July 2026-October 2026 REGULAR EXAMINATIONS
B.E/B.Tech
CSE,AIADS,IT,CSD, CSBS, AIML, CSE(CS)
III SEM R2023V1.2

COURSE CODE	COURSE TITLE
2321CSC301T	COMPUTER NETWORKS

CO1 Explain the architecture, devices, and protocols of computer networks.

CO2 Configure and analyze high-performance switching and routing techniques.

CO3 Compare transport layer protocols and implement congestion control strategies.

CO4 Apply network security measures to protect against various threats.

CO5 Analyze emerging technologies like IoT, 5G, and cloud networking and their applications in modern communication systems.

K1 – Remember K2 – Understand K3 – Apply K4 – Analyse K5 – Evaluate K6 – Create

Unit – I

Part A

Q.No	Questions	CO's	Unit	Bloom's Level
1.	How a computer network functions by identifying its core components (nodes and links) and illustrating how they interact to facilitate data exchange.	CO1	1A	K1
1 Ans	A computer network is a collection of interconnected devices that can communicate and share resources. The two primary building blocks are the Network Edge and the Network Core.	CO1	1A	K1
2.	How does a router explain or manage the movement of data packets between different networks like a local network and the internet?	CO1	1A	K1
2 Ans	The function of a router is to forward data packets between different computer networks, determining the best path for the data to travel from its source to its destination.	CO1	1A	K1
3.	Classify the division of responsibilities in a layered model and summarize how each tier communicates with its corresponding peer on a remote system	CO1	1A	K2

3 Ans	Layering is a design approach that divides the complex functionality of a network into a vertical stack of independent layers. Each layer is responsible for a specific task and provides services to the layer above it, while using the services of the layer below it. This modularity simplifies design, development, and troubleshooting.	CO1	1A	K2
4.	How many layers does the OSI Reference Model have, and describe about the topmost layer function.	CO1	1A	K1
4 Ans	The Application Layer serves as the direct interface between end-user software applications and the underlying network. Service Identification: It determines the identity and availability of communication partners for a specific data transfer. Resource Assessment: It verifies whether sufficient network resources exist to establish the requested connection.	CO1	1A	K1
5.	Discriminate between a switch and a gateway based on their primary roles in a network.	CO1	1A	K1
5 Ans	A switch is a device that connects devices within the same network (a Local Area Network), forwarding data based on MAC addresses. A gateway is a device that connects two different networks that may use different protocols, translating data between them to enable communication.	CO1	1A	K1
6.	Difference between a physical link and a transmission medium? Provide an example of each.	CO1	1A	K1
6 Ans	A physical link is the logical connection between two network devices, while the transmission medium is the physical material or channel through which the signal travels. Example of a physical link: A connection established between two routers. Example of a transmission medium: An optical fiber cable, or a wireless radio frequency.	CO1	1A	K1
7.	State the role of a modem? Why is it necessary when connecting to an Internet Service Provider (ISP)?	CO1	1A	K1
7 Ans	A modem (Modulator-Demodulator) converts digital signals from a computer into analog signals for transmission over traditional analog mediums like telephone lines, and vice-versa. It is necessary to convert the digital data from the network to a form that can be transmitted over the physical medium provided by the ISP.	CO1	1A	K1
8.	Describe "Network Topology" and provide an example.	CO1	1A	K1
8 Ans	Network topology refers to the physical or logical arrangement of devices and connections in a network. It defines how network nodes are linked together. An example is a Star topology, where all devices are connected to a central hub or switch.	CO1	1A	K1
9.	State the primary purpose of the "Network Edge" in the "Building a Network" concept?	CO1	1A	K1

9 Ans	The Network Edge refers to the part of the network where end devices (like computers, smartphones, and servers) are located. It serves as the entry and exit point for data into the network core.	CO1	1A	K1
10.	Brief the concept of "Signal Encoding Techniques." Why are they important for physical layer communication?	CO1	1A	K1
10 Ans	Signal encoding techniques are methods used to convert digital data into a form that can be transmitted as a physical signal (e.g., electrical voltage, light pulses, or radio waves) over a transmission medium. They are crucial because they define how the 1s and 0s of data are represented on the medium, ensuring reliable and accurate transmission by managing issues like synchronization and error detection.	CO1	1A	K1
11.	You are setting up a small office network and have one cable modem from your ISP. You need to connect 4 computers to the internet and allow them to share files locally. Which essential networking devices would you need, and what would be their primary roles?	CO1	1A	K2
11 Ans	You would need a router and a switch. The router would connect to the cable modem to share the internet connection with all devices and manage network traffic. The switch would allow all 4 computers to be physically connected to the local network and communicate with each other.	CO1	1A	K2
12.	A company's internal network uses a physical Star topology. What happens to the entire network if the central switch in this topology fails? Justify your answer.	CO1	1A	K2
12 Ans	The entire network would go down. In a Star topology, all devices are directly connected to the central switch, which acts as the central point of communication. If the switch fails, none of the connected devices can communicate with each other or access the network.	CO1	1A	K2
13.	Imagine you need to build a very simple, low-cost "network" between two devices using only their audio jacks and a standard 3.5mm audio cable. Which fundamental networking concept from transmission medium would you be applying at the physical level, and what would be the main challenge?	CO1	1A	K2
13 Ans	You would be applying the concept of Physical Links and Transmission Media. The main challenge would be Signal Encoding, as you would need to devise a custom way to encode digital data into audio tones (like a modem) to transmit information over the audio cable.	CO1	1A	K2
14.	A new standard for flexible displays allows network cables to be printed on the surface of a wall. Accordingly, what are two categories of network "devices" this technology would replace, and what specific function would it still be performing?	CO1	1A	K2

14 Ans	This technology would replace the physical transmission media (like copper or fiber optic cables). It would also potentially eliminate the need for physical connectors. The function it would still be performing is to provide the physical links between devices for data transmission.	CO1	1A	K2
15.	An engineer is troubleshooting a network and says, "The physical layer is working fine, but the communication is failing." What does this statement imply about the state of the physical connections and the higher-layer protocols?	CO1	1A	K2
15 Ans	This statement implies that the physical connections (cables, wireless signals) and the hardware on the physical layer are functioning correctly (e.g., there is a connection). The problem must therefore lie within one of the higher layers (like the Data Link or Network layers), meaning there is an issue with the protocol logic, addressing, or data formatting for the communication to be successful.	CO1	1A	K2

Part- B

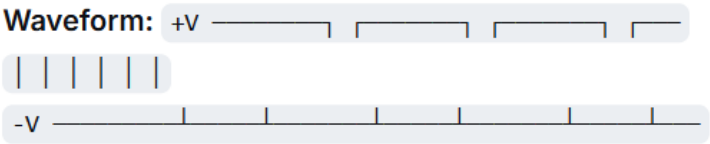
Q.No	Questions	CO's	Unit	Bloom's Level
1.	You are the network admin for a startup with 15 desktops and 5 printers. You have one fiber optic modem from the ISP. Due to budget constraints, you must choose between: A single large switch, OR A single router with a built-in 16-port switch. Which device would you choose and why? Justify your choice by explaining the role each device would play in this setup.	CO1	1B	K3
1 Ans	Choose the router with a built-in 16-port switch. — The router is essential because it connects the local network to the ISP's fiber modem and provides features like Network Address Translation (NAT) to share the single public IP address among all 15 computers and 5 printers. Its built-in switch allows all these local devices to be physically connected and communicate with each other within the office network. A single switch alone would not be able to connect to the internet, as it cannot perform routing or NAT functions. (Award 5 mark for identifying the correct device + 8 mark for correct justification).	CO1	1B	K3
2.	You need to connect two LANs in separate buildings located 200 meters apart into a single network. Available Mediums i)Cat5e Copper: Max distance 100 meters. ii)Single-mode Fiber: Long-distance optical cable. iii)Microwave Link: High-speed wireless connection. Which transmission medium would you select and why? What	CO1	1B	K3

	networking device would you place at each end to connect the buildings?			
2 Ans	Choose Single-mode fiber optic cable. Reason 1: At 200 meters, Cat5e is unsuitable because its effective distance limit is only 100 meters. Reason 2: Fiber optic cable provides high bandwidth, is immune to electromagnetic interference over long distances, and is more secure than a microwave link. Device: A Media Converter or a Switch with SFP (Small Form-factor Pluggable) fiber ports would be placed at each end to convert electrical signals from the internal LAN to optical signals for transmission. (Award 6 mark for identifying fiber + 7 mark for device and reasoning against Cat5e).	CO1	1B	K3
3.	You are tasked with building a wireless network in a large, open-plan warehouse where radio signals from traditional Wi-Fi access points are heavily absorbed by tall metal shelving units. As a network engineer, suggest an innovative approach to overcome this signal absorption problem. Which physical layer concept would you be modifying to solve this?	CO1	1B	K3
3 Ans	Instead of using a single high-power Wi-Fi access point, deploy a mesh network of multiple low-power access points placed on the shelves or ceiling, ensuring each point has a clear "line of sight" to at least one other point. Alternatively, use powerline networking adapters that transmit data over the existing electrical wiring within the warehouse. (Award 6 mark for a plausible innovative solution + 7 mark for The concept being modified is Transmission Media and Signal Encoding. By changing the physical medium (from air/radio waves to electrical wiring) or changing the signal propagation path (by using multiple smaller signals instead of one large one), you are innovating at the physical layer to ensure reliable signal transmission.	CO1	1B	K3

