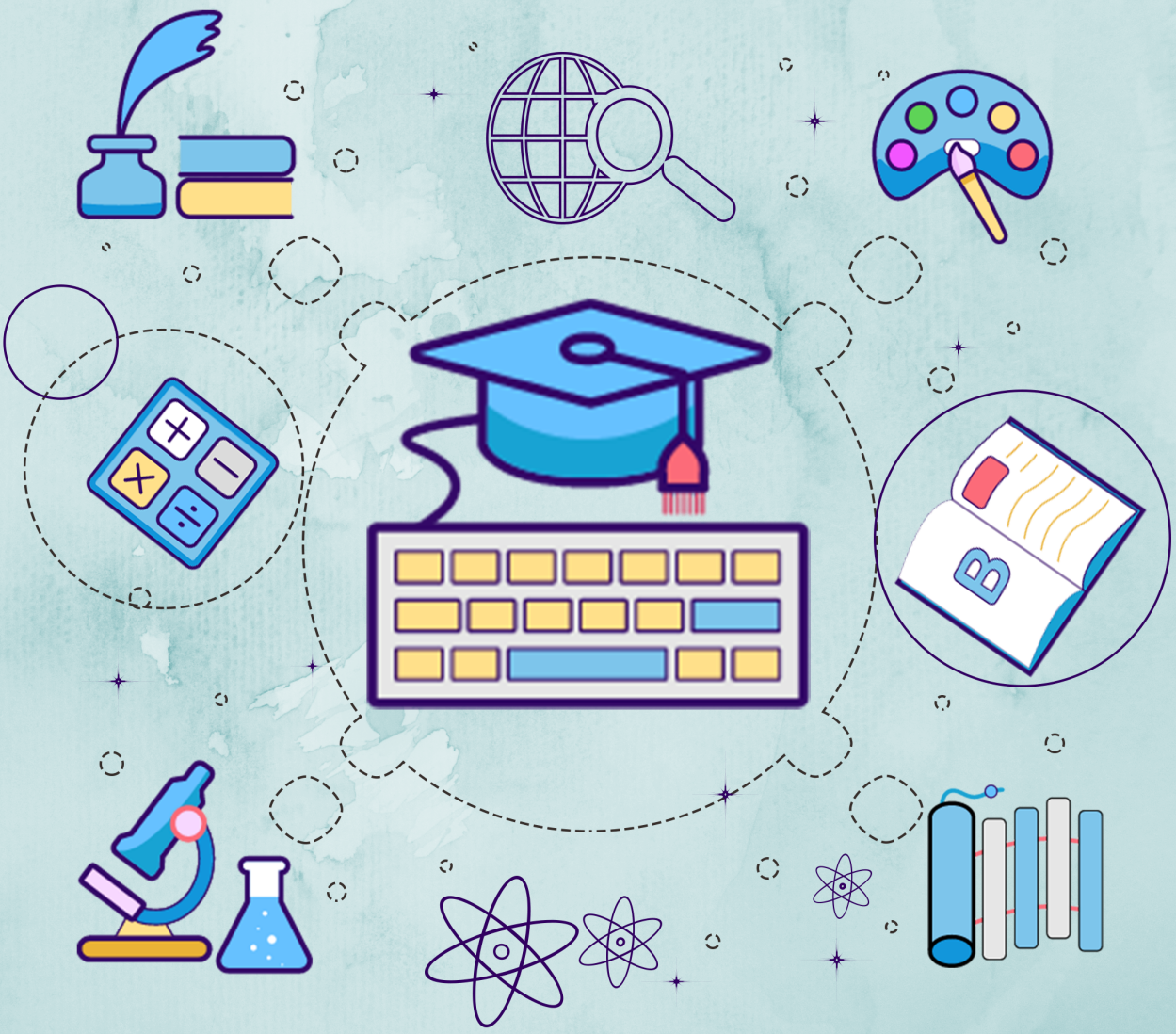
APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

KeralaNotes



SYLLABUS | STUDY MATERIALS | TEXTBOOK

PDF | SOLVED QUESTION PAPERS

www.keralanotes.com

KeralaNotes

KTU STUDY MATERIALS

COMPUTER NETWORKS

CST 303

Module 3

Related Link :

- KTU S5 STUDY MATERIALS
- KTU S5 NOTES
- KTU S5 SYLLABUS
- KTU S5 TEXTBOOK PDF
- KTU S5 PREVIOUS YEAR SOLVED QUESTION PAPER

CN

COMPUTER NETWORKS

Module 3

Module -3 (Network Layer)

Network layer design issues. Routing algorithms - The Optimality Principle, Shortest path routing, Flooding, Distance Vector Routing, Link State Routing, Multicast routing, Routing for mobile hosts. Congestion control algorithms.

Quality of Service (QoS) - requirements, Techniques for achieving good QoS.

Network Layer

- Network layer is responsible for source to destination(end to end) delivery of a packet across multiple network links.
- Routers and gateways operate in the network layer.
- routing the packets to final destination.
- It must also take care when choosing routes to avoid overloading in the network link

Functions Of Network Layer :

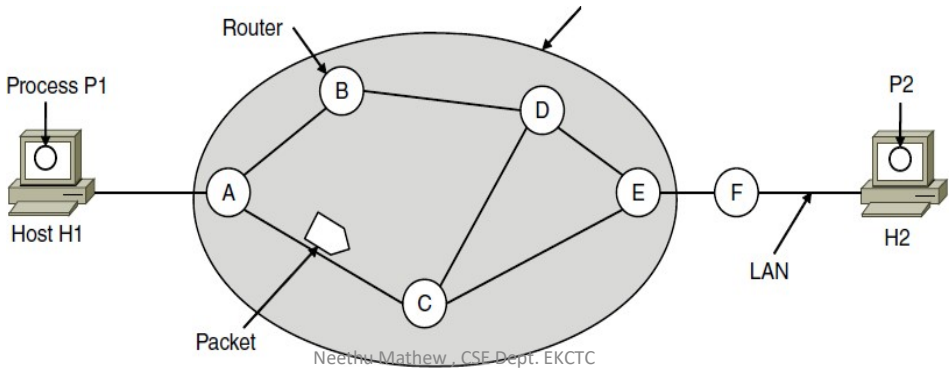
- Addressing
- Routing
- Internetworking
- Packetizing
- Fragmenting

Design issues - network layer

- ❑ Store-and-forward packet switching
- ❑ Services provided to transport layer
- ❑ Implementation of connectionless service
- ❑ Implementation of connection-oriented service
- ❑ Comparison of virtual-circuit and datagram networks

1. Store-and-forward packet switching

- 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 carrier
- 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
- The fig shows the environment of the network layer protocols :-



- The major components of the system are carriers equipment (routers connected by transmission lines) and

  customers' equipment , shown outside the oval.
- Host H1 is directly connected to one of the carrier's routers, A, by a leased line. In contrast, H2 is

  on a LAN, with a router, F, owned and operated by the customer. This router also has a leased

  line to the carrier's equipment.

2. Services provided to transport layer

The services designed with the following goals in mind:

- ✓ **The services provided should be independent of the underlying technology**. Users of the service need not be aware of the physical implementation of the network – for all they know, their messages could be transported via carrier
- ✓ **The transport layer should be shielded from the number, type, and topology of the routers present**. ie, All the

  transport layer wants is a communication link,it need not know how the link is made
- ✓ **The network addresses made available to the transport layer should use a uniform numbering plan**.

  There is a need for some uniform addressing scheme for network addresses
- ✓ The two classes of **service** the network layer can provide to its users:
  - **connectionless network service**.
  - **connection-oriented network service**. (Quality of service is the dominant factor, quality of service is very difficult to achieve, especially for real-time traffic such as voice and video.)

