VARDHAMAN COLLEGE OF ENGINEERING
(AUTONOMOUS)
Affiliated to **JNTUH**, Approved by **AICTE**, Accredited by **NAAC** with **A++** Grade, **ISO 9001:2015** Certified
Kacharam, Shamshabad, Hyderabad – 501218, Telangana, India.

Department of Artificial Intelligence and Machine Learning

III B.Tech I Sem (R-22)
Course: CN (A8519)

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.

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.

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.

NETWORK LAYER DESIGN ISSUES

1. Store and forward packet switching
2. Services provided to the transport layer
3. Implementation of Connectionless Service
4. Implementation of Connection-Oriented Service

1. Store-and-Forward Packet Switching:-

The major components of the network are the ISP's equipment are routers, switches, middle boxes connected by transmission lines.

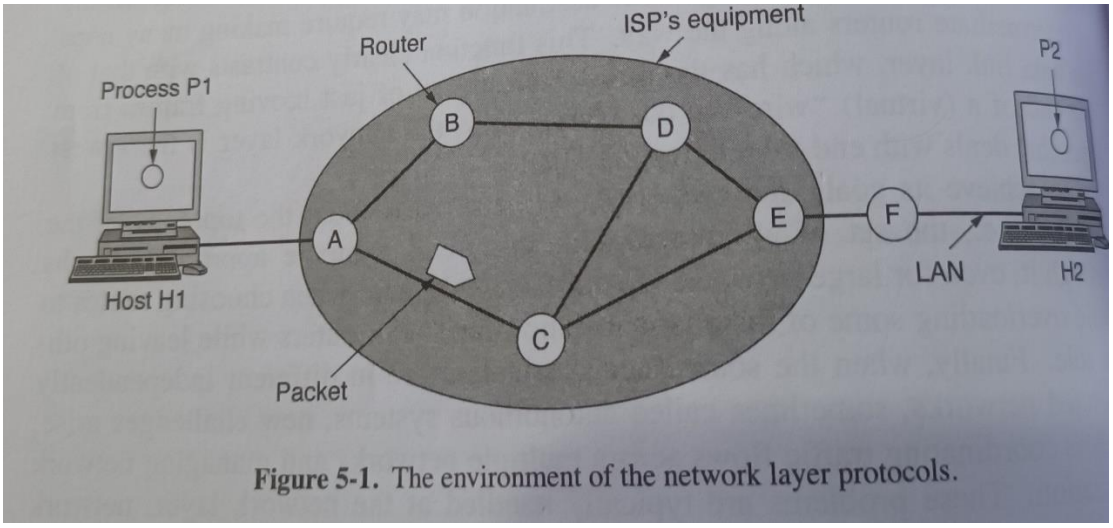


Figure 5-1. The environment of the network layer protocols.

- Host H1 is directly connected to one of the ISP's routers A.
- Host H2 is on a LAN connected through F router.
- A host with a packet to send transmits it to the nearest router, either on its own LAN or over a point to point link to the ISP.
- The packet is stored there until it has fully arrived and the link has finished its processing by verifying the checksum.
- Then it is forwarded to the next router along the path until it reaches the destination host, where it is delivered. This mechanism is store and forward packet switching.

2. Services provided to transport layer:-

The network layer provides services to the transport layer at the network layer/transport layer interface.

- The services should be independent of the router technology.
- The transport layer should be shielded from the number, type and topology of the routers present.
- The network addresses made available to the transport layer should use auniform numbering plan, even across LANs and WANs.

3. Implementation of Connectionless Service:-

- In **Connection less service**, packets are injected into the network individually and routed independently of each other. No advance setup is needed.In this context, the packets are frequently called **datagrams,** and the network is called a **datagram network**.
- In **Connection oriented service**, a path from the source router all the way to the destination router must be established before any data packets can be sent. This connection is called **Virtual Circuit (VC)** and the network is called **Virtual Circuit network.**

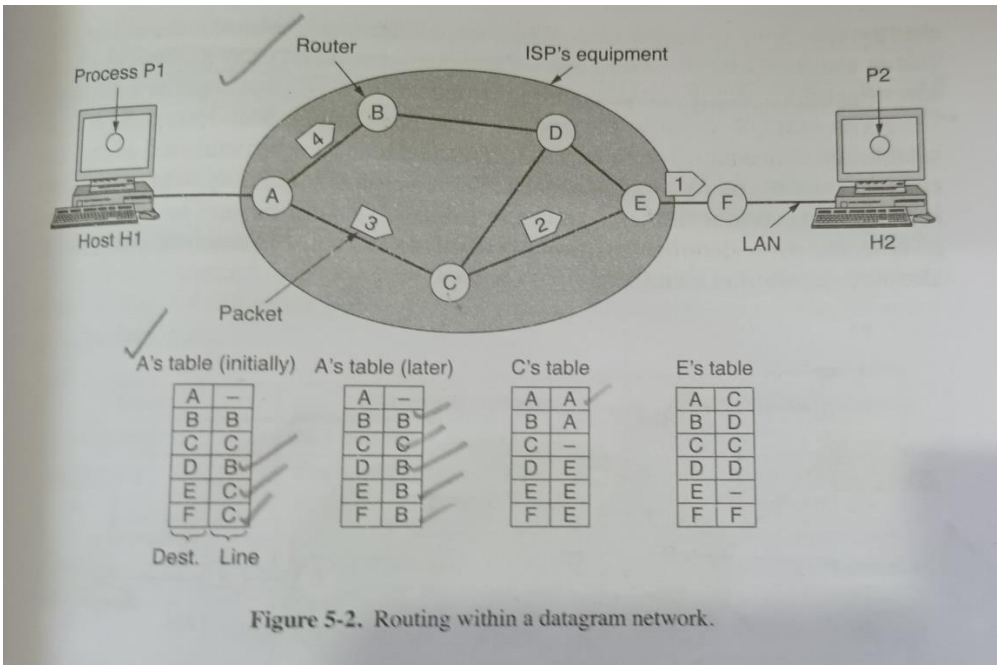


Figure 5-2. Routing within a datagram network.

Example:-

In the above example, Host H1 wants to send message to H2, message is split into packets. H1 have to send 4 packets. H1 send s to A. Router A has two ways to transmit initially. Packet 1,2,3 are forwarded from A to C to E to F accordingly. When Packet 4 wants to send, A choose B router to transmit to F. Each router will main a routing table. The algorithm that manages the tables and makes the routing decisions is called **routing algorithms.** Routing tables will be updated periodically.

4. Implementation of Connection – Oriented Service:-

- In this, we need to have a virtual circuit network. The idea behind virtual circuits is to avoid having to choose a new route for every packet sent.
- Before the transmission of the packets only connection will be established. Then only send will transmit the packets.
- When a connection is established a route from the source machine to the destination machine is chosen as a part of the connection setup and stored in tables inside the routers.
- That route is used for all traffic flowing over the connection, exactly same as telephone, system.
- When the connection is released, the virtual circuit is also terminated. With connected-oriented services, each packet carries an identifier telling which virtual circuit it belongs to.

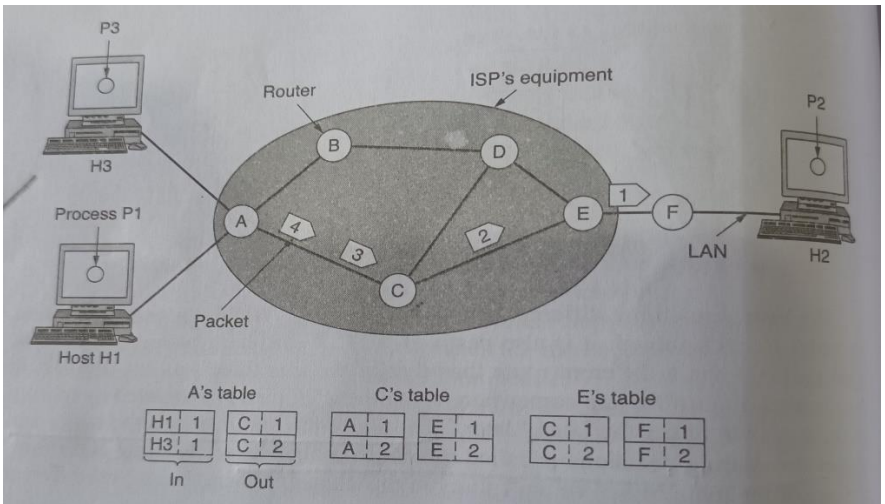


Figure 5-3. Routing within a virtual-circuit network.

Issue	Datagram network	Virtual-circuit network
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

Figure 5-4. Comparison of datagram and virtual-circuit networks.

ROUTING ALGORITHMS

- The main function of network layer is routing packets from source machine to destination machine.
- The routing algorithm is a network layer software responsible for deciding which output line an incoming packet should be transmitted on.
- It is useful to make a distinction between routing and forwarding.
- **Routing** – which is making the decision which routes to use.
- **Forwarding** – which is what happens when a packet arrives.
- A router is having two processes inside. One of them handles each packet as it arrives, looking up the outgoing line to use for it in the routing tables. This process is **forwarding**.

Routing is the process of establishing the routes that data packets must follow to reach the destination. In this process, a routing table is created which contains information regarding routes that data packets follow. Various routing algorithms are used for the purpose of deciding which route an incoming data packet needs to be transmitted on to reach the destination efficiently.

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.

The primary function of routing algorithm is to find the shortest and optimal path between source and destination in computer Networks.

