01fe18bcs211

3a) Three broadcasting algorithms.

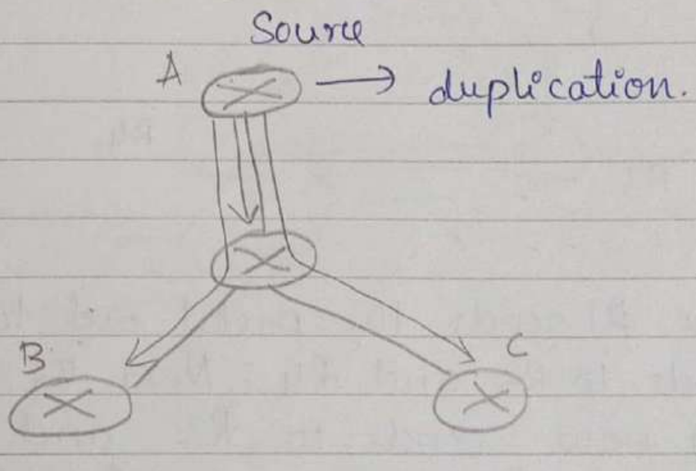
→ (i) Source duplication.

→ Here the source itself create n-differnt copies to broadcast to all other destinations.

→ this is also called N-way unicasting

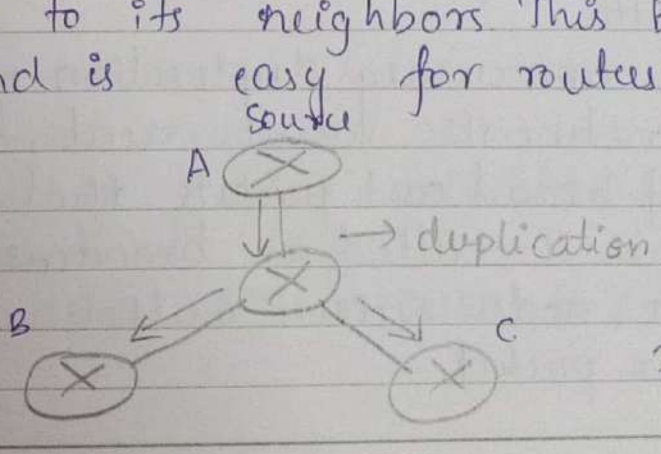
→ If the source node is connected to outside world via only one link then there will be a overload on the link.

→ And the source should have IP addresses of all the destinations



(ii) In-network duplication

where source will flood to neighbors and neighbors to its neighbors This balances the load. and is easy for routers



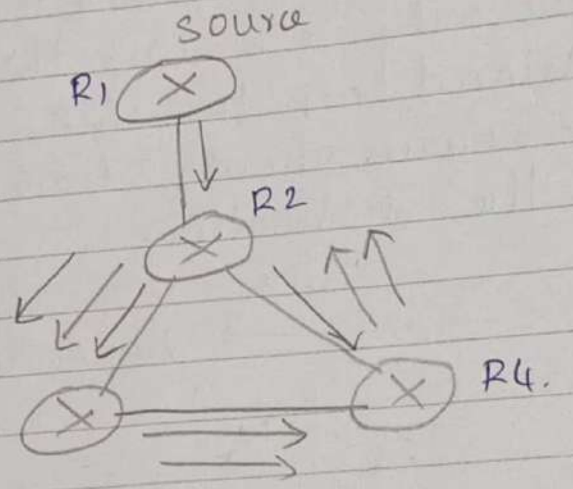
(iii) Uncontrolled flooding

→ Here the basic idea of flooding is used.

→ Every node forwards the packets to its neighbors except from the node it is has recieved.

→ But if the network has cycles then it will lead to continous flooding of broadcast packets.

→



→ Suppose R1 sends the packet out to R2 and R2 sends to R3 and R4. Next R3 sends to R4. R4 now sends to R2 and R2 → R3 R3 → R4 R4 → R2..... And this cycle never ends.

→ It creates traffic and consumes lot of bandwidth

→ There is unnecessary duplication of packets in the network and creating huge number of broad cast packets that render useless. This is called as broadcast storm.

