18CS52 - Mod3

Afnan Marquee

TOPICS

→ The network layer

- What's Inside a Router?
  - Input Processing
  - Switching
  - Output Processing
- Where Does Queuing Occour?
- Routing control Plane
- IPv6
- A Brief foray into IP security
- Routing Algorithms: The link-state (LS) Routing Algorithm
- The Distance-Vector (DV) Routing Algorithm
- Hierarchical Routing
- Routing in the Internet
- Inter-AS Routing in the Internet
- OSPF, BGP Routing
- Routing Broadcast Algorithms and Multicast

8. What do you mean by congestion control mechanism. III

9. Define flow control. Explain how flow is controlled by reciever window and ~~reciever~~ reciever buffer.

10. Suppose that two measured sample RTT values are 106ms and 120ms. I
    i) Compute Estimated RTT after each of these sample RTT value is obtained. Assume $\alpha = 0.125$ and Estimated RTT is 100ms. Just before the first of the samples obtained.
    ii) Compute DeVRTT. Assume $\beta = 0.25$ and DeVRTT is 5ms before first of the samples obtained.

11. Explain how connection establishment and termination is handled by TCP. I

Module 3

1. List and explain three switching techniques with a neat diagram
2. With the help of FSM, describe the sender side and reciever side of rdt 2.0
3. Write the algorithm for the following: II
    i) Link-State
    ii) Distance vector

4. Write a short note on: 11

i) Broadcast routing

ii) Multicast routing

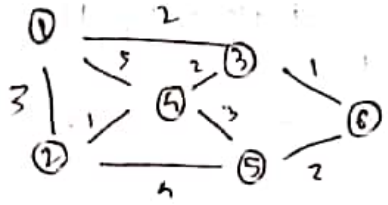
5. Define Routing. What are the goals of routing algorithm 111

6. A host in an organization has an IP address 200.45.34.56 and subnet address mask 200.455.240.0. What is Subnet Address.

7. Explain the format of IPv6 headers. 111

8. Explain OSPF 1

9. Find the shortest path from node 1 using link state algorithm 111



10. Explain RIP (Routing Information Protocol) with its message format. 111

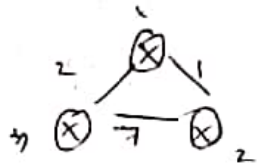
11. Explain spanning tree algorithm with its advantages & disadvantages.

12. What are the message types used in ICMP?

13. Explain IP fragmentation

14. Explain Router architecture 111

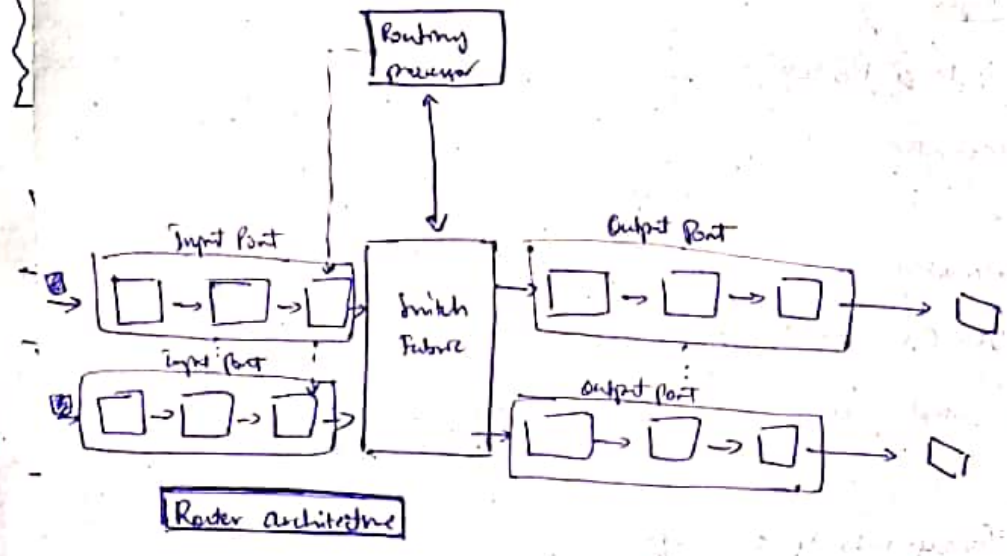
15. Apply distance vector algorithm for the following:



16. Elaborate the path attributes in BGP. and steps to select the BGP routes.

18CS54 - Module 3

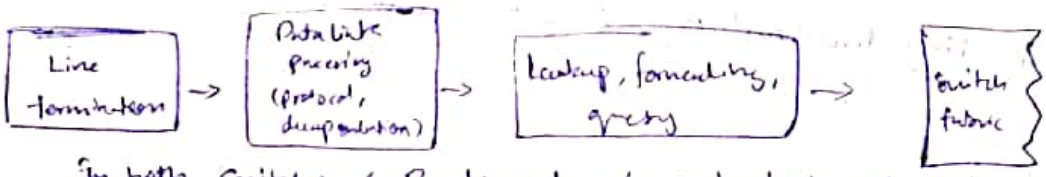
Introduction



Router architecture

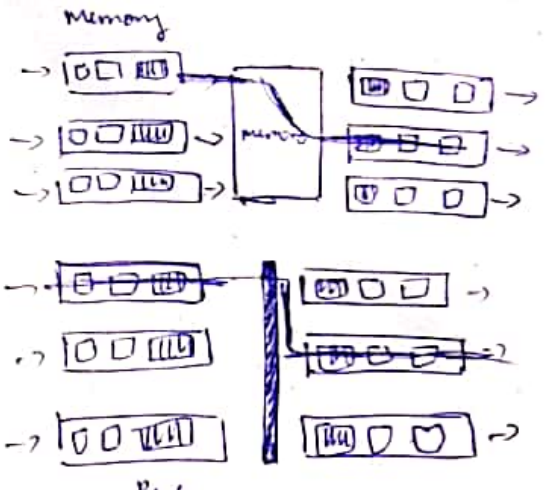
- → Input Port
- → Switching Fabric
- → Output Port
- → Routing processor

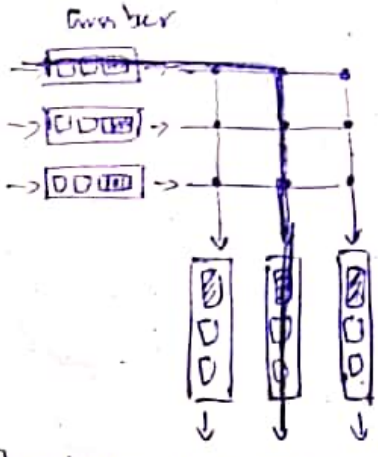
Input Processing



In both switching & Routing header is located and data is sent.

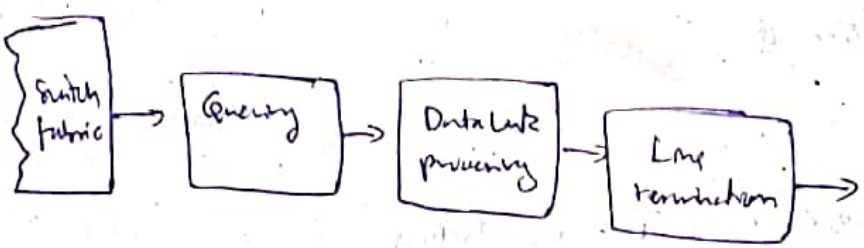
Switching





Three types of switching

Output Processing



Where does Queuing occur?

→ Both at input and output ports

→ Rswitch and Rline is used, each per switch should be cleared before next batch arrives.

→ Packet scheduler - chooses one packet among those queued for transmission.

