Hierarchial Routing

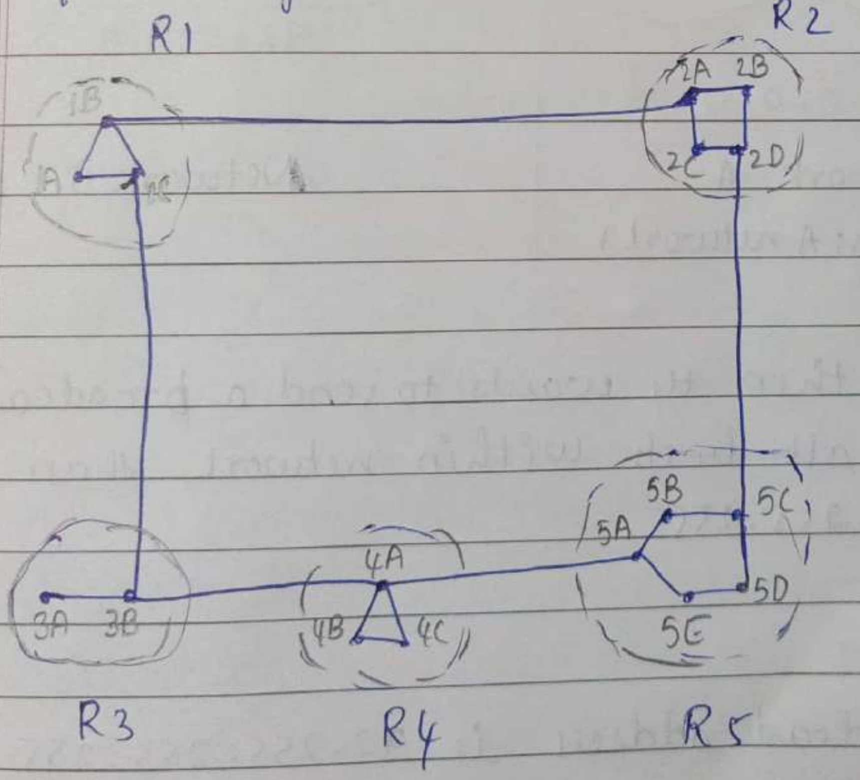
→ As networks grow in size, the router routing table grows proportionaly

→ Router memory, CPU time and more bandwidth consumed to send status reports about them.

→ Routers are divided into regions.

→ Each " knows all the details how to route packets to destinations within its own region

→ But knowing nothing about internal structure of other regions

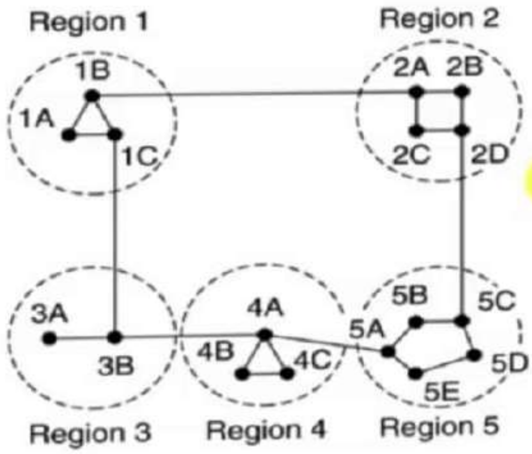


Hierarchial Table for 1A

Dest	Line	Hops
1A	-	-
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

In hierarchial table write all nodes within region & line and for other regions the shortest hop path.

Hierarchical Routing - Example



(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

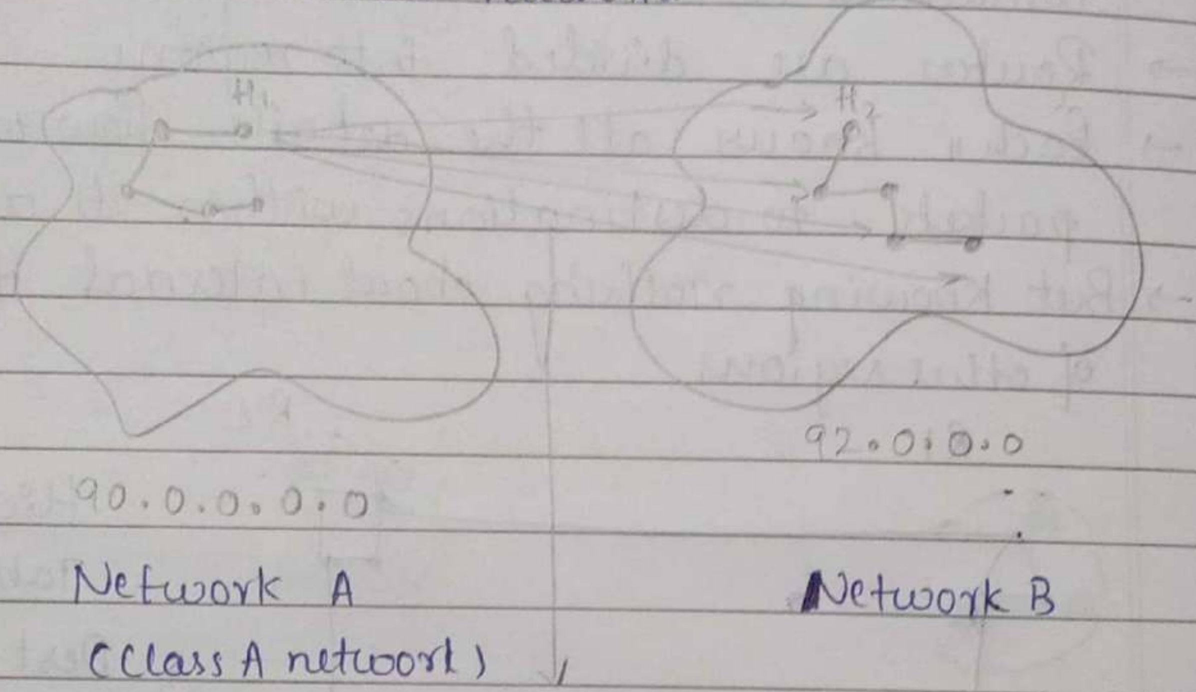
(c)

1> Unicast (1:1)

2> Brodcast: Send packets to all destinations simultaneously

1> Limited

-> Broadcast within network



If limited then H1 wants to send a broadcast packet to all hosts within network than 255.255.255.255

