Types of Routing Algorithms: DVR, LSR, PVR & Count to Infinity problem

Complete Course on Computer Networks for GATE 2023 & 2024

Sweta Kumari • Lesson 13 • Feb 23, 2022

NETWORK LAYER

Sweta Kumari

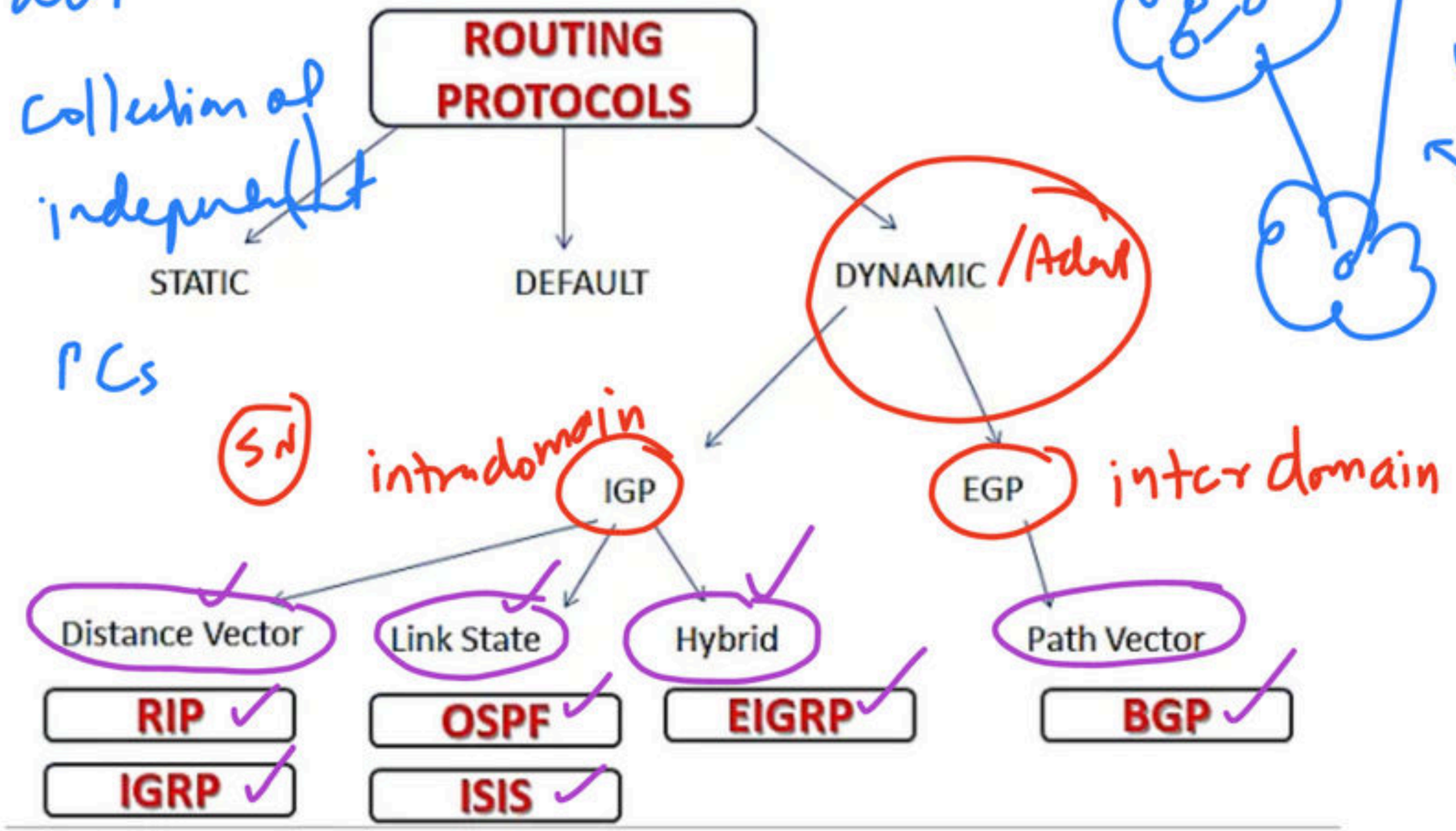
- Verified EDUCATOR For UGC NET Computer Science @GATE NoteBook
- Verified EDUCATOR For GATE CS IT @UNACADEMY

- Having 5 years Teaching Experience For UGC NET , GATE CS & Placements
- Teaches all Core CS/IT subjects.

Routing is a process which is performed by layer 3 (or network layer) devices in order to deliver the packet by choosing an optimal path from one network to another.

autonomous system —

collection of independent



IGP / Intradomain

Interior Gateway Protocol within AS

EGP / Interdomain

Exterior Gateway Protocol

b/w diff AS

WITHIN AS

IGP – Interior Gateway protocol

RIP – Routing Information protocol

IGRP – Interior Gateway Routing protocol

DVR

Distance Vector Routing

IGP / INTRADOMAIN

LSR (LINK STATE ROUTING)

SW

OSPF – Open Shortest Path First

ISIS – Intermediate system to Intermediate system

Hybrid Routing

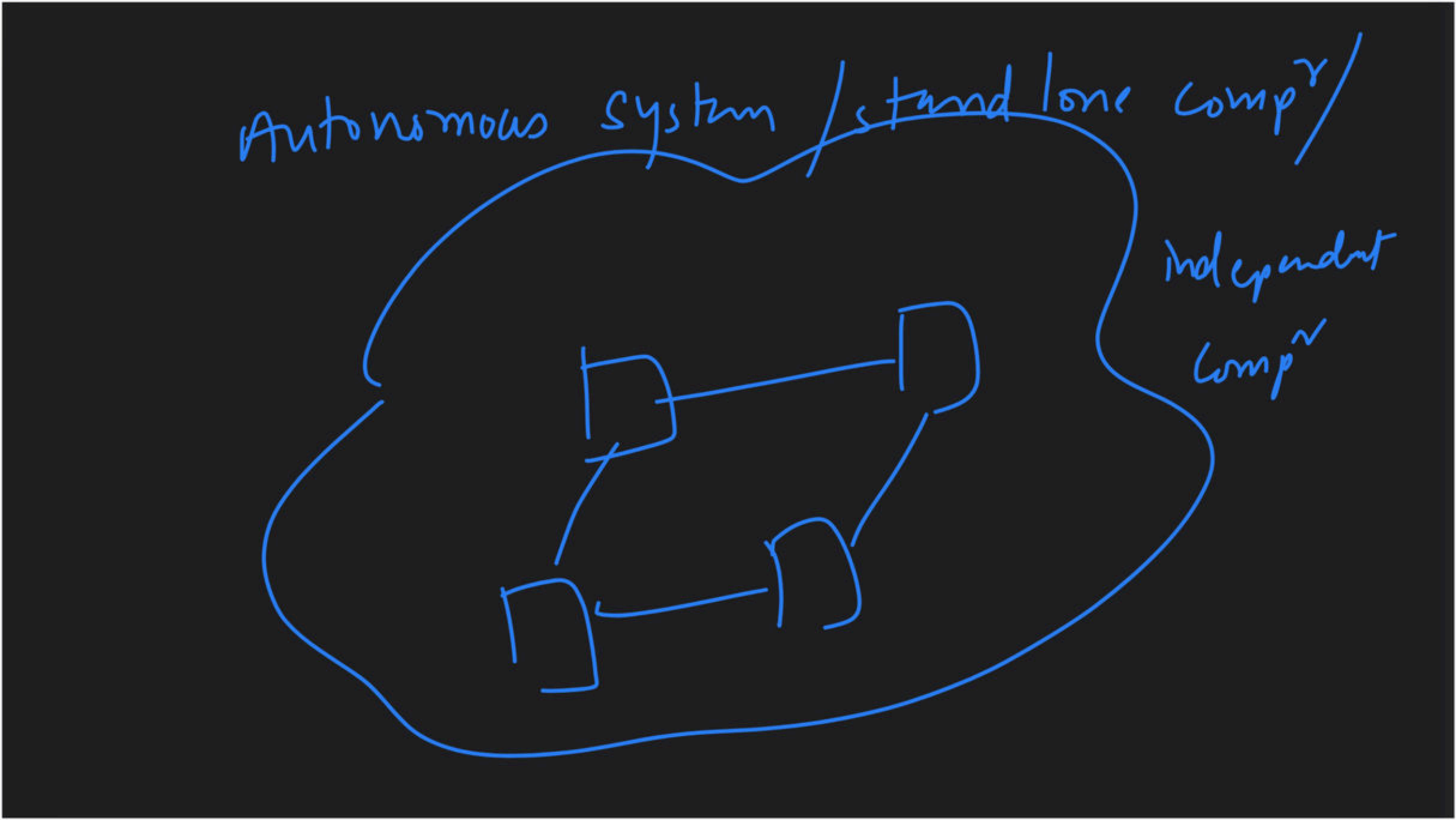
EIGRP – Enhanced Interior Gateway Protocol

Among Different AS (autonomous system)

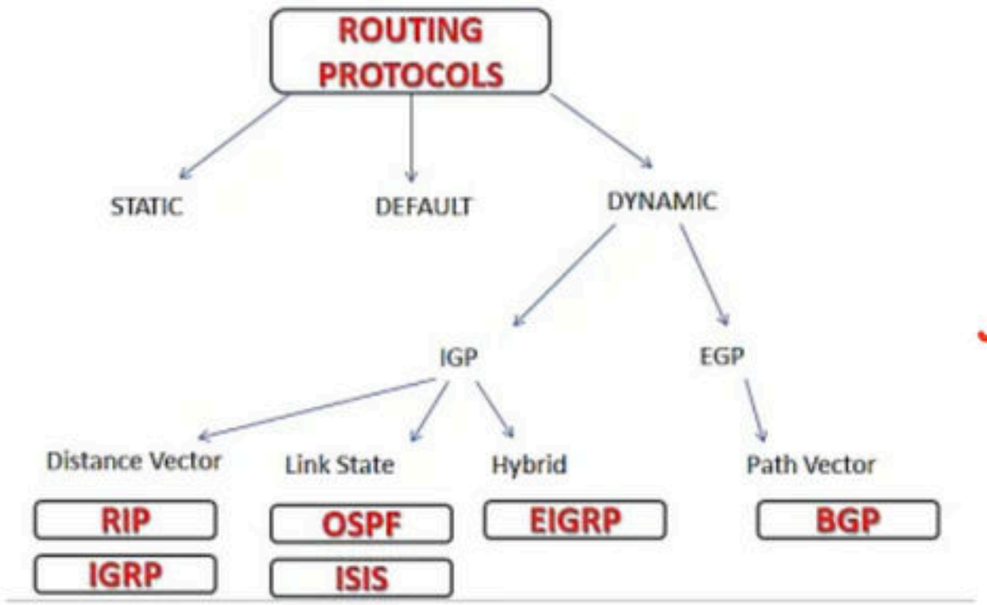
[EGP (Exterior Gateway Protocol) / Interdomain]

↳ Path Vector Routing

↳ BGP [Border Gateway Protocol) ✓


Autonomous System / standalone comp^r
Independent comp^r

Routing is a process which is performed by layer 3 (or network layer) devices in order to deliver the packet by choosing an optimal path from one network to another.



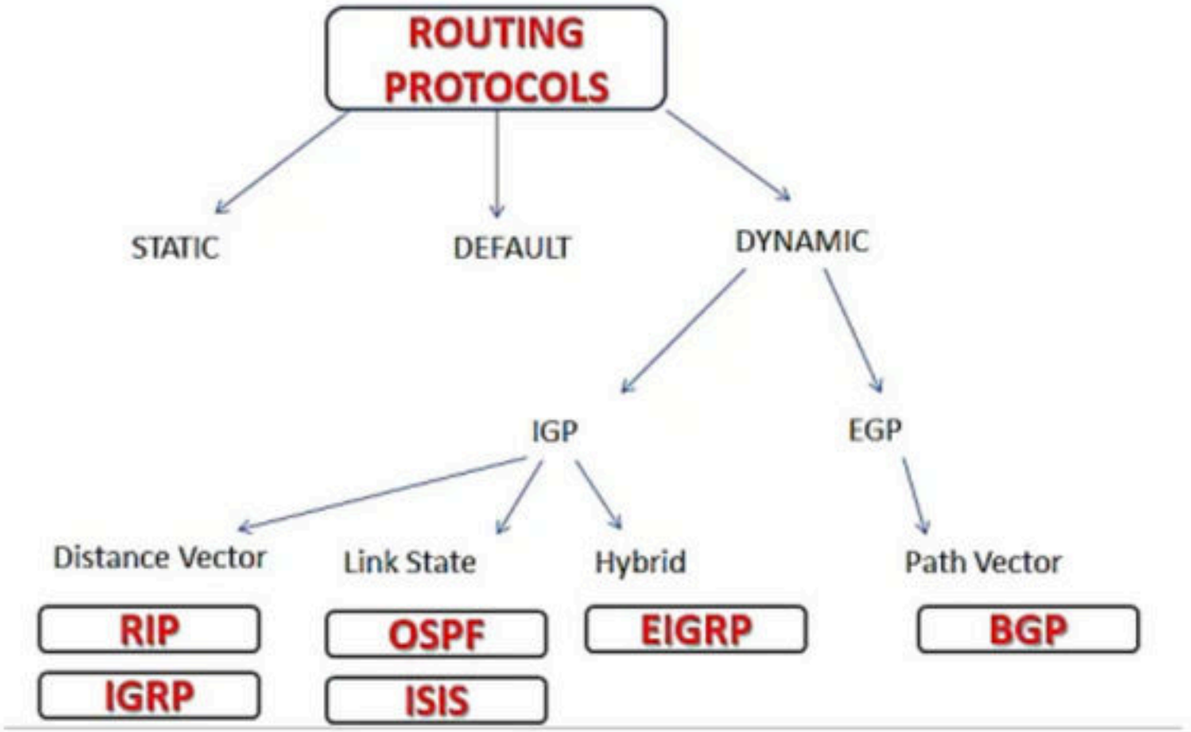
NON ADAPTIVE ALGORITHMS / STATIC ROUTING

= do not change their routing decisions once they have been selected.

ADAPTIVE ALGORITHM/ Dynamic Routing

= Change their routing decisions whenever network topology or traffic load changes.

= Use dynamic information such as current topology, load, delay, etc. to select routes.



IGP – Interior Gateway Protocol
EGP – Exterior Gateway Protocol
RIP – Routing Information Protocol
IGRP – Interior Gateway Routing Protocol
OSPF – Open Shortest Path First
ISIS – Intermediate System to Intermediate System
EIGRP – Enhanced Interior Gateway Routing Protocol
BGP – Border Gateway Protocol

Dynamic routing makes automatic adjustment of the routes using protocols. RIP and OSPF are the best examples.
More Bandwidth + Less Secure + Find Best Route

DEFAULT Routing = Router is configured to send all packets towards a single router (default router).
It is generally used with stub routers.
A stub router is a router which has only one route to reach all other networks.

