Long Answers

1. RIPV1

<table>
<tr><td>Command 1</td><td>Version 2</td><td>Must be zero 2</td></tr>
<tr><td colspan="2">Address family identifier 2</td><td>Must be zero 2</td></tr>
<tr><td colspan="3">IP Address 4</td></tr>
<tr><td colspan="3">Must be zero 4</td></tr>
<tr><td colspan="3">Must be zero 4</td></tr>
<tr><td colspan="3">Metric 4</td></tr>
</table>

- distance vector protocol
- Classful protocol, doesn't support VLSM or CIDR.
- Can connect to a max^m of 15 routers.
- Advertises 25 routes per RIP message
- Implements split horizon with poison reverse.
- Does not support authentication.
- Used in small, flat networks or at edge of larger network
- Default administrative distance is 120.
- Sends update through broadcast.
- Broadcasts at 255.255.255.255.

2. IGRP

- Proprietary distance vector routing protocol
- Cisco's idea
- Transfers routing information b/w linked routers in the host network or A.S.
- guarantees every router's routing table is kept upto date with the most direct route available.
- transmits updates every 90 sec, hold-down time 280 sec.
- IGRP Adminstritive distance is 100.

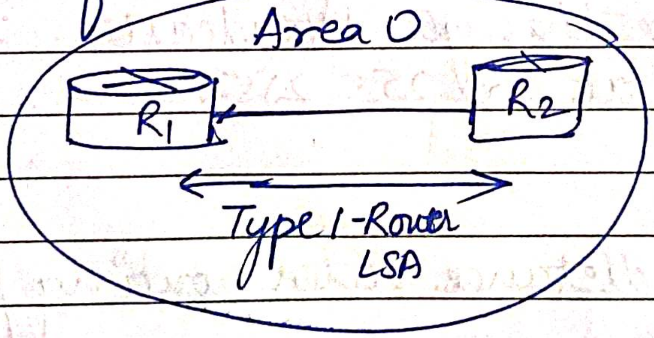
Date

- Can connect to a max^{m} of 255 routers
- Is more intelligent than RIP
- Used for med-large sized organization
- Procedure is simple & uncomplicated
- Quite accurate when it comes to selecting the most suited approach.