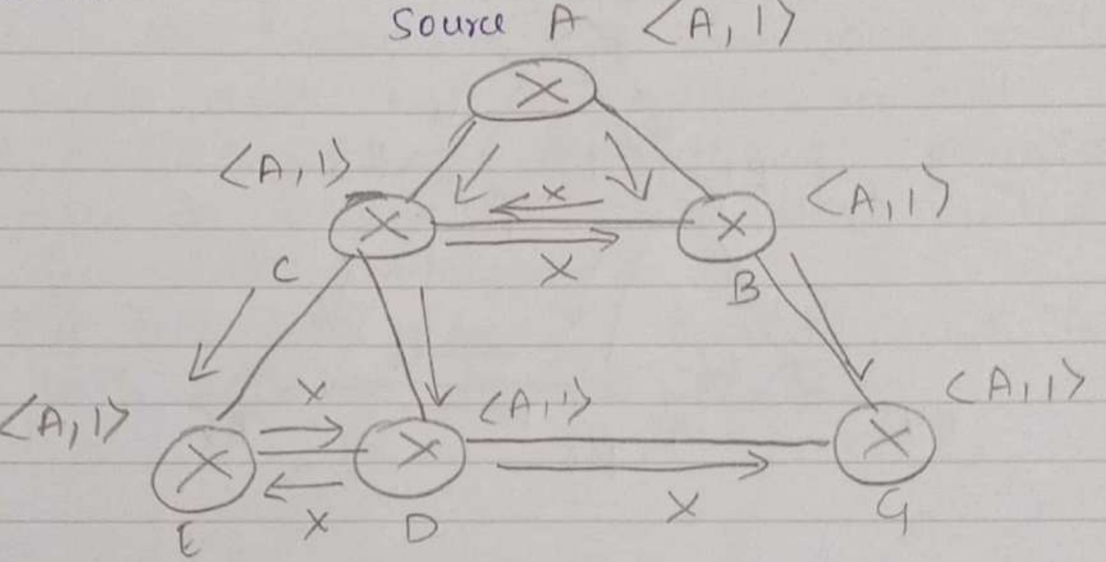
→ A single node recieves multiple copies of the same packet.

(iv) Controlled flooding

→ (i) Sequence - number based controlled flooding.

→ Here each source sends it's address as well as broadcast sequence number while broadcasting. All the routers maintains list of source address and broadcast sequence no. that is has recieved, duplicated and forwarded

→ So if a packet arrives at a node it checks in the list if the entry is already present it discards else duplicates, forwards and marks the entry in the list.



→ Here A is the source with source addres A and broadcast sequence no 1

→ x → when packet gets discarded

→ Solves broadcast storm

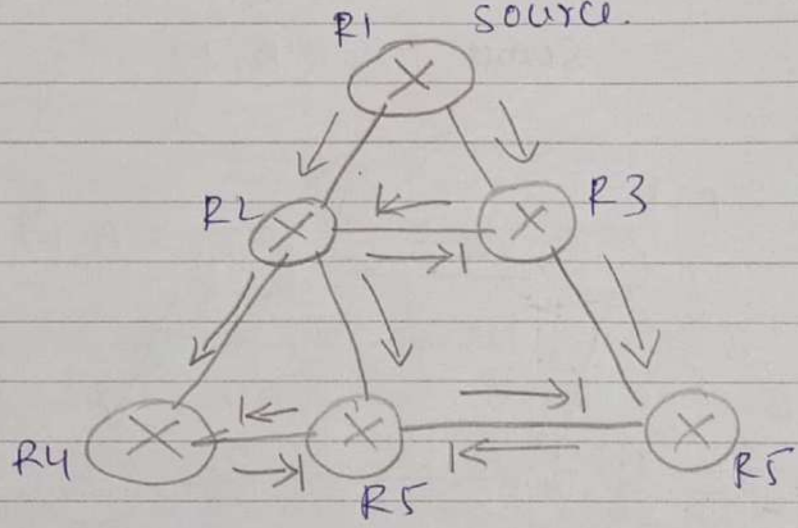
→ A single node still recieves duplicate packet.

