Network layer

The network layer is at the level-3 of the OSI reference model. It responses to the services request of the transport layer and is responsible for N to N i.e. source to destination packet delivery by taking up efficient path through the network for data transmission.It also manages options pertaining to host and network addressing, managing sub-networks, and internetworking.

Network layer takes the responsibility for routing packets from source to destination within or outside a subnet. Two different subnet may have different addressing schemes or non-compatible addressing types. Same with protocols, two different subnet may be operating on different protocols which are not compatible with each other. Network layer has the responsibility to route the packets from source to destination, mapping different addressing schemes and protocols.

Devices which work on Network Layer mainly focus on routing. Routing may include various tasks aimed to achieve a single goal. These can be:

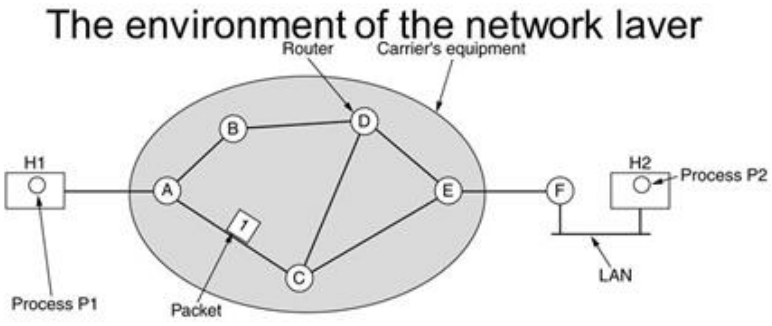
- Addressing devices and networks.
- Populating routing tables or static routes.
- Queuing incoming and outgoing data and then forwarding them according to quality of service constraints set for those packets.
- Internetworking between two different subnets.
- Delivering packets to destination with best efforts.
- Provides connection oriented and connection less mechanism.

❖ Network layer design issues

1. Stores and forward packet switching.
2. Services provided to transport layer.
3. Implementing connectionless service.
4. Connections oriented service.

1. Store and forward packet switching:

In the network layer, major task carried out is routing of packets from one router to another. I.e. the major components of the system are the carriersequipment's are used as follows.A host transmits a packet to the nearest router either on its own LAN or over a point to point link to the carrier. When this packet is received by the next checksum is verified then it is forwarded to the next router along with the path until it reaches the designation host. This mechanism is called store andforwardpacket switching.



2. Service provided to transport layer:

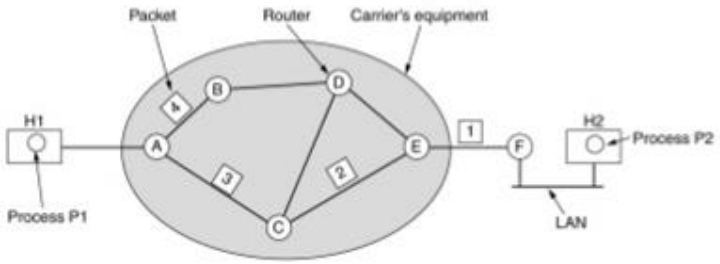
The network layer provides different services to the transport layer. These services have been designed with the following concepts:-

- The services should be independent of the router technology.
- The transport layer should be shielded from the number, type and topology of the router present in the network.
- The network addresses made available to the transport layer should be a uniform numbering format for any type of network.

3. Implementing connectionless services:

In connectionless service the packets are released individually in the subnet and routed independently so that each packet's routing decisions are not dependent on each other. The data packets here are called as data grams and thesubnet is called datagram subnet.

Implementation of Connectionless Service

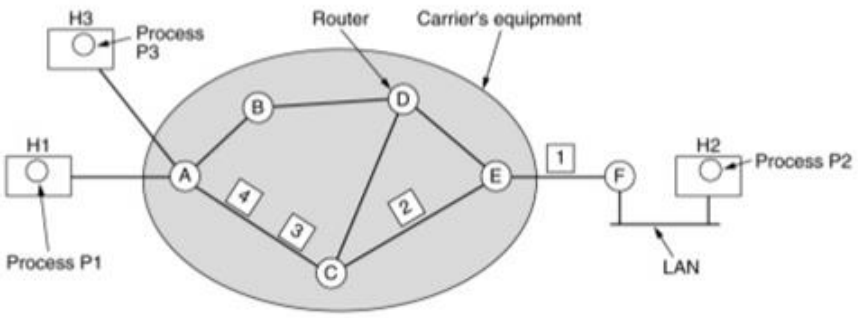


4. Connection oriented service:

The connection oriented service needs to form a virtual circuit subnet. The virtual circuit follows the following rules:-

- First a connection is required to be established.
- After establishment of a connection a route from the source machine to designation machine is chosen and stored in the tables inside the routers.
- The data packets are transmitted only along the path set by the virtual circuit.
- After the transmission, all the packets the connection is released and the virtual circuit is terminated.

Implementation of Connection-Oriented Service



Comparison of Virtual-Circuit and Datagram Subnet

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

Routing Algorithms

The routing algorithm is a part of network layer software which is responsible for deciding the output line for every incoming data packet for its transmission through the network. If the network uses datagram, routing decisions are made for every new packet. These packets when arrived at the routers make the routing decision by looking up the number of outgoing lines from the router and by looking at the information in the routing table. This process is called as **forwarding.**

If the network uses virtual circuit, routing decisions are made only when a new virtual circuit is been established. All the data packets follow this established route. This process is called as sessions routing.

