

Code: 23CS3502, 23AM3502, 23DS3502, 23IT3502

III B.Tech - I Semester - Regular Examinations - NOVEMBER 2025**COMPUTER NETWORKS**
(Common for CSE, AIML, DS, IT)

Duration: 3 hours

Max. Marks: 70

Note: 1. This question paper contains two Parts A and B.

2. Part-A contains 10 short answer questions. Each Question carries 2 Marks.

3. Part-B contains 5 essay questions with an internal choice from each unit. Each Question carries 10 marks.

4. All parts of Question paper must be answered in one place.

BL – Blooms Level

CO – Course Outcome

PART – A

		BL	CO
1.a)	Name any two functions of the Data Link layer in OSI.	L2	CO1
b)	State one advantage and one disadvantage of coaxial cable.	L2	CO1
c)	Mention any two advantages of using CRC over parity check.	L2	CO1
d)	Name any two error situations handled in the simplex protocol for noisy channels.	L2	CO1
e)	Mention two differences between FDMA and TDMA.	L3	CO2
f)	What is the principle of controlled access in MAC?	L3	CO2
g)	What is the main idea of the shortest path routing algorithm?	L3	CO3
h)	List two services provided by the network layer to the transport layer.	L3	CO3
i)	List any two services provided by UDP.	L4	CO4
j)	What are the two types of windows used in TCP flow control?	L4	CO4

UNIT-V				
10	a)	Analyse the fields of TCP header format.	L4	CO4
	b)	Analyse the E-mail architecture.	L4	CO4
OR				
11	a)	Compare and Contrast local login and remote login in terms of security and efficiency.	L4	CO4
	b)	Analyse DNS architecture with its record types.	L4	CO4

PART – B

		BL	CO	Max. Marks
--	--	----	----	------------

UNIT-I

2	a)	Describe the TCP/IP reference model and its layers.	L2	CO1	4 M
	b)	Compare the scalability of LAN, MAN, and WAN with real-world examples (e.g., home, metro city, global bank).	L2	CO1	6 M

OR

3	a)	Discuss the advantages and disadvantages of fiber optic cables compared with copper cables.	L2	CO1	4 M
	b)	The OSI and TCP/IP models differ in abstraction levels. Discuss how these differences influence protocol design and interoperability in modern networks.	L2	CO1	6 M

UNIT-II

4	a)	Write notes on flow control in the Data Link Layer.	L2	CO1	4 M
	b)	Why is the one-bit sliding window protocol considered as a special case of Go-Back-N? In Go-Back-N ARQ, if the window size is too large, what problems may occur?	L2	CO1	6 M

OR

5	a)	Compare simplex stop-and-wait and simplex noisy channel protocols.	L2	CO1	4 M
---	----	--	----	-----	-----

	b)	A noisy channel has a high error rate - Suggest modifications to the stop-and-wait protocol to improve efficiency.	L2	CO1	6 M
--	----	--	----	-----	-----

UNIT-III

6	a)	Why is CDMA more secure than FDMA and TDMA? Analyze.	L3	CO2	4 M
	b)	Controlled access eliminates collisions, but why is it less common in modern LANs compared to random access?	L3	CO2	6 M

OR

7	a)	Explain Slotted ALOHA and compare it with Pure ALOHA.	L3	CO2	4 M
	b)	Define CSMA. Explain collision detection with suitable example.	L3	CO2	6 M

UNIT-IV

8	a)	Explain the flooding algorithm and its limitations.	L3	CO3	4 M
	b)	Explain the implementation of connectionless service in the network layer.	L3	CO3	6 M

OR

9	a)	Compare distance vector and link state routing in terms of convergence and scalability.	L3	CO3	4 M
	b)	Compare the Virtual circuit and Datagram circuit network.	L3	CO3	6 M

III B.Tech - I Semester - Regular Examinations - NOVEMBER 2025
COMPUTER NETWORKS (23CS3502, 23AM3502, 23DS3502, 23IT3502)

SHORT SCHEME

PART A

1. Name any two functions of the Data Link layer in OSI.
 - List of functions of the Data Link layer. (2 marks)
2. State one advantage and one disadvantage of coaxial cable.
 - Advantage of coaxial cable. (1 mark)
 - Disadvantage of coaxial cable. (1 mark)
3. Mention any two advantages of using CRC over parity check.
 - Advantages of CRC over parity check. (2 marks)
4. Name any two error situations handled in the simplex protocol for noisy channels.
 - Two error situations handled by simplex protocol. (2 marks)
5. Mention two differences between FDMA and TDMA.
 - 1st difference between FDMA and TDMA. (1 mark)
 - 2nd difference between FDMA and TDMA. (1 mark)
6. What is the principle of controlled access in MAC?
 - Description of controlled access principle. (2 marks)
7. What is the main idea of the shortest path routing algorithm?
 - Explanation of shortest path routing algorithm. (2 marks)
8. List two services provided by the network layer to the transport layer.
 - List of services provided by the network layer. (2 marks)
9. List any two services provided by UDP.
 - List of services provided by UDP. (2 marks)
10. What are the two types of windows used in TCP flow control?
 - Types of windows used in TCP. (2 marks)

PART B

UNIT I

2. (a) **Describe the TCP/IP reference model and its layers. (4 marks)**
 - Architecture of TCP/IP reference model. (2 marks)
 - Explanation of each layer in TCP/IP model. (2 marks)

(b) **Compare the scalability of LAN, MAN, and WAN with real-world examples (home, metro city, global bank) (6 marks)**

 - Definition and comparison of LAN, MAN, WAN. (4 marks)
 - Real-world examples of each network type. (2 marks)
3. (a) **Discuss the advantages and disadvantages of fiber optic cables compared with copper cables. (4 marks)**
 - Advantages of fiber optic cables over copper cables. (2 marks)
 - Disadvantages of fiber optic cables over copper cables. (2 marks)

(b) **The OSI and TCP/IP models differ in abstraction levels. Discuss how these differences influence protocol design and interoperability in modern networks. (6 marks)**

 - Difference of OSI and TCP/IP models. (4 marks)
 - Influence protocol design and interoperability in modern networks. (2 marks)

UNIT II

4. (a) **Write notes on flow control in the Data Link Layer. (4 marks)**
 - Definition of flow control. (2 marks)
 - Types of flow control mechanisms. (2 marks)

(b) **Why is the one-bit sliding window protocol considered as a special case of Go-Back-N? In Go-Back-N ARQ, if the window size is too large, what problems may occur? (6 marks)**

