UNIT-3

1) Evaluate how Traffic Shaping is important for Quality of Service in Routing.

QoS Traffic Shaping Explained (networklessons.com) (to understand)

Traffic shaping, also known as packet shaping, is a congestion management method that regulates network data transfer by delaying the flow of less important or less desired packets. Traffic shaping attempts to prevent delay, jitter and loss by controlling the burst size and using a leaky bucket algorithm to smooth the output rate over at least eight time intervals.

What is traffic shaping used for?

Traffic shaping is a quality of service (QoS) technique that is configured on network interfaces to allow higher-priority traffic to flow at optimal levels even when the link becomes overutilized. By creating a bandwidth limit for less critical packets, traffic shaping lessens the possibility that more important packets will be delayed or dropped as they leave the interface.

Common uses of traffic shaping include:

- Time-sensitive data may be given priority over traffic that can be delayed briefly, often with little-to-no ill effect.
- In a corporate environment, business-related traffic may be given priority over other traffic.
- A large internet service provider (ISP) may shape traffic based on customer priority.
- An ISP may limit maximum bandwidth consumption for certain applications to reduce costs and create the capacity to take on additional subscribers. This practice can effectively limit a subscriber's "unlimited connection" and is often imposed without notification.
- Traffic shaping is an integral component of the proposed two-tiered internet, in which certain customers or services receive traffic priority for a premium charge.

Importance of traffic shaping

Traffic shaping is important when network uplinks become overwhelmed with data being sent out of an interface. Without traffic shaping, any excess traffic that cannot be sent out of an interface will either be dropped or queued, which can cause delays in all packets. This can result in poor performance of mission-critical applications. The enablement of traffic shaping allows administrators to specify certain applications that are considered less important -- and, therefore, creates intelligence around which packets will be dropped or delayed first. Overall, traffic shaping is one of the most important traffic management techniques for ensuring high network performance.

2) Explain Distance Vector Routing and Link State Routing in detail.

Lec 3.17: Distance vector routing algorithm in hindi | Computer Networks - YouTube, Lec-3.19: Link state routing in computer networks in Hindi - YouTube (to understand)

Distance Vector Routing –

- It is a dynamic routing algorithm in which each router computes distance between itself and each possible destination i.e. its immediate neighbors.
- The router share its knowledge about the whole network to its neighbors and accordingly updates table based on its neighbors.
- The sharing of information with the neighbors takes place at regular intervals.
- It makes use of **Bellman Ford Algorithm** for making routing tables.
- **Problems**
  – Count to infinity problem which can be solved by splitting horizon.
  – Good news spread fast and bad news spread slowly.
  – Persistent looping problem i.e. loop will be there forever.

Link State Routing –

- It is a dynamic routing algorithm in which each router shares knowledge of its neighbors with every other router in the network.
- A router sends its information about its neighbors only to all the routers through flooding.
- Information sharing takes place only whenever there is a change.
- It makes use of **Dijkastra's Algorithm** for making routing tables.
- **Problems**
  – Heavy traffic due to flooding of packets.
  – Flooding can result in infinite looping which can be solved by using **Time to live (TTL)** field.

Comparison between Distance Vector Routing and Link State Routing:

Distance Vector Routing	Link State Routing
--> Bandwidth required is less due to local sharing, small packets and no flooding.	--> Bandwidth required is more due to flooding and sending of large link state packets.
--> Based on local knowledge since it updates table based on information from neighbors.	--> Based on global knowledge i.e. it have knowledge about entire network.
--> Make use of Bellman Ford algo	--> Make use of Dijkastra's algo
--> Traffic is less	--> Traffic is more
--> Converges slowly i.e. good news spread fast and bad news spread slowly.	--> Converges faster.
--> Count to infinity problem.	--> No count to infinity problem.
--> Persistent looping problem i.e. loop will there forever.	--> No persistent loops, only transient loops.
--> Practical implementation is RIP and IGRP.	--> Practical implementation is OSPF and ISIS.

3) Explain network layer design issues in detail.

NETWORK LAYER DESIGN ISSUES - YouTube (to understand)

Network layer is majorly focused on getting packets from the source to the destination, routing error handling and congestion control.