There are mainly two types of routing ie Static and Dynamic Routing

Static Routing : Static Routing is also known as **non-adaptive** routing which doesn't change the routing table unless the network administrator changes or modifies them manually. Static

routing does not use complex routing algorithms and It provides high or more security than dynamic routing.

Dynamic Routing : Dynamic routing is also known as **adaptive** routing which changes the routing table according to the change in topology. Dynamic routing uses complex routing algorithms and it does not provide high security like static routing.

Differences b/w Adaptive and Non-Adaptive Routing Algorithm

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

ROUTING ALGORITHMS

→ The main function of router is to transmit the packets from source router to destination router.

→ These routing alg(m) are mainly used in n/w layer.

→ In a graph, we may have 'n' no of routes/paths in order to travel from source router to dest. router.

→ The major task of router is to choose a best path (shortest, least-cost path).

→ Classification of routing algorithms :-

1. Non-adaptive routing alg(m)
   ↳ also called as static routing alg(m)
2. Adaptive routing alg(m)
   ↳ Dynamic routing alg(m).

(i) Non-adaptive routing alg(m) :-

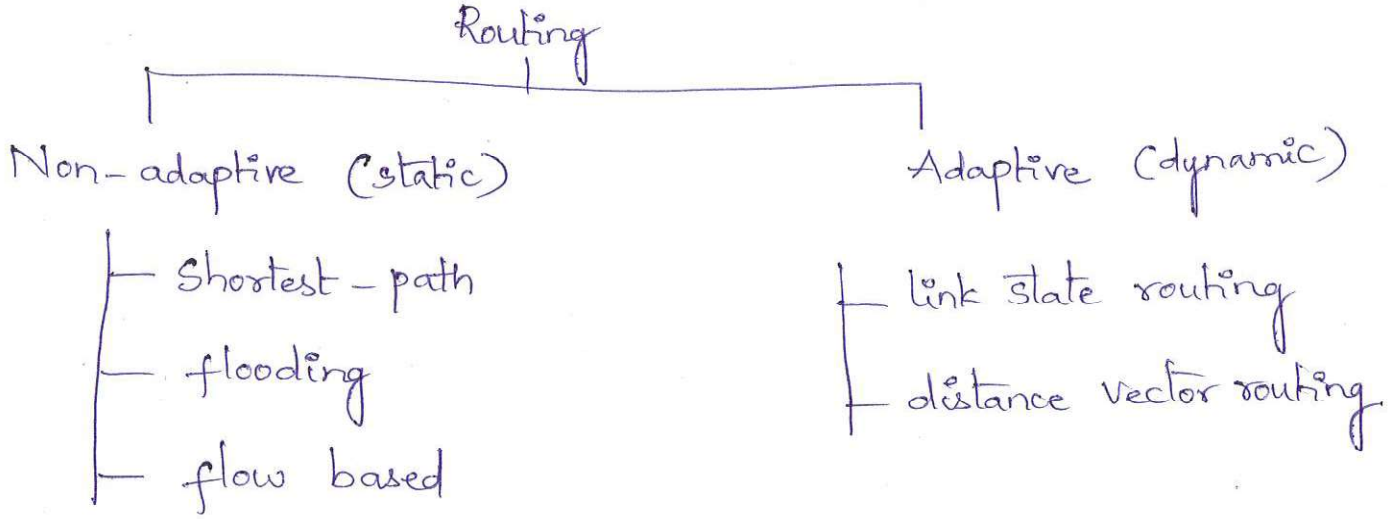
* Routing process will be designed in advance.
* It doesn't effect with change in n/w topology & traffic.
* It doesn't use any routing protocols. It is the responsibility of n/w administrator to configure that routing table.
* Every router will maintain routing table, fixed.
* Therefore, routing decision taken by n/w administrator.
* Route is always fixed/constant.

* Routing tables for all routers are preloaded before transmission.

(2) Adaptive routing alg(m) :-

* Adapts to traffic i.e., if router fails (or) link fails (or) heavy traffic, a router can change its route to transmit a packet.
* It uses different routing protocols. Router can make decision on its own. (dynamically)
* Routing tables will be changed periodically when in traffic (or) topology changes.
* Routing decisions changes, according to situation.
* No constant route.
* Routing tables will not be preloaded.
* Main parameters are hop count, distance, transmit time.

***



Routing alg(m)

- Adaptive
  - isolated
  - distributed
  - centralized
- Non-adaptive
  - flooding
  - random walk.

* Isolated :- * Its routing decisions using info without seeking info from other nodes.
  * It obtains the routing info by using local info.

* centralized :-
  * It is also called as global routing alg(m).
  * A centralized node has entire info about the n/w and makes all routing decisions.
    ↳ Finds least-cost path b/w source – destination.

* Distributed :-
  * It is decentralized alg(m).
  * It computes least-cost path b/w source – destination.
  * It takes info from neighbours & takes decisions about routing.

* Flooding :- Every incoming packet is sent on every out-going line except from which it arrived.
  ↳ Disadvantage – Node may contain several copies of single packet.

* Random Walk :- A packet sent by the node to one of its neighbour node randomly.

→ It is also called as probabilistic alg(m).

FLOODING (Broadcasting)

⇒ How to stop and eliminate duplicate packets

(1) Using a hop counter
   ↳ decrement in each router
   ↳ discard the packet if counter is '0' (zero).

(2) Apply sequence no in packet
   ↳ avoid sending packet (same) second time.
   ↳ Keep in each router per source a list of packets already seen.

(3) Selective flooding
   ↳ Use only those lines that are going approximately in right direction.

Properties of routing algorithm

* Correctness
* Simplicity
* robustness
* stability
* fairness
* efficiency

DISTANCE VECTOR ROUTING ALGORITHM.

* It is a dynamic alg(m).
* This alg(m) is distributed, iterative and asynchronous.
* This alg(m) is based on Bellman-Ford alg(m) equation.
* Bellman-Ford alg(m) is used to find shortest path b/w nodes in the given graph. (Least-cost path).
* Equation :-

$d_x(y)$ = cost of least cost path from x to y

where x is source, y is destination.

* Each node/router maintains a routing table initially by finding the distance to its neighbour node.
* Routing table consists of three parts

Destination	Distance	Next hop/router/node

* After construction of routing table, every router shares its routing table with its neighbour.
  - Routing table info here is only distance not entire table. (Distance Vector)
* By using neighbouring router distance, every router's routing table will be updated.

i.e., Two major steps are creating routing table,

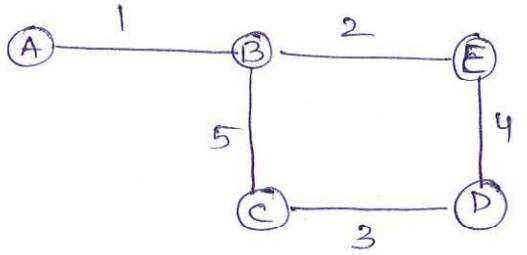
updating routing table.

* Update distance, based on neighbour node.

$$d_x(y) = \min_v \{ cost(x,v) + d_v(y) \}$$

where v is intermediate node.

Examples - 1



⇒ **Step 1 :-**

A

A	0	A
B	1	B
C	∞	—
D	∞	—
E	∞	—

B

A	1	A
B	0	B
C	5	C
D	∞	—
E	2	E

C

A	∞	—
B	5	B
C	0	C
D	3	D
E	∞	—

D

A	∞	—
B	∞	—
C	3	C
D	0	D
E	4	E

E

A	∞	—
B	2	B
C	∞	—
D	4	D
E	0	E

⇒ **Step 2 :-** Update all routers routing tables by using neighbouring router's distance vector.

Updated A

A	0	A
B	1	B
C	6	B, C
D	7	B, E, D
E	3	B, E

$A \to C \Rightarrow A \to B + B \to C$

$1 + 5 = 6.$

$A \to D \Rightarrow A \to B + B \to C + C \to D$

$1 + 5 + 3 = 9$ X

(or)

$A \to B + B \to E + E \to D$

$1 + 2 + 4 = (7)$ ✓

least cost

$A \to E \Rightarrow A \to B + B \to E$

$1 + 2 = 3$

Updated B

A	1	A
B	0	B
C	5	C
D	6	E, D
E	2	E

Updated C

A	6	B, A
B	5	B
C	0	C
D	3	D
E	7	E

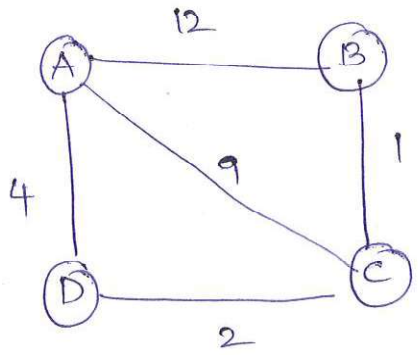
Updated D

A	7	E, B, A
B	6	E, B
C	3	C
D	0	D
E	4	E

Updated E

A	3	A
B	2	B
C	7	C
D	4	D
E	0	E

Example – 2



A

A	0	A
B	12	B
C	9	C
D	4	D

B

A	12	A
B	0	B
C	1	C
D	∞	—

C

A	9	A
B	1	B
C	0	C
D	2	D

D

A	4	A
B	∞	—
C	2	C
D	0	D

updated tables

A

A	0	A
B	7	D,C,B
C	6	D,C
D	4	D

B

A	7	C,D
B	0	B
C	1	C
D	3	C,D

C

A	6	D
B	1	B
C	0	C
D	2	D

D

A	4	A
B	3	C
C	2	C
D	0	D

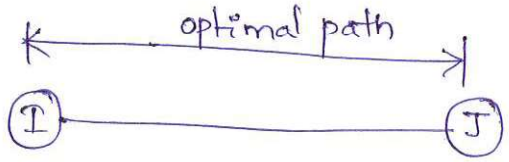
OPTIMALITY PRINCIPLE

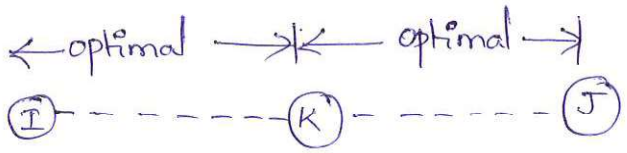
→ It states that if router j is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same route.