There are basically two categories of routing algorithms:

1. Adaptive routing algorithms.
2. Non-adaptive routing algorithms.

1. Adaptive routing algorithms:

In this type of routing,decisions are taken for each packet separately. I.e. routing decisions reflect to the changes in the topology and the traffic in the network. The router may select a new route for each packet. It is also called as Dynamic routing algorithm.

2. Non-adaptive routing algorithm:

In this routing, routing decisions are not taken again and a route for destination it sends all the packets to the destination by the same route. If there is some problem in the n/w links of the route, the transmission is terminated. Here the routing decisions are not based on the conditions or the topology of the n/w. It is also called as static routing algorithm.

Properties of routing algorithm :

1. Correctness
2. Simplicity
3. Robustness
4. Stability
5. Fairness
6. Optimality

Optimality Principal:

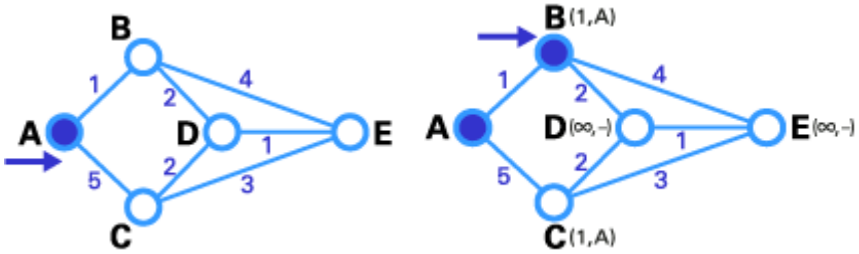
Before going to any specific algorithm of routing it is necessary to understand the general statement about optimal routes without regards to the n/w topology or traffic in the n/w. This statement is called as optimality principal. It states that there exists at least route from one node to ant other node in the same n/w and if a router A and if a router B is on the optimal path from A to router C then the optimal path from B to C also lies along the same route.

Shortest Path Routing Algorithm:

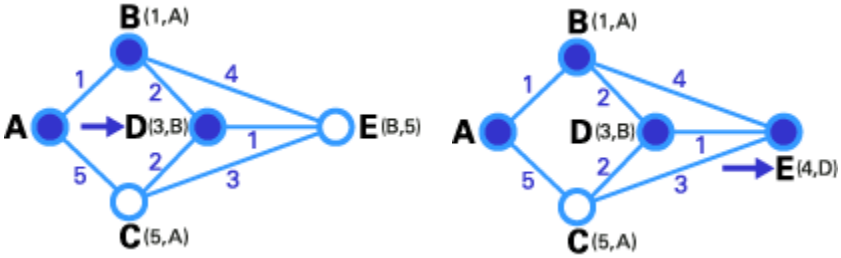
It is simple and easy technique of routing. The basic idea of this technique to built a graph of the subnet with each node of the graph representing a router and each arc of the graph representing a communication link. This technique finds the shortest paths b/w the nodes in the graph. The length of the path can be measured in a number of ways, such as number of hops in the link or on he basis of geographical distance etc.

There are various algorithms for computing the shortest path between two nodes on the graph one of the most used algorithm is Dijkstra (Single source algorithm). In this routing algorithm, one initial node is first marked as the source node (T-node). Then it find all the neighbors of the T-node and node with the shortest distance is marked thenthe node with the 2nd shortest distance from the source node T-nodeis marked and so on. In this way shortest distance to each node in the n/w form single source node is found.

Example:Dijkstra Algorithm



Step 1 Step 2



Step 4
Step 3

Here we want to find the best route between A and E. (You can see that there are six possible routes between A and E (ABE, ACE, ABDE, ACDE, ABDCE, ACDBE), and it's obvious that ABDE is the best route because its weight is the lowest. But life is not always so easy, and there are some complicated cases in which we have to use algorithms to find the best route.

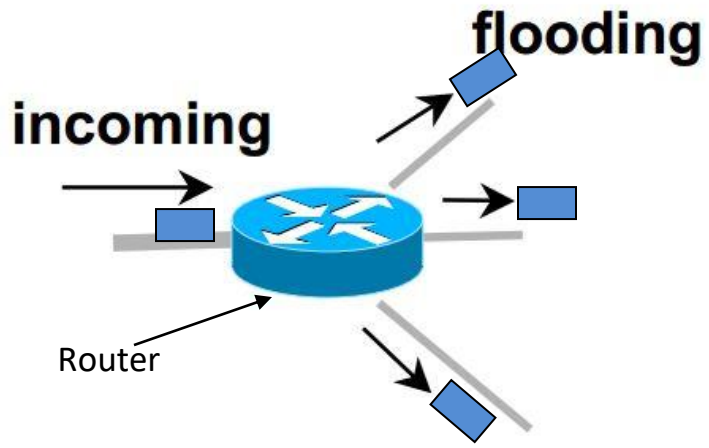
1. As you see in the first image, the source node (A) has been chosen as T-node, and so its label is permanent (we show permanent nodes with filled circles and T-nodes with the --> symbol).
2. In the next step, you see that the status record set of tentative nodes directly linked to T-node (B, C) has been changed. Also, since B has less weight, it has been chosen as T-node and its label has changed to permanent (see below).
3. In step 3, like in step 2, the status record set of tentative nodes that have a direct link to T-node (D, E), has been changed. Also, since D has less weight, it has been chosen as T-node and its label has changed to permanent.
4. In step 4, we don't have any tentative nodes, so we just identify the next T-node. Since E has the least weight, it has been chosen as T-node.