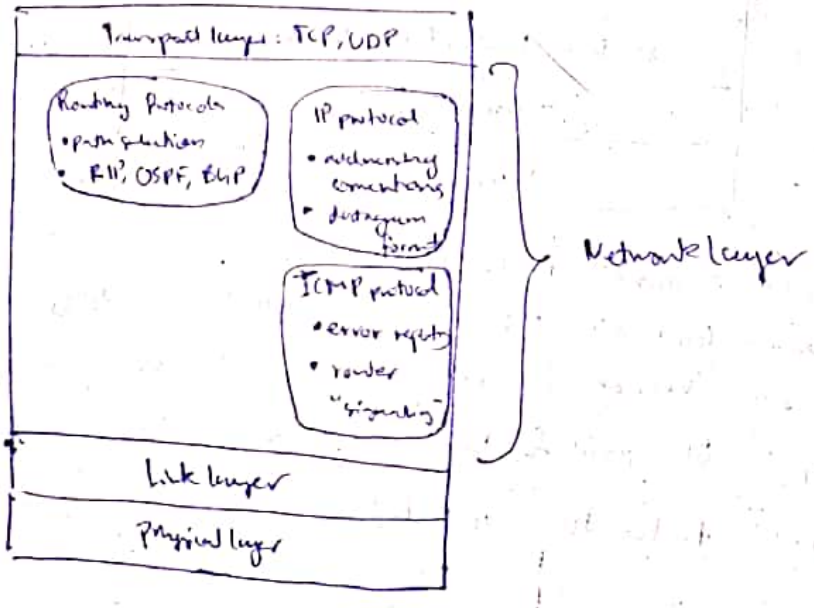
→ AQM (Active Queue Management) and RED (Random Early Detection) algorithms are used.

Internet Protocol (IP)

→ Responsible for protocoling, forwarding & delivery of a packet at network layer.

→ Connectionless & connectionless protocol.

→ IP does not provide flow control / error control & congestion control.



IP has two important components

- Internet addressing and
- Forwarding

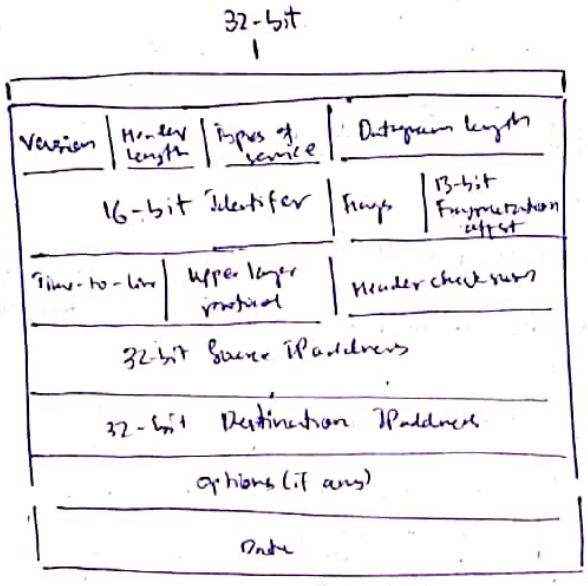
There are two versions of IP in use today

1) IP version 4 (IPv4) and
2) IP version 6 (IPv6)

There are three major components:

1) IP protocol
2) Routing component determines the path a packet follows
3) Network-layer is a facility to report errors in datagrams.

IPv4 datagram format



Payload : Contains data to be delivered
Header : Contains information essential to routing & delivery
Version : Version of IPv4 datagram i.e. 4
Flags : 3bit field for fragment values
Protocol : Rules to transfer data.

IP datagram Fragmentation

-> Size of packet is determined by the network, data is divided into packets (also called fragments)

-> Each fragment is routed independently.