→ optimal path means, the path which is short in distance and short in cost.

On another words,

* If path from I to J is optimal then, if any router exists b/w I & J i.e., K (assume) then path from I to K and K to J will also be optimal.





SHORTEST PATH ROUTING ALGORITHM

⟹ Dijkstra alg(m). (or) static routing alg(m).

* One way of shortest path measurement is (path length) is number of hops.

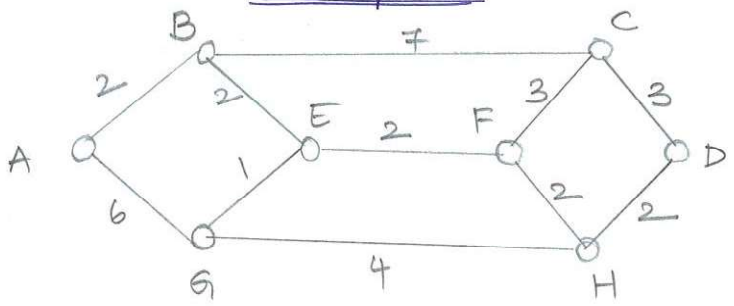
* Another metric is, geographic distance.

→ This alg(m), finds the shortest path b/w a given pair of routers.

→ shortest route based on function. Its parameters may be

cost, distance, traffic, time, bandwidth.

Example - 1



⇒ Key points :-

1. Each node is labeled (in parentheses) with its distance from the source node along the best known path.
2. The distances must be non-negative.
3. Initially, no paths are known, so all nodes are labeled with infinity.
4. As the alg(m) proceeds and paths are found, the labels may change.
5. A label may be either tentative (hollow circle), or permanent (filled / solid circle)
6. Initially, all labels are tentative. When it is discovered that a label represents the shortest possible path from the source to that node, it is made permanent and never changed.
7. In the graph, arrow mark (→) represents working node.

To illustrate this alg(m), consider the above graph as example.

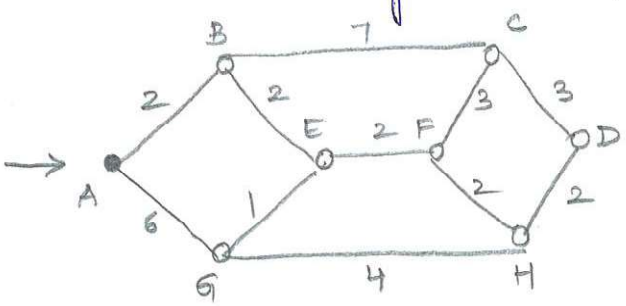
→ current working node is source — A

→ Each node is specified by path length (pair of cost and working node)

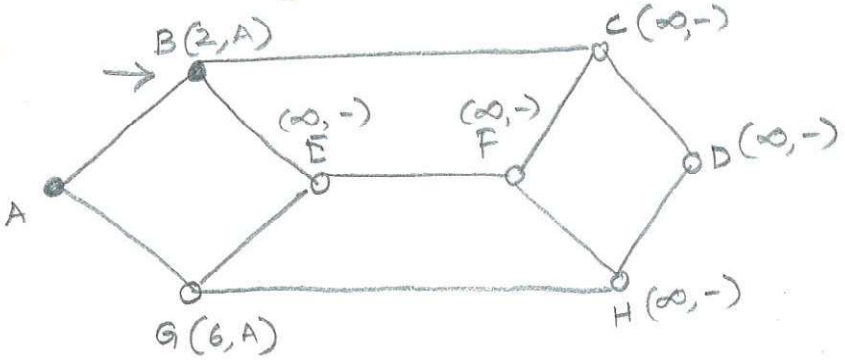
→ In path length, ∞ — path cost (unknown)

— (hyphen) — working node not known.

Step 1 :- Mark working node, permanent node — A (source)



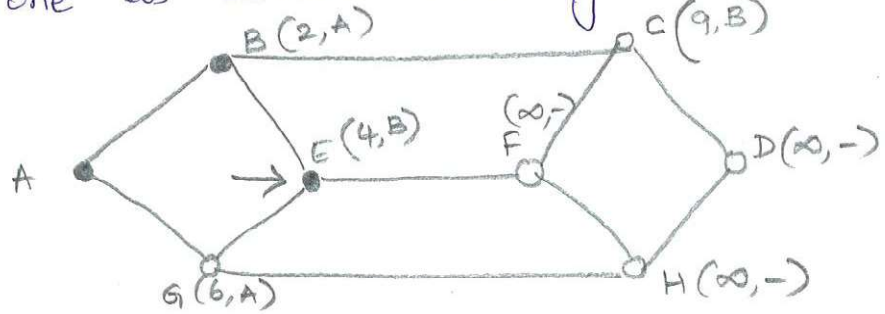
Step 2 :- visit and mark path length of A's neighbouring nodes. (B and G) and mark min one as working node.



* Mark other nodes path length also.
* Among B & G, B's path length is minimum. So, make it as working node.

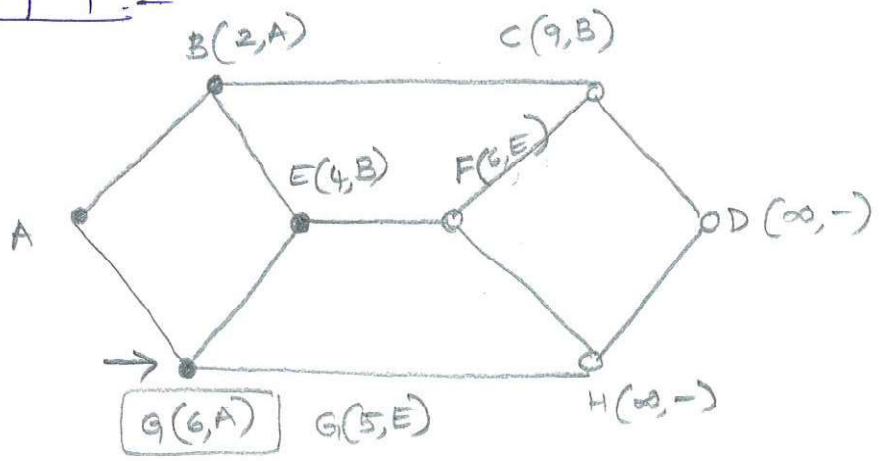
Step 3 :-

* Find neighbour nodes path length of B. Mark min one as current working node.



* Among C & E, E has min path length. So mark it as current working node. And find neighbour nodes length.

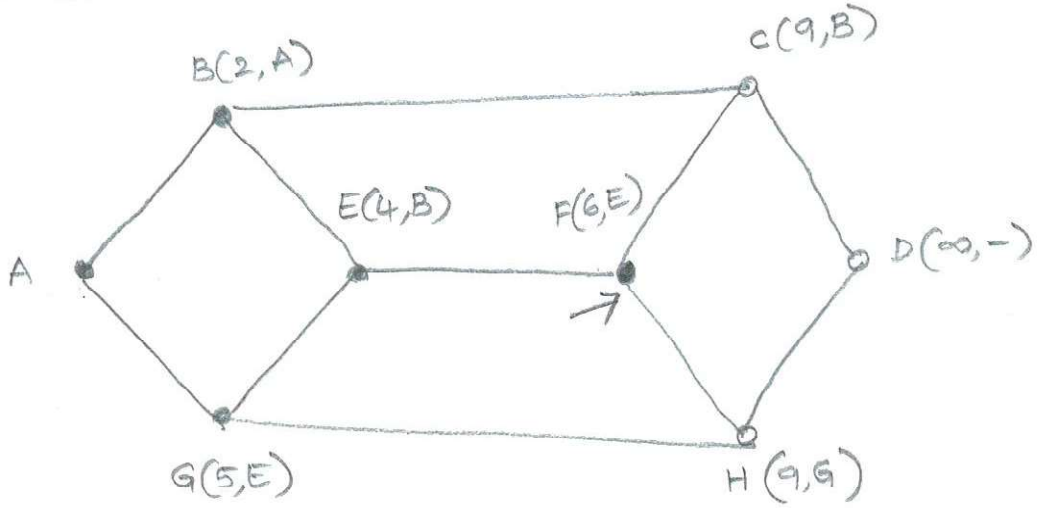
Step 4 :-



On this step, neighbours of E are F & G. While calculating path length of F & G, G path length is updated from G(6,A) → G(5,E). Among G & F, G's pathlength is min so mark it as current working node.

