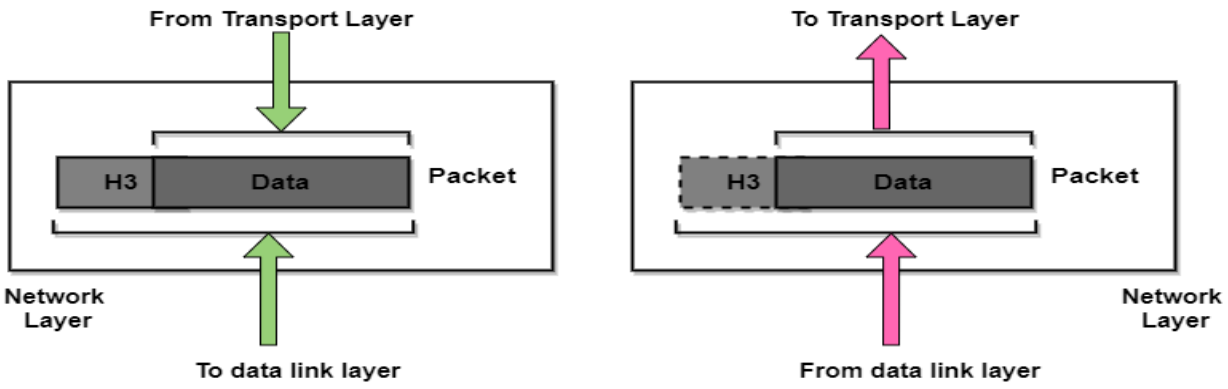
UNIT – III
Network Layer

- The Network Layer is the third layer of the OSI model.
- It handles the service requests from the transport layer and further forwards the service request to the data link layer.
- The network layer translates the logical addresses into physical addresses
- It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
- The main role of the network layer is to move the packets from sending host to the receiving host.



Design Issues for the Layers

- **Addressing**
  - consequence of having multiple destinations
- **Error Control**
  - The receiver should be able to inform sender which data was received correctly
- **Flow Control**
  - Keep sender from swamping slow receiver with data
  - Keep the sender from swamping with data slow networks
- **Multiplexing**
  - Use same communication channel for multiple, unrelated conversations
- **Routing**
  - When multiple paths between source and destination, one path must be chosen

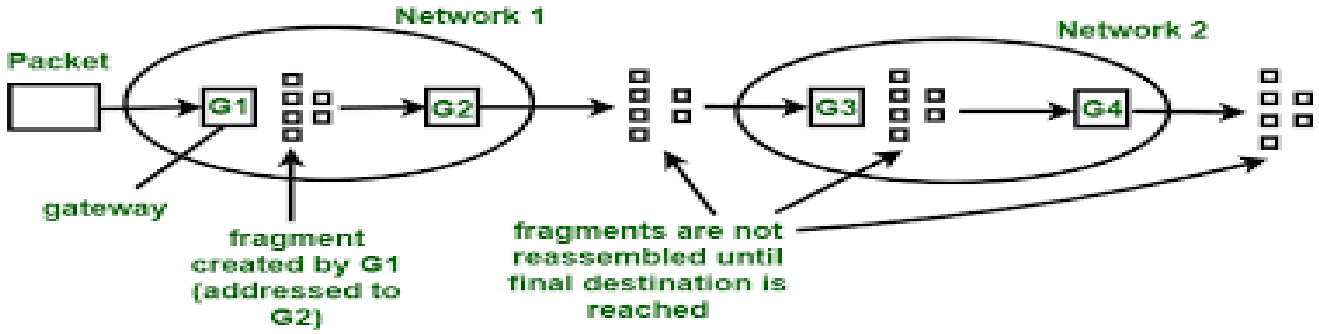
Services Provided by the Network Layer

- Guaranteed delivery: This layer provides the service which guarantees that the packet will arrive at its destination.
- Guaranteed delivery with bounded delay: This service guarantees that the packet will be delivered within a specified host-to-host delay bound.
- In-Order packets: This service ensures that the packet arrives at the destination in the order in which they are sent.
- Guaranteed max jitter: This service ensures that the amount of time taken between two successive transmissions at the sender is equal to the time between their receipt at the destination.

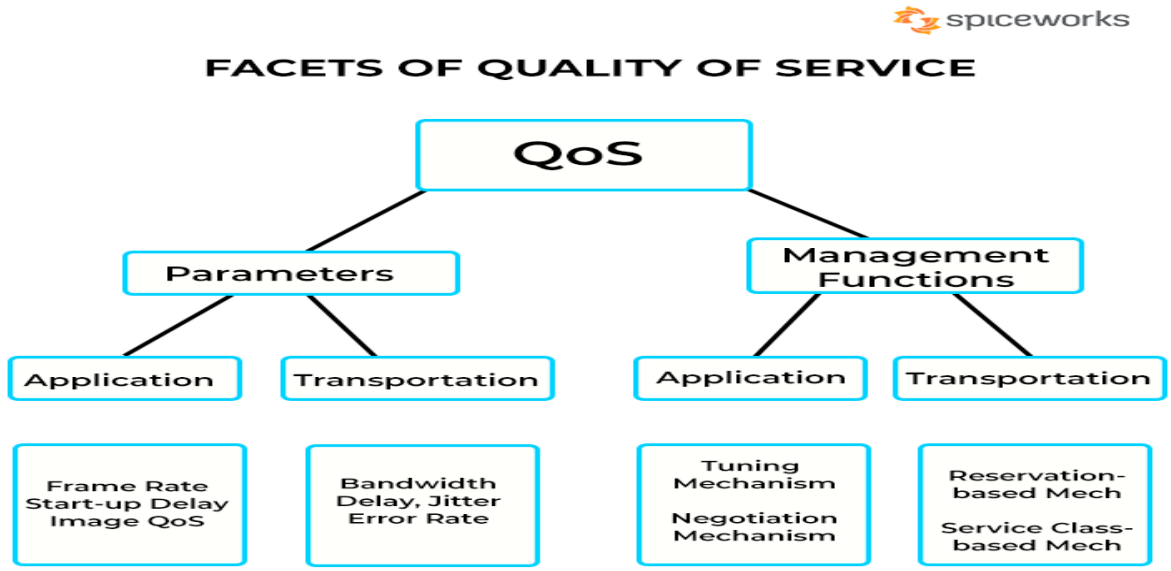
- Security services: The network layer provides security by using a session key between the source and destination host. The network layer in the source host encrypts the payloads of datagrams being sent to the destination host. The network layer in the destination host would then decrypt the payload. In such a way, the network layer maintains the data integrity and source authentication services.

The main functions performed by the network layer are:

- Routing: When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.
- Logical Addressing: The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.
- Internetworking: This is the main role of the network layer that it provides the logical connection between different types of networks.
- Fragmentation: The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.



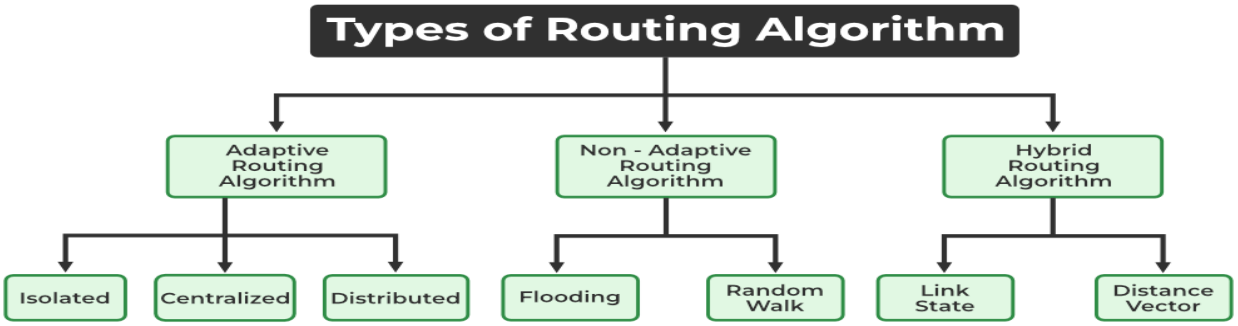
- QOS: Quality of service (QoS) is a set of technologies that work on a network to guarantee its ability to dependably run high-priority applications and traffic under limited network capacity. QoS technologies accomplish this by providing differentiated handling and capacity allocation to specific flows in network traffic.



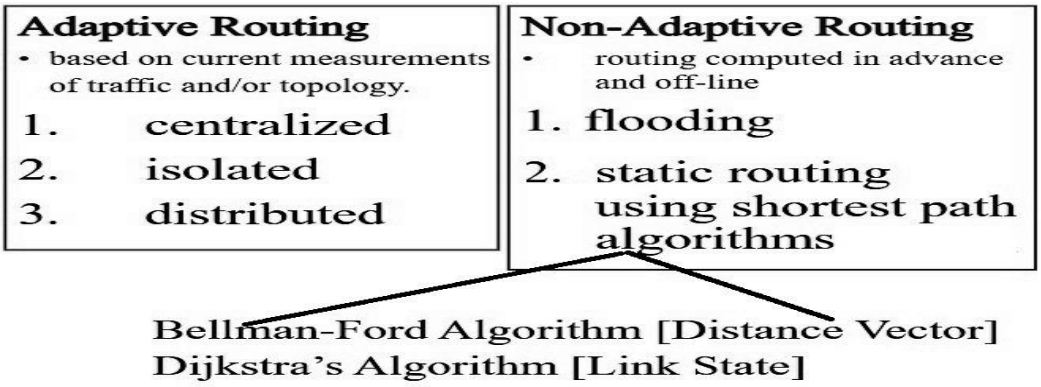
Functions of Network Layer

- **Routing** — find a path from one host to another host.
- **Congestion control** — mechanisms to prevent hosts from flooding the network.
- **Quality of Service (QoS)** - transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance.
- **Internetworking** provides translation between subnet using different protocols.

Routing algorithms



The main function of the network layer is routing packets from the source machine to the destination machine. Routing algorithm can be grouped into two major classes. Non adaptive and Adaptive algorithms.



Non adaptive	Adaptive
1) Routing decisions are not based on measurements or estimates of the current traffic and topology.	1) Routing decisions are based on measurements of the current traffic and topology.
2) The route is computed well in advance.	2) The route is computed depends on situation.

3) When the network is booted the routers are downloaded.

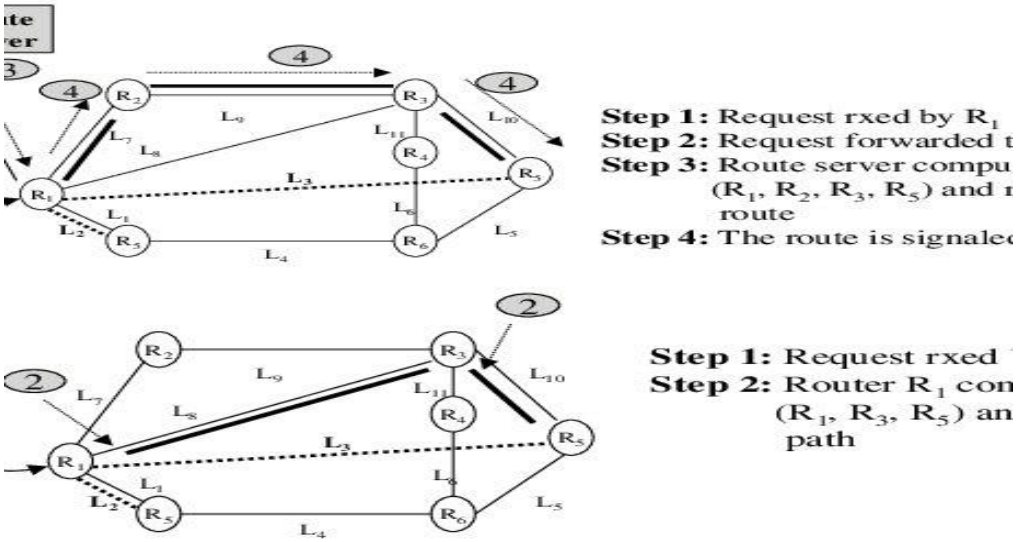
3) The routers are not downloaded.

4) This is a static routing.

4) This is a dynamic routing.

1. Isolation algorithm: It is an algorithm that obtains the routing information by using local information rather than gathering information from other nodes.

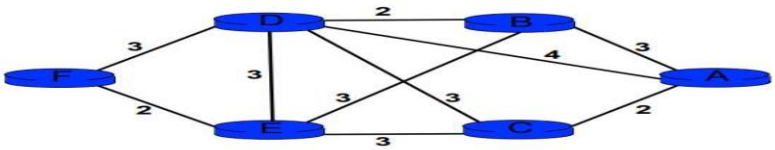
2. Centralized: In this method, a centralized node has entire information about the network and makes all the routing decisions. The advantage of this is only one node is required to keep the information of the entire network and the disadvantage is that if the central node goes down the entire network is done. The link state algorithm is referred to as a centralized algorithm since it is aware of the cost of each link in the network.



