REG.NO.:

SLOT: F2+TF2

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
FALL SEMESTER 2025-2026

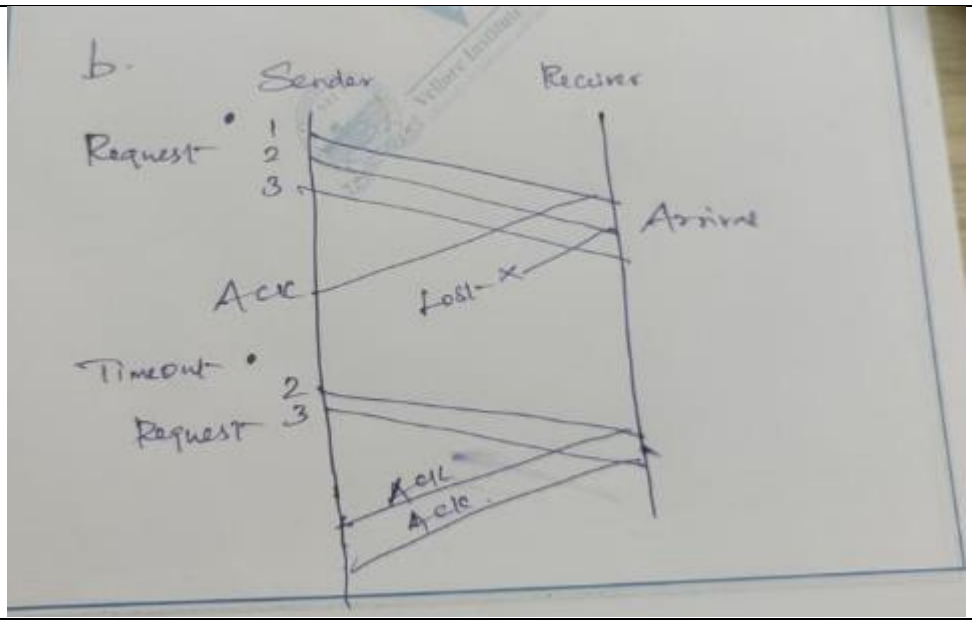
Programme Name & Branch : **B.TECH (CSE)**
Course Code and Course Name : **BCSE308L – COMPUTER NETWORKS**
Faculty Name(s) : **COMMON TO ALL**
Class Number(s) : **COMMON TO ALL**
Date of Examination :
Exam Duration : **90 minutes** **Maximum Marks: 50**

General instruction(s):

- Answer All Questions
- M - Max mark; CO – Course Outcome; BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyse, 5 – Evaluate, 6 – Create)
- Course Outcomes (Type the CO statements covered in this question paper. Use the CO number as per the syllabus copy)
  CO3: Identify and analyze error and flow control mechanisms in data link layer.
  CO4: Design sub-netting and analyze the performance of network layer with various routing protocols

Q. No	Question
1.	A) A Go-Back-n ARQ protocol is used with a sender window size of 8 and a sequence number range of 512. The receiver is expecting sequence number 100. a) List all possible sequence numbers that can be in the sender's window. b) If the sender transmits 3 packets and the 2nd packet is lost, explain how the retransmission will occur. **ANSWER:** **a) ARQ type:** Go-Back-N **Sender window size (WS):** 8 **Sequence number range:** 0 – 511 (i.e., total = 512) **Receiver expecting:** sequence number **100** (so last correctly received was 99). Sender Window - 100,101,102,103,104,105,106,107 – 8

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
FALL SEMESTER 2025-2026



B) Explain why CSMA/CA is preferred over CSMA/CD in wireless networks. Provide at least two reasons and illustrate your answer using a scenario, such as a university classroom with 50 laptops connected to Wi-Fi, where students are simultaneously submitting assignments, streaming lectures, and downloading resources. Include a communication diagram showing how CSMA/CA prevents collisions than CSMA/CD.

ANSWER:

CSMA/CA is Preferred in Wireless Networks

Reason 1 – Collision Detection Is Not Feasible in Wireless

- In **CSMA/CD**, a device can detect collisions by measuring signal interference on the cable while transmitting.
- In **wireless**, a node **cannot transmit and listen simultaneously** on the same channel because the transmitted signal is much stronger than any received signal — making collision detection impossible.
- Hence, **collision avoidance (CA)** is used — devices try to prevent collisions *before* they happen.