- Explanation of one-bit sliding window as a special case of Go-Back-N. (4 marks)
- Issues with large window size in Go-Back-N ARQ. (2 marks)
- 5. (a) **Compare simplex stop-and-wait and simplex noisy channel protocols. (4 marks)**
 - At least 4 comparisons of both protocols. (4 marks)
- (b) **A noisy channel has a high error rate - Suggest modifications to the stop-and-wait protocol to improve efficiency (6 marks)**
 - Describe the limitations of the stop-and-wait protocol. (4 marks)
 - Explanation of how modifications improve efficiency. (2 marks)

UNIT III

- 6. (a) **Why is CDMA more secure than FDMA and TDMA? Analyze. (4 marks)**
 - Analysis of security features of CDMA compared to FDMA/TDMA. (4 marks)
- (b) **Controlled access eliminates collisions, but why is it less common in modern LANs compared to random access? (6 marks)**
 - Discussion of controlled access. (4 marks)
 - Comparison with random access in modern LANs. (1 marks)
 - Reason for less use of controlled access in LANs. (1 marks)
- 7. (a) **Explain Slotted ALOHA and compare it with Pure ALOHA. (4 marks)**
 - Explanation of Slotted ALOHA. (2 marks)
 - Comparison between Slotted ALOHA and Pure ALOHA. (2 marks)
- (b) **Define CSMA. Explain collision detection with suitable examples. (6 marks)**
 - Definition of CSMA. (2 marks)
 - Definition of CSMA. (2 marks)
 - Explanation of collision detection with examples. (4 marks)
- 8. (a) **Explain the flooding algorithm and its limitations. (4 marks)**
 - Explanation of the flooding algorithm. (2 marks)
 - Limitations of the flooding algorithm. (2 mark)
- (b) **Explain the implementation of connectionless service in the network layer. (6 marks)**
 - Definition of connectionless service. (2 marks)
 - Implementation details in the network layer. (4 marks)
- 9. (a) **Compare distance vector and link state routing in terms of convergence and scalability. (4 marks)**
 - Comparison of distance vector and link state routing in terms of convergence and scalability. (4 marks)
- (b) **Compare the Virtual circuit and Datagram circuit network. (6 marks)**
 - Comparison of Virtual circuit and Datagram circuit network. (6 marks)

UNIT IV

- 10. (a) **Analyze the fields of the TCP header format. (5 marks)**
 - TCP header format. (2 marks)
 - Description of each field in the TCP header. (3 marks)
- (b) **Analyze the E-mail architecture. (5 marks)**
 - Email architecture diagram. (2 marks)
 - Explanation of the email architecture components. (3 marks)
- 11. (a) **Compare and contrast local login and remote login in terms of security and efficiency. (4 marks)**
 - Comparison in terms of security and efficiency. (4 marks)
- (b) **Analyze DNS architecture with its record types. (6 marks)**
 - DNS architecture. (3 marks)
 - Explanation of DNS record types. (3 marks)

III B.Tech - I Semester - Regular Examinations - NOVEMBER 2025

COMPUTER NETWORKS (23CS3502, 23AM3502, 23DS3502, 23IT3502)
SCHEME

PART A

1. Name any two functions of the Data Link layer in OSI.
 - **List of functions of the Data Link layer. (2 marks)**
 1. Framing
 2. Addressing.
 3. Error detection
 4. Correction.
2. State one advantage and one disadvantage of coaxial cable.
 - **Advantage of coaxial cable. (1 mark)**
 1. High bandwidth.
 2. Long distance transmission.
 - **Disadvantage of coaxial cable. (1 mark)**
 1. Prone to physical damage.
 2. Expensive installation.
3. Mention any two advantages of using CRC over parity check.
 - **Advantages of CRC over parity check. (2 marks)**
 1. CRC detects more types of errors compared to parity.
 2. CRC has better error detection capability for larger data blocks.
4. Name any two error situations handled in the simplex protocol for noisy channels.
 - **Two error situations handled by simplex protocol. (2 marks)**
 1. Lost or corrupted frames.
 2. Duplicate frames due to retransmissions.
5. Mention two differences between FDMA and TDMA.
 - **1st difference between FDMA and TDMA. (1 mark)**

FDMA divides the frequency spectrum whereas TDMA divides time into slots for transmission
 - **2nd difference between FDMA and TDMA. (1 mark)**

Each user (or channel) is assigned a unique frequency that they use for the duration of the communication using FDMA whereas TDMA each user transmits in a specific time slot, one after another.
6. What is the principle of controlled access in MAC?
 - **Description of controlled access principle. (2 marks)**

A central controller or a distributed agreement decides who can transmit. This can happen in different ways:

 1. Reservation: Stations reserve the channel for a future time.
 2. Polling: A master device asks each station in turn whether it has data to send.
 3. Token passing: A special "token" circulates; only the station holding the token can transmit.
7. What is the main idea of the shortest path routing algorithm?
 - **Explanation of shortest path routing algorithm. (2 marks)**

The shortest path routing algorithm finds the path between a source and destination that has the minimum total cost, where cost may be distance, time delay, or number of hops. It calculates the shortest path using Dijkstra's algorithm.

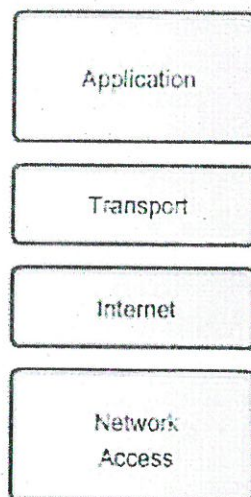
8. List two services provided by the network layer to the transport layer.
- **List of services provided by the network layer. (2 marks)**
 - Store and forwarding.
 - Packet routing.
 - Logical addressing
 - Error handling and flow control.
9. List any two services provided by UDP.
- **List of services provided by UDP. (2 marks)**
 - Process-to-process communication using port numbers
 - It's a connectionless communication.
 - Unreliable data delivery
 - No acknowledgment of received packets.
10. What are the two types of windows used in TCP flow control?
- **Types of windows used in TCP. (2 marks)**
 - Receive Window (rwnd): The receive window is the amount of data the receiver can accept without overflowing its buffer.
 - Congestion Window (cwnd): The congestion window is the amount of data the sender is allowed to transmit based on network congestion conditions.