3. Distributed: In this method, the node receives information from its neighbors and then takes the decision about routing the packets. A disadvantage is that the packet may be delayed if there is a change in between intervals in which it receives information and sends packets. It is also known as a decentralized algorithm as it computes the least-cost path between source and destination.

5. **Distributed Routing Algorithms and Centralized Control Plane** (25 points) (Approx. 25 minutes)

Consider the network shown in Figure 4, where the number on a link between two nodes are the distance (i.e., link cost) between them.

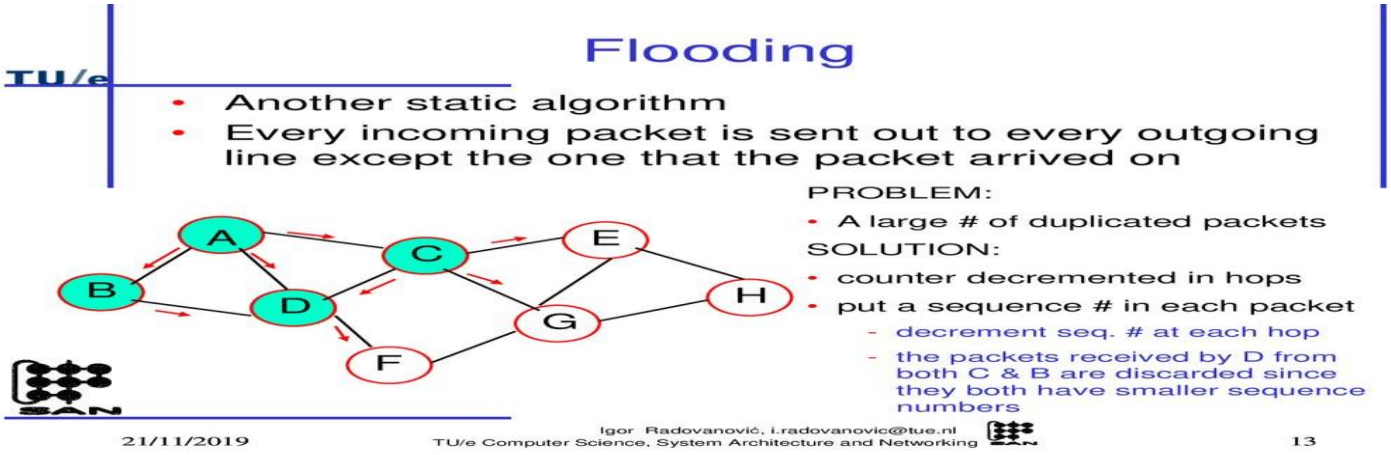


step	N	D(B),p(B)	D(C),p(C)	D(D),p(D)	D(E),p(E)	D(F),p(F)
0	A	3, A	2, A	4, A	∞, -	∞, -
1						
2						
3						
4						
5						

2. Non-Adaptive Algorithms

These are the algorithms that do not change their routing decisions once they have been selected. This is also known as static routing as a route to be taken is computed in advance and downloaded to routers when a router is booted.

1. Flooding: This adapts the technique in which every incoming packet is sent on every outgoing line except from which it arrived. One problem with this is that packets may go in a loop and as a result of which a node may receive duplicate packets. These problems can be overcome with the help of sequence numbers, hop count, and spanning trees.



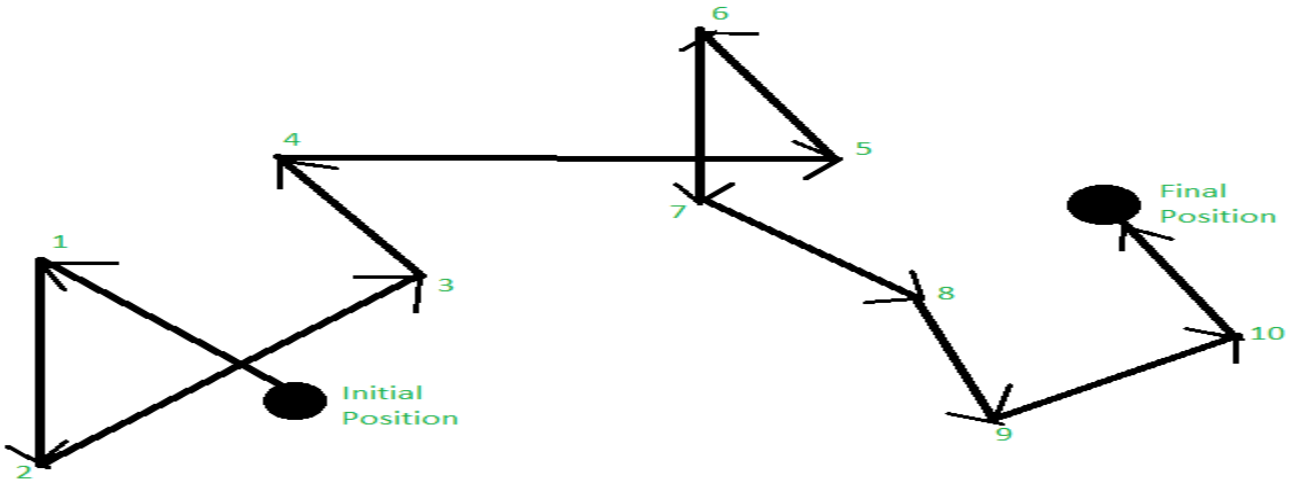
Characteristics –

- All possible routes between Source and Destination are tried. A packet will always get through if the path exists
- As all routes are tried, there will be at least one route which is the shortest
- All nodes directly or indirectly connected are visited

Limitations –

- Flooding generates a vast number of duplicate packets
- Suitable damping mechanism must be used

2. Random walk: In this method, packets are sent host by host or node by node to one of its neighbors randomly. This is a highly robust method that is usually implemented by sending packets onto the link which is least queued.



3. Hybrid Algorithms

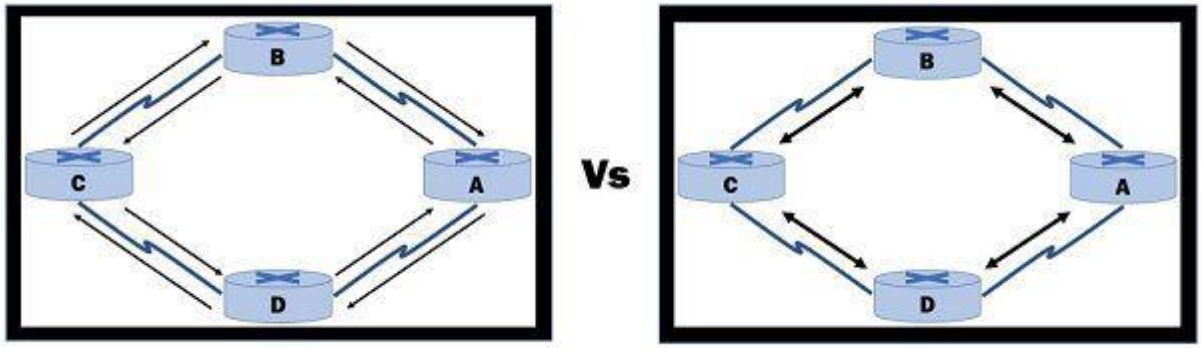
As the name suggests, these algorithms are a combination of both adaptive and non-adaptive algorithms. In this approach, the network is divided into several regions, and each region uses a different algorithm. Further, these are classified as follows:

1. Link-state: In this method, each router creates a detailed and complete map of the network which is then shared with all other routers. This allows for more accurate and efficient routing decisions to be made.

The three keys to understand the Link State Routing algorithm:

- Knowledge about the neighborhood: Instead of sending its routing table, a router sends the information about its neighborhood only. A router broadcast its identities and cost of the directly attached links to other routers.

- Flooding: Each router sends the information to every other router on the internetwork except its neighbors. This process is known as Flooding. Every router that receives the packet sends the copies to all its neighbors. Finally, each and every router receives a copy of the same information.
- Information sharing: A router sends the information to every other router only when the change occurs in the information.



Distance Vector Routing **Link State Routing**

2. Distance vector: In this method, each router maintains a table that contains information about the distance and direction to every other node in the network. This table is then shared with other routers in the network. The disadvantage of this method is that it may lead to routing loops.

Advantages of Distance Vector routing –

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

Disadvantages of Distance Vector routing –

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

Note – Distance Vector routing uses UDP(User datagram protocol) for transportation.

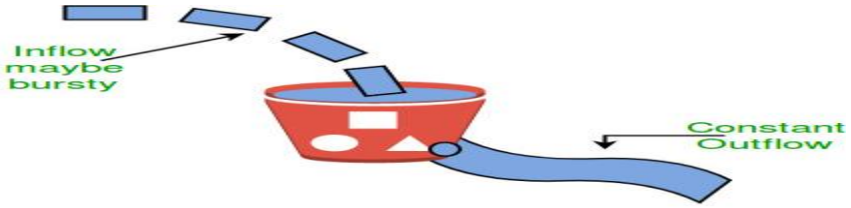
Difference between Routing and Flooding

Routing	Flooding
A routing table is required.	No Routing table is required.
May give the shortest path.	Always gives the shortest path.
Less Reliable.	More Reliable.
Traffic is less.	Traffic is high.
No duplicate packets.	Duplicate packets are present.

There are two congestion control algorithm which are as follows:

- Leaky Bucket Algorithm
- The leaky bucket algorithm discovers its use in the context of network traffic shaping or rate-limiting.
- A leaky bucket execution and a token bucket execution are predominantly used for traffic shaping algorithms.
- This algorithm is used to control the rate at which traffic is sent to the network and shape the burst traffic to a steady traffic stream.

- The disadvantages compared with the leaky-bucket algorithm are the inefficient use of available network resources.
- The large area of network resources such as bandwidth is not being used effectively.



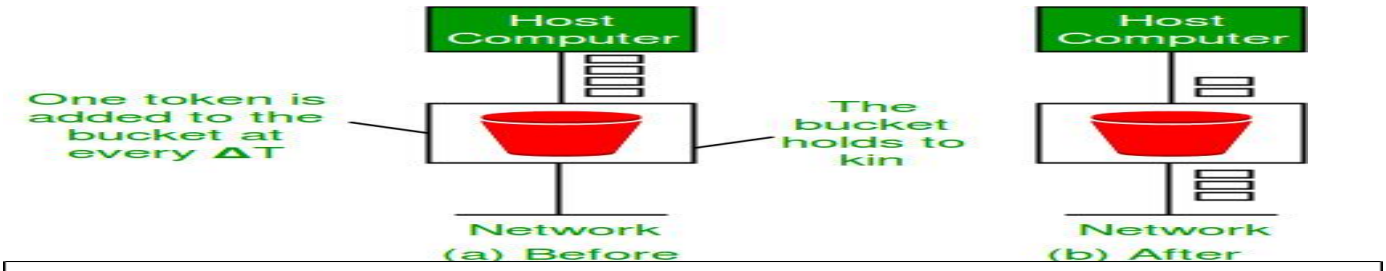
- Token bucket Algorithm
- The leaky bucket algorithm has a rigid output design at an average rate independent of the bursty traffic.
- In some applications, when large bursts arrive, the output is allowed to speed up. This calls for a more flexible algorithm, preferably one that never loses information. Therefore, a token bucket algorithm finds its uses in network traffic shaping or rate-limiting.
- It is a control algorithm that indicates when traffic should be sent. This order comes based on the display of tokens in the bucket.
- The bucket contains tokens. Each of the tokens defines a packet of predetermined size. Tokens in the bucket are deleted for the ability to share a packet.
- When tokens are shown, a flow to transmit traffic appears in the display of tokens.
- No token means no flow sends its packets. Hence, a flow transfers traffic up to its peak burst rate in good tokens in the bucket.