Reason 2 – Hidden and Exposed Station Problems

- Wireless nodes may not all hear each other due to range limits.
- For example, in a **university classroom with 50 laptops**:
    - Student A and Student C are at opposite ends of the room and **cannot sense each other's signals**.
    - Both may transmit at the same time to the same access point (AP) → **collision at the AP**.
- CSMA/CA uses **RTS/CTS (Request to Send / Clear to Send)** to solve this:
    - A sends RTS to AP.
    - AP replies CTS, notifying all nearby nodes to stay quiet.

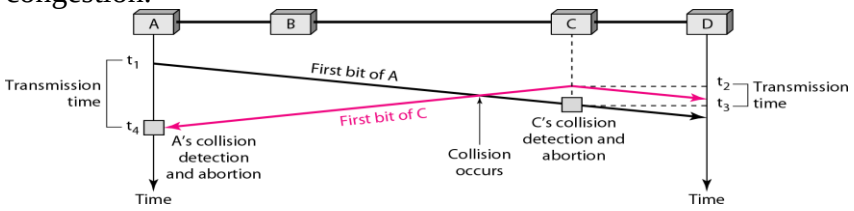
- This coordination **prevents hidden-node collisions**.

Scenario: University Classroom Example

Setting:

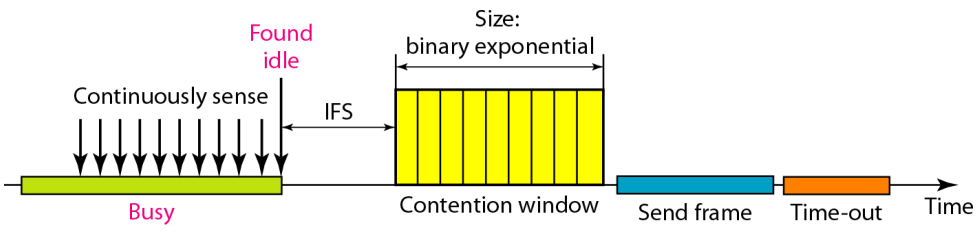
- 50 laptops connected to Wi-Fi (802.11).
- Activities: assignment uploads, lecture streaming, file downloads.
- Shared wireless medium → high contention.

Using CSMA/CD (if it were wireless)

- Each laptop listens before sending.
- But two far-apart laptops (hidden from each other) may transmit at once → **collisions at the AP**.
- No way to detect and stop mid-transmission → **data lost**, retransmissions increase congestion.
- 

Using CSMA/CA

1. **Carrier Sense:** Each laptop checks if the channel is idle.
2. **RTS/CTS exchange:**
   - Laptop A sends **RTS** → Access Point.
   - AP responds with **CTS** → all laptops hear CTS and defer transmission for a specified period.
3. **Data Transmission:**
   - Laptop A sends data safely; others wait.
4. **ACK:**
   - AP sends **ACK** confirming successful reception.