PART B

UNIT I

2. (a) **Describe the TCP/IP reference model and its layers. (4 marks)**
- **Architecture of TCP/IP reference model. (2 marks)**

TCP/IP Model



- **Explanation of each layer in TCP/IP model. (2 marks)**

1. Application Layer

The Application layer is the topmost layer of the TCP/IP model and provides services directly to end-user applications. It includes protocols such as HTTP for web browsing, FTP for file transfer, SMTP for email, and DNS for domain name

resolution. This layer is responsible for data presentation, user interface support, and enabling software applications to communicate over the network.

2. Transport Layer

The Transport layer ensures reliable or fast end-to-end communication between devices. It uses protocols like TCP, which provides reliable, connection-oriented communication with error control and flow control, and UDP, which offers fast, connectionless communication without overhead. This layer breaks data into segments and ensures proper delivery to the correct process on the destination device.

3. Internet Layer

The Internet layer handles logical addressing and routing of data across networks. It uses the Internet Protocol (IP) to assign addresses and determine the best path for packets to travel from the source to the destination. Other protocols such as ICMP and ARP assist with error reporting and address mapping. This layer is essential for internetworking and packet forwarding.

4. Network Access Layer

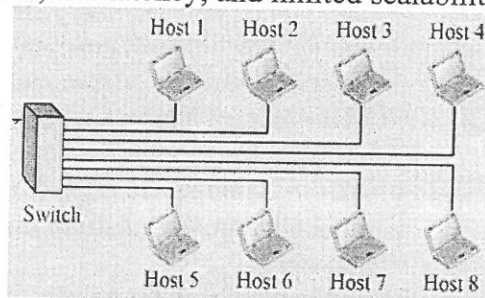
The Network Access layer (or Link layer) manages how data is physically sent over the network medium. It deals with MAC addressing, framing, error detection at the physical link, and interaction with hardware like switches, routers, Ethernet cables, and Wi-Fi. This layer ensures that data is correctly placed onto the physical network and received by the appropriate device.

(b) Compare the scalability of LAN, MAN, and WAN with real-world examples (home, metro city, global bank) (6 marks)

o Definition and comparison of LAN, MAN, WAN. (4 marks)

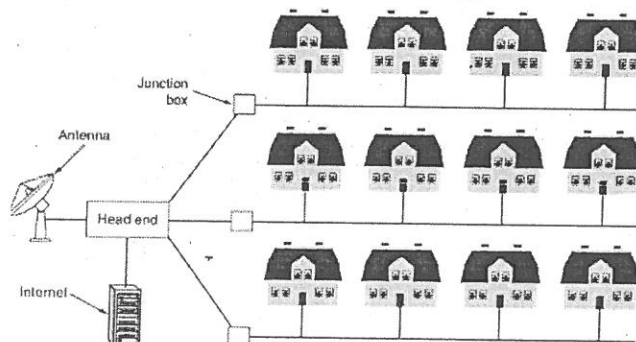
• LAN (Local Area Network):

A network covering a small area like a room, building, or campus. It has high speed, low latency, and limited scalability.



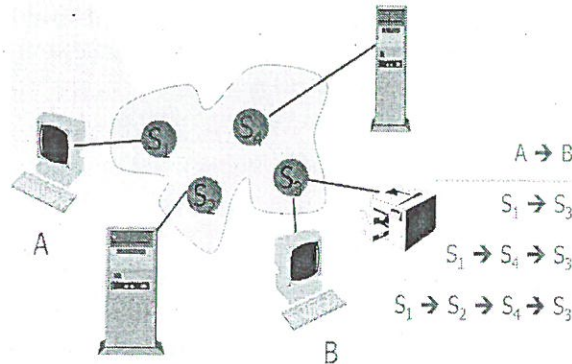
• MAN (Metropolitan Area Network):

A network that spans a city or large campus, interconnecting multiple LANs. It offers moderate speed, higher scalability than LAN, and covers several kilometers.



- **WAN (Wide Area Network):**

A network covering a country, continent, or the entire globe. It has lower speed compared to LAN/MAN but offers the highest scalability and longest distance coverage.



- LAN < MAN < WAN in terms of coverage area and scalability. LAN is fastest but least scalable; MAN provides city-wide scalability; WAN is the most scalable but generally lower in speed due to long-distance communication.

- **Real-world examples of each network type. (2 marks)**

- LAN Example: A home network connecting a laptop, smart TV, and router.
- MAN Example: A metro city fiber network providing internet across multiple areas of a city.
- WAN Example: A global bank network connecting branches across different countries.

3. (a) **Discuss the advantages and disadvantages of fiber optic cables compared with copper cables. (4 marks)**

- **Advantages of fiber optic cables over copper cables. (2 marks)**

- Bandwidth is above copper cables.
- Less power loss and allows data transmission for extended distances.
- Optical cable is resistance for electromagnetic interference.
- Fiber cable is sized as 4.5 times which is best than copper wires.

- **Disadvantages of fiber optic cables over copper cables. (2 marks)**

- These cable are very difficult to merge so there'll be loss of beam within cable.
- Installation of those cables is cost-effective, they're not as robust because wires.
- These cable are highly vulnerable while fitting.
- These cables are more delicate than copper wires.

(b) **The OSI and TCP/IP models differ in abstraction levels. Discuss how these differences influence protocol design and interoperability in modern networks. (6 marks)**

- **Difference of OSI and TCP/IP models. (4 marks)**

OSI Model	TCP/IP (Internet) Model
First the model was created, and then protocols were designed to fit it.	First the protocols were developed and later the model was described.
Clear distinction between service,	This model does not clearly separate

interface, and protocol.	service, interface, and protocol.
Protocols are better hidden due to strict layering.	Layer boundaries are less strict; protocols openly cross layers.
Number of layers are 7.	Number of layers are 4.
Internetworking was added later to the model.	Internetworking was included from the start; built for global connectivity.
Good for network design concepts.	Highly practical and widely adopted for real-world networking.

○ **Influence protocol design and interoperability in modern networks. (2 marks)**

- The TCP/IP was designed around working protocols and practical internetworking, most modern network protocols are built for flexibility, real-world performance, and interoperability across diverse systems.
- OSI's structured concepts, the separation of service, interface, and protocol still influence how new protocols are formally designed.
- The both models help ensure that modern networks maintain compatibility, efficient layering, and smooth communication across different hardware and software platforms.