3. Implementation of connectionless service

- If connectionless service is offered, 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

4. Implementation of connection oriented service

- A path from the source router to the destination router must be established before any data packets can be sent.
- This connection is called a VC (virtual circuit), (eg. telephone system)
- The idea behind virtual circuits is to avoid having to choose a new route for every packet sent.

5. Comparison of virtual-circuit and datagram networks

Issue	Datagram network	Virtual-circuit network VC
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

Router

- Network layer device
- Routers are devices that connect two or more networks
- Whenever a router encounters a packet, it must decide where to pass that packet.
- A router might be connected to multiple routers
- Each router has a routing table that decides the route to be followed for each packet
- Routers look into routing table when a new packet arrives

Routing table

Network id	Cost	Next
.....	.....	.....
.....	.....	.....

The routing table consists of at least three information fields:
1: Network ID: i.e., the destination network id.
2: Cost: i.e, the cost or metric of the path through which the packet is to be sent.
3: Next Hop: The next hop, or gateway. is the address of the next station to which the packet is to be sent on the way to its final destination.

Routing Algorithms

- Routing is the process of moving packets across a network from one host to another.
- It is usually performed by dedicated devices called routers.
- Routing is concerned with the problem of determining feasible paths or packets to follow from each source to destination
- Network layer must determine the route or path taken by each packets as they flow from a sender to receiver. The algorithms that calculate these paths are referred to as routing algorithms
    - It is responsible for deciding the output line over which a packet is to be sent

Properties of Routing algorithms

- Optimality – capability of routing algorithm to select the best route
- Simplicity and low overhead -With increasing complexity of the routing algorithms the overhead also increases
- Robustness – means they should perform correctly in the face of unusual circumstances such as hardware failure
- Stability -The routing algorithms should be stable under all possible circumstances.
- Flexibility – they should quickly & accurately adapt to a variety of network circumstances
- Fairness - Every node connected to the network should get a fair chance of transmitting their packets.

Types of Routing algorithms

(1) Non adaptive (static routing)

(2) adaptive (dynamic routing).

Non adaptive algorithms

- routing decision is not based on measurements or estimates of the current traffic and topology.
- The choice of the route is computed in advance, off-line, and downloaded to the routers when the network is booted.
- This procedure is sometimes called

static routing. Adaptive algorithms

- routing decisions are based on measurements or estimates of the current traffic and topology.
- Stability is an important goal for the routing algorithm.
- This procedure is called **dynamic routing.**

Different Routing Algorithms

- **The Optimality Principle**
- **Shortest Path Routing**
- **Flooding**
- **Distance Vector Routing**
- **Link State Routing**
- Hierarchical Routing
- Broadcast Routing
- **Multicast Routing**
- **Routing for Mobile Hosts**
- Routing in Ad Hoc Networks

Neethu Mathew , CSE Dept. EKCTC

The Optimality Principle

- The optimality principle 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.

Optimality Principle
If J is optimal path
from I ➐ K
Then , optimal path
from J ➐ K also same route

- As a direct consequence of the optimality principle, we can see that 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** and is illustrated in following Figure
- distance metric is the number of hops.
- Note that a sink tree is not necessarily unique; other trees with the same path lengths may exist.
- The goal of all routing algorithms is to discover and use the sink trees for all routers.

Shortest Path Routing

shortest-paths algorithms :- 1. Dijkstra's Algorithm

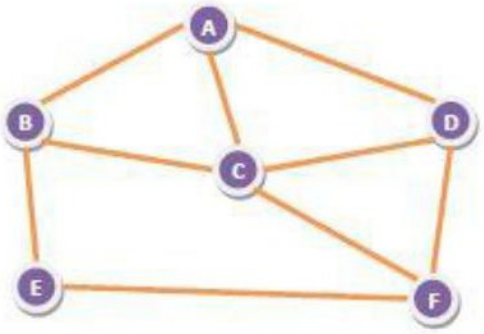
- In this Algorithm , the criteria for shortest path is distance.
- Shortest path problem is a problem of finding the shortest path(s) between vertices of a given graph
- Shortest path is a path that has the least cost as compared to all other existing paths.
- Min cost or least cost algorithm
- Vertices are assumed to act as routers and edges act as connecting media(link)
- A node has zero cost w.r.t itself
- Note: Dijkstra's Algorithm is applicable only when cost of all the nodes is non-negative.

1. Each **node** is labelled (in parentheses) with its distance from the source node along the best known path[eg. (2,A)].
2. Initially, no paths are known, so all nodes are labelled with infinity. As the algorithm proceeds and paths are found, the labels may change, reflecting better paths.
3. A **label** may be either tentative or permanent.
4. **Initially**, all labels are tentative.
5. **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 thereafter.

d(u)+w(u,v) <d(v) =>d(v)= d(u)+w(u,v)

Flooding

- Flooding is the static routing algorithm.
- Every incoming packet is sent out on every outgoing lines except the line on which it has arrived.
- One major problem of this algorithm is that it generates a large number of duplicate packets on the network.
- For example, let us consider the network in the figure, having six routers that are connected through transmission lines. Flooding obviously generates vast numbers of duplicate packets



- An incoming packet to A, will be sent to B, C and D.
- B will send the packet to C and E.
- C will send the packet to B, D and F.
- D will send the packet to C and F.
- E will send the packet to F.
- F will send the packet to C and E.

- Several measures are takes to stop the duplication of packets
- Measures :
  1. **hop counter :**
     - Every packet has a hop count associated with it .
     - This is decremented by one by each node which sees it
     - When the hop count becomes zero the packet is dropped (reached at destination).
  2. **Sequence number :**
     - Every packet is given a sequence number.
     - When a node receives the packet it sees its source address & sequence number.
     - If the nodes finds that it has sent the same packet earlier then it will not transmit the packet and will just discard it
- A variation of flooding that is slightly more practical is **selective flooding**. In this 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
- **Uncontrolled flooding** – Here, each router unconditionally transmits the incoming data packets to all its neighbours
- **Controlled flooding** – They use some methods to control the transmission of packets to the neighbouring nodes. The two popular algorithms for controlled flooding are Sequence Number Controlled Flooding (SNCF) and Reverse Path Forwarding (RPF).

❑ **APPLICATIONS**

Flooding is not practical in most applications, but it does have some uses. For example,

- In **military applications**, the tremendous robustness of flooding is highly desirable.
- In **distributed database applications**, it is sometimes necessary to update all the databases concurrently, in which case flooding can be useful.
- In **wireless networks**, all messages transmitted by a station can be received by all other stations within its radio range, flooding is useful.

❑ **ADVANTAGES**

- Highly Robust, emergency or immediate messages can be sent (eg military applications)
- Set up the route in virtual circuit
- Flooding always chooses the shortest path
- Broadcast messages to all the nodes
- This algorithm is very simple to implement.

❑ **DISADVANTAGES:**

- Flooding can be costly in terms of wasted bandwidth
- Messages can become duplicated in the network

Distance Vector Routing (DVR)

- It's a dynamic routing algorithm
- In DVR, least-cost route between any two nodes is the route with minimum distance
- In distance vector routing, **each router maintains a routing table** indexed by, and containing one entry for, each router in the subnet.
- This entry contains two parts:
  - ✓ the **preferred outgoing line** to use for that destination
  - ✓ **estimate of the distance** to that destination.
- each node maintains a vector (table) of minimum distances to every node.
- This table at each node guides the packets to the desired node by showing the next stop in the route (next-hop routing). ie,

  sending the packet to the desired node through the least cost route from the table
- 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.
- The distance vector routing algorithm is sometimes called by other names including distributed Bellman-Ford or Ford- Fulkerson. It was the original ARPANET routing algorithm and was also used in the Internet under the name RIP.