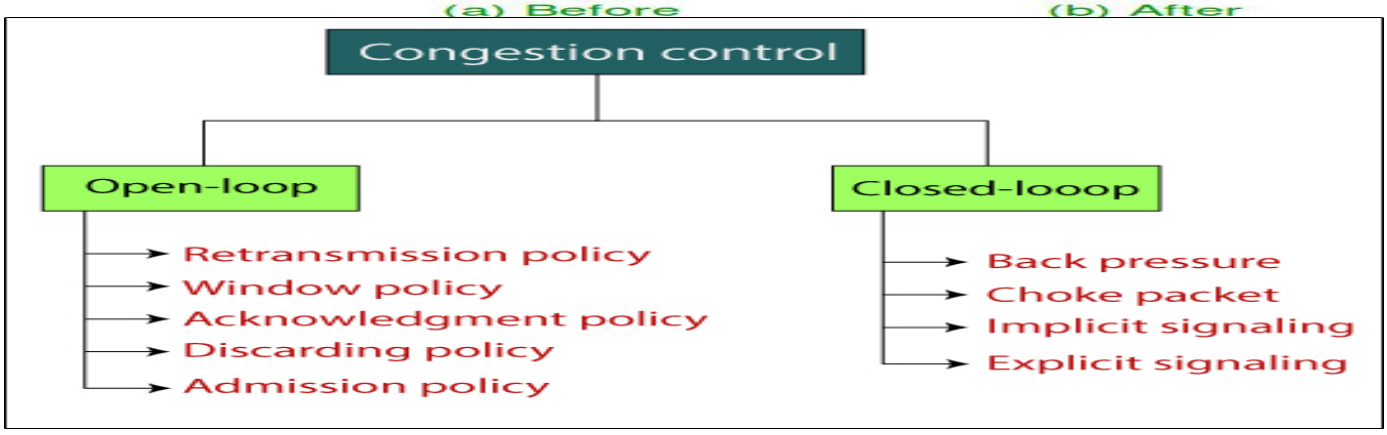
Need of token bucket Algorithm:-

The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is. So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

Steps of this algorithm can be described as follows:

1. In regular intervals tokens are thrown into the bucket. *f*
2. The bucket has a maximum capacity. *f*
3. If there is a ready packet, a token is removed from the bucket, and the packet is sent.
4. If there is no token in the bucket, the packet cannot be sent.





The following table highlights all the major differences between open loop control system and closed loop control system −

Basis of Difference	Open Loop Control System	Closed Loop Control System
Definition	A control system in which there is no feedback path is provided is called an open loop control system.	The control system in which there is a feedback path present is called a closed loop control system.
Also called	Open loop control system is also called non-feedback control system.	Closed loop control system is also called a feedback control system.
Control action	In open loop control system, the control action is independent of the output of the overall system.	In closed loop control system, the control action is dependent on the output of the system.
Design complexity	The design and construction of an open loop control system is quite simple.	Closed loop control system has comparatively complex design and construction.
Main Components	The major components of an open loop control system are − controller and plant.	The main components of a closed loop control system are − Controller, plant or process, feedback element and error detector (comparator).
Response	Open loop control system has fast response because there is no measurement and feedback of output.	The response of the closed loop control system is slow due to presence of feedback.
Reliability	The reliability of open loop control system is less.	The closed loop control system is more reliable.
Accuracy	The accuracy of open loop control system depends upon the system calibration and therefore, may be less.	Closed loop control system is comparatively accurate because the feedback maintains its accuracy.
Stability (in terms of output)	The stability of open loop control system is more, i.e., the output of the open loop system remains constant.	Closed loop control system is comparatively less stable.
Optimization	The open loop control system is not optimized.	Closed loop control system is optimized to produce the desired output.
Maintenance	Open loop control system requires less maintenance.	Comparatively more maintenance is needed in closed loop control system.
Implementation	Open loop control system is easy to implement.	The implementation of a closed loop control system is relatively difficult.
Cost	Open loop control system is less expensive.	The cost of the closed loop control system is relatively high.
Noise	Open loop control system has more internal noise.	In closed loop system, the internal noise in the system is less.
Examples	Common practical examples of open loop control systems are − automatic traffic light system, automatic washing machine, immersion heater, etc.	Examples of closed loop control systems include: ACs, fridge, toaster, rocket launching system, radar tracking system, etc.

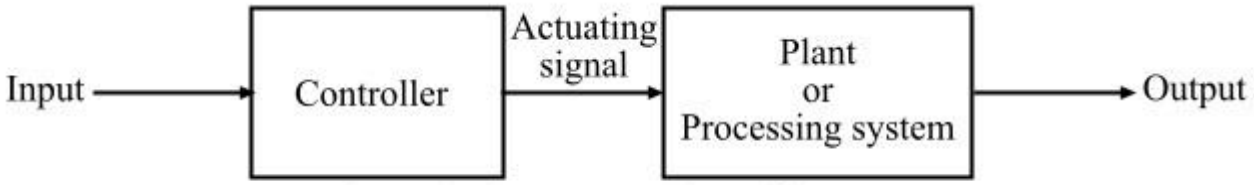


Figure 1 - Open Loop Control System

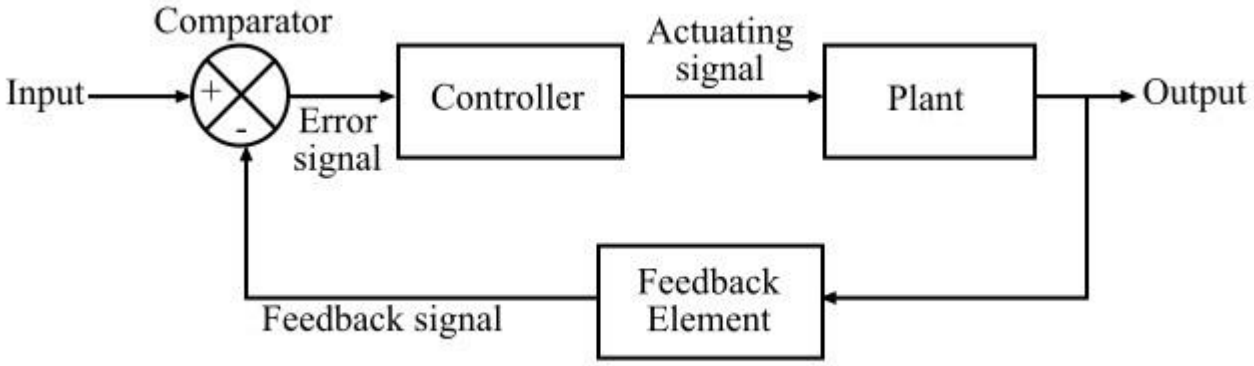


Figure 2 - Closed Loop Control System

Quality of service (QoS) is the use of mechanisms or technologies that work on a network to control traffic and ensure the performance of critical applications with limited network capacity. It enables organizations to adjust their overall network traffic by prioritizing specific high-performance applications.

QoS is typically applied to networks that carry traffic for resource-intensive systems. Common services for which it is required include internet protocol television (IPTV), online gaming, streaming media, videoconferencing, video on demand (VOD), and Voice over IP (VoIP).

QOS Concepts

The QOS concepts are explained below−

Congestion Management

The bursty feature of data traffic sometimes bounds to increase traffic more than a connection speed. QoS allows a router to put packets into different queues. Servicespecific queues more often depend on priority than buffer traffic in an individual queue and let the first packet by the first packet out.

Queue Management

The queues in a buffer can fill and overflow. A packet would be dropped if a queue is complete, and the router cannot prevent it from being dropped if it is a high priority packet. This is referred to as tail drop.

Link Efficiency

The low-speed links are bottlenecks for lower packets. The serialization delay caused by the high packets forces the lower packets to wait longer. The serialization delay is the time created to put a packet on the connection.

Elimination of overhead bits

It can also increase efficiency by removing too many overhead bits.

Traffic shaping and policing

Shaping can prevent the overflow problem in buffers by limiting the full bandwidth potential of the applications packets. Sometimes, many network topologies with a highbandwidth link connected with a low-bandwidth link in remote sites can overflow low bandwidth connections.

There are 2 types of Quality of Service Solutions:

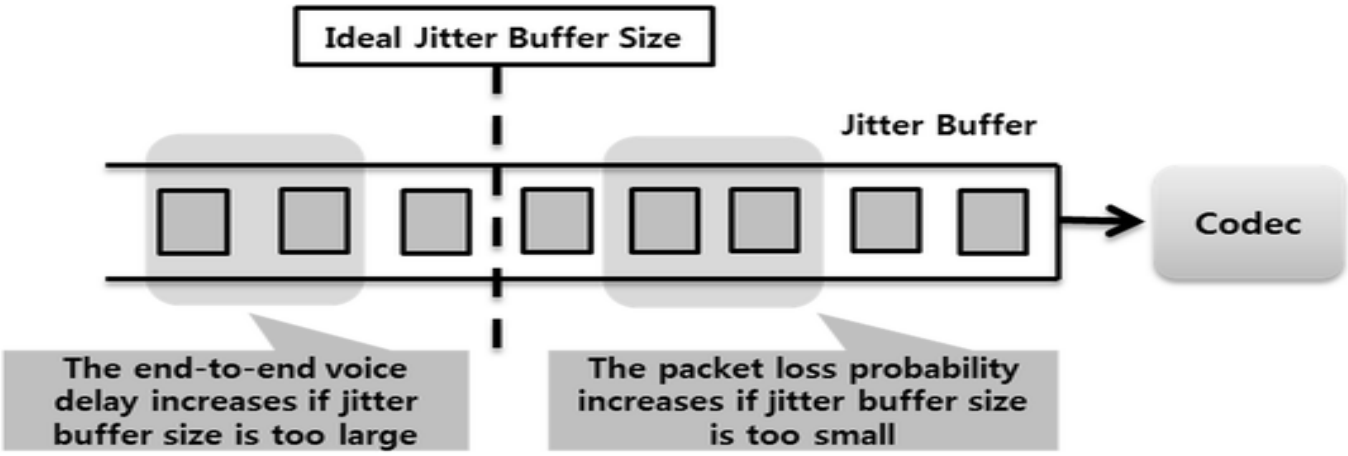
1. Stateless solution: Here, the server is not required to keep or store the server information or session details to itself. The routers maintain no fine-grained state about traffic, one positive factor of this is, that it's scalable and robust. But also, it has weak services as there is no guarantee about the kind of performance delay in a particular application which we encounter. In the stateless solution, the server and client are loosely coupled and can act.
2. Stateful solution: Here, the server is required to maintain the current state and session information, the routers maintain per-flow state as the flow is very important in providing the Quality-of-Service which is providing powerful services such as guaranteed services and high resource utilization, provides protection, and is much less scalable and robust. Here, the server and client are tightly bounded.

How to achieve Quality of Service?

Let's get into some details and say, your organization wants to achieve Quality of Service, which can be done by using some tools and techniques, like jitter buffer and traffic shaping.

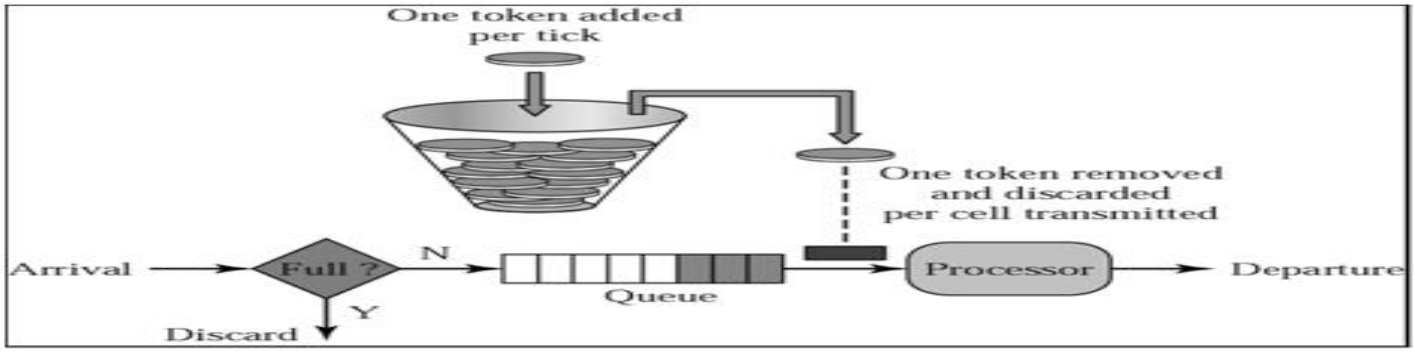
Jitter buffer

This is a temporary storage buffer which is used to store the incoming data packets, it is used in packet-based networks to ensure that the continuity of the data streams doesn't get disturbed, it does that by smoothing out the packet arrival times during periods of network congestion.



Traffic shaping

This technique which is also known as packet shaping is a congestion control or management technique that helps to regulate network data transfer by delaying the flow of least important or least necessary data packets.



Quality of Service Parameters:

QoS can be measured quantitatively by using several parameters

- Packet loss: it happens when the network links become congested and the routers and switches start dropping the packets. When these packets are dropped during real-time communication, such as audio or video, these sessions can experience jitter and gaps in speech.
- Jitter: occurs as the result of network congestion, timing drift, and route changes. And also, too much jitter can degrade the quality of audio communication.
- Latency: is the time delay, which is taken by a packet to travel from its source to its destination. For a great system, latency should be as low as possible, ideally, it should be close to zero.
- Bandwidth: is the capacity of a network channel to transmit maximum possible data through the channel in a certain amount of time. QoS optimizes a network by managing its bandwidth and setting the priorities for those applications which require more resources as compared to other applications.
- Mean opinion score: it is a metric for rating the audio quality which uses a five-point scale, with a five indicating the highest or best quality.