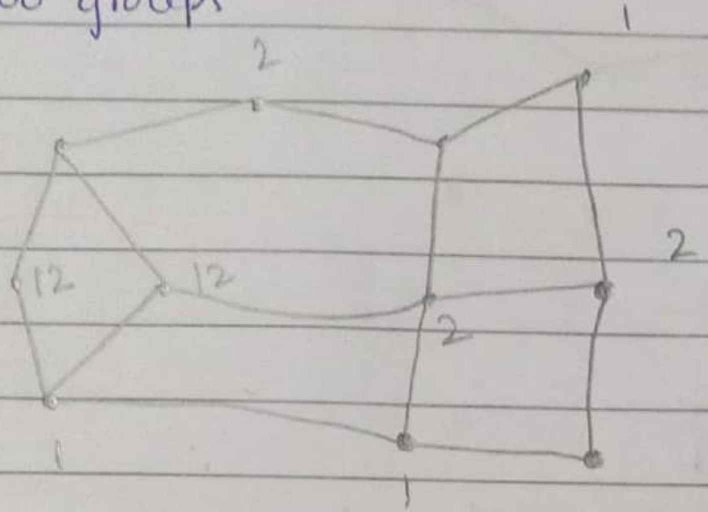
2> Direct

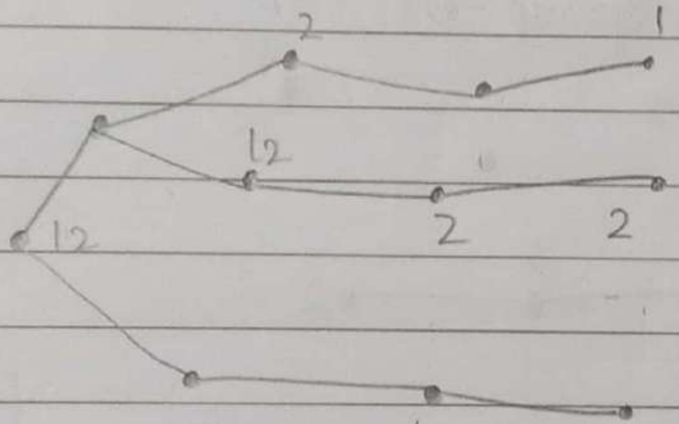
Then broadcast address is 92.255.255.255

3> Multicast. Sending msg to a group

-> Class D.

→ Some routers are attached to hosts belonging to one/ two groups



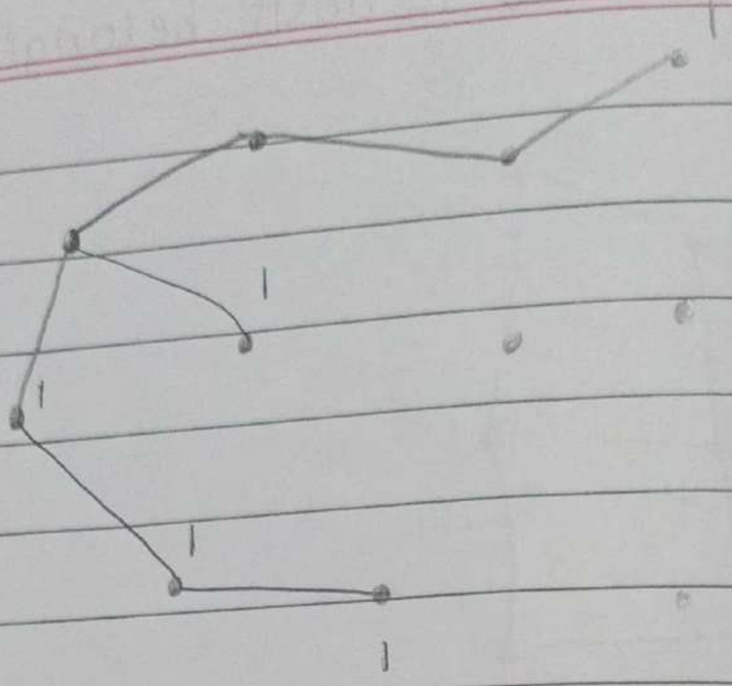


→ Spanning tree for left most router

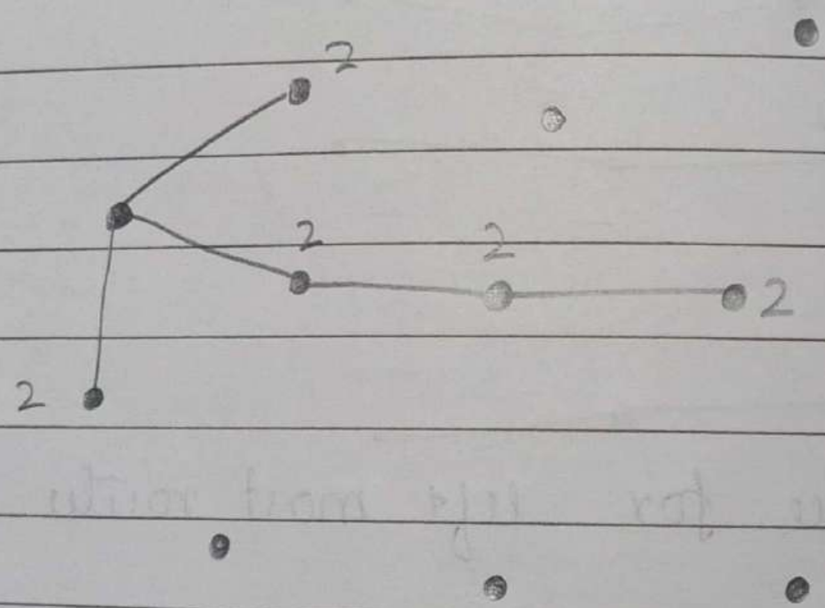
→ Needs IGMP

→ Each router computes a spanning tree covering all other routers

→ When a process sends a multicast packet to a group, the first router examines the spanning tree & prunes it, removing all lines that do not lead to hosts that are members of group.



Group - 01



Group - 02

Date
Page

Heirarchial Routing

→ If every router has router table and if no. of routers increases the routing table size increases and all routers can't handle network efficient.

→ Divide & conquer strategy

→ Divide network to regions and a router for a particular region only knows about its own domain & neighbor routers

→ Routers are classified into groups called regions

→ Each router has only info about the routers in it's own region and has no region about routers in other region. So router just save one record in their table for every region.

→ Improve network efficiency.