DISTANCE VECTOR ROUTING

- The Distance vector algorithm is a dynamic algorithm.
- It is also called Bellman-Ford routing algorithm and the Ford-Fulkerson algorithm
- It is mainly used in ARPANET, and RIP.
- Each router maintains a distance table known as Vector.
- Each node receives information from one or more of its directly attached neighbors, performs calculation and then distributes the result back to its neighbors.
- Information sharing at regular intervals - Within 30 seconds, the router sends the information to the neighboring routers.

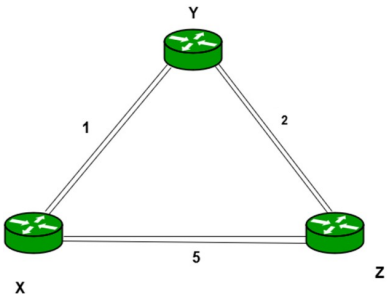
Neethu Mathew , CSE Dept. EKCTC

Distance Vector Algorithm –

1. A router transmits its distance vector to each of its neighbors in a routing packet.
2. Each router receives and saves the most recently received distance vector from each of its neighbors.
3. A router recalculates its distance vector when:
   a) It receives a distance vector from a neighbor containing different information than before.
   b) It discovers that a link to a neighbor has gone down.

   The DV calculation is based on minimizing the cost to each destination

Example : prepare the routing table for the following network

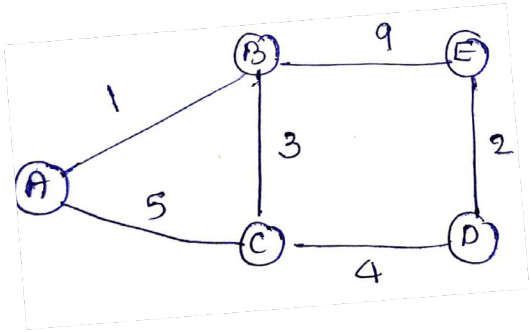


DVR Table for X	Cost	Next hop
X	0	-
Y	1	-
Z	3	Y

DVR Table for Y	Cost	Next hop
X	1	-
Y	0	-
Z	2	-

DVR Table for Z	Cost	Next hop
X	3	Y
Y	2	-
Z	0	-

Neethu Mathew , CSE Dept. EKCTC



* Routing table (B)

possible paths

- B to A
  - B – A : 1 ✓
  - B – C – A : 8
  - B – E – D – C – A : 20

  min is 1

- B to C
  - B – C : 3 ✓
  - B – A – C : 6
  - B – E – D – C : 15

- B to D
  - B – A – C – D : 10
  - B – C – D : 7 ✓
  - B – E – D : 11

- B to E
  - B – E : 9 ✓
  - B – C – D – E : 9
  - B – A – C – D – E : 12

select min path , less intermediate nodes

Distance vector routing table

DVR table for B

Destination	Cost	next hop
A	1	A
C	3	C
D	7	C
E	9	E

Find routing table for all other nodes

❑ **Advantages**

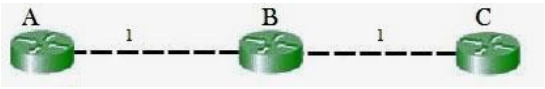
- It is simpler to configure and maintain than link state routing.

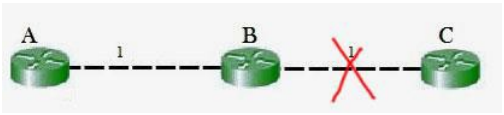
❑ **Drawbacks**

- React rapidly to good news when a router comes up.
- Though it finally converges to correct result, it takes long time when where is a bad news.
- There are several attempts to solve the problem, but none is perfect.
- It does not take line bandwidth into account.
- It took too long to converge.
- It is slower to converge than link state.
- It is at risk from the count-to-infinity problem.
- It creates more traffic . Hop count updates take place on a periodic basis, even if there are no changes in the network topology, so bandwidth-wasting broadcasts still occur.
- For larger networks, distance vector routing results in larger routing tables since each router must know about all other routers. This can lead to congestion on WAN links.

❑ **count-to-infinity problem:**

- The problem with Distance Vector Routing (DVR) is whenever a link is broken, other routers unknowingly given information that they know how to reach a disconnected node. This false information will propagate to all routers. This problem is known as Count to Infinity Problem.





- In this example, A know that it can get to C via B at a cost of 2 & B will know that it can get to C at a cost of 1
- If the link between B and C is disconnected, then B will know that it can no longer get to C via that link and will remove it from its table.
- Before it can send any updates it's possible that it will receive an update from A which will be advertising that it can get to

  C at a cost of 2.
- B can get to A at a cost of 1, so it will update a route to C via A at a cost of 3.
- A will then receive updates from B later and update its cost to 4.
- They will then go on feeding each other bad information toward infinity which is called as **Count to Infinity problem**

- The main issue with Distance Vector Routing (DVR) protocols is Routing Loops. Routing loops usually occur when an

  interface goes down or two routers send updates at the same time
- This routing loop in the DVR network causes the Count to Infinity Problem.

❑ **Solutions for count to infinity problem**

- Route poisoning
- Split horizon

link state routing (LSR)

- A method in which each router shares its neighbourhood information with every other router in the internetwork.
- Each node has a complete map of the topology
- Used in packet switching networks
- Link state routing protocol: OSPF, IS-IS
- Idea behind LSR is simple and can be stated as 5 parts. Each router must do the following
  - Discover its neighbors and learn their network addresses.
  - Measure the distance or cost metric to each of its neighbors.
  - Construct a packet telling all it has just learned.
  - Send this packet to and receive packets from all other routers.
  - Compute the shortest path to every other router.

5 steps

1. Learning about the neighbors

- When a 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. Measuring Link Cost

- Each router must know a reasonable estimate of the delay to each of its neighbors.
- The delay of links may be factored into cost
- The most direct way to determine this delay is to send a special ECHO packet over to neighbors 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 a reasonable

  estimate of the delay.
- Issue is whether to take the load into account when measuring the delay.

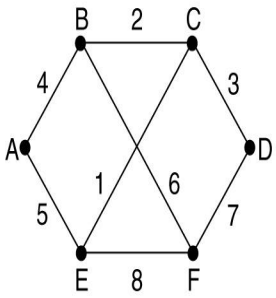
  To factor the load in, the round-trip timer must be started when the ECHO packet is queued.

  To ignore the load, the timer should be started when the ECHO packet reaches the front of the queue.

3. *Building Link State Packets(LSP)*

- Once the information 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 number and age, and a list of neighbours.
- The link state packets are built either at regular intervals or when some significant event occurs
- An example network is presented with costs shown as labels on the lines.
- The corresponding link state packets for all six routers are shown.
- Building the link state packets is easy.
- The hard part is determining when to build them.
  - One possibility is to build them periodically, that is, at regular intervals.
  - Another possibility is to build them when some significant event occurs, such as a line or neighbor going down

    or coming back up again or changing its properties appreciably.



(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)

(a) A subnet. (b) The link state packets for this subnet.