Lastly, E is the destination, so we stop here.

Flooding:

In this technique every incoming packets is sent out on every outgoing path from that node except the one from where it is arrived. Flooding generates vast number of duplicate packets until some measures are taken to avoid this process. One such measure to avoid receiving of duplicate packets at the destination is identifying each packet with a sequence number. So that the destination can distinguish between duplicate packets, and if the packet is reached to the destination it can easily terminate other duplicate packets. The technique of flooding is also called as broadcast routing or multidestination routing.

Another variation in flooding is **selectiveflooding**. In this algorithm, the flooding technique is carried out only by those routers who are sure about reaching to destination

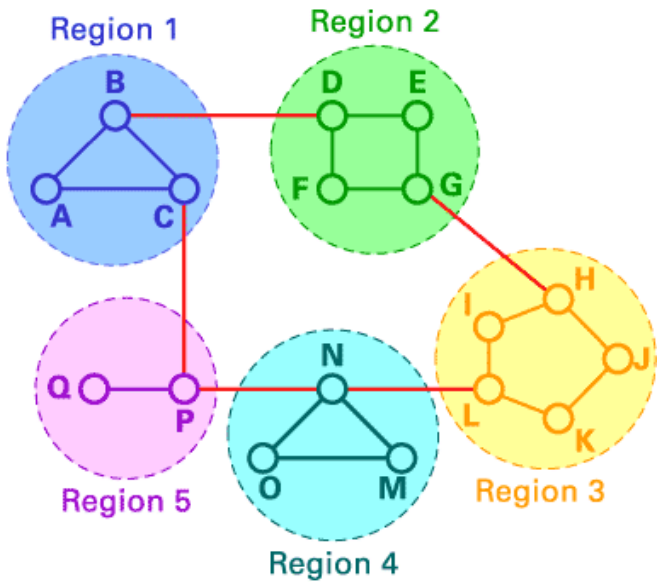


Hierarchical routing:

Because of the global nature of Internet system, it becomes more difficult to centralize the system management and operation. For this reason, the system must be hierarchical such that

it is organized into multiple levels with several group loops connected with one another at each level. Therefore, hierarchical routing is commonly used for such a system.

This technique is used for very vast networks. Here the routers in the n/w are grouped into **regions** then these regions are again grouped into **clusters** and the clusters into **zones**. Here each region will have the information of only those routers which are included into it and theclusters have the information of only those regions which are included in it and so on. If the data packet is transmitted, first it will be routed to the proper zone which consists of destination. Once it is reached to the zone it is directed to the proper region instead of wasting time for searching of the destination in other regions. From here the packet is transmitted to the proper router and then to the destination.



Example:

Consider a subnet with 720 routers, if there is no hierarchy each router has to maintain 720 routing tables. To avoid these, the subnet can be divided into 24 regions of 30 routers each. By this the router needs to have the information of only the 30 local routers and 23 region into the routing table i.e each router will have only 53 entries.

Link State routing:

Link-state routing protocols are one of the two main classes of routing protocols used in packet switching networks for computer communications. Examples of link-state routing protocols include open shortest path first (OSPF) and intermediate system to intermediate system (IS-IS).The link-state protocol is performed by every switching node in the network.

The basic concept of link-state routing is that every node constructs a map of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes. Each node then independently calculates the next best logical path from it to every possible destination in the network. The collection of best paths will then form the node's routing table.

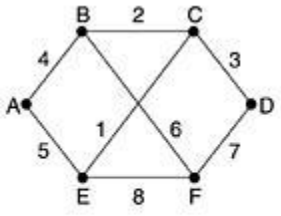
Link state routing can be stated as five part :

1. ***Discover its neighbors and learn their network addresses :*** When the router is booted, its first task is to learn who its neighbors are. It accomplishes this goal by

sending a special HELLO packet on each point to point line. The router on the other end is expected to send back a reply telling who it is.

2. ***Measure the delay or cost to each of its neighbors :*** The link state router requires each router to know, or at least have a reasonable estimate of, the delay to each of its neighbors. ECHO packet that the other side is required to send back immediately. By measuring the round-trip time and dividing it by two, the sending router can get the estimate of the delay.
3. ***Construct a packet telling all it has just learned :***here each router has to build a packet containing all data like identity of the sender, sequence number, age and list of neighbors.
4. ***Send this packet to all other routers :***In this part the link state packets are flooded to allover the network. To keep the flood check, each packet contains a sequence number that is incremented for each new packet sent.
5. ***Compute the shortest path to every other router :***Once a router has accumulated a full set of link state packets, it can construct the entire subnet graph because every link is represented. Shortest path routing algorithm can be run locally to construct the shortest path to all possible destinations.

This contrasts with distance-vector routing protocols, which work by having each node share its routing table with its neighbors. In a link-state protocol the only information passed between nodes is connectivity related.