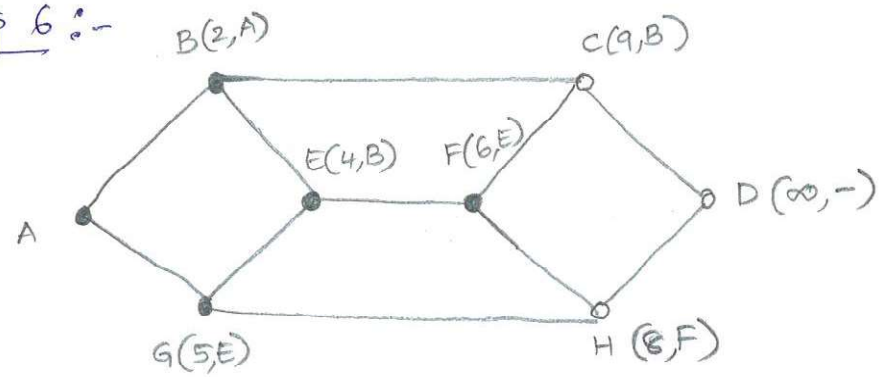
Step 5 :-

In this step, explore G's neighbour node (i.e., H path length). Identify current working node as which consists least cost.



Among, C, F, H, F has min pathlength. So mark it as current working node.

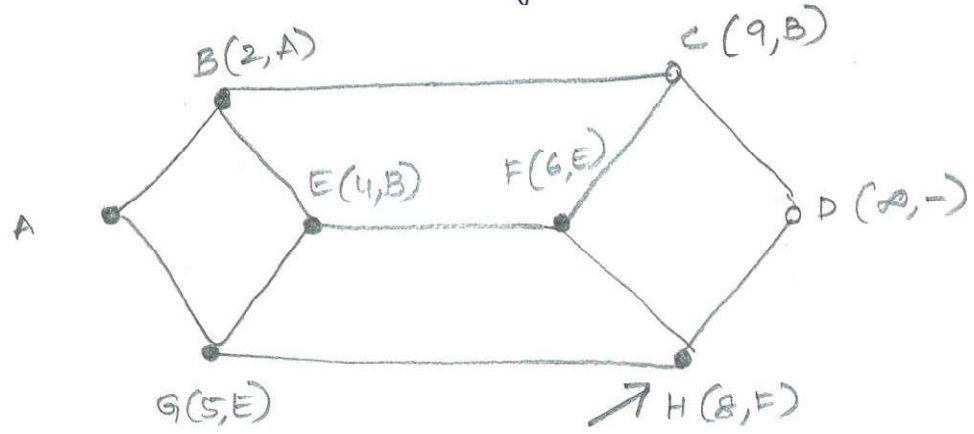
Step 6 :-

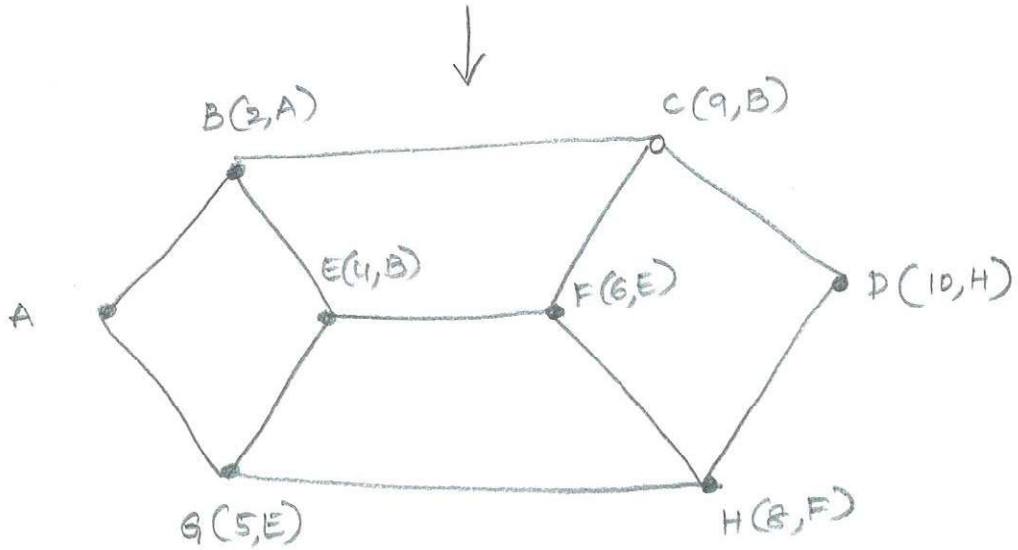


On above graph, H pathlength is updated because from F, among C & H, H length is min.

Step 7 :-

Among C,H, H is marked as working node and explore H's neighbour (i.e., D (destination) path).





finally Shortest path is,

A → B → E → F → H → D.

LINK STATE ROUTING ALGORITHM

→ The main aim of this algⁿ is to transmit packets from source to destination, by finding shortest path.

(remaining any router)

The idea behind link state routing is stated as follows.

1. Discover its neighbours & learn their n/w address.
2. Set the distance or cost metric to each of its neighbors.
3. Construct a packet telling all it has just learned.
4. Send this packet to and receive packets from all other routers.
5. Compute the shortest path to every other router.

On effect, the complete topology is distributed to every router.

→ Link state routing algⁿ is a dynamic routing algⁿ.

→ There are two phases.

(1) Flooding.

(2) Route calculation.

(1) Learning about neighbours :- When a router is booted, its first task is to learn about its neighbors. It accomplishes this by sending HELLO message/packet to its neighbors. Now corresponding neighboring routers contains the

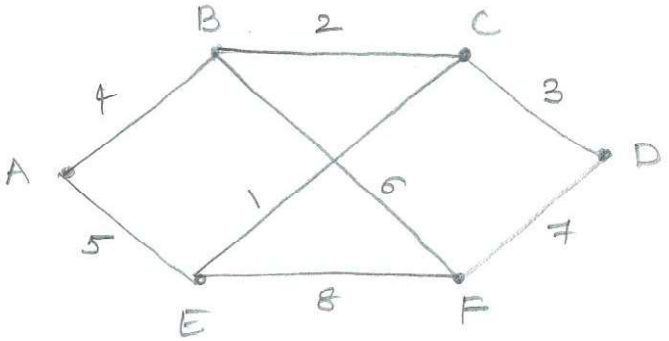
information about source. Every router will have inf(n) about its neighbouring router. Every router knows about what are neighbour routers, its cost inorder to reach neighbour.

(2) Setting Link costs :- The link state routing alg(m) requires each link to have a distance or cost metric for finding shortest paths.

(3) Building Link state packets :-

* Once the inf(n) needed for the exchange has been collected, the next step is for each router to build a packet containing all the data.
* The packet starts with the identity of the sender, followed by a sequence no & age. and a list of neighbors.
* The cost to each neighbor is also given.

Example :-



The link state packets for the above graph is as follows.

A	
Seq	
age	
B	4
E	5

B	
Seq	
age	
A	4
C	2
F	6

C	
Seq	
age	
B	2
D	3
E	1

D	
Seq	
age	
C	3
F	7

E	
Seq	
age	
A	5
C	1
F	8

F	
Seq	
age	
B	6
D	7
E	8

(4) Distributing the link state packets :-

* All of the routers must get all of the link state packets quickly & reliably.

* Distribution performed by flooding.

→ To keep flood check, each packet contains a sequence no that is incremented for each new packet sent.

→ Routers keep track of all the (source, sequence) pairs.

→ When a new link state packet comes in, it is checked against the list of pkts already seen.

→ If it is new, it is forwarded on all lines except the one it arrived on.

→ If it is a duplicate, it is discarded.

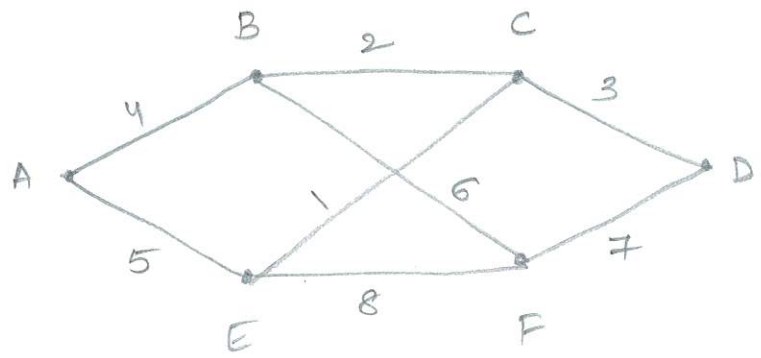
* Age field is also decremented by each router during the initial flooding process, to make sure that no packet can get lost & live for a period of time.

(5) Compute new routes :-

Now, dijkstra's alg(m) can run locally to construct the

shortest paths to all nodes.

⇒ For the given example, find the shortest path using link state routing alg(m), from node 'A' as source.



	B	C	D	E	F
A	(4)	∞	∞	5	∞
AB	(4)	6	∞	(5)	10
ABE	(4)	(6)	∞	(5)	10
ABEC	(4)	(6)	(9)	(5)	10
ABECD	(4)	(6)	(9)	(5)	(10)

ABECDF

⇒ shortest paths from A is as follows.