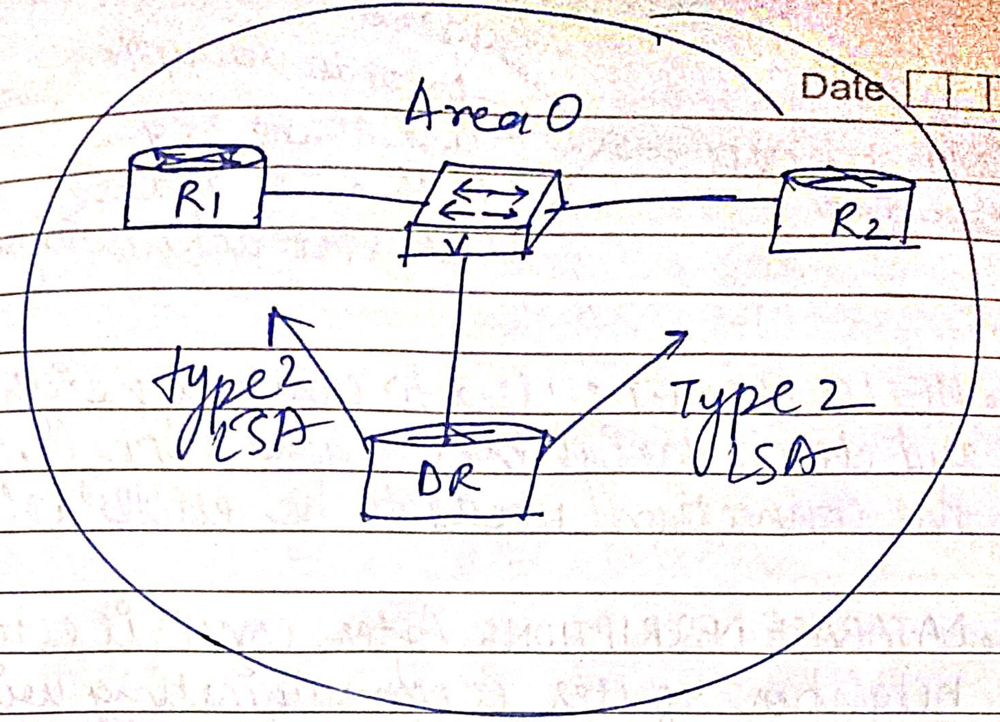
B. Router & Network LSA

LSA are messages communicated via multicast to other routers in the OSPF domain. They are sent from internal routers to DR/BDR routers to announce changes. This communication occurs on multicast address 244.0.0.6. DR announces changes to the ~~ROUTERS~~ other router via multicast address 244.0.0.5.

1. ROUTER LSA (type 1)
- packets are sent b/w routers within the same origin of area and do not leave the area.



2. NETWORK LSA (type 2)
- packets are generated by DR to describe all routers connected to its segment directly. LSA type 2 packets are flooded with neighbors in the same area of origin and remain within the area.



5. OSPF header & packet types

Version (8)	Type (8)	Message (16)
Source IP Address		
Area Identification		
Checksum	Auth.ⁿ Type	
Authentication (32)		

Version → 8 bit field, specifies OSPF protocol version
Type → specifies the type of OSPF packet, 8 bit field.
Message → 16 bit field, defines total length of message including the header
Source IP Add → a sending routing IP address, defines address from which the packets are sent.
Area identification → defines the area within which routing takes place.
Checksum → used for error detection and error correction.
Auth.ⁿ type → 2 types < 0, 1   0 → no auth.ⁿ available
1 → password based auth.
Authⁿ → 32 bit field, contains the actual value of authentication data.

Date

OSPF packets — 5
- hello
- Database description
- link state req.
- Link state update
- link state acknowledgement.

~~HELLO~~

1. HELLO PACKET: Used to create a neighborhood relⁿ and check neighbor's reachability., i.e. used when the connection needs to be established.

2. DATABASE DESCRIPTION: After connⁿ is established, if neighbor router is communicating with the system for the first time, it sends the database infoⁿ about the network topology to the system so that it can update or modify accordingly.

3. LINK STATE REQUEST: Link-state req. is sent by the router to obtain the information of a specified route. eg: router 1 & router 2.

4. LINK STATE UPDATE: Used by the router to advertise the state of its links. If router wants to broadcast the state of its links, it'll use link state update.

5. LINK STATE ACKNOWLEDGEMENT: Makes routing more reliable by forcing each router to send the acknowled. on each link state update. eg: router A, B, C.

Date

7. BGP Decision Process → path selection
→ Aggregation & dissemination

1. Path selection process

If IP prefix destⁿ is unwanted, discard the packet

↓

Apply degree of prefer. with highest local PREF attr.

↓

Originally located in BGP speaker

↓

Lowest AS no. using AS-Path ATTRIBUTE

↓

Smallest origin attribute

↓

Lowest MULTI-EXIT discriminator

↓

EBGP over IBGP

↓

Lowest cost to next hop

↓

EBGP neighbor with lowest BGP

↓

IBGP neighbours with lowest BGP

2. Aggregation & dissemination

Used after path selection

↓

possible due to CIDR

↓

Combines IP address blocks from 2 or more AS through super ~~subnetting~~netting at a downstream AS using ATOMIC-AGGREGATE and AGGREGATOR attr.

Reduces no. of routing table.