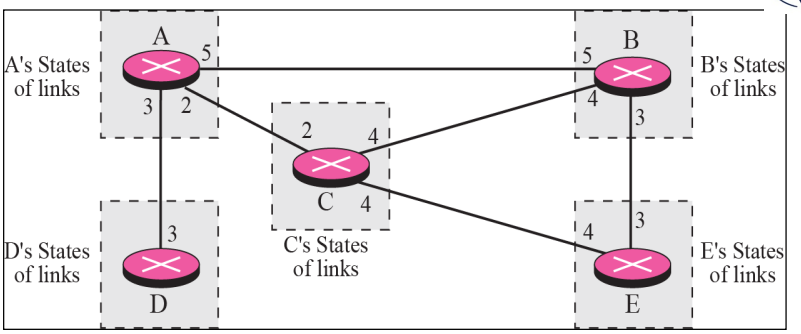
4. **Distributing Link State Packets**

- Link state packets are to be distributed reliably.
- As the packets are distributed and installed, the routers getting the first ones will change their routes. Consequently, the different routers may be using different versions of the topology, This can lead to inconsistencies, loops, unreachable machines, and other problems.
- Flooding is used to distribute the link state packets.
- To keep the flood in check, each packet contains a sequence number that is incremented for each new packet sent.
- Routers keep track of all the (source router, sequence) pairs they see.
- When a new link state packet comes in, it is checked against the list of packets 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.
- If a packet with a sequence number lower than the highest one seen so far ever arrives, it is rejected since the router

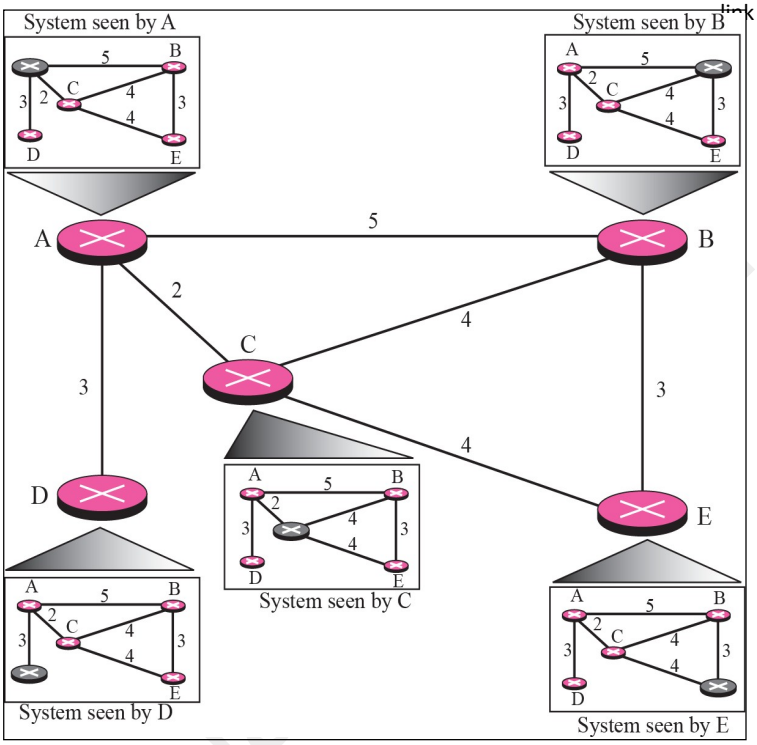
  has more recent data.

5. **Computing the shortest Routes**

- Once a router has accumulated a full set of link state packets, it can construct the entire subnet graph because every link is represented. Every link is represented twice, once for each direction. The two values can be averaged or used separately.
- Dijkstra’s algorithm can be run at each router to find the shortest path to every other router.
- Dijkstra's algorithm can be run locally to construct the shortest path to all possible destinations.
- The results of this algorithm can be installed in the routing tables, and normal operation resumed.
- For a subnet with n routers, each of which has k neighbors, the memory required to store the input data is proportional to kn.
- the computation time can be an issue. but, in many practical situations, link state routing works well



link state knowledge



Difference between link state routing &distance vector routing

Distance vector routing	Link state routing
Used in 1980 'S	Used in 1990"s
Band width is less	Band width is high
Traffic is les	Traffic is high
Count to infinity problem exist	Count to infinity problem not exists

Persistent loop	Transient loop
Protocol used is RIP	Protocol used is OSPF
Convergence is slow	Convergence is fast

Multicast Routing

Multicasting-

- In multicast communication, there is one source and a group of destinations.
- The relationship is one-to-many.
- In this type of communication, the source address is a unicast address, but the destination address is a group address, which defines one or more destinations. The group address identifies the members of the group.
- Some applications require that widely-separated processes work together in groups, for example, a group of processes implementing a distributed database system. In these situations, it is frequently necessary for one process to send a message to all the other members of the group. If the group is small, it can just send each other member a point-to point message. If the group is large, this strategy is expensive.
- Thus, we need a way to send messages to well-defined groups that are numerically large in size but small compared

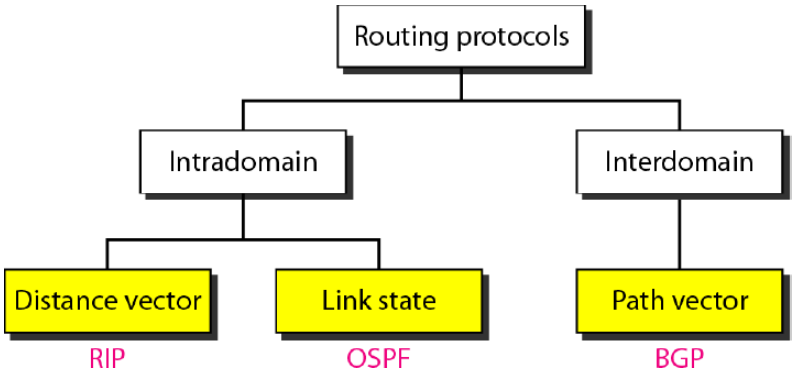
  to the network as a whole.
- Sending a message to such a group is called multicasting, and its routing algorithm is called multicast routing.

- Multicasting requires group management. Some way is needed to create and destroy groups, and to allow processes to

  join and leave groups.
- How these tasks are accomplished is not based on the routing algorithm. It is based on the fact that when a process joins a group, it informs its host of this fact. It is important that routers know which of their hosts belong to which groups.
- Either hosts must inform their routers about changes in group membership, or routers must query their hosts periodically. Either way, routers learn about which of their hosts are in which groups. Routers tell their neighbors, so the information propagates through the subnet.
- Multicasting- applications: distributed database, teleconferencing, distance learning, information dissemination etc

Routing Protocols

- Routing protocol specifies how routers communicate with Each other
- An autonomous system (AS) is a group of networks and routers under the authority of a single administration.
- Routing inside an autonomous system is called intra-domain routing.
- Routing between autonomous systems is called inter-domain routing



- Routing Information Protocol (RIP) is an implementation of the distance vector protocol.
- Open Shortest Path First (OSPF) is an implementation of the link state protocol.
- Border Gateway Protocol (BGP) is an implementation of the path vector protocol

1. Routing Information Protocol (RIP)

- An intra domain routing protocol
- Straightforward implementation of Distance Vector Routing
- Hop count as a Routing

metric for RIP Hope

count:

- Hop count is the number of routers occurring in between the source and destination network.
- RIP prevents routing loops by limiting the number of hops allowed in a path from source and destination.
- The maximum hop count for RIP is 15
- hop count of 16 is considered as network unreachable.

advantages of a RIP protocol:

- It is easy to configure
- It has less complexity
- The CPU utilization is less.

Features of RIP

1. Updates of the network are exchanged periodically.
2. Updates (routing information) are always broadcast.
3. Full routing tables are sent in updates.
4. Routers always trust routing information received from neighbor routers. This is also known as Routing on rumors.

