UNIT -III

NETWORK LAYER

Network Layer: Design issues, Routing algorithms: shortest path routing, Flooding, Hierarchical routing, Broadcast, Multicast, distance vector routing, Congestion Control Algorithms, Quality of Service, Internet working, The Network layer in the internet.

Network Layer:

- The network layer is concerned with getting packets from the source all the way to the destination.
- The network layer must know about the topology of the communication subnet in the set of all routers, and choose appropriate paths through it.
- Network layer is the lowest layer that deals with end-to –end transmission.

Design Issues

The design issues include the service provided to the transport layer & the internal design of the subnet.

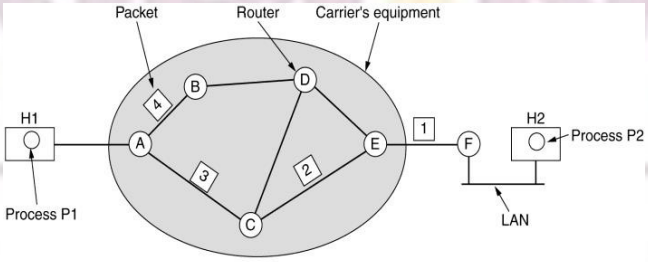
Services provided to the transport layer:

- The network layer provides services to the transport layer at the network layer / transport layer interface.
- The network layer services have been designed with following goals:

1. The services should be independent of the router technology.
2. The transport layer should be shielded from the number, type, and topology of the routers present.
3. The network address made available to the transport layer should use a uniform numbering plan, even across LAN'S & mans.

IMPLEMENATION OF CONNECTIONLESS SERVICE:

- If CL service is offered, packets are injected into the subnet individually & routed independently of each other.
- No advance setup is needed.
- Packets are called datagram's &the subnet is called a datagram subnet.
- Process p1 has a long message for p2. It sends the message to the transport layer with instructions to deliver it to process p2 on host H2.
- The message is four times longer than the maximum packet size, so the network layer has to break it into router A using some point – to – point protocol.
- Every router has a table telling it where to send packets for each possible destination.
- Each table entry is a pair of destination & the outgoing line to use for that destination.
- 'A' has only two outgoing lines to B & C- so every incoming packet must be sent to one of these routers , even if the ultimate destination is some other router.
- As they arrived at A, packets 1,2, &3 were stored each was forwarded to C. packet 1 was then forwarded to E& then to F.
- When the packet reaches F, it was encapsulated in a data link layer frame & sent to H2 over the LAN.
- Packets 2 and 3 follow the same route.
- For some reason , A decided to send packet H via a different route than that of the first three.
- It learned of a traffic jam somewhere along the ACE path & updated its routing table.
- The algorithm that manages the tables & makes the routing decisions is called the "routing algorithm".



A's table

Dest.	Line (initially)	Line (later)
A	–	–
B	B	B
C	C	C
D	B	B
E	C	B
F	C	B

C's table	
A	A
B	A
C	–
D	D
E	E
F	E

E's table	
A	C
B	D
C	C
D	D
E	–
F	F

Fig: Routing within a diagram subnet

IMPLEMENTATION OF CONNECTION –ORIENTED SERVICE:

- If connection oriented service is used a path from the source route to the destination router must be established before any data packets can be sent.

- This connection is called a virtual circuit(VC) and the subnet is called a virtual circuit subnet.
- The idea of virtual circuits is to avoid having to choose a new route for every packet sent.
- When a connection is established, a route from the source machine to the destination machine is chosen as part of the connection setup & stored in tables inside the routers.
- That route is used for all traffic flowing over the connection.
- When the connection is released , the virtual circuit is also terminated.
- With connection- oriented service, each packet carries an identifier telling which virtual circuit it belongs to.
- Host H1 has established connection 1 with host H2.
- A's table says if a packet bearing connection identifier 1 comes in from H1, it is to be sent to router C & given connection identifier 1.
- If H3 also wants to establish a connection to H2.
- It chooses connection identifier 1 & tells the subnet to establish the virtual circuit.
- 'A' can easily identified the connection 1 packets from H1 & connection 1 packets from H3, 'c' cannot do this.
- 'A' assigns a different connection identifier to the outgoing traffic for the second connection.
- To avoid the conflicts routers replace connection identifier in out going packets. This is called ***Label Switching***.

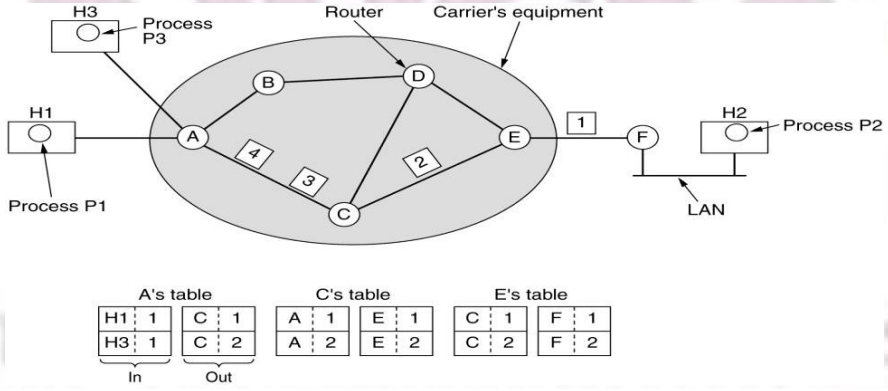


Fig: Routing within a virtual-circuit subnet

Comparison of virtual –circuit & datagram subnets:

Issue	Datagram subnet	Virtual circuit subnet

Circuit steup	Not needed	Required
Addressing	Each packet contains the full source & 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 setup ;all packets follow it.
Effect of router failures	None,except for packets lost during the crash	All VC's 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.