→ Two - level

Three- level

Clusters (Three level)

↓

Regions (Two level)

↓

Routers (Routing table for every router)

Multicasting

Tree - Based

- → fast, quick
- → less control msgs
- → less overhead
- → Link failure - path is also lost (as only one path exist)
- → Top-down approach
- → Vertical processing
- → for light weight appl'ns

Mesh - Based

- Resilient to link failure (Robust)
- Need more control msgs & solves
- → alternate/multiple paths exists

Source based

- → each router maintains one shortest path for each group.
- → separate multicast tree for every multicast source
- → rooted at source

Shared tree

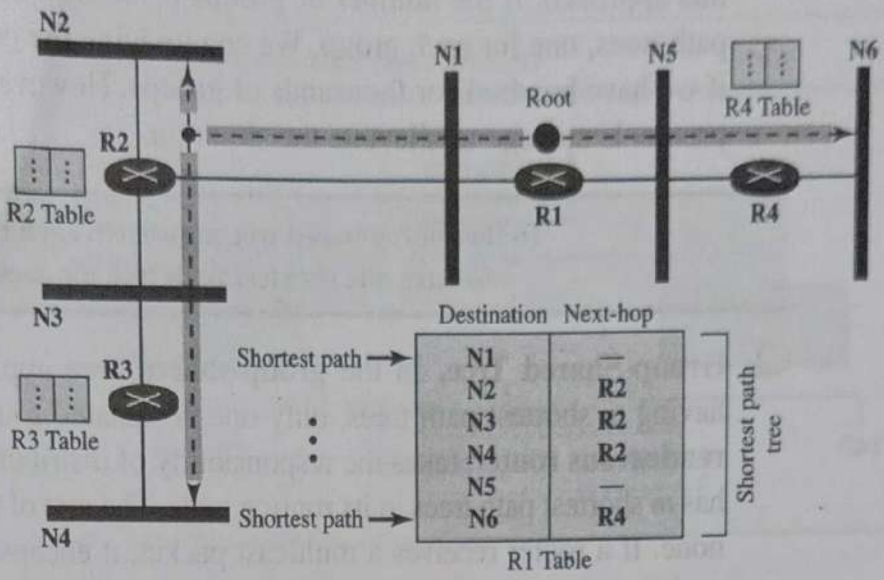
- → Only one router called centre core or rendezvous router, takes responsibility of multicast routing
- → Core has m shortest path in its routing table.

→ Needs to be dynamically updated

Others have none.

→ If routers recieve multicast packet it encapsulates in a unicast packet and sends to core router.

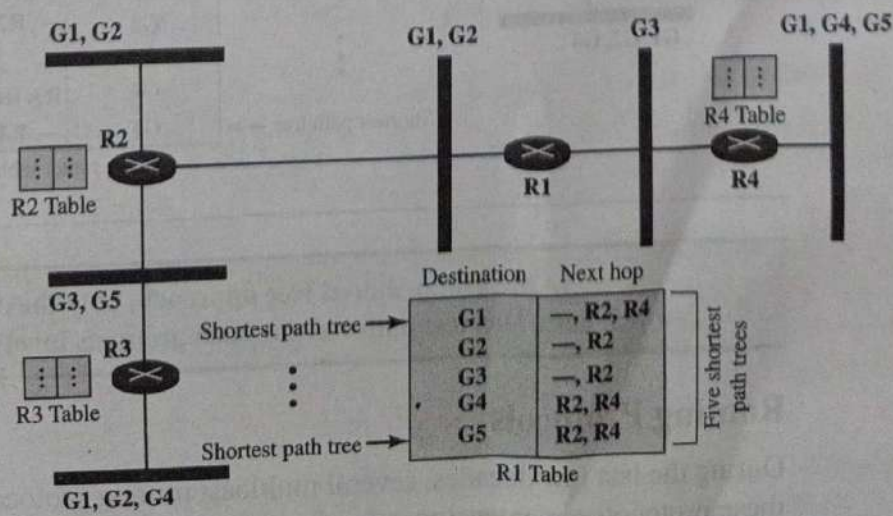
Figure 22.36 *Shortest path tree in unicast routing*



In multicast routing, each involved router needs to construct a shortest path tree for each group.

- **Source-Based Tree.** In the source-based tree approach, each router needs to have one shortest path tree for each group. The shortest path tree for a group defines the next hop for each network that has loyal member(s) for that group. In Figure 22.37, we assume that we have only five groups in the domain: G1, G2, G3, G4, and G5. At the moment G1 has loyal members in four networks, G2 in three, G3 in two, G4 in two, and G5 in two. We have shown the names of the groups with loyal members on each network. Figure 22.37 also shows the multicast routing table for router R1. There is one shortest path tree for each group; therefore there are five shortest path trees for five groups. If router R1 receives a packet with destination

Figure 22.37 *Source-based tree approach*

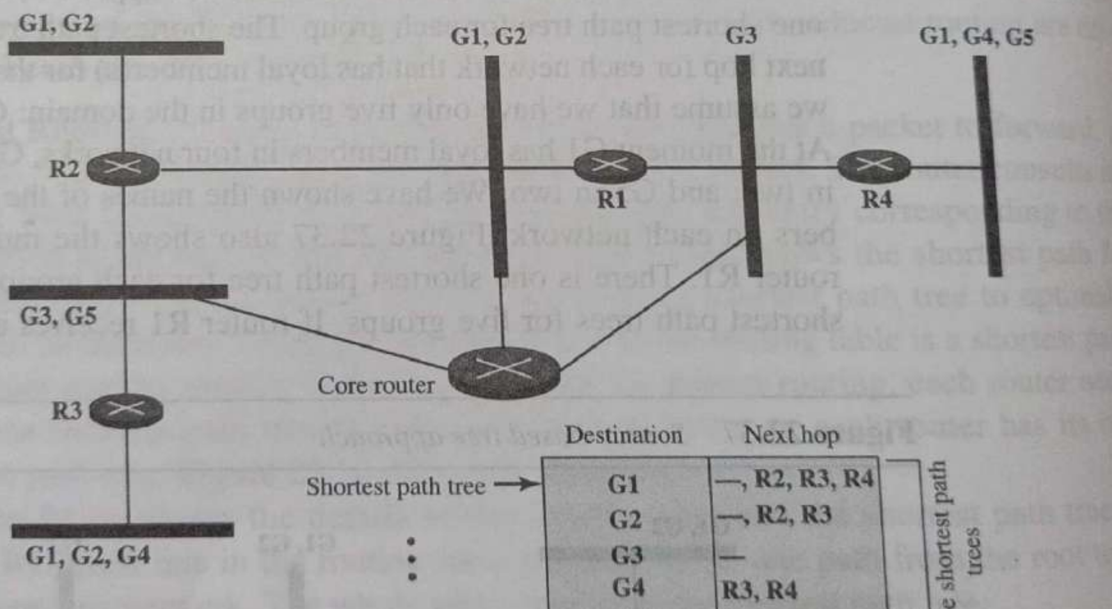


address G1, it needs to send a copy of the packet to the attached network, a copy to router R2, and a copy to router R4 so that all members of G1 can receive a copy. In this approach, if the number of groups is *m*, each router needs to have *m* shortest path trees, one for each group. We can imagine the complexity of the routing table if we have hundreds or thousands of groups. However, we will show how different protocols manage to alleviate the situation.