<table>
<tr><td></td><td>identifying the correct concept).</td><td></td><td></td><td></td></tr>
<tr><td>4.</td><td>A network is built using a physical Star Topology with a central switch. The network team decides to save costs by using a very cheap, unmanaged switch as the central hub. Over time, the switch's internal processor fails to handle a sudden surge in data, causing it to drop data packets randomly.
Examine the impact of this failure on the entire network. Compare this scenario to what would happen if the same failure occurred on a Ring Topology.</td><td>CO1</td><td>1B</td><td>K3</td></tr>
<tr><td>4
Ans</td><td><table><tr><td>Impact on Star Topology</td><td>Impact on Ring Topology</td></tr><tr><td>Partial/Total Isolation: Since the switch is the central point of connection, if it starts dropping packets, all devices connected to it will experience severe performance degradation and intermittent connectivity. Some devices may be completely unable to communicate. The failure is centralized, and the entire network's performance is dependent on this single device.</td><td>Complete Network Shutdown:
In a Ring Topology, if the central device (or the ring interface) fails, the ring is broken. Data travels in a loop, and if one point fails, the entire network becomes completely nonfunctional until the device is replaced or bypassed. (Award 6 mark for analyzing the Star impact + 7 mark for comparing/analyzing the Ring impact).</td></tr></table></td><td>CO1</td><td>1B</td><td>K3</td></tr>
<tr><td>5.</td><td>A network admin finds that signals from Device A, reach Device B with zero bit errors, yet Device B can't interpret the data.
Analyze this situation and deduce which layer of the OSI model (Physical, Data Link, or Network) is most likely causing the failure. Justify your answer.</td><td>CO1</td><td>1B</td><td>K4</td></tr>
<tr><td>5
Ans</td><td>The Data Link Layer (Layer 2) is the most likely cause of this communication failure.
1. Rule Out the Physical Layer The protocol analyzer confirms that the physical signal is transmitted with zero bit errors. This</td><td>CO1</td><td>1B</td><td>K4</td></tr>
</table>

	proves that the Physical Layer (Layer 1) is operating perfectly, as cables, connectors, and electrical/optical signals are intact. 2. Identify the Data Link Layer Mismatch Because the raw bits arrive safely; the failure happens when Device B tries to group those bits into meaningful data. The Data Link Layer (Layer 2) is responsible for framing, addressing, and media access control. If Device B cannot interpret the data, it is usually due to Layer 2 mismatches such as: Mismatched Framing: Device A might be using a framing protocol (like HDLC or PPP) that Device B does not support or expect. Encapsulation Types: A misconfiguration in encapsulation prevents Device B from finding the start and end of a data frame. Invalid MAC Addressing: Device B may be dropping the frames immediately if the destination MAC address does not match its own or an allowed broadcast/multicast address. (6 Marks) 3. Rule Out the Network Layer the Network Layer (Layer 3) handles routing and IP addressing. However, a device cannot process Layer 3 IP packets until the Layer 2 Data Link frame is successfully de-encapsulated (opened). Because Device B fails to understand the basic structure of the incoming data stream, the error stops the communication flow before it ever reaches the Network Layer. (7 Marks)			
6.	Compare the five-layer Internet Architecture and the seven-layer OSI model. A new app protocol runs directly atop the Transport Layer. Where does it sit in OSI? Also, how do OSI's extra Presentation and Session layers offer advantages over the Internet model for this protocol?	CO1	1B	K4
6 Ans	Where the New Protocol Fits in the OSI Model Since the new application protocol runs directly on top of the Transport Layer (e.g., TCP or UDP), it occupies the Application Layer (Layer 7) of the OSI model. In the OSI model, the upper three layers—Application (L7), Presentation (L6), and Session (L5)—are collectively responsible for network services to end-user applications. By running directly on top of Transport, this new protocol bypasses the dedicated Presentation and Session layers, meaning it must handle their responsibilities internally (if needed) or simply not use them. (4 Marks) Advantages of OSI's Extra Layers for This Protocol (4 Marks) The Internet Architecture (TCP/IP model) combines Application, Presentation, and Session into a single Application Layer. For a new protocol that sits directly on Transport, OSI's separation offers three key advantages that the Internet model.	CO1	1B	K4

<table>
<tr>
<td></td>
<td>
Summary Comparison
<table>
<tr><td>Aspect</td><td>Internet Architecture (5-Layer)</td><td>OSI Model (7-Layer)</td></tr>
<tr><td>Placement of new protocol</td><td>Application Layer (combined)</td><td>Application Layer (L7) – but can delegate downward</td></tr>
<tr><td>Data formatting/encryption</td><td>Must be built into the protocol itself</td><td>Offloaded to Presentation Layer (L6)</td></tr>
<tr><td>Session control & recovery</td><td>Must be manually coded by the developer</td><td>Offloaded to Session Layer (L5)</td></tr>
<tr><td>Modularity</td><td>Tighter coupling; changes affect the whole stack</td><td>Looser coupling; each layer can evolve independently</td></tr>
</table>
</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>
You need to transmit the following 8-bit data stream from a sensor to a central control room: Data Stream: 1 0 1 1 0 0 1 0
The transmission distance is 500 meters over a copper cable. You must choose an appropriate signal encoding technique for reliable data transmission. Encode the given data stream, using the following three encoding schemes. Show the resulting signal waveforms clearly for each:
<ul>
<li>NRZ (Non-Return-to-Zero)</li>
<li>NRZ-I (Non-Return-to-Zero Inverted)</li>
<li>Manchester Coding</li>
</ul>
Assume:
For NRZ: Positive voltage (+V) = 1, Negative voltage (-V) = 0
For NRZ-I: Transition at the beginning of a bit period = 1, No transition = 0. Initial state is Positive (+V).
For Manchester: Transition in the middle of bit period. Low-to-High = 1, High-to-Low = 0.
</td>
<td>CO1</td>
<td>1B</td>
<td>K4</td>
</tr>
</table>

<table>
<tr>
<td>7
Ans</td>
<td>
Given Data: 1 0 1 1 0 0 1 0
1. NRZ Encoding: (4 marks Each + 1 marks for plots)
+V for 1, -V for 0
<table>
<tr><td>Bit</td><td>1</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>0</td></tr>
<tr><td>NRZ Signal</td><td>+V</td><td>-V</td><td>+V</td><td>+V</td><td>-V</td><td>-V</td><td>+V</td><td>-V</td></tr>
</table>


NRZ-I Encoding:
Transition at start = 1, No transition = 0. Initial state = +V.
<table>
<tr><td>Bit</td><td>1</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>0</td></tr>
<tr><td>Transition?</td><td>Yes</td><td>No</td><td>Yes</td><td>Yes</td><td>No</td><td>No</td><td>Yes</td><td>No</td></tr>
<tr><td>Signal Level</td><td>-V</td><td>-V</td><td>+V</td><td>-V</td><td>-V</td><td>-V</td><td>+V</td><td>+V</td></tr>
</table>
Manchester Encoding:
Low-to-High (↑) = 1, High-to-Low (↓) = 0. Transition in middle of each bit.
<table>
<tr><td>Bit</td><td>1</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>0</td></tr>
<tr><td>Signal Pattern</td><td>↑</td><td>↓</td><td>↑</td><td>↑</td><td>↓</td><td>↓</td><td>↑</td><td>↓</td></tr>
</table>
</td>
<td>CO1</td>
<td>1B</td>
<td>K4</td>
</tr>
<tr>
<td>8.</td>
<td>A large organization is planning to expand. They are choosing between two network architectures:
Architecture A: A flat network with a single, large subnet and a single router connecting to the internet.
Architecture B: A hierarchical network with multiple smaller subnets, each connected by a separate router that communicates with a core router.
Analyze and compare these two architectures in terms of fault tolerance (what happens if one router fails?) and traffic management (how is congestion handled?).</td>
<td>CO1</td>
<td>1B</td>
<td>K4</td>
</tr>
</table>

<table>
<tr>
<td>8
Ans</td>
<td>Scenario Explanation – 5 Marks with Architecture type.
Justification - 8 Marks
<table>
<tr><th>Criteria</th><th>Architecture A
(Flat)</th><th>Architecture B
(Hierarchical)</th></tr>
<tr><td>Fault Tolerance</td><td>High Risk:
If the single router fails, the entire organization loses internet connectivity and internal communication. This is a single point of failure.</td><td>High Resilience:
If one department's router fails, only that specific subnet is affected. The rest of the organization continues to function normally.</td></tr>
<tr><td>Traffic Management</td><td>Poor:
All broadcast traffic and data packets are sent across the entire network, leading to high congestion, collisions, and unnecessary bandwidth consumption.</td><td>Excellent:
Traffic is contained within each subnet. Routers and switches can use layering to forward packets intelligently only to the subnet where the destination resides, significantly reducing congestion.</td></tr>
</table></td>
<td>CO1</td>
<td>1B</td>
<td>K4</td>
</tr>
</table>

Part C

Q.No	Questions	CO's	Unit	Bloom's Level
1.	Your campus has 5 buildings with 200 PCs each, connected via unmanaged switches and a single router. Propose a hierarchical design using network components, explaining which OSI layer each device operates at, Compare your hierarchical design against the existing flat network in terms of broadcast traffic, collision domains, and latency.	CO1	1C	K5

<table>
<tr>
<td>1
Ans</td>
<td>Proposed Hierarchical Design Using Network Components
The proposed hierarchical design follows the Three-Tier Hierarchical Model (Core, Distribution, Access layers), which is standard for campus networks.

• Components and Their OSI Layers (4Marks)
• Comparison: Hierarchical Design vs. Flat Network - (4Marks)
• Additional Analysis: Advantages of Hierarchical Design - (4Marks)

Comparison Table (Summary) - (3 Marks)
<table>
<tr><td>Criteria</td><td>Flat Network</td><td>Hierarchical Design</td><td>Winner</td></tr>
<tr><td>Broadcast Traffic</td><td>High (single broadcast domain)</td><td>Low (segmented into VLANs)</td><td>Hierarchical</td></tr>
<tr><td>Collision Domains</td><td>Limited by single uplink/ router</td><td>Multiple, distributed</td><td>Hierarchical</td></tr>
<tr><td>Latency</td><td>High, variable, bottlenecked</td><td>Low, predictable</td><td>Hierarchical</td></tr>
</table>
</td>
<td>CO1</td>
<td>1C</td>
<td>K5</td>
</tr>
<tr>
<td>2.</td>
<td>Zones are connecting directly to the central Data Center. Zone A and C use fiber; Zone B uses microwave; Zone D uses LoRa gateway connecting to Data Center. Based on your selected transmission media (Guided/Unguided),
Analyze the overall physical topology connecting all zones to the Data Center (describe with a diagram). Evaluate its fault tolerance by identifying single points of failure and their impact, and assess its scalability for future expansion. If the city adds 5 new zones in the future, how easily can they be integrated? Justify.</td>
<td>CO1</td>
<td>1C</td>
<td>K5</td>
</tr>
</table>

2 Ans	Physical Topology Analysis - (4Marks) The network uses a Physical Star Topology. The central Data Center serves as the central hub, and each individual zone connects directly to it as a separate spoke. Fault Tolerance Evaluation - (4Marks) Single Points of Failure (SPOF)The Central Data Center: If the central Data Center goes offline (due to a power outage, hardware crash, or fire), all zones lose connectivity instantly. Communication across the entire network completely collapses. Individual Spoke Links: Because each zone relies on a single, non-redundant path to the center, any link failure cuts off that specific zone completely. (4Marks) Scalability and Future Expansion Integration of 5 New Zones - (3Marks) Adding 5 new zones to this network is highly scalable and easy to implement due to the nature of a star topology.	CO1	1C	K5