Routing Algorithms

- The main function of the network layer is routing packets from the source machine to the destination machine.
- The routing algorithm is that part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on.
- If the subnet uses datagram's internally, this decision must be made a new for every arriving data packet since the best route may have changed since last time.
- If the subnet uses virtual circuits internally, routing decisions are made only when a new virtual circuit is being set up.
- Routing algorithms can be grouped into two major classes:

  1. ***non adaptive*** **2.** ***adaptive***.

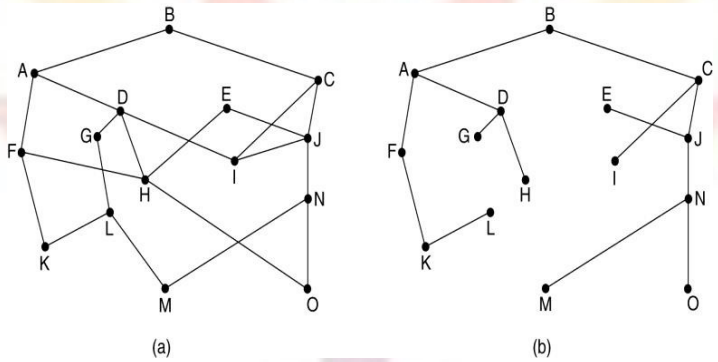
- **Nonadaptive algorithms** do not base their routing decisions on measurements or estimates of the current traffic and topology. This procedure is sometimes called **static routing.**

- **Adaptive algorithms**, in contrast, change their routing decisions to reflect changes in the topology, and usually the traffic as well. This procedure is sometimes called **Dynamic routing**.
- ***Static algorithms are →shortest path routing algorithm***
- ***Flooding algorithm***
- ***Dynamic algorithms are → distance vector routing algorithm.***

→link state routing algorithm

OPTIMALITY PRINCIPLE:

- Optimality principle state that no loops should be present in transferring the information.
- The set of optimal routes from all sources to a given destination form a tree rooted at the destination. Such a tree is called a **sink tree.**



(a) A subnet. (b) A sink tree for router B.

SHORTEST PATH ROUTING ALGORITHM:

In this routing algorithm we need to choose shortest path from source to destination.

- To choose a route between a given pair of routers, the algorithm just finds the shortest path between them.
- One-way of measuring path length is the number of hops.
- Another metric is the geographic distance in kilometers.
- Several algorithms for computing the shortest path between two nodes are known.
- Each node is labeled with its distance from the source node along the best known path.
- Initially no paths are known, so all nodes are labeled with infinity.
- As the algorithm proceeds and paths are found, the labels may change, reflecting better paths.
- A label may be either temporary or permanent.
- When it is discovered that a label represents the shortest possible path from the source to that node, it is made permanent & never changes thereafter.

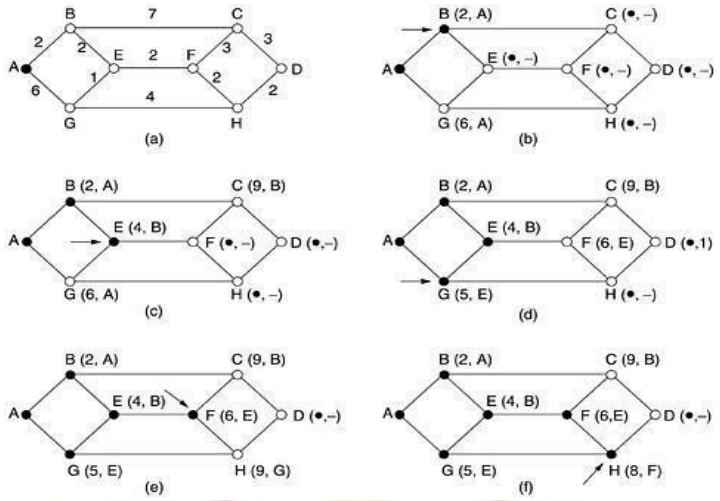


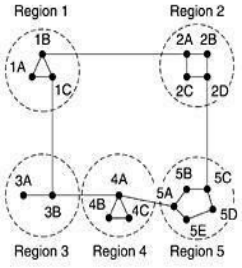
Fig. The first five steps used in computing the shortest path from *A* to *D*. The arrows indicate the working node.