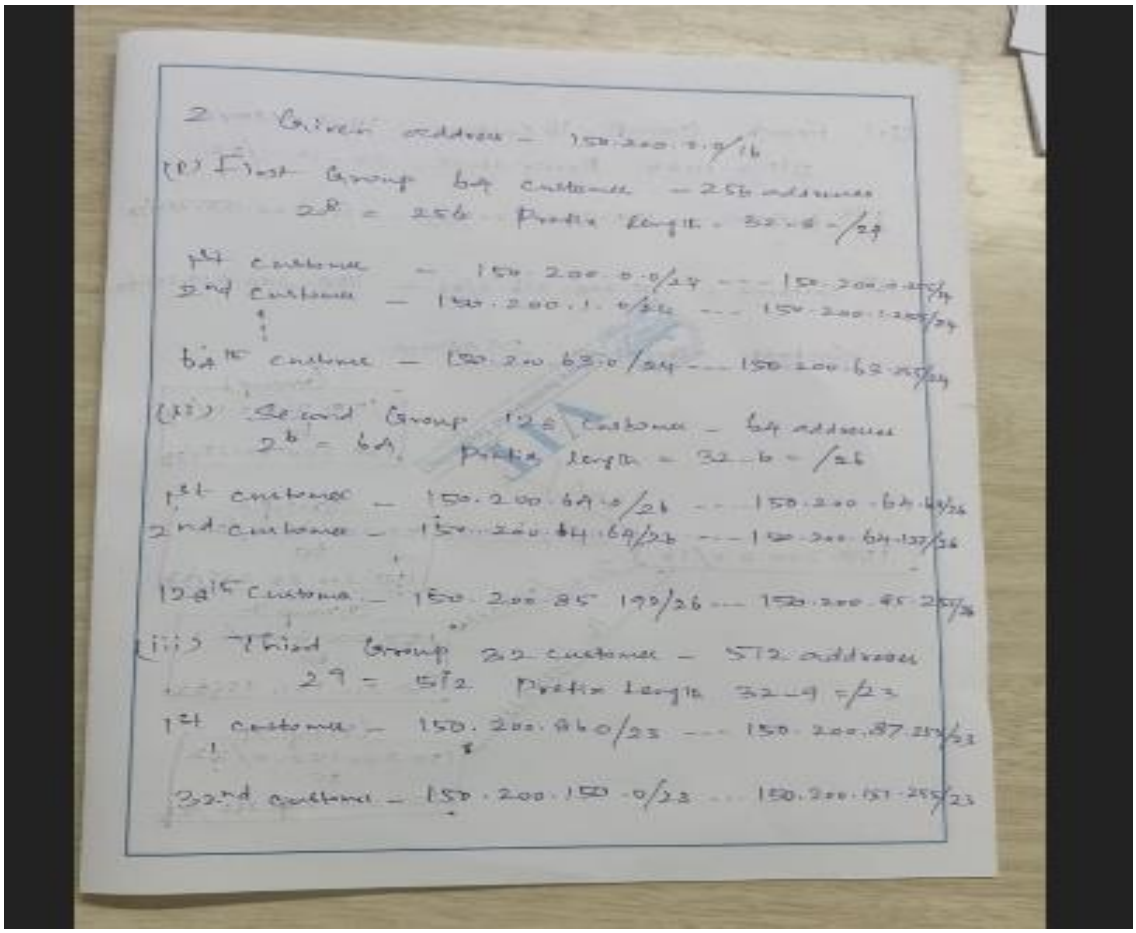


REG.NO.:

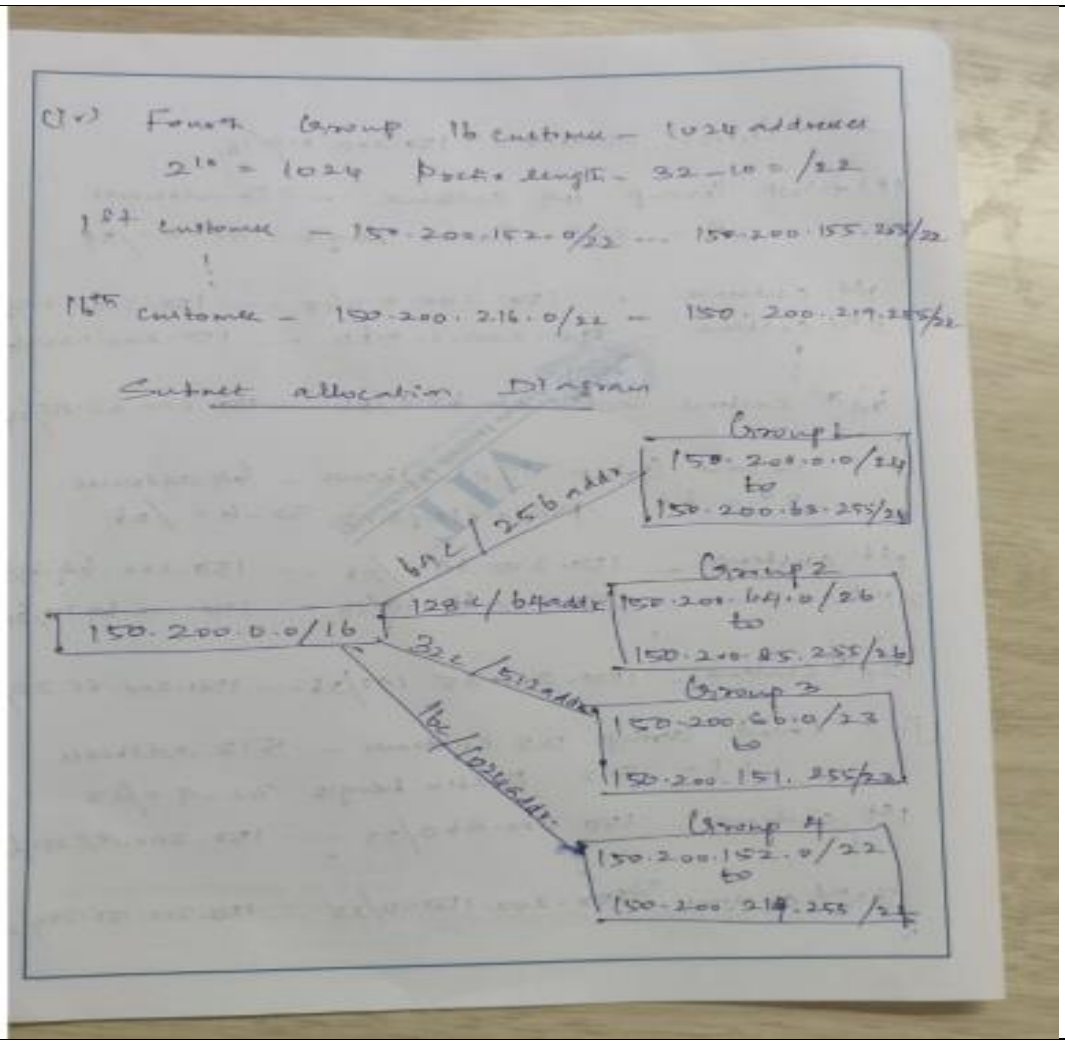
SLOT: F2+TF2

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
FALL SEMESTER 2025-2026

2.	A) An ISP is granted a block of addresses starting with 150.200.0.0/16. The ISP needs to distribute these addresses to several groups of customers as follows: The first group has 64 customers; each customer needs 256 addresses The second group has 128 customers; each customer needs 64 addresses The third group has 32 customers; each customer needs 512 addresses The fourth group has 16 customers; each customer needs 1024 addresses Draw a subnet allocation diagram showing how the 150.200.0.0/16 block is divided among all groups. **ANSWER:** 

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
FALL SEMESTER 2025-2026



B) A company has the private network 192.168.10.0/24 and is assigned a Public IP 203.0.113.5 by the ISP. All employees need Internet access. Explain how NAT will translate the private IPs to the public IP when accessing the Internet with NAT Address translation table.

ANSWER:

Private network: 192.168.10.0/24 (all employees)
Public IP: 203.0.113.5 (assigned by ISP)
Requirement: All employees need Internet access.

Since all employees share a single public IP, which maps multiple private IPs to a single public IP using different port numbers.

Private IP	Private Port	Public IP	Public Port
192.168.10.10	50000	203.0.113.5	40001
192.168.10.11	50001	203.0.113.5	40002
192.168.10.12	50002	203.0.113.5	40003

---

3. An IPv4 datagram has arrived with the following information in the header (in hexadecimal):

0x47 00 00 40 00 03 58 50 20 06 00 00 8D 2A 05 00 A4 0B 0F 03

a. Are there any optional field in the header field?
b. Is the packet corrupted?
c. Is the packet fragmented?
d. What is the size of the data? What is a upper layer Protocol?
e. How many more routers can the packet travel to?
f. What is the identification number of the packet?
g. What is the type of service?
h. If the packet is being sent over a network with a maximum transmission unit (MTU) of 40 bytes, will fragmentation occur? Explain.
i. Write the source and destination IP address and convert into binary and also identify their class and the subnet mask (2)

ANSWER:

0x47 00 00 40 00 03 58 50 20 06 00 00 8D 2A 05 00 A4 0B 0F 03

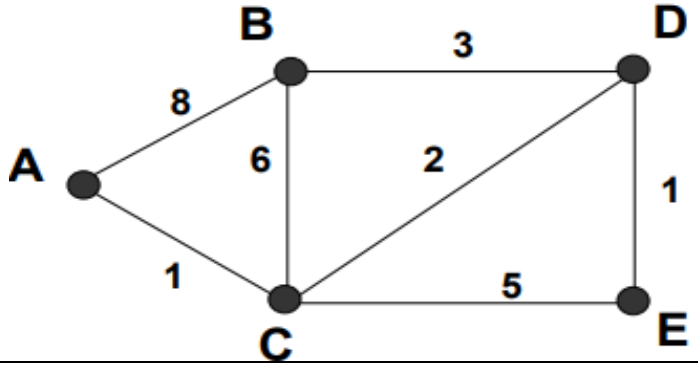
a. Are there any optional fields in the header?
Yes. IHL = 7 (words) → header length = 28 bytes. The minimum header is 5 words (20 bytes), so (7−5)×4 = 8 bytes of options are indicated.
Answer: Yes — 8 bytes of options are indicated.