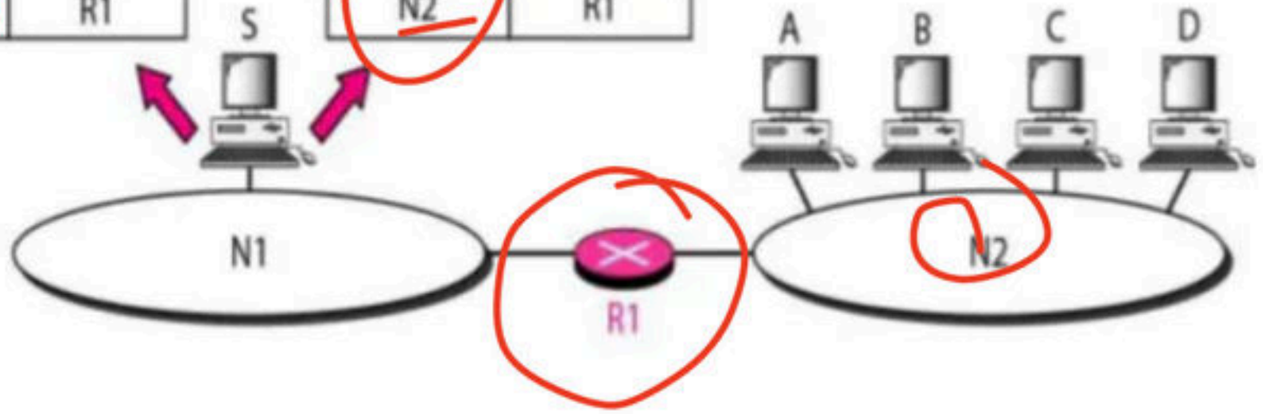
2 types of Routing Table

Routing table for host S based on host-specific method

Destination	Next hop
A	R1
B	R1
C	R1
D	R1

Routing table for host S based on network-specific method

Destination	Next hop
N2	R1



EXAMPLE

a. Routing tables based on route

Destination	Route
Host B	R1, R2, host B

Routing table for host A

Destination	Route
Host B	R2, host B

Routing table for R1

Destination	Route
Host B	Host B

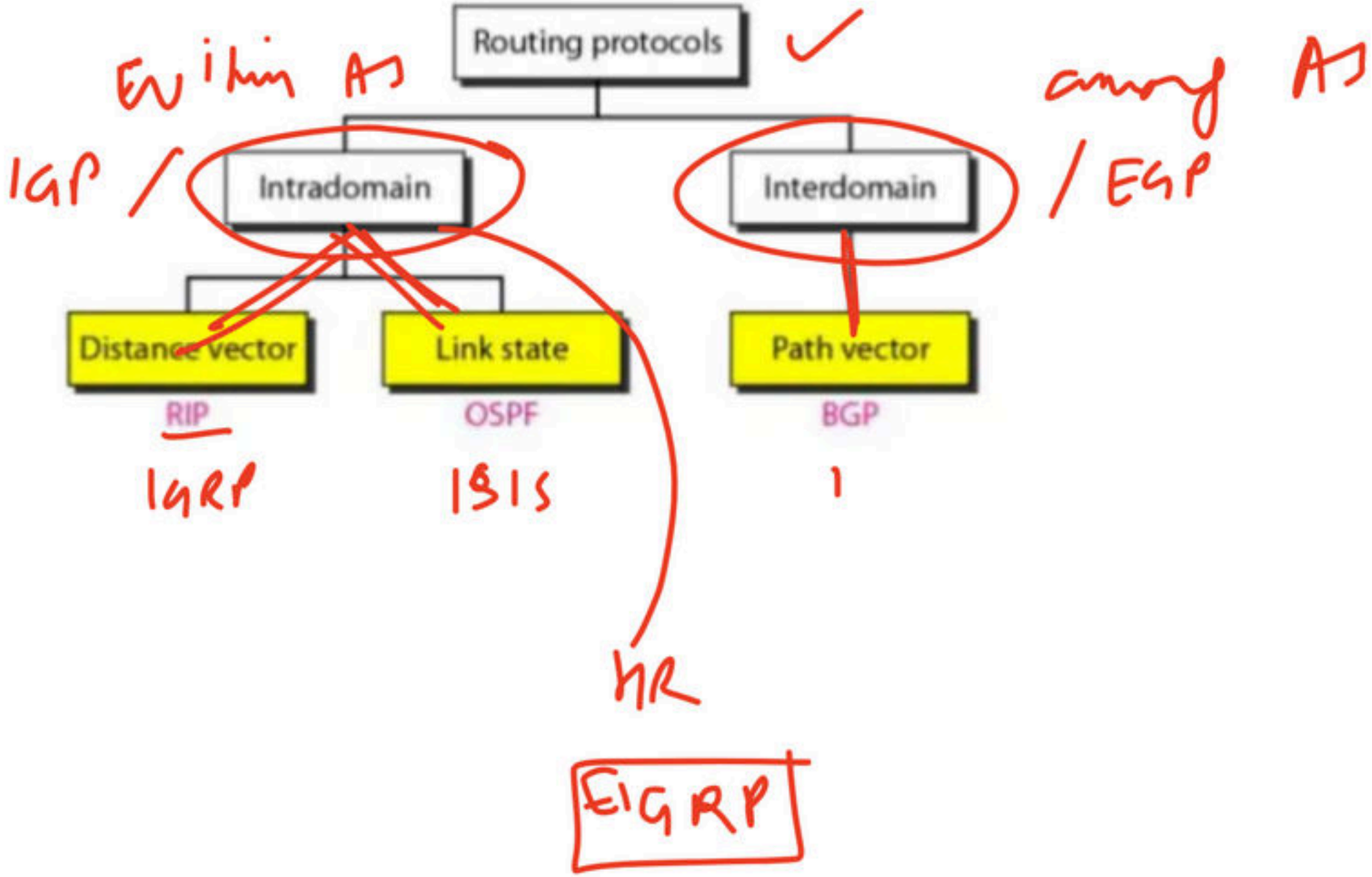
Routing table for R2

b. Routing tables based on next hop

Destination	Next hop
Host B	R1

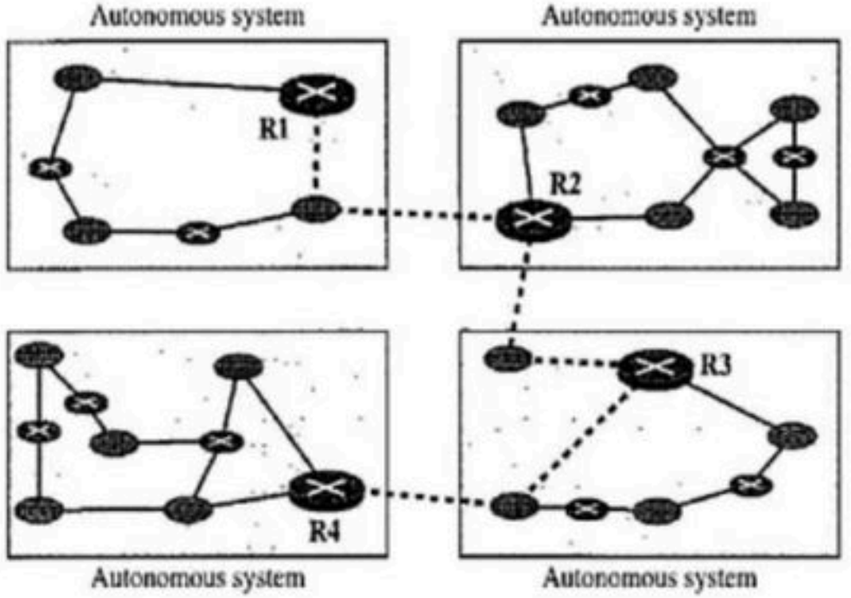
Destination	Next hop
Host B	R2

Destination	Next hop
Host B	—


Routing protocols
Intradomain
Interdomain
Distance vector
Link state
Path vector
RIP
OSPF
BGP

INTRADOMAIN & INTERDOMAIN ROUTING

Today, an internet can be so large that one routing protocol cannot handle the task of updating the routing tables of all routers. For this reason, an internet is divided into autonomous systems. An **autonomous system (AS)** is a group of networks and routers under the authority of a single administration. Routing inside an autonomous system is referred to as **intradomain routing.** Routing between autonomous systems is referred to as **interdomain routing.** Each autonomous system can choose one or more intradomain routing protocols to handle routing inside the autonomous system. However, only one interdomain routing protocol handles routing between autonomous systems (see Figure 22.12).



Intra domain : link state and distance vector
Interdomain : path vector

Routing Information Protocol (RIP) is an implementation of the distance vector protocol. **Open Shortest Path First (OSPF)** is an implementation of the link state protocol. **Border Gateway Protocol (BGP)** is an implementation of the path vector protocol.

Distance Vector Routing Protocol :

Selects best path in the basis of hop counts. Ex : RIP.

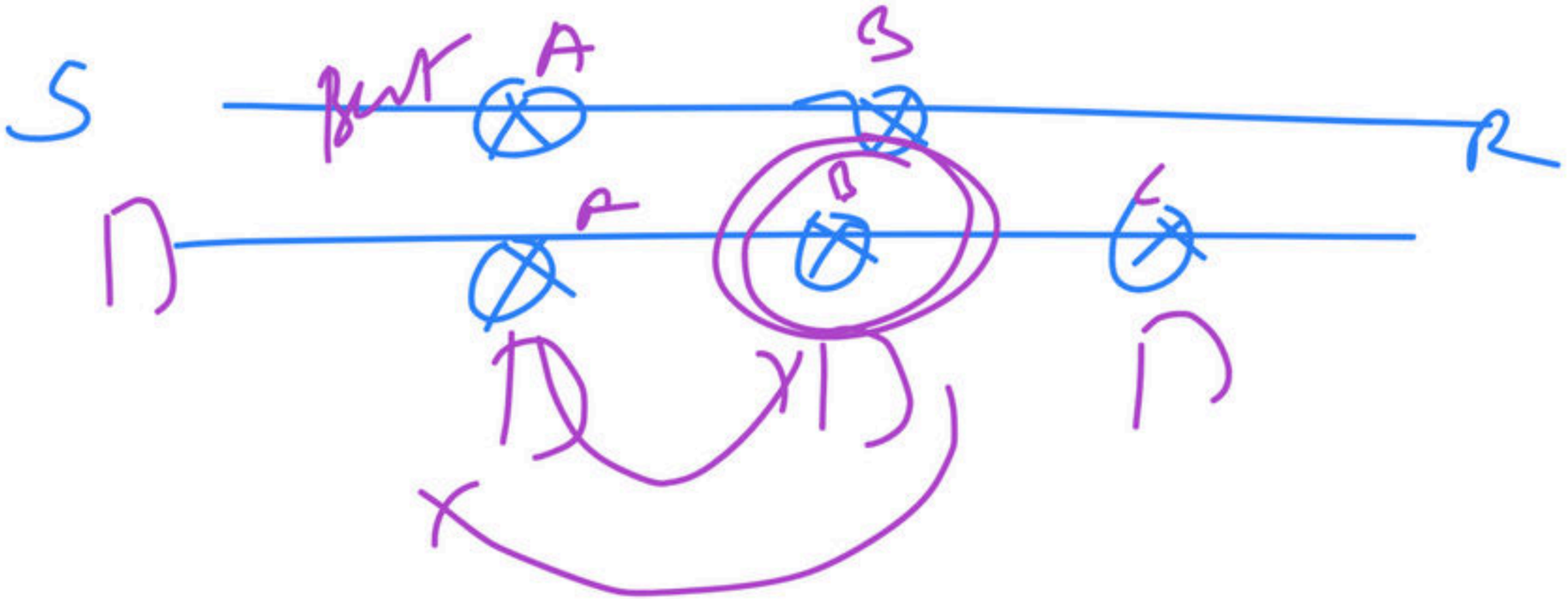
The path with least hop count is the best path.

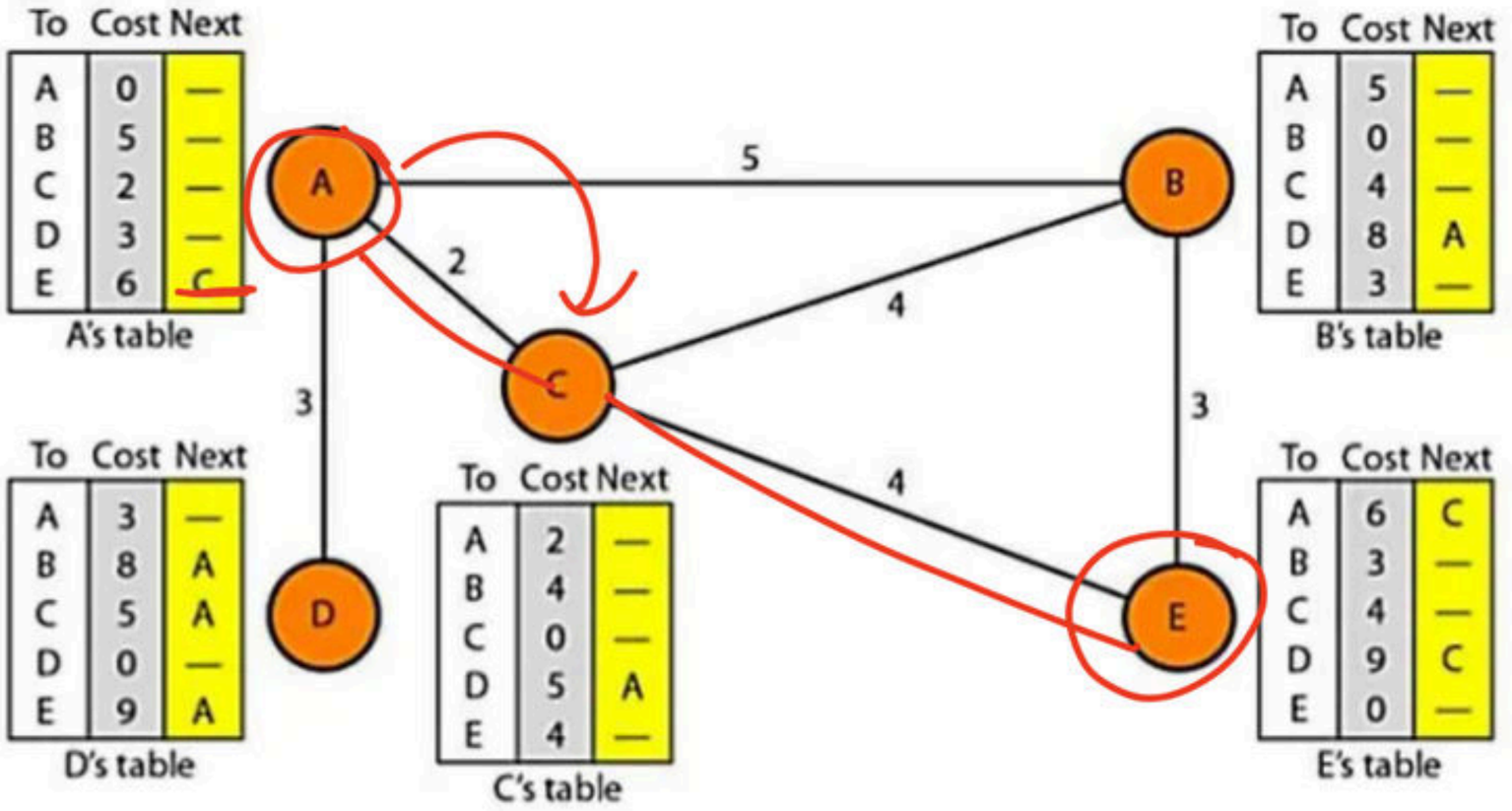
Features –

1. **Routing information is always broadcast.**

(Unnecessary TRAFFIC)

1. **Routers always trust on routing information received from neighbor routers.**
2. **Full Routing tables are exchanged (Security Issues)**

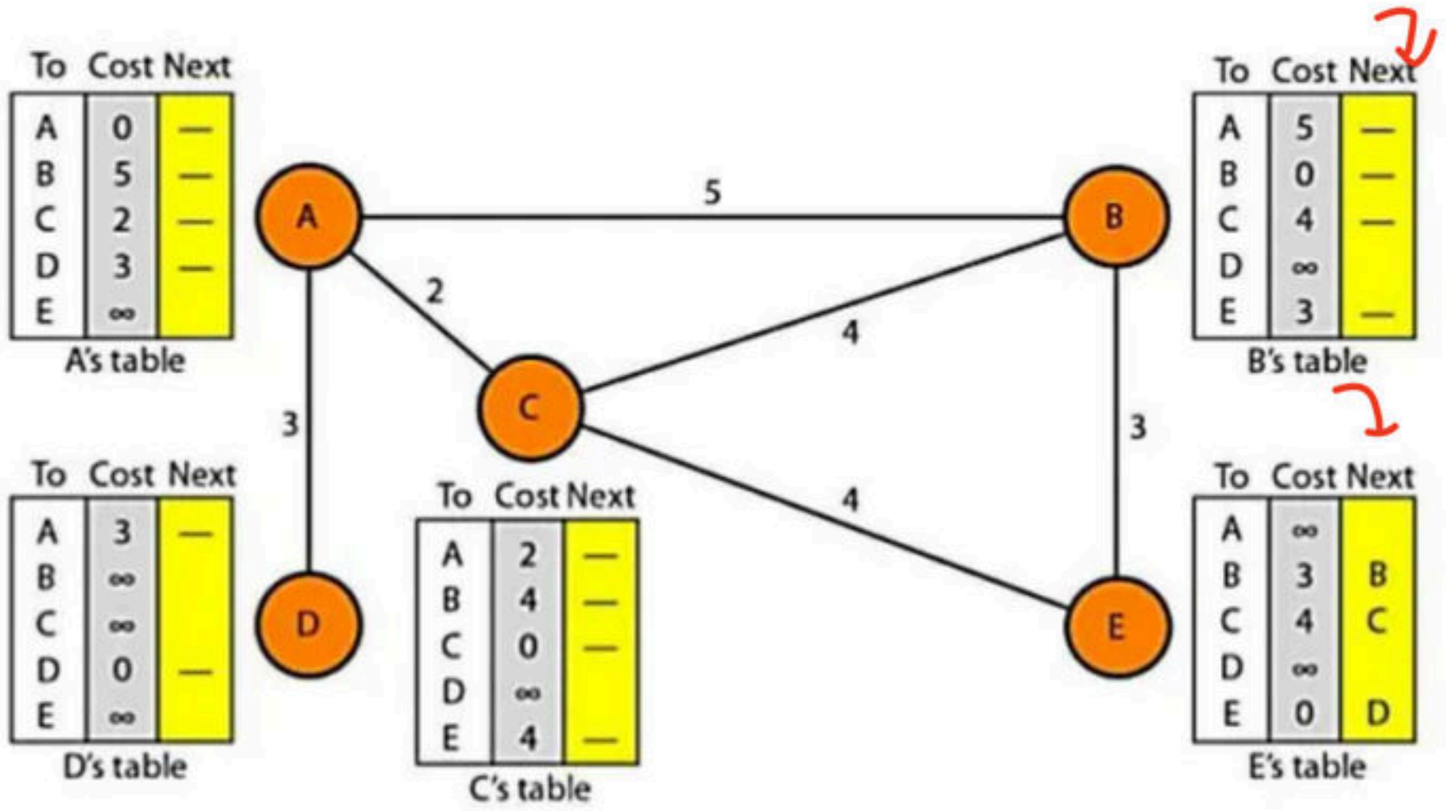


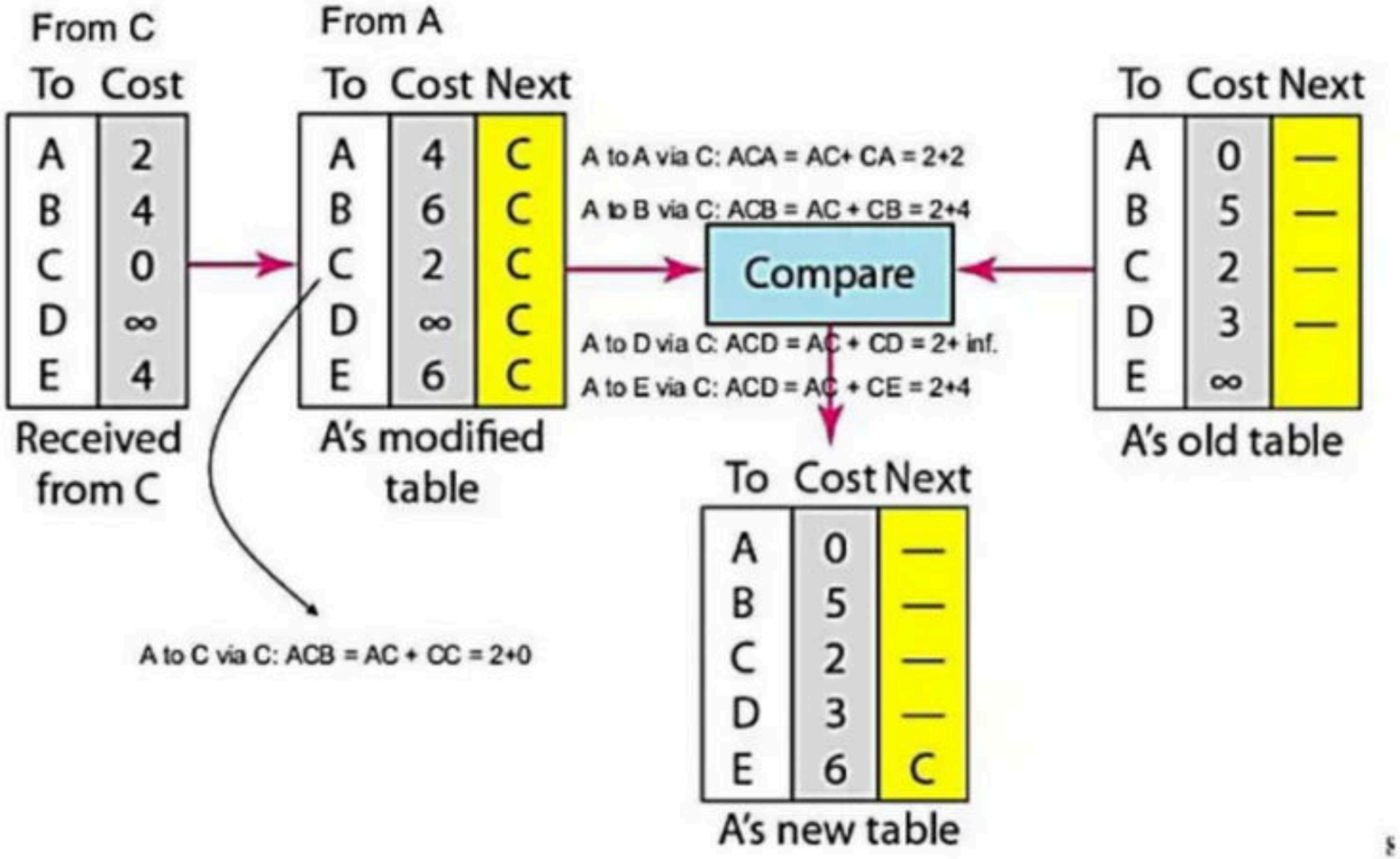


DISTANCE VECTOR ROUTING

Initialization of tables

Mark infinite for unreachable


To Cost Next
A 0 —
B 5 —
C 2 —
D 3 —
E ∞ —
A's table
A
B
C
D
E
5
2
3
4
4
3
To Cost Next
A 5 —
B 0 —
C 4 —
D ∞
E 3 —
B's table
To Cost Next
A 3 —
B ∞
C ∞
D 0 —
E ∞
D's table
To Cost Next
A 2 —
B 4 —
C 0 —
D ∞
E 4 —
C's table
To Cost Next
A ∞
B 3 B
C 4 C
D ∞
E 0 D
E's table