FLOODING:

- Flooding is another static algorithm.
- In flooding, every incoming packet is sent out on every outgoing line except the one it achieved on.
- Flooding generates vast number of duplicate packets, an infinite number we need to take measures to damp the process.
- One such measure is to have a hop counter contained in the header of each packet, which is decremented at each hop, with the packet being discarded when the counter reaches zero.
- The hop counter should be initialized to the length of the path from source to destination.
- To avoid duplicates, the source router put a sequence number in each packet it receives from its hosts.
- Each router needs a list per source router telling which sequence numbers originating at that source have already been seen.
- If an incoming packet is on the list, it is not flooded.
- Each list should be maintained a counter, k, and mean that all sequence numbers through k have been seen.
- When a packet comes in. it is easy to check if the packet is a duplicate; if so, it is discarded.
- A variation of flooding is selective flooding.
- In selective flooding algorithm the routers do not send every incoming packet out on every line.
- Only on those lines that are going approximately in the right direction.
- Flooding can be useful in distributed database applications to update all the databases concurrently.

HIERARCHICAL ROUTING:

- As networks grow in size, the router routing tables grow proportionally.
- It takes more CPU time is needed to scan them and more bandwidth is needed to send status reports about them.
- When hierarchal routing is used the routers are divided into regions.
- Each router know the details about how to route packets to destinations with in its own region.
- Knowing nothing about the internal structure of the regions.
- When different networks are interconnected , we can assume the network as a separate region in order to free the routers in one network from having to know the topological structure of the other ones.
- Above fig. is an example of routing in a two level hierarchy with five regions.
- The full routing table for router 1A has 17 entries.
- When routing is done hierarchically , there are entries for all the local routers as before, but all other regions have been condensed into a single router, so all traffic for region 2 goes via the 1B-2A line.
- But, the rest of the remote traffic goes via the 1C-3B line.
- Hierarchical routing has reduced the table from 17 to 7 entries.
- The savings in the table space increase & there is problem of increased path length.
- Example is the best route from 1A to 5C is via region 2.
- But with hierarchical routing all traffic to region 5 goes via region 3, because that is better for most destinations in region 5.



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

Fig. Hierarchical routing

Broadcast Routing:

- Sending a packet to all destinations simultaneously is called broadcasting.
- Various methods are used for broad casting.

- One broadcasting method is the source simply sends a distinct packet to each destination.
- In this bandwidth is wasted & the source has to maintain the list of all destinations.
- The second broadcasting method is flooding. Flooding is useful as a broadcasting method if none of the above methods described below are applicable.
- The problem with flooding is it generates too many packets and consumes too much bandwidth.
- A third algorithm is multi destination routing. In this method, each packet contains a list of all destinations.
- When a packet arrives at a router, the router checks all the destinations to determine the set of output lines that will be needed.
- A fourth broadcast algorithm use the sink tree for the router initiating the broadcast or any other spanning tree.
- A spanning tree is a subset of the subset of the subnet that includes all the routers but contain s no loops.
- If each router knows which of its lines belong to the spanning tree , except the line it arrived on, it copy an incoming broadcast packet onto all the spanning tree lines.
- It makes use of bandwidth, generating the minimum number of packets necessary to do the job.
- Last broadcast algorithm is to approximate the behavior of the previous one, even when the routers do not know anything at all about spanning trees.
- When a broadcast packet arrives at a router, the router checks if it is on the line that is normally used for sending packets to the source of the broadcast.
- If so, the broadcast packet itself followed the best route from the router & is therefore the first copy to arrive at the router.
- The router forwards copies of it onto all lines except the one it arrived on.
- If the broadcast packet arrive on a line other than the preferred one for reaching the source, the packet is discarded as a duplicate. The algorithm called ***reverse path forwarding***.

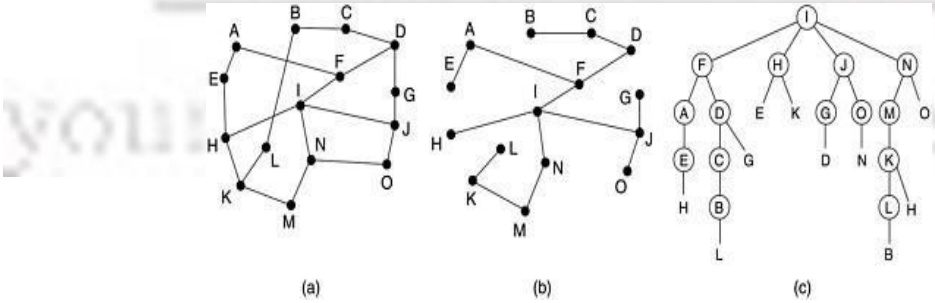


Fig. Reverse path forwarding. (a) A subnet. (b) A sink tree. (c)The tree built by reverse path forwarding.

Multicast Routing:

- Some applications need processes work together in groups, a group of processes implementing a distributed database system.
- It is frequently necessary for one process to send a message to all other members of the group.
- Sending a message to such a group is called multicasting. The routing algorithm is called ***multicast routing.***
- To do multicasting, group management is required.
- When a process joins a group, its informs its host.
- The routers must know which of their hosts belong to which groups.
- Hosts must inform their routers about changes in group membership, or routers must query their hosts periodically.
- In multicast routing, each router computes a spanning tree covering all other routers in the subnet.