(iii) Reverse Path forwarding (RPF).

→ Here source sends the packets to its neighbors

→ All nodes sends the packets on its outgoing link except the source link or the link from where it has recieved packet only if the packet came via the link that is in the ~~shorte~~ its own shortest unicast path back to the source.

→ It need not have full information about the whole unicast shortest path back to the source but only about its neighbor on the unicast shortest path back to the source.



Pg No: 4

(iv) Spanning tree based

→ It follows centralized approach.

→ The source sends the ~~pa~~ packet to all its neighbors to ~~kr~~ tell them it wants to broadcast

→ Then all other nodes sends tree-join message to the source using tree-join packet

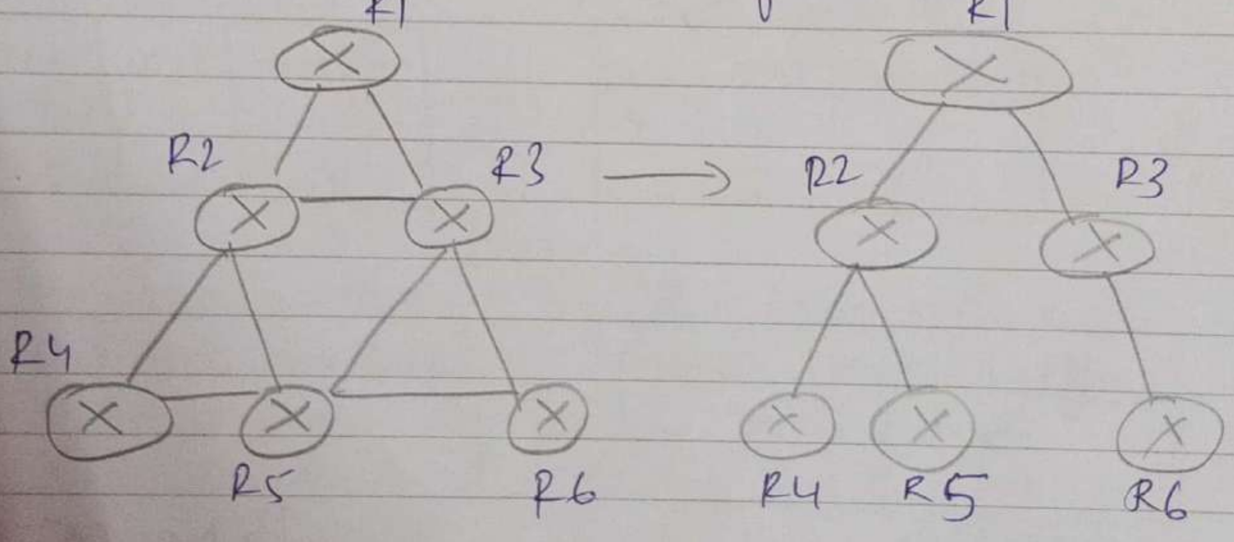
→ the tree-join packets travel back either to source or any other node that is already part of ~~shortest path~~ mininum spanning tree. (MST)

→ A tree is used because it doesn't contain cycle

→ A MST contains all the nodes without cycle and having minimum cost.

→ Building and maintaing spanning tree is costly so it's best suited for static network.

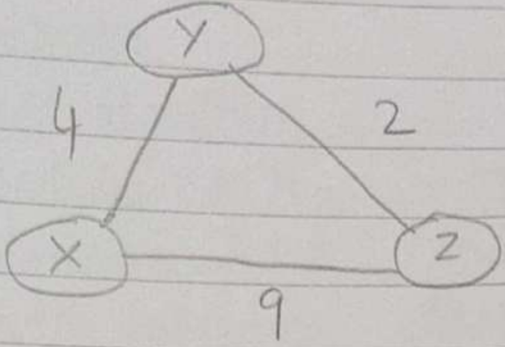
→ A tree-join message travels and its path becomes branch of MST.