(a)

Link State Packets

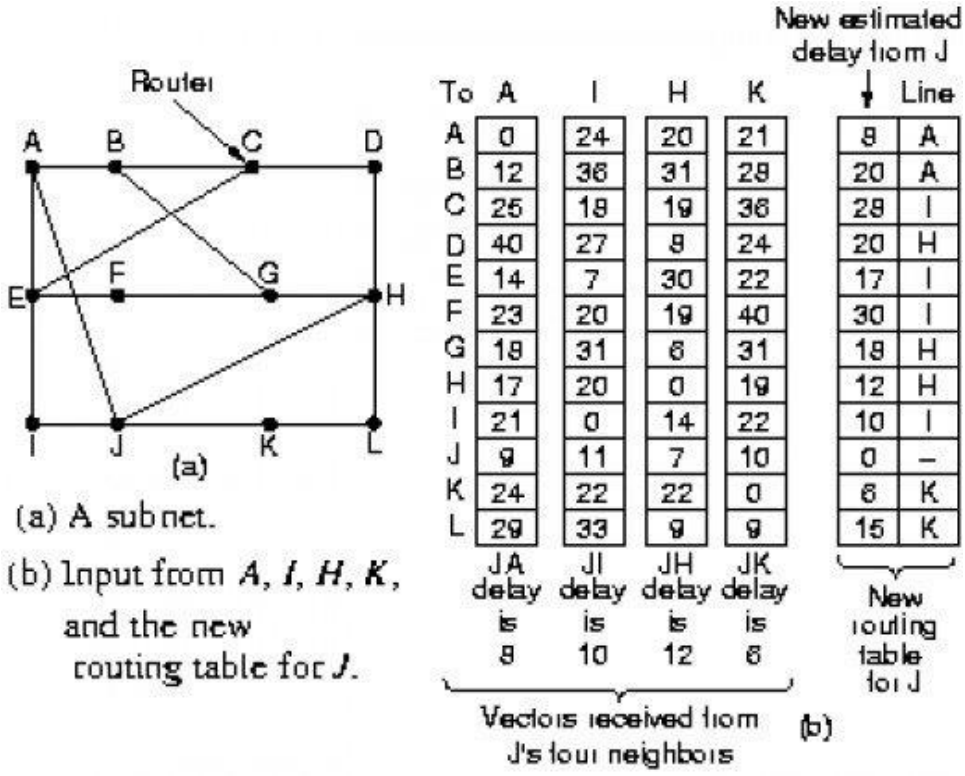
A	B	C	D	E	F
Seq.	Seq.	Seq.	Seq.	Seq.	Seq.
Age	Age	Age	Age	Age	Age
B 4	A 4	B 2	C 3	A 5	B 6
E 5	C 2	D 3	F 7	C 1	D 7
	F 6	E 1		F 8	E 8

(b)

Distance Vector routing :

Distance Vector is simple routing protocol which takes routing decision on the number of hops between source and destination. A route with less number of hops is considered as the best route. Every router advertises its set best routes to other routers. Ultimately, all routers build up their network topology based on the advertisements of their peer routers.

Distance vector routing algorithms operate by having each router maintain a table giving the best known distance to each destination and which line to use to get there. These tables are updated by exchanging information with the neighbours containing one entry for each router in the subnet. This entry contains two parts: the preferred outgoing line to use for that destination and an estimate of the time or distance to that destination. The metric might use number of hops, time delay in milliseconds, total number of packets queued along the path, or something similar.

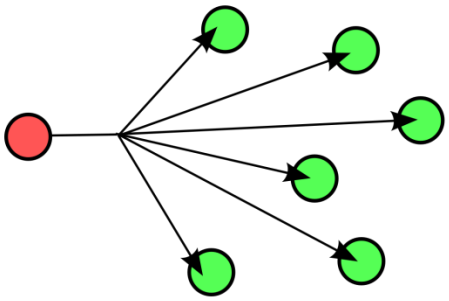


Broadcast Routing Algorithm:

Sending a data packet to all the destinations simultaneously throughout the n/w is called as broadcasting. There are various methods to implement this technique.

- **Broadcast routing:**

  In this method, the source creates andsends distinct data packets to all the destinations in the n/w. this method come across many disadvantages like wastage of bandwidth and it also requires the source to have a complete list of all destination.

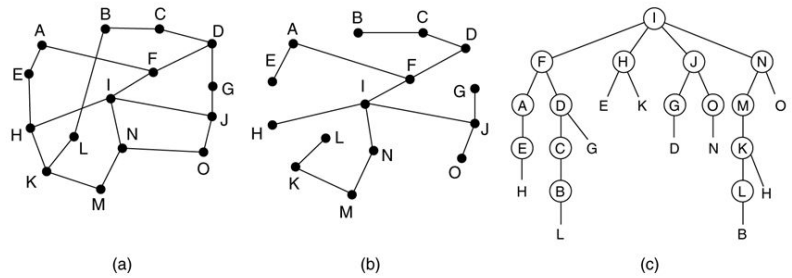


- **Flooding:** --explained above--
- **Multidestination routing:**

  In this algorithm the data packet is sent through multiple selected destination and not to all the node in the n/w. Here each packet contains list of destinations. When a packet arrives at a router, the router checks the list and selects the output line.Multicast routing is special case of broadcast routing with significance difference and challenges. In broadcast routing, packets are sent to all nodes even if they do not want it. But in Multicast routing, the data is sent to only nodes which wants to receive the packets.