Implementing Quality of Service:

We can implement Quality of service through three of the following existing models:

1. Best Effort: if we are applying this model then, it means that we are prioritizing all the data packets equally. But since we all setting the priority order like this, then there is no guarantee that all the data packets will be delivered, but it will put up the best effort to deliver all of them. Point to remember is, that the best-effort model is applied when networks haven't configured with the QoS policies or incase their network infrastructure does not support QoS.
2. Integrated Services: or IntServ, this QoS model reserves the bandwidth along a specific path on the network. The applications ask the network's resource reservation for themselves and parallelly the network devices monitor the flow of packets to make sure network resources can accept packets. Point to remember: while implementing Integrated Services Model, the IntServ-capable routers and resource reservation protocol are necessary. This model has limited scalability and high consumption of the network resources.
3. Differentiated Services: in this QoS model, the network elements such as routers and switches are configured to serve multiple categories of traffic with different priority orders. A company can categorize the network traffic based on its requirements. Eg. Assigning higher priority to audio traffic etc.

Let us understand the difference between Integrated Services and Differentiated Services:

Integrated Services	Differentiated Services
This Architecture mainly specifies the elements to guarantee Quality of Service (QoS) on the network.	This Architecture mainly specifies a simple and scalable mechanism for classifying and managing the traffic of the network and also provides QoS on the modern IP networks.
These services mainly involve the prior reservation of the resources before sending in order to achieve Quality of Service.	These services mark the packets with the priority and then sends it to the network and there is no concept of prior reservation.
It is also known as IntServ.	It is also known as DiffSer.

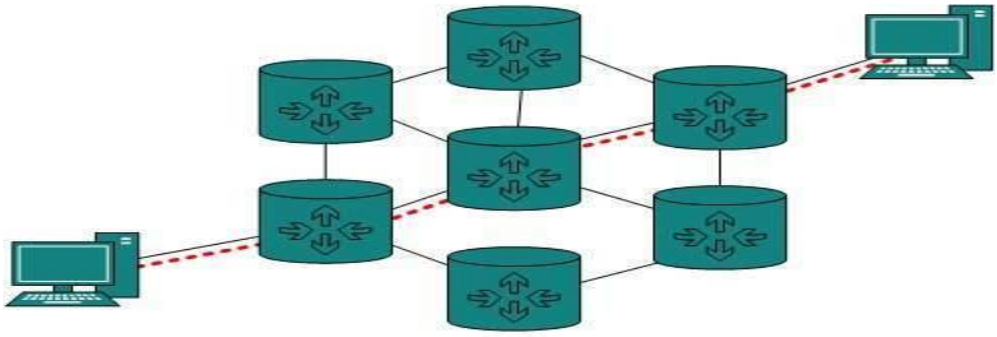
Integrated Services	Differentiated Services
These are not Scalable	These are Scalable.
These involve per flow Setup	These involve long term Setup
In this end to end service scope is available.	In this domain service scope is involved

Internetworking in Computer Network

In real world scenario, networks under same administration are generally scattered geographically. There may exist requirement of connecting two different networks of same kind as well as of different kinds. Routing between two networks is called internetworking.

Networks can be considered different based on various parameters such as, Protocol, topology, Layer-2 network and addressing scheme.

In internetworking, routers have knowledge of each other's address and addresses beyond them. They can be statically configured go on different network or they can learn by using internetworking routing protocol.

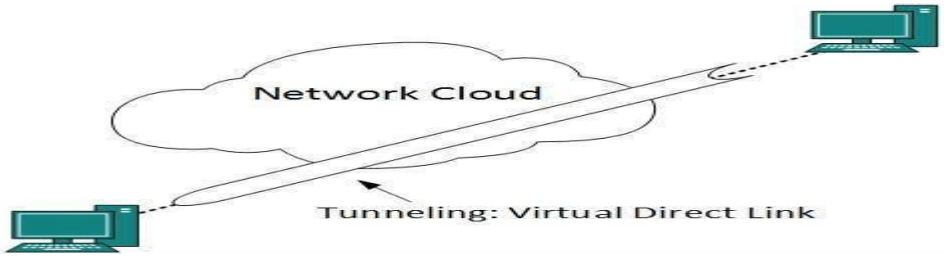


Routing protocols which are used within an organization or administration are called Interior Gateway Protocols or IGP. RIP, OSPF are examples of IGP. Routing between different organizations or administrations may have Exterior Gateway Protocol, and there is only one EGP i.e. Border Gateway Protocol.

Tunneling

If they are two geographically separate networks, which want to communicate with each other, they may deploy a dedicated line between or they have to pass their data through intermediate networks.

Tunneling is a mechanism by which two or more same networks communicate with each other, by passing intermediate networking complexities. Tunneling is configured at both ends.



When the data enters from one end of Tunnel, it is tagged. This tagged data is then routed inside the intermediate or transit network to reach the other end of Tunnel. When data exists the Tunnel its tag is removed and delivered to the other part of the network.

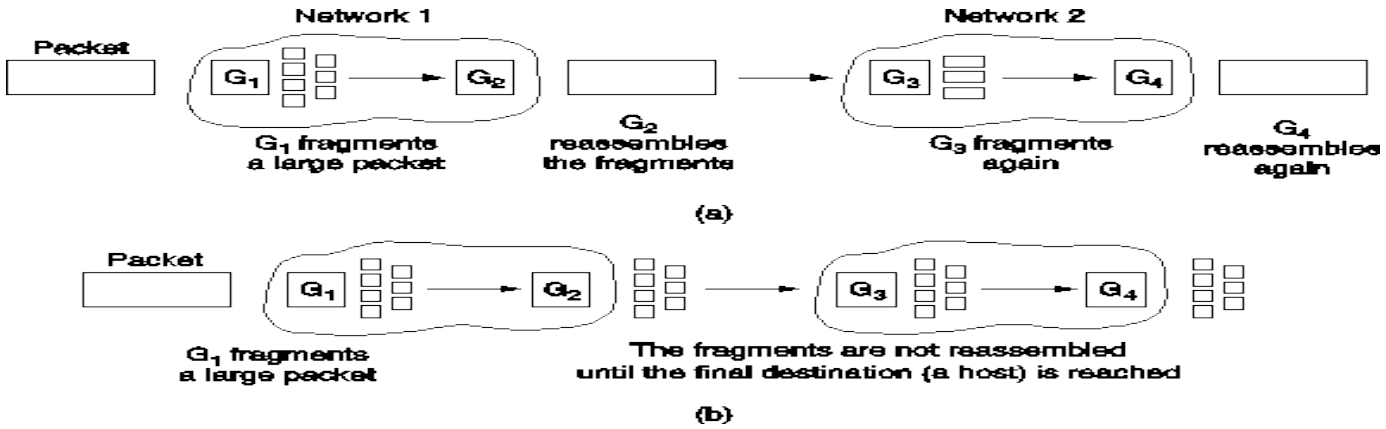
Both ends seem as if they are directly connected and tagging makes data travel through transit network without any modifications.

Packet Fragmentation

Most Ethernet segments have their maximum transmission unit (MTU) fixed to 1500 bytes. A data packet can have more or less packet length depending upon the application. Devices in the transit path also have their hardware and software capabilities which tell what amount of data that device can handle and what size of packet it can process.

If the data packet size is less than or equal to the size of packet the transit network can handle, it is processed neutrally. If the packet is larger, it is broken into smaller pieces and then forwarded. This is called packet fragmentation. Each fragment contains the same destination and source address and routed through transit path easily. At the receiving end it is assembled again.

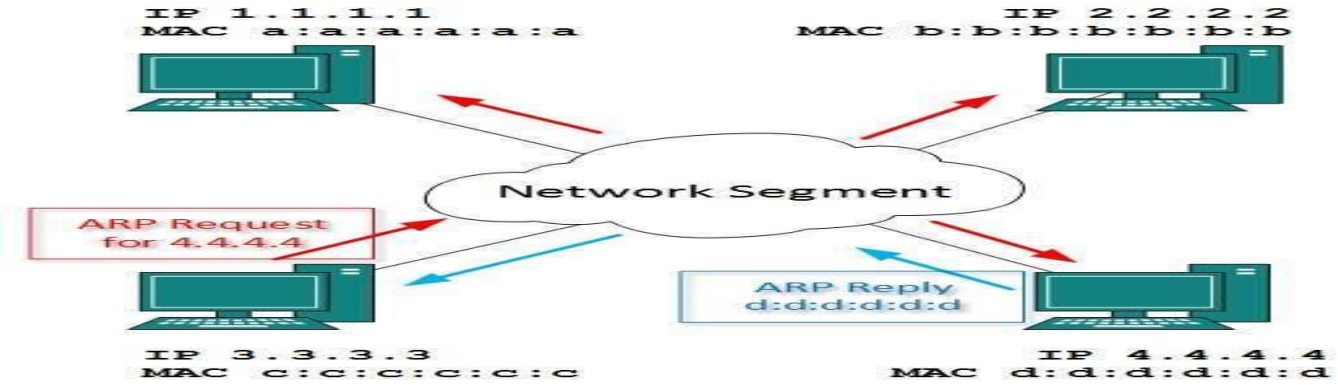
Every computer in a network has an IP address by which it can be uniquely identified and addressed. An IP address is Layer-3 (Network Layer) logical address. This address may change every time a computer restarts. A computer can have one IP at one instance of time and another IP at some different time.



Address Resolution Protocol(ARP)

While communicating, a host needs Layer-2 (MAC) address of the destination machine which belongs to the same broadcast domain or network. A MAC address is physically burnt into the Network Interface Card (NIC) of a machine and it never changes.

On the other hand, IP address on the public domain is rarely changed. If the NIC is changed in case of some fault, the MAC address also changes. This way, for Layer-2 communication to take place, a mapping between the two is required.



To know the MAC address of remote host on a broadcast domain, a computer wishing to initiate communication sends out an ARP broadcast message asking, “Who has this IP address?” Because it is a broadcast, all hosts on the network segment (broadcast domain) receive this packet and process it. ARP packet contains the IP address of destination host, the sending host wishes to talk to. When a host receives an ARP packet destined to it, it replies back with its own MAC address.

Once the host gets destination MAC address, it can communicate with remote host using Layer-2 link protocol. This MAC to IP mapping is saved into ARP cache of both sending and receiving hosts. Next time, if they require to communicate, they can directly refer to their respective ARP cache.

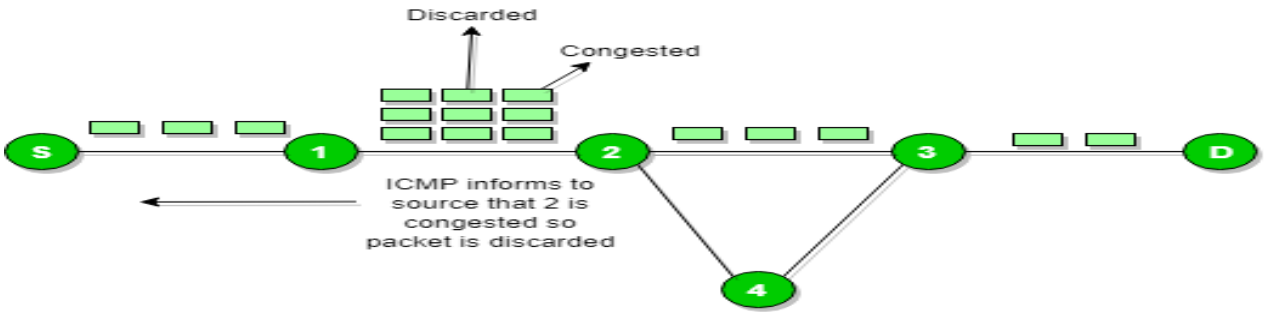
Reverse ARP is a mechanism where host knows the MAC address of remote host but requires to know IP address to communicate.

Internet Control Message Protocol (ICMP)

ICMP is network diagnostic and error reporting protocol. ICMP belongs to IP protocol suite and uses IP as carrier protocol. After constructing ICMP packet, it is encapsulated in IP packet. Because IP itself is a best-effort non-reliable protocol, so is ICMP.

Any feedback about network is sent back to the originating host. If some error in the network occurs, it is reported by means of ICMP. ICMP contains dozens of diagnostic and error reporting messages.

ICMP-echo and ICMP-echo-reply are the most commonly used ICMP messages to check the reachability of end-to-end hosts. When a host receives an ICMP-echo request, it is bound to send back an ICMP-echo-reply. If there is any problem in the transit network, the ICMP will report that problem.



Internet Protocol Version 4 (IPv4)

IPv4 is 32-bit addressing scheme used as TCP/IP host addressing mechanism. IP addressing enables every host on the TCP/IP network to be uniquely identifiable.