b. The header checksum field is `0x0000` (normally a non-zero 16-bit checksum). You cannot reliably verify the checksum because the full 28-byte header (options) is not present in the provided bytes.
Answer: Yes — the header is inconsistent / likely corrupted (IHL indicates options but the options bytes are not present; checksum is 0x0000).

c. Flags = `010` → DF = 1 (Don't Fragment), MF = 0 (More Fragments = 0).
Answer: The header fields are inconsistent. If taken literally the non-zero fragment offset says *yes* it's a fragment, but DF=1 makes fragmentation illegal — so practical conclusion: **the fragment information is inconsistent (header corrupted); cannot reliably say it's a valid fragmented packet.**

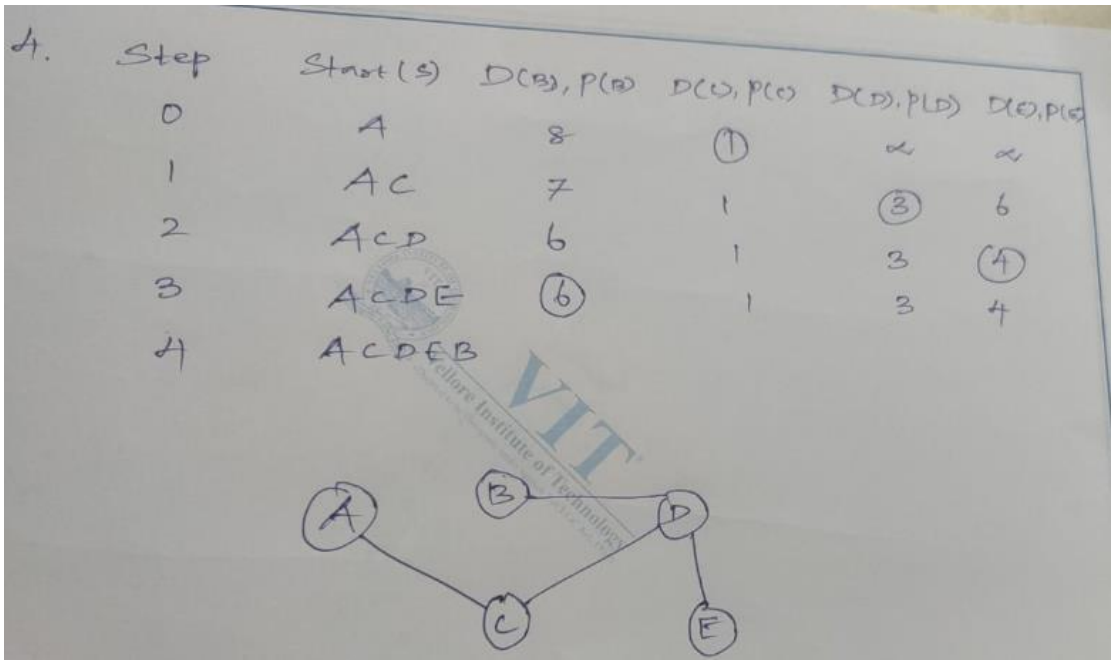
d. **What is the size of the data? What is the upper-layer protocol?**

Total length = 64 bytes; header length = 28 bytes → **data (payload) = 64 − 28 = 36 bytes**. Protocol field `0x06` → **TCP**.
Answer: Data size = **36 bytes**; upper-layer protocol = **TCP (protocol number 6)**.