In the source-based tree approach, each router needs to have one shortest path tree for each group.

- **Group-Shared Tree.** In the **group-shared tree** approach, instead of each router having *m* shortest path trees, only one designated router, called the center core, or **rendezvous router,** takes the responsibility of distributing multicast traffic. The core has *m* shortest path trees in its routing table. The rest of the routers in the domain have none. If a router receives a multicast packet, it encapsulates the packet in a unicast packet and sends it to the core router. The core router removes the multicast packet from its capsule, and consults its routing table to route the packet. Figure 22.38 shows the idea.

Figure 22.38 *Group-shared tree approach*



Destination	Next hop
G1	—, R2, R3, R4
G2	—, R2, R3
G3	—
G4	R3, R4
G5	—, R4

In the group-shared tree approach, only the core router, which has a shortest path tree for each group, is involved in multicasting.

Routing Protocols

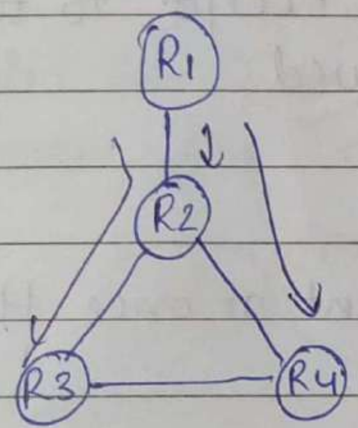
During the last few decades, several multicast routing protocols have emerged. Some of these protocols are extensions of unicast routing protocols; others are totally new.

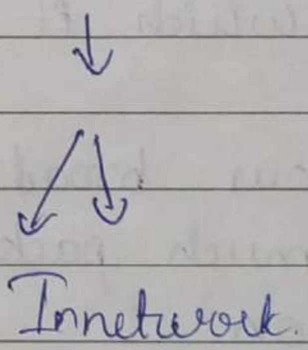
→ Single source and single destination is called unicast

→ Broadcast and multicast

→ Broadcast: Send data to all nodes in the network.

Multicast: " " to set of " " " "
(subnet).





Source

R1 wants to send data to all other nodes

It can be done using:

i) n-way unicasting

R1 creates n copies of that packets and send to different destination.

All n copies via one link so it's overloaded

Network duplication

$R_1 \xrightarrow[1]{} R_2 \xrightarrow[2]{} R_3, R_4$.

Page

Broadcast algorithms

1) Multidestination routing

2) flooding

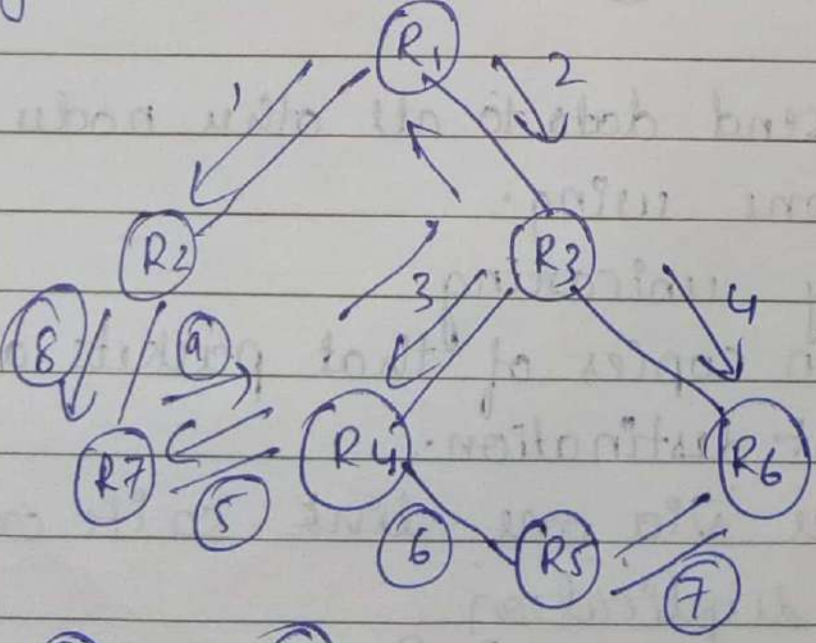
3) Reverse path forwarding.

1) Uncontrolled flooding

Every intermediate node transmits the broadcast packet to all nodes except to the node from which it recieved

→ Continous broadcast

→ Too much packets sent at once there will be congestion

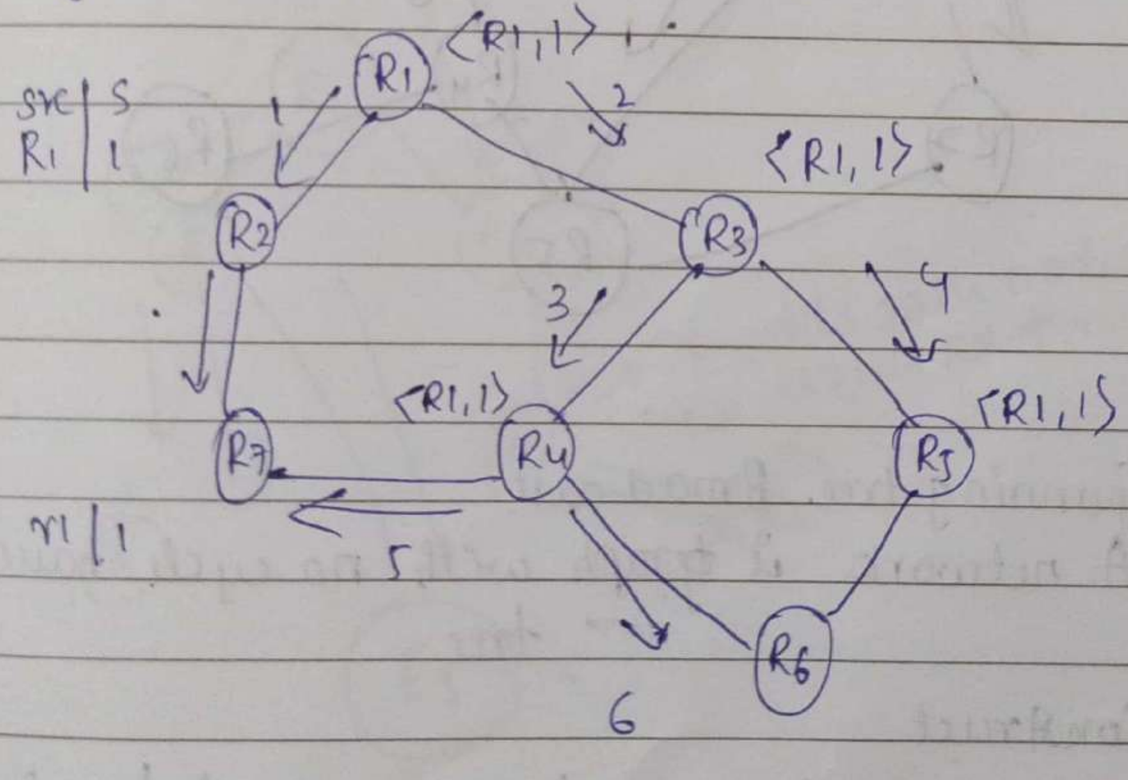


8 and 5

→ packets don't die at all
→ every node keeps sending data again & again especially if it's cycle