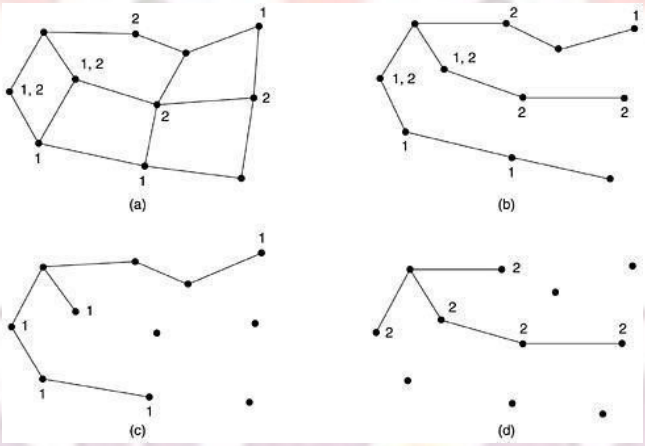


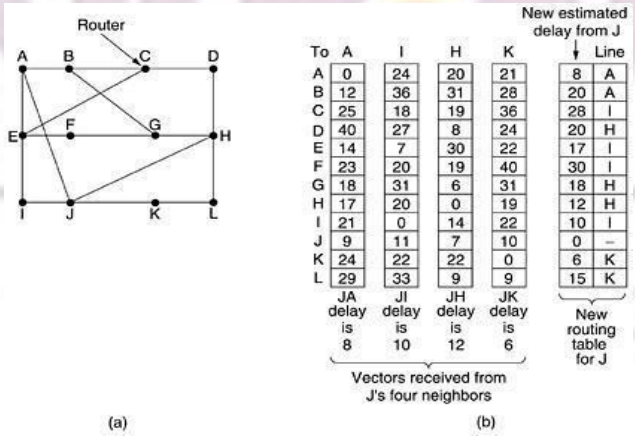
Fig: (a) A network. (b) A spanning tree for the leftmost router.
(c) A multicast tree for group 1. (d) A multicast tree for group 2.

- The above fig shows the subnet with two groups 1 and 2.
- Some routers are attached to hosts that belong to one or both of these groups.
- The spanning tree for the leftmost router is as shown below.
- The process sends a multicast packet to a group.
- The first router examines its spanning tree & prunes it, removing all the lines that do not lead to hosts that are members of the group.
- Multicast packets are forwarded only along the appropriate spanning tree.
- Multicast tree for group 1 is shown below:
- Multicast packets are forwarded only along the appropriate tree.
- Pruning the spanning tree is possible by using link state routing & distance vector routing.

- If link state routing is used , the spanning tree can be pruned by starting at the end of each path & working toward the root , removing all routers that do not belong to the group.
- If distance vector routing is used, whenever a router with no hosts interested in a particular group, the other routers receives a multicast message for that group, it responds with a PRUNE message, telling the sender not to send it any more multicasts for that group.
- The disadvantage of that algorithm is not used for large networks.

DISTANCE VECTOR ROUTING:

- Distance vector routing algorithm is the dynamic algorithm.
- Distance vector routing algorithm is also called as bellman- ford (or) ford-Fulkerson algorithm.
- Distance vector routing algorithm operate by having each router maintain a table giving the best known distance to each destination & which line use to get there.
- The tables are updated by exchanging information with the neighbors'.
- Each router maintains a routing table, containing one entry for each router in the subnet.
- Entry contains two parts: the outgoing line to use for that destination& an estimate of the time or distance to that destination.
- Router knows the delay to each of its neighbor.
- Once every T msec each router sends to each neighbor a list of its estimated delays to each destination. It also receives the similar list from each neighbor.
- If a table has come in from neighbor X. X is estimate how long it takes to get to route I is indicated as xi.
- If the delay to router x is M msec, if can reach the router I via x in Xi+M msec.
- For each neighbor by performing this calculation a router can find out which estimate seems the best & use that estimate & the corresponding line in its new routing table.



To	A	I	H	K	New estimated delay from J	Line
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	–
K	24	22	22	0	6	K
L	29	33	9	9	15	K
	JA delay is 8	JI delay is 10	JH delay is 12	JK delay is 6	New routing table for J	

Vectors received from J's four neighbors

Fig: (a) A subnet. (b) Input from *A*, *I*, *H*, *K*, and the new routing table for *J*.

- The delay vectors received from the neighbors of router j.

- In the example, A has delay of 12 msec to B, 25 msec to C, 40 msec to D etc.
- J has measured its delay to its neighbors' A,I,H, &K as 8,9,10,12 & 6 msec respectively.
- Now J computes its new route to router G.
- A can get to G in 18 msec,J can get to A in 8 msec.
- J knows it can count on a delay of 26 msec to G.
- Similarly, it computes the delay to G via I,H,& K as 41,18,&37 msec respectively.
- The best of these values is 18 msec so it makes an entry in its routing table that the delay to G is 18 msec. & that the route to use is via H.