RIP Problems

- RIP takes a long time to stabilize
  - Even for a small network, it takes several minutes until the routing tables have settled after a change
- RIP has all the problems of distance vector algorithms, e.g., count-to-Infinity
  - RIP uses split horizon to avoid count-to-infinity
- The maximum path in RIP is 15 hops

In brief **the RIP protocol works** as follows:

- Each router initializes its **routing table** with a list of locally connected networks. Periodically, each router advertises the entire contents of its routing table over all of its RIP-enabled interfaces.
- Whenever a RIP router receives such an advertisement, it puts all of the appropriate routes into its routing table and begins using it to forward packets. This process **ensures** that every network connected to every router eventually becomes known to all routers.
- If a router does not continue to receive advertisements for a remote route, it eventually times out that route and stops forwarding packets over it.
- Every route has a property called **a metric**, which indicates the "distance" to the route's destination.
- Every time a router receives a route advertisement, it increments the metric.
- The **maximum metric** permitted by RIP is 16, which means that a route is unreachable. Ie., the protocol cannot scale to
  networks more than 15 hops to a given destination.
- RIP also includes some **optimizations** of this basic algorithm to improve stabilization of the routing database and to eliminate routing loops.
  - When a route is determined to be **unreachable**, RIP routers do not delete it straightaway. Instead they continue to
    advertise the route with a metric of 16 (unreachable).
  - A **"Request"** message allows a newly-started router to rapidly query all of its neighbours' routing tables.

RIP messages:---------

Request

- A request message is sent by a router that has just come up or by a router that has some time-out entries
- A request can ask about specific entries or all entries

Response

- A response can be either solicited (ask for a proposal) or unsolicited (30s or when there is a change in the routing table)

RIP Timers

✓ *Periodic timer*

- It controls the advertising of regular update message (25 ~ 30 sec)

✓ *Expiration timer*

- It governs the validity of a route (180 sec)

✓ *Garbage collection timer*

- An invalid route is not purged(remove that not in use) from the routing table until this timer expires (120 sec)

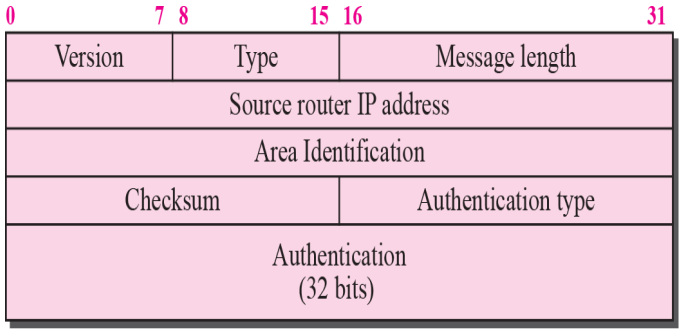
❑ OSPF (Open Shortest Path First) protocol

- The OSPF protocol is one of a family of IP Routing protocols
- The Open Shortest Path First (OSPF) protocol is an intra-domain routing protocol based on link state routing.
- It Divides an autonomous system(AS) into areas to handle routing efficiently
- At the Border of an area, special routers called area border routers summarize the information about area and send to other areas. All areas inside AS connected to a special area called backbone. Routers inside backbone are called backbone routers
- OSPF allows to assign a cost called metric to each route
- This Metric based on type of service : Minimum delay , maximum throughput, reliability, etc.
- Connection is called a link.
- 4 types of link: point to point,transient,stub,virtual

Features of OSPF

- Provides **authentication** of routing messages
- Enables **load balancing** by allowing traffic to be split evenly across routes with equal cost
- Supports **subnetting** (is the practice of dividing a network into two or smaller networks)
- Supports **multicasting**
- Allows **hierarchical routing**
- Handles **error detection** by itself

OSPF Packet format :



- **Version**: version of the OSPF
- **Type** : It specifies the type of the packets, there are 4 types

  of packets

  * hello packet
  * link state request
  * link state update
  * Link state acknowledgement
- **Source address** :It defines the address of the node to be send.
- **Area id :** It specifies ID of different areas
- **Check sum** :It deals with error detection and correction
- **Authentication type** :It has two value either zero or other

  numbers except zero
- **Authentication data:** used by authentication procedure

The five types of OSPF messages

Message type	Description
Hello	Used to discover who the neighbors are
Link state update	Provides the sender's costs to its neighbors
Link state ack	Acknowledges link state update
Database description	Announces which updates the sender has
Link state request	Requests information from the partner

Neethu Mathew , CSE Dept. EKCTC

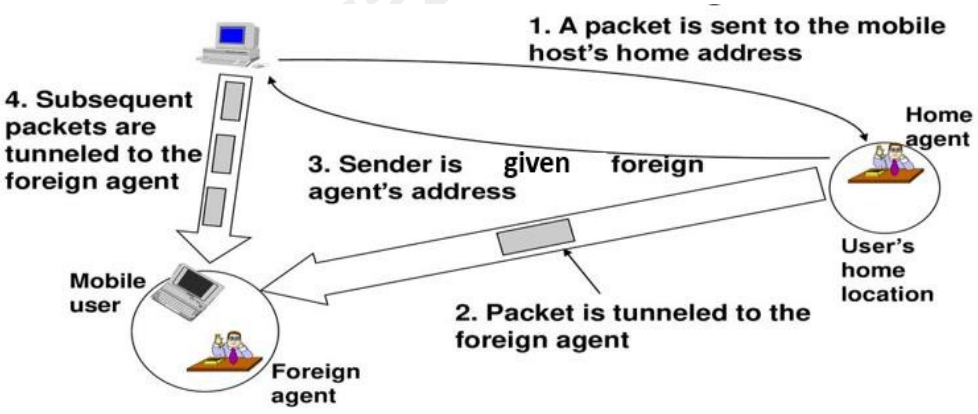
Comparison of RIP and OSPF

RIP	OSPF
It is a distance vector protocol	It is a link state protocol
The metrics used in RIP is hop count	The metrics used in OSPF are bandwidth and delay
RIP uses distance vector algorithm to calculate the best path	OSPF uses the SPF algorithm to calculate the best path
In RIP protocol, networks are not divided in areas or tables	In OSPF, routing is carried out in autonomous system, into areas, sub areas as well as backbone areas
Maximum hop count is 15	No hop count

ROUTING FOR MOBILE HOST

- Millions of people have portable computers nowadays, and they generally want to read their email and access their normal file systems wherever in the world they may be. These mobile hosts introduce a new complication: to route a packet to a mobile host, the network first has to find it.
- Hosts that never move are said to be stationary. They are connected to the network by copper wires or fiber optics. In contrast, we can distinguish two other kinds of hosts. Migratory hosts are basically stationary hosts who move from one fixed site to another from time to time but use the network only when they are physically connected to it. Roaming hosts actually compute on the run and want to maintain their connections as they move around. We will use the term mobile hosts to mean either of the latter two categories, that is, all hosts that are away from home and still want to be connected.
- All hosts are assumed to have a permanent home location that never changes.
- The routing goal in systems with mobile hosts is to make it possible to send packets to mobile hosts using their home addresses and have the packets efficiently reach them wherever they may be. The trick, of course, is to find them
- the world is divided up (geographically) into small units. Let us call them areas, where an area is typically a LAN or wireless cell. Each area has one or more foreign agents, which are processes that keep track of all mobile hosts visiting the area. In addition, each area has a home agent, which keeps track of hosts whose home is in the area, but who are currently visiting another area.

Neethu Mathew , CSE Dept. EKCTC



Neethu Mathew , CSE Dept. EKCTC

When a new host enters an area, either by connecting to it or just wandering into the cell, his computer must register itself with the foreign agent there.

