

## CNS

classmate  
Date \_\_\_\_\_  
Page \_\_\_\_\_

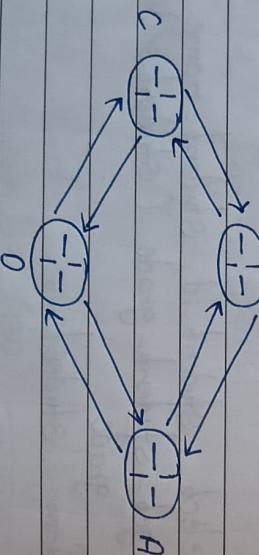
~~DEFINER is used so MySQL doesn't get confused by ; inside the function.~~

Q. Pg.no.12  
Distance Vector Routing explain.

Distance Vector Routing is a dynamic routing algorithm where each router maintains a table (vector) that stores the distance (cost) to every destination. It is used in Intra-domain routing (e.g., RIPv).

It is based on the Bellman - Ford algorithm.

B



- Features -

- Simple & easy to implement.
- Uses periodic updates
- Updates are exchanged periodically (e.g. every 30 seconds in RIPv).
- Routers send their entire routing table to neighbours.
- Protocols - RIPv, IGRP.
- Works well for small networks.

- Working:-

- ① Initialization - Each router knows only the cost to its directly connected neighbors.

- ② Sharing - Periodically, each router sends its

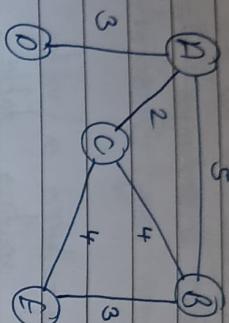
- Disadvantages -
- Slow convergence (slow speed of exchanging data).
  - Not scalable for large, complex networks.

entire routing table to all its immediate neighbors.  
e.g. it updates & exchanges the data b/w routers in every 30 seconds.

- ③ Updating - When a router receives a neighbor's routing table, it updates its own table & continues until all routers have consistent routing tables (convergence).

classmate  
Date \_\_\_\_\_  
Page \_\_\_\_\_

### Q. Short note on RIP (Routing Information Protocol)



		To cost	Next	To cost	Next	To cost	Next
To	cost			To	cost		
A	0	-	A	5	-	A	2
B	$\infty$	-	B	0	-	B	4
C	2	-	C	4	-	C	0
D	3	-	D	$\infty$	-	D	$\infty$
E	$\infty$	-	E	3	-	E	4

A's table

C's table

		To cost	Next	To cost	Next	To cost	Next
To	cost			To	cost		
A	0	-	A	$\infty$	-	A	2
B	$\infty$	-	B	3	-	B	4
C	2	-	C	4	-	C	0
D	3	-	D	$\infty$	-	D	$\infty$
E	$\infty$	-	E	3	-	E	4

B's Table

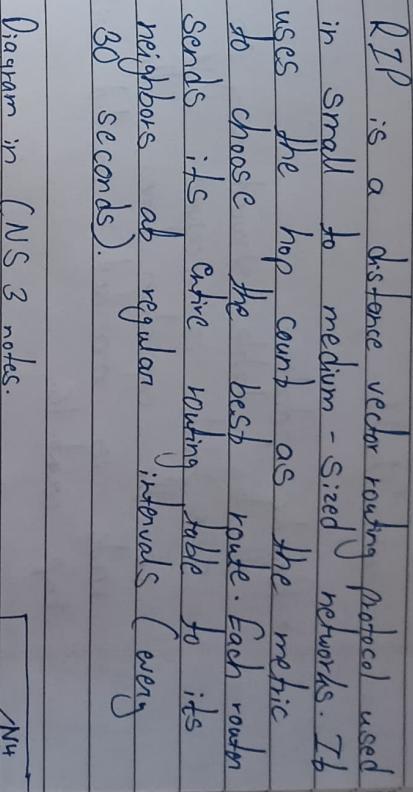


Diagram in CNS 3 notes.

		To cost	Next	To cost	Next	To cost	Next
To	cost			To	cost		
N1	3	-	N2	$\infty$	-	N3	$\infty$
N2	$\infty$	-	N1	3	-	N4	$\infty$
N3	2	-	N2	4	-	N1	$\infty$
N4	0	-	N3	$\infty$	-	N2	$\infty$
N5	$\infty$	-	N4	0	-	N3	$\infty$

E's table

Hop counts in RIP.

key features.