A → B = 4

A → C = 6

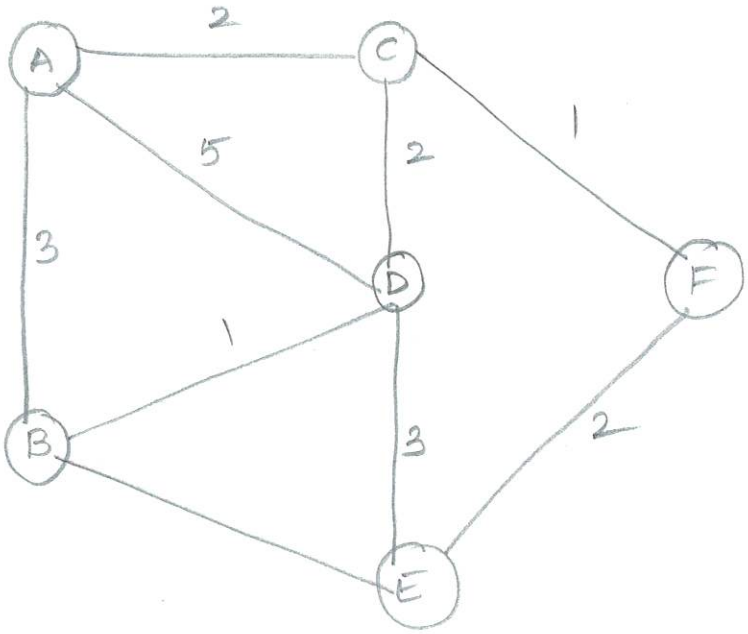
A → D = 9

A → E = 5

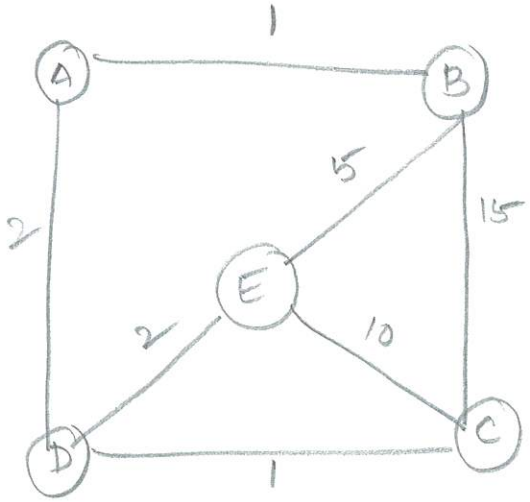
A → F = 10

Examples

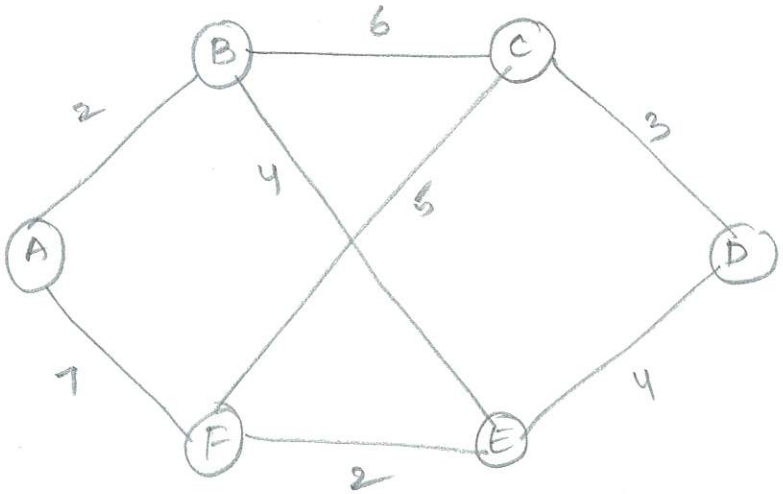
1.



2.



3.



CONGESTION CONTROL

Congestion control is a crucial concept in computer networks. It refers to the methods used to prevent network overload and ensure smooth data flow. When too much data is sent through the network at once, it can cause delays and data loss.

Congestion control techniques help manage the traffic, so all users can enjoy a stable and efficient network connection. These techniques are essential for maintaining the performance and reliability of modern networks.

Congestion in a computer network happens when there is too much data being sent at the same time, causing the network to slow down. Just like traffic congestion on a busy road, network congestion leads to delays and sometimes data loss.

Congestion control refers to the mechanisms and techniques used to control congestion and keep the traffic below the capacity of the network.

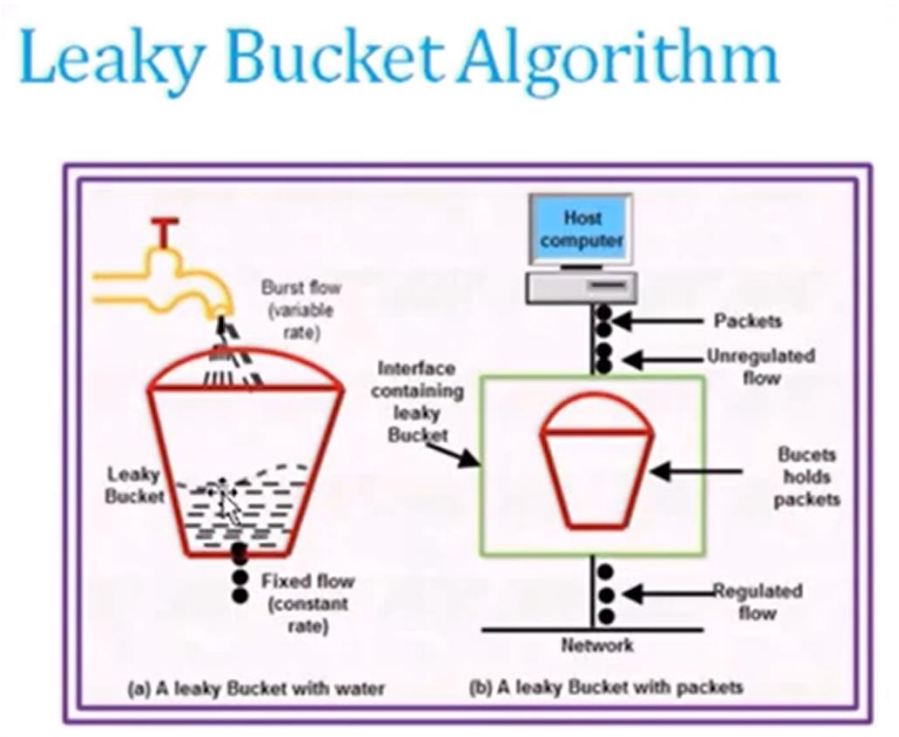
Causes of Congestion:-

1. Packet arrival rate exceeds the outgoing link capacity.
2. Insufficient memory to store incoming packets.
3. Bursty traffic.
4. Slow Processor.

Congestion control algorithms :-

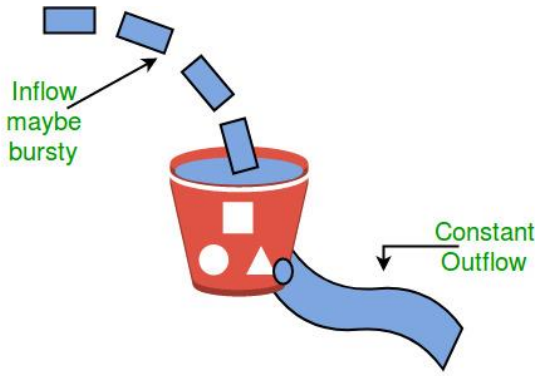
1. Leaky bucket algorithm
2. Token bucket algorithm

1. 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.

Let us consider an example to understand Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at constant rate. When the bucket is full with water additional water entering spills over the sides and is lost.



Similarly, each network interface contains a leaky bucket and the following steps are involved in leaky bucket algorithm:

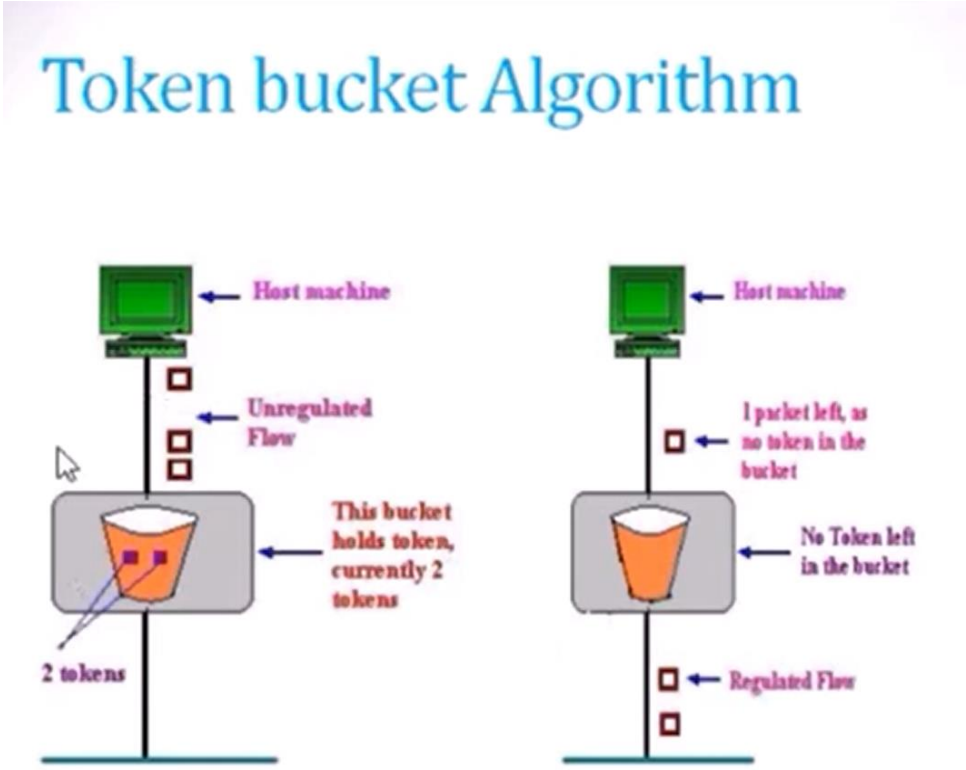
- When host wants to send packet, packet is thrown into the bucket.
- The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
- Bursty traffic is converted to a uniform traffic by the leaky bucket.
- In practice the bucket is a finite queue that outputs at a finite rate.