UNIT II

4. (a) **Write notes on flow control in the Data Link Layer. (4 marks)**

○ **Definition of flow control. (2 marks)**

- Flow control is the technique used to prevent a sender from overloading the receiver with packets.
- It ensures that the receiver can process incoming frames at its own pace by limiting the amount or rate of data transmitted by the sender.
- Flow control is essential because the source may send PDUs faster than the destination can process them, higher-level protocol users may be slow in retrieving data, or the destination may need to limit incoming flow to match retransmission requirements.

○ **Types of flow control mechanisms. (2 marks)**

Flow control operates using two mechanisms as described below:

1. **Implicit Mechanism:**

An ACK packet implies permission to send additional data. The arrival of an acknowledgment signals that the receiver is ready for more packets.

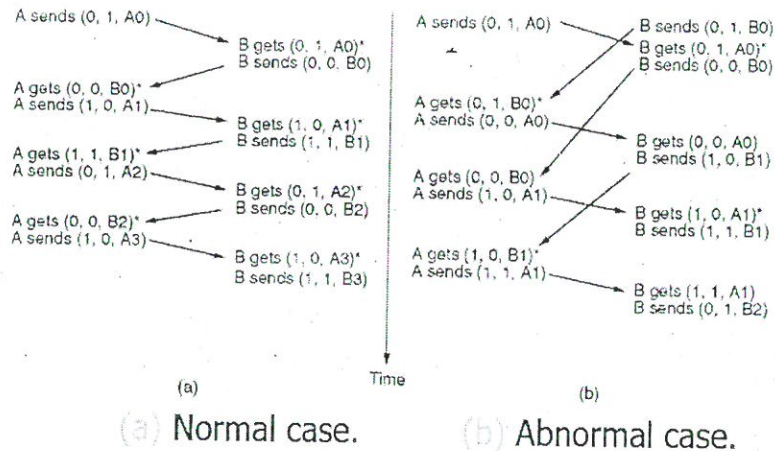
2. **Explicit Mechanism:**

The receiver directly communicates its window size, clearly specifying how many frames the sender is allowed to transmit. This ensures controlled, window-based data flow between sender and receiver.

(b) **Why is the one-bit sliding window protocol considered as a special case of Go-Back-N? In Go-Back-N ARQ, if the window size is too large, what problems may occur? (6 marks)**

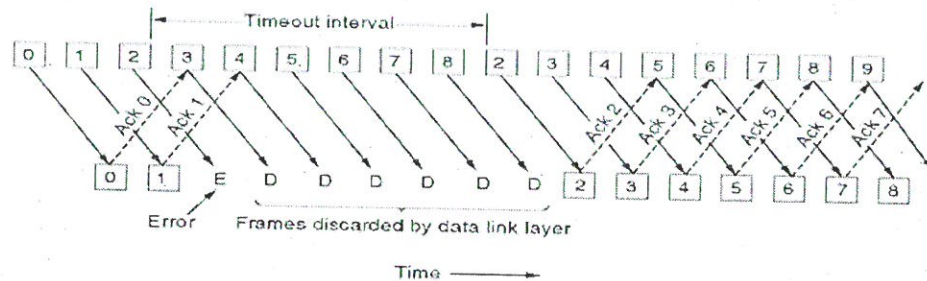
○ **Explanation of one-bit sliding window as a special case of Go-Back-N. (4 marks)**

A One-Bit Sliding Window Protocol:



The one-bit sliding window protocol is considered a special case of the Go-Back-N ARQ protocol because it operates with a window size of exactly one frame. In Go-Back-N, the sender is allowed to transmit multiple frames before receiving an acknowledgment, depending on the window size. However, when the sender's window size is restricted to 1, the sender must wait for an ACK for each frame before sending the next frame, which is exactly how the one-bit sliding window protocol works. Thus, it represents the simplest form of Go-Back-N, where there is no pipelining, and any lost or damaged frame requires the sender to go back and retransmit that same frame, just like in Go-Back-N behavior.

Go-Back-N

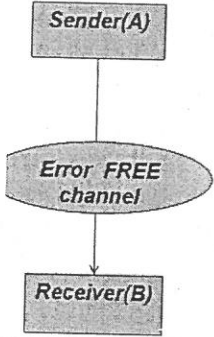
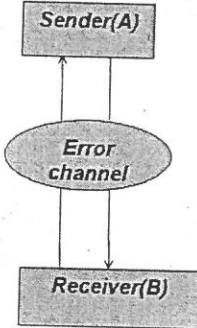


- Go-Back-N represents the most common form of error control based on the sliding window mechanism.
 - The number of unacknowledged frames that the sender can transmit is determined by the window size.
 - When a frame is received in error, the destination discards that frame and all subsequent frames until the damaged frame is correctly received.
 - The sender resends the frame (and all following frames) either when it receives a Reject message or when the timer expires.
- **Issues with large window size in Go-Back-N ARQ. (2 marks)**
- If the window size in Go-Back-N ARQ is too large, several problems may occur.
1. The sender may flood the receiver with more frames than it can buffer, causing buffer overflow and frame loss.
 2. If an error occurs in a single frame, Go-Back-N requires retransmission of all subsequent frames, so a large window can lead to a high retransmission overhead, wasting bandwidth.

3. Error recovery becomes inefficient, and the network may experience increased congestion and delays, as the sender must resend a large block of frames whenever a single frame is lost or corrupted.

5. (a) Compare simplex stop-and-wait and simplex noisy channel protocols. (4 marks)

- At least 4 comparisons of both protocols. (4 marks)

Simplex Stop-and-Wait Protocol	Simplex Noisy Channel Protocol
Assumes an error-free channel.	Assumes a noisy/error-prone channel.
No need for error detection or recovery.	Requires error detection, ACKs, timers, and retransmissions
Sender sends one frame and waits for ACK, no frames get corrupted or lost	Sender sends one frame and waits if damaged/lost, sender retransmits after timeout.
Simple and straightforward.	More complex due to timers, ACK processing, and retransmission.
High reliability only in ideal, noise-free conditions.	High reliability even when errors occur.
	