Routing protocols  
↓  
Intra-domain

Intra-domain

\* Distance vector protocol.

Distance Vector

Link State

Path vector

(RIP)

(OSPF)

Distance Vector

Link State

Path vector

(RIP)

(OSPF)

## Q. Link state Routing.

- 16 hops = infinite, route considered unreachable.

- Periodic updates.
- Routing table shared every 30 seconds.
- If no update is received within 180 sec i.e. the expiration timer, then the route is marked invalid with hop count 16.

### \* Advantages.

- Easy to configure.
- Simple to implement.
- Low resource usage.
- Suitable for small & medium networks.

### \* Limitations.

- Max hop = 15  $\rightarrow$  not suitable for large networks.
- Slow convergence.

### Working.

#### 1) Neighbor Discovery.

Router identifies its directly connected neighbors using HELLO packets.

#### 2) Flooding of LSPs.

LSPs are broadcasted to all routers using controlled flooding.

#### 3) Shortest Path Calculation.

- Router runs Dijkstra's Algorithm to compute the shortest path tree.

Ans:-

Link state routing is a dynamic routing algo in which every router builds a complete map of the network & calculates the shortest path using Dijkstra's Shortest Path First (SPF).

algo. Each router does not rely on neighbours routing tables. Instead it advertises the state of its own links to all routers in the network.

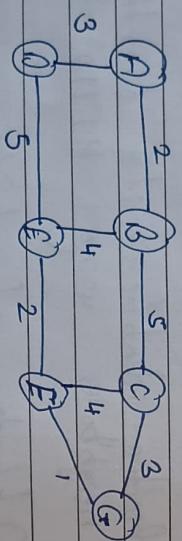
Q. Short note - ARP. (Address Resolution Protocol)

Ans:-

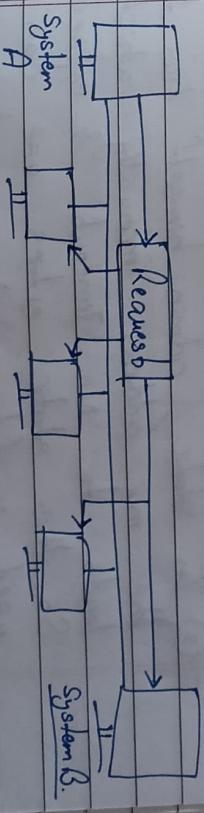
- ARP is a network layer protocol.
- ARP is used to map a logical IP address to its corresponding MAC Address with a LAN. Here MAC is media access control.
- Since communication at the data link layer requires MAC addresses ARP is essential to enable IP-based communication inside a local network.

Examples of Link State Protocols.

- OSPF (Open Shortest Path First).



- ARP Cache is a table stored in the host's memory that keeps recently resolved IP to MAC address mappings.
- Purpose: avoids broadcasting an ARP request every time; if the mapping is already in the cache, the host can directly use it.

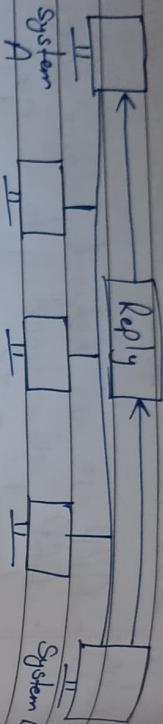


ARP request is broadcasting.

A	B	C	D	E	F	G
0	2	∞	3	∞	∞	∞
A	0	2	∞	3	∞	∞
B	2	0	5	2	4	∞
C	∞	5	0	2	4	3
D	0	3	2	0	5	∞
E	∞	4	2	0	5	2
F	0	∞	4	2	0	1
G	∞	0	3	∞	2	0

## [Some diagram for RARP]

classmate  
Date \_\_\_\_\_  
Page \_\_\_\_\_



RARP reply is Unicast

- ARP Cache Types.

- ① Dynamic Entries
- ② Static Entries.

① Dynamic Entries - When we have IP address and we request MAC Address and store that in ARP cache table automatically. Then it is known as Dynamic Entries. This Entries have specific Time out after that the mac address is expired.

