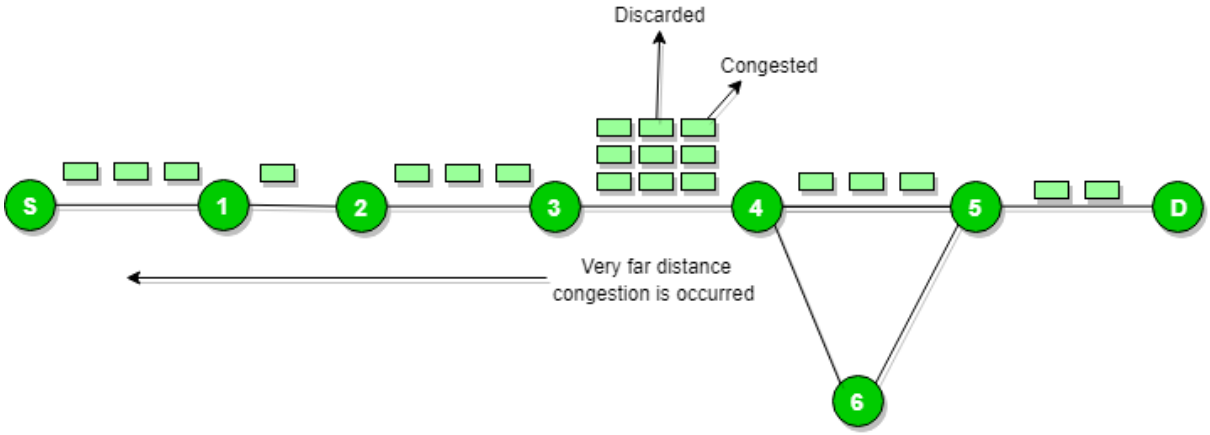
A source quench message is a request to decrease the traffic rate for messages sent to the host destination) or we can say when receiving host detects that the rate of sending packets (traffic rate) to it is too fast it sends the source quench message to the source to slow the pace down so that no packet can be lost.

Unit-3



Source Quench Message

ICMP will take the source IP from the discarded packet and inform the source by sending a source quench message. The source will reduce the speed of transmission so that router will be free from congestion.



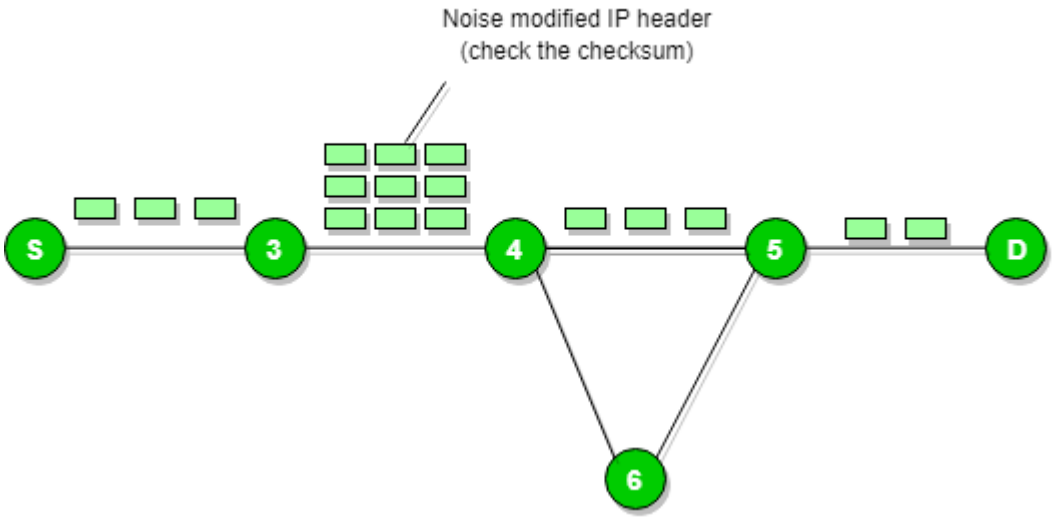
Source Quench Message with Reduced Speed

When the congestion router is far away from the source the ICMP will send a hop-by-hop source quench message so that every router will reduce the speed of transmission.

Parameter Problem

Whenever packets come to the router then the calculated header checksum should be equal to the received header checksum then only the packet is accepted by the router.