Fields related to Fragmentation & Reassembly

-> Identification

-> Flags

-> Fragmentation offset (identifies location of a fragment)

IPv4 addressing

-> IP address is divided into two parts: Network ID (NID) & Host ID (HID)

-> All hosts are connected to same network.

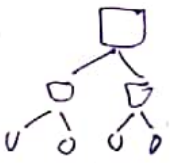
-> IP address version 4 uses 32-bit addresses written as

10000000	10000111	01000100	00000101
128	135	68	5

is written as 128.135.68.5

-> Classful IP addressing: divided into four classes A, B, C, D and E

- Limitation of classful addressing is that its hard to manage all 64,000 hosts
- Solution: Use subnetting



Network no.	Subnet ID	Host ID

- How to subnet an IP address?

IP address: 10010110 01100100 00001100 10110000

Subnet mask: 11111111 11111111 11111111 10000000

Subnet no.: 10010110 01100100 00001100 10000000 (150.100.12.128)

This no. (150.100.12.176) is used to mask the packet to correct subnet in an work organization.

CIDR (Classless Interdomain Routing)

-> Advantage is that a single IP address can be used to designate many unique IP address. This is called supernetting.

-> CIDR ends with a slash to differentiate it from normal IP address.

Obtaining Block of Addresses

-> To obtain a block of IP addresses for use within an organization's subnet, a network administrator contacts the ISP.

-> It is managed under ICANN
  - to allocate IP addresses
  - to manage DNS servers
  - to assign domain names and resolve domain name disputes
  - to allocate addresses to regional Internet registeries.

Obtaining a host address: DHCP

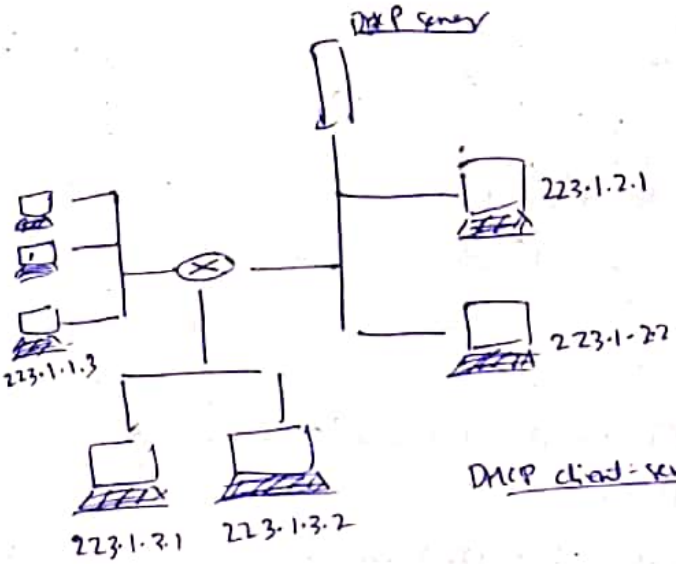
Two ways of assign IP address to a host:

1- Manual configuration

2- Dynamic Host Configuration Protocol.

DHCP protocol

- It enables auto-configuration of IP addresses to host
- It is a dynamic protocol
- It is client-server protocol.
- Each subnet has a DHCP Server.



DHCP client-server scenario

- DHCP protocol is a 4 step process:
  - -> DHCP server discovery
  - -> DHCP server offer
  - -> DHCP request
  - -> DHCP ACK

NAT (Network Address Translation)

- It enables hosts to use Internet without the need to have globally unique addresses.
- It enables an organization to have large set of addresses internally and one address externally.
- Allows public/private connection.
- Single IP address represents the entire group of computers

ICMP (Internet Control Message Protocol)

-> It is a network layer protocol
-> This is used to handle error and other control messages
-> It does not correct the error, but just reports the error to the source.
-> 2 types of ICMP are defined:

0 -> echo reply
3 -> destination network unreachable
4 -> Source congestion control etc.