The registration procedure typically works like this:

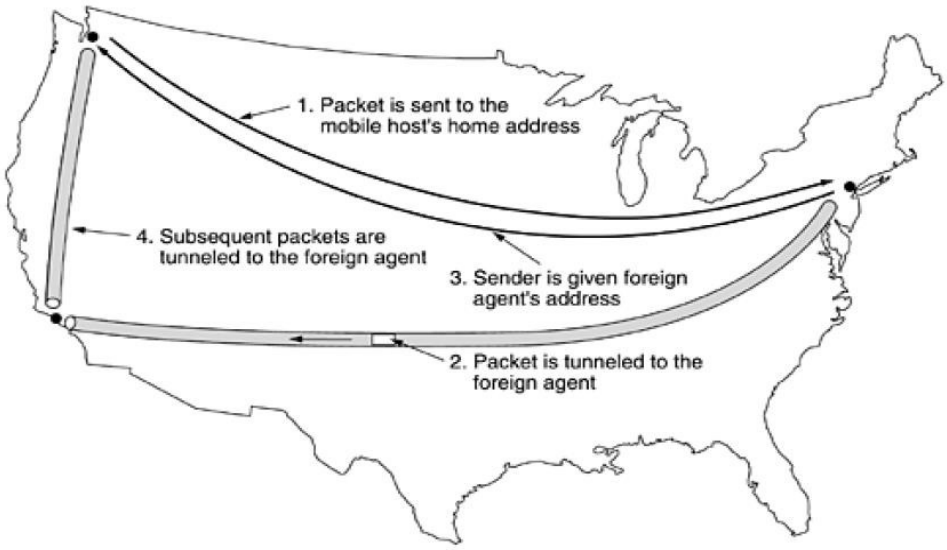
- 1) Periodically, each foreign agent broadcasts a packet announcing its existence and address. A newly arrived mobile host may wait for one these messages, but if one arrives quickly enough, the mobile host can broadcast a packet saying:" are there any foreign agent around? "
- 2) The mobile host just register with the foreign agent, giving its home address, current data link layer address, and some

  security information.
- 3) The foreign agent contacts the mobile hosts home agent and says, one of your hosts is over here, It also includes the

  security information, to convince the home agent that the mobile hosts are really there.
- 4) The home agent examines the security information, which contains a timestamp, to prove that it was generated within the past few seconds. If it is happy, it tells the foreign agent to proceed.
- 5) When the foreign agent gets the acknowledgement from the home agent, it makes an entry in its table and informs the

  mobile hosts that it is now registered.

Fig :Packet routing for mobile hosts



- When a packet is sent to a mobile host, it is routed to the host's home LAN because that is what the address says should be done, as illustrated in step 1 of following figure. Here the sender, in the northwest city of Seattle, wants to send a packet to a host normally across the United States in New York. Packets sent to the mobile host on its home LAN in New York are intercepted by the home agent there. The home agent then looks up the mobile host's new (temporary) location and finds the address of the foreign agent handling the mobile host, in Los Angeles.

- The home agent then does two things.
- First, it encapsulates the packet in the payload field of an outer packet and sends the latter to the foreign agent (step 2 in Fig.).
- This mechanism is called tunneling;
- After getting the encapsulated packet, the foreign agent removes the original packet from the payload field and sends it to the mobile host as a data link frame.
- Second, the home agent tells the sender to henceforth send packets to the mobile host by encapsulating them in the payload of packets explicitly addressed to the foreign agent instead of just sending them to the mobile host's home address (step 3).
- Subsequent packets can now be routed directly to the host via the foreign agent (step 4), bypassing the home location entirely.

Congestion

- Synonymous to traffic jam in networks
- When too many packets are present in the subnet, performance degrades. This situation is called **congestion**.
- **Congestion** in a network may occur when the load on the network (no. of packets a network can handle) is greater than capacity of the network.
- **Congestion control** refers to the mechanisms and techniques to control the congestion and keep the load below the capacity
- Congestion control is a process of maintaining the number of packets in the network below a certain level at which performance falls off dramatically.

Causes of congestion

How Congestions Happens ?

The following factors responsible for congestion:

- Insufficient memory to store arriving packets
- Slow network links
- Slow processors
- Mismatch between system parts
- Shortage of buffer space

General Principles of Congestion Control

- Solutions to congestion problems can be divided into two categories:
  - ✓ **open loop**
  - ✓ **closed loop.**
- Congestion control refers to the techniques & mechanisms which can either prevent congestion from happening or remove congestion after it has taken place.
- Open loop congestion control is based on prevention of congestion whereas the closed loop solutions are for removing the congestion

Open loop:

- Open loop solutions try to solve the problems by excellent design to prevent the congestion from happening
- Open loop control is exercised by using the tools such as deciding when to accept the new packets,when to discard the packets, which packets are to be discarded and making the scheduling decisions at various points.
- Open loop solutions attempt to solve the problem by good design, to make sure it does not occur in the first place. Once

  the system is up and running, midcourse corrections are not made.

Closed loop:-

- Closed loop congestion control uses some kind of feedback.
- This approach has three parts when applied to congestion control.

1) Detect when and where congestion occurs by Monitoring the system.

2) Pass information about congestion to places where action can be taken.

3) Adjust system operations to correct the problem.

Congestion Prevention Policies

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

1. Policies Related to Data Link Layer

(i) Retransmission Policy

The retransmission policy and the retransmission timers must be designed to optimise efficiency and at the same time prevent congestion. The retransmission policy deals with how fast a sender times out. If a sender times out early then it will retransmit all the packets which can lead to congestion. Using retransmission policy, we can avoid this and prevent congestion.

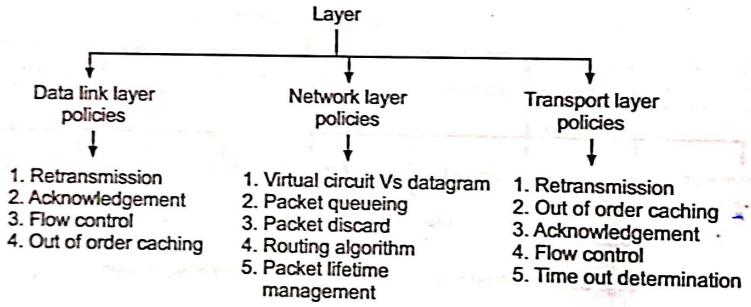


Fig. 9.19. Policies affecting the congestion

(ii) Out of Order Caching Policy

If the receiver routinely discard all the packets which are out of order, then retransmission of these packets will take place. This will increase the load and result in congestion.

(iii) Acknowledgement Policy

If each received packet is acknowledged immediately then the acknowledgement packets will increase the traffic. If the acknowledgement is delayed (piggybacking) then there is a possibility of time out and retransmission. Therefore, a tight flow control has to be exercised to avoid congestion.

(iv) 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.

2. Policies Related to Network Layer

(i) Choice between Virtual Circuit and Datagrams

This choice at the network layer will affect the congestion because several congestion control algorithms work only with virtual circuit subnets.

(ii) Packet Queueing and Service

This policy is related to whether the routers have one queue per input line and one queue per output line or both. The policy is also related to the order in which the packets are processed e.g. round robin or priority based etc.

(iii) Discard Policy

This policy lays a rule which tells the routers about which packet is to be discarded. A good discard policy can prevent congestion and a bad one will worsen the situation.

(iv) Routing Algorithms

The routing algorithms can spread the traffic over all the lines to avoid congestion.

(v) Package lifetime management

The policy decides the time for which a packet may live before being discarded. This time should be of adequate value so that congestion can be avoided.

3. Policies Related to Transport Layer

The policies at the transport layer are same as those at the data link layer. But at transport layer determining the time out interval is more difficult. If it is too short then extra packets are sent unnecessarily whereas if it is too long, congestion will get reduced at the cost of increased response time.