Unit-3

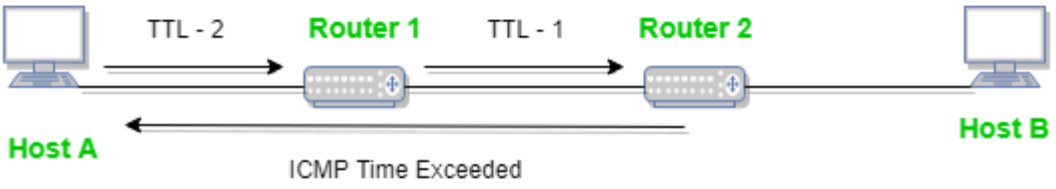


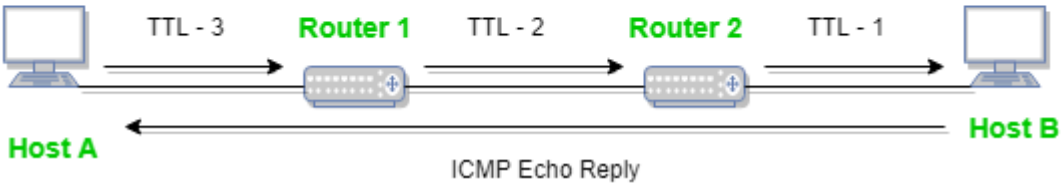
Parameter Problem

If there is a mismatch packet will be dropped by the router.

ICMP will take the source IP from the discarded packet and inform the source by sending a parameter problem message.

Time Exceeded Message





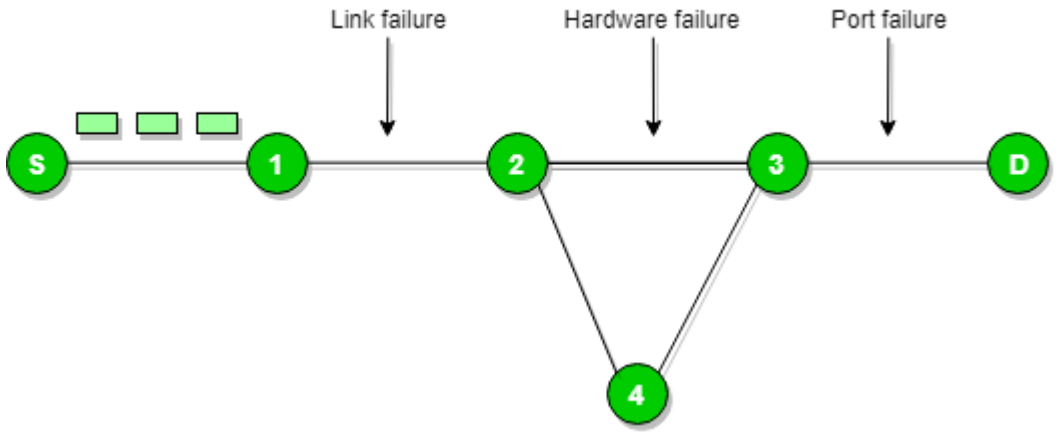
Time Exceeded Message (Time to Live-TTL)

Unit-3

A notification with the subject line “Time Exceeded” is typically generated by routers or gateways. You need to know what an IP header is in a packet in order to comprehend this ICMP message in its entirety. The IP protocol structure is covered in great detail in the section on IP Protocol, which is freely available to our readers.

Destination Un-reachable

The destination is unreachable and is generated by the host or its inbound gateway to inform the client that the destination is unreachable for some reason.



Destination Un-reachable

There is no necessary condition that only the router gives the ICMP error message time the destination host sends an ICMP error message when any type of failure (link failure, hardware failure, port failure, etc) happens in the network.

Advantages of ICMP

- Network devices use ICMP to send error messages, and administrators can use the Ping and Tracert commands to debug the network.
- These alerts are used by administrators to identify issues with network connectivity.
- A prime example is when a destination or gateway host notifies the source host via an ICMP message if there is a problem or a change in network connectivity that needs to be reported. Examples include when a destination host or networking becomes unavailable, when a packet is lost during transmission, etc.
- Furthermore, network performance and connection monitoring tools commonly employ ICMP to identify the existence of issues that the network team has to resolve.
- One quick and simple method to test connections and find the source is to use the ICMP protocol, which consists of queries and answers.