IPv6

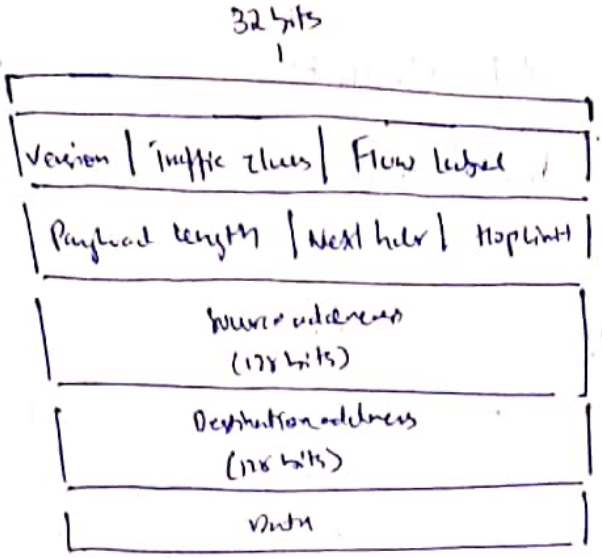
-> CIDR, subnetting and NAT could not solve address space exhaustion faced by IPv4.
-> IPv6 was evolved to solve this problem.

changes from IPv4 to IPv6

-> Expanded Addressing Capabilities
- IPv6 increases the size of IP address from 32 to 128 bits
- More flexible

-> Flow & labelling Priority
- Group similar things
  for ex: Audio and video transmission may be considered as same flow.

IPv6 datagram Format



The fields are: Version, Traffic class, Flow label, Payload length, Next header, Hop limit, Data.

The fields not present in IPv6 but present in IPv4: Fragmentation is done only by source but not by routers. Header checksum is used to perform checksumming, this functionality was removed to speed up the processing in the router.

Difference between IPv4 & IPv6

IPv4	IPv6
• IPv4 addresses are 32 bit length	IPv6 addresses are 128 bit length
• Fragmentation is done by routers sender and forwarding routers	Fragmentation is done only by sender
• Does not identify packet flow for QoS handling	Contains flow label for QoS handling
• Includes options upto 40 bytes	Extension headers used for optional data
• Includes checksum	Does not include checksum

• ARP is available	ARP is replaced
• Broadcast messages are available	Broadcast messages are not available
• Manual Configuration	Auto configuration
• IPSec is optional	IPSec is required.

Transition from IPv4 to IPv6

1) Dual Stack
2) Tunneling

Dual Stack:

- It has both IPv4 / IPv6 nodes.
  When operating with IPv6 / IPv6 addresses
  and the same goes for IPv4.
- At each point IPv4 ↔ IPv6 changes are required.

Tunneling

- The intervening - set of IPv4 routers b/w two IPv6 routers are referred as a tunnel.

IP security

- IPsec is a popular secure network-layer protocol
- It is widely deployed in Virtual Private Networks.
- Compatible with IPv4 & IPv6
- On the source side:
  1) Encryption of segment
  2) Appends additional security
  3) Encapsulates resulting payload in a IP datagram.
- On destination side:
  1) Recieves datagram from Internet
  2) Decryption
  3) Passes to transport layer.

Routing Algorithms

-> Finding a good path from source to destination
-> Good path has the least cost.

Routing Algorithm classification

1) Global or decentralized
2) Static or dynamic
3) Load-sensitive or Load-insensitive.

Global or Decentralized Global Routing Algorithm

-> This algorithm has complete knowledge about the network and the least-cost path is determined.

Decentralized Routing Algorithm

-> No node has complete information about all the cost of network links
-> Each node has only the knowledge of the costs of its own directly attached links

Static or Dynamic Routing

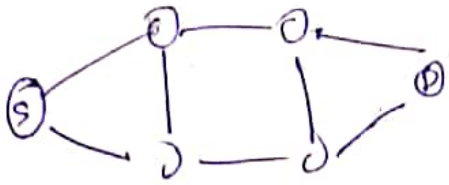
-> Static Routes change very slow over time
-> Dynamic Route change periodically or in response to topology change / link change.