→ Broadcast storm - too many copies of broadcast packets in the network.
→ multiple copies are sent to same nodes / recieved at node.
R7 ← R2 & R4

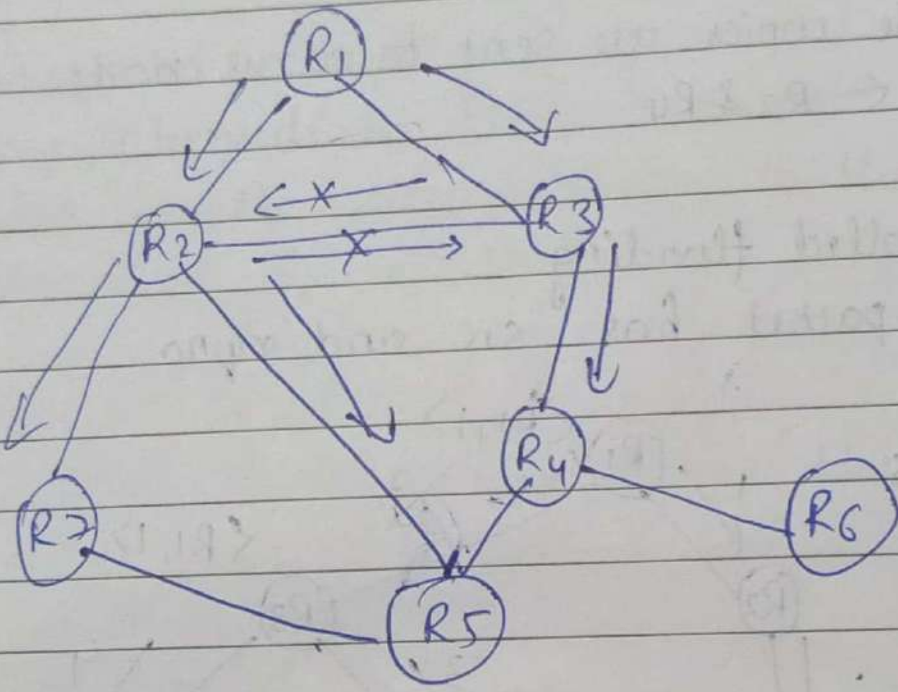
Controlled flooding
→ Every packet has src and seq no



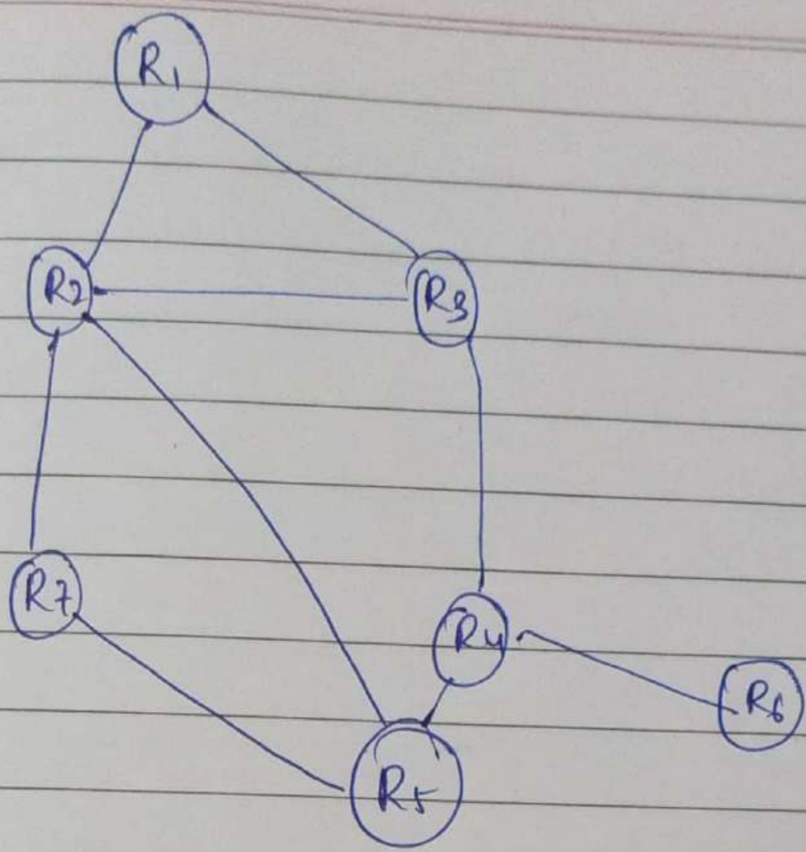
Layer 3-switch / router solves broadcast storm