IPv4 provides hierarchical addressing scheme which enables it to divide the network into sub-networks, each with well-defined number of hosts. IP addresses are divided into many categories:

- Class A - it uses first octet for network addresses and last three octets for host addressing
- Class B - it uses first two octets for network addresses and last two for host addressing
- Class C - it uses first three octets for network addresses and last one for host addressing
- Class D - it provides flat IP addressing scheme in contrast to hierarchical structure for above three.
- Class E - It is used as experimental.

IPv4 also has well-defined address spaces to be used as private addresses (not routable on internet), and public addresses (provided by ISPs and are routable on internet).

Though IP is not reliable one; it provides 'Best-Effort-Delivery' mechanism.

Internet Protocol Version 6 (IPv6)

Exhaustion of IPv4 addresses gave birth to a next generation Internet Protocol version 6. IPv6 addresses its nodes with 128-bit wide address providing plenty of address space for future to be used on entire planet or beyond.

IPv6 has introduced Anycast addressing but has removed the concept of broadcasting. IPv6 enables devices to self-acquire an IPv6 address and communicate within that subnet. This auto-configuration removes the dependability of Dynamic Host Configuration Protocol (DHCP) servers. This way, even if the DHCP server on that subnet is down, the hosts can communicate with each other.

IPv6 provides new feature of IPv6 mobility. Mobile IPv6 equipped machines can roam around without the need of changing their IP addresses.

IPv6 is still in transition phase and is expected to replace IPv4 completely in coming years. At present, there are few networks which are running on IPv6. There are some transition mechanisms available for IPv6 enabled networks to speak and roam around different networks easily on IPv4. These are:

- Dual stack implementation
- Tunneling
- NAT-PT

What is IP?

An IP stands for internet protocol. An IP address is assigned to each device connected to a network. Each device uses an IP address for communication. It also behaves as an identifier as this address is used to identify the device on a network. It defines the technical format of the packets. Mainly, both the networks, i.e., IP and TCP, are combined together, so together, they are referred to as a TCP/IP. It creates a virtual connection between the source and the destination.

We can also define an IP address as a numeric address assigned to each device on a network. An IP address is assigned to each device so that the device on a network can be identified uniquely. To facilitate the routing of packets, TCP/IP protocol uses a 32-bit logical address known as IPv4(Internet Protocol version 4).

An IP address consists of two parts, i.e., the first one is a network address, and the other one is a host address.

There are two types of IP addresses:

- IPv4
- IPv6

What is IPv4?

IPv4 is a version 4 of IP. It is a current version and the most commonly used IP address. It is a 32-bit address written in four numbers separated by 'dot', i.e., periods. This address is unique for each device.

For example, 66.94.29.13

The above example represents the IP address in which each group of numbers separated by periods is called an Octet. Each number in an octet is in the range from 0-255. This address can produce 4,294,967,296 possible unique addresses.

In today's computer network world, computers do not understand the IP addresses in the standard numeric format as the computers understand the numbers in binary form only. The binary number can be either 1 or 0. The IPv4 consists of four sets, and these sets represent the octet. The bits in each octet represent a number.

Each bit in an octet can be either 1 or 0. If the bit the 1, then the number it represents will count, and if the bit is 0, then the number it represents does not count.

Drawback of IPv4

Currently, the population of the world is 7.6 billion. Every user is having more than one device connected with the internet, and private companies also rely on the internet. As we know that IPv4 produces 4 billion addresses, which are not enough for each device connected to the internet on a planet. Although the various techniques were invented, such as variable- length mask, network address translation, port address translation, classes, inter-domain translation, to conserve the bandwidth of IP address and slow down the depletion of an IP address. In these techniques, public IP is converted into a private IP due to which the user having public IP can also use the internet. But still, this was not so efficient, so it gave rise to the development of the next generation of IP addresses, i.e., IPv6.

What is IPv6?

IPv4 produces 4 billion addresses, and the developers think that these addresses are enough, but they were wrong. IPv6 is the next generation of IP addresses. The main difference between IPv4 and IPv6 is the address size of IP addresses. The IPv4 is a 32-bit address, whereas IPv6 is a 128-bit hexadecimal address. IPv6 provides a large address space, and it contains a simple header as compared to IPv4.

It provides transition strategies that convert IPv4 into IPv6, and these strategies are as follows:

- Dual stacking: It allows us to have both the versions, i.e., IPv4 and IPv6, on the same device.
- Tunneling: In this approach, all the users have IPv6 communicates with an IPv4 network to reach IPv6.

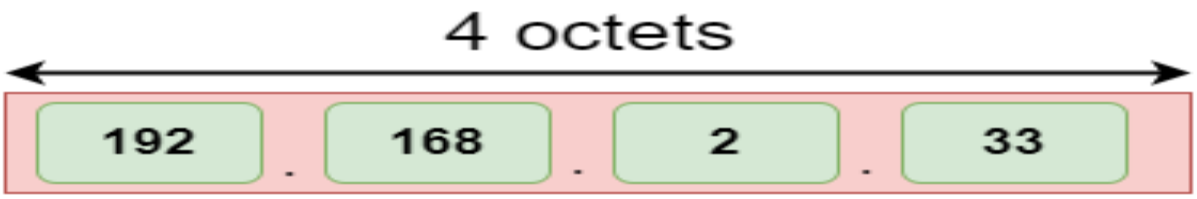
- Network Address Translation: The translation allows the communication between the hosts having a different version of IP.

This hexadecimal address contains both numbers and alphabets. Due to the usage of both the numbers and alphabets, IPv6 is capable of producing over 340 undecillion ($3.4*10^{38}$) addresses.

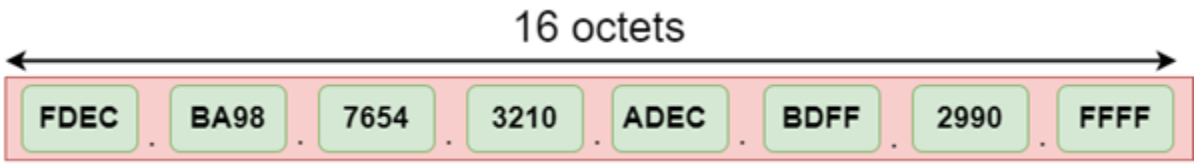
IPv6 is a 128-bit hexadecimal address made up of 8 sets of 16 bits each, and these 8 sets are separated by a colon. In IPv6, each hexadecimal character represents 4 bits. So, we need to convert 4 bits to a hexadecimal number at a time

Address format

The address format of IPv4:



The address format of IPv6:



The above diagram shows the address format of IPv4 and IPv6. An IPv4 is a 32-bit decimal address. It contains 4 octets or fields separated by 'dot', and each field is 8-bit in size. The number that each field contains should be in the range of 0-255. Whereas an IPv6 is a 128-bit hexadecimal address. It contains 8 fields separated by a colon, and each field is 16-bit in size.

Differences between IPv4 and IPv6

	Ipv4	Ipv6
Address length	IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
Fields	IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon.
Classes	IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.	IPv6 does not contain classes of IP addresses.
Number of IP address	IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.
VLSM	It supports VLSM (Virtual Length Subnet Mask). Here, VLSM means that Ipv4 converts IP addresses into a subnet of different sizes.	It does not support VLSM.
Address configuration	It supports manual and DHCP configuration.	It supports manual, DHCP, auto-configuration, and renumbering.

Address space	It generates 4 billion unique addresses	It generates 340 undecillion unique addresses.
End-to-end connection integrity	In IPv4, end-to-end connection integrity is unachievable.	In the case of IPv6, end-to-end connection integrity is achievable.
Security features	In IPv4, security depends on the application. This IP address is not developed in keeping the security feature in mind.	In IPv6, IPSEC is developed for security purposes.
Address representation	In IPv4, the IP address is represented in decimal.	In IPv6, the representation of the IP address in hexadecimal.
Fragmentation	Fragmentation is done by the senders and the forwarding routers.	Fragmentation is done by the senders only.
Packetflow identification	It does not provide any mechanism for packet flow identification.	It uses flow label field in the header for the packet flow identification.
Checksum field	The checksum field is available in IPv4.	The checksum field is not available in IPv6.
Transmission scheme	IPv4 is broadcasting.	On the other hand, IPv6 is multicasting, which provides efficient network operations.
Encryption and Authentication	It does not provide encryption and authentication.	It provides encryption and authentication.
Number of octets	It consists of 4 octets.	It consists of 8 fields, and each field contains 2 octets. Therefore, the total number of octets in IPv6 is 16.

Internet Control Protocol

- IP packets use logical (host to host) addresses and need to be encapsulated in a frame with the help of physical (node-to-node) addresses.
- Some protocols are needed to create mapping between physical and logical addresses.

Static Mapping

- It creates a table that associates a logical address with a physical address.
- This address is stored on each machine in the network.
- Each machine has an IP address of another machine but not its physical address. Hence, physical addresses are usually seen in the table.

Dynamic Mapping

In this mapping, each machine knows one of the two addresses (logical or physical address) and tries to find the other one.

Types of Internet Protocols

- File retrieval protocols This type of service was one of the earliest ways of retrieving information from computers connected to the Internet. You could view the names of the files stored on the serving computer, but you didn't have any type of graphics and sometimes no description of a file's content. You would need to have advanced knowledge of which files contained the information you sought.

- FTP (File Transfer Protocol) This was one of the first Internet services developed and it allows users to move files from one computer to another. Using the FTP program, a user can logon to a remote computer, browse through its files, and either download or upload files (if the remote computer allows). These can be any type of file, but the user is only allowed to see the file name; no description of the file content is included. You might encounter the FTP protocol if you try to download any software applications from the World Wide Web. Many sites that offer downloadable applications use the FTP protocol.

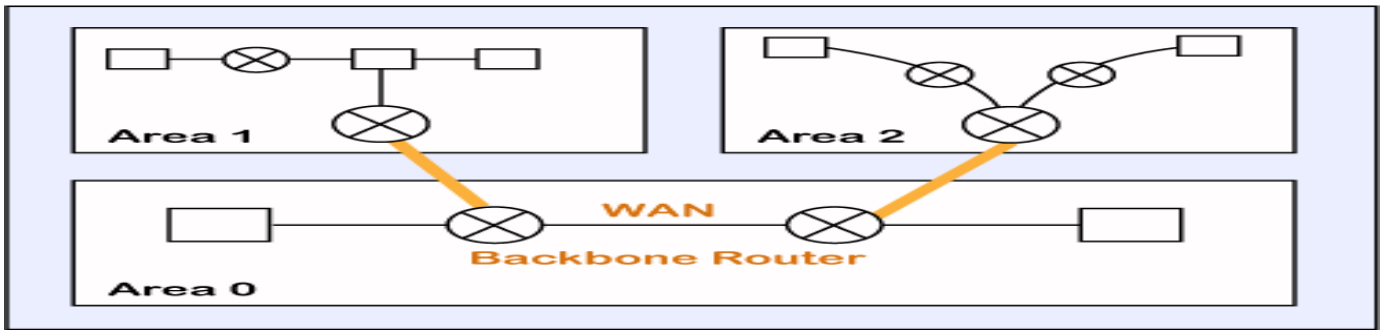
- Gopher Gopher offers downloadable files with some content description to make it easier to find the file you need. The files are arranged on the remote computer in a hierarchical manner, much like the files on your computer's hard drive are arranged. This protocol isn't widely used anymore, but you can still find some operational gopher sites.

- Telnet. You can connect to and use a remote computer program by using the telnet protocol. Generally you would telnet into a specific application housed on a serving computer that would allow you to use that application as if it were on your own computer. Again, using this protocol requires special software.

OSPF Protocol

The OSPF stands for Open Shortest Path First. It is a widely used and supported routing protocol. It is an intradomain protocol, which means that it is used within an area or a network. It is an interior gateway protocol that has been designed within a single autonomous system. It is based on a link-state routing algorithm in which each router contains the information of every domain, and based on this information, it determines the shortest path. The goal of routing is to learn routes. The OSPF achieves by learning about every router and subnet within the entire network. Every router contains the same information about the network. The way the router learns this information by sending LSA (Link State Advertisements). These LSAs contain information about every router, subnet, and other networking information. Once the LSAs have been flooded, the OSPF stores the information in a link-state database known as LSDB. The main goal is to have the same information about every router in an LSDBs.

OSPF Areas



OSPF divides the autonomous systems into areas where the area is a collection of networks, hosts, and routers. Like internet service providers divide the internet into a different autonomous system for easy management and OSPF further divides the autonomous systems into Areas.

How does OSPF work?

There are three steps that can explain the working of OSPF:

Step 1: The first step is to become OSPF neighbors. The two connecting routers running OSPF on the same link creates a neighbor relationship.

Step 2: The second step is to exchange database information. After becoming the neighbors, the two routers exchange the LSDB information with each other.

Step 3: The third step is to choose the best route. Once the LSDB information has been exchanged with each other, the router chooses the best route to be added to a routing table based on the calculation of SPF.