Q. RARP:

- Works only on in a single broadcast domain (LAN).
  - Vulnerable to ARP spoofing attacks (Hackers can send fake replies).
- Ans:-
- RARP (Reverse Address resolution protocol) is the reverse of ARP.
  - While ARP maps IP  $\rightarrow$  MAC, RARP is used to find the IP address of a device when only its MAC address is known.

- Advantages of RARP

② In static, admin himself has to put the mac address manually which leads to No Timeouts & expired. So this static entries can be used in future whenever it is needed. No need to call it again. No need to request again for same mac address.

Configurations.

- Useful for devices like diskless workstation that don't have storage to keep IP configurations.

- Automatically assigns IP's based on MAC.

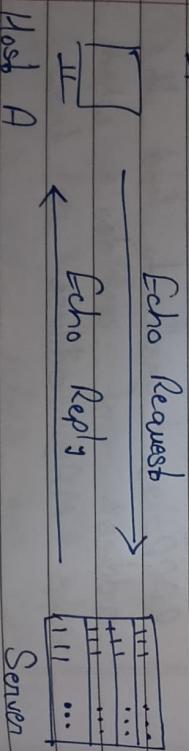
### Disadvantages

- Requires a RARP server on every network segment.
- Works only within a broadcast domain.
- Later replaced by more advanced protocols like DHCP & BootP.

### Some Common Message Types.

- Type 0 - Echo reply (Response to ping).
- Type 3 - Destination Unreachable
- Type 5 - Redirect
- Type 8 - Echo Request
- Type 11 - Time Exceeded
- Type 12 - Parameter Problem.
- Type 13/14 - Timestamp Request.

### ICMP in DDoS Attacks.

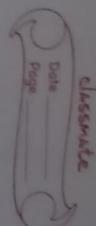
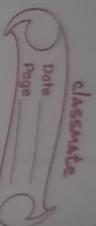


Attackers misuse ICMP for Denial of Services (DoS) attacks:

- Ping of Death -> oversized ping packets cause buffer overflow.
- ICMP Flood (Ping flood) -> excessive pings overwhelm a target.
- Smurf Attack -> ICMP requests with spoofed source IP's flood a victim.
- E.g.: If a router cannot + deliver a packet before the destination is unreachable, it sends an ICMP Destination Unreachable msg to the sender.

### ICMP Packet formats.

Type (8 bit)	Code (8 bit)	Checksum (16 bit)
Extended Header (32 bit)	Data Payload (Variable length)	



## IGMP (Internet Group Management Protocol)

Ans -

- Multicast is one to many communication (e.g. stock updates, live streaming).
- IP supports multicast addressing.
- IGMP is not routing protocol instead, it manages group membership.
- Used locally in LAN b/w hosts & multicast routers.

## Q. Mobile IP

Ans -

- Mobile IP is a protocol that enables a host or node to move across different networks while maintaining the same permanent IP address.
- This ensures continuous computing activities without interruption when the host changes its point of attachment.

## ② Routing

- Routing is a process of selecting the best path for data to travel from the source to the destination.
- Routing protocols (RIP, OSPF, BGP, etc.) help routers discover & maintain routes.

## ③ Packet Forwarding

- Once the route is decided, the network layer forwards packets to the next hop router or to the final destination using the routing table.

The major functions of Network Layer are:-

## Logical Addressing

- Network Layer assigns IP addresses to devices so communication can occur between devices networks.

- Each device has a unique logical IP address used to identify the sender & receiver.

## Q.

- Ans -
- 1. The network layer (Layer 3) of the OSI model is responsible for delivery of packets from the source of the destination across multiple network. It performs logical addressing, routing & forwarding of data.

## ① Packet Fragmentation & Reassembly

- If a packet is larger than the network, the network layer breaks it into smaller fragments. At the destination the fragments are reassembled to get the original packet.

### ⑤ Congestion Control.

- The network layer helps detect & manage network congestion (overloaded routers). It may drop packets or apply techniques like traffic shaping & load sharing.

### ⑥ Error Handling & Diagnostics

- The network layer supports error reporting & diagnostics using protocols such as ICMP (e.g. Destination Unreachable)

### ⑦ QoS (Quality of Service)

- Network Layer provides priority or guaranteed bandwidth for certain traffic (e.g. voice / video) to ensure high-quality transmission.