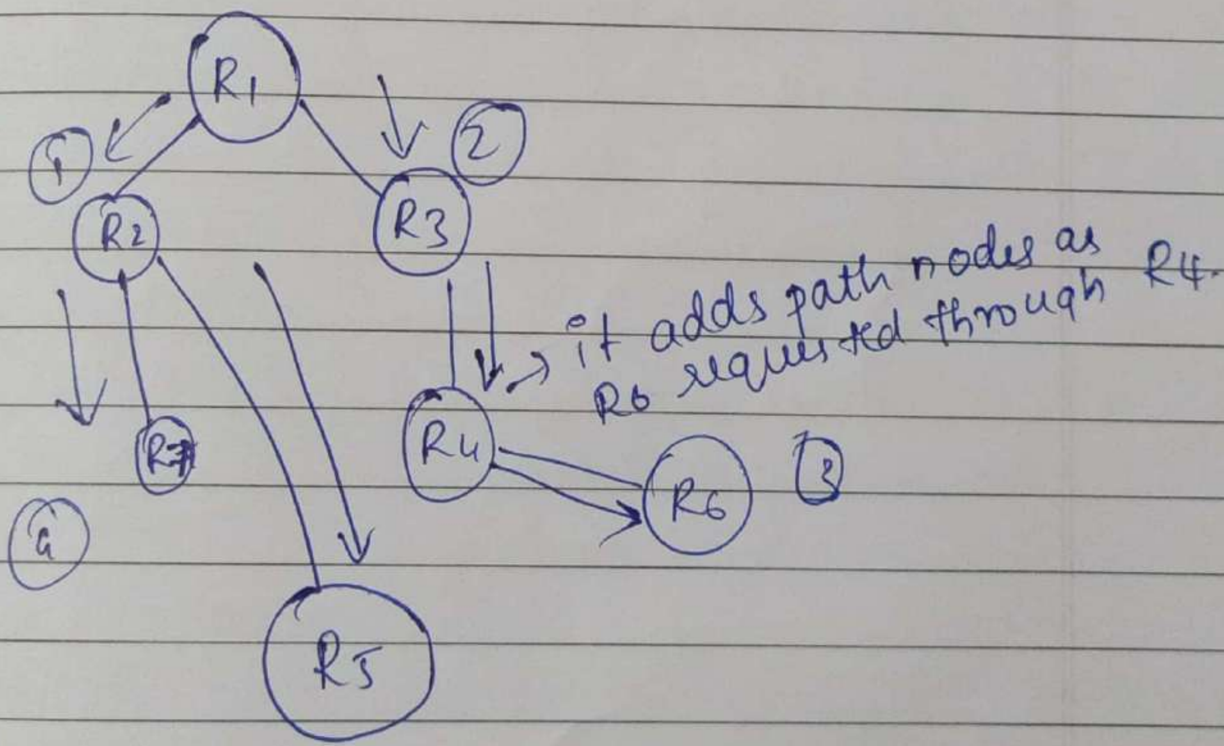
→ multiple copies are recieved at same node

* Reverse path forwarding
→ a node broadcasts a packet if it recieves from the node which exists in the shortest path to the source node.
→ Recieve same packet multiple times.



* Spanning-tree Broadcast
→ A network is graph with no cycle basically tree
→ Construct
→ every node in network send tree join request to source. called tree join packet help source node to create the spanning tree

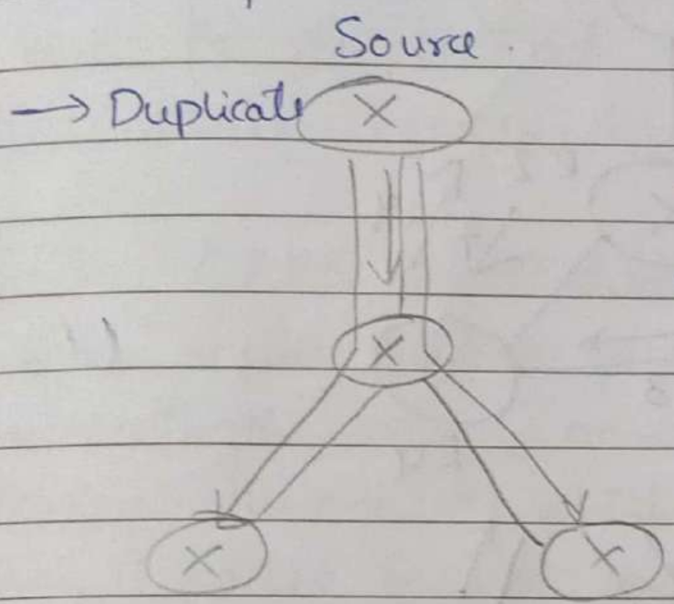




- suitable for static networks.
- overhead of constructing tree
- to prevent switching loops in networks with redundant switched paths.

Broadcast

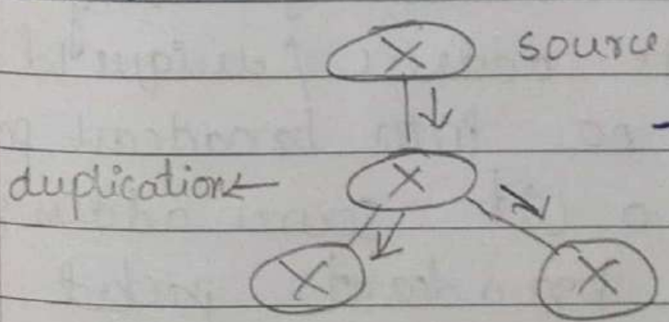
1) Source duplication



→ inefficient
→ If source is connected to network via single link the N copies of the same pocket traverse through this link.
→ overload the network

→ how to know broadcast recipients & it's addresses
→ Link state routing protocols used broadcast to disseminate the link-state information that is used to compute unicast routes. so broadcast is used to update unicast route.

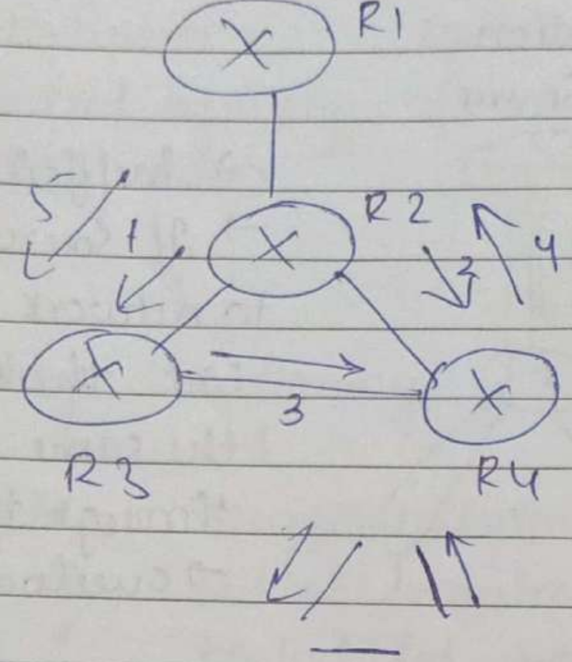
2) In network.