Unit- 2

Part A

Q.No	Questions	CO's	Unit	Bloom's Level
1.	How do VLANs resolve broadcast and security issues in a flat network with 3 departments and 300 users? Also, how do VLANs boost performance?	CO2	2A	K1
1 Ans	Create separate VLANs for Finance (VLAN 10), HR (VLAN 20), and Engineering (VLAN 30). Broadcasts from one VLAN are not forwarded to other VLANs. Inter-VLAN communication requires routing through a Layer 3 device	CO2	2A	K1
2.	For a single inter-switch link carrying VLANs 10, 20, and 30, describe the setup, the required IEEE standard, and the reason it's essential.	CO2	2A	K2
2 Ans	Configure the link as a VLAN Trunk using IEEE 802.1Q standard. Without trunking, each VLAN would require a separate physical cable between the switches, which is not scalable.	CO2	2A	K2
3.	Why does OSPF performance degrade in a large single-area network with 600 routers? How do multiple OSPF areas improve convergence?	CO2	2A	K1
3 Ans	In a single OSPF area, every router maintains a complete Link-State Database (LSDB) of the entire network. Any topology change triggers an LSA flood to all routers, forcing every router to recomputed its SPF (Shortest Path First) tree. This causes high CPU usage and slow convergence.	CO2	2A	K1

4.	An organization has a single public IP address provided by the ISP, offer internets for 200 devices. how NAT enables multiple devices to share a single public IP address. For this process state the role of NAT router?	CO2	2A	K2
4 Ans	NAT allows multiple private IP addresses (e.g., 192.168.1.x) to be translated to a single public IP address when accessing the internet. When a device sends a packet to the internet, the router replaces the private source IP with its public IP and assigns a unique port number	CO2	2A	K2
5.	State the concept of CIDR. How is it an innovative improvement over classful addressing?	CO2	2A	K1
5 Ans	CIDR eliminates fixed class boundaries (Class A, B, C) and uses variable-length subnet masks (VLSM). Addresses are represented as prefix lengths (e.g., /24, /25, /26).	CO2	2A	K1
6.	An organization has been allocated the IP block 200.10.0.0/24. It has 4 departments and with the 50,30,20 and 10 host requirements respectively: Is it possible to allocate subnets using classful addressing and how CIDR is necessary for this scenario.	CO2	2A	K2
6 Ans	Yes, it is possible to allocate these subnets using equal-sized classful subnetting (Fixed-Length Subnet Masking), but CIDR/VLSM is necessary to prevent severe IP address waste and to allow for future network growth. (CIDR) introduces Variable Length Subnet Masking (VLSM), allowing you to customize the subnet sizes to fit each department perfectly.	CO2	2A	K2
7.	Explain the term "subnet mask" in the context of classless addressing. How does it help in identifying the network portion of an IP address?	CO2	2A	K1
7 Ans	A subnet mask is a 32-bit number that separates an IP address into network portion and host portion. In CIDR notation, it is represented as a prefix length (e.g., /24 means 255.255.255.0).	CO2	2A	K1
8.	Your boss, who once said “subnetting is just fancy math,” has given you the IP block 172.16.0.0/20 and demanded 8 equal subnets. He doesn't care about your feelings. He wants the new subnet mask and the number of usable hosts per subnet. Show your calculations before he asks you to explain it in IPv6.	CO2	2A	K2

<table>
<tr><td>8 Ans</td><td>Original prefix: /20 (16,384 total addresses)

Need 8 subnets → $2^3 = 8$ → borrow 3 bits

New prefix: /20 + 3 = /23

New Mask: 255.255.254.0

Host bits: 32 - 23 = 9

Usable hosts: $2^9 - 2 = 510$</td><td>CO2</td><td>2A</td><td>K2</td></tr>
<tr><td>9.</td><td>Distinguish between NAT (Network Address Translation) and CIDR. How do they complement each other in IPv4 networks?</td><td>CO2</td><td>2A</td><td>K1</td></tr>
<tr><td>9 Ans</td><td><table>
<tr><th>NAT</th><th>CIDR</th></tr>
<tr><td>NAT translates private IP addresses to public IP addresses, allowing multiple devices to share a single public IP.</td><td>CIDR efficiently allocates and aggregates IP address space, conserving IPv4 addresses.</td></tr>
<tr><td colspan="2">CIDR conserves public IP addresses by efficient allocation and route aggregation.

NAT conserves public IP addresses by allowing private addressing internally.</td></tr>
</table></td><td>CO2</td><td>2A</td><td>K1</td></tr>
<tr><td>10.</td><td>Your network uses private IP addresses in the range 192.168.10.0/24. You need to connect to the internet through a single public IP provided by your ISP. Explain the role of NAT in this scenario. What are the limitations of using NAT?</td><td>CO2</td><td>2A</td><td>K2</td></tr>
<tr><td>10 Ans</td><td>NAT translates private IP addresses (192.168.10.x) to the single public IP address when devices access the internet. It maintains a NAT table mapping internal addresses to port numbers (PAT) for return traffic.
Limitations:
1. Breaks End-to-End Connectivity: Some applications (e.g., peer-to-peer, VoIP) require direct public IP addresses.
2. Processing Overhead: NAT adds latency due to translation.</td><td>CO2</td><td>2A</td><td>K2</td></tr>
<tr><td>11.</td><td>A company has two offices in different cities. Each office uses OSPF internally. They want to connect both offices to the internet and to each other. How BGP is used between the two offices rather than extending OSPF across both locations.</td><td>CO2</td><td>2A</td><td>K2</td></tr>
<tr><td>11 Ans</td><td>Border Gateway Protocol (BGP) is used to connect the two offices because it is designed to route traffic between independent networks (Autonomous Systems), whereas OSPF is only built to handle routing inside a single</td><td>CO2</td><td>2A</td><td>K2</td></tr>
</table>

<table>
<tr><td></td><td>network. Extending OSPF across different cities over the internet causes major performance and stability issues.</td><td></td><td></td><td></td></tr>
<tr><td>12.</td><td>IPv4 addresses are running out globally. IPv6 was introduced as a long-term solution. Compare IPv4 and IPv6 in terms of address space and built-in security features.</td><td>CO2</td><td>2A</td><td>K1</td></tr>
<tr><td>12 Ans</td><td>The depletion of IPv4 addresses made the transition to IPv6 essential. The core differences between the two protocols lie in their scaling capacity and core security architectures.
<table>
<tr><th>IPv4</th><th>IPv6</th></tr>
<tr><td>Address Space
IPv4 Limit: Uses a 32-bit address format, capping the maximum number of unique addresses at 4.3 billion (2^{32})</td><td>IPv6 Capacity: Expands to a 128-bit hexadecimal format, yielding 340 undecillion unique addresses (2^{128}).</td></tr>
<tr><td>Built-In Security Features
IPv4 Security: Designed without native security; relies entirely on add-on protocols like IPsec or SSL/TLS configured at the application or network level.</td><td>IPv6 Security: Built with IPsec support mandated in its base specification, meaning encryption and cryptographic identity verification are natively engineered into the protocol.</td></tr>
</table></td><td>CO2</td><td>2A</td><td>K1</td></tr>
<tr><td>13.</td><td>By Configuring a switch and need to separate traffic from different departments. You decide to use VLANs. State the difference between an Access Port and a Trunk Port on a switch as per scenario.</td><td>CO2</td><td>2A</td><td>K1</td></tr>
<tr><td>13 Ans</td><td>In your scenario, Access Ports connect the individual devices within a department to the switch, while Trunk Ports carry traffic for all departments simultaneously between switches.
Access Port -Single Membership: An access port belongs to exactly one VLAN (e.g., Port 1 is assigned only to the HR department's VLAN).
Trunk Port - Multiple Memberships: A trunk port carries traffic for multiple VLANs at the same time across a single physical link.</td><td>CO2</td><td>2A</td><td>K1</td></tr>
<tr><td>14.</td><td>An organization is using a single router as the default gateway for all VLANs. The router is becoming overloaded, causing high latency. Explain how using a Layer 3 switch for inter-VLAN routing is a better alternative.</td><td>CO2</td><td>2A</td><td>K1</td></tr>
<tr><td>14 Ans</td><td>Using a Layer 3 switch for inter-VLAN routing is a better alternative because it moves the traffic-routing job from a single software-based router to dedicated, high-speed hardware chips inside the switch itself. This eliminates the bottleneck and dramatically lowers latency. Better</td><td>CO2</td><td>2A</td><td>K1</td></tr>
</table>

	alternative: Layer 3 switches use specialized chips called ASICs (Application-Specific Integrated Circuits) to route packets at the hardware layer, delivering near-zero latency ("wire-speed" routing).			
15.	A network administrator is using Wireshark to troubleshoot a network issue. The administrator captures packets and examines the headers. how protocol stack analysis with Wireshark helps in troubleshooting.	CO2	2A	K2
15 Ans	Protocol stack analysis with Wireshark helps in troubleshooting by breaking down a captured packet into its individual layers (from the physical wire up to the application), allowing you to pinpoint the exact level where a communication breakdown occurs.	CO2	2A	K2

Part- B

<table>
<tr><th>Q.No</th><th>Questions</th><th>CO’s</th><th>Unit</th><th>Bloom’s Level</th></tr>
<tr><td>1.</td><td>The founder of Ctrl+Alt+Del Technologies, Mr. Neesamani, believes every IT problem can be solved by restarting the router. After hearing "IPv6 is the future," he wants an instant migration. The current 5,000-device network isn't so optimistic. Explain NAT with PAT, Illustrate an IPv6 addressing plan using 2001:db8:abcd::/48, and propose a phased dual-stack migration that avoids turning “Monday morning” into a network apocalypse.</td><td>CO2</td><td>2B</td><td>K4</td></tr>
<tr><td>1 Ans</td><td>NAT with PAT Explanation (4 Marks)
<table>
<tr><th>NAT with PAT</th><th>Explanation</th></tr>
<tr><td>NAT (Network Address Translation)</td><td>Translates private IP addresses (e.g., 10.x.x.x) to the single public IP address when devices access the internet.</td></tr>
<tr><td>PAT (Port Address Translation)</td><td>Uses unique source port numbers to distinguish between multiple internal devices sharing the same public IP.</td></tr>
<tr><td>NAT Table</td><td>Maintains a mapping of (private IP:port) ↔ (public IP:port) for return traffic.</td></tr>
</table>
Example:
Device A (10.0.0.10:12345) → NAT router translates to (203.0.113.5:50001)
Device B (10.0.0.20:12345) → NAT router translates to (203.0.113.5:50002)
When response arrives, router uses the NAT table to forward to the correct device.
IPv6 Addressing Plan (4 Marks)
IPv6 Design Allocation</td><td>CO2</td><td>2B</td><td>K4</td></tr>
</table>