- **Reverse path forwarding:**

  In this algorithm an attempt to approximate the behaviour of the previous one is done. Here even if the routers do not have information about the topology, it forwards the data packet by analysing the behaviour of the data packet in the previous path.Reverse path forwarding is a technique, in which router knows in advance about its predecessor from where it should receive broadcast. This technique is used to detect and discard duplicates.



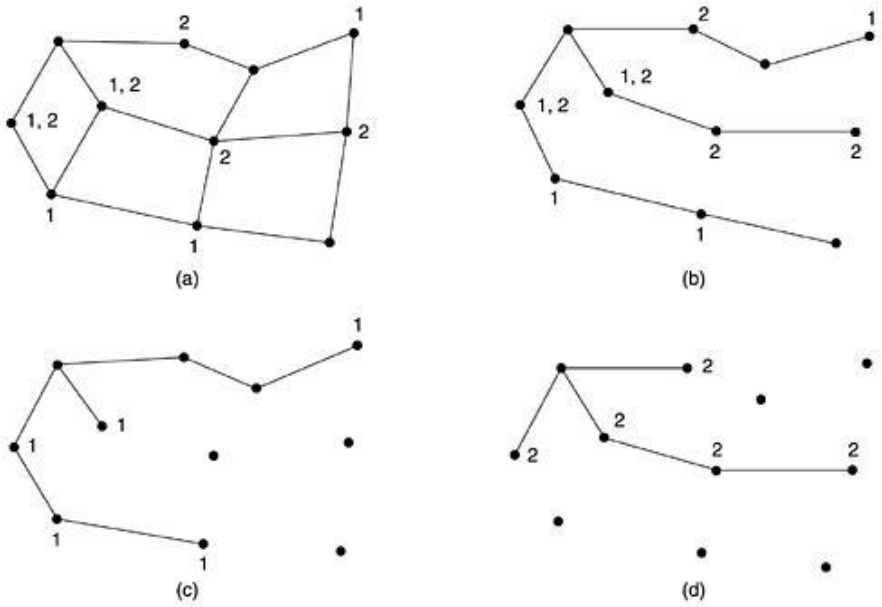
Reverse path forwarding. (a) A subnet. (b) a Sink tree. (c) The tree built by reverse path forwarding.

Multicast Routing:

Sending a message or data packet to specific group of nodes in the n/w is called as multicast routing.

Multicasting requires group management. Some way is needed to create and destroy groups, and it also allows processes for a member to join or leave the group. These tasks are accomplished without the concern of routing algorithm. Here it is very important that the routers should know which of their host belong to which group. Either the host must inform their routers about the changes or the router must query their host periodically. To perform multicast routing each router computes a spanning tree of the n/w covering all the routers.

Example:



In this algorithm when a process sends a multicast packet to a group the first router examines its spanning tree, removing all the lines that do not lead to any member of the groups. And then the broadcasting takes place only within the group with which the data packet is addressed.

Congestion

Congestion is a situation that occur when the number of packets being transmitted through the network approaches the packet handling capacity of the network i.e. when the number of packets are dumped into the subnet by a host, if the number of packet is within the carrying capacity of the channel, all the packets will be delivered to the destination but if the n/w gets overloaded it leads to congestion in the n/w and starts dropping the packets.

Reasons for congestion:

- Sudden arrival of packets on a particular output lines by a multiple input lines. Here the memory of the router becomes inefficient and the packets are dropped.
- Slow processor can also cause congestion.
- Low bandwidth channel can also cause congestions.

General Principle of Congestion Control:

The congestion problem in the n/w leads to loss of data packets like routing algorithms, several algorithms should be implemented so that this situation can be controlled. The congestion control algorithms are classified into two major categories.

1) **Open loop:**

Open loop solution attempt to solve the problem by taking good decisions at the initial stage, it ensures that the congestion does not occur in the n/w.

- Admission control.
- Resource reservation.
- Retransmission policy.
- Window policy.
- Acknowledgement policy.
- Discarding policy, etc.

2) **Close loop:**

In contrast close loop solutions are based on the concept of feedback. Close loop algorithm follows a dynamic approach i.e. it reacts during the congestion occurrence period according to the situation. The congestion control is managed by observation of queue length, number of retransmitted packets, routers memory, and average packet delay.

- Back pressure
- Choke packet
- Implicit signalling
- Explicit signalling

Techniques under open loop forcongestion control:

1. **Admission control technique:**

This is the widely used technique in virtual circuit n/w. Once congestion has occurred, no more virtual circuit are been setup. This is very similar to a telephone system in which there are no dial tones in the case the source gets overloaded. A source specifies its traffic flow indicating a set of parameters called as traffic descriptors, which includes peak rate, average rate and maximum traffic burst size. Based on the characteristics of traffic flow admission control mechanism reserves the bandwidth channel for transmission.

2. **Retransmission Policy :**

If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. Retransmission in general may increase congestion in the network. However, a good retransmission policy can prevent congestion. The retransmission policy and the

retransmission timer must be designed to optimize efficiency and at the same time prevent congestion. For example, the retransmission policy used by TCP is designed to prevent congestion.

3. **Window Policy :**

The type of window at the sender may also affect congestion. The Selective Repeat window is better than the Go-Back-N window for congestion control.

4. **Acknowledgment Policy :**

The acknowledgment policy imposed by the receiver may also affect congestion. A receiver may decide to acknowledge only N packets at a time. We need to know that the acknowledgments are also part of the load in a network. Sending less number of acknowledgments means imposing less load on the network.