Congestion control algorithms

- When too many packets are present in the subnet, performance degrades. This situation is called congestion.
- Congestion ctrl occurs if move no .of packets are transmitted with in the maximum range of carrying capacity.
- Congestion problem occurs when
  1. The processor is slow.
  2. If more input lines & only one output line.
  3. Bandwidth of lines may be less than what we required.
  - The difference between congestion ctrl & flow control is.
  - Congestion ctrl make sure the subnet is able to carry the offered traffic.
- If involves the behavior of all the hosts, all the routers, the store- and –forwarding processing with in the routers & all other factors that relate to the carrying capacity of the subnet.
- Flow control relates to the point –to – point traffic between a given sender & a given receiver.
- It make sure that a fast sender cannot continually transmit data faster than the receiver can absorb it.
- Flow control involves some direct feedback from the receiver to the sender.

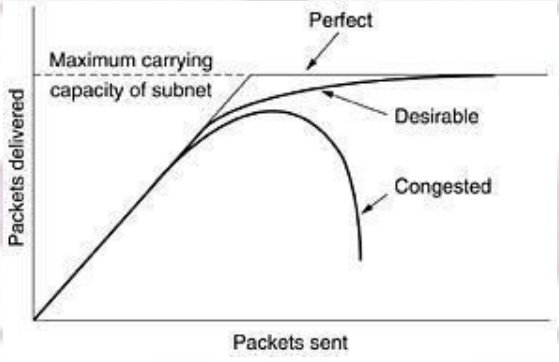


Fig: When too much traffic is offered, congestion sets in and performance

degrades sharply.

General principles of congestion control:

- General principles are divided into open loop and closed loop.
- Open loop: no modifications are allowed in the execution while the information is going on. Open loop is provided by good design.
- Closed loop or feedback loop: this approach has 3 packets.

1. We have to monitor the system when & where congestion occurs.
2. We have to inform to source which can take action regarding the congestion.
3. We have to adjust the total system operation to correct the problem.

Congestion prevention policies:

- Congestion control in open loop systems.
- These systems minimize congestion in the first place.
- We see different policies that can affect congestion at data link , network & transport layer.

At the data link layer:

1. Retransmission policy.
2. Out of order caching policy.
3. Acknowledge meant policy.
4. Flow control policy.

At the network layer:

1. Compare virtual circuit & datagram inside the subnet.
2. Packet queuing &service policy.
3. Packet discards policy.
4. Routing algorithm.
5. Packet lifetime management.

At the transport layer:

1. Retransmission policy.
2. Out of order caching policy.
3. Acknowledgement policy.
4. Flow control policy.
5. Time out determination.

Traffic shaping:

- Regulating the average rate of data transmission is called traffic shaping.
- Traffic shaping reduces congestion.
- Monitoring a traffic flow is called traffic policy.
- Algorithms of traffic shaping are
  1. The leaky bucket algorithm.
  2. The token bucket algorithm.

The leaky bucket algorithm:

- The rate at which water enters the bucket, the outflow is at a constant rate, r, when there is any water in the bucket and zero when the bucket is empty.

- Also, once the bucket is full, any additional water entering it spills over the sides and is lost
- It is a single server queuing system with constant service time.

- Each host is connected to the network by an interface containing a leaky bucket is a finite internal queue.
- If a packet arrives at a queue when it is full, the packet is discarded.
- The host is allowed to put one packet per clock tick onto the network.
- This mechanism turns an uneven flow of packets from the user processes inside the host into an even flow of packets onto the network.
- It greatly reduces the chances of congestion.
- When packets are all the same size. e.g.: ATM cells this algorithm can be used as described.
- When variable sized packets are used, it allows a fixed number of bytes per tick, rather just one packet.
- If the byte count is too low, the next packet must wait until the next tick.

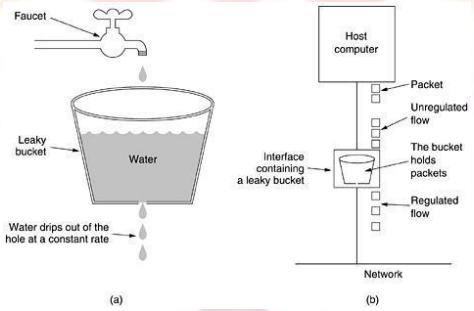


Fig: (a) A leaky bucket with water. (b) A leaky bucket with packets.

Token bucket algorithm:

In this algorithm, the leaky bucket holds tokens, generated by a clock at the rate of one token every delta Tsec.

- For a packet to be transmitted, it must capture and destroy one token.
- We have a bucket holding three tokens, with five packets waiting to be transmitted
- Three of the five packets have passed, but the other two are waiting for two more tokens to be generated.
- Token bucket algorithm provides a different kind of traffic shaping than the leaky bucket algorithm.
- The difference between two algorithms is token bucket algorithm throws away tokens when the bucket fills up but never discards packets.
- The leaky bucket algorithm discards packets when the bucket fills up.

- In token bucket algorithm a packet can only be transmitted if enough tokens are available.
- The implementation of token bucket algorithm is just a variable that count tokens.

- The counter is incremented by one every delta T and decremented by one whenever a packet is sent.
- When the counter hits zero, no packets may be sent.
- One way to get smoother traffic is to put a leaky bucket after the token bucket.
- The network has to simulate the algorithm &make sure that no more packets or bytes are being sent than are permitted.