<table>
<tr>
<td></td>
<td>ISP Prefix: 2001:db8: abcd::/48 Provides 2^{16} = 65,536 subnets (each /64)
Subnet Allocation:
Office 1: 2001:db8: abcd:0001::/64
Office 2: 2001:db8: abcd:0002: :/64
Office 3: 2001:db8: abcd:0003: :/64
Future Expansion: 2001:db8: abcd:0004: :/64 to FFFF: :/64
Phased Dual-Stack Migration Strategy - (5 Marks)
<table>
<tr><th>Phase</th><th>Description</th><th>Duration</th></tr>
<tr><td>Phase 1: Assessment & Planning</td><td>Audit all devices for IPv6 compatibility. Upgrade network infrastructure (routers, switches, firewalls) to support IPv6. Train IT staff.</td><td>Month 1-2</td></tr>
<tr><td>Phase 2: Dual-Stack Deployment</td><td>Enable IPv6 on all network devices alongside IPv4. Configure IPv6 on routers and switches. Deploy IPv6 DNS (AAAA records). Ensure all servers support IPv6.</td><td>Month 3-6</td></tr>
<tr><td>Phase 3: Service Migration</td><td>Migrate critical services (web servers, email, VPN) to IPv6. Test all applications in dual-stack mode. Gradually move internal clients to IPv6. Use IPv6 for new devices.</td><td>Month 7-12</td></tr>
</table>
Why Dual-Stack Avoids a "Network Apocalypse":
Zero Downtime: IPv4 continues to work while IPv6 is gradually introduced.
Incremental Rollout: Issues can be identified and fixed without affecting all users.
Fallback Option: If IPv6 fails, IPv4 is still available.</td>
<td></td><td></td><td></td>
</tr>
<tr>
<td>2.</td>
<td>Welcome to the University! Five buildings with 200 computers each use unmanaged switches and a single router. Broadcast traffic spreads like campus gossip, one router failure shuts down the campus, and troubleshooting is a nightmare. As the new Network Superhero like you, Sketch a three-tier hierarchical network, identify the devices and their OSI layers, and explain how VLANs can reduce broadcast traffic and improve network performance and reliability.</td>
<td>CO2</td><td>2B</td><td>K3</td>
</tr>
<tr>
<td>2
Ans</td>
<td>The Three-Tier Network Design & OSI Device (4 Marks)
will divide the university network into three distinct layers to organize traffic efficiently.
[Core Layer] <-- High-Speed Routing Backbone |
[Distribution Layer] <-- VLAN Routing & Security Policies |
[Access Layer] <-- End-Device Connectivity (Buildings)</td>
<td>CO2</td><td>2B</td><td>K3</td>
</tr>
</table>

<table>
<tr><td></td><td>Access Layer (The Building Entrances)
The Mission: Connects the 1,000 end-user computers directly to the network.
Distribution Layer (The Neighborhood Hubs)
The Mission: Aggregates all the cables coming from the buildings, enforces security policies, and routes traffic between different departments.
Core Layer (The Campus Highway)
The Mission: Shuffles massive amounts of data between the distribution hubs and the outside internet at lightning speed. It does no policy checking or packet filtering.
2. Taming the Campus Gossip with VLANs (4 Marks)
Virtual Local Area Networks (VLANs) completely change how the network performs and survives.
Boosting Performance Because routers and Layer 3 switches stop broadcasts at the VLAN boundary, CPU cycles on student and staff computers are no longer wasted processing random background network noise.
Injecting Rock-Solid Reliability Fault Isolation: If a computer in Building C catches a virus or causes a broadcast storm, the damage is completely contained inside that specific VLAN. The other four buildings continue running perfectly. (5 Marks)</td><td></td><td></td><td></td></tr>
<tr><td>3.</td><td>The hospital has 500 networked devices, including life-saving patient monitors, email, and administrative systems, all sharing the same network with no traffic prioritization. During peak hours, critical medical data is delayed by regular traffic. As the Network Lifesaver, design a VLAN structure to separate critical and non-critical traffic, explain how RED manages congestion, and analyze how VLANs, QoS, and RED work together to ensure low latency and priority for life-critical communications.</td><td>CO2</td><td>2B</td><td>K4</td></tr>
<tr><td>3
Ans</td><td>Design a VLAN Structure (4 Marks)
To separate critical and non-critical traffic, the hospital network can be divided into multiple VLANs.
<table>
<tr><th>VLAN ID</th><th>Department/Devices</th><th>Purpose</th></tr>
<tr><td>VLAN 10</td><td>Patient Monitoring Devices</td><td>Critical medical traffic</td></tr>
<tr><td>VLAN 20</td><td>Doctors and Nurses</td><td>Access to patient records</td></tr>
<tr><td>VLAN 30</td><td>Administrative Staff</td><td>Email, billing, HR</td></tr>
<tr><td>VLAN 40</td><td>Guest Wi-Fi</td><td>Internet access for visitors</td></tr>
<tr><td>VLAN 50</td><td>Servers & Data Center</td><td>Hospital applications and databases</td></tr>
</table>
RED (Random Early Detection) for Queue Management (4 M)
RED is a congestion avoidance mechanism used in routers and Layer 3 switches.</td><td>CO2</td><td>2B</td><td>K4</td></tr>
</table>

	Working The router continuously monitors the average queue length. When the queue begins filling, RED randomly drops or marks some packets before the buffer becomes full. TCP sources detect packet loss and reduce their transmission rate. Congestion is relieved before the queue overflows. Advantages Prevents buffer overflow. Reduces packet loss. Avoids global TCP synchronization. Maintains smoother network performance. How VLANs + QoS + RED Ensure Low Latency (5 Mark) VLANs Separate critical patient-monitoring devices from normal office traffic. Reduce unnecessary broadcasts. Improve security and network efficiency. QoS (Quality of Service) QoS classifies and prioritizes traffic. Example priority: Patient monitoring devices (Highest Priority) Voice/Video communication Hospital applications Email Web browsing (Lowest Priority) QoS ensures that life-critical packets are transmitted before less important traffic. RED RED detects congestion early by randomly dropping lower-priority packets before queues become full. This prevents excessive delays and allows high-priority traffic to continue flowing efficiently.			
4.	Your boss believes one public IP can serve 500 employees forever—just like one pizza can feed the whole office! Explain how NAT with PAT performs this networking magic, compare NAT and CIDR, and analyze the problems and possible solutions when the magic starts wearing off.	CO2	2B	K3
4 Ans	How does NAT with PAT perform the networking magic? Network Address Translation (NAT) allows devices with private IP addresses (e.g., 192.168.10.0/24) to communicate with the Internet using a public IP address. (4 Marks) Port Address Translation (PAT), also called NAT Overload, extends NAT by allowing multiple devices to share a single public IP address. It distinguishes each connection using unique port numbers. (4 Marks) **Feature** | **NAT** | **CIDR**	CO2	2B	K3

<table>
<tr><td></td><td>
<table>
<tr><td>Full Form</td><td>Network Address Translation</td><td>Classless Inter-Domain Routing</td></tr>
<tr><td>Purpose</td><td>Conserves public IP addresses by sharing them</td><td>Conserves IP addresses through efficient allocation</td></tr>
<tr><td>Works At</td><td>Network gateway/router</td><td>IP addressing and routing</td></tr>
<tr><td>Uses Private IPs?</td><td>Yes</td><td>No</td></tr>
<tr><td>Reduces Public IP Usage?</td><td>Yes</td><td>Indirectly</td></tr>
</table>
Problems when the magic starts wearing off
As the company grows from 200 to 500 devices, one public IP can still work, but several challenges arise. (5 Ma)
Large NAT Table
More devices create more active sessions.
The router must maintain a larger translation table.
Requires more CPU and memory.
</td><td></td><td></td><td></td></tr>
<tr><td>5.</td><td>An ISP inherited eight consecutive /24 networks (192.168.0.0/24–192.168.7.0/24), and the routers are complaining about carrying too many routes. The network engineer wants "one route to rule them all." Estimate the summarized (supernet) route, explain how CIDR route aggregation works, and analyze how it reduces routing table size and improves router performance.</td><td>CO2</td><td>2B</td><td>K4</td></tr>
<tr><td>5
Ans</td><td>These eight consecutive /24 networks share the first 21 bits.
Supernet Route: (4 Marks)
192.168.0.0/21
How CIDR Route Aggregation Works (4 M)
CIDR combines multiple contiguous networks with the same prefix into a single summarized route. Instead of advertising eight separate routes, the ISP advertises one 192.168.0.0/21 route, reducing routing information.
Benefits of Route Aggregation (5M)
Reduces routing table size.
Speeds up route lookup and packet forwarding.
Lowers CPU and memory usage on routers.
Simplifies network management.</td><td>CO2</td><td>2B</td><td>K4</td></tr>
<tr><td>6.</td><td>Chennai and Mumbai offices each use OSPF internally. The company now wants to connect the two offices securely over the public Internet. Your network administrator suggests extending OSPF across the Internet. As the Routing Referee, decide whether this is a good idea. If not, recommend a more suitable routing protocol, explain why it is a better choice, describe its key features, and compare it with OSPF for this scenario.</td><td>CO2</td><td>2B</td><td>K3</td></tr>
</table>

<table>
<tr>
<td>6
Ans</td>
<td>Recommendation (4 Marks)
No. I would not recommend extending OSPF directly across the public Internet. Instead, I recommend using BGP (Border Gateway Protocol) to connect the Chennai and Mumbai offices over the Internet.
Why BGP is More Suitable (4 Marks)
BGP is an Exterior Gateway Protocol (EGP) designed to exchange routing information between different networks (Autonomous Systems) over the Internet.
Reasons for choosing BGP:
Designed for Internet-scale routing.
Highly scalable and stable.
Supports policy-based routing, allowing administrators to control path selection.
Comparison: BGP vs. OSPF (5 Marks)
<table>
<tr><th>Feature</th><th>OSPF</th><th>BGP</th></tr>
<tr><td>Protocol Type</td><td>Interior Gateway Protocol (IGP)</td><td>Exterior Gateway Protocol (EGP)</td></tr>
<tr><td>Routing Algorithm</td><td>Link-State</td><td>Path Vector</td></tr>
<tr><td>Best Used For</td><td>Routing within an organization</td><td>Routing between organizations or over the Internet</td></tr>
<tr><td>Scalability</td><td>Medium to Large</td><td>Very Large (Internet-scale)</td></tr>
<tr><td>Convergence</td><td>Fast</td><td>Slower but more stable</td></tr>
</table>
</td>
<td>CO2</td>
<td>2B</td>
<td>K3</td>
</tr>
<tr>
<td>7.</td>
<td>Global Connect's network is behaving like a busy family WhatsApp group! BGP routers are arguing over the best route, while thousands of users are shouting, "Send me the cricket match!" using multicast streaming. As the Network Referee, explain why BGP is called a path-vector protocol and how the AS Path stops routers from going in circles. Then, explain how IGMP ensures that only users who actually want to watch the video receive the stream, instead of sending it to everyone</td>
<td>CO2</td>
<td>2B</td>
<td>K3</td>
</tr>
<tr>
<td>7
Ans</td>
<td>BGP is a Path-Vector ProtocolFull Path Tracking: BGP does not just look at distance metrics. It tracks the exact list of Autonomous Systems (AS) a route must travel through.AS Path Attribute: Think of it like a travel passport. Every network the data crosses stamps its unique AS Number (ASN) onto the route info.