Date

10. Diff b/w all protocols in distance vector protocol family.

	RIPV1	RIPV2	IGRP	EIGRP	RIPng
Add. family	IPV4	IPV4	IPV4	IPV4	IPV6
Metric	Hop	Hop	Composite	Composite	Hop
Info. commn	Unreliable Broadcast	Unreliable Multicast	Unreliable Multicast	Reliable Multicast	Unreliable Multicast
Rout" comp"	Bellman Ford	Bellman Ford	Bellman Ford.	Diffusing Computation	Bellman Ford
VLSM/CIDR	No	Yes	NO	Yes	V6-based
Remark	Slow convergence split horizon	SC, SH	SC, SH	Fast, loop free convergence, Chatty protocol	SC, SH.

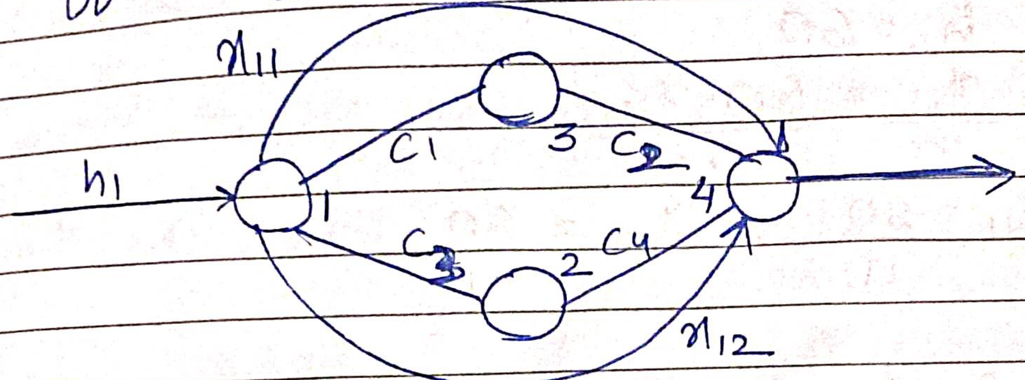
8. Protocol Message format

OPEN, UPDATE, KEEPALIVE, NOTIFICATION

Marker (16 bytes)	
length (2 byte)	Type (1 byte)

Date

3. Traffic engineering - four node network



$h_1 = x_{11} + x_{12}$
↓
traffic volume

path should be non-negative, i.e. $x_{11} \geq 0$, $x_{12} \geq 0$

$x_{11} \leq C_1$, $x_{11} \leq C_2$, $x_{12} \leq C_3$, $x_{12} \leq C_4$ $\quad$ C_1, C_2, C_3, C_4
↓
capacity constrai

minimize (x) $F = \max \left\{ \frac{x_{11}}{C_1}, \frac{x_{11}}{C_2}, \frac{x_{12}}{C_3}, \frac{x_{12}}{C_4} \right\}$

Can be written as linear programming

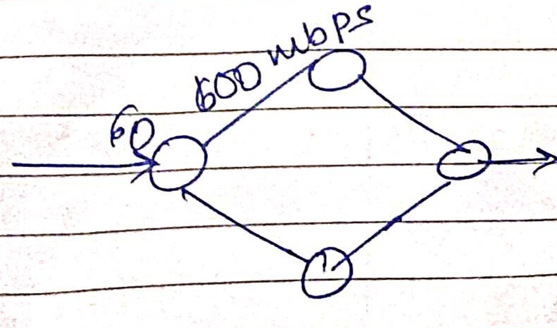
$F = r$

$x_{11} + x_{12} = h_1$

$x_{11} \leq C_1 r$, $x_{11} \leq C_2 r$, $x_{12} \leq C_3 r$, $x_{12} \leq C_4 r$