→ load gets distributed
→ network nodes themselves play active role in duplication

Un

3> Controlled flooding



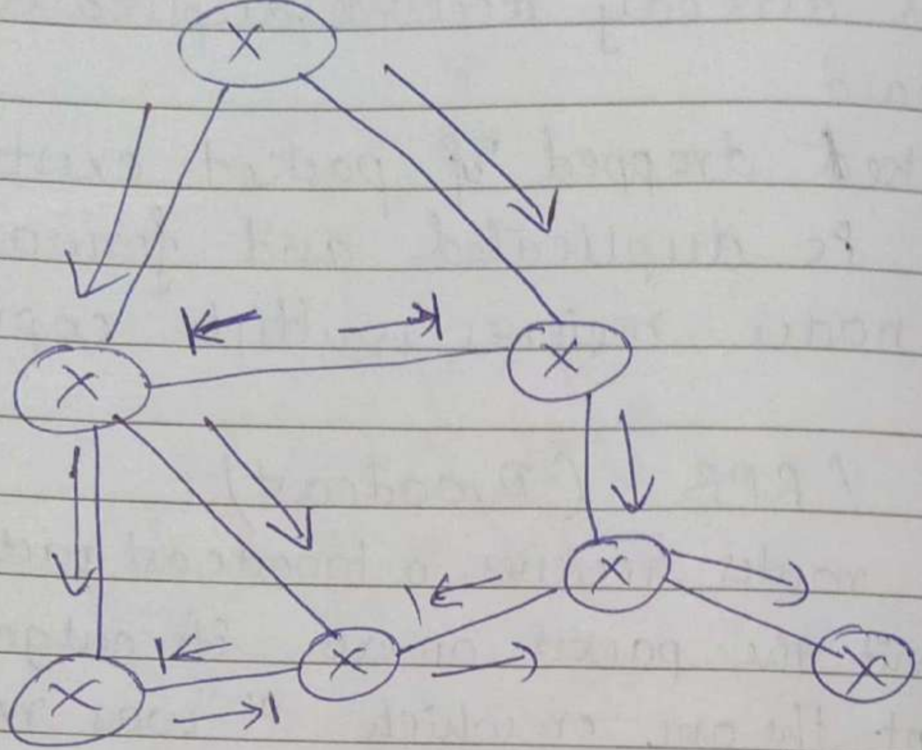
Endless cycling of broadcast packets
Broadcast: endless multiplication of broadcast packet that results in many broadcast packets being created in network would be rendered useless.

4) Controlled flooding (avoid broadcast storms)
(i) Sequence number controlled flooding
→ Source node puts its address / unique id and broadcast seq no into broadcast packet
→ Each node has a list source address & seq no. of each broadcast packet

Date
Page

it has already recieved, duplicated or forward
→ packet dropped if packet exists in list else is duplicated and forwarded
→ Still node recieves multiple copies

(ii) RPF / RPB (Broadcast) with given SA
→ when router recieves a broadcast packet it will transmit the packet on all it's outgoing links (except the one on which it was recieved) only if packet arrived on link that is in it's own shortest unicast path back to the source.
→ Else discard the incoming packet on link without forwarding on any of it's outgoing link
→ needs to know the next neighbor on it's unicast path (shortest) to sender. it uses this neighbors identity only to determine whether or not to flood a broadcast packet that is recieved.



4) Spanning tree (i) Center-based approach
→ Centre (core node or rendezvous point is defined.
→ Nodes send unicast treejoins msgs via tree join packet to centre.
→ Tree join msgs is forwarded using unicast routing until it reaches centre or the node. or arrives at node belonging to spanning tree
→ path that tree-join message follows define branch of spanning tree

classmate
Date
Page

Heirarchial Routing

→ If every router has router table and if no. of routers increases the routing table size increases and all routers can't handle network efficiently.

→ Divide & conquer strategy

→ Divide network to regions and a router for a particular region only knows about its own domain & neighbor routers

→ Routers are classified into groups called regions

→ Each router has only info about the routers in it's own region and has no region about routers in other region. So router just save one record in their table for every region.

→ Improve network efficieny.

→ Two-level

Three-level

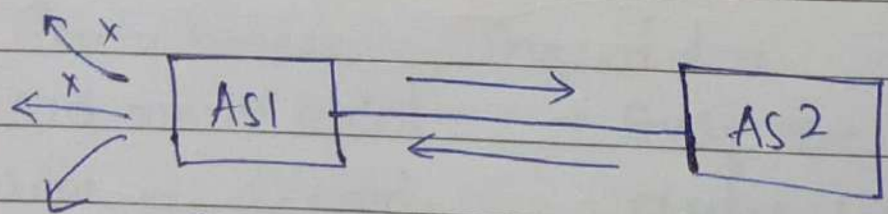
Clusters (Three level)
↓
Regions (Two level)
↓
Routers (Routing table for every router)

BGP (Border Gateway protocol)

→ Interdomain routing protocol
→ Uses path vector routing
→ Internet is divided into hierarchial domains called autonomous systems
→ Appl'n layer protocol uses TCP
→ Open standard : standard protocol can run on any device
→ Inter-AS domain routing
  ↳ exchanging routing info b/w 2/more autonomous system
→ Supports internets.
  ↳ it operates on Internet backbone
→ classless protocol

Types of autonomous System (AS)