How a router forms a neighbor relationship?

Router ID (RID): The router ID is a number that uniquely identifies each router on a network. The router ID is in the format of the IPv4 address. There are few ways to set the router ID, the first way is to set the router ID manually and the other way is to let the router decides itself.

The following is the logic that the router chooses to set the router ID:

- Manually assigned: The router checks whether the router ID is manually set or not. If it manually set, then it is a router ID. If it is not manually set, then it will choose the highest 'up' status loopback interface IP address. If there are no loopback interfaces, then it will choose the highest 'up' status non-loopback interface IP address.

Two routers connected to each other through point to point or multiple routers are connected can communicate with each other through an OSPF protocol. The two routers are adjacent only when both the routers send the HELLO packet to each other. When both the routers receive the acknowledgment of the HELLO packet, then they come in a two-way state. As OSPF is a link state routing protocol, so it allows to create the neighbor relationship between the routers. The two routers can be neighbors only when they belong to the same subnet, share the same area id, subnet mask, timers, and authentication. The OSPF relationship is a relationship formed between the routers so that they can know each other. The two routers can be neighbors if atleast one of them is designated router or backup designated router in a network, or connected through a point-to-point link.

Types of links in OSPF

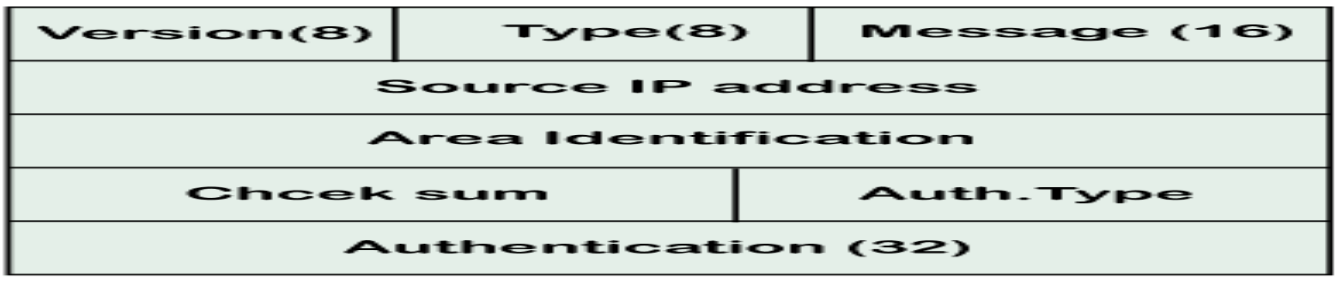
A link is basically a connection, so the connection between two routers is known as a link.

There are four types of links in OSPF:

1. Point-to-point link: The point-to-point link directly connects the two routers without any host or router in between.
2. Transient link: When several routers are attached in a network, they are known as a transient link. The transient link has two different implementations: Unrealistic topology: When all the routers are connected to each other, it is known as an unrealistic topology. Realistic topology: When some designated router exists in a network then it is known as a realistic topology. Here designated router is a router to which all the routers are connected. All the packets sent by the routers will be passed through the designated router.
3. Stub link: It is a network that is connected to the single router. Data enters to the network through the single router and leaves the network through the same router.
4. Virtual link: If the link between the two routers is broken, the administration creates the virtual path between the routers, and that path could be a long one also.

OSPF Message Format

The following are the fields in an OSPF message format:



- Version: It is an 8-bit field that specifies the OSPF protocol version.
- Type: It is an 8-bit field. It specifies the type of the OSPF packet.
- Message: It is a 16-bit field that defines the total length of the message, including the header. Therefore, the total length is equal to the sum of the length of the message and header.
- Source IP address: It defines the address from which the packets are sent. It is a sending routing IP address.
- Area identification: It defines the area within which the routing takes place.
- Checksum: It is used for error correction and error detection.
- Authentication type: There are two types of authentication, i.e., 0 and 1. Here, 0 means for none that specifies no authentication is available and 1 means for pwd that specifies the password-based authentication.
- Authentication: It is a 32-bit field that contains the actual value of the authentication data.

OSPF Packets

There are five different types of packets in OSPF:

- Hello
- Database Description
- Link state request
- Link state update
- Link state Acknowledgment

Let's discuss each packet in detail.

1. Hello packet

The Hello packet is used to create a neighborhood relationship and check the neighbor's reachability. Therefore, the Hello packet is used when the connection between the routers need to be established.

2. Database Description

After establishing a connection, if the neighbor router is communicating with the system first time, it sends the database information about the network topology to the system so that the system can update or modify accordingly.

3. Link state request

The link-state request is sent by the router to obtain the information of a specified route. Suppose there are two routers, i.e., router 1 and router 2, and router 1 wants to know the information about the router 2, so router 1 sends the link state request to the router 2. When router 2 receives the link state request, then it sends the link-state information to router 1.

4. Link state update

The link-state update is used by the router to advertise the state of its links. If any router wants to broadcast the state of its links, it uses the link-state update.

5. Link state acknowledgment

The link-state acknowledgment makes the routing more reliable by forcing each router to send the acknowledgment on each link state update. For example, router A sends the link state update to the router B and router C, then in return, the router B and C sends the link-state acknowledgment to the router A, so that the router A gets to know that both the routers have received the link-state update.

OSPF States

The device running the OSPF protocol undergoes the following states:

- Down: If the device is in a down state, it has not received the HELLO packet. Here, down does not mean that the device is physically down; it means that the OSPF process has not been started yet.
- Init: If the device comes in an init state, it means that the device has received the HELLO packet from the other router.
- 2WAY: If the device is in a 2WAY state, which means that both the routers have received the HELLO packet from the other router, and the connection gets established between the routers.
- Exstart: Once the exchange between the routers get started, both the routers move to the Exstart state. In this state, master and slave are selected based on the router's id. The master controls the sequence of numbers, and starts the exchange process.
- Exchange: In the exchange state, both the routers send a list of LSAs to each other that contain a database description.
- Loading: On the loading state, the LSR, LSU, and LSA are exchanged.
- Full: Once the exchange of the LSAs is completed, the routers move to the full state.
- There are three versions of OSPF:
    - OSPFv1: This is the first version of OSPF created in the year 1989. It is no longer in use.
    - OSPFv2: This is the second version of OSPF created in 1998. It is used in IPv4. This version is important for CCNA 200-301.
    - OSPFv3: This is the latest version of OSPF created in the year 2008. This version is used for IPv6 and as well as for IPv4.

Router attributes

Before going to the Extract state, OSPF chooses one router as a Designated router and another router as a backup designated router. These routers are not the type, but they are the attributes of a router. In the case of broadcast networks, the router selects one router as a designated router and another router as a backup designated router. The election of designated and the backup designated router is done to avoid the flooding in a network and to minimize the number of adjacencies. They serve as a central point for exchanging the routing information among all the routers. Since point-to-point links are directly connected, so DR and BDR are not elected.

Based on the following rules, the DR and BDR are elected:

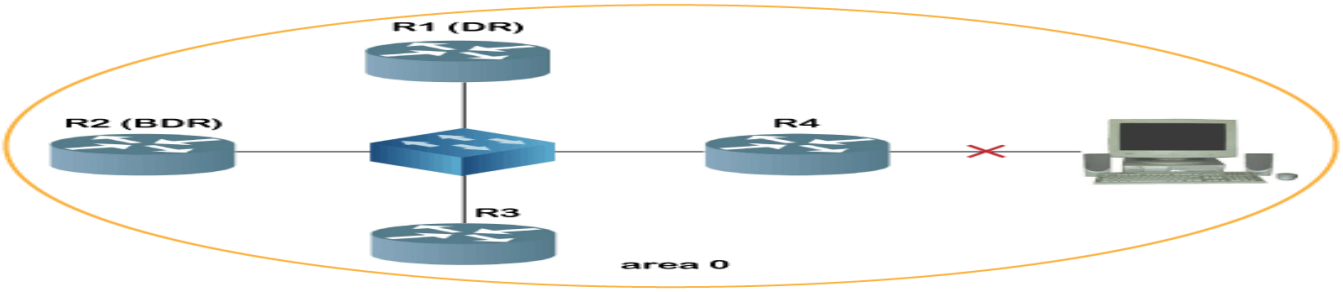
- The router with the highest OSPF priority is chosen as the DR. By default, the highest priority is set as 1.
- If there is no highest priority, then the router with the highest router Id is chosen as the DR, and the router with the second-highest priority is chosen as the BDR.

The following are the major advantages of the OSPF protocol:

- OSPF can be configured on both IPv4 and IPv6 versions of IPs.
- It can carry out load balancing.
- It uses the SPF algorithm to present a loop-free technology.
- It is not Cisco proprietary. It can run on many routers.
- It is a classless protocol.
- It has unlimited hop counts.
- It works very fast.

The following are the disadvantages of the OSPF protocol:

- It needs extra storage. Therefore, it means that it needs an extra CPU process to run the SPF algorithm.
- It needs more RAM to save adjacency topology.
- It is very complex. Therefore, it’s very difficult to troubleshoot.



In the above figure, R1 is chosen as the DR, while R2 is chosen as the BDR as R1 has the highest router ID, whereas the R2 has the second-highest router ID. If the link fails between R4 and the system, then R4 updates only R1 and R4 about its link failure. Then, DR updates all the non-DR and non-BDR about the change, and in this case, except R4, only R3 is available as a non-DR and non-BDR.

BGP (Border Gateway Protocol)

BGP (Border Gateway Protocol) is the protocol underlying the global routing system of the internet. It manages how packets get routed from network to network through the exchange of routing and reachability information among edge routers. BGP directs packets between autonomous systems (AS), which are networks managed by a single enterprise or service provider.

BGP creates network stability by guaranteeing routers can adapt to route failures: when one path goes down, a new path is quickly found. BGP makes routing decisions based on paths, defined by rules or network policies set by network administrators.

How does BGP work?

Each router maintains a routing table controlling how packets are directed. Routing table information is generated by the BGP process on the router, based on incoming information from other routers, and information in the BGP routing information base (RIB), which is a data table stored on a server on the BGP router. The RIB contains information both from directly connected external peers, as well as internal peers, and based on policies for what routes should be used and what information should be published, continually updates the routing table as changes occur.

What is BGP used for?

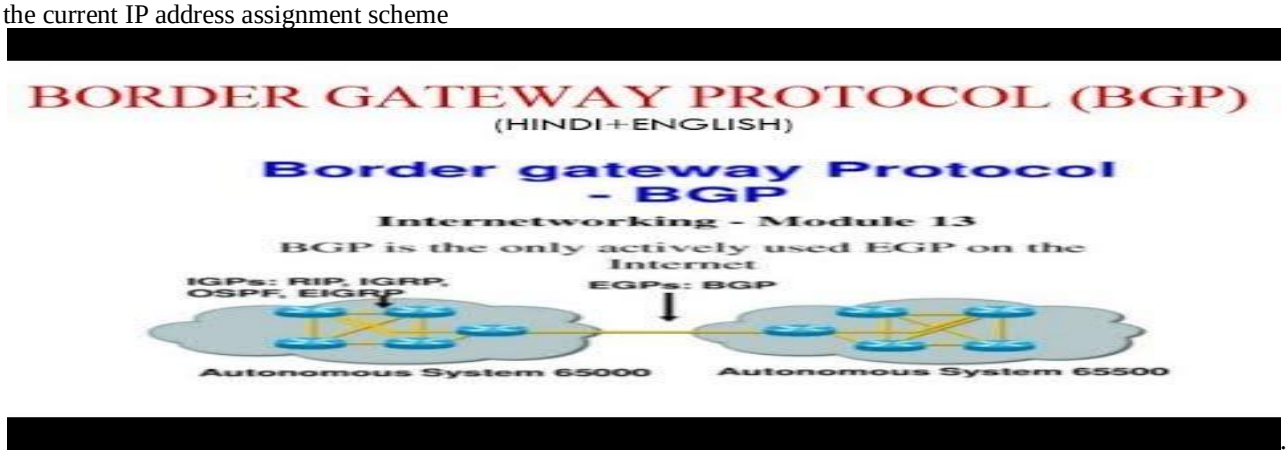
BGP offers network stability that guarantees routers can quickly adapt to send packets through another reconnection if one internet path goes down. BGP makes routing decisions based on paths, rules or network policies configured by a network administrator. Each BGP router maintains a standard routing table used to direct packets in transit. BGP uses client-server topology to communicate routing information, with the client-server initiating a BGP session by sending a request to the server.

BGP routing basics

BGP sends updated router table information only when something changes, and only the affected information. BGP has no automatic discovery mechanism, which means connections between peers must be set up manually, with peer addresses programmed in at both ends.

BGP makes best-path decisions based on current reachability, hop counts and other path characteristics. In situations where multiple paths are available -- as within a major hosting facility -- BGP policies communicate an organization's preferences for what path traffic should follow in and out. BGP community tags can control route advertisement behavior among peers.