(b) A noisy channel has a high error rate, suggest modifications to the stop-and-wait protocol to improve efficiency (6 marks)

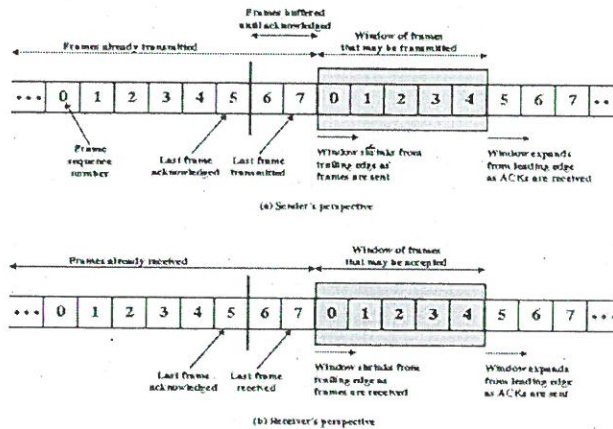
- Describe the limitations of the stop-and-wait protocol. (4 marks)

The stop-and-wait protocol becomes highly inefficient in a noisy channel due to several limitations.

1. It allows the sender to transmit only one frame at a time, causing the channel to remain idle while waiting for acknowledgments.
2. In a noisy environment, frames or ACKs may be lost or corrupted frequently, forcing the sender to retransmit the same frame repeatedly, which further reduces throughput.
3. The protocol also relies on long timeout periods, and each error forces a complete restart of the single-frame transmission.
4. Because the sender cannot pipeline multiple frames, the protocol suffers from low utilization, especially when the propagation delay is high.
5. Stop-and-wait wastes bandwidth and performs poorly under high error rates.

- Explanation of how modifications improve efficiency. (2 marks)

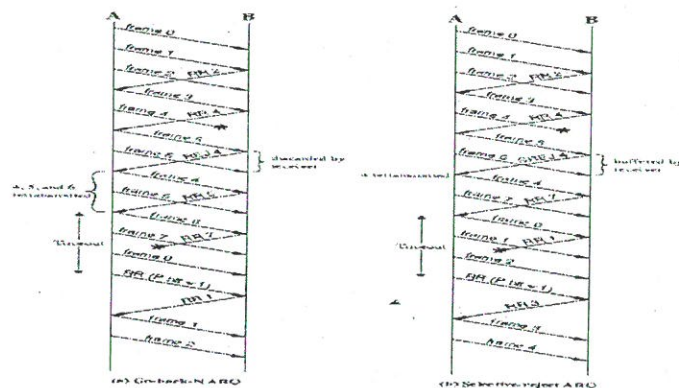
- Efficiency can be improved by extending stop-and-wait into **pipelined sliding-window protocols** such as **Go-Back-N** or **Selective Repeat**.



- Allow multiple frames to be in transit at the same time.
- Source can send n frames without waiting for acknowledgements.
- Destination can accept n frames.
- Destination acknowledges a frame by sending acknowledgement with sequence number of next frame expected (and implicitly ready for next n frames)
- These protocols allow the sender to transmit multiple frames before waiting for acknowledgments, keeping the channel busy and increasing throughput.

Go-Back-N: Upon receiving a frame in error, destination discards that frame and all subsequent frames until damaged frame received correctly. Sender resends frame (and all subsequent frames) either when it receives a Reject message or timer expires

Selective Repeat further enhances efficiency by retransmitting only the damaged frames, reducing unnecessary retransmissions.



Sliding-window protocols

These modifications improve channel utilization, reduce idle time, and maintain performance even when the error rate is high.

UNIT III

6. (a) Why is CDMA more secure than FDMA and TDMA? Analyze. (4 marks)
- Analysis of security features of CDMA compared to FDMA/TDMA. (4 marks)

CDMA	FDMA	TDMA
All users share the same frequency band but use unique spreading codes .	Users are assigned separate frequency bands .	Users share frequency but use separate time slots .
By unique pseudo-random codes.	By different frequencies.	By different time slots.
Very high; difficult to detect or decode without the code.	Low; intruder can tune to the frequency.	Medium; intruder can capture time-slot transmissions.
High security due to spread-spectrum and code-based access. Signals appear as noise without the code.	Low security because each user occupies a fixed frequency that can be tuned easily.	Moderate security but time slots can be captured or analyzed.
Most secure because of code-based privacy and inherent anti-jamming properties.	Least secure.	More secure than FDMA but less secure than CDMA.

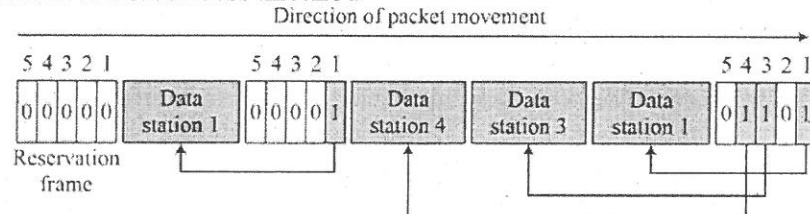
- (b) Controlled access eliminates collisions, but why is it less common in modern LANs compared to random access? (6 marks)

- Discussion of controlled access. (4 marks)

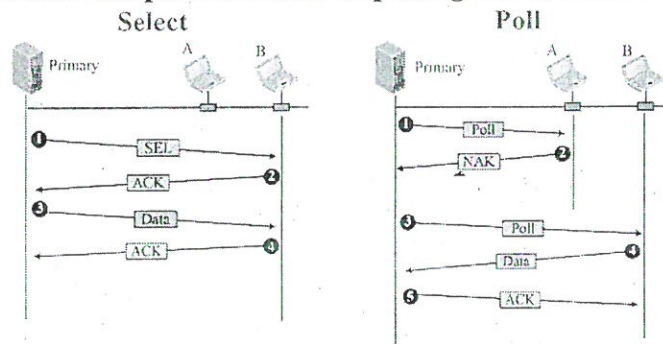
In controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations. Types of Controlled Access Protocols

- Reservation
 - Select
 - Poll
- Token Passing
 - Logical Ring

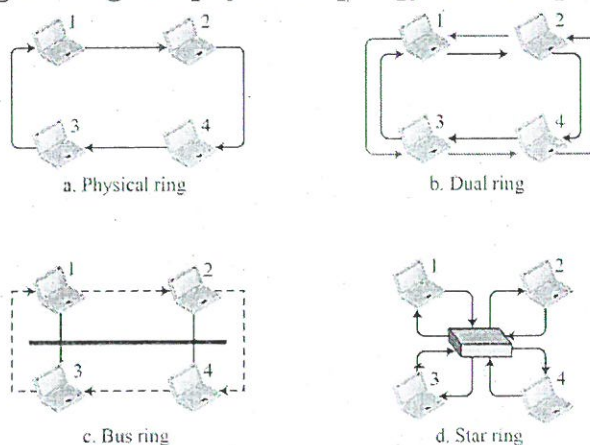
Reservation access method



Select and poll functions in polling-access method



Logical ring and physical topology in token-passing access method



Comparison with random access in modern LANs. (1 marks)

- In contrast, random-access methods like CSMA/CD allow nodes to transmit whenever the medium appears idle, leading to occasional collisions but offering simple, fast, and flexible operation.
- Modern LANs using switches practically eliminate collisions even with random access rules, while providing far greater scalability, lower delay, and plug-and-play configuration.
- Random-access Ethernet has therefore become more efficient and easier to deploy than controlled access mechanisms.