$x_{11} \geq 0$, $x_{12} \geq 0$

1. All links have same capacity



$x_{11} + x_{12} = 60$

$x_{11} \leq 100 r$

$x_{12} \leq 100 r$

$x_{11}, x_{12} \geq 0$

Date

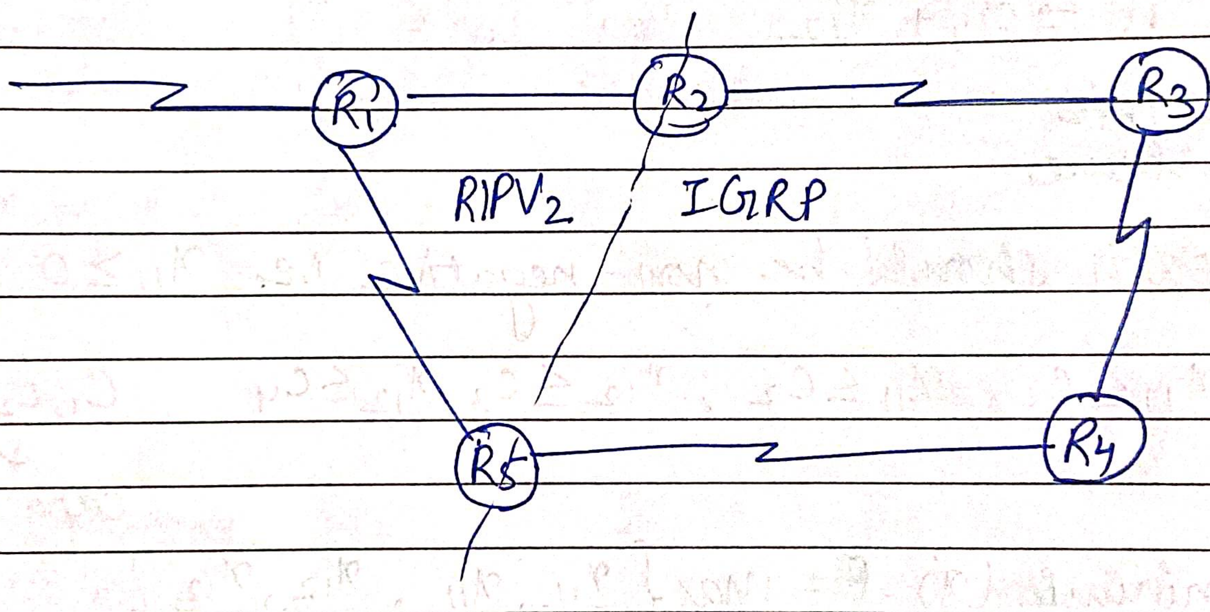
② Link capacity is different

$$\lambda_1 = 60$$

$$\frac{x_{11}}{10} = \frac{60 - x_{11}}{100}$$

$$x_{11} = \frac{60}{11}, \quad x_{12} = \frac{60}{11}.$$

SAQ: Q15 Route Redistribution



Unit 5

Date

Q1. Wireless Routing Protocol

Based on routing information update Mechanism

1. Table driven → Proactive, route is known,
   eg – DSDV, CGSR
2. On-demand → Reactive, route is created when there is data.
   eg → DSR, AODV
3. Hybrid → Mix of proactive & reactive
   eg → ZRP.

Q2. Issues in designing a routing protocol.

1. Mobility: frequent path breaks, wireless network routing protocols cannot be used, freq. changing network topology.

2. Bandwidth constraint: Wireless has limited bandwidth routing protocols need to use bandwidth optimally by keeping overhead as low as possible.

3. Error-prone shared broadcast radio channel: Adhoc wireless network routing protocol interact with the MAC layer to find alt. routes through better quality links, collision of data & control packet

4. Hidden and exposed terminal problems: packets collide due to simultaneous transmission of nodes that are hidden from each other.

Date

Q 3. Table-driven routing protocol.

- Maintain global topology info. in form of tables at every node.
- Tables are maintained/updated frequently to maintain consistent and accurate network state info.
- Each node maintains routing info. to all other nodes in the network.
- When topology changes, updates are propogated throughout the network.
- eg: DSDV, CGRS, WRP, STAR.

Q4. Adv & Dis adv. of DSDV.