3b)

ICMP	IGMP.
→ It is mainly used for error reporting	→ It is used to manage groups, memberships
→ It is in unicast routing.	→ It helps or assits multicasting protocol
→ It is network layer protocol	→ It is also network layer protocol.
→ It operates between host to host, host to router or router to router.	→ It operates between host or client to multicast router
→ Internet Control Message protocol	→ Internet group management protocol
→ Companion to IP	→ Companion to IP

3c)



Step1: Every node sends HELLO packets to neighbors and updates its link table.

Initially, all nodes know about it's neighbors.

Y's table

Z	2	-
X	4	-
dust	cost	nexthop

X's table

Y	4	-
Z	9	-
dest	cost	nexthop

Z's table

Y	2	-
X	9	-
dust	cost	nexthop

Step2: Exchange with neighbors.

Y's table with Z

Z	2	-
X	4	-

Y's table with X

Z	2	-
X	4	-

X's table with Y

dest	cost	nexthop
Y	4	-
Z	6	Y

X's table with Z

dest	cost	nexthop
Y	4	-
Z	6	Y

Z's table with Y

dest	cost	nexthop
Y	2	-
X	6	Y

Z's table with X

dest	cost	nexthop
Y	2	-
X	6	Y

Step 3.

Final X's table

dest	cost	nexthop
Y	4	–
Z	6	Y

Final Y's table

dest	cost	nexthop
X	4	–
Z	2	–

Final Z's table

Y	2	–
X	6	Y
dest	cost	nexthop

a)

Distance - Vector	Link - State
→ Decentralized algorithm	→ Global algorithm
→ Local knowledge - as the routing information is just exchanged with neighbors	→ Global knowledge as routing information is exchanged with all nodes in the network
→ Metric is hop count	→ Metric is bandwidth etc.
→ Traffic is less	→ Traffic is more
→ Load insensitive ie cost doesn't reflect congestion	→ Load insensitive i.e cost doesn't reflect congestion
→ Size of link state packet is less	→ Size is more as it maintains more information like sequence number etc.
→ Count to infinity problem exists	→ No count to infinity problem.
→ Practical implementation is RIP	→ Practical implementation is OSPF
→ Only distance vector or cost is exchanged	→ Cost and nexthop both are exchanged
→ Less bandwidth is required as there is no flooding	→ More bandwidth is required due to flooding

01fe18bcs211
Pg No: 9

2b)(a)BGP or Border Gateway Protocol

→ Is used for inter-domain routing.

→ It is Stand protocol and is the Internet Backbone.

→ It is used to exhange routing information between routers belonging to two different autonomous systems (AS)

→ The network is divided into different hierarchial areas called AS

→ Two routers exchanging the routing information are called BGP peers.

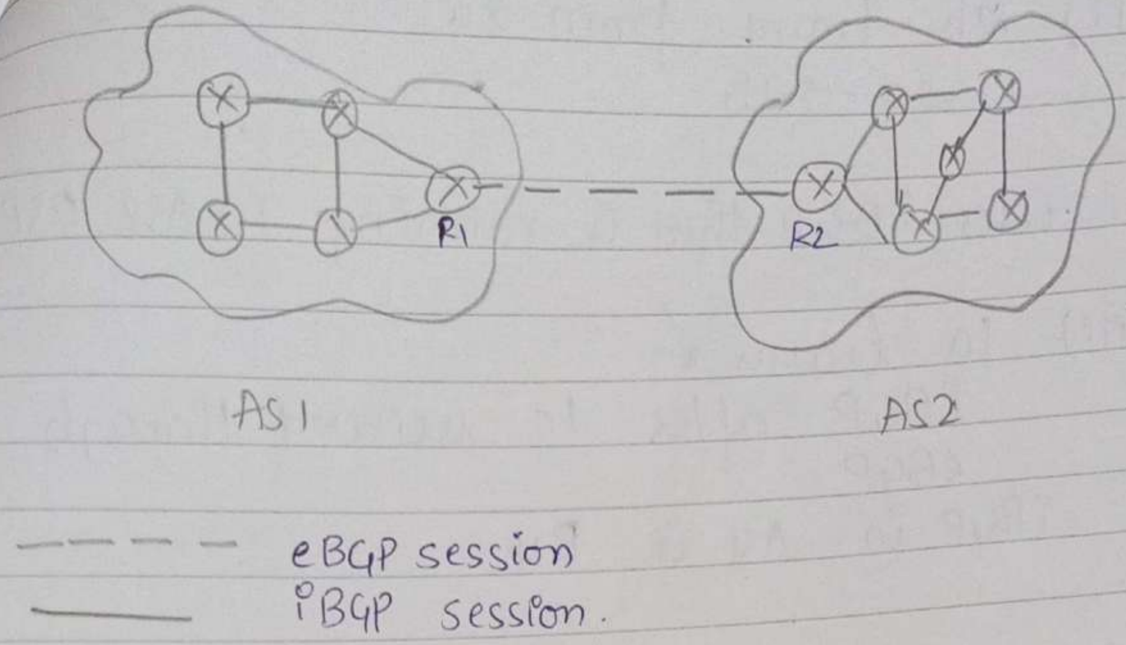
→ BGP makes use of TCP connection to transfer the routing information reliably. It makes use of port 179. It is application layer protocol.