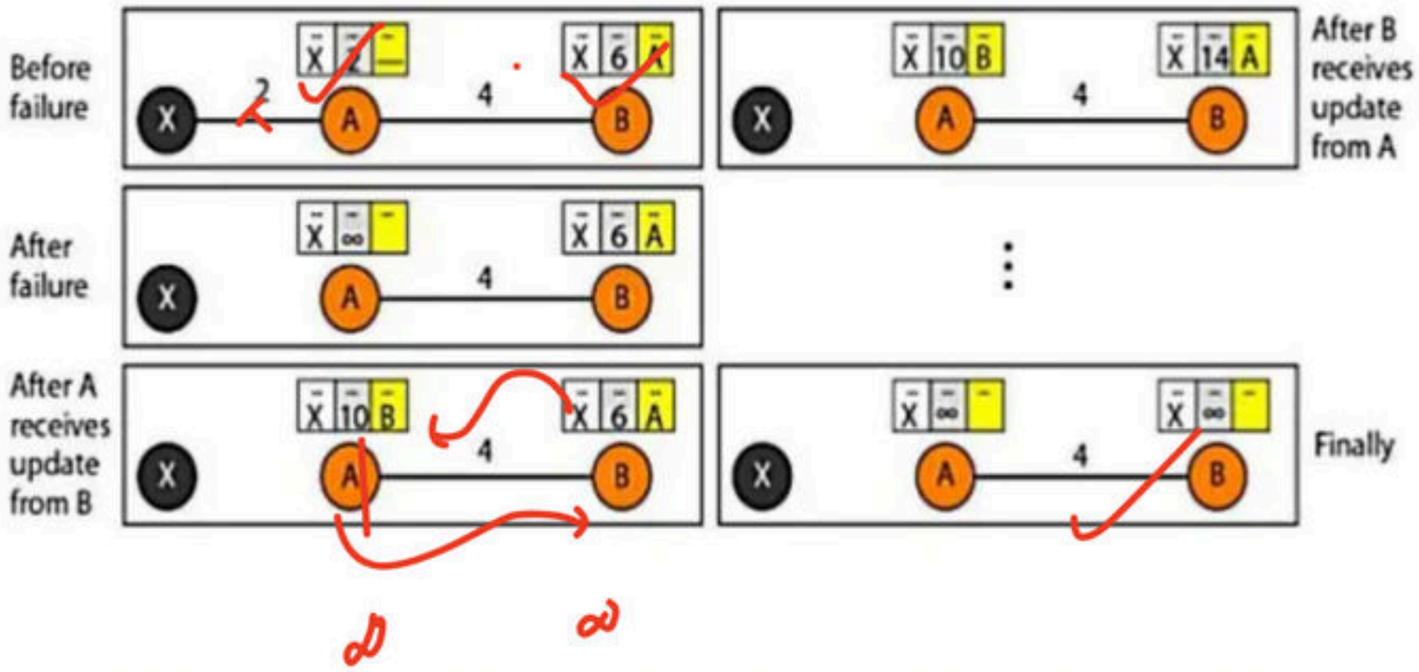


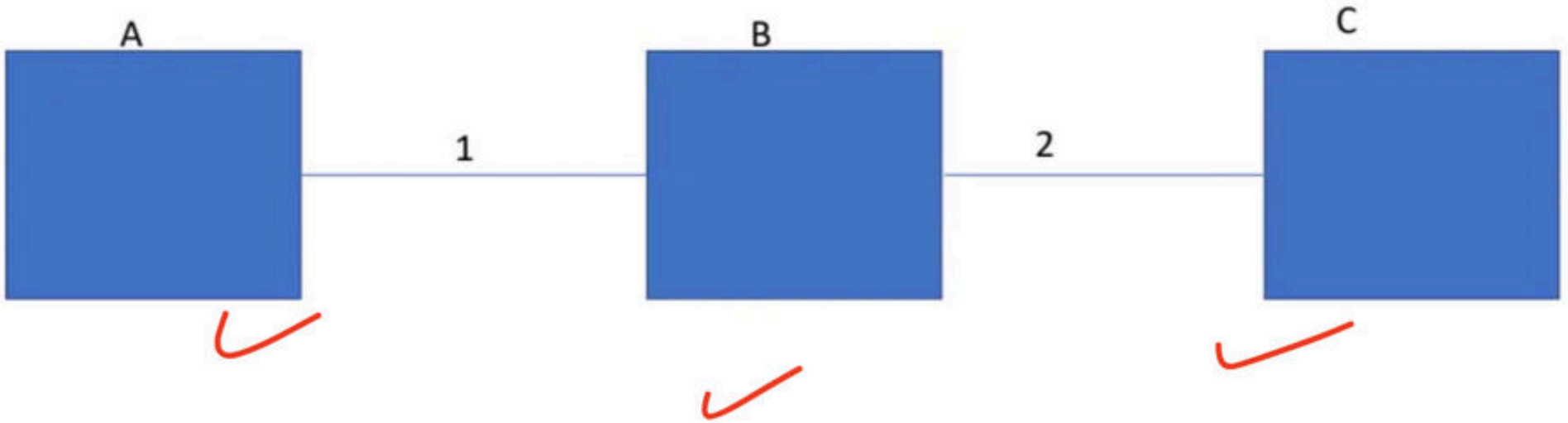
DISTANCE VECTOR ROUTING

Updating in distance vector routing : C to A

TWO NODE LOOP INSTABILITY

A problem with distance vector routing is instability, which means that a network using this protocol can become unstable. To understand the problem, let us look at the scenario depicted in Figure 22.17. the link between A and X fails.



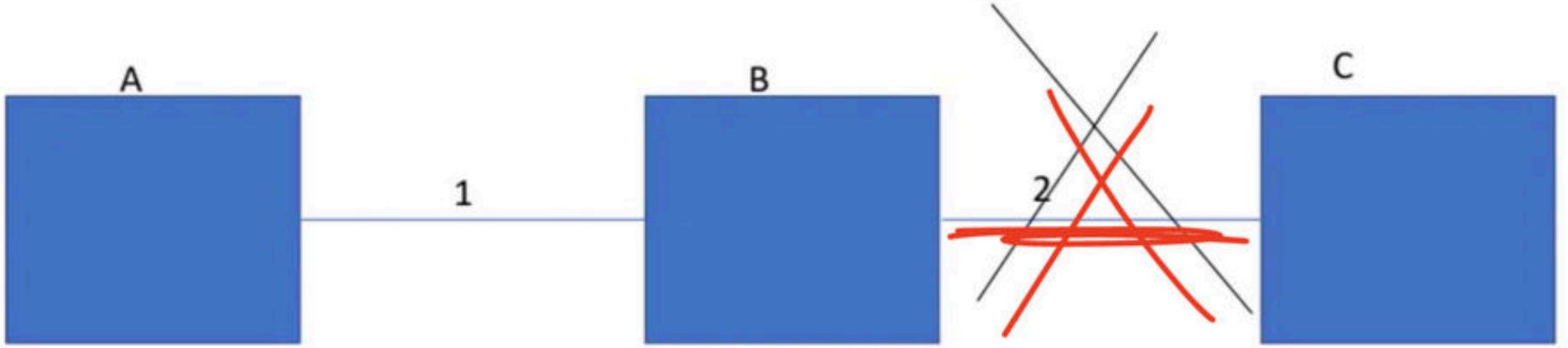


TO	COST	VIA
B	1	B
C	3	B

TO	COST	VIA
A	1	A
C	2	C

TO	COST	VIA
A	3	B
B	2	B

COUNT TO INFINITY PROBLEM IN DVR

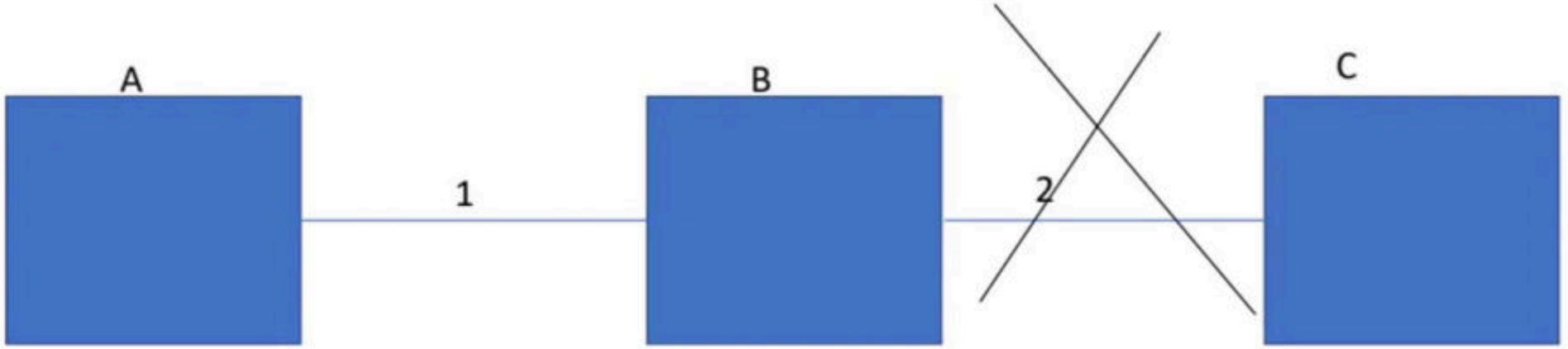


TO	COST	VIA
B	1	B
C	3	B

TO	COST	VIA
A	1	A
C		

TO	COST	VIA
A		
B		

COUNT TO INFINITY PROBLEM IN DVR

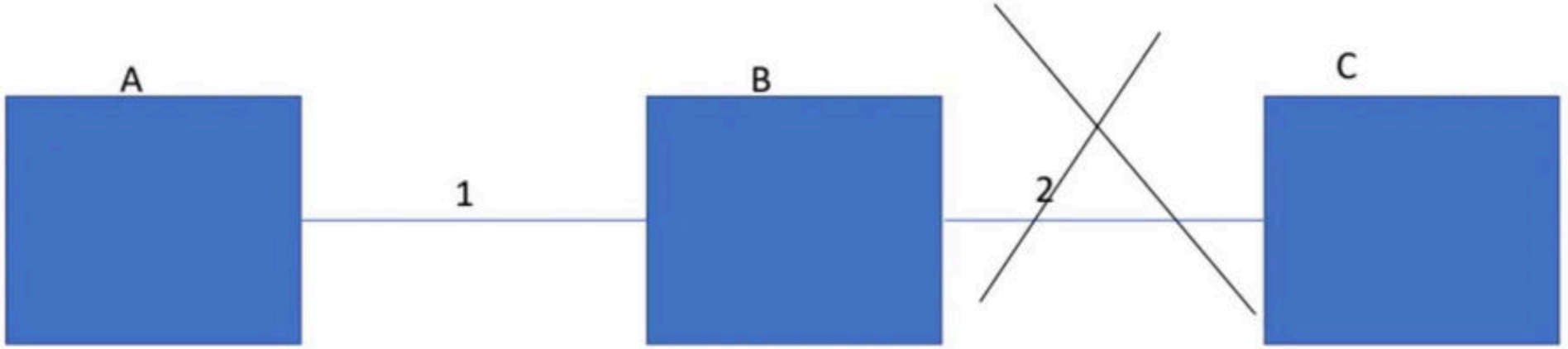


TO	COST	VIA
B	1	B
C	3	B

TO	COST	VIA
A	1	A
C		

TO	COST	VIA
A		
B		

COUNT TO INFINITY PROBLEM IN DVR

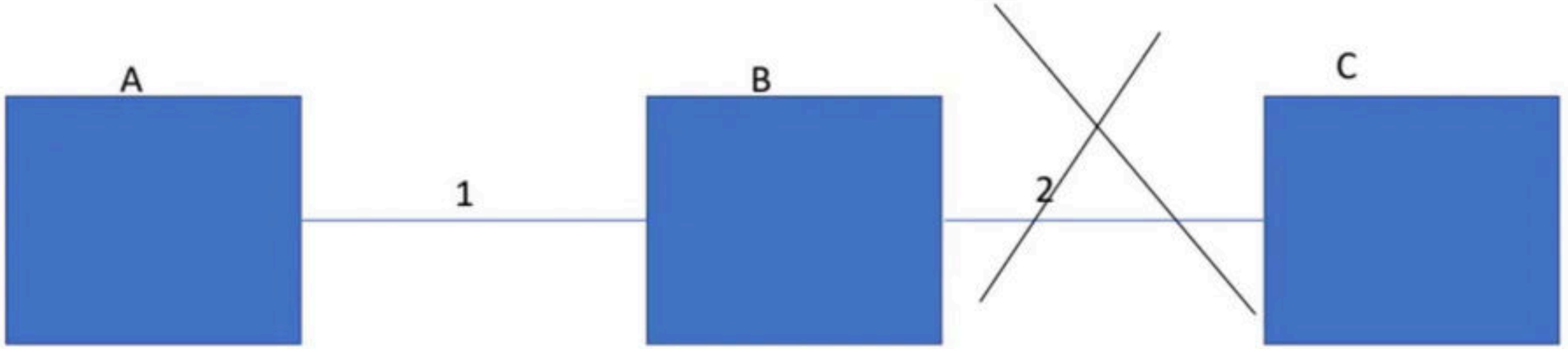


TO	COST	VIA
B	1	B
C	3	B

TO	COST	VIA
A	1	A
C	4	A

TO	COST	VIA
A		
B		

COUNT TO INFINITY PROBLEM IN DVR



TO	COST	VIA
B	1	B
C	5 - inf	B

TO	COST	VIA
A	1	A
C	4 - inf	A

TO	COST	VIA
A		
B		

COUNT TO INFINITY PROBLEM IN DVR


S
P
Q
R
(-1, 2)
11 C

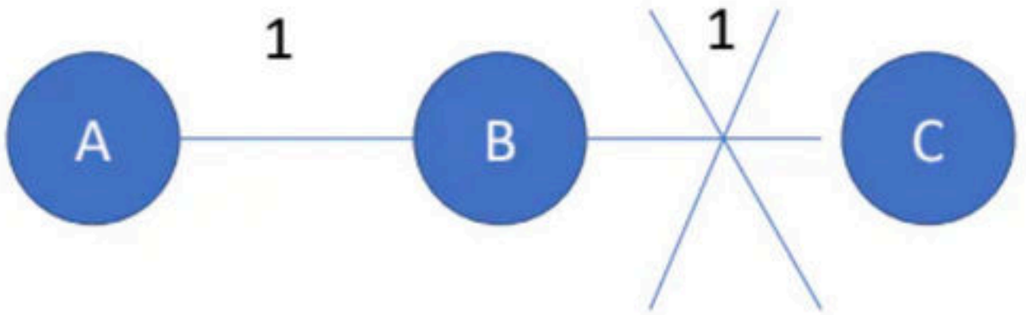
Solutions for Instability

Defining Infinity The first obvious solution is to redefine infinity to a smaller number, such as 100. For our previous scenario, the system will be stable in less than 20 updates. As a matter of fact, most implementations of the distance vector protocol define the distance between each node to be 1 and define 16 as infinity. However, this means that the distance vector routing cannot be used in large systems. The size of the network, in each direction, can not exceed 15 hops.

The main issue with Distance Vector Routing (DVR) protocols is Routing Loops, since Bellman-Ford Algorithm cannot prevent loops.

This routing loop in DVR network causes Count to Infinity Problem.

Routing loops usually occur when any interface goes down or two-routers send updates at the same time.



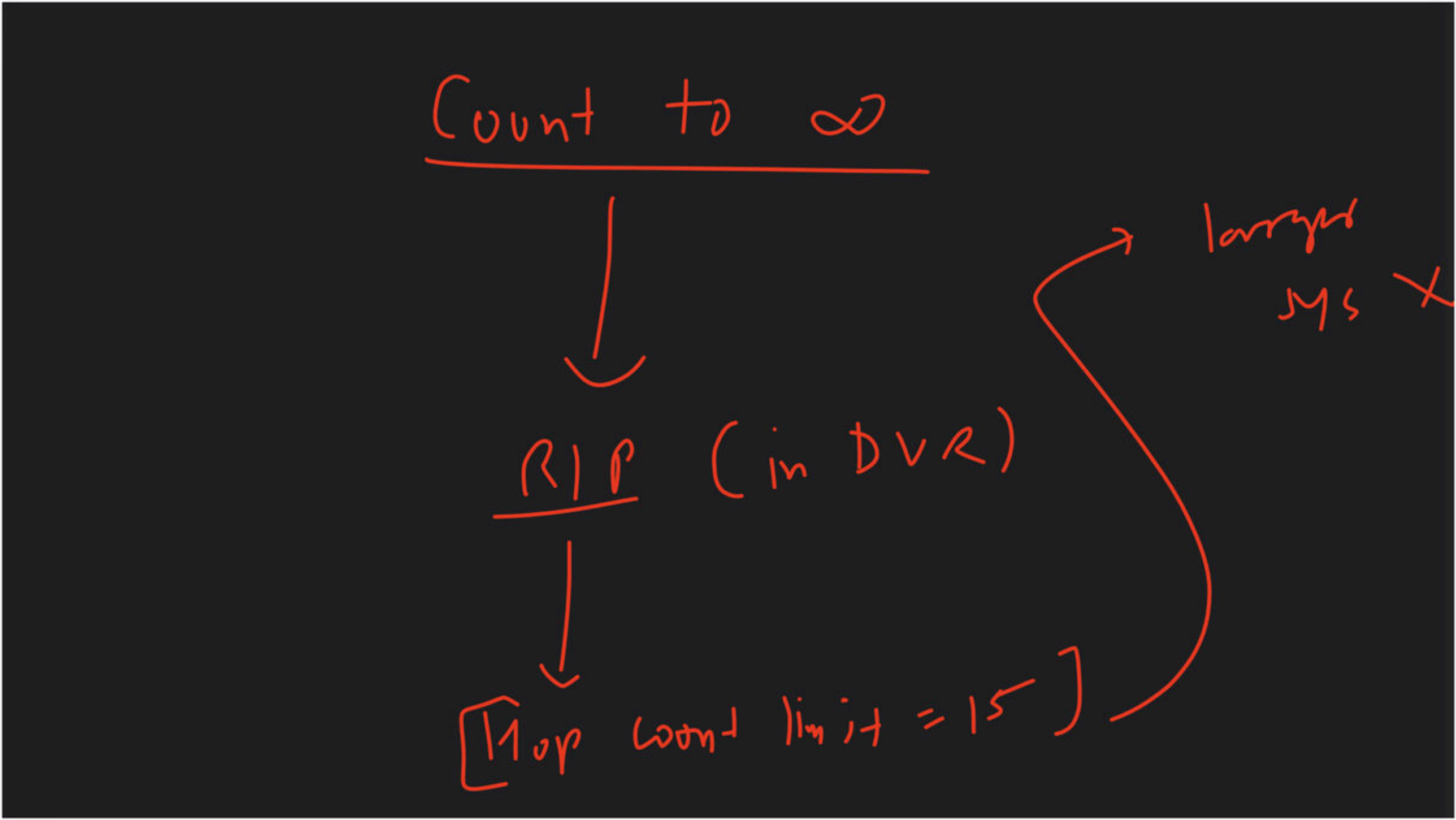
This false information will propagate to all routers . This problem is known as count to infinity.