Disadvantages of ICMP

Unit-3

- If the router drops a packet, it may be due to an error; but, because to the way the IP (internet protocol) is designed, there is no way for the sender to be notified of this problem.
- Assume, while a data packet is being transmitted over the internet, that its lifetime is over and that the value of the time to live field has dropped to zero. In this case, the data packet is destroyed.
- Although devices frequently need to interact with one another, there isn't a standard method for them to do so in Internet Protocol. For instance, the host needs to verify the destination's vital signs to see if it is still operational before transmitting data.

Unit-3

IGMP Protocol

IGMP is an abbreviated form of Internet Group Management Protocol(IGMP). Mainly the Internet Protocol can be involved in the two types of communication i.e, Unicasting and multicasting. IGMP is one of the necessary but not the efficient protocol that is involved in Multicasting.

IGMP is basically a companion of Internet Protocol(IP).

IGMP is not a multicasting routing protocol but it is a protocol that manages the group membership. This protocol mainly helps the multicast routers in order to create and update a list of loyal members that are related to each router interface.

This protocol is used in streaming videos, gaming, or web conferencing tools.

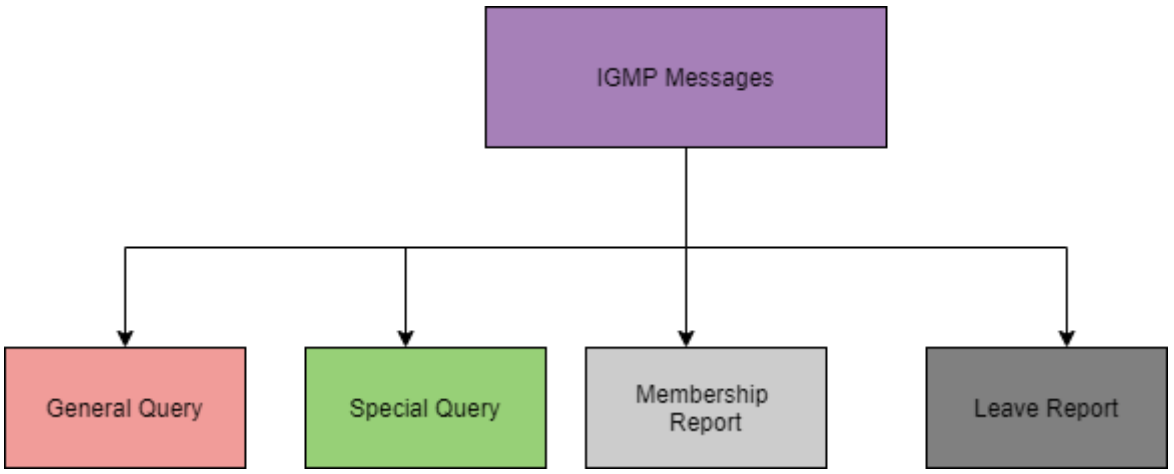
IGMP Messages

There are two versions of IGMP: IGMPv1 and IGMPv2.

The version IGMPv2 has three types of messages:

- The Query
- The Membership report
- The Leave report.

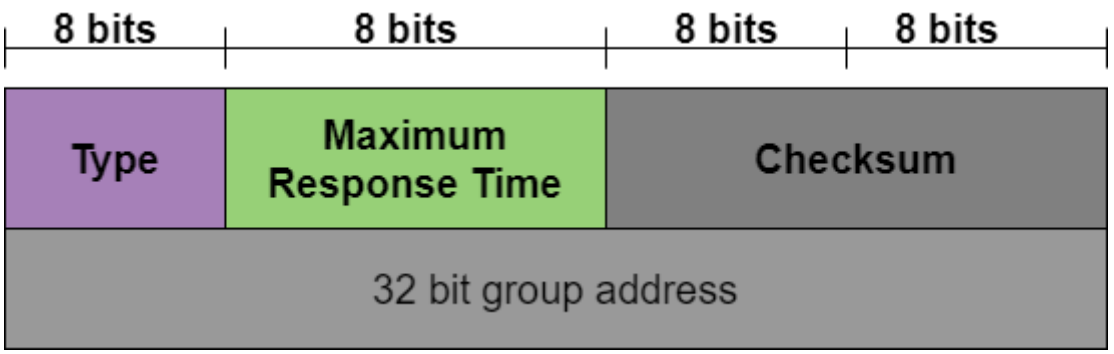
There are two types of Query messages: **General and Special**



Message Format

Let us now take a look at the format of IGMP(Version 2):

Unit-3



Type

This is an 8-bit field and is mainly used to define the type of the message. The value of the type can be in both hexadecimal as well as binary notations.