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

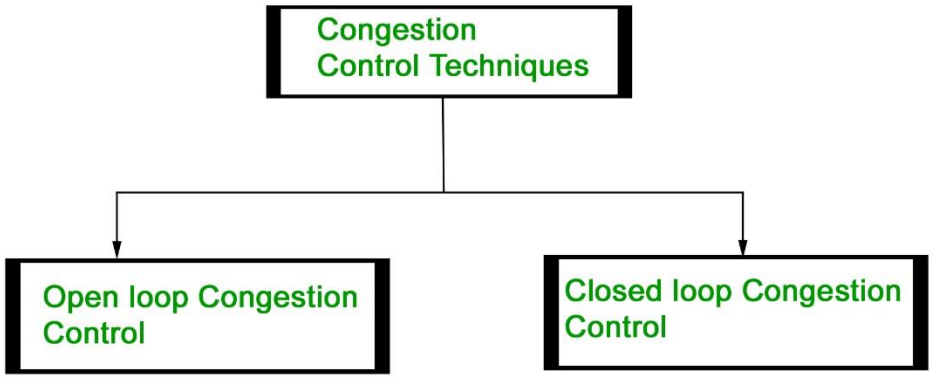
The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is. So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

Steps of this algorithm can be described as follows:

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

CONGESTION CONTROL TECHNIQUES

Congestion control refers to the techniques used to control or prevent congestion. Congestion control techniques can be broadly classified into two categories:



1. Open Loop Congestion Control

Open loop congestion control policies are applied to prevent congestion before it happens. The congestion control is handled either by the source or the destination.

Policies adopted by open loop congestion control

1. **Retransmission Policy :**
   It is the policy in which retransmission of the packets are taken care of. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. This transmission may increase the congestion in the network.
   To prevent congestion, retransmission timers must be designed to prevent congestion and also able to optimize efficiency.

2. **Window Policy :**
   The type of window at the sender's side may also affect the congestion. Several packets in the Go-back-n window are re-sent, although some packets may be received successfully at the receiver side. This duplication may increase the congestion in the network and make it worse.
   Therefore, Selective repeat window should be adopted as it sends the specific packet that may have been lost.

3. **Discarding Policy :**
   A good discarding policy adopted by the routers is that the routers may prevent congestion and at the same time partially discard the corrupted or less sensitive packages and also be able to maintain the quality of a message.
   In case of audio file transmission, routers can discard less sensitive packets to prevent congestion and also maintain the quality of the audio file.

4. **Acknowledgment Policy :**
   Since acknowledgements are also the part of the load in the network, the acknowledgment policy imposed by the receiver may also affect congestion. Several approaches can be used to prevent congestion related to acknowledgment.

The receiver should send acknowledgement for N packets rather than sending acknowledgement for a single packet. The receiver should send an acknowledgment only if it has to send a packet or a timer expires.

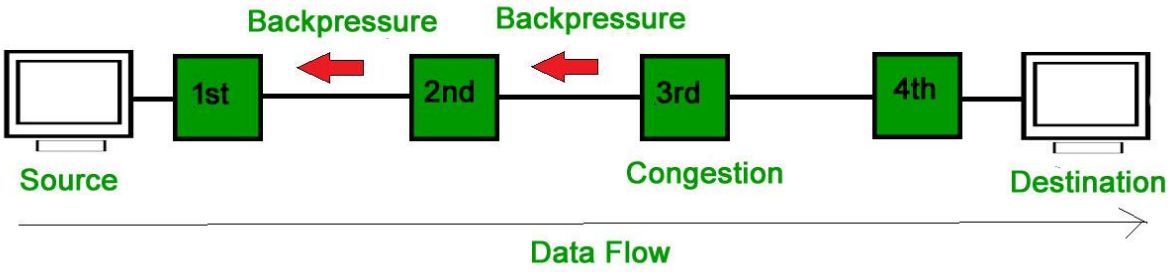
5. **Admission Policy :**
   In admission policy a mechanism should be used to prevent congestion. Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of a congestion or there is a congestion in the network, router should deny establishing a virtual network connection to prevent further congestion.

2. Closed Loop Congestion Control

Closed loop congestion control techniques are used remove congestion after it happens. Several techniques are used by different protocols; some of them are:

1. Backpressure :

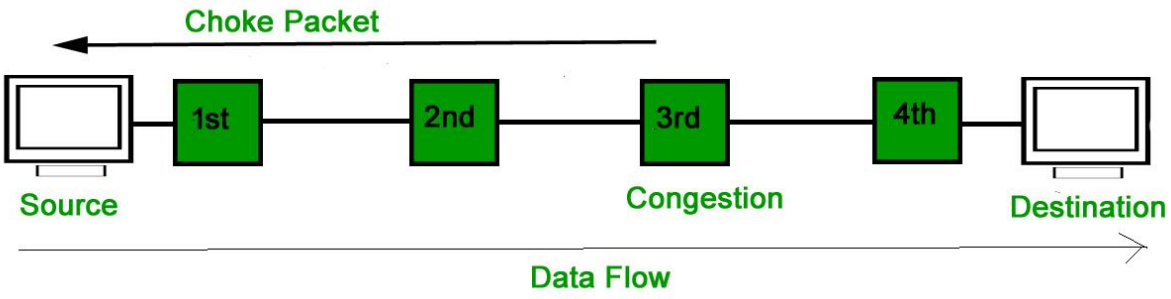
Backpressure is a technique in which a congested node stops receiving packets from upstream node. This may cause the upstream node or nodes to become congested and reject receiving data from above nodes. Backpressure is a node-to-node congestion control technique that propagate in the opposite direction of data flow. The backpressure technique can be applied only to virtual circuit where each node has information of its above upstream node.



In above diagram the 3rd node is congested and stops receiving packets as a result 2nd node may be get congested due to slowing down of the output data flow. Similarly 1st node may get congested and inform the source to slow down.

2. Choke Packet Technique :

Choke packet technique is applicable to both virtual networks as well as datagram subnets. A choke packet is a packet sent by a node to the source to inform it of congestion. Each router monitors its resources and the utilization at each of its output lines. Whenever the resource utilization exceeds the threshold value which is set by the administrator, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic. The intermediate nodes through which the packets has travelled are not warned about congestion.



3. Implicit Signalling :
In implicit signalling, there is no communication between the congested nodes and the source. The source guesses that there is congestion in a network. For example when sender sends several packets and there is no acknowledgment for a while, one assumption is that there is a congestion.

4. Explicit Signalling :
In explicit signalling, if a node experiences congestion it can explicitly sends a packet to the source or destination to inform about congestion. The difference between choke packet and explicit signalling is that the signal is included in the packets that carry data rather than creating a different packet as in case of choke packet technique.
Explicit signalling can occur in either forward or backward direction.

- **Forward Signalling :** In forward signalling, a signal is sent in the direction of the congestion. The destination is warned about congestion. The receiver in this case adopt policies to prevent further congestion.
- **Backward Signalling :** In backward signalling, a signal is sent in the opposite direction of the congestion. The source is warned about congestion and it needs to slow down.

THE NETWORK LAYER IN THE INTERNET

Definition:-

The internet is an interconnected collection of many networks.

Design Principles for Internet:-

1. Make sure it works.
2. Keep it simple.
3. Make clear choices.
4. Exploit modularity.
5. Expect heterogeneity.
6. Avoid static options and parameters.
7. Look for a good design, it need not be perfect.
8. Be strict when sending and tolerant when receiving.
9. Think about scalability
10. Consider performance and cost.

ADDRESSING

IP address can be specified by either binary notation and dotted notation.

In binary notation, address is displayed as 32 bits. Each octet is referred to as a byte.

Example: 01110101 10010101 00011101 00000010

In dotted notation, written in decimal form with a decimal point separating the bytes.

Example: 117.149.29.2

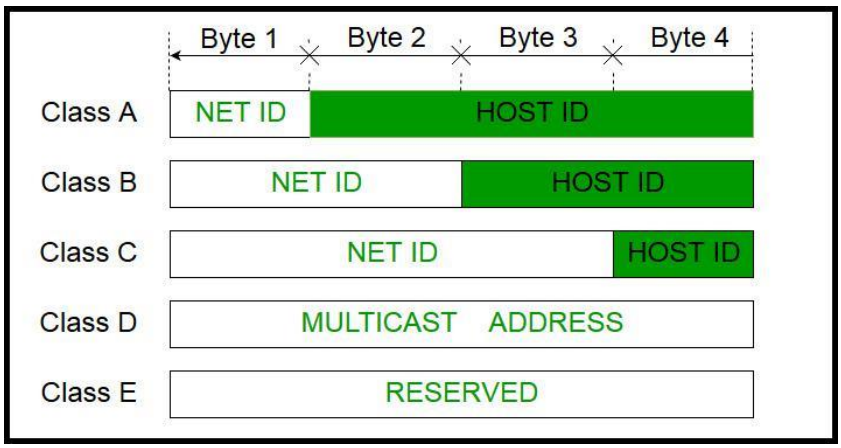
- Classful and classless addressing are methods used in networking to manage IP addresses.
- Classful addressing divides IP addresses into fixed classes (A, B, C, D, E), each with predefined ranges.
- In contrast, classless addressing, also known as CIDR (Classless Inter-Domain Routing), offers more flexibility by allowing addresses to be subdivided into smaller blocks called subnets. This flexibility helps optimize address allocation and supports the growth of the internet by efficiently managing IP address resources.