Load sensitive or Load insensitive Algorithms

-> Load sensitive : Link costs vary dynamically
-> Load insensitive: Link costs do not reflect the current level of congestion.

LS routing algorithm | Dijkstra's algorithm

Dijkstra's algorithm computes the least-cost path from one node to all other nodes in the network.



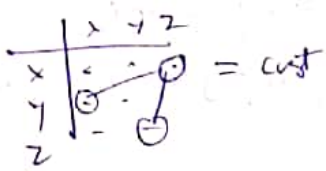
Dijkstra's algorithm calculates least cost path from s to d. and all other nodes too.

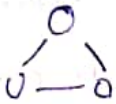
DV Routing Algorithm Bellman Ford Algorithm

Distance Vector (DV) algorithm is i) iterative
ii) Asynchronous
iii) Distributed

Distance vector calculates the the cost of path to all nodes from all nodes, through all nodes.

Node Table





Graph

A comparison of LS and DV Routing-algorithms:

Distance Vector Protocol	Link State Protocol
Entire routing-table is sent as an update	Updates are incremental & entire routing table is not sent an update.
Distance-vector protocol send periodic update every 30 to 90 second	Updates are triggered not periodic.
Updates are broadcasted	Updates are multicasted
Updates are sent to directly connected neighbors only	Updates are sent to entire network to just directly connected neighbour
Routers do not have end-end visibility of entire network	Routers have visibility of entire network of that area only.
Prone to routing loops	No routing loops
Each node talks to only its directly connected neighbours	Each node talks with all other nodes

Hierarchical Routing

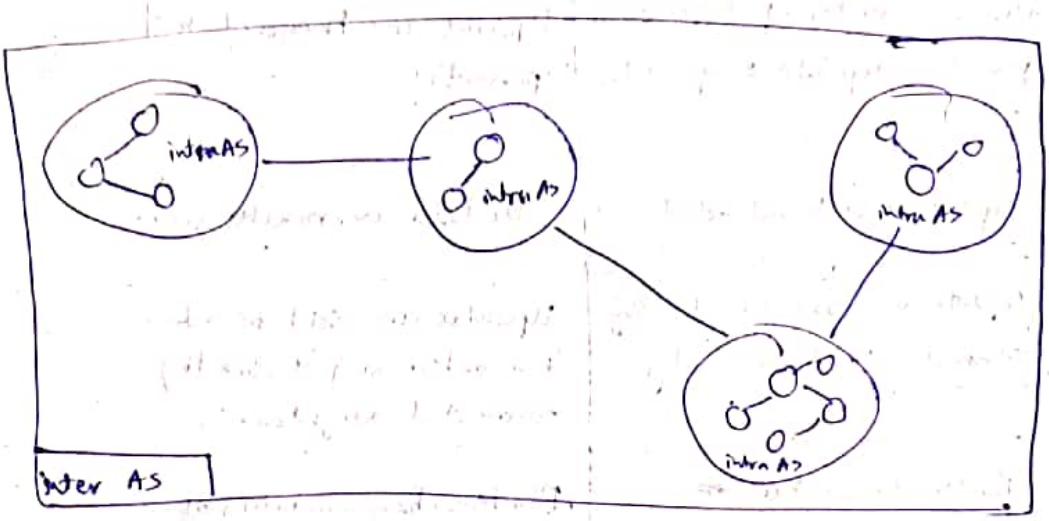
- Two problems of a simple-routing algorithms:
  - As the no. of routers increase, overhead involved in computing & storing routing info increases.
  - An organization should be able to run and administer its network. At the same time, the organization should be able to connect its network to internet.

Both of these 2 problems can be solved by organizing routers into autonomous-system (AS).