Type
General or Special Query
Membership report
Leave Report

Maximum Response Time

The size of this field is also 8 bit and it mainly defines the amount of time in which query must be answered. The value of this field is nonzero in the query message; while its value is zero in the other two types.

Checksum

The size of this field is 16 bit and it carries the checksum. The checksum is mainly calculated over the 8-byte message.

Unit-3

Group Address

The value of this field is 0 in the case of the general query message. In the case of a special query, membership report, and leave report messages the value of this field defines the groupid.

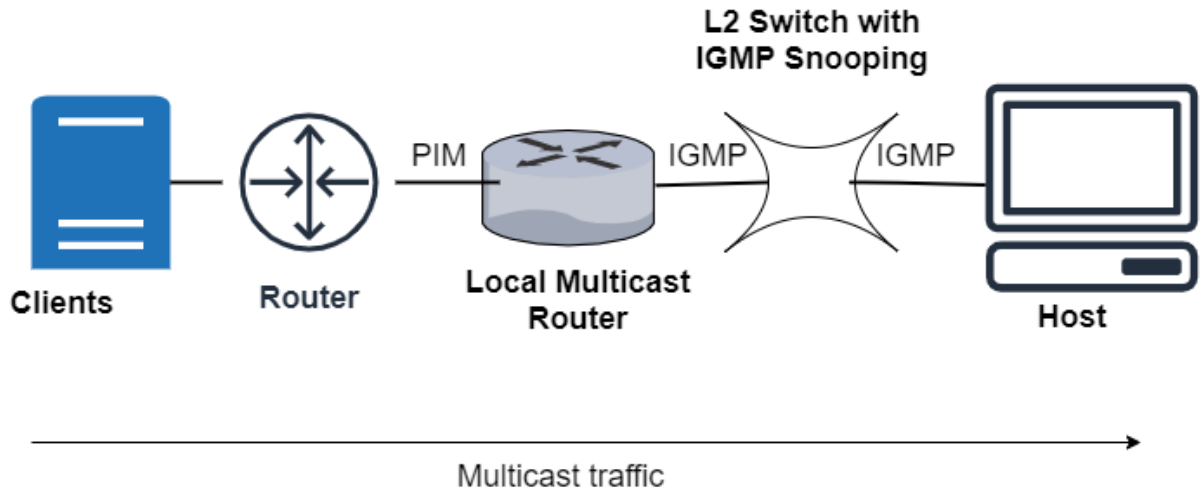
Working of IGMP

This protocol mainly works on the device that has the capability of handling multiple groups and used for dynamic multicasting; these devices mainly allow the host in order to join or leave the membership in the multicast group.

Also, these devices are allowed to add and remove the clients from the group.

IGMP protocol mainly **operates in** between the **host and local multicast router**.

At the time when there is a creation of the multicast group, the multicast group address is in the range of class D (224–239) IP addresses and is forwarded as the destination IP address in the packet.



L2 means level-2 devices like switches; these are mainly used in between the host and multicast router for the snooping of IGMP.

IGMP snooping: It is a process that is used to listen to the IGMP network traffic in a controlled manner.