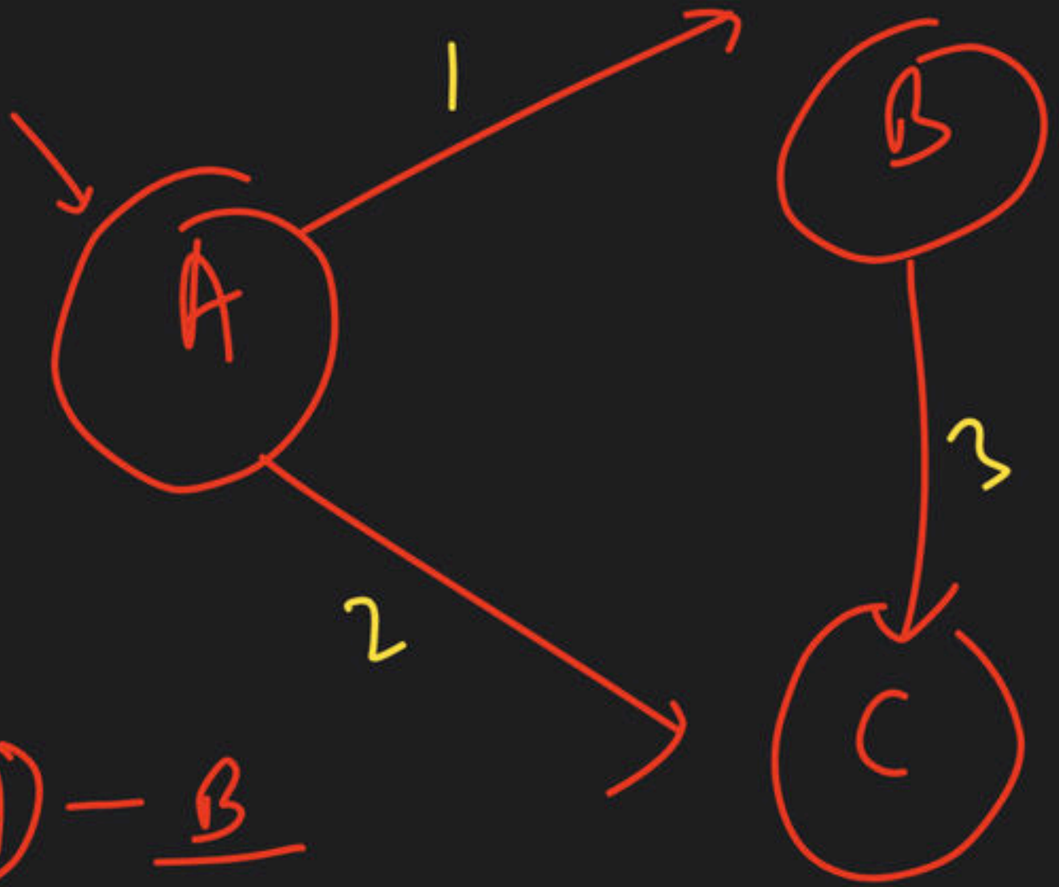
Solution to this problem is split horizon with poison reverse technique(used by RIP to reduce the chance of forming loops and uses maximum number of hop counts to counter the problem.)

1. **Split horizons** states that if a neighboring router sends a route to a router , the receiving router will not propagate this route back to the advertising router on the same interface.
2. **Split horizon with poison reverse** Make Routing announcement is to immediately remove most looping routes before they can propagate through the network.
3. **Limitations -** increase the size of routing announcements but overall efficiency of network is good in case of faults.

A → B (1)
A → C (2)
B → C (X)
Before B inform A , A inform B to go to C at cost 2.
B → A → C at cost 3
A receive msg from B (Cost updated = 4)
feeding each other bad information toward infinity which is called as Count to Infinity problem.


Relu ?


Count to ∞
RIP (in DVR)
[Hop count limit = 15]
largest sys



Bellman Dijkstra

A — B

A — C

$\begin{cases} A-B \Rightarrow 1 \\ A-C = 2 \end{cases}$

Single source shortest path

The network uses a Distance Vector Routing protocol. Once the routes have stabilized, the distance vectors at different nodes are as following.

N1: (0, 1, 7, 8, 4) N2: (1, 0, 6, 7, 3)

N3: (7, 6, 0, 2, 6) N4: (8, 7, 2, 0, 4) N5: (4, 3, 6, 4, 0)

Each distance vector is the distance of the best known path at the instance to nodes, N1 to N5, where the distance to itself is 0. Also, all links are symmetric and the cost is identical in both directions. In each round, all nodes exchange their distance vectors with their respective neighbors. Then all nodes update their distance vectors. In between two rounds, any change in cost of a link will cause the two incident nodes to change only that entry in their distance vectors. The cost of link N2-N3 reduces to 2(in both directions). After the next round of updates, what will be the new distance vector at node, N3.

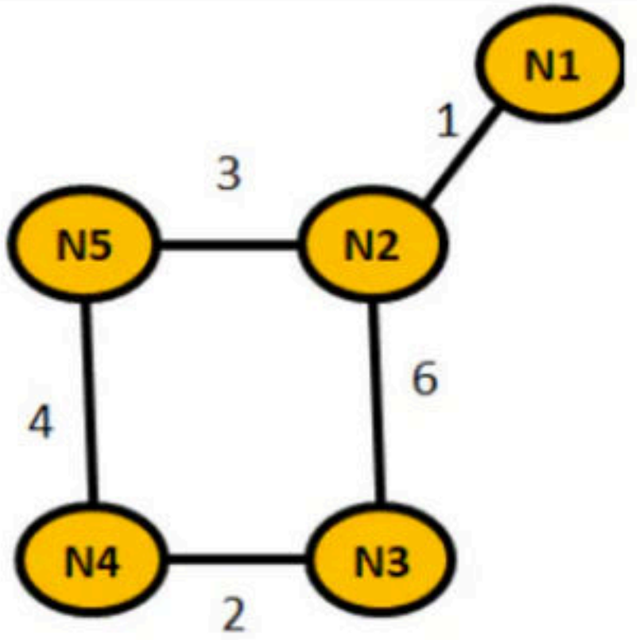
(A) (3, 2, 0, 2, 5)

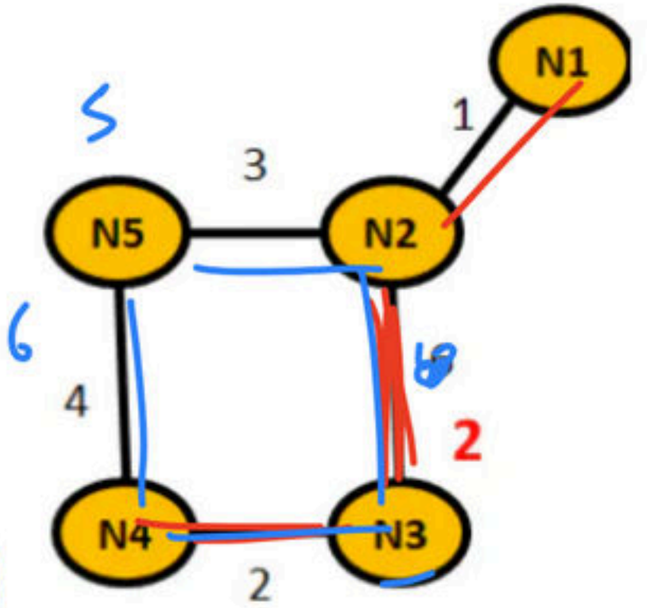
(B) (3, 2, 0, 2, 6)

(C) (7, 2, 0, 2, 5)

(D) (7, 2, 0, 2, 6)

GATE CS 2011





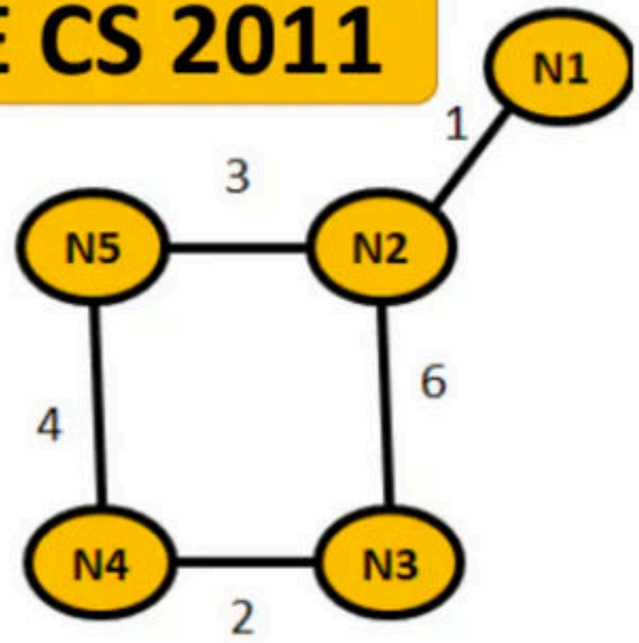
GATE CS 2011

The network uses a Distance Vector Routing protocol. Once the routes have stabilized, the distance vectors at different nodes are as following.

N1: (0, 1, 7, 8, 4) N2: (1, 0, 6, 7, 3)

N3: (7, 6, 0, 2, 6) N4: (8, 7, 2, 0, 4) N5: (4, 3, 6, 4, 0)

Each distance vector is the distance of the best known path at the instance to nodes, N1 to N5, where the distance to itself is 0. Also, all links are symmetric and the cost is identical in both directions. In each round, all nodes exchange their distance vectors with their respective neighbors. Then all nodes update their distance vectors. In between two rounds, any change in cost of a link will cause the two incident nodes to change only that entry in their distance vectors. The cost of link N2-N3 reduces to 2(in both directions). After the next round of updates, what will be the new distance vector at node, N3.



(A) (3, 2, 0, 2, 5)

(B) (3, 2, 0, 2, 6)

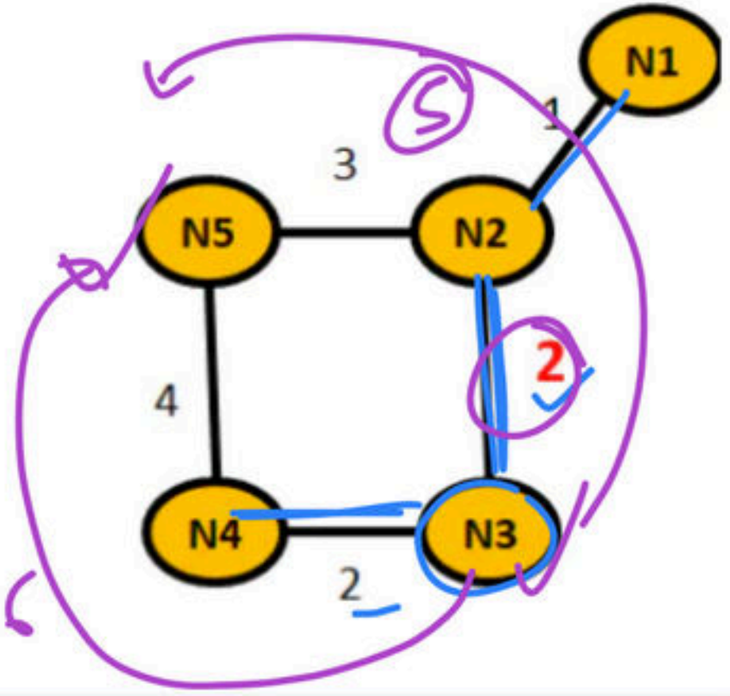
(C) (7, 2, 0, 2, 5)

(D) (7, 2, 0, 2, 6)

N3

D

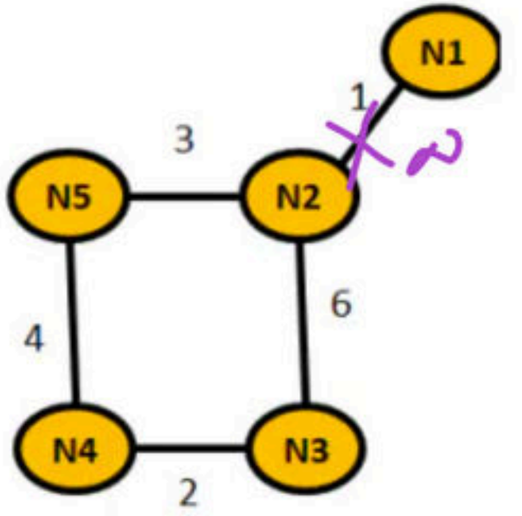
N1=	3
N2 =	2
N3 =	0
N4 =	2
N5 =	5

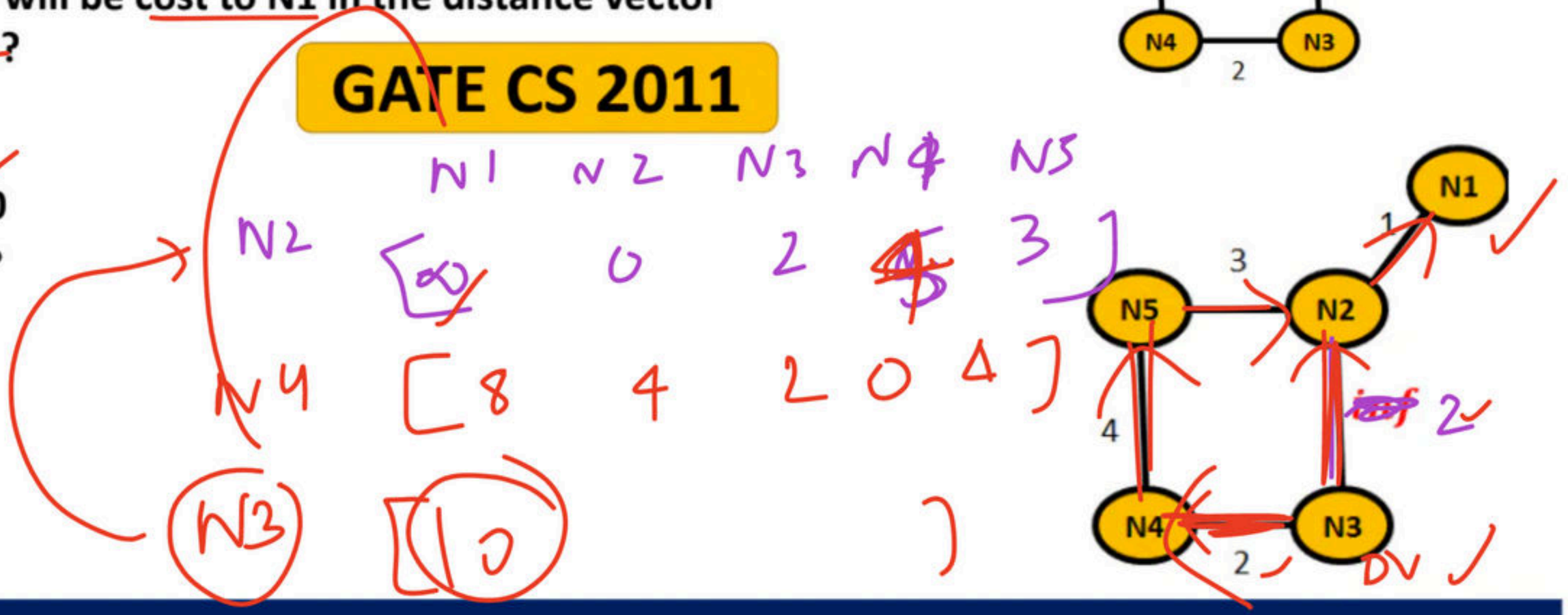


After the update in the previous question, the link N1-N2 goes down. N2 will reflect this change immediately in its distance vector as cost, ∞. After the NEXT ROUND of update, what will be cost to N1 in the distance vector of N3?

(A) 3
(B) 9
(C) 10
(D) ∞

GATE CS 2011

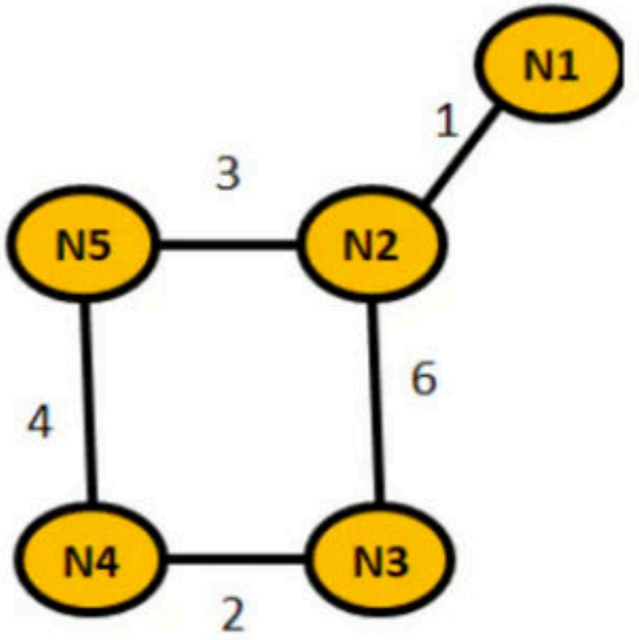


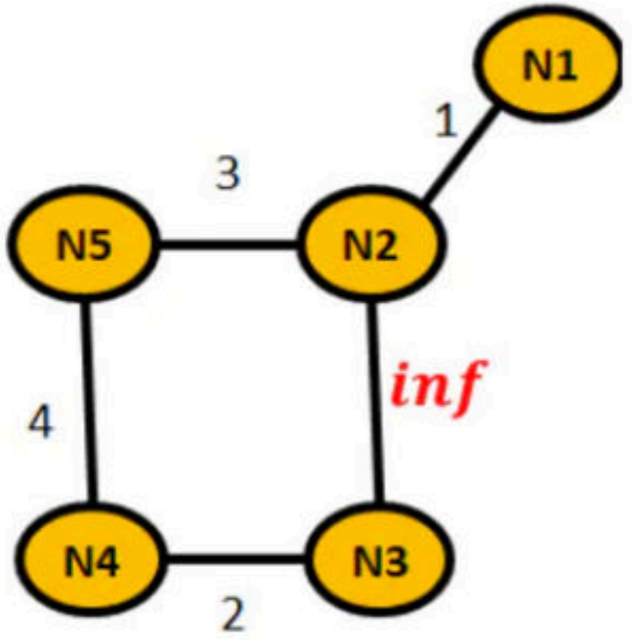


After the update in the previous question, the link N1-N2 goes down. N2 will reflect this change immediately in its distance vector as cost, ∞. After the NEXT ROUND of update, what will be cost to N1 in the distance vector of N3?

(A) 3
(B) 9
(C) 10
(D) ∞

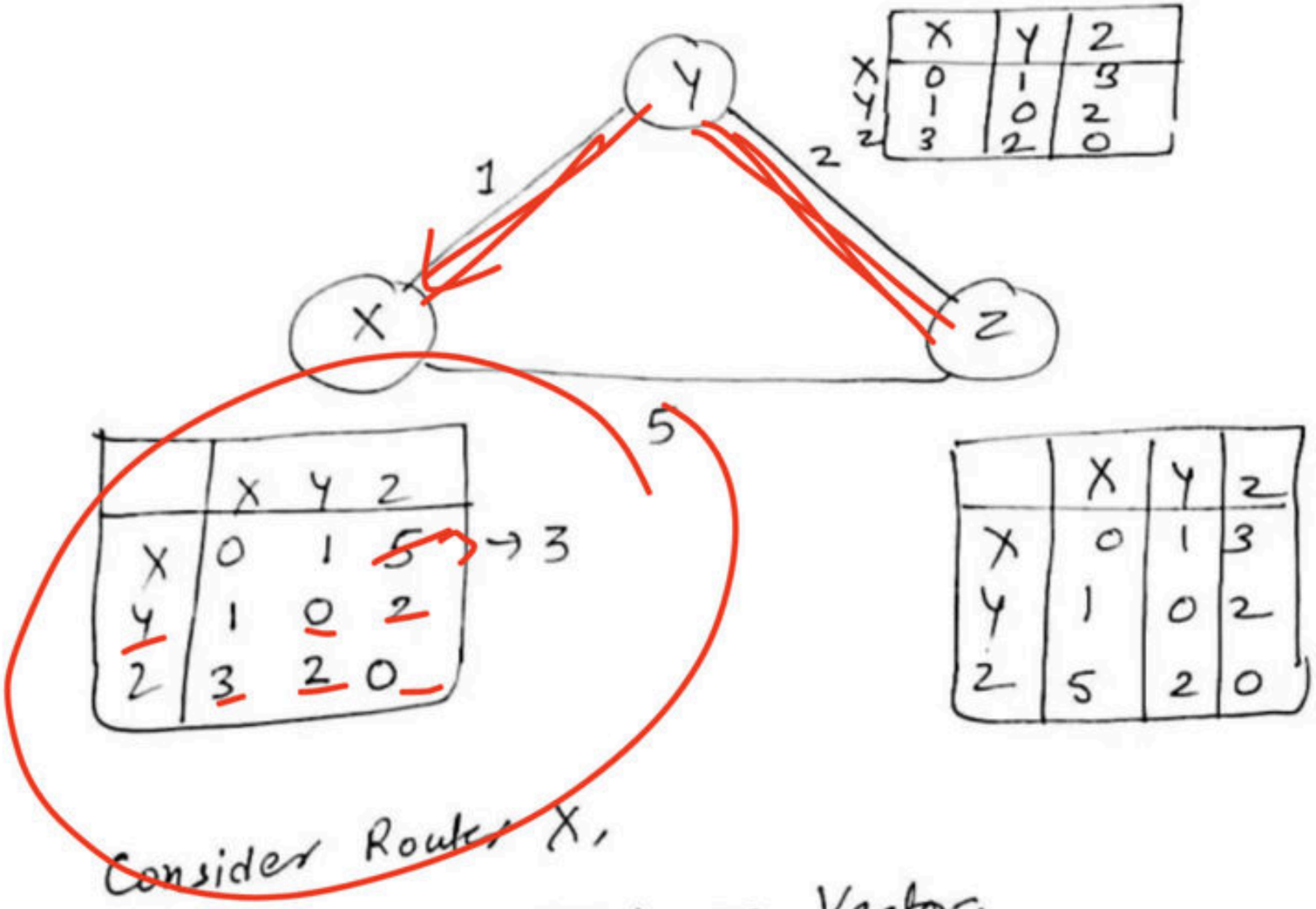
GATE CS 2011





DISTANCE VECTOR ROUTING

- ROUTER Informs ⟶ NEIGHBORS (about topology changes)
- Uses Bellman Ford.
- Information kept by Router:
  1. Router ID
  2. Cost of link associated with Router.
  3. Distance to Itself 0.
  4. Distance to All other Routers = ∞.