	e. TTL = `0x20` = **32**. TTL is decremented by 1 at each router; so it can traverse up to **32 more hops/routers** **Answer: 32** more routers (hops). f. **What is the identification number of the packet?** Identification = `0x0003` = **3**. g. **What is the type of service?** TOS byte = `0x00`. In current terms DSCP = 0, ECN = 0. Old precedence/delay/throughput/reliability bits are all zero. h. **Answer:** Because **DF=1**, the packet **will not be fragmented** — instead it will be **dropped** by a router that finds MTU=40 and an ICMP "fragmentation needed" should be sent back. If DF were 0, you would need **5 fragments** (given header length 28 bytes and 36 bytes of data). If fragmentation were allowed (i.e., DF=0), compute fragments: each fragment must carry an IP header (same IHL = 28 bytes including options). With MTU 40, payload per fragment = 40 − 28 = **12 bytes** of data maximum. Fragment payloads (except possibly the last) must be multiples of 8 bytes. So the largest usable payload per fragment is 8 bytes. Total data = 36 bytes → fragments would be: 8,8,8,8,4 → **5 fragments** (first four with 8 bytes, last with 4 bytes). i. Source = **141.42.5.0** = `10001101.00101010.00000101.00000000` — Class **B**, default mask **255.255.0.0**. Destination = **164.11.15.3** = `10100100.00001011.00001111.00000011` — Class **B**, default mask **255.255.0.0**.
4.	A smart city authority is setting up a sensor network to monitor traffic congestion at major junctions. Each junction is represented as a node in the network, and the links between them represent data communication channels. The numeric value on each link indicates the cost of transmitting traffic data between the two junctions (this cost could be based on bandwidth usage, delay, or energy consumption). The control centre, located at Node A, must efficiently collect traffic updates from all other junctions with the least transmission cost. To determine this, the city engineers decide to apply Dijkstra's Least-Cost Algorithm. Consider a packet-switched network with Node A as the source. Using Dijkstra's shortest path (least-cost) algorithm, compute the least-cost paths from Node A to all other nodes. (6) 

a. Why is Dijkstra's Algorithm suitable for this traffic monitoring scenario instead of Bellman-Ford? (2)
b. If the communication cost of one link suddenly increases (e.g., due to congestion), explain how it affects the least-cost paths and how the algorithm would adapt. (2)

ANSWER:



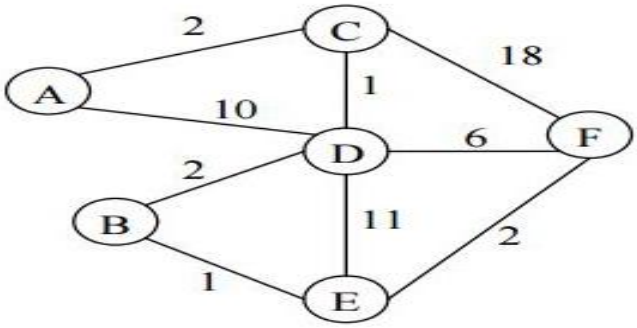
a. Why Dijkstra's Algorithm is suitable instead of Bellman-Ford:

Non-negative link costs:

I. In the traffic monitoring scenario, the transmission costs between junctions (bandwidth usage, delay, energy) are always non-negative.
II. Dijkstra's algorithm efficiently finds the shortest path in graphs with non-negative weights, whereas Bellman-Ford is designed to handle negative weights

b. Effect of a sudden increase in communication cost on least-cost paths:

1. **Impact on least-cost paths:**
   - If the cost of a link increases (e.g., due to congestion), paths that previously included that link may no longer be the least-cost paths.
   - Alternative routes with lower total cost may now become preferable.
2. **Algorithm adaptation:**
   - Dijkstra's algorithm can be **re-run from the source node** to recompute updated least-cost paths.