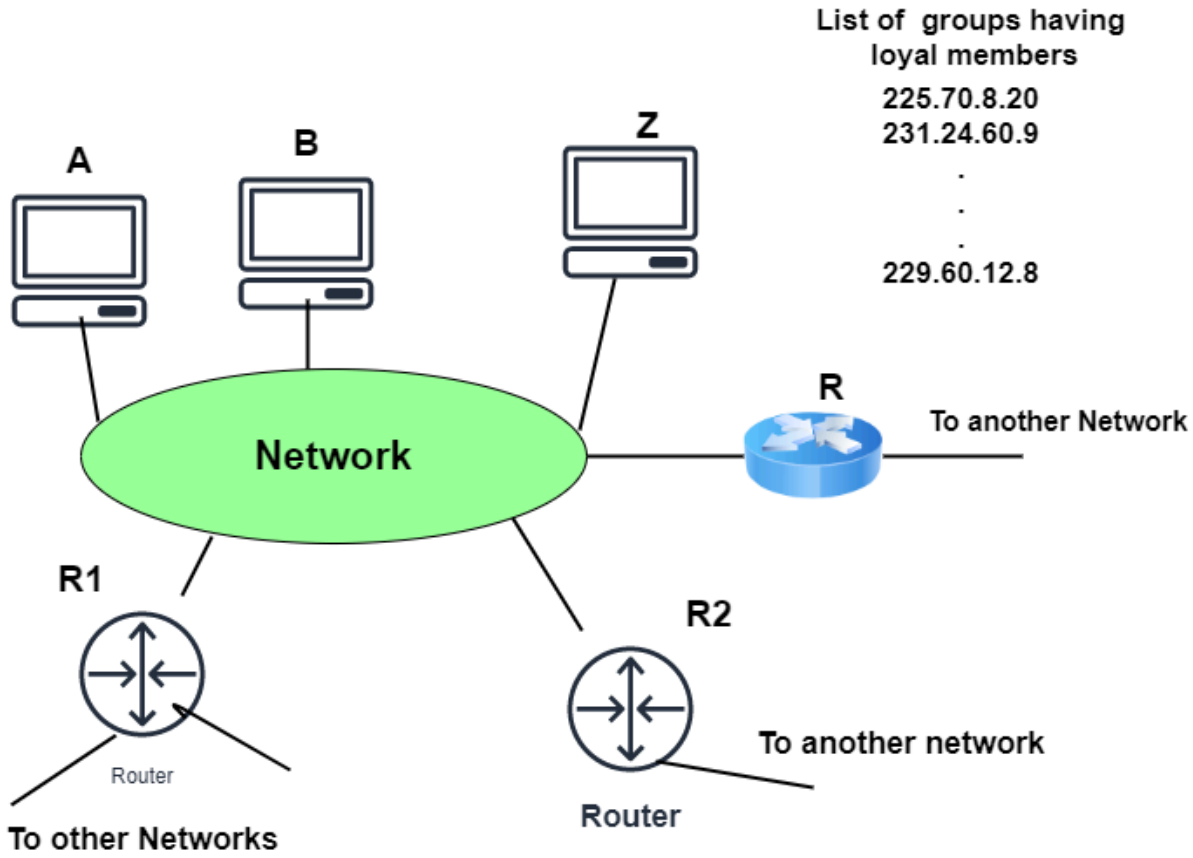
The switch mainly receives the message from the host and then forwards the membership report mainly to the local multicast router. After that, the multicast traffic is then further forwarded to remote routers from local multicast routers using PIM (Protocol Independent Multicast) protocol so that the clients can receive the message/data packets.

If the Clients wish to join the network then they can send a join message in the query and then the switch intercepts the message and then adds the ports of clients to its multicast routing table.

IGMP Operation

The Internet Group Management Protocol operates locally. The Multicast router that is connected to the network mainly has a list of multicast addresses of the group with at least one loyal member in that network. And for each group, there is mainly one router that has the duty of distributing the multicast packets destined for that group.

This simply indicates that in the case if there are three multicast routers connected to a network then their list of **groupids** are **mutually exclusive.**



Given below are the operations of IGMP:

- **Joining a Group**
  - In this operation, both the host and the router can join a group. Whenever a process on the host wants to join a group then it simply sends the request to the host. After that, the host then adds the name of the process and the name of the group to its list.
  - In case, if this is the first entry of that particular group, then the host sends the membership report message to the multicast router of the group.

    - And if the entry is not the first entry then there is no need of sending such a message.
- **Leaving a group**
    - Whenever the host finds that there is no process that is interested in the group then it mainly leaves a report message.
    - The membership is not disinfected by the multicast router of the group, rather than it immediately transmits the query packets repeatedly to see if anyone is still interested or not.
    - And in case if it gets the response in the form of a membership report message then the membership of the host or network is preserved.
- **Monitoring Membership**
  Mainly the general query message does not define a particular group.
- **Delayed Response**
  In order to prevent unnecessary traffic, the IGMP mainly makes use of a delayed response strategy.

Advantages of IGMP

The listed below are some of the benefits offered by the IGMP:

- With the help of this protocol, the bandwidth is utilized efficiently aa because all the shared links are connected.
- Using this protocol, the host can immediately leave a multicast group and then join another group.
- The performance of this protocol is optimized as there is no transmission of junk packets to the host.

Disadvantages of IGMP

Given below are some of the drawbacks of the IGMP :

- During filtering and security, it does not offers good efficiency.
- This protocol is vulnerable to Denial of Service(DoS) attacks.
- Network congestion can occur due to a lack of TCP.