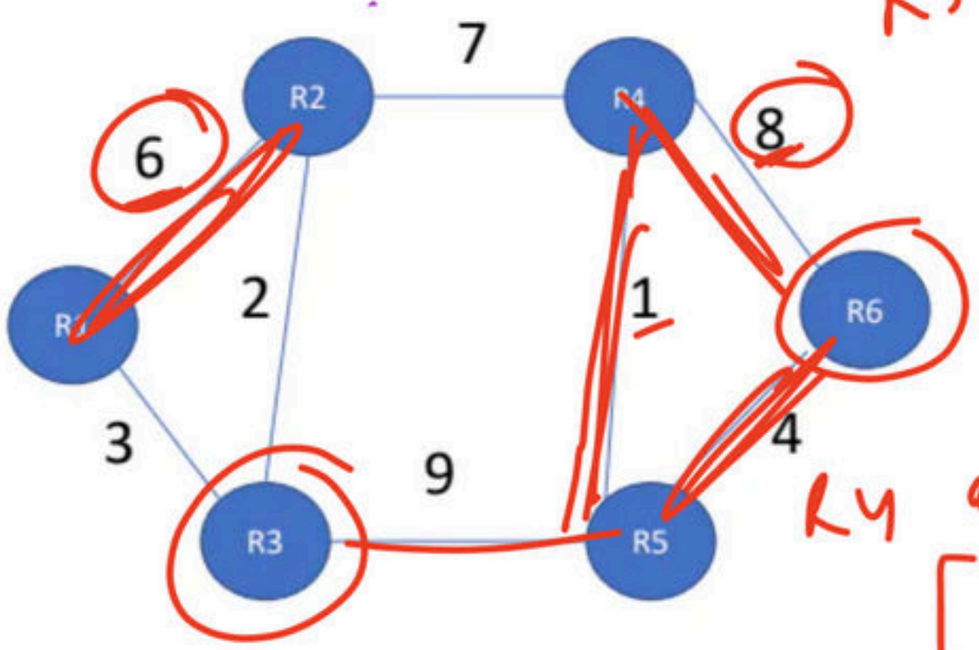


Consider Router X,

Only shares Distance Vector.

GATE 2010

Consider a network with 6 routers R1 to R6 connected with links having weights as shown in the following diagram



All the routers use the distance vector based routing algorithm to update their routing tables. Each router starts with its routing table initialized to contain an entry for each neighbour with the weight of the respective connecting link. After all the routing tables stabilize, how many links in the network will never be used for carrying any data?

R1 R2 R3 R4 R5 R6

R1 [0 5 3 12 9 16]

R2 [2 7 8 12]

R3 R4 R5 R6

R3 [9 9 13]

R5 R1 [4]

R4 R5 R6 [15]

R1-R3

R2-R3

R2-R4

R3-R5

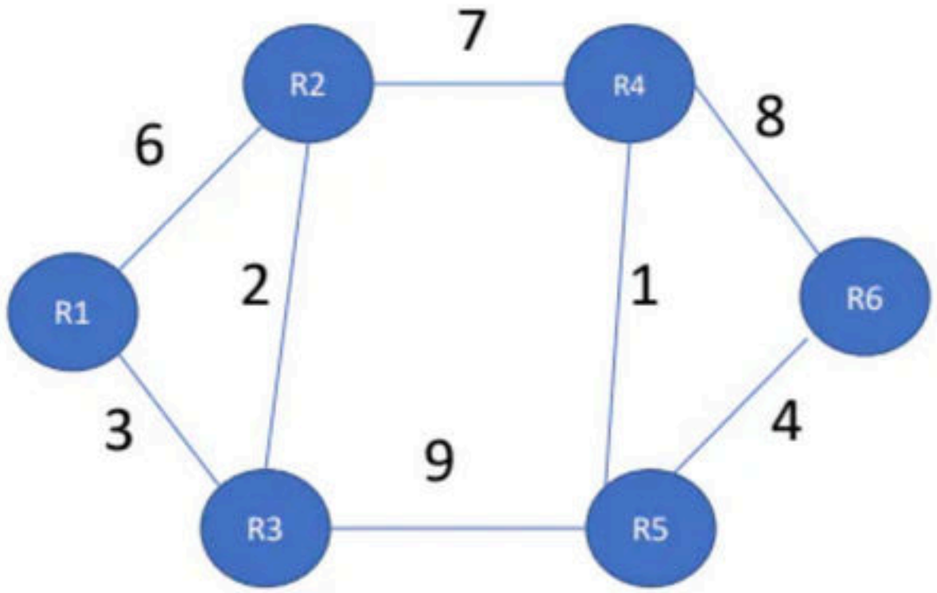
R5-R6

R4-R5

2

GATE 2010

Consider a network with 6 routers R1 to R6 connected with links having weights as shown in the following diagram

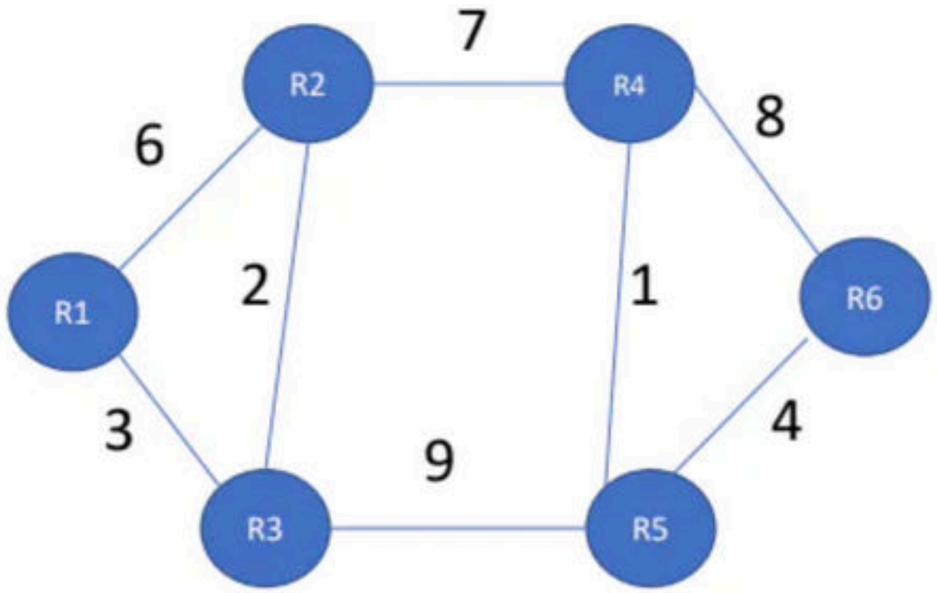


All the routers use the distance vector based routing algorithm to update their routing tables. Each router starts with its routing table initialized to contain an entry for each neighbour with the weight of the respective connecting link. After all the routing tables stabilize, how many links in the network will never be used for carrying any data?

Shortest Distances from R1 to R2, R3, R4, R5 and R6
R1 (5, 3, 12, 12, 16)
Links used: R1-R3, R3-R2, R2-R4, R3-R5, R5-R6

GATE 2010

Consider a network with 6 routers R1 to R6 connected with links having weights as shown in the following diagram

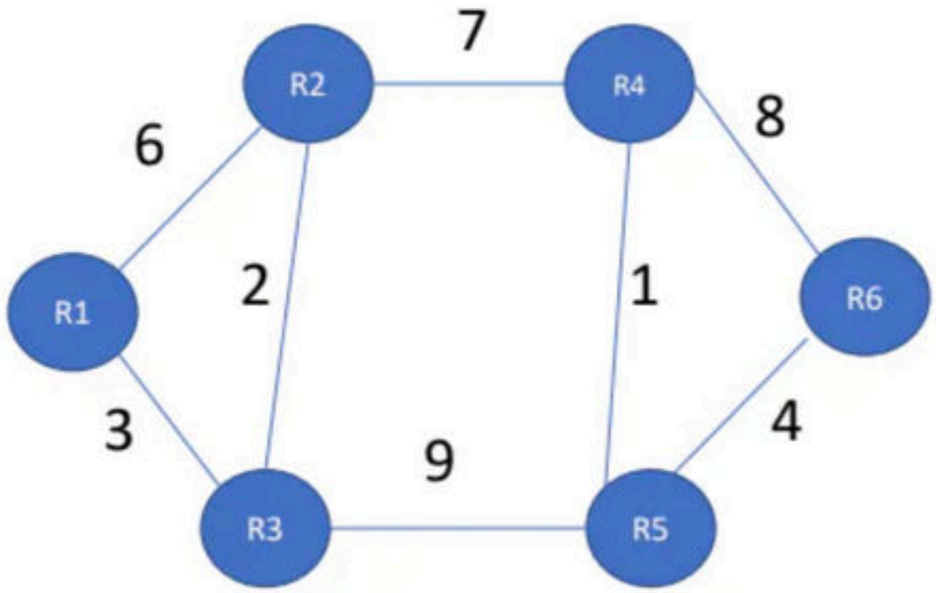


All the routers use the distance vector based routing algorithm to update their routing tables. Each router starts with its routing table initialized to contain an entry for each neighbour with the weight of the respective connecting link. After all the routing tables stabilize, how many links in the network will never be used for carrying any data?

Shortest Distances from R1 to R2, R3, R4, R5 and R6
R1 (5, 3, 12, 12, 16)
Links used: R1-R3, R3-R2, R2-R4, R3-R5, R5-R6
Shortest Distances from R2 to R3, R4, R5 and R6
R2 (2, 7, 8, 12)
Links used: R2-R3, R2-R4, R4-R5, R5-R6

GATE 2010

Consider a network with 6 routers R1 to R6 connected with links having weights as shown in the following diagram



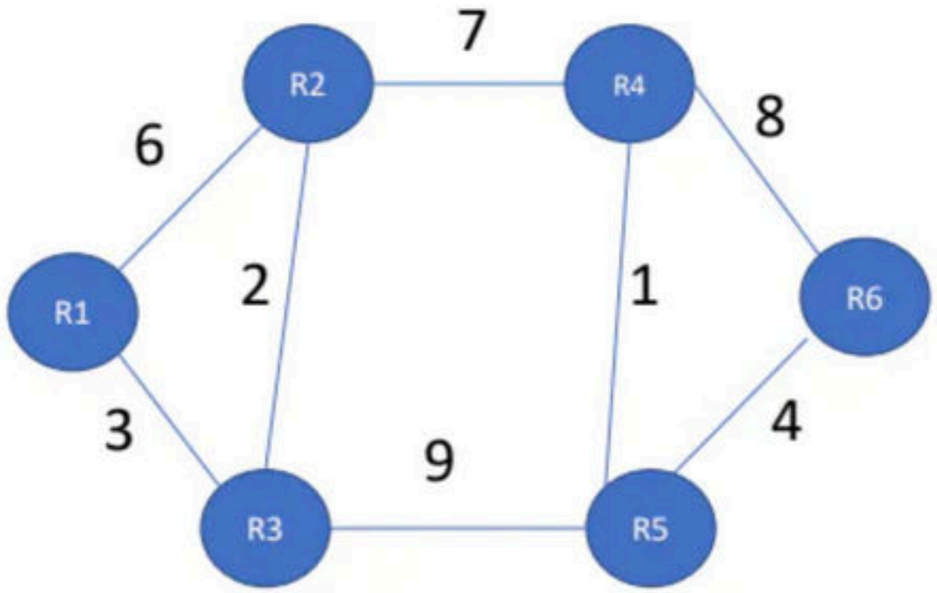
All the routers use the distance vector based routing algorithm to update their routing tables. Each router starts with its routing table initialized to contain an entry for each neighbour with the weight of the respective connecting link. After all the routing tables stabilize, how many links in the network will never be used for carrying any data?

Shortest Distances from R1 to R2, R3, R4, R5 and R6
R1 (5, 3, 12, 12, 16)
Links used: R1-R3, R3-R2, R2-R4, R3-R5, R5-R6
Shortest Distances from R2 to R3, R4, R5 and R6
R2 (2, 7, 8, 12)
Links used: R2-R3, R2-R4, R4-R5, R5-R6
Shortest Distances from R3 to R4, R5 and R6
R3 (9, 9, 13)
Links used: R3-R2, R2-R4, R3-R5, R5-R6
Shortest Distances from R4 to R5 and R6

Compiler
5 pm

GATE 2010

Consider a network with 6 routers R1 to R6 connected with links having weights as shown in the following diagram

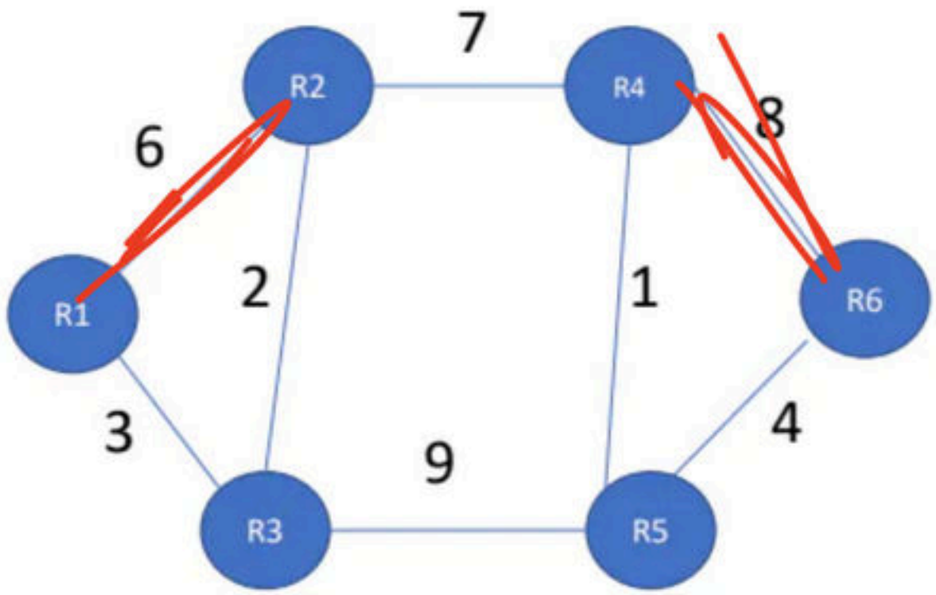


All the routers use the distance vector based routing algorithm to update their routing tables. Each router starts with its routing table initialized to contain an entry for each neighbour with the weight of the respective connecting link. After all the routing tables stabilize, how many links in the network will never be used for carrying any data?

Shortest Distances from R1 to R2, R3, R4, R5 and R6
R1 (5, 3, 12, 12, 16)
Links used: R1-R3, R3-R2, R2-R4, R3-R5, R5-R6
Shortest Distances from R2 to R3, R4, R5 and R6
R2 (2, 7, 8, 12)
Links used: R2-R3, R2-R4, R4-R5, R5-R6
Shortest Distances from R3 to R4, R5 and R6
R3 (9, 9, 13)
Links used: R3-R2, R2-R4, R3-R5, R5-R6
Shortest Distances from R4 to R5 and R6
R4 (1, 5)
Links used: R4-R5, R5-R6
Shortest Distance from R5 to R6

GATE 2010

Consider a network with 6 routers R1 to R6 connected with links having weights as shown in the following diagram



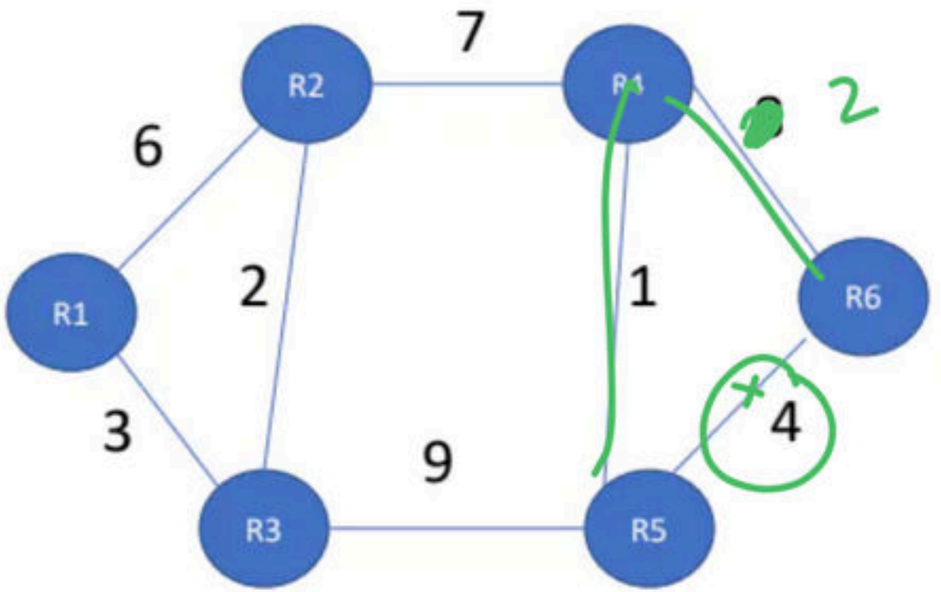
All the routers use the distance vector based routing algorithm to update their routing tables. Each router starts with its routing table initialized to contain an entry for each neighbour with the weight of the respective connecting link. After all the routing tables stabilize, how many links in the network will never be used for carrying any data?

Shortest Distances from R1 to R2, R3, R4, R5 and R6
R1 (5, 3, 12, 12, 16)
Links used: R1-R3, R3-R2, R2-R4, R3-R5, R5-R6
Shortest Distances from R2 to R3, R4, R5 and R6
R2 (2, 7, 8, 12)
Links used: R2-R3, R2-R4, R4-R5, R5-R6
Shortest Distances from R3 to R4, R5 and R6
R3 (9, 9, 13)
Links used: R3-R2, R2-R4, R3-R5, R5-R6
Shortest Distances from R4 to R5 and R6
R4 (1, 5)
Links used: R4-R5, R5-R6
Shortest Distance from R5 to R6
R5 (4)
Links Used: R5-R6
If we mark, all the used links one by one, we can see that following links are never used.
R1-R2
R4-R6

Suppose the weights of all unused links in the previous question are changed to 2 and the distance vector algorithm is used again until all routing tables stabilize. How many links will now remain unused?