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 determines the classes of the IP address.

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 or network administrator assigns an IP address to each device that is connected to its network.



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.

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 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 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

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 – 255.255.255.255. This class doesn't have any subnet mask. The higher-order bits of the first octet of class E are always set to 1111.

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.

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.

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.

INTERNET PROTOCOL V4 (IPV4)

- Every router or node in the internet has an IP address that can be used in the source address and destination address fields of IP packets.
- IPV4 address is a 32-bit.
- IPV4 datagram consists of a header part and a body or payload part.
- The header has a 20-byte fixed part and a variable length optional part. The bits are transmitted from left to right and top to bottom.

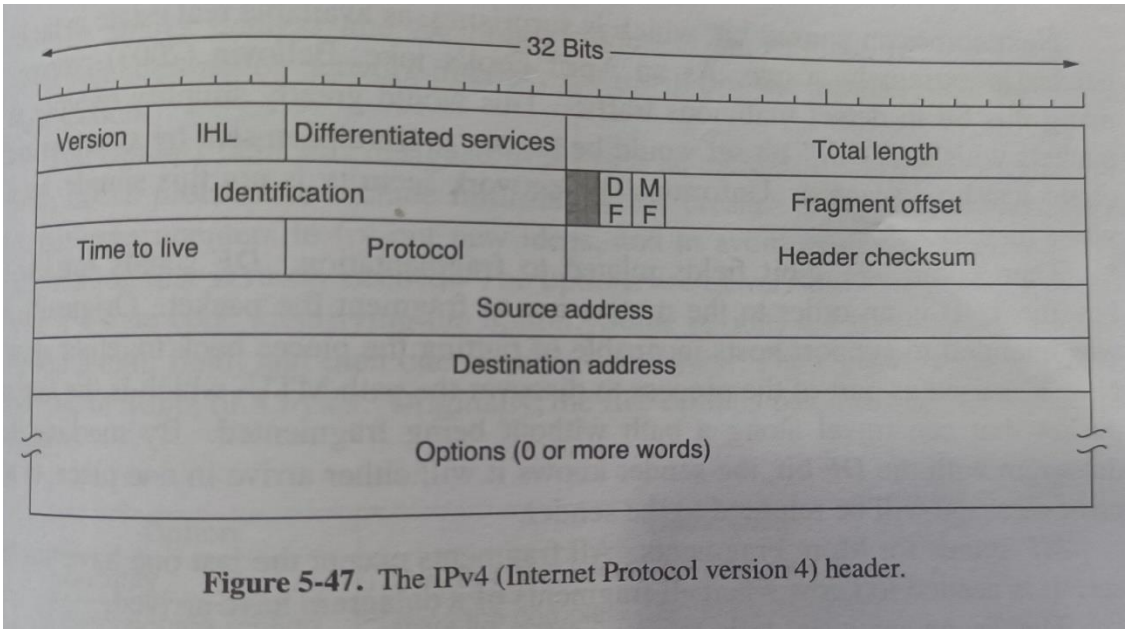


Figure 5-47. The IPv4 (Internet Protocol version 4) header.

- **Version (4 bits):** This field specifies the version of the IP protocol being used, which is IPv4 in this case.
- **Header Length (4 bits):** The header length field indicates the length of the IPv4 header in 32-bit words. Since the header is a fixed size of 20 bytes, the value of this field is typically 5.
- **Type of Service (8 bits):** This field is used to define the quality of service (QoS) for the packet, including priorities and other parameters for routing and processing.
- **Total Length (16 bits):** The total length field specifies the length of the entire IPv4 packet, including both the header and the data, in bytes.
- **Identification (16 bits):** The identification field is used for packet fragmentation and reassembly. It helps in grouping fragments of a larger packet together.
- **Flags (3 bits):** These bits are used for controlling and identifying packet fragmentation. The flags include the "Don't Fragment" (DF) and "More Fragments" (MF) flags.
- **Fragment Offset (13 bits):** The fragment offset field specifies the position of the fragment within the original packet. It is used to reassemble fragmented packets correctly.
- **Time to Live (TTL) (8 bits):** The TTL field represents the maximum number of hops (routers or network segments) that the packet can traverse before it is discarded. Each router decrements this value by one.
- **Protocol (8 bits):** This field indicates the type of protocol used in the data portion of the packet, such as TCP, UDP, ICMP, or others.

- **Header Checksum (16 bits):** The header checksum field is used to verify the integrity of the IPv4 header during transmission. Routers and devices recalculate this checksum to check for errors.
- **Source IP Address (32 bits):** This field contains the IP address of the sender or source of the packet.
- **Destination IP Address (32 bits):** This field holds the IP address of the recipient or destination of the packet.

Purpose of IPv4 Header Fields

- **Version and Header Length:** These fields identify the version of the IP protocol and the length of the header, respectively.
- **Type of Service:** The Type of Service field is used to classify packets based on their requirements, allowing for differentiated handling of various types of traffic.
- **Total Length:** This field specifies the overall length of the packet, ensuring that routers and devices can process it correctly.
- **Identification, Flags, and Fragment Offset:** These fields facilitate packet fragmentation and reassembly, crucial for handling large packets that cannot be transmitted in one piece.
- **TTL:** The Time to Live field prevents packets from circulating endlessly in the network by specifying a maximum number of hops they can take.
- **Protocol:** The Protocol field indicates the transport layer protocol used in the packet, enabling routers to forward the packet to the appropriate service.
- **Header Checksum:** This checksum verifies the integrity of the header, reducing the chances of forwarding corrupted packets.
- **Source and Destination IP Addresses:** These fields specify the source and destination of the packet, allowing routers to make routing decisions based on the destination address.

SUPERNETTING & SUBNETTING

A computer network is a group of devices linked together to share resources and data. Each network device has an id number known as an IP address. *Subnetting* and *Supernetting* are two methods for organizing IP addresses in a logical order based on the situation. Subnetting is the technique of separating a network into subnetworks, and supernetting combines small networks into an extensive network. Subnetting increases the bits in network addresses. On the other hand, supernetting increases the bits in host addresses. It is intended to make the routing process easier, decrease the routing table information size and require less RAM in the router. FLSM and VLSM methods are utilized in subnetting, and CIDR is utilized in supernetting.

SUBNETTING:-

Subnetting is a method of dividing a single physical network into numerous smaller logical sub-networks. These subnetworks are referred to as subnets. An IP address is formed by combining a network and host segments. A subnet is created by accepting bits from the IP address host part and is used to split the original network into smaller subnetworks.

The process of subnetting involves turning host bits into network bits. Its approach was originally intended to slow the depletion of IP addresses. It permits the administrator to split a single class A, class B, or class C network into smaller sections. ***VLSM (Variable Length Subnet Mask)*** divides IP address space into subnets of varying sizes while preventing memory waste. Furthermore, ***FLSM (Fixed Length Subnet Mask)*** occurs when the number of hosts in subnets is the same.

There are various advantages and disadvantages of Subnetting. Some main advantages and disadvantages of Subnetting are as follows:

Advantages

1. Subnetting reduces broadcast volume and hence reduces network traffic.
2. The permitted host numbers in the local area network are increased by subnetting.
3. Subnetworks are simple to handle and maintain.
4. The network security may easily be utilized amongst sub-networks instead of using it on the entire network.
5. It increases the flexibility of address.

Disadvantages

1. You require a qualified administrator to perform the subnetting process.
2. The subnetting process is quite expensive.

SUPERNETTING:-

Supernetting is the inverse of subnetting, in which many networks are combined into a single network. During supernetting, the mask bits are moved to the left of the default mask. It is sometimes referred to as router summarization and aggregation. It leads to the production of more addresses at the cost of network addresses, where network bits are essentially turned into host bits.

Supernetting is operated by ***internet service providers (ISPs)*** rather than regular users to ensure the best IP address distribution. ***Classless Inter-Domain Routing (CIDR)*** is a network routing method that is utilized to route network traffic over the internet. CIDR is a supernetting technology in which many subnets are joined for network routing. To put it another way, CIDR allows IP addresses to be organized in subnetworks regardless of their value.

There are various advantages and disadvantages of Supernetting. Some main advantages and disadvantages of Supernetting are as follows:

Advantages

1. The router memory table size is reduced by condensing numerous routing data entries into a single entry.
2. It also minimizes network traffic.
3. It also speeds up the lookup of routing tables.
4. It allows the router to isolate topology changes from other routers.

Disadvantages

1. The supernet's networks must all use the same IP address class.
2. The block combination should be constructed in power 2; if three blocks are required, then four blocks must be assigned.
3. The entire network should be in the same class.

NETWORK ADDRESS TRANSLATION

One public IP address is needed to access the Internet, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, a private IP address must be translated into a public IP address.

Network Address Translation (NAT) is a process in which one or more local IP addresses are translated into one or more Global IP addresses and vice versa to provide Internet access to the local hosts. It also does the translation of port numbers, i.e., masks the port number of the host with another port number in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on a router or firewall.