Network layer design issues:

The network layer comes with some design issues they are described as follows:

1. Store and Forward packet switching:

The host sends the packet to the nearest router. This packet is stored there until it has fully arrived once the link is fully processed by verifying the checksum then it is forwarded to the next router till it reaches the destination. This mechanism is called "Store and Forward packet switching."

2. Services provided to Transport Layer:

Through the network/transport layer interface, the network layer transfers it' s services to the transport layer. These services are described below.
But before providing these services to the transfer layer, following goals must be kept in mind:-

- Offering services must not depend on router technology.
- The transport layer needs to be protected from the type, number and topology of the available router.
- The network addresses for the transport layer should use uniform numbering pattern also at LAN and WAN connections.

Based on the connections there are 2 types of services provided:

- **Connectionless –** The routing and insertion of packets into subnet is done individually. No added setup is required.
- **Connection-Oriented –** Subnet must offer reliable service and all the packets must be transmitted over a single route.

3. Implementation of Connectionless Service:

Packet are termed as "datagrams" and corresponding subnet as "datagram subnets". When the message size that has to be transmitted is 4 times the size of the packet, then the network layer divides into 4 packets and transmits each packet to router via a few protocols. Each data packet has a destination address and is routed independently irrespective of the packets.

4. Implementation of Connection Oriented service:

To use a connection-oriented service, first we establish a connection, use it and then release it. In connection-oriented services, the data packets are delivered to the receiver in the same order in which they have been sent by the sender.
It can be done in either two ways:

- **Circuit Switched Connection –** A dedicated physical path or a circuit is established between the communicating nodes and then data stream is transferred.
- **Virtual Circuit Switched Connection –** The data stream is transferred over a packet switched network, in such a way that it seems to the user that there is a dedicated path from the sender to the receiver. A virtual path is established here. While, other connections may also be using the same path.

4) What is the need to change from IPV4 to IPV6?

IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency. Let’s look at how IP version 6 is better than IPv4:

1. More Efficient Routing – IPv6 reduces the size of routing tables and makes routing more efficient and hierarchical. In IPv6 networks, fragmentation is handled by the source device, rather than a router, using a protocol for discovery of the path’s maximum transmission unit.

2. More efficient packet processing – Compared with the IPv4, IPv6 contains no IP-level checksum, so the checksum does not need to be recalculated at every router hop.

3. Directed Data Flows – IPv6 supports multicast rather than broadcast. Multicast allows bandwidth-intensive packet flows to be sent to multiple destinations simultaneously, saving network bandwidth.

4. Simplified network configuration – IPv6 devices can independently auto-configure themselves when connected to other IPv6 devices. Configuration tasks that can be carried out automatically include IP address assignment and device numbering.

5. Security – IPSec security, which provides confidentiality, authentication, and data integrity, is engraved into IPv6.

4) Write IPV6 header and describe its field. (Refer Extra Q.12)

5) Explain Hierarchical Routing with diagram.

Hierarchical routing algorithm - types of routing algorithm - YouTube (to understand)

Hierarchical Routing

This is essentially a 'Divide and Conquer' strategy. The network is divided into different regions and a router for a particular region knows only about its own domain and other routers. Thus, the network is viewed at two levels:

1) The Sub-network level, where each node in a region has information about its peers in the same region and about the region's interface with other regions. Different regions may have different 'local' routing algorithms. Each local algorithm handles the traffic between nodes of the same region and also directs the outgoing packets to the appropriate interface.
2) The Network Level, where each region is considered as a single node connected to its interface nodes. The routing algorithms at this level handle the routing of packets between two interface nodes, and is isolated from intra-regional transfer.

Networks can be organized in hierarchies of many levels; e.g. local networks of a city at one level, the cities of a country at a level above it, and finally the network of all nations.

In Hierarchical routing, the interfaces need to store information about:

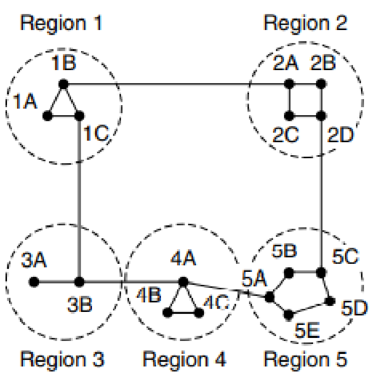
- All nodes in its region which are at one level below it.
- Its peer interfaces.
- At least one interface at a level above it, for outgoing packages.