(A) 0
(B) 1
(C) 2
(D) 3

R5 - R6



R4

R5 R6

1 2

R5

R6

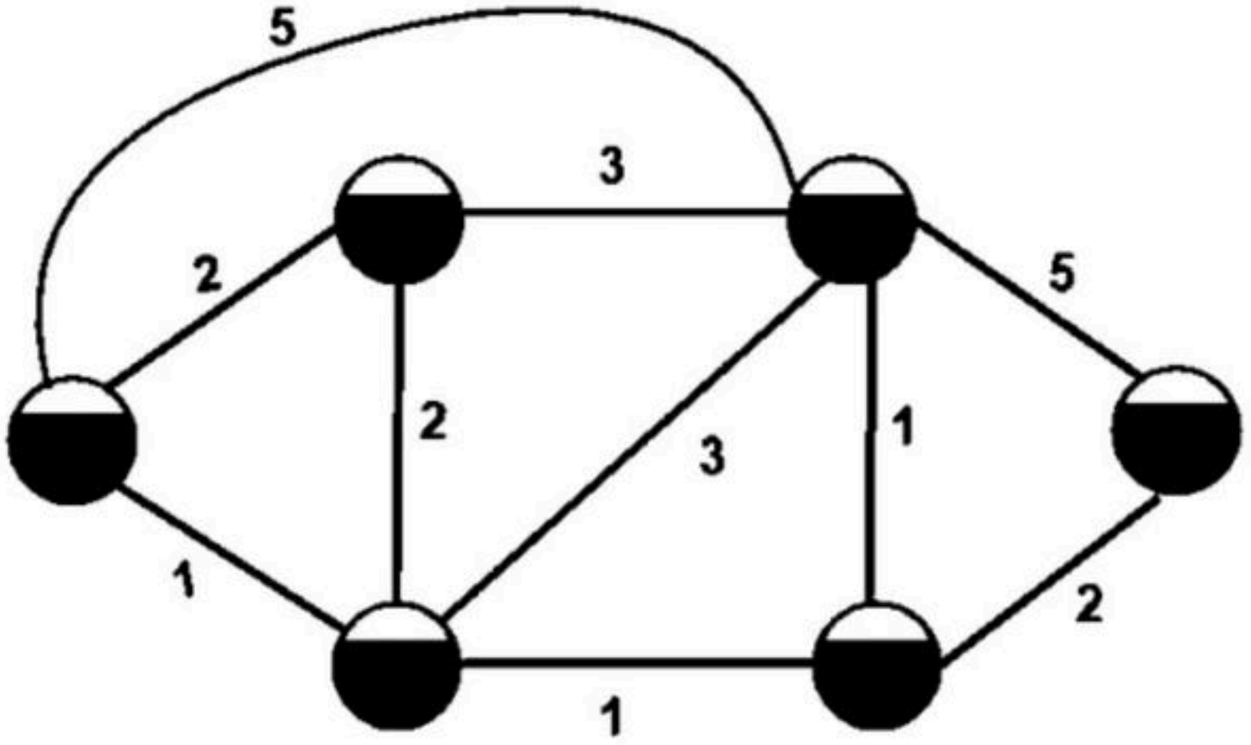
3

Disadv → (DVR) Simpler to Configure

- ✓ Count to ∞ problem
- ✓ More Traffic
- ✓ LARGE N/W → Large Routing Table
  Lead to Congestion.

DVR Uses UDP

Distance Vector Routing	Link State Routing
Bandwidth required is less due to local sharing , small packets and no flooding.	Bandwidth required is more due to flooding and sending of large link state packets.
Based on local knowledge since it updates table based on information from neighbors.	Based on global knowledge i.e. it have knowledge about entire network.
Make use of Bellman ford algo.	Make use of Djikstra algo.
Traffic is less.	Traffic is more.
Converges slowly i.e. good news spread fast and bad news spread slowly.	Converges faster.
Count to infinity problem.	No count to infinity problem.
Persistent Looping problem.	No persistent loops.
Practical implementation is RIP & IGRP.	Practical implementation is OSPF & ISIS



LINK STATE ROUTING

The prior difference between Distance vector and link state routing is that in distance vector routing the router share the knowledge of the entire autonomous system whereas in link state routing the router share the knowledge of only their neighbour routers in the autonomous system

LINK STATE ROUTING

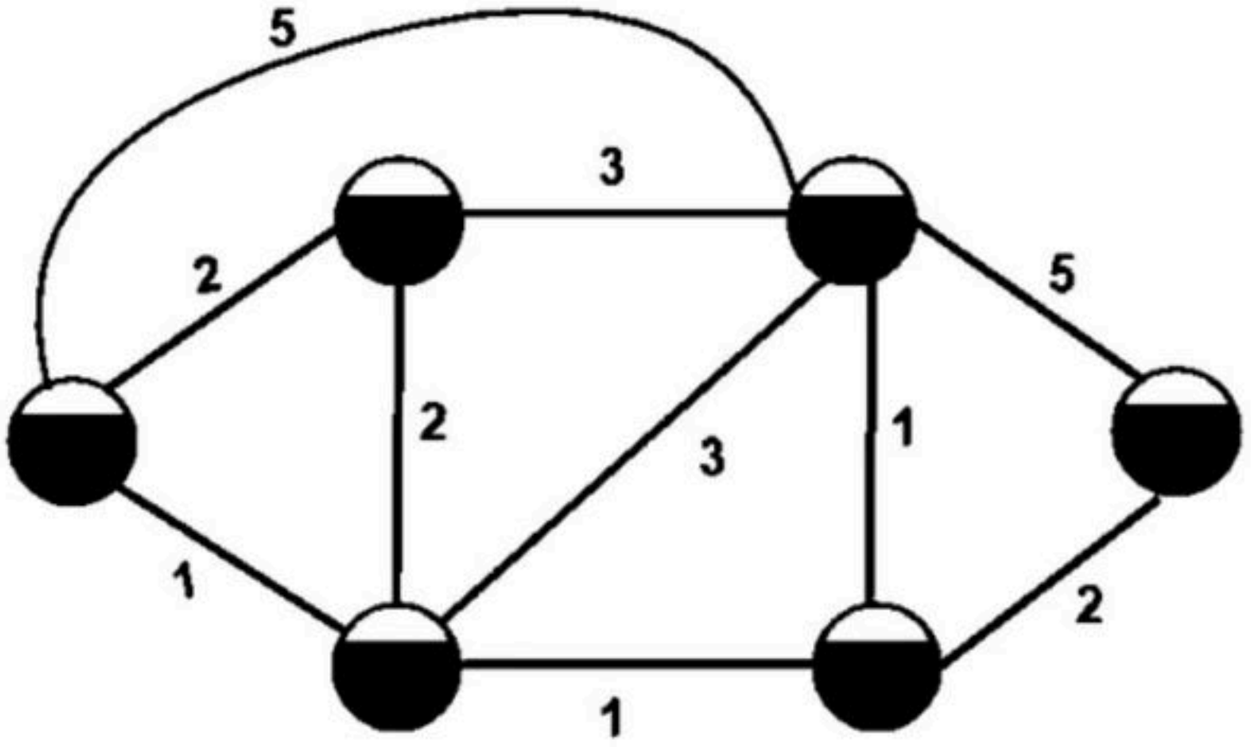
Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router in the internetwork.

The three keys to understand the Link State Routing algorithm:

•**Knowledge about the neighborhood:** Instead of sending its routing table, a router sends the information about its neighborhood only. A router broadcast its identities and cost of the directly attached links to other routers.

•**Flooding:** Each router sends the information to every other router on the internetwork except its neighbors. This process is known as Flooding. Every router that receives the packet sends the copies to all its neighbors. Finally, each and every router receives a copy of the same information.

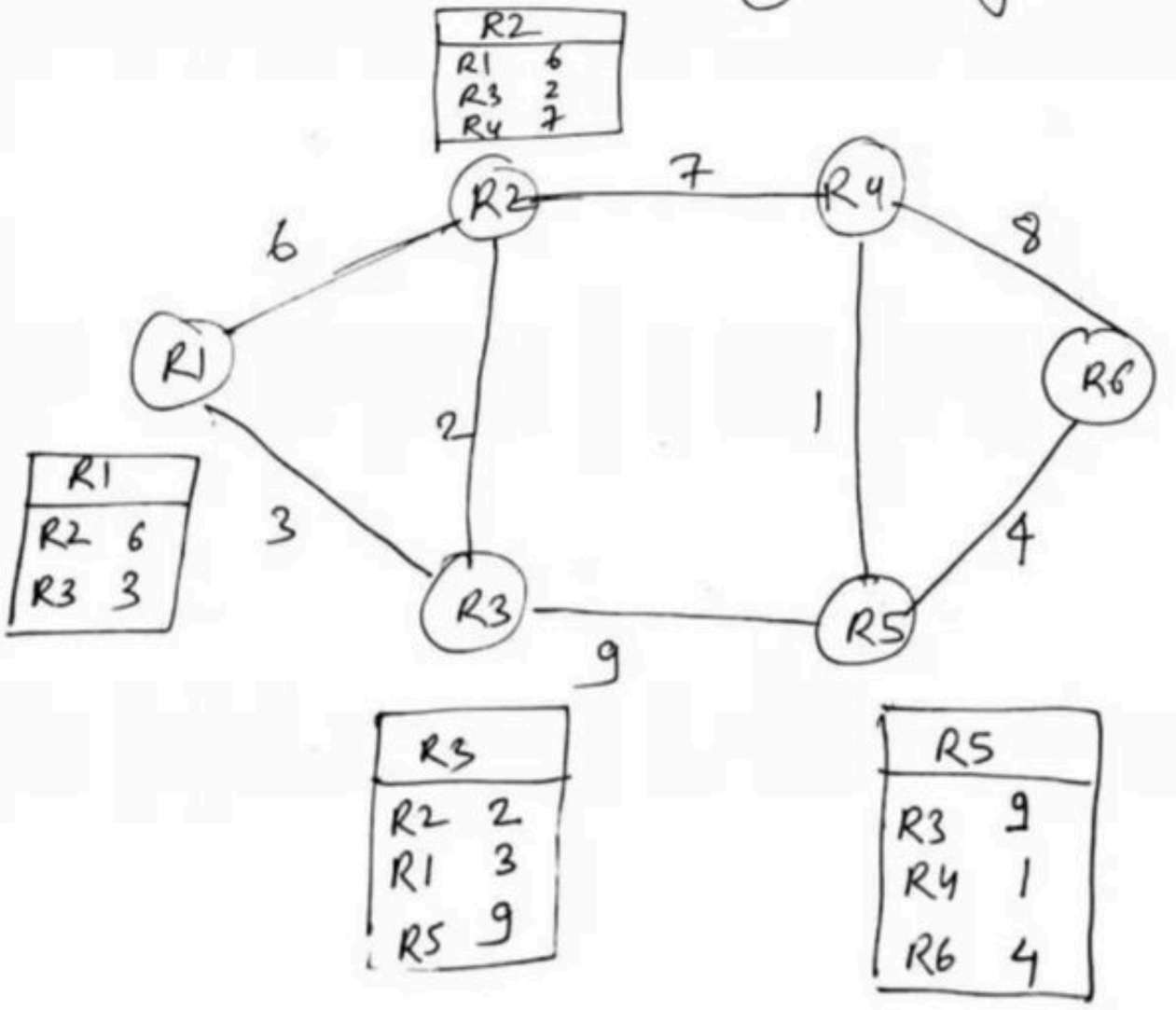
•**Information sharing:** A router sends the information to every other router only when the change occurs in the information.



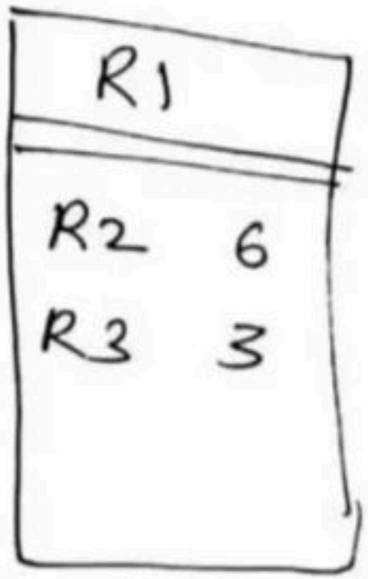
The prior difference between Distance vector and link state routing is that in distance vector routing the router share the knowledge of the entire autonomous system whereas in link state routing the router share the knowledge of only their neighbour routers in the autonomous system

LSR uses flooding

① Link state Table
② Flooding



Link state Table (Uses Flooding)

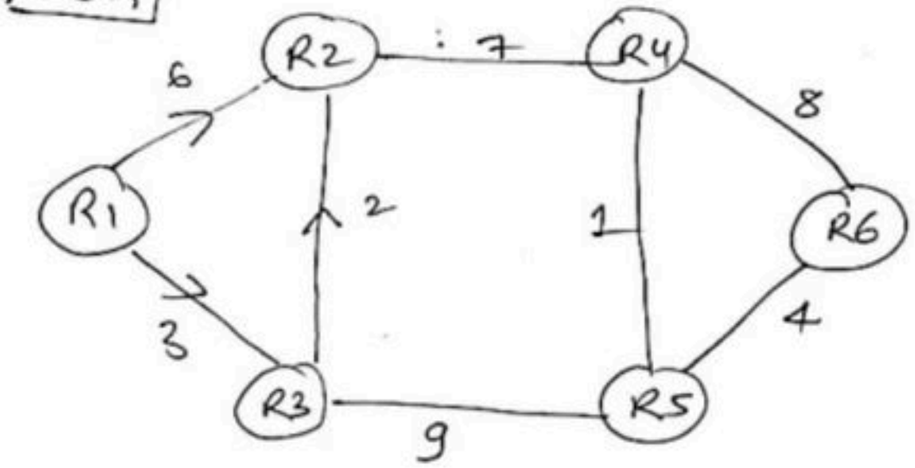


Sequence No. + TTL field.

Shares Distance Vector & whole Database.

Bdw ↑ ∝ Message size.

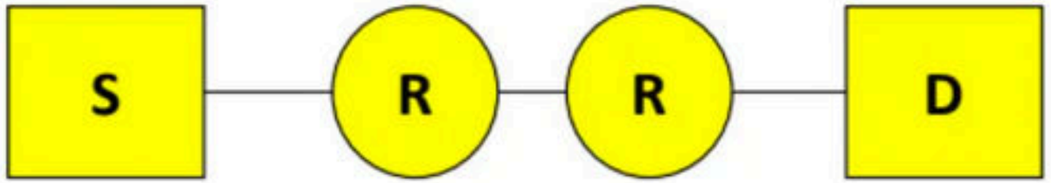
LSR



R1		via
R1	0	R1
R2	~~6~~ 5	R3
R3	3	R1
R4	12	R3 R2
R5	12	R3
R6	16	R3 R5

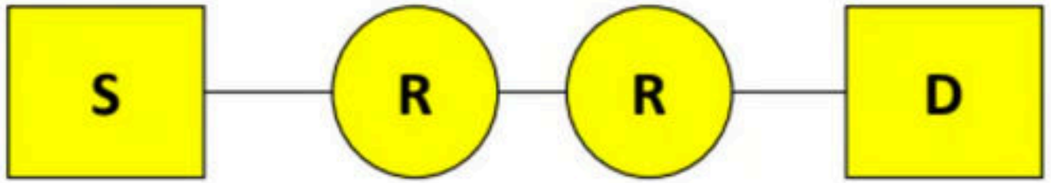
Assume that source S and destination D are connected through two intermediate routers labeled R. Determine how many times each packet has to visit the network layer and the data link layer during a transmission from S to D.

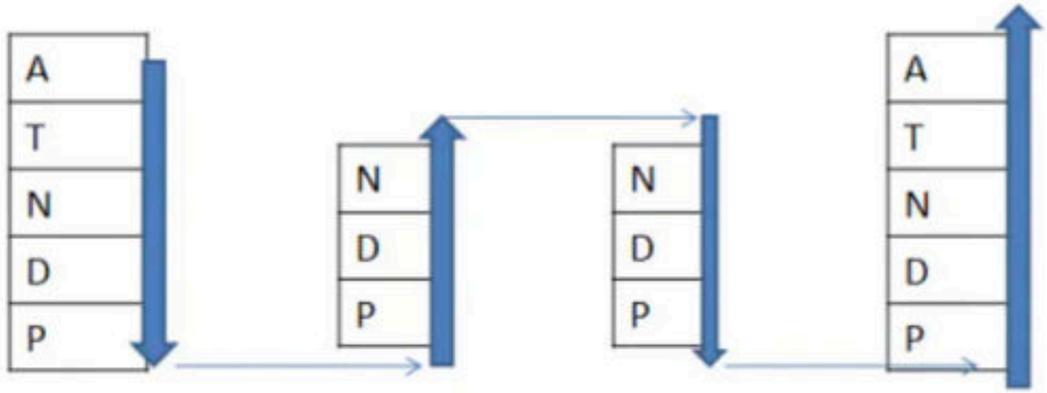
GATE CS 2013



(A) Network layer – 4 times and Data link layer – 4 times
(B) Network layer – 4 times and Data link layer – 3 times
(C) Network layer – 4 times and Data link layer – 6 times
(D) Network layer – 2 times and Data link layer – 6 times

Assume that source S and destination D are connected through two intermediate routers labeled R. Determine how many times each packet has to visit the network layer and the data link layer during a transmission from S to D.



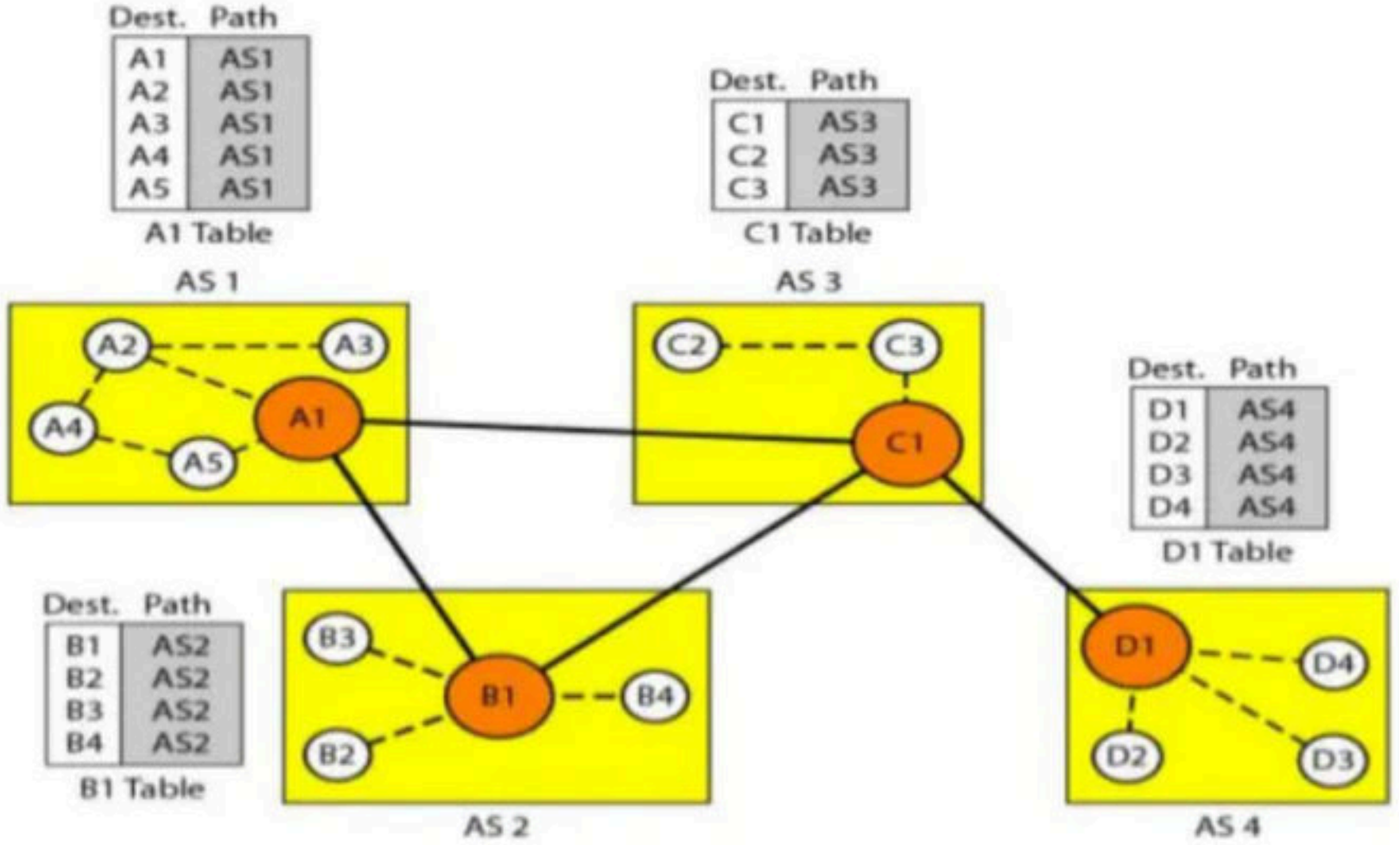


(A) Network layer – 4 times and Data link layer – 4 times
(B) Network layer – 4 times and Data link layer – 3 times
(C) Network layer – 4 times and Data link layer – 6 times
(D) Network layer – 2 times and Data link layer – 6 times

PATH VECTOR ROUTING

Initialization

At the beginning, each speaker node can know only the reachability of nodes inside its autonomous system. Figure 22.30 shows the initial tables for each speaker node in a system made of four ASs.