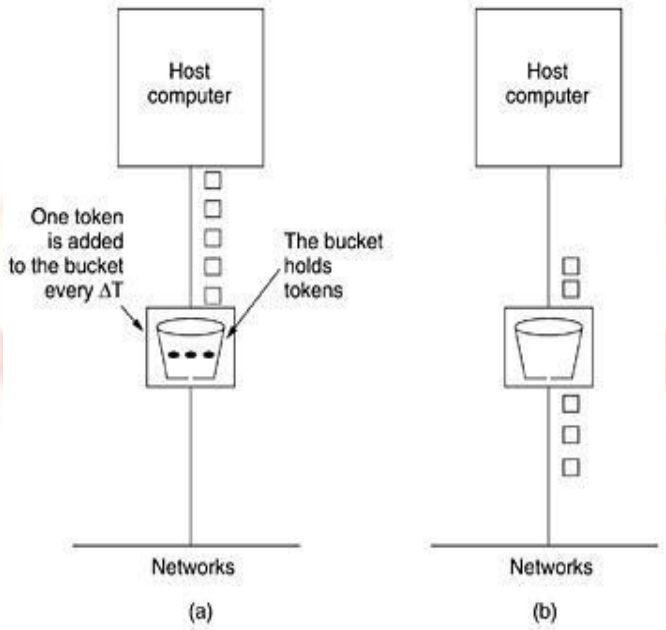


Fig: The token bucket algorithm. (a) Before. (b) After.

Congestion control in virtual circuit subnets:

- We ctrl congestion in virtual circuits dynamically.
- 'Admission control' is widely used to keep congestion that has already started from getting worse.
- Congestion ctrl in virtual circuit comes under closed loop.
- Once Congestion has been signaled, no more virtual circuits are set up until the problem has solved.
- With this, the setup to new transport layer connection fails.
- An alternative approach is to allow new virtual circuits but carefully route all new virtual circuits around problem areas.
- Another approach is to make an agreement between the host & subnet when a virtual circuit is set up.This agreement specifies the volume & shape of the traffic, quality of service required, & otherparameters.

- In this way, congestion is unlikely to occur on the new virtual circuits because all the necessary resources and guaranteed to be available.

Congestion control in datagram subnets:

- Each router can easily monitor the utilization of its output lines & other resources.
- Each newly-arriving packed is checked to see if its output line is in warning state.
- If it is, in warning state an action can be taken in several alternatives.

Warning bits:

- As the route was in the warning state, it continued to set the acknowledgements with it set.
- The source monitored the fraction of acknowledgements with the bit set & adjusted its transmission rate accordingly.
- As the warning bits continued to flow in, the source continued to decrease its transmission rate.

Choke packets:

- The router sends a choke packet back to the source host.
- When the source host gets the choke packet, it is required to reduce the traffic sent to the specified destination by x percent.
- Other packets aimed at the same destination generate more choke packets. The host should ignore choke packets referring to that destination for a fixed time interval.
- After the time period expired, if one choke packet arrives, the line is still congested, so the host reduces the flow & begins ignoring choke packets again.
- If no choke packets arrive during the time period , the host may increase the flow again

Hot-by-hop chokes packets:

- Sending a choke packet to the source hosts over long distances does not work well as the reaction is so slow.
- An approach is to have the choke packet take effect at every hop it passes through.
- The effect of this hop-by-hop scheme is to provide quick relief at point of congestion.

Load shedding:

- With this we can completely eliminate the congestion.
- Load shedding gives priority to all the packets which we are transmitting
- In this we can eliminate some messages at the sender.

Jitter control:

- If we are sending audio or video at constant rate in quality should be high.

- The variations in packet arrival time are called jitter.
- When a packet arrives at a router, the router checks to see how much the packet is behind or ahead of its schedule.
- The packets that are ahead of schedule get slowed down & packets that are behind schedule get speeded up.

Congestion control for multicasting:

- In multicasting we need to send messages to a group. There are multiple senders and multiple receivers.
- We use protocol called RSVP (Resource Reservation Protocol).
    - Rsvp: Resource Reservation Protocol
- This protocol is used for making the reservations other protocols are used for sending the data.
- Rsvp allows multiple senders to transmit to multiple groups of receivers.
    - Note: refer text book for diagram
- Hosts 1&2are multicast senders,
  hosts 3, 4 &5are multicast receivers.
- To eliminate congestion, any of the receivers in a group can send a reservation message up the tree to the sender.
- At each step, the router notes the reservation and reserves the necessary bandwidth
- If insufficient band with is available it reports back failure.
- Host 3 has requested a channel a host 1
- Once it has been established packets can flow 1 to 3 with out congestion.
- If host 3 next reserves a channel to the other sender host to a second path is reserved
- When making a reservation, a reserve can specify one or more sources that it wants to receive from.
- The routers use this information to optimize band width planning.

Internet working

- Different networks are connected together to form an internet.
- The purpose of inter connecting all these networks is to allow users on one network to communicate with users on other network & also sending packets from one network to other network.