5. **Discarding Policy :**

A good discarding policy by the routers may prevent congestion.

6. **Resource Reservation :**

Once we have a specific route for a flow, it becomes possible to reserve resources along that route to make sure the needed capacity is available. Three different kinds of resources can potentially be reserved are

- Bandwidth
- Buffer space
- CPU cycle

Techniques under closed loop for congestion control :

1. **Backpressure :**

The technique of backpressure refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node. This may cause the upstream node to become congested, and they in turn reject data from their upstream nodes. And so on . Back pressure is a node-to-node congestion control that starts with a node and propogates, in the opposite direction of data flow, to the source.

2. **Choke Packet :**

A choke packet is a packet sent by a node to the source to inform it of congestion. In this method, the warning is from the router, which has encountered congestion, to the source station directly. The intermediate nodes through which the packet has travelled are not warned.

3. **Implicit Signalling :**

In implicit signalling, there is no communication between the congested node and the source. The source guesses that there is a congestion somewhere in the network from other symptoms.

4. **Explicit Signalling :**

The node that experiences congestion can explicitly send a signal to the source or destination. ***Backward Signalling***A bit can be set in a packet moving in the direction opposite to the congestion. This bit can warn the source that there is congestion. ***Forward Signalling*** A bit

can be set in a packet moving in the direction of the congestion. This can warn the destination that there is congestion.

Congestion Control in Virtual-Circuit Subnets

1. One technique that is widely used to keep congestion that has already started from getting worse is admission control. The idea is simple, once congestion has been signed, no more virtual circuits are set up until the problem has gone away. Thus, attempts to setup new transport layer connection fail.
2. An alternative approach is to allow new virtual circuits but carefully route all new virtual circuits around problem areas.
3. Another strategy relating to virtual circuits is to negotiate an agreement between the host and subnet when a virtual circuit is setup by resource reservation. This agreement normally specifies the volume and shape of the traffic, qualityof service required and other parameters.

Congestion Control in Datagram Subnets

Each router can easily monitor the utilization of its output lines and other resources. Each newly-arriving packet is checked to see if its output line is in warning state. If it is, some action is taken. The action can be one of the several following alternatives:

1. **The Warning Bit :**

   The architecture signalled the warning state by setting a special bit in the packets header. When the packet arrived at its destination, the transport entity copied the bit into the next acknowledgement sent back to the source. The source then cut back on traffic.

   As long as the router was in the warning state, it continued to set the warning bit, which meant that the source continued to get acknowledgements with it set. The source monitored the fraction of acknowledgements with the bit set and adjusted its transmission rate accordingly. As long as the warning bits continued to flow in, the source continued to decrease its transmission rate. When they slowed to a trickle, it increased its transmission rate. Note that since every router along the path could set the warning bit, traffic increased only when no router was in trouble.

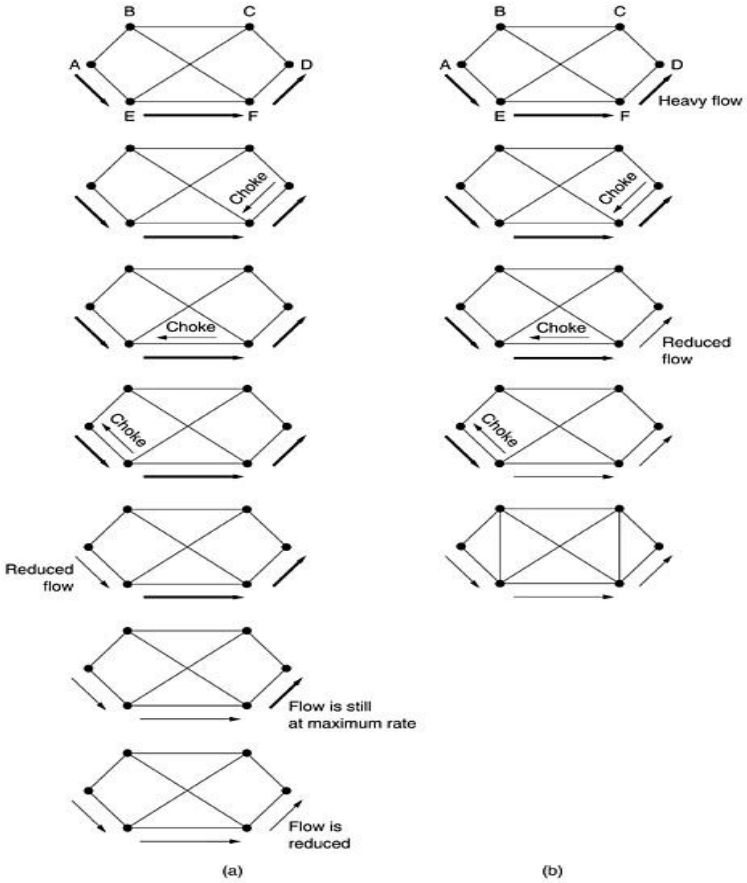
2. **Choke Packets :**

   In this approach, the router sends a **choke packet** back to the source host, giving it the destination found in the packet. The original packet is tagged so that it will not generate any more choke packet farther along the path and is then forwarded in the usual way.