-> Two types of routing protocol:

1) Intra AS routing protocol: refers to routing inside an autonomous system.

2) Inter AS routing protocol: refers to routing between autonomous system.



Routing in the Internet

-> The purpose of routing is to determine the path ~~time~~ which takes the least time to reach from source to destination.

-> IntraAS, also known as Interior gateway protocols. It is used to determine how routing is performed within an AS.

Most common intra-AS routing protocols:

① Routing Information Protocol

② Open shortest Path First

Routing Information Protocol

- Widely used for intra-AS routing in the Internet
- Distance vector Protocol. Uses hopcount as cost metric.
- Calculates the shortest path distance from router to subnets.

- Routing table is used which has

Destination Subnet	Next Router	Number of Hops to destination
—	—	—
—	—	—
—	—	—
:	:	:

- Routers can send 1) Response Message
  2) Request Message

Open Shortest Path First

- OSPF is a Link state protocol.
- It uses flooding of link state information and Dijkstra's Least cost path algorithm
- Here is how it works:
  i) Router constructs a complete topological map of the system
  ii) It runs the Dijkstra's Algorithm to determine a shortest paths to all subnets
  iii) It updates any changes in 3 every 30 mins by broadcasting the changes to all the nodes.
- Advantages include:
  1) Security
  2) Multiple Same cost paths could be used
  3) Integrated Support for Unicast & Multicast Routing
  4) Support for Hierarchy within a single Routing Domain.

BGP

- BGP is widely used for inter AS routing
- Obtain subnet reachability information, Propagate, determine good routes to subnets based on i) Reachability information and ii) AS policy.
- Pairs of routers exchange routing information over semi permanent TCP connections using port - 179.
- Two routers are called Peers.
- There are two types of session:
  - i) External BGP (eBGP) session
  - ii) Internal BGP (iBGP) session

Path attributes & Routes:

- An autonomous-system is identified by its globally unique ASN (Autonomous-System Number)
- It has a prefix across a session.
- Two important attributes: 1) AS-PATH
  2) NEXT-HOP

AS-PATH

- Routers use the AS-PATH attribute to detect and prevent looping advertisments.
- Routers also use the AS-Path attribute in choosing among multiple paths to the same prefix.

NEXT HOP

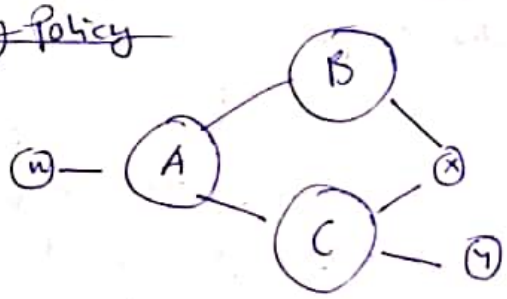
- It provides a critical link between the inter-AS and intra-AS routing protocols.

- Inbound route policy decides whether to accept or filter the route and whether to set certain attributes such as the router preference metrics.

* Route Selection

- For 2 or more ~~routes~~ routes to the same prefix, the following elimination rules are invoked.
  1) The Route with the shortest AS-PATH is selected.
  2) If more than one route still remains, the closest NEXT-HOP router is selected else BGP identifier is used to select the route.

Routing Policy



provider network

customer network

- Let A, B, C, W, X & Y = six interconnected autonomous systems.
  W, X & Y = three stub-networks.
  A, B & C = three backbone providers networks.
- All traffic entering a stub-network must be ~~Approved~~ for that network.
- X itself may be source / destination of all traffic leaving / entering X.
- There are currently no official standards that govern how backbone ISPs route among themselves.

Broadcast & Multicast Routing Broadcast Routing Algorithms

- Broadcast routing means sending a message from source node to all other nodes.

N-Way Unicast

- Given N destination-nodes, the source node makes N copies of the packet and transmits then the N copies to N destinations using unicast routing.