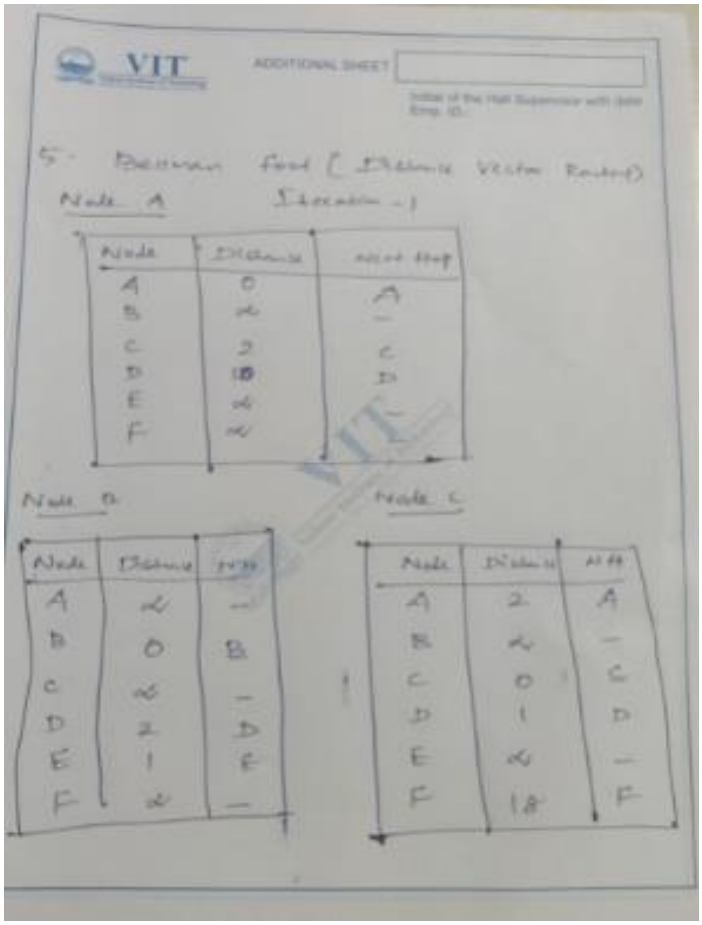
	○ If the network is dynamic, incremental approaches (can efficiently recompute paths without recalculating everything. ○ **Example:** If the link cost from Node A to Node B increases, the path A → B → C may become more expensive than a path A → D → C. The algorithm will adjust and select the new minimum-cost route.
5.	In a 5G-enabled smart hospital, each department have Administration, ICU, Radiology, Pharmacy, Emergency and Outpatient is equipped with an intelligent router forming a packet-switched network. The communication links between these departments have associated costs that reflect bandwidth usage, latency, or congestion. (Map the node according to the sequence to departments). Consider Administration (Node A) as the source, with direct links to Radiology and Pharmacy and other inter-department links as defined. Apply the Bellman-Ford algorithm with A as the source vertex to determine the least-cost paths to all other departments. Show all intermediate steps of distance vector updates, construct the routing table at Node A after each iteration, and indicate the final shortest paths. (6)  a. Suppose a link failure or oscillations in link cost occurs between any two departments (A→D), what is the effect of DV? (2) b. Suggest what are all the solutions can be applied in this hospital network to prevent routing loops and accelerate convergence for Q2.a. Apply any one. (2)

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
FALL SEMESTER 2025-2026

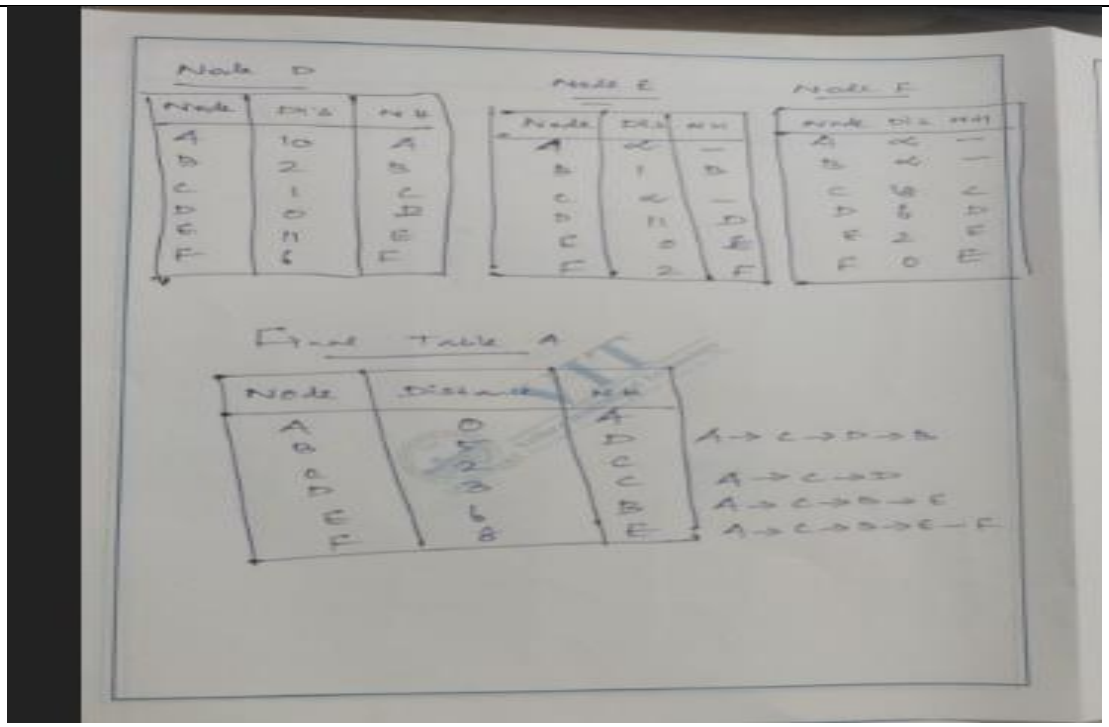
ANSWER:

- Define distances at each node x
  - $d_x(y)$ = cost of least-cost path from x to y
- Update distances based on neighbors
  - $d_x(y) = \min \{c(x,v) + d_v(y)\}$ over all neighbors v



VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
FALL SEMESTER 2025-2026



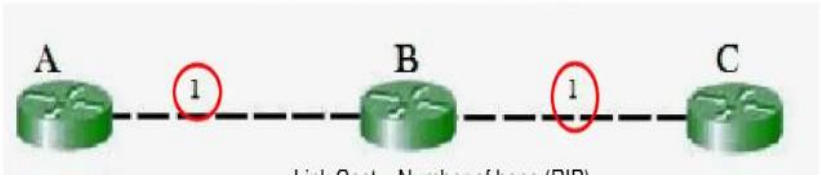
a. Suppose a link failure or oscillations in link cost occurs between any two departments (A→D), what is the effect of DV?

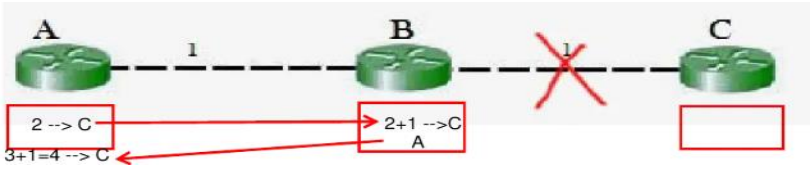
In DV routing, each node only knows the distance to its neighbours and shares its **distance vector** with them periodically.

When A → D fails:

1. Node A detects that its direct link to D is no longer reachable (distance becomes ∞).
2. A updates its distance vector and informs neighbours (C, B, etc.) that the cost to D is now ∞.
3. Neighbouring nodes recompute their shortest paths using the updated info and propagate changes and its lead to Count to Infinity problem
4. The oscillating costs propagate through the network, causing nodes to continuously recalculate shortest paths.
5. Frequent oscillations can lead to routing instability, slower convergence, and temporary routing loops.

Counting to infinity problem:





b. Suggest what are all the solutions can be applied in this hospital network to prevent routing loops and accelerate convergence for Q2.a. Apply any one.

Split horizon or Poison reverse

• **Split Horizon:** Prevents a router from advertising a route back to the router from which it was learned.

l **Split horizon**

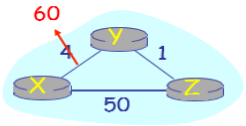
◆ **Never advertise a destination through its next hop**

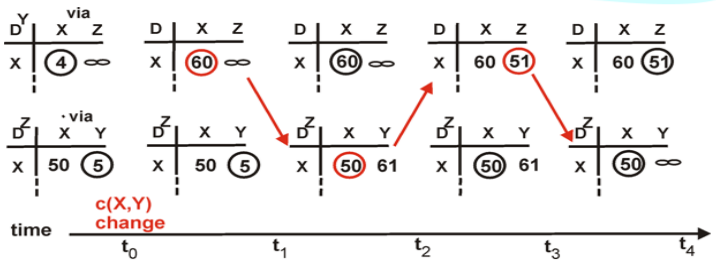
» *A* doesn't advertise *C* to *B*

Poison Reverse Example

If *Z* routes through *Y* to get to *X*:

• *Z* tells *Y* its (*Z*'s) distance to *X* is infinite (so *Y* won't route to *X* via *Z*)





2. Poison reverse: Send negative information when advertising a destination through its next hop Limitation: Only works for "loop" s of size 2