   When the source host gets the choke packet, it is required to reduce the traffic sent to the specified destination by *X*percent. Since other packets aimed at the same destination are probably already under way and will generate yet more choke packets, the host should ignore choke packets referring to that destination for a fixed time interval. After that period has expired, the host listens for more choke packets for another interval. If one arrives, the line is still congested, so the host reduces the flow still more and begins ignoring choke packets again. If no choke packets arrive during the listening period, the host may increase the flow again. The feedback implicit in this protocol can prevent congestion.

3. Hop-by Hop Choke Packet :

An alternative approach is to have the choke packet take effect at every hop it passes through. Here as soon as the choke packet reaches F, F requires to reduce the flow to D. Doing so will require F to devote more buffers to the flow, since the source is still sending away at full blast, but it gives D immediate relief. In the next step, the choke packet reaches E, which tells E to reduce the flow to F. This action puts a greater demand on E's buffers but gives F immediate relief. Finally, the choke packet reaches A and the flow genuinely slows down.



4. Load Shedding :

Load shedding is a fancy way of saying that when routers are being inundated by packets that they cannot handle, they just throw them away. This is done to save the entire grid from collapsing.

It is well known that dealing with congestion after it is first detected is more effective than letting it gum up the works and then trying to deal with it. This observation leads to the idea of discarding packets before all the buffer space is really exhausted. A popular algorithm for doing this is called **RED (Random Early Detection)**.

5. Jitter Control :

For applications such as audio and video streaming, it does not matter much if the packet take 20 msec or 30 msec to be delivered, as long as the transit time is constant. The variation in the packet arrival times is called **jitter**.

The jitter can be bounded by computing the expected transit time for each hop along the path. When a packet arrives at a router, the router checks to see how much the packet is behind or ahead of its schedule. This information is stored in the packet and updated at each hop. If the packet is ahead of schedule, it is held just long enough to get it back on schedule. If it is behind schedule, the router tries to get it out the door quickly.

Traffic policing and implementation:

Traffic policing is a process of monitoring enforcing the traffic flow of packets during the connection period. Most implementations of traffic policing are done by a technique called token bucket algorithm. In this algorithm the bucket is considered as the n/w and traffic flow is considered as water being poured into bucket.

The following assumptions are made with this algorithm.

- The bucket has certain depth to hold water just like that a n/w can accept a certain number of packets.
- The bucket leaks at a certain rate no matter at what rate water enters the bucket. In the similar way in the n/w no matter at what rate the packet arrives at the input lines of a router, the outgoing link has a fixed rate of transmission.
- If the bucket does not overflow when the water is poured into it, then the bucket of water is set to be conforming. Similarly in the n/w, if the traffic is within the control all the packets will be transmitted easily.
- The bucket will spillover if it is full and if additional water is poured into it. Similarly in n/w if it gets more packets it will lead to congestion and the additional packets will be lost.

If it is expected that the traffic flow should be very smooth then the bucket has to be of a shallow type i.e. if the flow of data is more bursty in nature the bucket should be more deeper.

2) Traffic shaping and implementation:

Traffic shaping is the process of altering the traffic flow.

Example :

Consider an example where a host is generating data at 24kpbs. It can be transmitted in the n/w by several ways

- The same data can be transmitted at the rate of 75kbps for 0.4sec.
- This same data again can be transmitted at the rate of 100kbps for 0.3 seconds.
- There are the possible traffic patterns at the average rate of 25kbps.

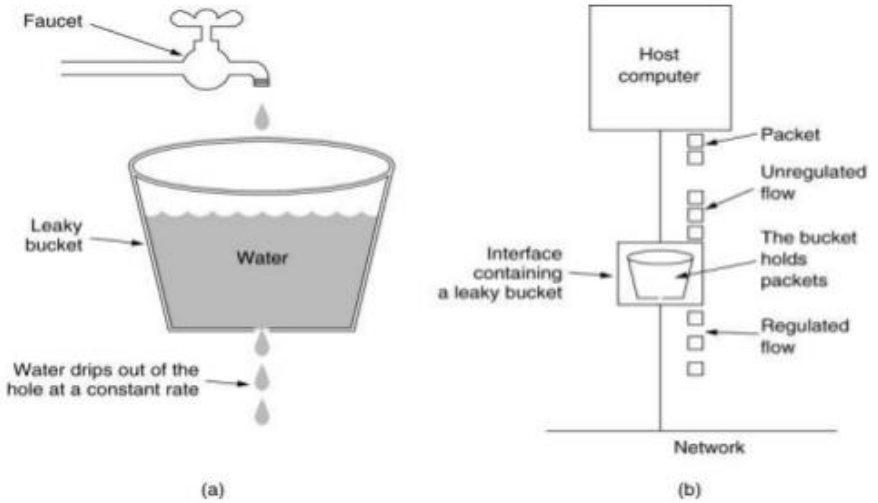
There are another two mechanisms of traffic shaping are:

- Leaky bucket traffic shaper
- Token bucket traffic shaper

Leaky bucket traffic shaper:

It is very simple mechanism in which the data packets are stored in buffers and are passed at constant interval to smoothen the traffic. This size of the buffer defines the maximum brust that can be accommodated.

The Leaky Bucket Algorithm



(a) A leaky bucket with water. (b) a leaky bucket with packets.