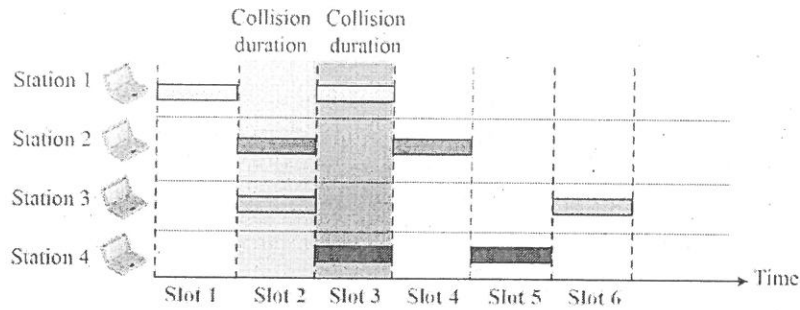
Reason for less use of controlled access in LANs. (1 marks)

- Controlled access is less common in modern LANs because it introduces high coordination overhead, reduces efficiency under light loads, and lacks the flexibility and scalability required for today's high-speed switched networks.
- Random access with switching achieves collision-free communication without the complexity of controlled-access schemes.

7. (a) Explain Slotted ALOHA and compare it with Pure ALOHA. (4 marks)

Explanation of Slotted ALOHA. (2 marks)

Slotted ALOHA is a random access protocol in which time is divided into equal-sized time slots. A station is allowed to transmit only at the beginning of a slot, which reduces the chances of collisions. If two or more stations transmit in the same slot, a collision occurs and the stations retransmit after a random delay.



- Comparison between Slotted ALOHA and Pure ALOHA. (2 marks)

Pure ALOHA	Slotted ALOHA
Stations can transmit anytime	Stations can transmit only at slot boundaries
Collision Probability is higher, because frames can overlap randomly	Collision Probability is lower, because collisions occur only when two stations choose the same slot
Throughput is 18%	Throughput is 37% (almost double)
No need for synchronization	Requires time synchronization among all stations

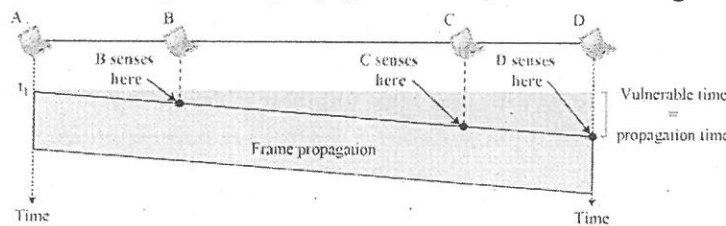
- (b) Define CSMA. Explain collision detection with suitable examples. (6 marks)

- Definition of CSMA. (2 marks)

Carrier Sense Multiple Access (CSMA) is a random access protocol in which a station listens to the channel (carrier sense) before transmitting. If the channel is idle, it transmits; if the channel is busy, it waits. This helps reduce the chances of collision by ensuring that no two stations transmit simultaneously without checking the medium.

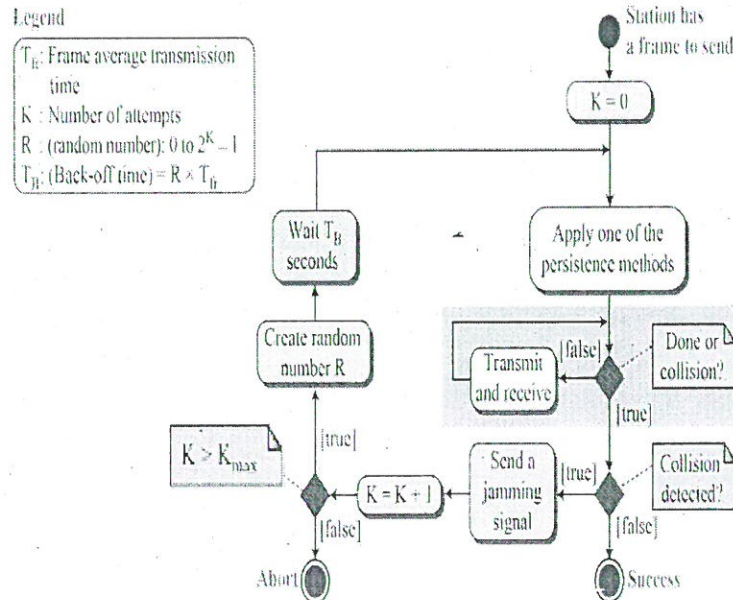
- Explanation of collision detection with examples. (4 marks)

Even though stations sense the channel before transmitting, collisions can still occur, mainly due to propagation delay as show in figure bellow.



CSMA with Collision Detection (CSMA/CD), used in traditional Ethernet, helps detect these collisions quickly. How Collision Detection Works

- A station listens to the medium.
- If the medium is free, it begins transmission.
- While transmitting, the station monitors the channel to detect any interference or sudden change in signal strength.
- If a collision is detected, the station immediately stops transmission and sends a jam signal to notify all other nodes.
- After that, it waits for a random backoff time before attempting to retransmit.



Flow diagram for the CSMA/CD

UNIT III

8. (a) Explain the flooding algorithm and its limitations. (4 marks)

o Explanation of the flooding algorithm. (2 marks)

Flooding is a network routing technique in which every incoming packet is sent through all outgoing links except the one it arrived on, ensuring that the packet reaches all nodes in the network. No routing table or knowledge of network topology is required. Every node blindly forwards the packet to all neighbors. It is useful for broadcasting messages to all nodes and Network discovery.

o Limitations of the flooding algorithm. (2 mark)

1. Redundant Packets / Duplicates: Multiple copies of the same packet circulate in the network, leading to unnecessary traffic.
2. Congestion: Too many duplicate packets can cause network overload, wasting bandwidth and slowing down the network.
3. Loops / Infinite Circulation: Without a hop count or sequence number, packets may keep circulating in loops indefinitely.
4. High Resource Usage: Nodes must process many unnecessary packets, increasing processing load and memory usage.