BGP in networking is based on TCP/IP. It operates on the OSI Transport Layer (Layer 4) to control the Network Layer (Layer 3). As described in RFC4271 and ratified in 2006, the current version of BGP-4 supports both IPv6 and Classless Inter-Domain Routing (CIDR), which enables the continued viability of IPv4. Use of the CIDR is a way to have more addresses within the network than with the current IP address assignment scheme



Common BGP issues

Common issues with BGP include information exchange failures. Information exchanges don't always succeed as information can be improperly formatted or contain incorrect data. Routers can run out of memory or storage, or be too slow to respond to updates. Routers send error codes and subcodes to communicate problems including timeouts, malformed requests and processing problems.

BGP security

BGP is also vulnerable to attacks based on misinformation. Malicious actors can flood a router with bad packets in a denial-of-service attack, for example. They can also claim to be the source of routing information for an AS, and (temporarily) control where traffic headed from that AS goes, a practice known as BGP hijacking.

Difference between internal and external BGP, OSPF

When BGP is used to route within a single AS, it is called internal BGP, or iBGP. When used to connect one AS to others, it is called external BGP, or eBGP.

Internet Control Message Protocol version 4 (ICMPv4)

Introduction

As we are aware the IPv4 protocol doesn't have any mechanism to report errors or correct errors. So, IP functions in assistance with ICMP, report errors. ICMP never gets involved in correcting the errors. Higher-level protocols take care of correcting errors. Every time, ICMPv4 deliver an error report to the original source of the datagram.

There can be several reasons behind reporting the error like:

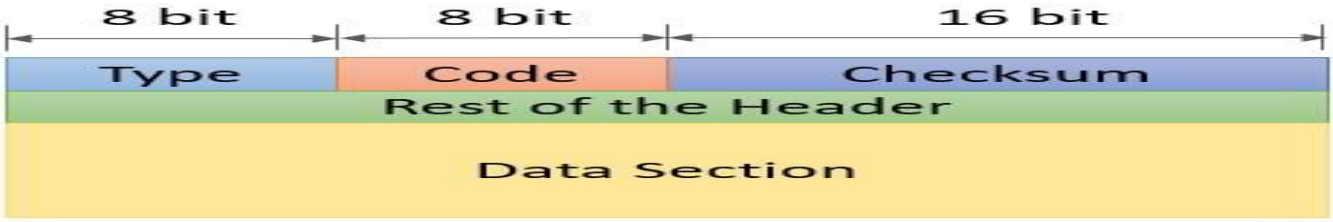
- A router with a datagram for a host in another network, may not find the next hop (router) to the final destination host.
- Datagram's time-to-live field has become zero.
- There may be ambiguity in the header of the IP datagram.
- It may happen that all the fragments of the datagram do not arrive within a time limit to the destination host.

And there can be several reasons to report the error.

Though ICMP is a network layer protocol, its messages are not passed to the lower layer (i.e. data link layer). Initially, the IP datagram encapsulates ICMP messages and then they are passed to the lower layer.

ICMPv4 Message Format

Below we have the message format for the ICMPv4 message. It has an 8-byte header and apart from this, it has a variable size data section. Though the header format gets changed for each type of message. Still, the first 4 bytes of each message remains the same.



General Format of ICMP Messages

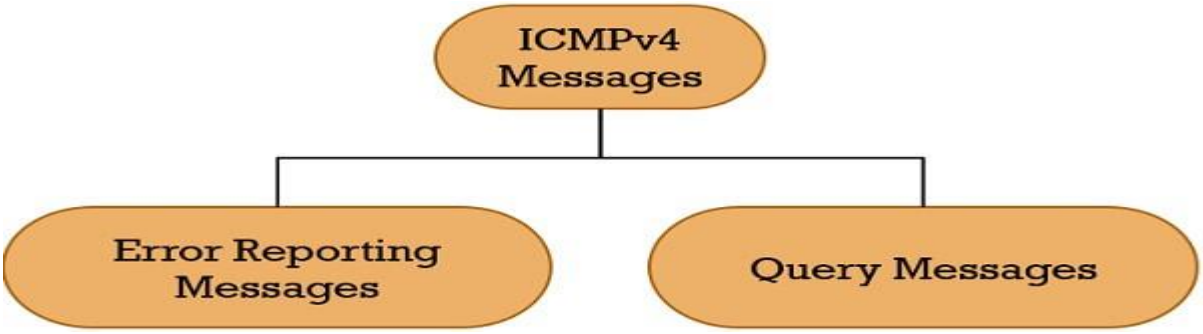
Among these first 4 bytes, the first byte describes the 'type' of the message. The second byte clarifies the reason behind the 'type' of the message. The next two bytes define the checksum field of the message.

The rest 4 bytes defines the rest of the header which is specific for each message type. The data section varies according to the type of message. The error reporting message's data section holds the information to identify the original datagram that has an error. The data section of the query message holds more information regarding the type of query.

Types of ICMPv4 Messages

The types of ICMPv4 messages as:

1. Error Reporting Messages
2. Query Messages



Error Reporting Messages

The most important function of ICMPv4 is to report the error. Although it is not responsible to correct the errors. The higher-level protocols take the responsibility of correcting the errors.

ICMPv4 always send the error report to the original source of the datagram. As the datagram has only two addresses in its header:

1. Source address
2. Destination address.

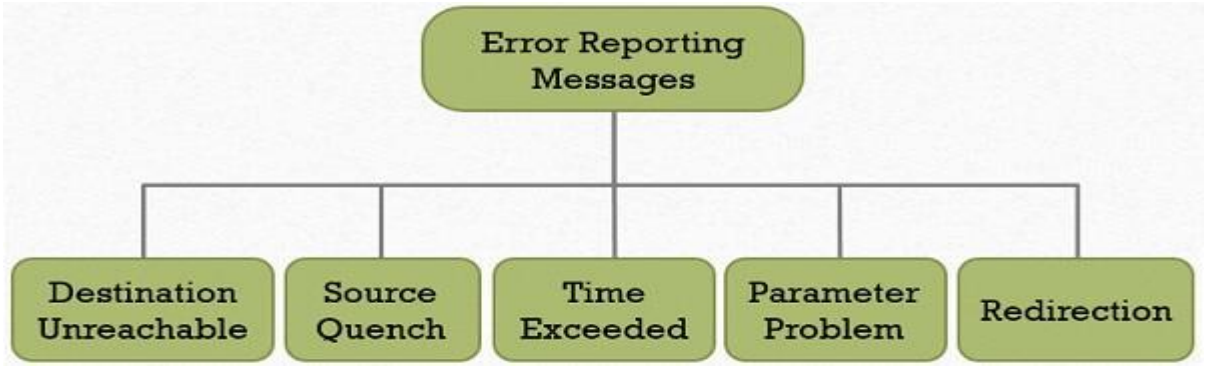
So, ICMPv4 uses the source address for reporting the error.

There are some important characteristics of the ICMPv4 message:

- ICMPv4 error messages are not generated in response to ICMP error messages. As this can create infinite repetition.
- The error message does not generate for the fragmented datagram. If the fragment is not the first fragment.
- ICMPv4 error message is not generated for the datagram having the special address, 127.0.0.0 or 0.0.0.0.
- This message is not generated for the datagrams with the broadcast address or a multicast address in its destination field.

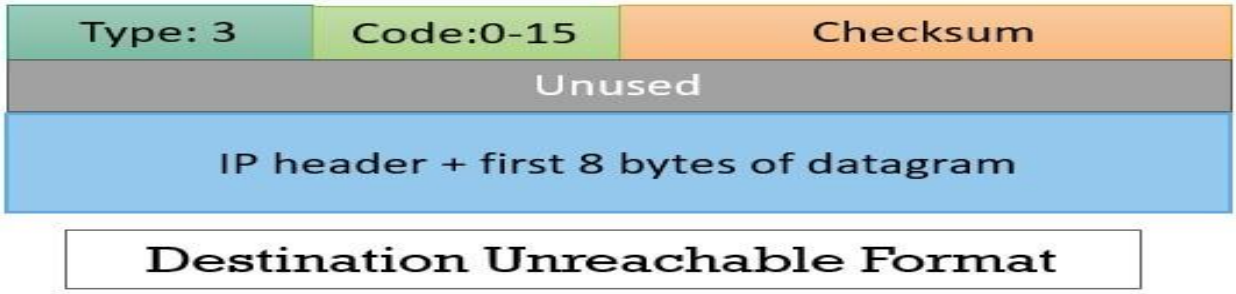
ICMPv4 Error Reporting Messages are further classified as:

1. Destination Unreachable
2. Source Quench
3. Time Exceeded
4. Parameter Problems
5. Redirection



Destination Unreachable

Consider if a host or a router is unable to deliver or route the datagram. Then they discard the datagram. And send a destination unreachable error message to the original source host.



Destination Unreachable Format

Refer to the image above, you will observe that the Type section of the destination unreachable error message is '3'. The Code section defines the reasons for discarding the message. For destination, unreachable message code ranges from 0-15.

Unreachable Messages Codes

1. Code 0 – Network unreachable. There is the possibility of hardware failure.
2. Code 1 – Destination host unreachable. There is the possibility of hardware failure.
3. Code 2 – Protocol unreachable. This means the protocol may not be running for which the datagram is destined.
4. Code 3 – Port unreachable. This means. the process (application program) for which the datagram is destined may not be running.
5. Code 4 – If the sender has specified not to fragment datagram. But routing is impossible without fragmentation.
6. Code 5 – Unable to accomplish source routing. This means one or more routers defined in the source routing option is unreachable.
7. Code 6 – The router has no information regarding the destination host network.
8. Code 7 – The router doesn't have any information about the existence of the destination host. It is difficult to identify whether the destination host exists or not.
9. Code 8 – The originating source host is isolated.
10. Code 9 – Unable to communicate with the destination network. Due to administration prohibition.
11. Code 10 – Unable to communicate with the destination host. Due to administration prohibition.
12. Code 11 – For the specified service. The network is unreachable.
13. Code 12 – For the specified service. The host is unreachable.
14. Code 13 – The destination host is unreachable. As the administrator has put a filter over it.
15. Code 14 – Due to violation of host precedence, the host is unreachable.
16. Code 15 – Host is unreachable as its precedence was cut off.

The destination host generates the destination unreachable error message with the code as 2 or 3 . And the router generates a message with the rest of the codes.

Source Quench

The source quench error message informs the source that the datagram has been discarded. Due to congestion in the router or destination host.

Source Quench Format

Time Exceeded

Every datagram has a field 'time-to-live', which decrements by 1 every time it visits a router. There can be two reasons to send the time exceeded message to the source host which is defined by code 0 and code 1.

Time Exceeded Message Format

1. Code 0 – When this time-to-live field decrements to zero the router discards the datagram. And send a time exceeded error message to the originating source of the datagram.
2. Code 1 – If the destination host doesn't receive all the fragments of a datagram in a set time. Then it discards all the fragments and sends a time exceeded error message to the source host.

Parameter Problem

If the destination host or the router find any ambiguity in the header of the IP datagram. Then they discard the datagram. And send a parameter problem error message to the originating source host of the datagram.

Parameter Problem Message Format

1. Code 0 defines that there is ambiguity in the header field of the datagram. And the pointer field's value points to the byte of the datagram header, which has a problem.
2. Code 1 defines that the required part of the header is missing. Here, the pointer field is not used.

Redirection

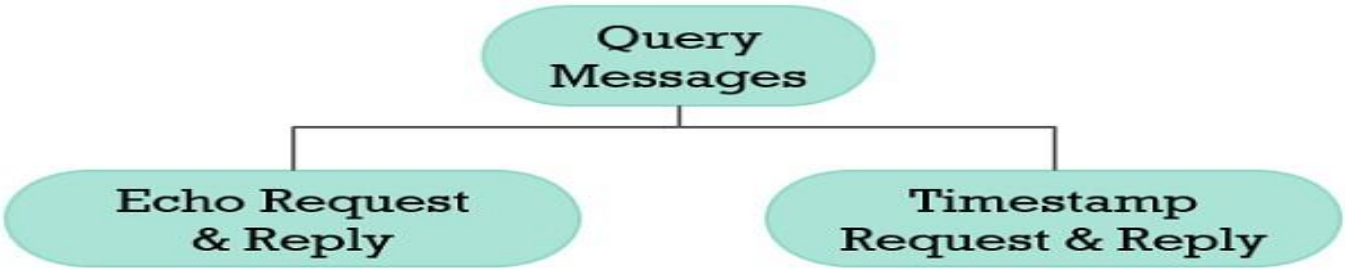
A router sends a redirection message to the localhost in the same network to update its routing table. The router here does not discard the received datagram. Instead, it forwards it to the appropriate router.