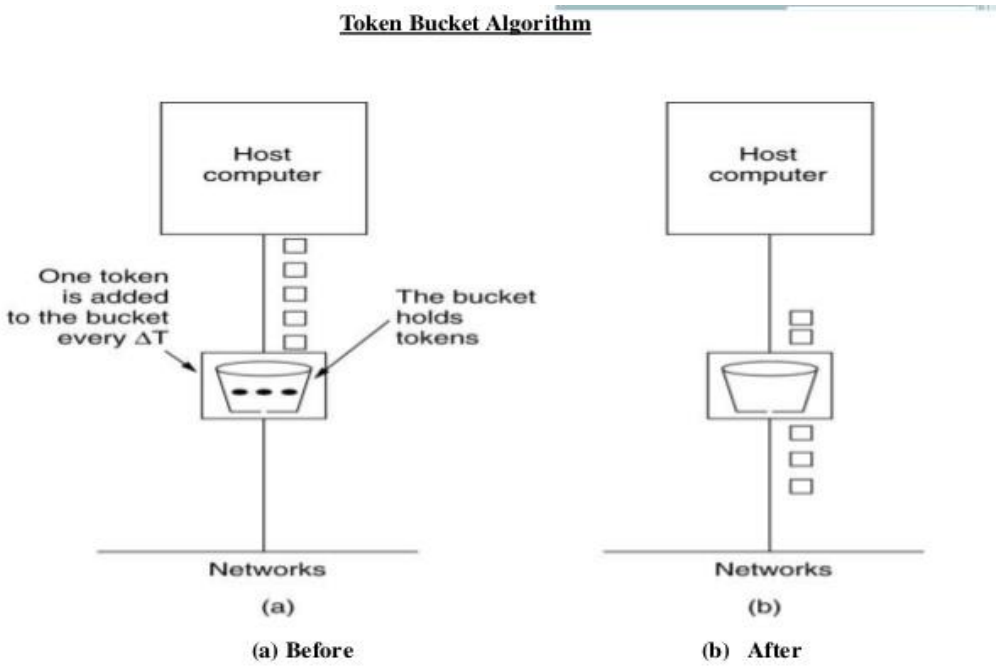
Parameters:

1. Smooth out traffic by passing packets only when there is a token. Does not permit burstiness.
2. Discards packets for which no tokens are available (no concept of queue)
3. Application: Traffic shaping or traffic policing.

This mechanism is slight different from leaky bucket algorithm in traffic policing. The bucket in traffic policing is just a counter where as a bucket in traffic shaper is a memory buffer that stores the packet.

Token bucket traffic shaper:

To overcome the disadvantage of leaky bucket, token bucket traffic shaper is introduced. Token is used here as a permit to transmit a packet, Unless there is a token no packet will be transmitted. The token bucket holds token which are generated periodically at a constant rate. New tokens are discarded in case if the token bucket is full. A packet can be transmitted if there is a token in the token buffer, otherwise it waits until the token is generated.



Token bucket:

Parameters:.

1. Token bucket smoothens traffic too, but permits burstiness which is equivalent to the number of tokens accumulated in the bucket.
2. Discards tokens when bucket is full, but never discards packets (infinite queue).
3. Application: Network traffic shaping or rate limiting.

Congestion Prevention Policies

These systems are designed to minimize congestion in the first place, rather than letting it happen and reacting after the fact. They try to achieve their goal by using appropriate policies at various levels. Different policies that can affect congestion at data link, network and transpost layers are :

Layer	Policies
Transport Layer	• Retransmission policy • Out-of-order caching policy • Acknowledgement policy • Flow control policy • Time determination
Network Layer	• Virtual circuits versus datagram inside the subnet • Packet queuing and service policy • Packet discard policy • Routing algorithm • Packet lifetime management
Data Link Layer	• Retransmission policy • Out-of-order caching policy • Acknowledgement policy • Flow control policy

Internetworking

Internetworking started as a way to connect different types of computer networking technologies. Computer network term is used to describe two or more computers that are linked to each other. When two or more computer LANs or WANs or computer network segments are connected using devices such as a router and configure by logical addressing scheme with a protocol such as IP, then it is called as computer internetworking.

Type of Internetworking

Internetworking is implemented in Layer 3 (Network Layer) of this model The most notable example of internetworking is the Internet (capitalized). There are three variants of internetwork or Internetworking, depending on who administers and who participates in them :

1. Intranet
2. Extranet
3. Internet

1. Intranet

An intranet is a set of interconnected networks or Internetworking, using the Internet Protocol and uses IP-based tools such as web browsers and ftp tools, that is under the control of a single administrative entity. That administrative entity closes the intranet to the rest of the world, and allows only specific users. Most commonly, an intranet is the internal network of a company or other enterprise. A large intranet will typically have its own web server to provide users with browseable information. It allows the employees and collegues to work with each other in a virtual space.

2. Extranet

An extranet is a network of internetwork or Internetworking that is limited in scope to a single organisation or entity but which also has limited connections to the networks of one or more other usually, but not necessarily, trusted organizations or entities . The major difference between intranet and extranet is that an intranet is typically used internally. While a extranet allows businesses to communicate with clients and vendors.

3. Internet

A specific Internetworking, consisting of a worldwide interconnection of governmental, academic, public, and private networks based upon the Advanced Research Projects Agency Network (ARPANET) developed by ARPA of the U.S. Department of Defence also home to the World Wide Web (WWW) and referred to as the 'Internet' with a capital 'I' to distinguish it from other generic internetworks. Participants in the Internet, or their service providers, use IP Addresses obtained from address registries that control assignments.