Networks can differ in many ways: the networks differ based on the following

Item	Some Possibilities
Service offered	Connection oriented versus connectionless
Protocols	IP, IPX, SNA, ATM, MPLS, AppleTalk, etc.
Addressing	Flat (802) versus hierarchical (IP)
Multicasting	Present or absent (also broadcasting)
Packet size	Every network has its own maximum
Quality of service	Present or absent; many different kinds
Error handling	Reliable, ordered, and unordered delivery
Flow control	Sliding window, rate control, other, or none
Congestion control	Leaky bucket, token bucket, RED, choke packets, etc.
Security	Privacy rules, encryption, etc.
Parameters	Different timeouts, flow specifications, etc.
Accounting	By connect time, by packet, by byte, or not at all

Networks can be interconnected by different devices.

- In the physical layer, networks can be connected by repeats or hubs.
- In the data link layer, networks can be connected by bridges and switches.
- In the network layer, routers are used to connect two networks.

  A router that can handle multiple protocols is called a multiprotocol router. in the transport layer, to interface between two transports connections we use transport gateways.

  In the application layer, networks can be connected by application gateways.

  In the application layer, networks can be connected by application gateways.
- Application gateways translate message semantics.
- Internetworking is possible in 2 ways:
- Connection oriented concatenation of virtual – circuit subnets.
- Connection less internetworking.

Concatenated virtual circuit:

- In this circuits a connection to a host in a distant network is set up in a way the connections are normally established.
- The subnet builds a virtual circuit to the router nearest the destination network as the destination is remote.
- It constructs virtual circuits from that router to an external gateway. (Multiprotocol Router)
- The gateway records the existence of the virtual circuits in its tables.
- It builds other virtual circuits to a router in the next subnet.
- This process continues until the destination host has been reached.
- Data packets begin flowing along the path.
- All data packets must traverse the same sequence of gateways.
- Packets in a flow are never reordered by the network.

- In this approach a sequence of virtual circuits is set up from the source through one or more gateways to the destination.
- This works better when all the networks have the same properties.

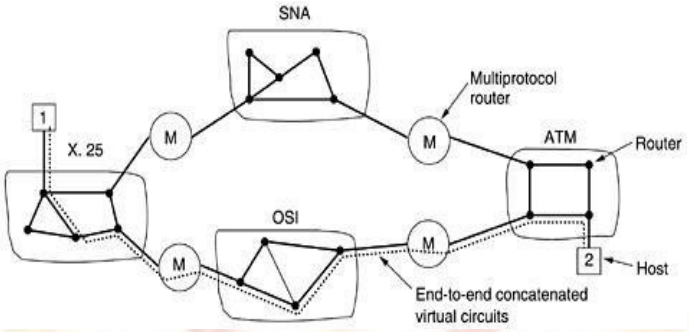


Fig: Internetworking using concatenated virtual circuits.

Connectionless internetworking:

- This model does not require all packets belonging to one connection to traverse the same sequence of gateways.
- From host-1 to host -2 datagram's take different routers through the internetwork.
- Routing decision made separately for each packet, depending on the traffic at the moment the packet is sent.
- There is no guarantee that the packet arrive at the destination in order, assuming that they arrive at all.
- If each network has it s own network layer protocol, it is not possible for a packet from one network to transit another one.
- Multiprotocol routers translate from one format to another if the formats are with same information fields.

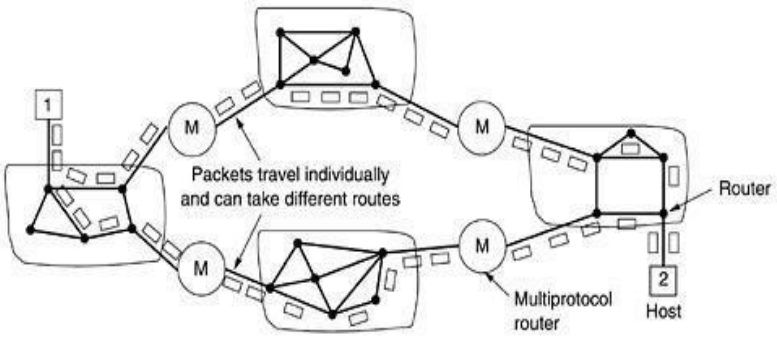


Fig: A connectionless internet.

- We can design a universal internet packet & have all routers recognize it.

  IP packet is designed to be carried through many networks.

INTERNETWORK ROUTING:

- Consider an example in which the internetwork of five networks are connected by 6 routes
- Make a graph in that every route can directly access to every other router connected to any network to which it is connected.