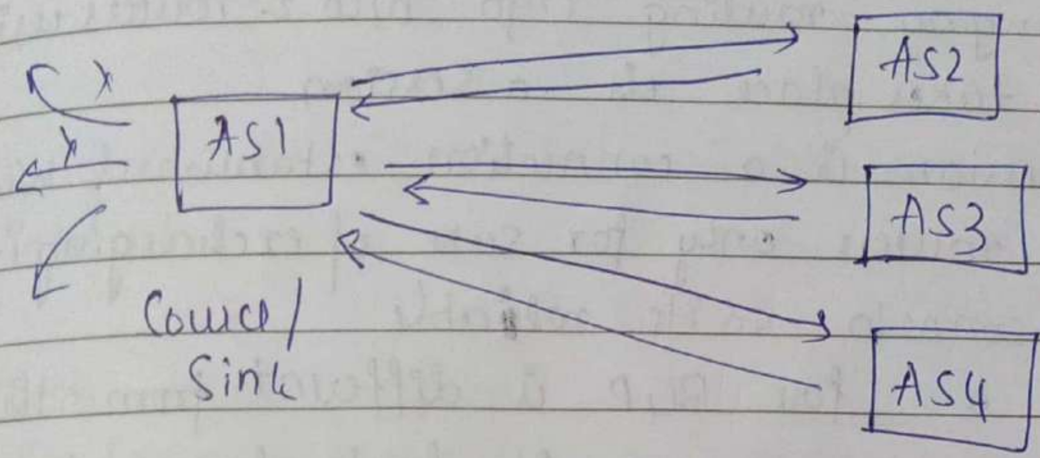
1) Stub AS



Source/Sink

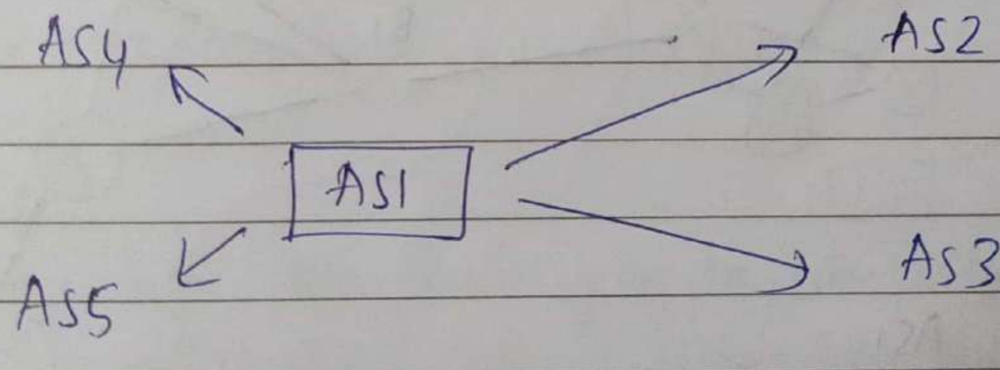
→ A system with one connection from one AS to another
→ Data traffic can't pass through Stub AS
It can either be source/sink

2) Multihomed AS



It is AS that can have more than one connection to another AS. But it can still be either sink/source for data traffic. No transient data traffic flow, which means that data can be passed from one AS to another.

3) Transient AS



It is multihomed AS, but it provides transient traffic flow

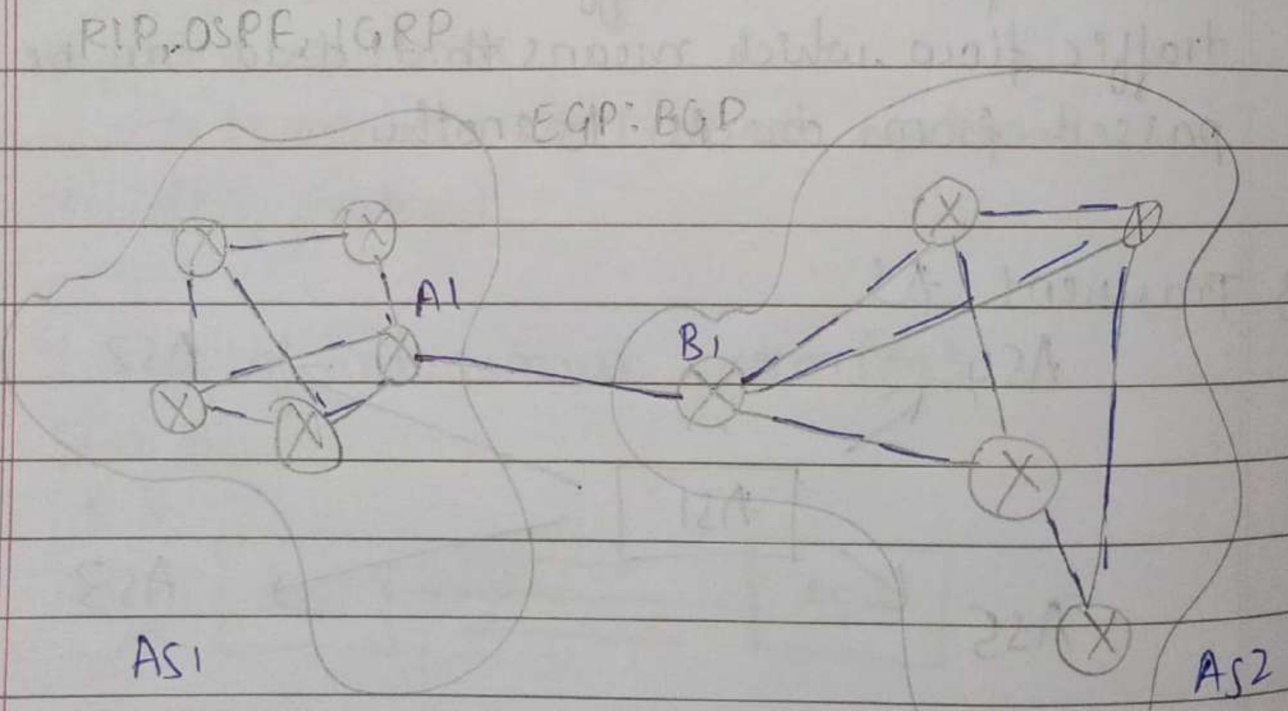
BGP Sessions

→ Exchanging routing info b/w 2 routers using BGP takes place in a session

→ A session is a connection established b/w two BGP routers only for sake of exchanging info

→ TCP conne'n so it's reliable

→ TCP " for BGP is different from other appl'n programs as it lasts longer is also called as <u>semi-permanent connection</u>



→ IGP protocols are used to communicate within AS

→

Date
Page

i- interior gateway protocol
e- exterior " "

→ Designed to scale huge inter-network like internet

→ Path vector protocol
Sending path info as well as routes

↳ It helps in loop prevention mechanism

→ Port number = 179
→ Metric = Lot of attributes

OSPF = 10^8/BW
RIP = hop count

e-BGP
→ Exchange info b/w belonging to two different AS
→ iBGP - " " (routing info) " b/w two routers inside AS
→ 1,2 - AS number
→ A1 — B1 session is eBGP (——)
→ - - - - iBGP

Date
Page

Attributes

Well-Known (recognized by every BGP router)
Optional (need not be recognized by every BGP router)

- Well-Known
  - mandatory → appears in descrip'n of route → Eg1 ORIGIN (source of routing info RIP, OSPF)
  - discretionary → recognized by router but not required to be included in every message update
- Optional
  - Transitive → passed to next router that has not implemented this attribute
  - Non-transitive → must be discarded if the receiving router hasn't implemented it

Eg1 ORIGIN
(source of routing info RIP, OSPF)

Eg2 AS PATH
list of AS through which the destination can be reached

Eg4, NEXT_HOP
next router to which data packet must be sent

BGP

→ Two routers at end of the connection are called BGP peers

→ TCP connection along with the BGP msgs are sent over a connection called a BGP session.

↓

a BGP sessions that spans two ASs - eBGP
" " " b/w routers in same AS - iBGP

→ helps AS to learn which destinations are reachable via its neighboring ASs.

→ The destinations are CIDRized prefixes

→ Prefix, along with attributes is called route

→ RIP

→ routing updates are exchanged b/w neighbors every 30s using RIP response message.

→ The RIP response message sent by a router host contains list up to 25 destination subnets within AS

→ RIP msgs are also called as RIP advertisements.

→ hop count - no. of subnets traversed along shortest path from source to dest subnet. Including dest subnet

→ Each router has RIP table called routing table

Why AS?
→ Scale
→ Administrative autonomy
↳ for security