Uncontrolled Flooding

- The source node sends a copy of the packet to all the neighbours
- In a connected graph, a copy of the broadcast packet is delivered to all nodes in the graph.

Controlled Flooding

- A node can avoid a broadcast-storm by choosing when to flood a packet and when not to flood a packet.
- Two methods for controlled flooding:
  1) Sequence no. controlled flooding
     - Source node puts its address as well as broadcast no. into a broadcast packet and sends packet to all neighbours.
     - Each node maintains a list of the source-address & sequence of each broad-cast packet.
     - If a router has already received a packet, it will drop it.

Spanning Tree Broadcast

- A spanning tree where cost is minimum of all of the graph's spanning trees is called a MST.

- Here is how it works

  -> Firstly, the nodes construct a spanning tree
  -> The node sends broadcast-packet out on all incident links that belong to the spanning tree.
  -> The receiving-node forwards the broadcast packet to all neighbours in the spanning tree.

Center Based Approach

- This is a method used for building a spanning tree.
- Here is how it works:

  1) A center-node is defined
  2) Then, the nodes send unicast tree-join messages to the center node.
  3) Finally, tree-join message is forwarded toward the center. until the message either
     -> arrives at a node that already belongs to the spanning-tree or
     -> Arrives at the center.

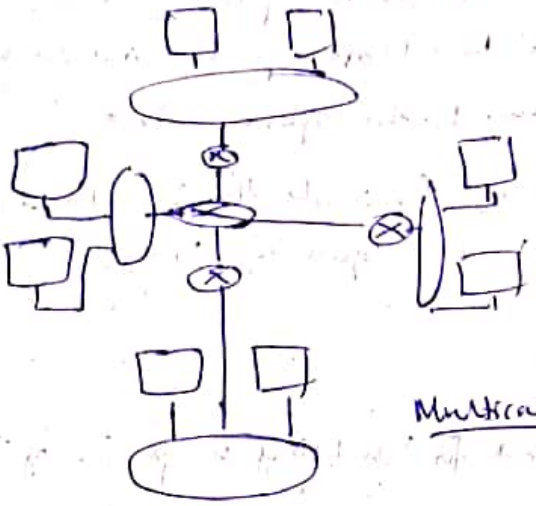
Multicast

- Multicasting means a multicast-packet is delivered to only a subset of network-nodes.
- Used for:

  1) Bulk data transfer
  2) Streaming continuous media
  3) Data feeds
  4) Web cache.

- A multicast packet is addressed using address indirection.
- A single identifier is used for the group of recievers.

∴ Using this single identifier, a copy of the packet is delivered to all multicast recievers.



Multicasting

A datagram addressed to the group is delivered to all members of the multicast group.

IGMP

1) Internet Group Management Protocol

It provides multicast routers info about the membership-status of hosts connected to the operations.

2) Multicast Routing Protocols

These protocols are used to coordinate the multicast routers throughout the Internet.

IGMP messages are encapsulated within an IP datagrams.

→ Membership query: A host sends a membership query message.
→ Membership report: A host sends membership report message when an application first joins a multicast group.

→ Leave group : This message is optional.

Multicast Routing Algorithm

- The methods used for building a multicast-routing tree:
  1) Single group-shared tree.
  2) Source-specific routing tree.

1) Multicast Routing using a Group-Shared Tree
   - A single Group-shared tree is used to distribute the traffic for all senders in the group.

2) Multicast Routing using a Source Based Tree
   - A source-specific routing tree is constructed for each individual sender in the group.

- Three multicast routing protocols are:
  1) Distance Vector Multicast Routing Protocol (DVMRP)
     It uses RPF algorithm (Reverse Path Forwarding)
  2) Protocol Independent Multicast (PIM)
     It divides multicast routing into sparse and dense mode.
  3) Source Specific Multicast (SSM)
     Only a single sender is allowed to send traffic into the multicast tree. This simplifies the tree construction & maintenance.