- In the above example B can directly access A and C via network 2 and also D via network 3
- A two level routing algorithm is used
- With in each network an interior gate way protocol is used
- Between in the network an exterior gate way protocol is used
- Each network in an inter network is independent of all the others

Fragmentation:

- Problem occurs when a large packets wants to travel through a N/W whose maximum packets sizes is too small
- The solution to this problem is to allow gate ways to break up packets in to fragments
- Which fragment is send as separate internet packets
- For recombining the fragments back in to the original packet we use two approaches
- *Transparent fragmentation*
- *Non Transparent fragmentation*
- In Transparent fragmentation we reassemble the fragment at each gate way until the designation is reached
- In Non Transparent fragmentation we reassemble the fragments only at the digestion

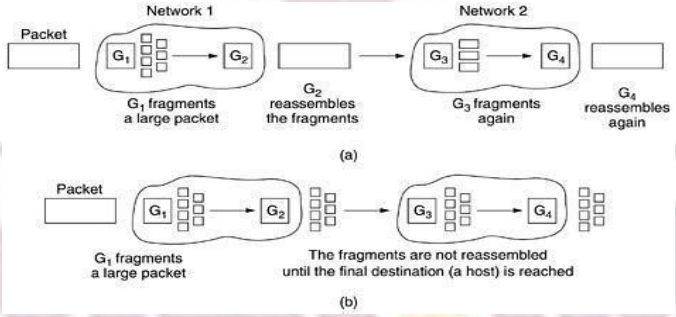


Fig: (a) Transparent fragmentation. (b) Nontransparent fragmentation

Network layer in the internet

IP protocol :

- At the network layer, the internet can viewed as a collection of sub network or autonomous systems (AS) that are inter connected
- an IP datagram consists off a header part and a test part
- the header has 20 bits fixed part and variable length optional part

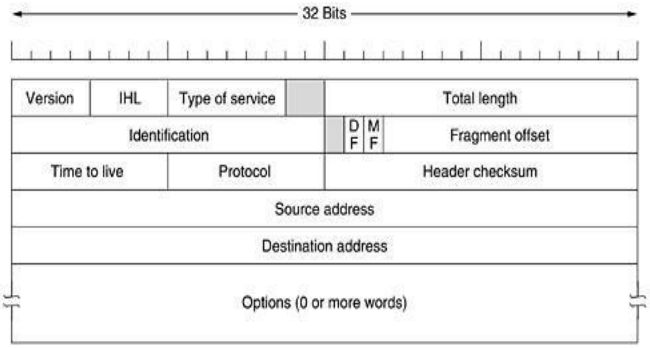


Fig: The IPv4 (Internet Protocol) header.

- Version fields are which version of the protocol the datagram belongs.
- IHL field tell how long the header is in 32-bit words
- Type of service specifies what kind of service we are applying.
- Total length indicates both header and data.
- Maximum length 65,535 bytes.
- Identification field identifies the new fragment arrived.
- All the fragments of a datagram's contains the same identification value.
- DF stands for don't fragment.
- If the DF bit is set, data is not fragmented it is send as a single datagram.
- MF stands for more fragments.
- It is used to know when all fragments of a datagram have arrived.
- Fragment offset determine s where the fragment belongs in the current datagram.
- All the fragments except last are in a datagram must be a multiple of 8bytes.
- There is a maximum of 8192 fragments per datagram.
- Time to live field used to specify the packet life time.
- Protocol field tells which transport process to give it to. TCP&UDP some others are used.
- Head checksum field verifies the header only.
- The source address and destination address indicates the network number and host number.
- Option field is variable length .if uses the options that are defined.

Option	Description
Security	Specifies how secret the datagram is
Strict source routing	Gives the complete path to be followed
Loose source routing	Gives a list of routers not to be missed
Record route	Makes each router append its IP address
Timestamp	Makes each router append its address and timestamp

Fig: Some of the IP options.

IP ADDRESS:

- On the Internet every host & router has an IP address.
- IP address consists of network number and host number.
- Network numbers are managed by a nonprofit corporation called *ICANN (Internet Corporation for Assigned Names and Numbers)* to avoid conflicts.
- No two machines on the Internet have the same IP address.
- If host belongs 2 networks, host contains 2 IP addresses.
- IP addresses are 32 bits long & are used in the source Address & Destination Address fields of IP packets.
- IP packet does not actually refer to a host, it refers only network interface.
- IP addresses are in dotted decimal notation.
- IP address is of 32 bits & representation is ().().().()
- IP address are of five different classes based on host range address.
- Least IP address is 0.0.0.0
- Highest IP address is 255.255.255.255

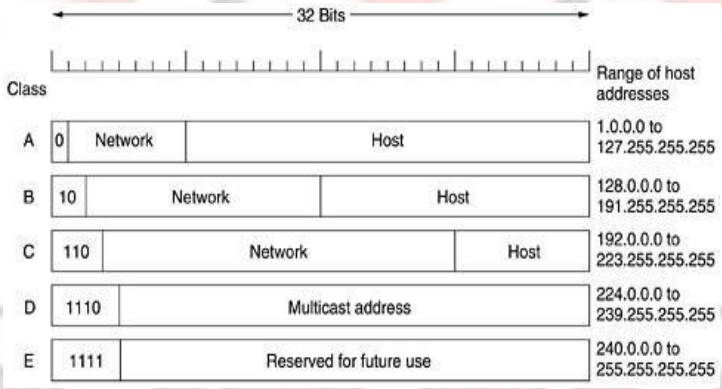


Fig: IP address formats.

- The value 0 means this network or this host current network.
- The value 1 used to indicate all hosts on the indicated network.