Redirection Message Format

1. The message with this code 0 redirects for the network-specific route.
2. The message with this code 1 redirects for the host-specific route.
3. However the message with this code 2 redirects for the network-specific route for a specific type of service.
4. And the message with this code 3 redirects for the host-specific route for a specific type of service.

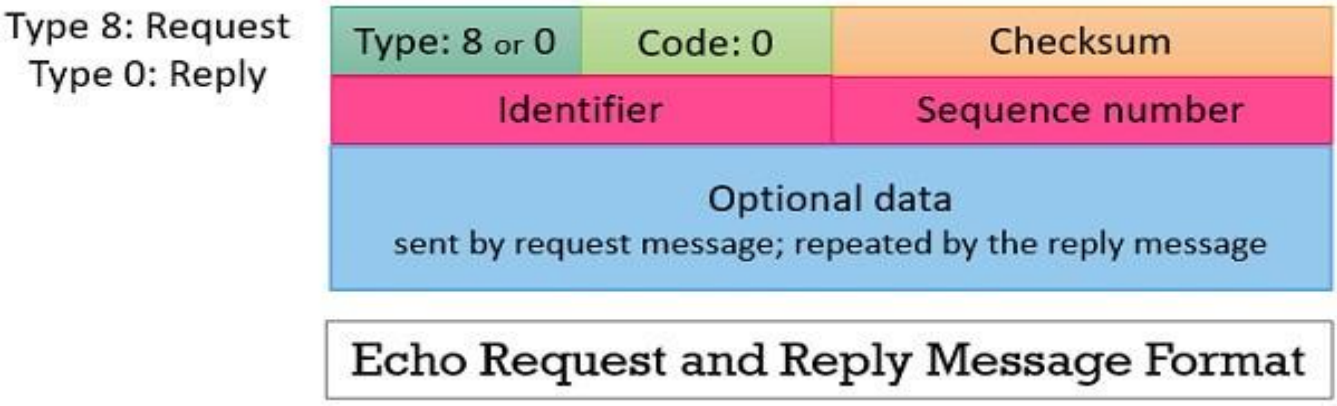
Query Messages

Query messages are for identifying network problems. Earlier there were five query messages among which three are deprecated. The two query messages that are being used today are:



Echo request and reply

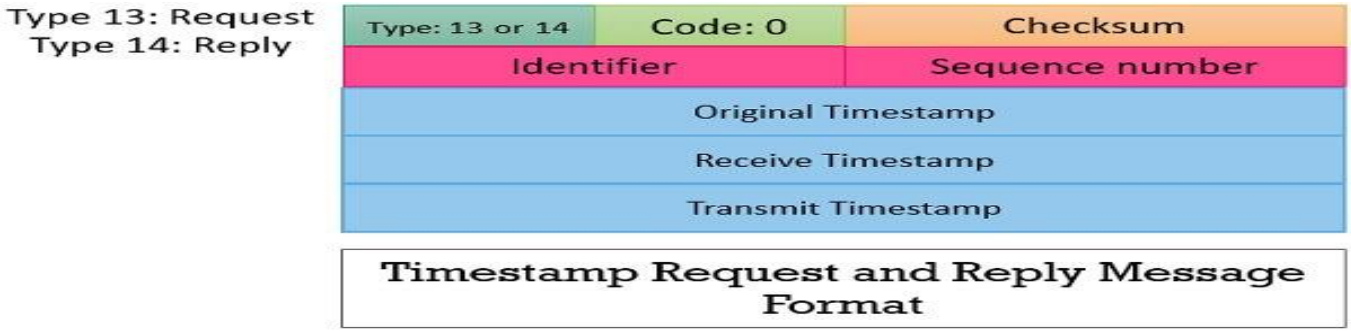
When echo request and reply messages are exchanged from one host or a router to another host or a router. It confirms that the two hosts or routers can communicate with each other.



If a host or a router wants to communicate with another host or a router. Then it sends the echo request message to the corresponding host or router with which it wants to communicate. The host or router receiving the echo request message prepares an echo reply message. And send it to the original sender confirming that it is ready to communicate.

Timestamp request and reply

Timestamp request and reply messages calculate the round trip time. It is the time required by an IP datagram to travel between two hosts or routers. This pair of messages are also used for synchronizing the clocks of two machines (hosts or routers).



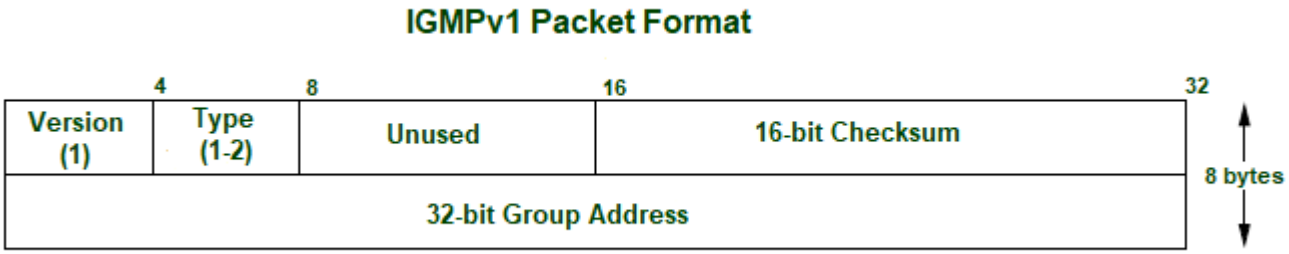
ICMPv4 protocol is a network layer protocol.

- This protocol is an error reporting protocol. And it reports an error that occurs while IP datagram travels from the source host to the destination host.
- ICMPv4 is a message-oriented protocol that is used in assistance with IP protocol as IP protocol lack error reporting.
- Ip datagram encapsulates ICMPv4 message before passing it to datalink layer.
- It is only responsible for reporting the error. ICMPv4 protocol doesn't correct the error.
- ICMPv4 is classified into two types of error messages and query messages which are also further classified as you can see above.

In version 6 of the TCP/IP protocol suite ICMPv4 is also revised with addition to version 6 of ICMPv6. The two internet debugging tools that utilize ICMPv4 are ping and traceroute.

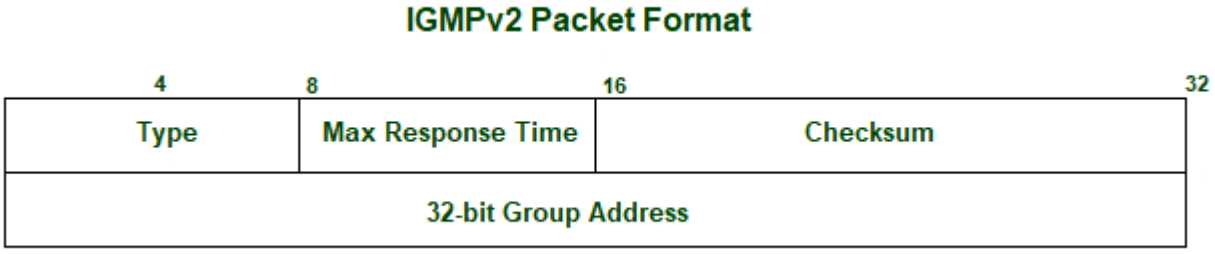
IGMP
is acronym for Internet Group Management Protocol. IGMP is a communication protocol used by hosts and adjacent routers for multicasting communication with IP networks and uses the resources efficiently to transmit the message/data packets. Multicast communication can have single or multiple senders and receivers and thus, IGMP can be used in streaming videos, gaming or web conferencing tools. This protocol is used on IPv4 networks and for using this on IPv6, multicasting is managed by Multicast Listener Discovery (MLD). Like other network protocols, IGMP is used on network layer. MLDv1 is almost same in functioning as IGMPv2 and MLDv2 is almost similar to IGMPv3. The communication protocol, IGMPv1 was developed in 1989 at Stanford University. IGMPv1 was updated to IGMPv2 in year 1997 and again updated to IGMPv3 in year 2002.
Applications:

- Streaming – Multicast routing protocol are used for audio and video streaming over the network i.e., either one-to-many or many-to-many.
- Gaming – Internet group management protocol is often used in simulation games which has multiple users over the network such as online games.
- Web Conferencing tools – Video conferencing is a new method to meet people from your own convenience and IGMP connects to the users for conferencing and transfers the message/data packets efficiently.



- Version – Set to 1.
- Type – 1 for Host Membership Query and Host Membership Report.
- Unused – 8-bits of zero which are of no use.
- Checksum – It is the one's complement of the sum of IGMP messages.
- Group Address – The group address field is zero when sent and ignored when received in membership query message. In a membership report message, the group address field takes the IP host group address of the group being reported.

2. IGMPv2 : IGMPv2 is the revised version of IGMPv1 communication protocol. It has added functionality of leaving the multicast group using group membership. The message packet format in IGMPv2:



Type:
0x11 for Membership Query

0x12 for IGMPv1 Membership Report

0x16 for IGMPv2 Membership Report

0x22 for IGMPv3 Membership Report

- Max Response Time – This field is ignored for message types other than membership query. For membership query type, it is the maximum time allowed before sending a response report. The value is in units of 0.1 seconds.
- Checksum – It is the one's complement of the sum of IGMP message.

- Group Address – It is set as 0 when sending a general query. Otherwise, multicast address for group-specific or source-specific queries.

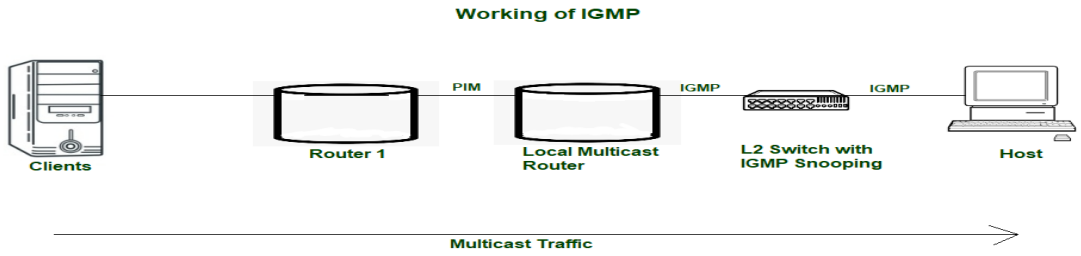
3. IGMPv3 : IGMPv2 was revised to IGMPv3 and added source-specific multicast and membership report aggregation. These reports are sent to 224.0.0.22. The message packet format in IGMPv3:

IGMPv3 Packet Format

Bit Offset	0-3	4	5-7	8-15	16-31
0	Type = 0x11			Max Response Code	Checksum
32	Group Address				
64	Resv	S	QRV	QQIC	Number of Sources (N)
96	Source Address[1]				
128	Source Address[2]				
	Source Address[N]				

- Max Response Time – This field is ignored for message types other than membership query. For membership query type, it is the maximum time allowed before sending a response report. The value is in units of 0.1 seconds.
- Checksum – It is the one's complement of the one's complement of the sum of IGMP message.
- Group Address – It is set as 0 when sending a general query. Otherwise, multicast address for group-specific or source-specific queries.
- Resv – It is set zero of sent and ignored when received.
- S flag – It represents Suppress Router-side Processing flag. When the flag is set, it indicates to suppress the timer updates that multicast routers perform upon receiving any query.
- QRV – It represents Querier's Robustness Variable. Routers keeps on retrieving the QRV value from the most recently received query as their own value until the most recently received QRV is zero.
- QQIC – It represents Querier's Query Interval Code.
- Number of sources – It represents the number of source addresses present in the query. For general query or group-specific query, this field is zero and for group-and-source-specific query, this field is non-zero.
- Source Address[i] – It represents the IP unicast address for N fields.

Working: IGMP works on devices that are capable of handling multicast groups and dynamic multicasting. These devices allows the host to join or leave the membership in the multicast group. These devices also allows to add and remove clients from the group. This communication protocol is operated between host and local multicast router. When a multicast group is created, the multicast group address is in range of class D (224-239) IP addresses and is forwarded as destination IP address in the packet.



L2 or Level-2 devices such as switches are used in between host and multicast router for IGMP snooping. IGMP snooping is a process to listen to the IGMP network traffic in controlled manner. Switch receives the message from host and forwards the membership report to the local multicast router. The multicast traffic is further forwarded to remote routers from local multicast routers using PIM (Protocol Independent Multicast) so that clients can receive the message/data packets. Clients wishing to join the network sends join message in the query and switch intercepts the message and adds the ports of clients to its multicast routing table.

Advantages:

- IGMP communication protocol efficiently transmits the multicast data to the receivers and so, no junk packets are transmitted to the host which shows optimized performance.
- Bandwidth is consumed totally as all the shared links are connected.
- Hosts can leave a multicast group and join another.

Disadvantages:

- It does not provide good efficiency in filtering and security.
- Due to lack of TCP, network congestion can occur.