Advantages of Hierarchical Routing :

- Smaller sizes of routing tables.
- Substantially lesser calculations and updates of routing tables.

Disadvantage :

- Once the hierarchy is imposed on the network, it is followed and possibility of direct paths is ignored. This may lead to sub optimal routing.



(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)

Figure 5-14. Hierarchical routing.

5) Explain Multicast Routing with diagram. (No material)

[Multicast Routing Algorithm - YouTube](to understand)

Multicast Routing Algorithm - YouTube (to understand)

6) Explain the approaches to Congestion Control in Network layer. (No material)

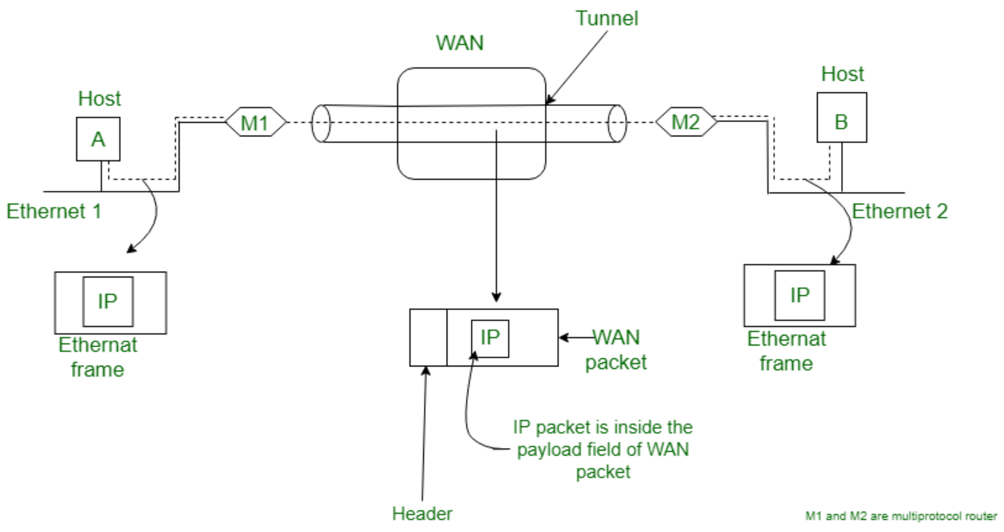
What is Congestion Control ? - YouTube (to understand)

7) Explain Tunneling and Internetwork Routing concept with diagram.

Tunnelling | Computer Networks - YouTube (to understand)

Tunneling

A technique of internetworking called **Tunneling** is used when source and destination networks of same type are to be connected through a network of different type. For example, let us consider an Ethernet to be connected to another Ethernet through a WAN as:



Tunneling

The task is sent on an IP packet from host A of Ethernet-1 to the host B of ethernet-2 via a WAN.

Sequence of events:

1. Host A construct a packet which contains the IP address of Host B.
2. It then inserts this IP packet into an Ethernet frame and this frame is addressed to the multiprotocol router M1
3. Host A then puts this frame on Ethernet.
4. When M1 receives this frame, it removes the IP packet, inserts it in the payload packet of the WAN network layer packet and addresses the WAN packet to M2. The multiprotocol router M2 removes the IP packet and send it to host B in an Ethernet frame.

Internetwork Routing

The following terms are essential to your understanding of routing:

End Systems - As defined by the International Standards Organization (ISO), end systems are network devices without the ability to forward packets between portions of a network. End systems are also known as hosts.

Intermediate Systems - Network devices with the ability to forward packets between portions of a network. Bridges, switches, and routers are examples of intermediate systems.

Network - A portion of the networking infrastructure (encompassing repeaters, hubs, and bridges/Layer 2 switches that is bound by a network layer intermediate system and is associated with the same network layer address.

Router - A network layer intermediate system used to connect networks together based on a common network layer protocol.

Hardware Router - A router that performs routing as a dedicated function and has specific hardware designed and optimized for routing.

Software Router - A router that is not dedicated to performing routing but performs routing as one of multiple processes running on the router computer. The Windows 2000 Server Router Service is a software router.

Internetwork - At least two networks connected using routers. Figure 1.1 illustrates an internetwork.