Traffic Shaping

One of the important reason behind congestion is the burstly nature of the traffic. If the traffic has a uniform data rate than congestion could be less common. Traffic shaping is an open loop control. It manages the congestion by forcing the packet transmission rate to be more predictable. Thus, traffic shaping will regulate the average rate or the burstness of data transmission. Monitoring a traffic flow is called as **traffic policing.** Cleck if a packet stream (connection) obeys its descriptor, and if it violates its descriptor, give penalty. For this, the network may want to monitor the traffic flow during the connection period. The process of monitoring and enforcing the traffic flow is called traffic policing. Penalty will be :

(i) Drop packets that violate the descriptor

(ii) Give low priority to them.

9.11.6. Congestion Control in Virtual Circuit Subnets

All the congestion control techniques discussed till now were open loop techniques. Now, let us discuss a dynamic technique called **admission control.**

1. Admission Control Principle

This technique is used to keep the congestion which has already begun to a manageable level. Its principle is as follows : once congestion has been detected, do not set up any more virtual circuits until the congestion is cleared. The advantage is that it is a simple and easy to carry out control.

2. Alternative Approach

An alternative approach to admission control is to allow the virtual circuits to set up even when a congestion has taken place. However, carefully route all the new virtual circuits around the problem area.

9.12. CONGESTION CONTROL IN DATAGRAM SUBNETS

Now, let us discuss some congestion control approaches which can be used in the datagram subnets (and also in virtual circuit subnets).

(i) Choke packets

(ii) Load shedding

(iii) Jitter control.

9.12.1. Choke Packets

This approach can be used in virtual circuits as well as in the datagram subnets. In this technique, each router associates a real variable with each of its output lines. This real variable say u has a value between 0 and 1 and it indicates the percentage utilization of that line. If the value of u goes above the threshold then the output line will enter into a warning state. The router will check each newly arriving packet to see if its output line is in the warning state. If it is in the warning state then the router will send back a **choke packet** signal to the sending host. The sender host will not generate any more choke packets. Several variations on the congestion control algorithm have been proposed, depending on the value of thresholds.

Depending upon the threshold value, the choke packets can contain a mild warning, a sterm warning or an ultimatum. Another variation can be in terms of queue lengths or buffer utilization instead of using the line utilization as a deciding factor.

Drawback

The problem with choke packet technique is that the action to be taken by the source host on receiving a choke packet is voluntary and not compulsory.

9.12.2. Load Shedding

Admission control, choke packets, fair queueing are the techniques suitable for light congestion. But if these techniques cannot make the congestion to disappear, then the load shedding technique is to be used. The principle of load shedding states that when the routers are being inaundated by the packets that they cannot handle, they should simply throw the packets away. A router which is flooding with packets due to congestion can drop any packet at random. But there are better ways of doing this. The policy for dropping a packet depends on the type of packet. For file transfer, an old packet is more important than a new packet. In contrast, for multimedia a new packet is more important than an old one. Hence, the policy for file transfer called wine (old is better than new) and that for the multimedia is called milk (new is better than old). An intelligent discard policy can be decided depending on the applications. To implement such an intelligent discard policy, co-operation from the sender is essential. The application should mark their packets in priority classes to indicate how important they are.

If this is done then when the packets are to be discarded the routers can first drop packets from lowest class (i.e. the packets which are least important). Then the routers will discard the packets from next lower class and so on. One or more header bits are required to put the priority for making the class of a packet. In every ATM cell, 1 bit is reserved in the header for marking the priority. Every ATM cell is labeled either as a low priority or high priority.

9.12.3. Jitter Control

1. Definition of Jitter

Jitter may be defined as the variation in delay for the packets belonging to the same flow. The real time audio and video cannot tolerate jitter on the other hand the jitter does not matter if the packets are carrying an information contained in a file. For the audio and video transmission if the packets take 20 msec to 30 msec (delay) to reach the destination, it does not matter, provided that the delay remains constant. The quality of sound or video will be hampered if the delays associated with different packets have different values. Therefore, practically we can say that 99% packets should be delivered with a delay ranging from 24.5 msec to 25.5 msec.

2. Jitter Control

When a packet arrives at a router, the router will check to see whether the packet is behind or ahead and by what time. This information is stored in the packet and updated at every hop. If the packet is ahead of the schedule (early) then the router will hold it for a slightly longer time and if the packet is behind the schedule (late), then the router will try to send it out as quickly as possible. This will help in keeping the average delay per packet constant and will avoid time jitter.

Quality of Service (QoS) - requirements, Techniques for achieving good QoS.

- A stream of packets from a source to a destination is called a flow.
- In a connection-oriented network, all the packets belonging to a flow follow the same route; in a connectionless

  network, they may follow different routes.
- The needs of each flow can be characterized by 4 primary parameters: ***reliability, delay, jitter, and bandwidth***. Together these determine the **QoS (Quality of Service)** the flow requires.

Techniques for Achieving Good Quality of Service

- ❑ Overprovisioning
- ❑ Buffering
- ❑ Traffic Shaping
- ❑ **Leaky bucket algorithm**
- ❑ **Token bucket algorithm**
- ❑ Resource reservation
- ❑ Proportional routing
- ❑ Admission control
- ❑ Packet Scheduling

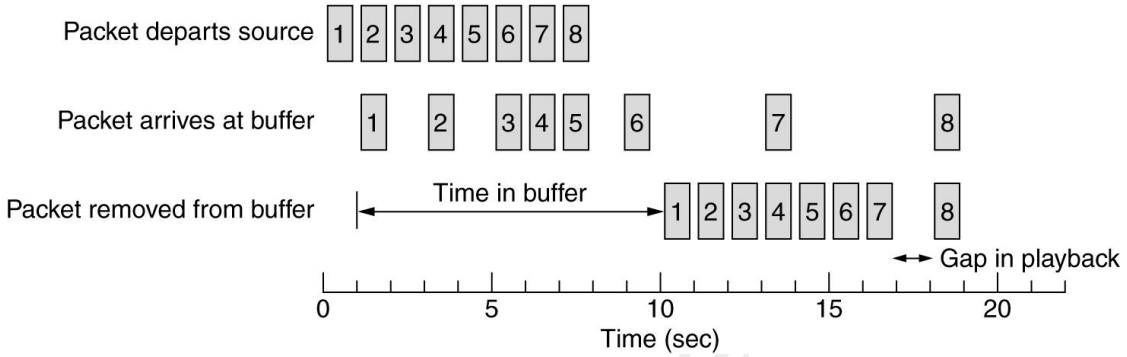
❑ **Overprovisioning :**

- To provide so much router capacity, buffer space, &bandwidth that the packets just fly through easily.
- The trouble with this solution is that it is expensive.
- As time goes on and designers have a better idea of how much is enough, this technique may even become practical.

❑ **Buffering :**

- Flows can be buffered on the receiving side before being delivered.
- Buffering them does not affect the reliability or bandwidth, and increases the delay, but it smooths out the jitter. For audio

  and video on demand, jitter is the main problem, so this technique helps a lot.



Smoothing the output stream by buffering packets.