(b) Explain the implementation of connectionless service in the network layer. (6 marks)

o Definition of connectionless service. (2 marks)

A connectionless service is a communication method in which data packets are sent independently without establishing a dedicated connection between the sender and receiver. Each packet is treated as a self-contained unit and may take different routes to reach the destination. There is no setup phase, no guarantee of delivery, and no sequencing control in the network layer.

o Implementation details in the network layer. (4 marks)

- Packets travel as independent datagrams.
- Each router forwards packets using destination-based routing tables.
- No connection setup or state is maintained.

- Different packets may take different routes, shown by multiple paths between routers.

The diagram shows a datagram network where each packet is routed independently without establishing a dedicated connection. Routers (A, B, C, D, E, F) maintain routing tables that map destinations to the next hop.

Each packet from Process P1 at H1 is sent into the network without prior setup. The packet carries the full destination address (H2). Router A receives the packet. A looks into its routing table (shown as "A's table") to determine which link leads toward the destination. Initially, A may not know the best path, but later its table improves (based on routing algorithm updates).

Every router in the network forwards packets independently by consulting its own routing table. For example, when the destination is router F (which connects to host H2), router A checks its updated routing table and forwards the packet to C. Router C, based on its own table, then forwards the packet to E. Router E uses its routing information to send the packet to F, and finally router F delivers it to the LAN connected to H2. At each step, the forwarding decision is made locally by the router, without depending on previous packets or any established connection.

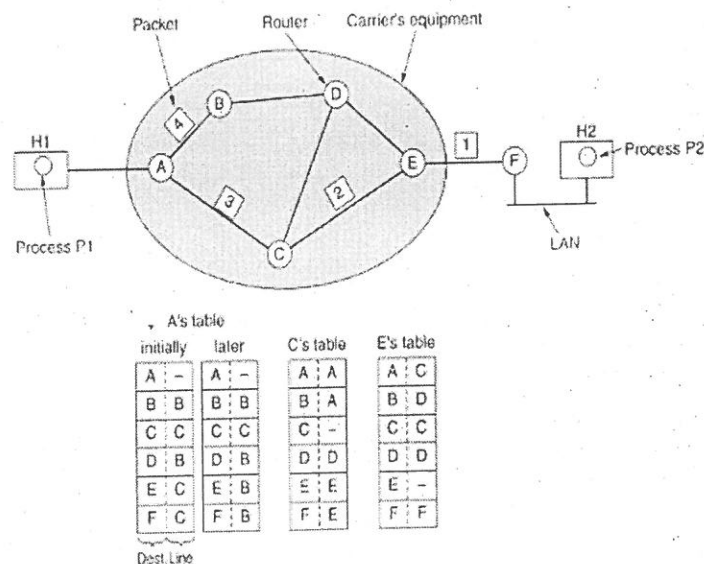


Figure Implementation of connection less service.

9. (a) Compare distance vector and link state routing in terms of convergence and scalability. (4 marks)

- Comparison of distance vector and link state routing in terms of convergence and scalability. (4 marks)

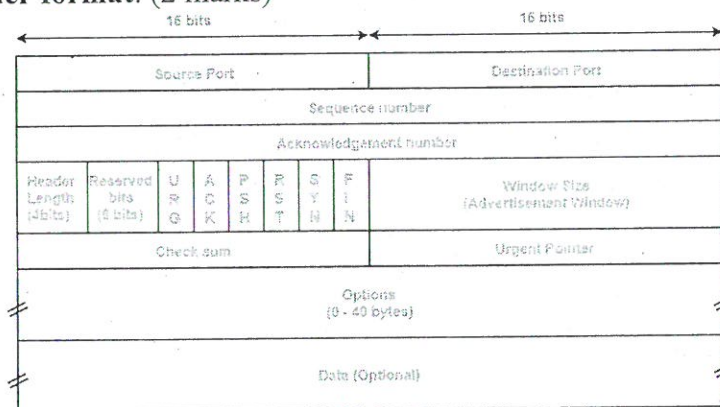
Feature	Distance Vector Routing	Link State Routing
Convergence	Slow convergence; updates spread gradually, and may suffer from <i>count-to-infinity</i> problems.	Fast convergence; routers flood updates immediately and compute routes using Dijkstra's algorithm.
Scalability	Suitable for small to medium networks; limited scalability due to slow convergence.	Highly scalable; supports large networks but requires more CPU, memory, and bandwidth.

- (b) Compare the Virtual circuit and Datagram circuit network. (6 marks)
- Comparison of Virtual circuit and Datagram circuit network. (6 marks)

Virtual Circuit Network	Datagram Network
Requires a connection establishment phase before data transfer.	No connection setup; each packet is sent independently.
All packets follow the same predefined path.	Packets may take different paths to reach the destination.
Packets carry a short virtual circuit identifier (VCI).	Each packet carries the full destination address.
More reliable; resources can be reserved, ensuring guaranteed service.	Less reliable; delivery is best-effort with no guarantee.
Low overhead after setup; routing decision made only once.	High overhead; routing decision made for every packet.
Congestion Control is easier, because path and flow are known in advance.	Congestion Control is difficult, since packets move independently without path knowledge.
Failure in path requires re-establishing the virtual circuit.	More robust; packets can be routed around failures dynamically.
Used in ATM, Frame Relay, and some QoS-based networks.	Used in IP networks, such as the Internet.

UNIT IV

10. (a) Analyze the fields of the TCP header format. (5 marks)
- TCP header format. (2 marks)



TCP Header

- Description of each field in the TCP header. (3 marks)

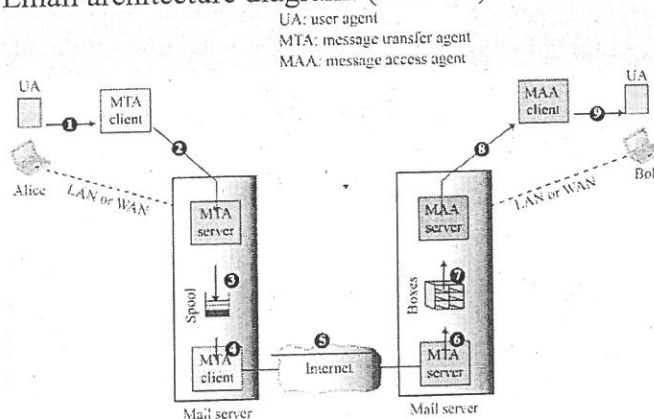
The TCP header contains several fields used for reliable, connection-oriented communication. A standard TCP header is 20 bytes long (without options) and includes fields such as ports, sequence numbers, flags, window size, checksum, and others. Optional fields may extend the header beyond 20 bytes.