Example:
AS 65001 receives a route with AS path: [65002, 65003, 65001]. Since 65001 is already in the path, the router rejects it.

(4Marks)

How AS Path Stops Routers from Going in CirclesSelf-Check</td>
<td>CO2</td>
<td>2B</td>
<td>K3</td>
</tr>
</table>

<table>
<tr><td></td><td>Rule: Before accepting a route update, a router checks the passport stamps.Loop Prevention: If a router sees its own ASN already stamped in the path, it knows the route has looped.

Instant Drop: The router rejects that path immediately to kill the loop.
(4 Marks)

How IGMP Restricts the Video StreamNo Spamming: IGMP acts like a strict opt-in subscription service for local network links.The "Join" Request: A user's device sends an IGMP Membership Report to the local router saying, "Put me on the cricket match stream list."
The "Leave" Request: When done, the device sends a Leave Group message, or stops responding to router checks.Targeted Delivery: The router only forwards the video data to interfaces with active subscribers, keeping the stream away from non-interested users.
Video Streaming Application:
Only clients that send IGMP Join messages receive the video stream. Non-subscribers do not receive unnecessary multicast traffic, saving bandwidth.
(5 Marks)</td><td></td><td></td><td></td></tr>
<tr><td>8.</td><td>As the network architect at HungryApp, explain why BGP is a path-vector protocol using the food delivery analogy — where delivery drivers log every restaurant they pass — and how the AS Path prevents drivers from going in circles. Additionally, explain how IGMP ensures that live tracking updates are sent only to customers with active orders, not to all 5 million app users.</td><td>CO2</td><td>2B</td><td>K4</td></tr>
<tr><td>8
Ans</td><td>BGP Path-Vector & AS Path (6Marks)

Concept explanation and Table it

<table><tr><td>Concept</td><td>Food Delivery Analogy</td></tr><tr><td>Path-Vector Protocol</td><td>BGP is like a delivery driver who logs every restaurant they passed through, not just the total distance.</td></tr><tr><td>AS Path Attribute</td><td>The AS Path is like the delivery log — it records every stop the driver made.</td></tr><tr><td>Loop Prevention</td><td>When a driver sees their own restaurant already in the log, they know they've been there before and refuse to deliver to avoid going in circles.</td></tr></table></td><td>CO2</td><td>2B</td><td>K4</td></tr>
</table>

	IGMP Multicast (7 Marks) Concept: Food Delivery Analogy IGMP: IGMP is like the order list — only customers who placed an order receive live tracking updates. Multicast vs. Broadcast: Without IGMP, updates would be sent to all 5 million users (broadcast) — wasting bandwidth. With IGMP, updates go only to active order customers. Join/Leave Process: - Join: Customer places an order → Added to tracking list. - Leave: Order delivered → Removed from tracking list.			

Part C

Q.No	Questions	CO's	Unit	Bloom's Level
1.	The City Mayor demands IPv6 migration for 1 million IoT sensors, 500 government offices, and 100,000 Wi-Fi hotspots — all within 30 days — plus route aggregation into a single route. Evaluate the feasibility of this mandate, analyze the challenges of migrating legacy sensors (10 years old, no IPv6), Assess route aggregation for 2001:db8:city::/32 across 10 zones with varying densities (Zone A: 200,000 sensors). Justify a realistic zone-by-zone phased migration timeline and convince the Mayor why 30 days is technically impossible.	CO2	2C	K5

1 Ans	Feasibility Evaluation (5 Marks) Feasibility: NOT feasible in 30 days. Route Aggregation (5 Marks) **Aggregation:** City advertises a single **2001:db8:city::/32** route to ISP, reducing routing table size. Phased Timeline & Convincing the Mayor (5 Marks)	CO2	2C	K5

Challenge	Analysis
1M IoT Sensors	10-year-old sensors lack IPv6 stack; hardware replacement impossible in 30 days.
500 Government Offices	Legacy applications break with IPv6; require application-level upgrades.
100K Wi-Fi Hotspots	Fragmented vendors; coordination alone takes months.
Staff Training	500+ IT staff need IPv6 training — cannot happen in 30 days.
Risk	City-wide service disruption (traffic lights, water supply).

Zone	Sensors	Subnet Allocation
Zone A	200,000	2001:db8:city:0001::/48
Zone B	50,000	2001:db8:city:0002::/48
Zone C	100,000	2001:db8:city:0003::/48

Phase	Duration	Activities
Phase 1: Assessment	Months 1-3	Audit sensors, identify IPv6 support, upgrade infrastructure, train staff.
Phase 2: Pilot Zone	Months 4-6	Deploy dual-stack in Zone A (smallest). Test 6LoWPAN.
Phase 3: Expansion	Months 7-15	Expand to Zones B, C, D based on pilot learnings.

<table>
<tr><td></td><td>
<table>
<tr><td>Phase 4: Full Deployment</td><td>Months 16-22</td><td>Deploy to remaining zones.</td></tr>
<tr><td>Phase 5: IPv4 Phase-Out</td><td>Months 23-24</td><td>Retain IPv4 only for legacy devices. Use NAT64/DNS64.</td></tr>
</table>
Applicable Convince Points:
• "A 30-day migration will cause city-wide failure — traffic lights offline, water meters not reading, waste bins overflowing."
• "A zone-by-zone phased approach ensures zero disruption. We can deliver a stable IPv6-enabled city in 24 months."
</td><td></td><td></td><td></td></tr>
<tr><td>2.</td><td>GlobalBank's CEO demands 99.999% availability for a 50-country, 10,000-branch network suffering from OSPF convergence delays, BGP route flapping, and global synchronization causing TCP window reductions. Analyze the root causes of each problem. Evaluate whether OSPF timer tuning, BGP dampening, and RED with WRED are sufficient for high-frequency trading.</td><td>CO2</td><td>2C</td><td>K5</td></tr>
<tr><td>2 Ans</td><td>
Root Cause Analysis (5 Marks)
<table>
<tr><td>Problem</td><td>Root Cause</td></tr>
<tr><td>OSPF Convergence Delays</td><td>Single-area design (500+ routers) causes LSA flooding to all routers; SPF recomputation on every router; takes seconds to converge.</td></tr>
<tr><td>BGP Route Flapping</td><td>Intermittent link failures, BGP session timeouts, misconfiguration — frequent withdrawals and re-advertisements.</td></tr>
<tr><td>Global Synchronization</td><td>Tail-drop congestion causes all TCP flows to drop simultaneously; all flows reduce window sizes, causing underutilization and synchronized recovery cycles.</td></tr>
</table>
Solution Effectiveness (3 Marks)
<table>
<tr><td>Solution</td><td>Effectiveness</td><td>Limitations</td></tr>
</table>
</td><td>CO2</td><td>2C</td><td>K5</td></tr>
</table>

OSPF Timer Tuning	Reduces hello/dead intervals for faster detection.	Too aggressive causes flapping; does not address flooding scope.
BGP Dampening	Suppresses flapping routes after penalty threshold.	Over-dampening can hide legitimate routes; doesn't fix root cause.
RED with WRED	Prevents global sync via random early drops; WRED differentiates traffic classes.	Requires careful tuning; doesn't distinguish critical vs. non-critical traffic without QoS.

Sufficiency & Superior Alternatives (5 Marks)

Problem	Are Solutions Sufficient?	Superior Alternatives
OSPF Convergence	No. Timer tuning doesn't solve flooding scope.	BFD (Bidirectional Forwarding Detection) — sub-second (50ms) failure detection. Multiple OSPF Areas — limit SPF scope.
BGP Flapping	No. Dampening hides symptoms, not causes.	BGP Fast External Failover — immediate withdrawal. BFD for BGP — sub-second session failure detection.

	Applicable Convince points: • "Five-nines (99.999%) means only 5 minutes of downtime per year. A single silver bullet cannot achieve this." • "We need a **layered approach** — BFD for fast detection, QoS for traffic prioritization, and redundancy for failover."			

Unit- 3

Part A

Q.No	Questions	CO's	Unit	Bloom's Level
1.	Describe the transition between the CLOSED and ESTABLISHED states in the TCP state machine, including the intermediate states and the events that trigger each transition. Apply this to the scenario where a client initiates a connection to the server.	CO3	3A	K1
1 Ans	The TCP connection starts in the CLOSED state. When a client initiates a connection, it sends a SYN packet and enters the SYN-SENT state. The server, in the LISTEN state, responds with a SYN+ACK and moves to SYN-RECEIVED. The client replies with an ACK, completing the three-way handshake. Both client and server then enter the ESTABLISHED state, where reliable data transfer begins.	CO3	3A	K1
2.	Differentiate between TCP Reno and TCP New Reno in terms of their recovery mechanisms. Which algorithm would you recommend for your company's order processing system and why?	CO3	3A	K1
2 Ans	<table><tr><th>TCP Reno</th><th>TCP New Reno</th></tr><tr><td>Retransmits only one lost packet per RTT.</td><td>Retransmits multiple lost packets within the same recovery phase.</td></tr><tr><td>Exits Fast Recovery after receiving a partial ACK.</td><td>Remains in Fast Recovery until all lost packets are recovered.</td></tr><tr><td>Less efficient when multiple packet losses occur.</td><td>Better performance with multiple packet losses.</td></tr><tr><td>Lower throughput under heavy congestion.</td><td>Higher throughput and improved recovery efficiency.</td></tr></table>	CO3	3A	K1