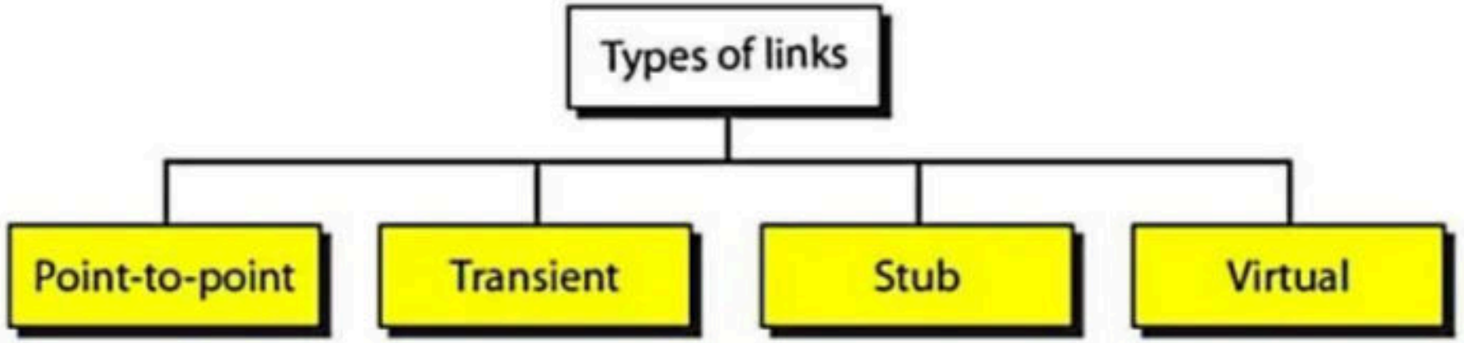
Open shortest path first (OSPF) is a link-state routing protocol which is used to find the best path between the source and the destination.

OSPF Messages :

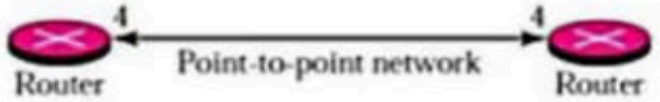
Hello message (Type 1) – It is used by the routers to introduce itself to the other routers.
Database description message (Type 2) – It is normally send in response to the Hello message.
Link-state request message (Type 3) – It is used by the routers that need information about specific Link-State packet.
Link-state update message (Type 4) – It is the main OSPF message for building Link-State Database.
Link-state acknowledgement message (Type 5) – It is used to create reliability in the OSPF protocol.

OSPF allows administrator to assign a cost , called the metric to each rout
The metric can be used on a type of service (minimum delay , maximum throughput and so on…)

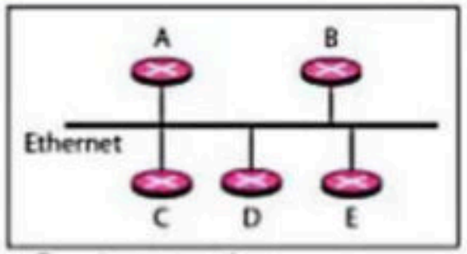
Types of Links



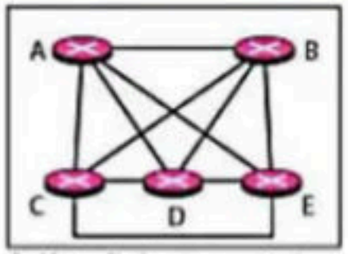
POINT TO PINT LINK : To connect 2 routers without any other host or router in between



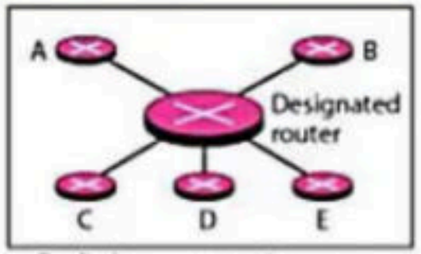
TRANSIENT LINK : a network with several routers attached to it.



a. Transient network



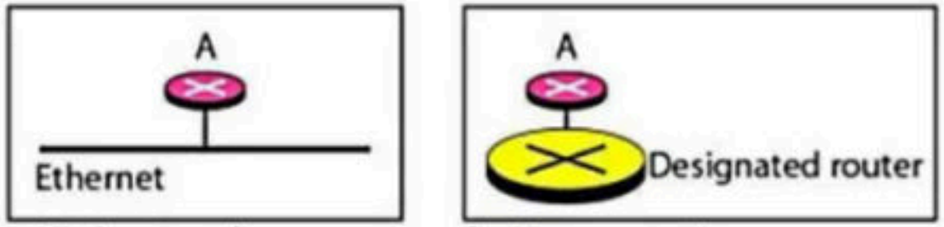
b. Unrealistic representation



c. Realistic representation

Stub Link

A **stub link** is a network that is connected to only one router. The data packets enter the network through this single router and leave the network through this same **router.**



a. Stub network

b. Representation

Virtual Link

When the link between two routers is broken, the administration may create a **virtual link** between them, using a longer path that probably goes through several routers.

Consider the following three statements about link state and distance vector routing protocols, for a large network with 500 network nodes and 4000 links.
[S1] The computational overhead in link state protocols is higher than in distance vector protocols.
[S2] A distance vector protocol (with split horizon) avoids persistent routing loops, but not a link state protocol.
[S3] After a topology change, a link state protocol will converge faster than a distance vector protocol.

Which one of the following is correct about S1, S2, and S3 ?

(A) S1, S2, and S3 are all true.
(B) S1, S2, and S3 are all false.
(C) S1 and S2 are true, but S3 is false
(D) S1 and S3 are true, but S2 is false

GATE CS 2014

Consider the following three statements about link state and distance vector routing protocols, for a large network with 500 network nodes and 4000 links.

[S1] The computational overhead in link state protocols is higher than in distance vector protocols.

[S2] A distance vector protocol (with split horizon) avoids persistent routing loops, but not a link state protocol.

[S3] After a topology change, a link state protocol will converge faster than a distance vector protocol.

Which one of the following is correct about S1, S2, and S3 ?

S1 is clearly true as in Link State all nodes compute shortest path for whole network graph.

S3 is also true as Distance Vector protocol has count to infinity problem and converges slower.

S2 is false. In distance vector protocol, split horizon with poison reverse reduces the chance of forming loops and uses a maximum number of hops to counter the 'count-to-infinity' problem.

Which one of the following is TRUE about interior Gateway routing protocols – Routing Information Protocol (RIP) and Open Shortest Path First (OSPF)

(A) RIP uses distance vector routing and OSPF uses link state routing

(B) OSPF uses distance vector routing and RIP uses link state routing

(C) Both RIP and OSPF use link state routing

(D) Both RIP and OSPF use distance vector routing

GATE CS 2014

HW

Which one of the following is TRUE about interior Gateway routing protocols – Routing Information Protocol (RIP) and Open Shortest Path First (OSPF)

(A) RIP uses distance vector routing and OSPF uses link state routing

(B) OSPF uses distance vector routing and RIP uses link state routing

(C) Both RIP and OSPF use link state routing

(D) Both RIP and OSPF use distance vector routing

GATE CS 2014

Both Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) are Interior Gateway Protocol, i.e., they both are used within an autonomous system.

RIP is an old protocol (not used anymore) based on distance vector routing.

OSPF is based on Link State Routing.

Two popular routing algorithms are Distance Vector(DV) and Link State (LS) routing. Which of the following are true?

(S1) Count to infinity is a problem only with DV and not LS routing
(S2) In LS, the shortest path algorithm is run only at one node
(S3) In DV, the shortest path algorithm is run only at one node
(S4) DV requires lesser number of network messages than LS

GATE CS 2008

(A) S1, S2 and S4 only
(B) S1, S3 and S4 only
(C) S2 and S3 only
(D) S1 and S4 only

H.W

Two popular routing algorithms are Distance Vector(DV) and Link State (LS) routing. Which of the following are true?

(S1) Count to infinity is a problem only with DV and not LS routing

(S2) In LS, the shortest path algorithm is run only at one node

(S3) In DV, the shortest path algorithm is run only at one node

(S4) DV requires lesser number of network messages than LS

(A) S1, S2 and S4 only

(B) S1, S3 and S4 only

(C) S2 and S3 only

(D) S1 and S4 only

An IP machine Q has a path to another IP machine H via three IP routers R1, R2, and R3.
Q—R1—R2—R3—H
H acts as an HTTP server, and Q connects to H via HTTP and downloads a file. Session layer encryption is used, with DES as the shared key encryption protocol. Consider the following four pieces of information:
[I1] The URL of the file downloaded by Q
[I2] The TCP port numbers at Q and H
[I3] The IP addresses of Q and H
[I4] The link layer addresses of Q and H
Which of I1, I2, I3, and I4 can an intruder learn through sniffing at R2 alone?
(A) Only I1 and I2
(B) Only I1
(C) Only I2 and I3
(D) Only I3 and I4

Sniffing is the process of monitoring and capturing all the packets passing through a given network using **sniffing** tools. It is a form of "tapping phone wires" and get to know about the conversation. It is also called wiretapping applied to the computer networks.

h w

An IP machine Q has a path to another IP machine H via three IP routers R1, R2, and R3.
Q—R1—R2—R3—H
H acts as an HTTP server, and Q connects to H via HTTP and downloads a file. Session layer encryption is used, with DES as the shared key encryption protocol. Consider the following four pieces of information:
[I1] The URL of the file downloaded by Q
[I2] The TCP port numbers at Q and H
[I3] The IP addresses of Q and H
[I4] The link layer addresses of Q and H
Which of I1, I2, I3, and I4 can an intruder learn through sniffing at R2 alone?
(A) Only I1 and I2
(B) Only I1
(C) Only I2 and I3
(D) Only I3 and I4

An Intruder can't learn [I1] through sniffing at R2 because URLs and Download are functioned at Application layer of OSI Model.
An Intruder can learn [I2] through sniffing at R2 because Port Numbers are encapsulated in the payload field of IP Datagram.
An Intruder can learn [I3] through sniffing at R2 because IP Addresses and Routers are functioned at network layer of OSI Model.
An Intruder can't learn [I4] through sniffing at R2 because it is related to Data Link Layer of OSI Model.

The address of a class B host is to be split into subnets with a 6-bit subnet number. What is the maximum number of subnets and the maximum number of hosts in each subnet?

(A) 62 subnets and 262142 hosts.
(B) 64 subnets and 262142 hosts.
(C) 62 subnets and 1022 hosts.
(D) 64 subnets and 1024 hosts.

The address of a class B host is to be split into subnets with a 6-bit subnet number. What is the maximum number of subnets and the maximum number of hosts in each subnet?

(A) 62 subnets and 262142 hosts.
(B) 64 subnets and 262142 hosts.
(C) 62 subnets and 1022 hosts.
(D) 64 subnets and 1024 hosts.

Maximum number of subnets = 2^6-2 =62.
Note that 2 is subtracted from 2^6. The RFC 950 specification reserves the subnet values consisting of all zeros and all ones (broadcast), reducing the number of available subnets by two.

Maximum number of hosts is 2^10-2 = 1022.
2 is subtracted for Number of hosts is also. The address with all bits as 1 is reserved as broadcast address and address with all host id bits as 0 is used as network address of subnet.
In general, the number of addresses usable for addressing specific hosts in each network is always 2^N – 2 where N is the number of bits for host id.

RFC 950 vs RFC 1878

In GATE if this concept comes again in next year, we should follow New convention , as new convention is based on RFC 1878 while old convention is based on RFC 950 , so new one is more acceptable .

Wikipedia says
The RFC 950 specification recommended reserving the subnet values consisting of all zeros and all ones (broadcast), reducing the number of available subnets by two.

However, **due to the inefficiencies introduced by this convention it was abandoned for use on the public Internet, and is only relevant when dealing with legacy equipment that does not implement CIDR.**

The only reason not to use the all-zeroes subnet is that it is ambiguous when the prefix length is not available.

RFC 950 itself did not make the use of the zero subnet illegal; **it was however considered best practice by engineers**."

A class C network is assigned with a subnet mask of 255.255.255.248 . The total number of hosts possible in all the sub networks together in the above network is .....

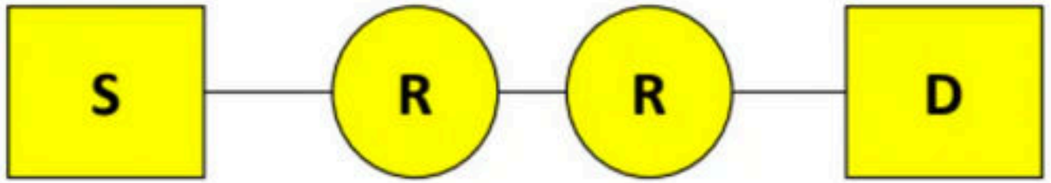
A class C network is assigned with a subnet mask of 255.255.255.248 . The total number of hosts possible in all the sub networks together in the above network is .....

Given ,
Subnet mask = 255.255.255.248 and the network is given to be of class C..
So number of subnet bits = 5
Hence number of subnets = 2^5 = 32
Number of host bits for each subnet = 3
Hence number of hosts in each subnet = 2^3 - 2 = 6
Hence total number of hosts = Number of subnets * number of hosts in each subnet
= 32 * 6
= 192

In general the number of available hosts on a subnet is 2^h-2, where *h* is the number of bits used for the host portion of the address. The number of available subnets is 2^n, where *n* is the number of bits used for the network portion of the address. This is the RFC 1878 standard used by the IETF, the IEEE and COMPTIA

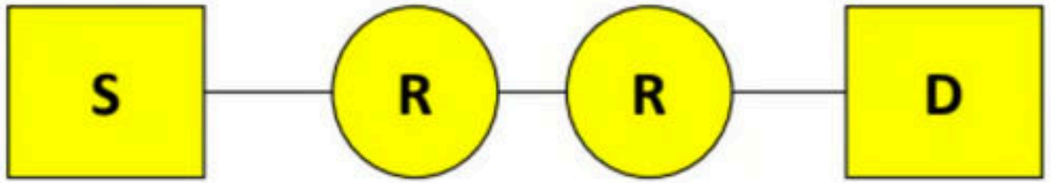
Assume that source S and destination D are connected through two intermediate routers labeled R. Determine how many times each packet has to visit the network layer and the data link layer during a transmission from S to D.

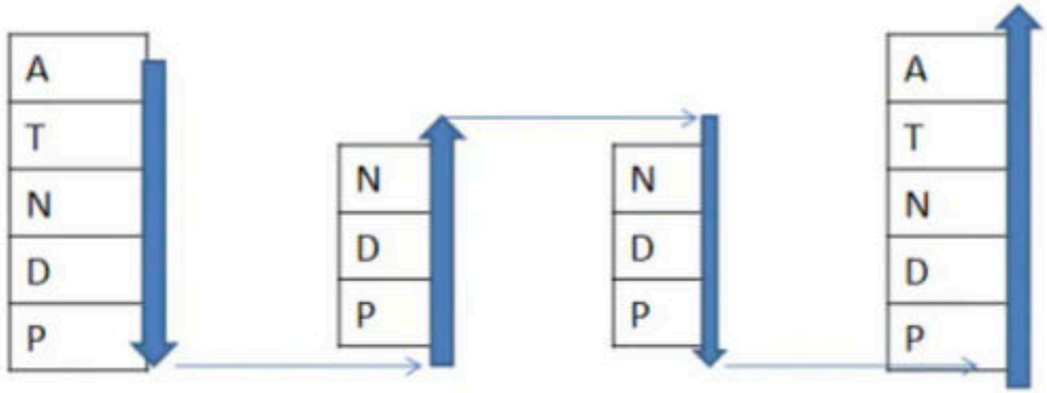
GATE CS 2013



(A) Network layer – 4 times and Data link layer – 4 times
(B) Network layer – 4 times and Data link layer – 3 times
(C) Network layer – 4 times and Data link layer – 6 times
(D) Network layer – 2 times and Data link layer – 6 times

Assume that source S and destination D are connected through two intermediate routers labeled R. Determine how many times each packet has to visit the network layer and the data link layer during a transmission from S to D.





(A) Network layer – 4 times and Data link layer – 4 times
(B) Network layer – 4 times and Data link layer – 3 times
(C) Network layer – 4 times and Data link layer – 6 times
(D) Network layer – 2 times and Data link layer – 6 times

GATE 2020 QUESTION ON IP ADDRESS

An organization requires a range of IP address to assign one to each of its 1500 computers. The organization has approached an Internet Service Provider (ISP) for this task. The ISP uses CIDR and serves the requests from the available IP address space 202.61.0.0/17. The ISP wants to assign an address space to the organization which will minimize the number of routing entries in the ISP's router using route aggregation. Which of the following address spaces are potential candidates from which the ISP can allot any one of the organization ?

I. 202.61.84.0 / 21
II. 202.61.104.0 / 21
III. 202.61.64.0 / 21
IV. 202.61.144.0 / 21

(A) I and II only
(B) II and III only
(C) III and IV only
(D) I and IV only

Given IP address , 17 bits are in NID and rest HID

1500 hosts we need minimum 11 bits HID

SID bits available 4 bits

202.61.0.0/17

If we expand the given Network bits we can see:

202.61.84.0/21=202.61.01010100.0 Host Bits should be zero
202.61.104.0/21=202.61.01101000.0 Possible
202.61.64.0/21=202.61.01000000.0 Possible
202.61.144.0/21=202.61.10010000.0 16th bit cannot be 1

How do I reduce the size of my routing table?

To conserve the space occupied by the routing table, aggregation can be used to reduce the size of the routing table.
IP supernetting is an aggregation technique. Classless interdomain routing (CIDR) addressing uses aggregation to reduce routing table sizes.

GATE CS 2020

Consider the following statements about the functionality of an IP based r

- I. A router does not modify the IP packets during forwarding.
- II. It is not necessary for a router to implement any routing protocol.
- III. A router should reassemble IP fragments if the MTU of the outgoing link is larger than the size of the incoming IP packet.

Which of the above statements is/are TRUE ?