- Source Port (16 bits): Identifies the sending application on the source device.
- Destination Port (16 bits): Identifies the receiving application on the destination device.

3. Sequence Number (32 bits): Indicates the byte number of the first byte in the current segment. Used for ordered, reliable delivery.
4. Acknowledgment Number (32 bits): Indicates the next expected byte from the sender. Used in acknowledgment and flow control.
5. Header Length (Data Offset) – 4 bits: Specifies the size of the TCP header (in 32-bit words).
6. Control Flags (6 bits):
 - SYN: Start connection
 - ACK: Acknowledgment valid
 - FIN: End connection
 - RST: Reset connection
 - PSH: Push data to application
 - URG: Urgent data
7. Window Size (16 bits): Specifies the amount of data the receiver can accept; used for flow control.
8. Checksum (16 bits): Used for error detection of the header and data.
9. Urgent Pointer (16 bits): Points to the end of urgent data when URG flag is set.
10. Options (Variable length)
Used for advanced features like Maximum Segment Size (MSS) and Window Scaling.

(b) Analyze the E-mail architecture. (5 marks)

- Email architecture diagram. (2 marks)



- **Explanation of the email architecture components. (3 marks)**

Electronic mail (or e-mail) allows users to exchange messages. The nature of this application, however, is different from other applications discussed so far. In an application such as HTTP or FTP, the server program is running all the time, waiting for a request from a client. When the request arrives, the server provides the service. In the case of electronic mail, the situation is different. It uses three different agents: a User Agent (UA), a Mail Transfer Agent (MTA), and a Message Access Agent (MAA).

The electronic mail system needs two UAs, two pairs of MTAs (client and server), and a pair of MAAs (client and server).

a) User Agent (UA): The mail client used by sender and receiver (e.g., Outlook, Gmail app). It allows users to compose, read, send, and manage emails.

b) Mail Submission Server (SMTP Server): When a user sends an email, the client submits it to the SMTP server. This server accepts outgoing mail and forwards it to the next server.

c) Message Transfer Agent (MTA): This is the main SMTP server responsible for routing and transferring email across networks. It looks up the destination domain (via DNS) and forwards the mail to the correct remote MTA.

d) Mail Delivery Agent (MDA): The MDA is responsible for final delivery into the recipient's mailbox. It stores messages in the user's mailbox on the server.

e) Mail Access Server (POP3/IMAP Server): Users retrieve email using POP3 or IMAP:

- POP3 downloads mail to the device.
- IMAP keeps mail on the server and synchronizes across devices.

11. (a) Compare and contrast local login and remote login in terms of security and efficiency. (4 marks)

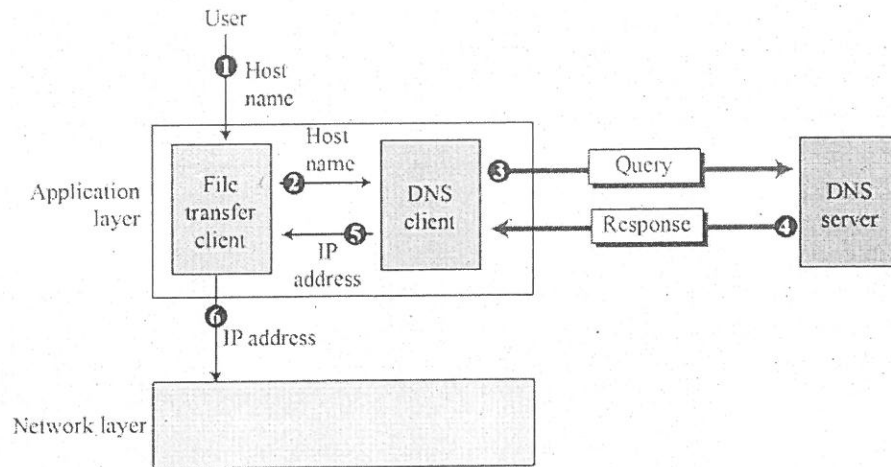
o Comparison in terms of security and efficiency. (4 marks)

Feature	Local Login	Remote Login
Security	More secure since user accesses the system directly with no network involvement; no risk of packet sniffing or MITM attacks.	Less secure because login occurs over a network; vulnerable to eavesdropping or hijacking unless encrypted (e.g., SSH).
Efficiency	Highly efficient; fast response as all processing happens locally with no network delay.	Less efficient; performance depends on network speed, latency, and reliability, causing possible delays.

(b) Analyze DNS architecture with its record types. (6 marks)

o DNS architecture. (3 marks)

To identify an entity, TCP/IP protocols use the IP address, which uniquely identifies the connection of a host to the Internet. However, people prefer to use names instead of numeric addresses. Therefore, the Internet needs to have a directory system that can map a name to an address. This is analogous to the telephone network. A telephone network is designed to use telephone numbers, not names. People can either keep a private file to map a name to the corresponding telephone number or can call the telephone directory to do so. Since the Internet is so huge today, a central directory system cannot hold all the mapping. In addition, if the central computer fails, the whole communication network will collapse. A better solution is to distribute the information among many computers in the world. In this method, the host that needs mapping can contact the closest computer holding the needed information. This method is used by the Domain Name System (DNS). TCP/IP uses a DNS client and a DNS server to map a name to an address. The architecture as shown in bellow.



○ **Explanation of DNS record types. (3 marks)**

According to the DNS resource record structure in the document, each DNS server stores resource records defined as a 5-tuple:

(Domain Name, Type, Class, TTL, Value).

- The domain name field is what identifies the resource record.
- The value defines the information kept about the domain name.
- The TTL defines the number of seconds for which the information is valid.
- The class defines the type of network class address.
- The type defines how the value should be interpreted.

The Type field determines how the value must be interpreted. The main DNS record types are:

Type	Interpretation of Value
A	A 32-bit IPv4 address
NS	Identifies the authoritative servers for a zone
CNAME	Defines an alias for the official name of a host
SOA	Marks the beginning of a zone
MX	Redirects mail to a mail server
AAAA	An IPv6 address