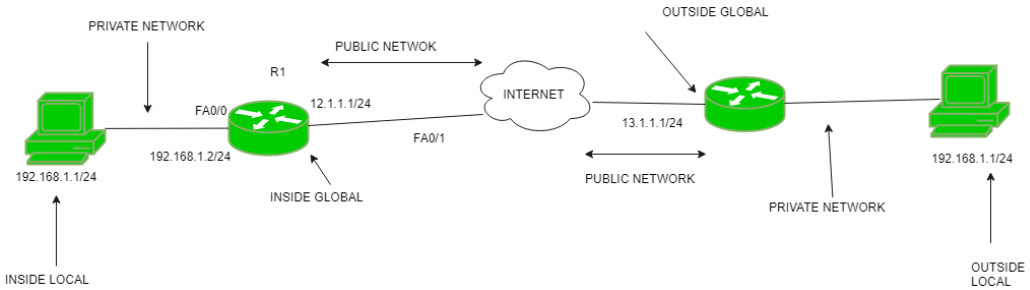
Working of Network Address Translation (NAT):-

Generally, the border router is configured for NAT i.e. the router which has one interface in the local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.

If NAT runs out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent.

NAT inside and outside addresses

Inside refers to the addresses which must be translated. Outside refers to the addresses which are not in control of an organization. These are the network Addresses in which the translation of the addresses will be done.



- **Inside local address –** An IP address that is assigned to a host on the Inside (local) network. The address is probably not an IP address assigned by the service provider i.e., these are private IP addresses. This is the inside host seen from the inside network.
- **Inside global address –** IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.
- **Outside local address –** This is the actual IP address of the destination host in the local network after translation.
- **Outside global address –** This is the outside host as seen from the outside network. It is the IP address of the outside destination host before translation.

Network Address Translation (NAT) Types

There are 3 ways to configure NAT:

Static NAT

In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global addresses. This is generally used for Web hosting. These are not used in organizations as there are many devices that will need Internet access and to provide Internet access, a public IP address is needed. Suppose, if there are 3000 devices that need access to the Internet, the organization has to buy 3000 public addresses that will be very costly.

Dynamic NAT

In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP addresses. If the IP address of the pool is not free, then the packet will be dropped as only a fixed number of private IP addresses can be translated to public addresses.

Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access the Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who want to access the Internet is fixed. This is also very costly as the organization has to buy many global IP addresses to make a pool.

Port Address Translation (PAT)

This is also known as NAT overload. In this, many local (private) IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

Advantages of NAT

- NAT conserves legally registered IP addresses.
- It provides privacy as the device's IP address, sending and receiving the traffic, will be hidden.
- Eliminates address renumbering when a network evolves.

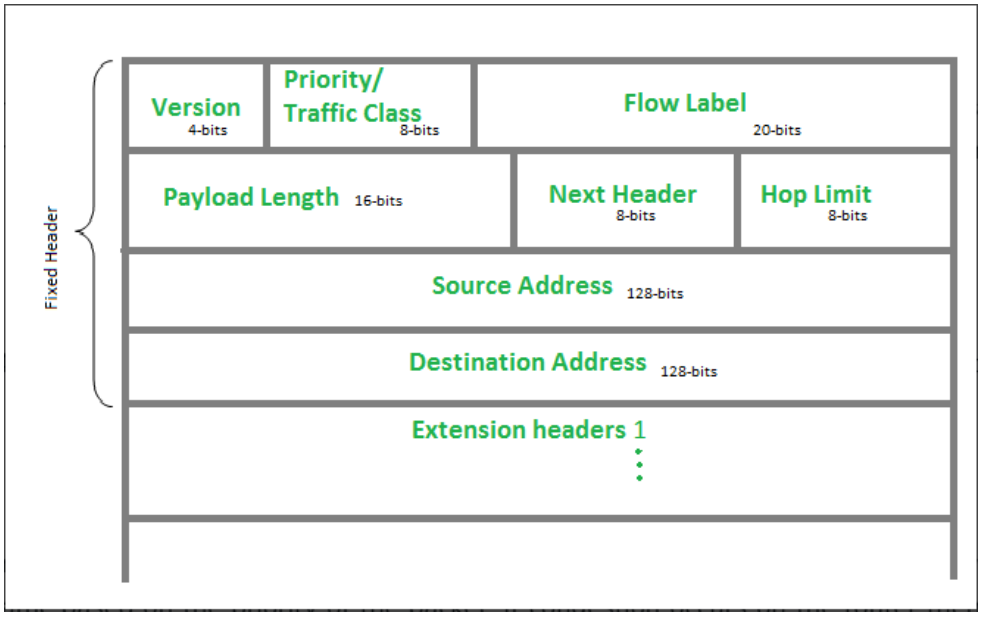
Disadvantage of NAT

- Translation results in switching path delays.
- Certain applications will not function while NAT is enabled.
- Complicates tunneling protocols such as IPsec.
- Also, the router being a network layer device, should not tamper with port numbers(transport layer) but it has to do so because of NAT.

INTERNET PROTOCOL V6 (IPV6)

The IPv6 header is a part of the data packet structure used in Internet Protocol version 6 (IPv6), which is the latest version of the Internet Protocol. IPv6 is designed to replace IPv4, offering a much larger address space and improved features. The header in IPv6 contains important information needed for routing and delivering packets across networks.

IPv6 Fixed Header



Version (4-bits)

The size of this field is 4-bit. Indicates the version of the Internet Protocol, which is always 6 for IPv6, so the bit sequence is 0110.

Traffic Class(8-bit)

The Traffic Class field indicates class or priority of IPv6 packet which is similar to *Service Field* in IPv4 packet. It helps routers to handle the traffic based on the priority of the packet. If congestion occurs on the router then packets with the least priority will be discarded. As of now, only 4-bits are being used (and the remaining bits are under research), in which 0 to 7 are assigned to congestion controllled traffic and 8 to 15 are assigned to Uncontrolled traffic.

Priority assignment of Congestion controlled traffic :

Priority	Meaning
0	No Specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

Uncontrolled data traffic is mainly used for Audio/Video data. So we give higher priority to Uncontrolled data traffic. The source node is allowed to set the priorities but on the way, routers can change it. Therefore, the destination should not expect the same priority which was set by the source node.

Flow Label (20-bits)

Flow Label field is used by a source to label the packets belonging to the same flow in order to request special handling by intermediate IPv6 routers, such as non-default quality-of-service or real-time service. In order to distinguish the flow, an intermediate router can use the source address, a destination address, and flow label of the packets. Between a source and destination, multiple flows may exist because many processes might be running at the same time. Routers or Host that does not support the functionality of flow label field and for default router handling, flow label field is set to 0. While setting up the flow label, the source is also supposed to specify the lifetime of the flow.

Payload Length (16-bits)

It is a 16-bit (unsigned integer) field, indicates the total size of the payload which tells routers about the amount of information a particular packet contains in its payload. The payload Length field includes extension headers(if any) and an upper-layer packet. In case the length of the payload is greater than 65,535 bytes (payload up to 65,535 bytes can be indicated with 16-bits), then the payload length field will be set to 0 and the jumbo payload option is used in the Hop-by-Hop options extension header.

Next Header (8-bits)

Next Header indicates the type of extension header(if present) immediately following the IPv6 header. Whereas In some cases it indicates the protocols contained within upper-layer packets, such as TCP, UDP.

Hop Limit (8-bits)

Hop Limit field is the same as TTL in IPv4 packets. It indicates the maximum number of intermediate nodes IPv6 packet is allowed to travel. Its value gets decremented by one, by each

node that forwards the packet and the packet is discarded if the value decrements to 0. This is used to discard the packets that are stuck in an infinite loop because of some routing error.

Source Address (128-bits)

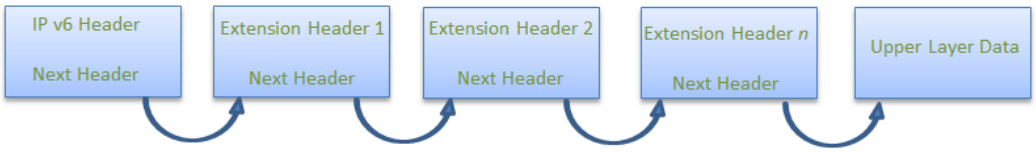
Source Address is the 128-bit IPv6 address of the original source of the packet.

Destination Address (128-bits)

The destination Address field indicates the IPv6 address of the final destination(in most cases). All the intermediate nodes can use this information in order to correctly route the packet.

Extension Headers

In order to rectify the limitations of the *IPv4 Option Field*, Extension Headers are introduced in IP version 6. The extension header mechanism is a very important part of the IPv6 architecture. The next Header field of IPv6 fixed header points to the first Extension Header and this first extension header points to the second extension header and so on.

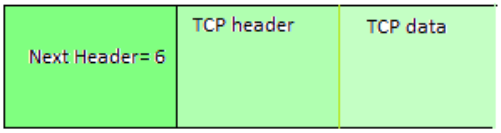


Types of Extension Header

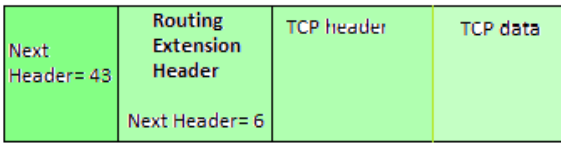
IPv6 packet may contain zero, one or more extension headers but these should be present in their recommended order:

Order	Header Type	Next Header Code
1	Basic IPv6 Header	-
2	Hop-by-Hop Options	0
3	Destination Options (with Routing Options)	60
4	Routing Header	43
5	Fragment Header	44
6	Authentication Header	51
7	Encapsulation Security Payload Header	50
8	Destination Options	60
9	Mobility Header	135
	No next header	59
Upper Layer	TCP	6
Upper Layer	UDP	17
Upper Layer	ICMPv6	58

Example: *TCP is used in IPv6 packet*



Example2:



Rule: Hop-by-Hop options header(if present) should always be placed after the IPv6 base header.

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.
Packet flow 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.