3.	In your office, the coffee machine is a shared resource. Employees are constantly sending requests (packets) to get coffee (data). How TCP Vegas differs from TCP Reno in detecting network congestion using this analogy. How does Vegas use RTT to predict congestion	CO3	3A	K2
3 Ans	TCP Reno detects congestion only after packet loss occurs, using duplicate ACKs or timeouts as indicators. In contrast, TCP Vegas predicts congestion before packet loss by measuring changes in Round-Trip Time (RTT)**.** If RTT increases, Vegas assumes the network is becoming congested and reduces its sending rate proactively, resulting in fewer packet losses and better network utilization.	CO3	3A	K2
4.	Summarize how Cubic TCP adjusts its congestion window growth compared to traditional AIMD.	CO3	3A	K1
4 Ans	Traditional AIMD increases the congestion window linearly and decreases it by half after packet loss. Cubic TCP uses a cubic mathematical function to grow the congestion window. It grows rapidly in high-speed networks, slows near the previous maximum window size, and then accelerates again, allowing better utilization of high-bandwidth, long-delay networks while maintaining fairness.	CO3	3A	K1
5.	A network administrator is explaining TCP congestion control to a junior engineer. He describes the AIMD algorithm as a "slow and cautious" approach to managing the congestion window. How does the AIMD algorithm control congestion in TCP?	CO3	3A	K2
5 Ans	Additive Increase Multiplicative Decrease (AIMD) is a congestion control algorithm where: The congestion window (cwnd) increases gradually (typically by one MSS per RTT) when no congestion is detected. When congestion is detected through packet loss, the congestion window is reduced multiplicatively, usually to half of its current size. This approach balances efficient bandwidth utilization with network stability.	CO3	3A	K2
6.	Describe how Slow Start increases the congestion window size during TCP connection startup.	CO3	3A	K1
6 Ans	During **Slow Start**, TCP initializes the congestion window with a small value (typically 1–10 MSS). For every ACK received, the congestion window increases by one MSS, causing it to **double every RTT**. This exponential growth continues until the congestion window reaches the **slow-start threshold (ssthresh)** or packet loss occurs, after which TCP switches to congestion avoidance.	CO3	3A	K1
7.	TCP normally waits for a timeout to retransmit lost packets, which wastes time and reduces throughput. Fast Retransmit improves this by detecting loss earlier using duplicate ACKs. Explain the purpose of Fast Retransmit in	CO3	3A	K1

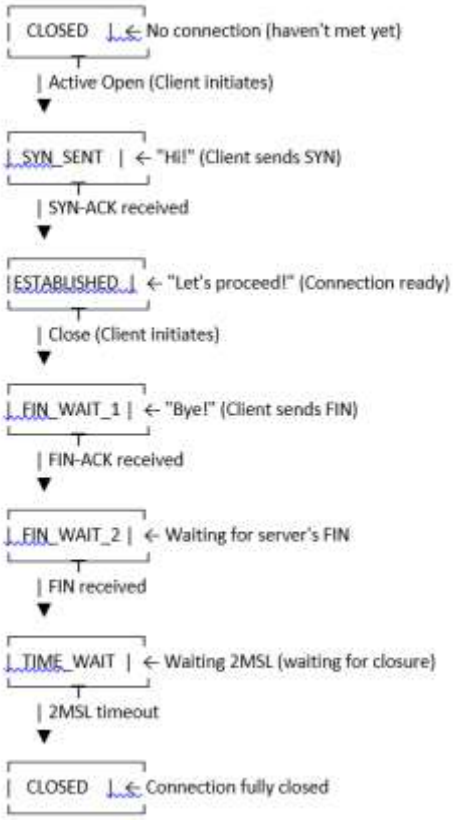
<table>
<tr><td></td><td>TCP. How does it avoid waiting for a timeout</td><td></td><td></td><td></td></tr>
<tr><td>7 Ans</td><td>Fast Retransmit allows TCP to quickly retransmit a lost packet after receiving three duplicate ACKs, indicating that a packet is missing. Instead of waiting for the retransmission timeout (RTO), TCP immediately resends the lost packet, reducing recovery time and improving throughput.</td><td>CO3</td><td>3A</td><td>K1</td></tr>
<tr><td>8.</td><td>Stop-and-Wait ARQ sends one packet and waits for an ACK before sending the next. Go-Back-N ARQ sends multiple packets before waiting for an ACK and retransmits all packets from the lost one.Compare Stop-and-Wait ARQ and Go-Back-N ARQ</td><td>CO3</td><td>3A</td><td>K1</td></tr>
<tr><td>8 Ans</td><td><table>
<tr><th>Stop-and-Wait ARQ</th><th>Go-Back-N ARQ</th></tr>
<tr><td>Sends one frame at a time.</td><td>Sends multiple frames continuously.</td></tr>
<tr><td>Waits for ACK before sending the next frame.</td><td>Uses a sliding window mechanism.</td></tr>
<tr><td>Simple but inefficient on high-delay links.</td><td>Higher efficiency and throughput.</td></tr>
<tr><td>Retransmits only the lost frame.</td><td>Retransmits the lost frame and all subsequent frames.</td></tr>
<tr><td>Lower bandwidth utilization.</td><td>Better bandwidth utilization.</td></tr>
</table></td><td>CO3</td><td>3A</td><td>K1</td></tr>
<tr><td>9.</td><td>Imagine you write answers for 12 questions even though only 10 are required. If the examiner loses 2 answers, you still get full marks because of the extra answers you included. How FEC works in data transfer. How does it recover lost data without retransmission?</td><td>CO3</td><td>3A</td><td>K2</td></tr>
<tr><td>9 Ans</td><td>Forward Error Correction (FEC) adds redundant error-correcting bits to transmitted data. The receiver uses these extra bits to detect and correct certain errors without requesting retransmission. Sender adds redundant data (extra answers) to the original message. Receiver uses redundant data to reconstruct lost/corrupted packets — no need to ask the sender to resend. Low latency — ideal for real-time apps</td><td>CO3</td><td>3A</td><td>K2</td></tr>
<tr><td>10.</td><td>Describe two key features of SCTP that distinguish it from TCP. How do these features benefit data transfer?</td><td>CO3</td><td>3A</td><td>K1</td></tr>
</table>

10 Ans	Two important features of SCTP (Stream Control Transmission Protocol) are: • Multi-streaming: Supports multiple independent data streams within a single connection, preventing head-of-line blocking. • Multi-homing**:** Allows an endpoint to use multiple IP addresses, improving fault tolerance by automatically switching to another path if one fails.	CO3	3A	K1
11.	Imagine you are on a video call with your friend. RTP is the video and audio stream — the actual content of the call. RTCP is your friend periodically saying, "Wait, you're lagging," "Your video is pixelated," or "I can barely hear you." This feedback helps the call quality adjust dynamically. How the relationship between RTP and RTCP in real-time media transmission.	CO3	3A	K2
11 Ans	RTP (Real-time Transport Protocol) carries real-time audio and video data between endpoints. RTCP (Real-time Transport Control Protocol) accompanies RTP by exchanging control information such as packet loss, delay, jitter, and synchronization data. RTP delivers the media, while RTCP monitors transmission quality and provides feedback for performance optimization.	CO3	3A	K2
12.	In a video conference, packets arrive at irregular intervals, causing frozen frames and out-of-sync audio. Summarize how jitter affects real-time streaming quality and how it is managed.	CO3	3A	K2
12 Ans	Jitter is the variation in packet arrival times. High jitter causes: • Audio distortion or choppy voice. • Video freezing or frame skips. • Lip-sync problems between audio and video. Applications use jitter buffers to smooth packet arrival and improve playback quality.	CO3	3A	K2
13.	You are browsing a website that loads images, text, and videos simultaneously. With TCP, if one element (e.g., an image) is delayed, the entire page stalls. With SCTP, each element can be delivered independently. Why SCTP supports multi-streaming and how this benefits applications like web browsing.	CO3	3A	K2
13 Ans	Multi-streaming enables SCTP to transmit multiple independent streams over one association. If packets are lost in one stream, only that stream is delayed, while others continue transmitting normally. This minimizes head-of-line blocking and improves performance for applications such as multimedia communication, web	CO3	3A	K2

	services, and signaling protocols.			
14.	Describe how RTCP feedback (e.g., sender/receiver reports) helps monitor QoS in real-time sessions.	CO3	3A	K1
14 Ans	RTCP periodically exchanges Sender Reports (SR) and Receiver Reports (RR) containing: • Packet loss statistics • Jitter measurements • Round-trip delay • Throughput information • Synchronization timestamps This feedback allows applications to monitor Quality of Service (QoS) and adjust encoding rates or transmission parameters to maintain good audio/video quality.	CO3	3A	K1
15.	Your office has two internet connections — one fiber and one backup 4G. If the fiber line goes down, the backup takes over without dropping active sessions. Explain the concept of "multi-homing" in SCTP and how it ensures uninterrupted connectivity.	CO3	3A	K1
15 Ans	SCTP (Stream Control Transmission Protocol) allows a single association (connection) to have multiple IP addresses assigned to each endpoint. One IP is designated as the primary path, and others are alternate paths. The SCTP association is established with two local IPs — one for the fiber connection and one for the 4G backup. - The fiber IP is set as the primary path. - The 4G IP is configured as an alternate path. - SCTP continuously monitors the primary path using heartbeat messages.	CO3	3A	K1

Part- B

Q. No	Questions	CO's	Unit	Bloom's Level
1.	Illustrate the TCP state machine with a neat state transition diagram, and apply it to trace the sequence of states during connection establishment (three-way handshake) and connection termination (four-way handshake) for a client-server FTP session. Explore the below scenario: First date: "Hi!" → "Hi!" → "Let's proceed!" (3 steps) → Conversation → "Bye!" → "Bye!" → "Bye!" → "Take care!" (4 steps).	CO 3	3B	K3
1 Ans	TCP State Machine diagram: (4 Marks)	CO 3	3B	K3



First Date Analogy: TCP State Transitions (4 Marks)

Step	First Date Analogy	TCP Event	Client State	Server State
Before Date	Haven't met yet	No connection	CLOSED	CLOSED
Step 1	"Hi!" (Client initiates)	Client sends SYN	SYN_SENT	LISTEN
Step 2	"Hi!" (Server responds)	Server sends SYN-ACK	SYN_SENT	SYN_RCVD
Step 3	"Let's proceed!" (Client confirms)	Client sends ACK	ESTABLISHED	ESTABLISHED
—	Conversation (FTP Data	Data transfer occurs	ESTABLISHED	ESTABLISHED

	Transfer)			
Step 4	"Bye!" (Client initiates)	Client sends FIN	FIN_WAIT_1	ESTABLISHED
Step 5	"Bye!" (Server acknowledges)	Server sends ACK	FIN_WAIT_2	CLOSE_WAIT
Step 6	"Bye!" (Server initiates)	Server sends FIN	FIN_WAIT_2	LAST_ACK
Step 7	"Take care!" (Client confirms)	Client sends ACK	TIME_WAIT	CLOSED
Step 8	Move on (2MSL timeout)	2MSL timeout expires	CLOSED	CLOSED

Key Observations (5 Marks)

Aspect	TCP Behavior	First Date Analogy
Stateful	TCP maintains state at both ends.	Both parties know where they are in the relationship.
Three-Way Handshake	Ensures both sides are ready.	Both confirm they are interested before proceeding.
Four-Way Handshake	Graceful termination.	Polite goodbye from both sides.