→ If the session is used to transfer (exchange info between two routers of the same network/AS then it is called as iBGP or internal session.

→ If the session is used to exchange routing information between two different AS then it's called eBGP session.

→ there are two variants
(i) eBGP (exterior BGP)
(ii) iBGP (interior BGP)

01fe18bcs211
Pg No:10



There are two AS's AS1 and AS2. R1 and R2 are in eBGP session. Any routing information here uses eBGP for exchange.

b) (i) 2a learns from x.
2a ~~and~~ is in AS2.
The x prefix info passes to 2a:

4a → 4b	RIP
4b → 4c	RIP
4c → 3c	eBGP
3c → 3b	OSPF
3b → 3a	OSPF
3a → 1c	eBGP
1c → 1a	RIP
1a → 1b	RIP
1b → 2a	eBGP.

So it learns through eBGP.

(ii) 2b learns from 2a
2a → 2b

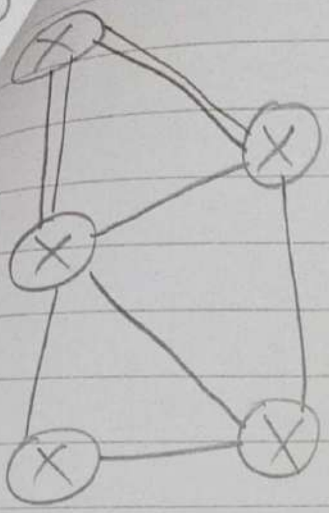
uses iBGP that is running in AS2 OSPF

(iii) 1a learns x
iBGP after 1c recieved through eBGP
iBGP in AS1 is RIP

(iv) 1b also RIP

2c)

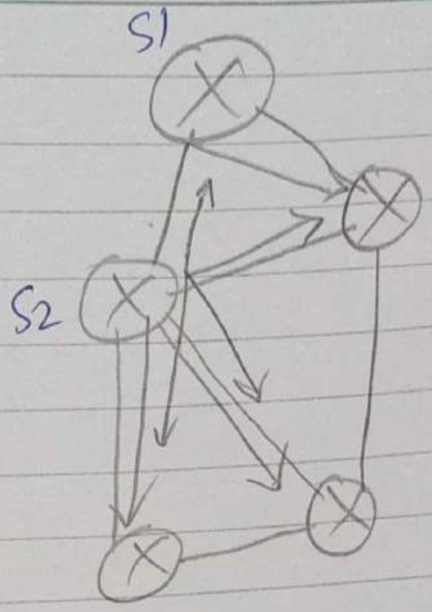
Group-shared tree	Source based tree
→ Only one multicast router is kept responsible called as centre/core/rendezvous router	→ No centre/core router All routers are involved in multicasting
→ Only one router maintains m shortest path to all other nodes	→ All routers maintains the shortest path to other nodes.
→ It's bidirectional.	→ It's unidirectional



Shared

→ It is not reverse path forwarding.

→ DVMRP and PIM uses source based tree



Source-based

→ It is Reverse path forwarding

→ BGMP uses shared tree.