(A) I and II only
(B) I only
(C) II and III only
(D) II only

GATE CS 2020

Consider the following statements about the functionality of an IP based r
•I. A router does not modify the IP packets during forwarding.
•II. It is not necessary for a router to implement any routing protocol.
•III. A router should reassemble IP fragments if the MTU of the outgoing link is larger than the size of the incoming IP packet.
Which of the above statements is/are TRUE ?
(A) I and II only
(B) I only
(C) II and III only
(D) II only

•**I.** False. A router modifies the IP packets during forwarding because TTL (Time to Live) is changing.
•**II.** True. A router need not implement any routing protocol. It can just forward packets in all the directions without doing any routing.
•**III.** False. Router does not assemble the packets. Assembling is done at destination system.

Which one of the following fields of an IP header is NOT modified by a typical IP router?

(A) Checksum
(B) Source address
(C) Time to Live (TTL)
(D) Length

GATE CS 2014

Which one of the following fields of an IP header is NOT modified by a typical IP router?

(A) Checksum
(B) Source address
(C) Time to Live (TTL)
(D) Length

GATE CS 2014

Answer: (B)

Explanation: Length and checksum can be modified when IP fragmentation happens. Time To Live is reduced by every router on the route to destination.
Only Source Address is what IP address can not change SO B is the answer.

Host A (on TCP/IP v4 network A) sends an IP datagram D to host B (also on TCP/IP v4 network B). Assume that no error occurred during the transmission of D. When D reaches B, which of the following IP header field(s) may be different from that of the original datagram D?

GATE CS 2014

(i) TTL
(ii) Checksum
(iii) Fragment Offset

(A) (i) only
(B) (i) and (ii) only
(C) (ii) and (iii) only
(D) (i), (ii) and (iii)

Host A (on TCP/IP v4 network A) sends an IP datagram D to host B (also on TCP/IP v4 network B). Assume that no error occurred during the transmission of D. When D reaches B, which of the following IP header field(s) may be different from that of the original datagram D?

GATE CS 2014

(i) TTL
(ii) Checksum
(iii) Fragment Offset

(A) (i) only
(B) (i) and (ii) only
(C) (ii) and (iii) only
(D) (i), (ii) and (iii)

All (i), (ii) and (iii) are changed:

(i) TTL is decremented at every hop. So TTL is different from original value
(ii) Since TTL changes, the Checksum of the packet also changes.
(iii) A packet is fragmented if it has a size greater than the Maximum Transmission Unit (MTU) of the network. There may be intermediate networks that may change fragment offset by fragmenting the packet.

An organization has a class B network and wishes to form subnets for 64 departments. The subnet mask would be:

(a) 255.255.0.0

(b) 255.255.64.0

(c) 255.255.128.0

(d) 255.255.252.0

GATE CS 2006

An organization has a class B network and wishes to form subnets for 64 departments. The subnet mask would be:

(a) 255.255.0.0

(b) 255.255.64.0

(c) 255.255.128.0

(d) 255.255.252.0

GATE CS 2006

Answer (d)

The size of network ID is 16 bit in class B networks. So bits after 16th bit must be used to create 64 departments.

Total 6 bits are needed to identify 64 different departments. Therefore, subnet mask will be 255.255.252.0.

Which of the following is NOT true with respect to a transparent bridge and a router?

(A) Both bridge and router selectively forward data packets

(B) A bridge uses IP addresses while a router uses MAC addresses

(C) A bridge builds up its routing table by inspecting incoming packets

(D) A router can connect between a LAN and a WAN

GATE CS 2004

Which of the following is NOT true with respect to a transparent bridge and a router?

(A) Both bridge and router selectively forward data packets

(B) A bridge uses IP addresses while a router uses MAC addresses

(C) A bridge builds up its routing table by inspecting incoming packets

(D) A router can connect between a LAN and a WAN

GATE CS 2004

Answer: (B)

The address resolution protocol (ARP) is used for

(A) Finding the IP address from the DNS

(B) Finding the IP address of the default gateway

(C) Finding the IP address that corresponds to a MAC address

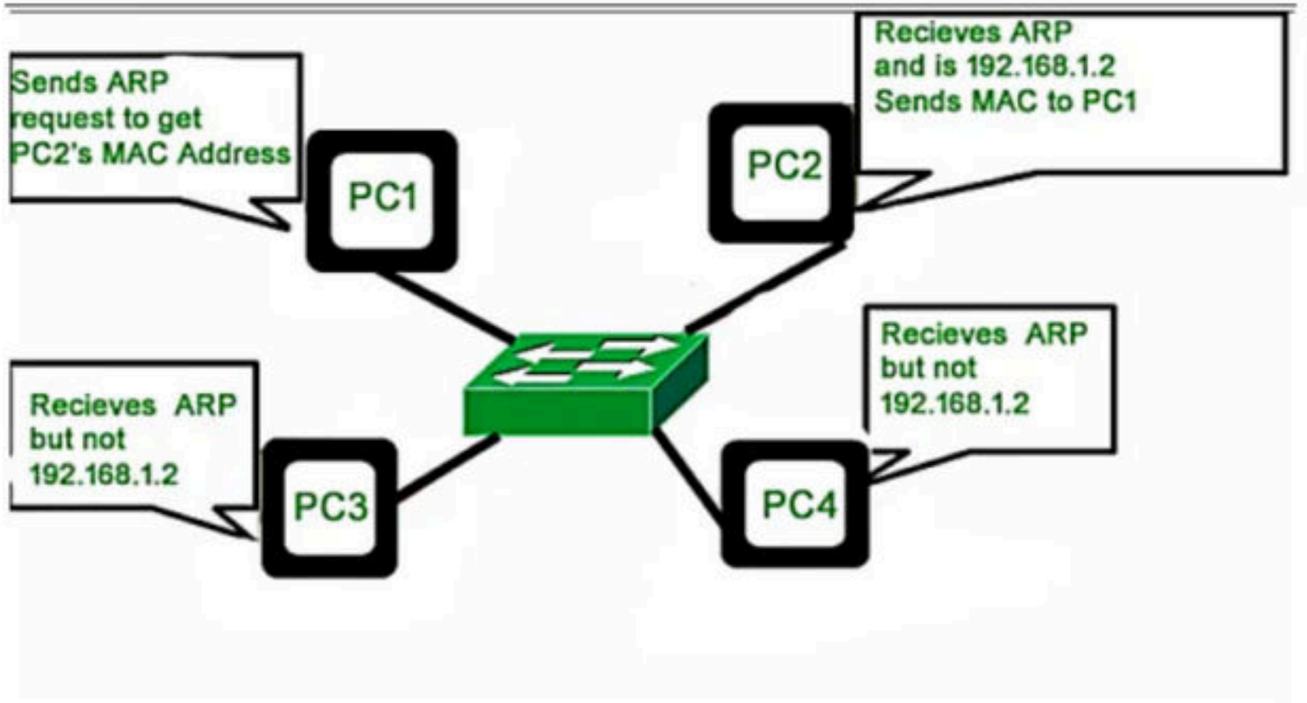
(D) Finding the MAC address that corresponds to an IP address

GATE CS 2005

The address resolution protocol (ARP) is used for
(A) Finding the IP address from the DNS
(B) Finding the IP address of the default gateway
(C) Finding the IP address that corresponds to a MAC address
(D) Finding the MAC address that corresponds to an IP address

GATE CS 2005

When a packet is passed to the data link layer from network layer IP address of the sender , MAC address of the sender and the gateway of the network is attached. The MAC address of the sender is known to the sender but not the MAC address of the gateway .So ARP (Address Resolution Protocol) request is generated with the IP address of the gateway and is broadcasted ,everyone except the gateway discards it and gateway sends it's MAC address.



An IP datagram of size 1000 bytes arrives at a router. The router has to forward this packet on a link whose MTU (maximum transmission unit) is 100 bytes. Assume that the size of the IP header is 20 bytes. The number of fragments that the IP datagram will be divided into for transmission is :

Note : This question was asked as Numerical Answer Type.

(A) 10
(B) 50
(C) 12
(D) 13

GATE CS 2016

An IP datagram of size 1000 bytes arrives at a router. The router has to forward this packet on a link whose MTU (maximum transmission unit) is 100 bytes. Assume that the size of the IP header is 20 bytes. The number of fragments that the IP datagram will be divided into for transmission is :

Note : This question was asked as Numerical Answer Type.

GATE CS 2016

(A) 10
(B) 50
(C) 12
(D) 13

Answer: (D)

Explanation: MTU = 100 bytes
Size of IP header = 20 bytes
So, size of data that can be transmitted in one fragment = 100 – 20 = 80 bytes
Size of data to be transmitted = Size of datagram – size of header = 1000 – 20 = 980 bytes

Now, we have a datagram of size 1000 bytes.
So, we need ceil(980/80) = 13 fragments.

Thus, there will be 13 fragments of the datagram.
So, D is the correct choice.

In the network 200.10.11.144/27, the fourth octet (in decimal) of the last IP address of the network which can be assigned to a host is _____

(A) 158
(B) 255
(C) 222
(D) 223

GATE CS 2015

In the network 200.10.11.144/27, the fourth octet (in decimal) of the last IP address of the network which can be assigned to a host is _____

(A) 158
(B) 255
(C) 222
(D) 223

GATE CS 2015

The last or fourth octet of network address is 144
144 in binary is 10010000.

The first three bits of this octal are fixed as 100,
the remaining bits can get maximum value as 11111.
So the maximum possible last octal IP address is
10011111 which is 159.

The question seems to by asking about host address.
The address with all 1s in host part is broadcast address
and can't be assigned to a host. So the maximum possible
last octal in a host IP is 10011110 which is 158.

The maximum possible network address that can be assigned
is 200.10.11.158/31 which has last octet as 158.

Host A sends a UDP datagram containing 8880 bytes of user data to host B over an Ethernet LAN. Ethernet frames may carry data up to 1500 bytes (i.e. MTU = 1500 bytes). Size of UDP header is 8 bytes and size of IP header is 20 bytes. There is no option field in IP header. How may total number of IP fragments will be transmitted and what will be the contents of offset field in the last fragment?

(A) 6 and 925
(B) 6 and 7400
(C) 7 and 1110
(D) 7 and 8880

GATE CS 2015

Host A sends a UDP datagram containing 8880 bytes of user data to host B over an Ethernet LAN. Ethernet frames may carry data up to 1500 bytes (i.e. MTU = 1500 bytes). Size of UDP header is 8 bytes and size of IP header is 20 bytes. There is no option field in IP header. How may total number of IP fragments will be transmitted and what will be the contents of offset field in the last fragment?

(A) 6 and 925
(B) 6 and 7400
(C) 7 and 1110
(D) 7 and 8880

GATE CS 2015

UDP data = 8880 bytes
UDP header = 8 bytes
IP Header = 20 bytes

Total Size excluding IP Header = 8888 bytes.

Number of fragments = $\lceil 8888 / 1480 \rceil$
= 7

Refer the Kurose book slides on IP (Offset is always scaled by 8)

Offset of last segment = (1480 * 6) / 8 = 1110

Every host in an IPv4 network has a 1-second resolution real-time clock with battery backup. Each host needs to generate up to 1000 unique identifiers per second. Assume that each host has a globally unique IPv4 address. Design a 50-bit globally unique ID for this purpose. After what period (in seconds) will the identifiers generated by a host wrap around?

(A) 128
(B) 64
(C) 256
(D) 512

GATE CS 2014

Every host in an IPv4 network has a 1-second resolution real-time clock with battery backup. Each host needs to generate up to 1000 unique identifiers per second. Assume that each host has a globally unique IPv4 address. Design a 50-bit globally unique ID for this purpose. After what period (in seconds) will the identifiers generated by a host wrap around?

(A) 128
(B) 64
(C) 256
(D) 512

GATE CS 2014

Answer: (C)

Explanation: Wrap-around time is nothing but in how many seconds will all the hosts generate all IDs possible. (i.e. TOTAL_IDS / NO. OF IDS PER SEC).
Total IDs possible with 50-bit is 2^50.
One host generating 1000 identifiers per sec. So all hosts will generate 2^32 * 1000 —-> 2^32 * 2^10——> 2^42 unique IDs.
If we Divide them, we get answer (i.e. 2^50/2^42=2^8)

An IP router with a Maximum Transmission Unit (MTU) of 1500 bytes has received an IP packet of size 4404 bytes with an IP header of length 20 bytes. The values of the relevant fields in the header of the third IP fragment generated by the router for this packet are

(A) MF bit: 0, Datagram Length: 1444; Offset: 370
(B) MF bit: 1, Datagram Length: 1424; Offset: 185
(C) MF bit: 1, Datagram Length: 1500; Offset: 37
(D) MF bit: 0, Datagram Length: 1424; Offset: 2960

GATE CS 2014

An IP router with a Maximum Transmission Unit (MTU) of 1500 bytes has received an IP packet of size 4404 bytes with an IP header of length 20 bytes. The values of the relevant fields in the header of the third IP fragment generated by the router for this packet are

(A) MF bit: 0, Datagram Length: 1444; Offset: 370
(B) MF bit: 1, Datagram Length: 1424; Offset: 185
(C) MF bit: 1, Datagram Length: 1500; Offset: 37
(D) MF bit: 0, Datagram Length: 1424; Offset: 2960

GATE CS 2014

```
Number of packet fragments = ⌈ (total size of packet)/(MTU) ⌉ = ⌈ 4404/1500 ⌉ = ⌈ 2.936 ⌉ = 3

So Datagram with data 4404 byte fragmented into 3 fragments.
```

The first frame carries bytes 0 to 1479 (because MTU is 1500 bytes and HLEN is 20 byte so the total bytes in fragments is maximum 1500-20=1480). the offset for this datagram is 0/8 = 0.
The second fragment carries byte 1480 to 2959. The offset for this datagram is 1480/8 = 185.finally the third fragment carries byte 2960 to 4404.the offset is 370.and for all fragments except last one the M bit is 1.so in the third bit M is 0..

Classless Inter-domain Routing (CIDR) receives a packet with address 131.23.151.76. The router's routing table has the following entries:

Prefix	Output Interface Identifier
131.16.0.0/12	3
131.28.0.0/14	5
131.19.0.0/16	2
131.22.0.0/15	1

The identifier of the output interface on which this packet will be forwarded is _____.

(A) 1
(B) 2
(C) 3
(D) 5

GATE CS 2014

Classless Inter-domain Routing (CIDR) receives a packet with address 131.23.151.76. The router's routing table has the following entries:

Prefix	Output Interface Identifier
131.16.0.0/12	3
131.28.0.0/14	5
131.19.0.0/16	2
131.22.0.0/15	1

The identifier of the output interface on which this packet will be forwarded is _____.

(A) 1
(B) 2
(C) 3
(D) 5

GATE CS 2014

In this question, we need to find out Netmask for each entry and BITWISE AND with given packet address, whichever equals the Netid, is the ans. Ex. 1st entry in table: 131.16.0.0/12. its MASK is first 12 bits of network(they are all 1) and remaining 20 bits of host(they are all 0). so MASK is 255.240.0.0 AND 131.23.151.76 = 131.16.0.0.

Last entry is 131.22.0.0/15 MASK—>255.254.0.0 AND 131.23.151.76 = 131.22.0.0. Two ans coming interfaces 1,3.

Longest Prefix Matching is used to decide among two. When one destination address matches more than one forwarding table entry. The most specific of the matching table entries is used as the interface.

In an IPv4 datagram, the M bit is 0, the value of HLEN is 10, the value of total length is 400 and the fragment offset value is 300. The position of the datagram, the sequence numbers of the first and the last bytes of the payload, respectively are

(A) Last fragment, 2400 and 2789
(B) First fragment, 2400 and 2759
(C) Last fragment, 2400 and 2759
(D) Middle fragment, 300 and 689

GATE CS 2013

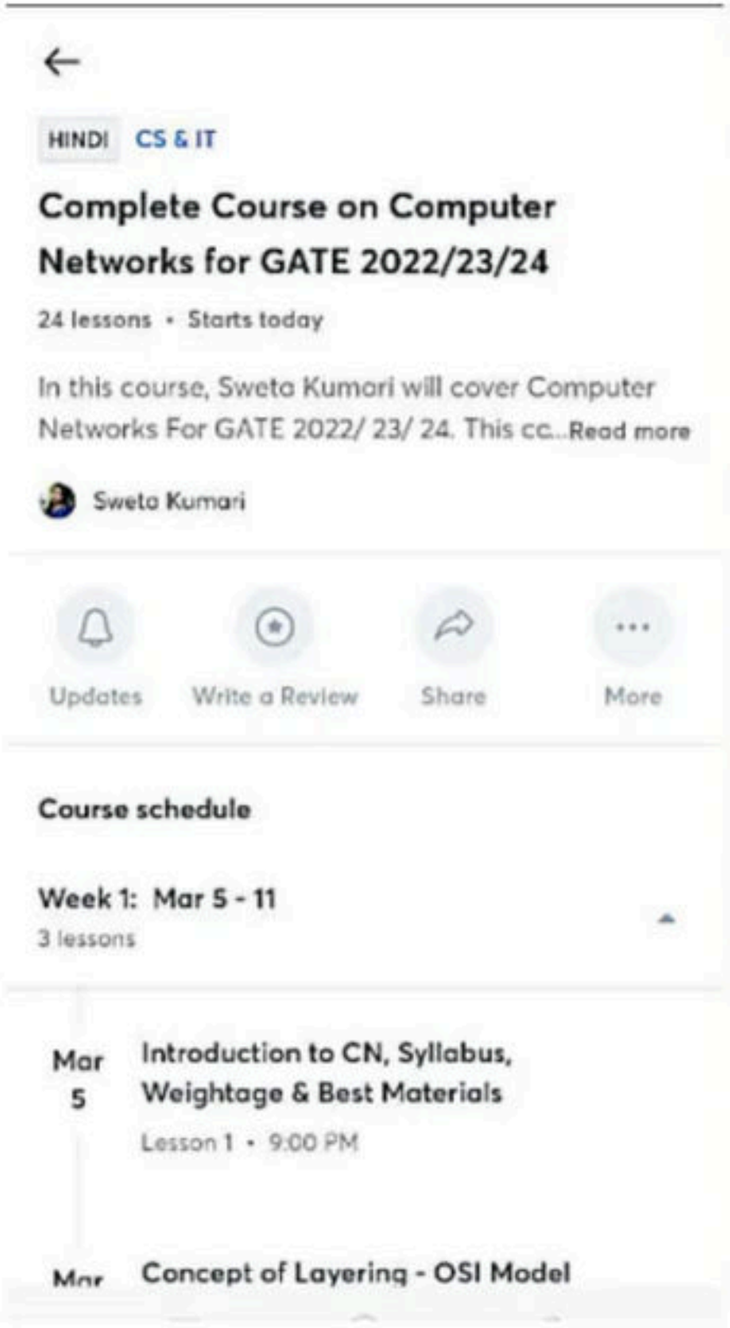
In an IPv4 datagram, the M bit is 0, the value of HLEN is 10, the value of total length is 400 and the fragment offset value is 300. The position of the datagram, the sequence numbers of the first and the last bytes of the payload, respectively are

(A) Last fragment, 2400 and 2789
(B) First fragment, 2400 and 2759
(C) Last fragment, 2400 and 2759
(D) Middle fragment, 300 and 689

GATE CS 2013

Answer: (C)

Explanation: M = 0 indicates that this packet is the last packet among all fragments of original packet. So the answer is either A or C.
It is given that HLEN field is 10. Header length is number of 32 bit words. So header length = 10 * 4 = 40
Also, given that total length = 400.
Total length indicates total length of the packet including header.
So, packet length excluding header = 400 – 40 = 360
Last byte address = 2400 + 360 – 1 = 2759 (Because numbering starts from 0)



PLEASE RATE AND REVIEW THE COURSE ☺

LIKE AND SHARE