	TIME_WAIT	Client waits 2MSL to ensure ACK is received.	Client waits to ensure server knows it's over.			
	CLOSE_WAIT	Server waits for application to close.	Server takes time to process the goodbye.			
2.	Imagine a highway with multiple accidents (packet losses). Traffic control (TCP) receives three warning signals (duplicate ACKs) and then a complete roadblock (timeout). Trace the congestion control states also Compare how TCP Reno (panics and resets) and TCP New Reno (calmly handles all accidents) would respond.			CO 3	3B	K4
2 Ans	Highway Accident Analogy: TCP Congestion Control States (4 Marks)			CO 3	3B	K4

Highway Analogy	TCP State	What Happens
Road is clear	Slow Start	Traffic flows freely; cwnd grows exponentially (doubles every RTT).
Traffic builds up	Congestion Avoidance	cwnd grows linearly (probes for bandwidth cautiously).
3 Warning Signals (Hazards)	Fast Retransmit	Accidents detected early; sender retransmits lost packet immediately.
Detour/Recovery	Fast Recovery	Traffic reroutes; cwnd = ssthresh + 3; sender waits for recovery confirmation.
Complete Roadblock	Timeout → Slow Start	Severe congestion; reset cwnd = 1 MSS; start from scratch.

A TCP connection receives three duplicate ACKs (warning signals) followed by a timeout (complete roadblock). (4 Marks)

Step	Event	State Transition

1	Connection starts	Slow Start
2	cwnd reaches ssthresh	Slow Start → Congestion Avoidance
3	3 Duplicate ACKs received	Congestion Avoidance → Fast Retransmit
4	Enter recovery	Fast Retransmit → Fast Recovery
5	Timeout occurs (before recovery completes)	Fast Recovery → Slow Start
6	Retransmit lost packet	Slow Start continues

Detailed Comparison: TCP Reno vs. TCP New Reno (5 Marks)

Criteria	TCP Reno	TCP New Reno
How It Handles First Loss	Fast Retransmit → Fast Recovery	Fast Retransmit → Fast Recovery
Handling Subsequent Losses	Can only recover from one packet loss per RTT. Second loss → timeout → Slow Start.	Can recover from multiple losses in the same window using partial ACKs.
Response to Duplicate ACKs	After first loss, ignores further duplicate ACKs until Fast Recovery exits.	Uses partial ACKs to stay in Fast Recovery and retransmit all lost packets.
Timeout Behavior	Falls back to Slow Start drastically reducing throughput.	Avoids multiple timeouts; handles all losses within the same RTT.
Performance	Degrades significantly with multiple losses.	Better performance in high-loss networks (wireless, congested links).

3.	Imagine an elevator that can carry a certain number of people (cwnd). It starts with 8 people (segments). The elevator adds 1 person per floor (RTT) but when it gets overloaded (packet loss at	CO 3	3B	K3

	RTT 4), it drops half the people and starts again. Apply AIMD to trace cwnd over 6 RTTs and illustrate the sawtooth pattern.			
3 Ans	AIMD Algorithm Explanation (4 Marks) **Phase** | **Action** | **Formula** Additive Increase | Increase cwnd by 1 MSS every RTT (no loss) | cwnd = cwnd + 1 Multiplicative Decrease | On packet loss, halve the cwnd | cwnd = cwnd / 2 cwnd Trace Over 6 RTTs Given: Initial cwnd = 8 segments, packet loss at RTT 4. (5 Marks) **RTT** | **Event** | **cwnd (segments)** | **Calculation** 0 | Start | 8 | Initial value 1 | No loss | 9 | 8 + 1 2 | No loss | 10 | 9 + 1 3 | No loss | 11 | 10 + 1 4 | Packet Loss! | 5 | 11 / 2 = 5 (rounded down) 5 | No loss | 6 | 5 + 1 6 | No loss | 7 | 6 + 1 Pattern Description: • RTT 0-3: cwnd increases linearly (8 → 9 → 10 → 11) — Additive Increase • RTT 4: Packet loss occurs → cwnd drops from 11 to 5 — Multiplicative Decrease • RTT 5-6: cwnd increases linearly again (5 → 6 → 7) — Additive Increase • This creates the characteristic sawtooth pattern of TCP congestion control.	CO 3	3B	K3

Summary Table (4 Marks)

RTT	cwnd	Event
0	8	Start
1	9	Additive Increase
2	10	Additive Increase
3	11	Additive Increase
4	**5**	Multiplicative Decrease (Loss!)
5	6	Additive Increase
6	7	Additive Increase

4.	Examine the architectural differences between SCTP and TCP, and analyze how SCTP's multi-streaming and multi-homing features overcome the "head-of-line blocking" problem faced by TCP. Justify the suitability of SCTP for signaling in telecommunication networks (e.g., SS7 over IP).	CO 3	3B	K3
4 Ans	Architectural Differences Between SCTP and TCP (4 Marks)	CO 3	3B	K3

Feature	TCP (Transmission Control Protocol)	SCTP (Stream Control Transmission Protocol)
Message Orientation	Byte-stream oriented — does not preserve message boundaries. Data is sent as a continuous stream.	Message-oriented — preserves message boundaries. Each message is sent as a distinct chunk.
Streaming Support	Single stream — all data flows in one ordered sequence.	Multi-streaming — supports multiple independent streams within a single association.

Addressing	Single IP per endpoint — only one IP address per connection.	Multi-homing — supports multiple IP addresses per endpoint for redundancy.

Head-of-Line Blocking Problem in TCP (4 Marks)

Aspect	Explanation
What is Head-of-Line Blocking?	In TCP, all data flows through a single ordered stream. If a packet is lost, all subsequent packets must wait until the lost packet is retransmitted and received in order. This causes delays and reduces throughput.
Why It Happens	TCP guarantees in-order delivery. If Packet 3 is lost, Packet 4 and Packet 5 (which may have already arrived) are held in the receiver's buffer. They cannot be delivered to the application until Packet 3 is recovered.
Impact	Increased latency and reduced efficiency — especially problematic for applications with multiple independent data streams (e.g., web browsing with multiple objects, VoIP signaling + voice).

How SCTP Overcomes Head-of-Line Blocking

SCTP Feature	How It Solves Head-of-Line Blocking
Multi-Streaming	SCTP supports multiple independent streams within a single association. Each stream has its own sequence numbering and delivery order. Example: If Packet 3 in Stream 1 is lost, only Stream 1 is affected. Stream 2, Stream 3, and Stream 4 continue delivering data without waiting. Benefit: Head-of-line blocking is contained to the affected stream. Other streams are unaffected, improving overall throughput and reducing latency.
Message	SCTP preserves message boundaries,

	<table><tr><td>Boundaries</td><td>allowing applications to send and receive structured messages (chunks) without the application having to delimit the data. Benefit: Simplifies application logic and reduces processing overhead.</td></tr></table> Multi-Homing: Network Redundancy (5 Marks) <table><tr><td>Aspect</td><td>SCTP Multi-Homing Benefit</td></tr><tr><td>What is Multi-Homing?</td><td>SCTP allows an endpoint to have multiple IP addresses associated with a single association. One IP is designated as the primary path, and others are alternate paths.</td></tr><tr><td>How It Works</td><td>SCTP monitors the primary path using heartbeat messages. If the primary path fails, SCTP automatically switches to an alternate path without terminating the association.</td></tr><tr><td>Benefit</td><td>Fault tolerance and high availability — network failures do not disrupt critical applications.</td></tr></table> Conclusion • TCP is a general-purpose protocol suitable for web, email, and file transfer, but its single-stream, single-path architecture makes it unsuitable for telecommunication signaling. • SCTP overcomes TCP's limitations with multi-streaming (avoiding head-of-line blocking) and multi-homing (providing network redundancy). • SCTP is the ideal choice for signaling in telecommunication networks (SS7 over IP, SIGTRAN, 3GPP/4G/5G) due to its reliability, low latency, message orientation, and high availability.			
5.	Analyze the role of RTP and RTCP in supporting real-time multimedia transmission, and examine how RTCP's jitter calculation and feedback mechanism enable adaptive jitter buffer management. Determine the impact of network jitter on Quality of Service (QoS) for VoIP applications.	CO 3	3B	K4
5 Ans	The Real-Time Transport Protocol (RTP) delivers multimedia payloads with sequence numbers and timestamps, while the RTP Control Protocol (RTCP) provides out-of-band statistical feedback on transmission quality—including packet loss and inter-arrival jitter—to support adaptive performance. Roles of RTP and RTCPRTP: Handles data-plane delivery over	CO 3	3B	K4

	UDP, sequencing and timestamping packets for real-time playout without guaranteeing delivery or order. RTCP: Operates on the control plane, issuing periodic Sender Reports (SR) and Receiver Reports (RR) to monitor Quality of Service (QoS) and synchronize distinct media streams. RTCP Jitter Calculation & Adaptive Jitter Buffers • Jitter Metric: RTCP computes inter-arrival jitter (J(i) dynamically using a smoothed moving average of the difference in packet spacing relative to RTP timestamps: (J(i) = J(i-1) + (D(i-1, i) - J(i-1))/16). • Feedback Mechanism: Receivers package these calculated jitter metrics into Receiver Reports and transmit them back to senders or local playout engines. • Adaptive Buffer Management: The application reads this variance data to dynamically resize the jitter buffer depth—expanding it during network jitter spikes to prevent drops, or shrinking it during stable periods to minimize conversational latency. Impact of Network Jitter on VoIP QoS Audio Choppiness & Distortion: Unmitigated network jitter causes voice packets to arrive erratically, resulting in clipped or garbled speech. Late Packet Discard: Packets arriving outside the current jitter buffer window are treated as lost, directly lowering the Mean Opinion Score (MOS). Added Latency: Over-compensating with an excessively large static or poorly tuned buffer introduces conversational delay, degrading real-time interactivity.			
6.	Analyze the congestion window behavior of AIMD-based algorithms versus Cubic TCP's cubic growth function under a long fat network (LFN) with high bandwidth-delay product, and examine why traditional AIMD-based TCP variants underutilize available bandwidth in such environments.	CO 3	3B	K4