❑ **Traffic Shaping:**

- One of the main causes of congestion is that traffic is often bursty.
- Traffic shaping is about regulating the average rate (and burstiness) of data transmission.
- Monitoring a traffic flow is called traffic policing.
- Agreeing to a traffic shape and policing it afterward are easier with virtual-circuit subnets than with datagram subnets.
- When a connection is set up, the user and the subnet(i.e., the customer and the carrier) agree on a certain traffic

  pattern (i.e., shape) for that circuit. Sometimes this is called a service level agreement.
- Traffic shaping is a mechanism to control the amount and rate of traffic sent to the network
- The 2 traffic shaping techniques are :-

  ❖ Leaky bucket

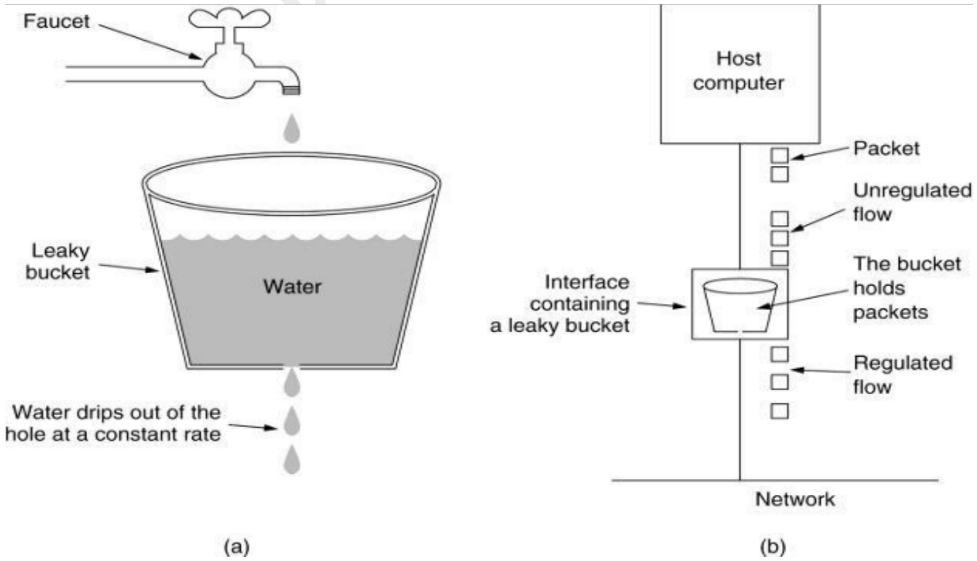
  ❖ Token bucket

❑ Leaky bucket algorithm:-

- It is the algorithm used to control congestion in network traffic
- Its working is similar to a Leaky bucket and hence the name
- Leaky bucket is a bucket with a hole at bottom
- Flow of water from bucket is at a constant rate which is independent of water entering the bucket
- If bucket is full, any additional water entering in the bucket is thrown out
- Same technique is applied to control congestion in network traffic
- Every host in the network is having a buffer with finite queue length
- Packets which are put in the buffer when buffer is full are thrown away. The buffer may drain onto the subnet either

  by some no. of packets per unit time, or by some total no. of bytes per unit time

- Imagine a bucket with a small hole in the bottom, as illustrated in Fig .(a)
- No matter the rate at which water enters the bucket, the outflow is at a constant rate 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
- In practice the bucket is a finite queue that outputs at a finite rate



(a) A leaky bucket with water. **(b) A leaky bucket withpackets**

- Each host is connected to the network by an interface containing a leaky bucket, that is, a finite internal queue.
- If a packet arrives at the queue when it is full, the packet is discarded. In other words, if one or more processes within the host try to send a packet when the maximum number is already queued, the new packet is discarded. This arrangement can be built into the hardware interface or simulated by the host operating system.
- 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, smoothing out bursts and greatly reducing the chances of congestion. The Leaky Bucket algorithm can be implemented for packets or a constant amount of bytes, send within each time interval.
- Conceptually each network interface contains a leaky bucket. And the following steps are performed:
  - When the host has to send a packet, the packet is thrown into the bucket.
  - The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
  - Burst traffic is converted to a uniform traffic by the leaky bucket.

❑ Token bucket algorithm

- A variant on the leaky bucket
- Similar to the leaky bucket but it allows for varying output rates
- This is useful when larger burst of traffic arrive
- In this approach , a token bucket is used to manage the queue regulator that controls the rate of packet flow into the network
- Each token grants the ability to transmit a fixed no. of bytes, if the token bucket fills,newly generated tokens are discarded
- If the flow delivers more packets than the queue can store, the excess packets are discarded
- The leaky bucket algorithm enforces a rigid output pattern at the average rate, no matter how bursty the traffic is. For many applications, it is better to allow the output to speed up somewhat when large bursts arrive. One such algorithm is the token bucket algorithm.

- In this algorithm, the leaky bucket holds tokens, generated by a clock at the rate of one token every T sec.
- In Fig. 4 (a) a bucket is holding three tokens, with five packets waiting to be transmitted.
- For a packet to be transmitted, it must capture and destroy one token.
- In Fig. (b) three of the five packets have gotten through, but the other two are stuck waiting for two more tokens to be generated.

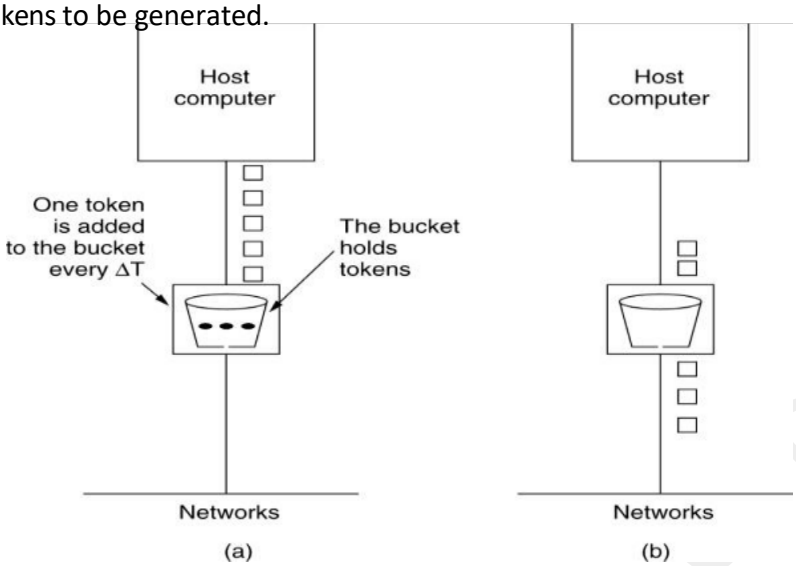


Figure: The token bucket algorithm. (a) Before. (b) After.

❑ **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:

1. Bandwidth.
2. Buffer space.
3. CPU cycles.

❑ **Admission control**

- Admission control refers to the mechanism used by a router, or a switch, to accept or reject a flow based on predefined parameters called flow specifications.
- Before a router accepts a flow for processing, it checks the flow specifications to see if its capacity (in terms of bandwidth, buffer size, CPU speed, etc.) and its previous commitments to other flows can handle the new flow.

❑ **Proportional routing**

- Most routing algorithms try to find the best path for each destination and send all traffic to that destination over the

  best path.
- A different approach that has been proposed to provide a higher quality of service is to split the traffic for each destination over multiple paths.
- Since routers generally do not have a complete overview of network-wide traffic, the only feasible way to split traffic

  over multiple routes is to use locally-available information.
- A simple method is to divide the traffic equally or in proportion to the capacity of the outgoing links.

❑ **Packet Scheduling**

- Packets from different flows arrive at a switch or router for processing.
- A good scheduling technique treats the different flows in a fair and appropriate manner.
- Several scheduling techniques are designed to improve the quality of service.
- Three of them are:
  1. FIFO queuing,
  2. priority queuing,
  3. weighted fair queuing

- In first-in, first-out (FIFO) queuing, packets wait in a buffer (queue) until the node (router or switch) is ready to process them. If the average arrival rate is higher than the average processing rate, the queue will fill up and new packets will be discarded.
- In priority queuing, packets are first assigned to a priority class. Each priority class has its own queue. The packets in the highest-priority queue are processed first. Packets in the lowest-priority queue are processed last. Note that the system does not stop serving a queue until it is empty.
- In weighted fair queuing technique, the packets are still assigned to different classes and admitted to different queues. The queues, however, are weighted based on the priority of the queues; higher priority means a higher weight. The system processes packets in each queue in a round-robin fashion with the number of packets selected from each queue based on the corresponding weight.