6 Ans	Bandwidth Underutilization of Traditional AIMD in LFNs (4 Marks) Traditional AIMD-based TCP (like TCP Reno) severely underutilizes Long Fat Networks (LFNs) due to its rigid growth and drastic recovery mechanics: Slow Linear Increase: The Additive Increase phase increments the congestion window (cwnd) by only 1 MSS per Round-Trip Time (RTT). In a high-bandwidth, high-latency LFN requiring a (cwnd) of hundreds of thousands of packets, recovering from a single drop takes hours. Aggressive Multiplicative Decrease: Upon detecting packet loss, the Multiplicative Decrease phase slashes the (cwnd) by 50%. The Recovery Deficit: For example, on a 10 Gbps link with a 100 ms RTT (cwnd approx 83,333) packets), a single loss cuts the window by 41,666 packets. At 1 MSS per RTT, it takes nearly 70 minutes of error-free transmission just to reclaim the lost bandwidth. AIMD Window Dynamics (5 Marks) Growth Profile: Strictly linear (cwnd(t+1) = cwnd(t) + 1)). Growth rate is independent of the distance from the target capacity, making it highly inefficient when far from the saturation point.RTT Dependency: The window expands as a function of RTT. In an LFN with high propagation delay, growth slows down drastically, punishing long-distance connections. Cubic TCP Window Dynamics Growth Profile: Governed by a cubic function: (cwnd(t) = C(t - K)^3 + W_max), where (W_max) is the window size before the last loss, (C) is a scaling factor, and (K) is the time required to reach (W_max) under no loss. Three-Phase Curve: Concave Phase: Immediately after a loss backoff, the window grows rapidly to quickly reclaim empty pipeline space, then flattens out as it approaches the previous stable capacity (W_max). (4 Marks) • RTT Independence: Window growth is calculated using absolute elapsed wall-clock time (t) since the last loss, rather than RTT. This ensures that long-delay LFN paths scale up at the exact same rate as short-delay paths. • Backoff: Uses a gentler multiplicative decrease factor of 0.7 (cwnd_new = 0.7 times cwnd_old), keeping the pipeline 20% fuller than Reno after a packet drop.	CO 3	3B	K4
7.	A delivery truck carries 10 packages (data packets) across a long bridge (satellite link) with 500 ms delay. The driver adds 2 extra packages (FEC) so that even if 2 packages fall off the truck, the receiver still gets all 10. Illustrate how FEC works without	CO 3	3B	K3

	retransmission. Compare FEC overhead with ARQ (which would require going back to get fallen packages).			
7 Ans	How FEC Works (No Retransmission) (4 Marks) • At the Warehouse (Sender): The driver takes the 10 original packages and runs their contents through a mathematical formula to create 2 redundant "blueprint" packages (FEC parity). The truck crosses the bridge carrying a total of 12 packages. • On the Bridge (Satellite Link): The trip takes 500 ms. Due to rough roads, 2 packages fall off the truck and are lost. • At the Destination (Receiver): The truck arrives with only 10 packages. Instead of turning the truck around, the receiver opens the remaining packages—which include a mix of original contents and the blueprint packages. Using the blueprints, the receiver mathematically reconstructs the exact contents of the 2 lost packages on the spot. • Total Time: 500 ms. Delivery is successful on the first try with zero arrival delay. FEC vs. ARQ Comparison (5 Marks) If the driver used an Automatic Repeat reQuest (ARQ) system instead, no extra blueprint packages would be loaded, but a feedback loop would be required. 1. ARQ Mechanics & Delay Timeline • 0 ms: The truck leaves with exactly 10 packages. • 500 ms: The truck arrives at the destination missing 2 packages. • 1000 ms: The receiver sends a message back across the bridge (taking another 500 ms) telling the driver to send replacements. • 1500 ms: The replacement truck crosses the bridge with the 2 missing packages. 2. Overhead Evaluation (4 Marks) • FEC Overhead (Cargo Space): Consumes a 20% constant space overhead (2 extra packages added to the 10 original packages). It uses more fuel/bandwidth upfront regardless of whether packages fall off. • ARQ Overhead (Time & Travel): Consumes 0% cargo space overhead initially, but introduces a massive 200% time overhead (1000 ms of extra waiting time) and requires a second physical trip across the bridge.	CO 3	3B	K3
8.	Grandma is on a video call with you. She complains about "frozen video," "robot voice," and "delayed reactions." You need to explain why UDP is better than TCP for her call. Compare TCP, UDP, SCTP, and RTP/RTCP for real-time video calls based on delay, jitter, packet loss, and bandwidth. Justify the best protocol combination for making Grandma happy.	CO 3	3B	K4
8 An	QoS Requirements for Real-Time Applications (4 Marks)	CO 3	3B	K4

s

QoS Requirement	Description	Impact on Real-Time Apps
Bandwidth	Sufficient data rate for audio/video streams.	Insufficient bandwidth causes low resolution and buffering.
Delay (Latency)	End-to-end transmission time (< 150 ms for VoIP).	High delay causes echo and awkward pauses in conversation.
Jitter	Variation in packet arrival times.	High jitter causes choppy video and audio distortion.

Protocol Support for QoS Requirements (4 Marks)

Protocol	Bandwidth	Delay	Jitter	Packet Loss
TCP	Moderate	High (due to retransmission)	High (retransmission causes jitter)	Low (reliable delivery)
UDP	High (low overhead)	Low (no retransmission)	Unmanaged (no jitter control)	High (no recovery)
SCTP	High (multi-streaming)	Low (multi-stream avoids HOL blocking)	Moderate (some jitter control)	Low (reliable per stream)

Summary Table (5 Marks)

Protocol	Best For	Why
TCP	File transfer, email	Reliable but high delay.
UDP	Real-time apps	Low delay but no QoS.

			(base transport)					
		RTP/RTCP	VoIP, Video Conferencing	Designed for real-time — jitter buffers, feedback, adaptive bitrate.				
		SCTP	Telecom signaling (SS7 over IP)	Multi-streaming, multi-homing — but not widely used for media.				

Part- C

Q.No	Questions	CO's	Unit	Bloom's Level
1.	A cloud data center handles thousands of concurrent TCP connections. The network experiences frequent congestion, causing throughput drops and timeouts. Analyze how AIMD, Slow Start, Fast Retransmit, and Fast Recovery work together to manage congestion. Evaluate their effectiveness in preventing congestion and maintaining throughput in large-scale networks.	CO3	3C	K5
1 Ans	1. Slow Start (6 Marks) TCP begins each connection (or after a timeout) with a small congestion window (cwnd), typically 1–10 MSS. For every ACK received, cwnd increases by 1 MSS, causing exponential growth (doubling every RTT). This continues until cwnd reaches the slow start threshold (ssthresh), at which point TCP switches to congestion avoidance. TCP Limitations for Real-Time Applications & Proposed Enhancements (7 Marks) Limitations of TCP for Real-Time Traffic 1. Head-of-Line (HOL) Blocking: A single lost segment stalls delivery of all subsequently received (but already buffered) data until retransmission succeeds — intolerable for live audio/video where late data is useless. 2. Retransmission-Induced Delay: TCP guarantees reliability, not timeliness; retransmissions after RTO can add hundreds of milliseconds, disrupting real-time playback. 3. Connection Setup Overhead: The 3-way handshake (and TLS handshake atop it) adds RTTs before any	CO3	3C	K5

	data flows — costly for short-lived, latency-sensitive sessions. 4. Single Byte-Stream Model: TCP delivers one ordered stream; it cannot let independent logical channels (e.g., audio vs. video vs. control) proceed independently when one is blocked. 5. Congestion Control Mismatch: AIMD's cwnd cuts cause abrupt rate drops unsuitable for constant-rate media codecs, producing jitter and stutter. 6. No Multicast/Timing Support: TCP lacks native timestamping, sequencing semantics for media synchronization, or multicast delivery.			
2.	A cloud gaming service suffers from lag and frame drops because of TCP's head-of-line blocking and retransmission delays. Evaluate TCP's limitations for real-time interactive applications. Suggest how SCTP, RTP/RTCP, QUIC can enhance performance.	CO3	3C	K5
2 Ans	[Marks Limitations 5 marks Enhancements 5 marks, STP marks Total 15 marks] Head-of-Line (HOL) Blocking TCP delivers data strictly in sequence order. A single lost segment forces the receiver to withhold all subsequently arrived data — even if that data belongs to independent logical units (e.g., a later video frame) — until the missing segment is retransmitted. Retransmission Latency Loss recovery relies on 3 duplicate ACKs (Fast Retransmit, ≥1 RTT delay) or, in worse cases, a full RTO (often 200ms+ due to conservative RTT variance estimation). Real-time voice quality standards (ITU-T G.114) require <150ms one-way latency — a single retransmission event can breach this budget entirely. Congestion Control Mismatch AIMD halves cwnd on any detected loss, assuming loss ⟺ congestion. On wireless or lossy links, this assumption fails: bit-error loss triggers unnecessary throttling exactly when sustained throughput is needed for smooth media playback, producing stutter and buffering. Handshake Overhead	CO3	3C	K5

	The TCP 3-way handshake plus a TLS handshake (pre-1.3) adds 2–3 RTTs before data flows — disproportionately costly for short, latency-critical sessions like call setup or interactive control messages. No Native Timing/Multiplexing Semantics TCP has no concept of message boundaries, timestamps, or independent parallel streams within one connection — everything shares a single blocking pipe, forcing applications to build synchronization and multiplexing logic externally (and imperfectly). Poor Mobility Handling TCP connections are bound to a fixed 4-tuple (IP + port). Any network change (e.g., Wi-Fi to cellular handoff) breaks the connection, disrupting ongoing real-time sessions and forcing costly re-establishment. Proposed Enhancements RTP/RTCP over UDP • Runs over UDP → no retransmission delay, no HOL blocking; late data is simply skipped. • RTP adds sequence numbers and timestamps, enabling receiver-side jitter buffering and audio/video sync without imposing strict ordering. QUIC • Built on UDP with integrated TLS 1.3, enabling 0-RTT or 1-RTT connection establishment — collapses handshake latency dramatically versus TCP+TLS. • Independent stream multiplexing removes transport-level HOL blocking (unlike TCP-based HTTP/2). • Connection migration via connection IDs (not tied to IP/port) allows seamless handoff across network changes without renegotiation — critical for mobile real-time apps. • Pluggable, user-space congestion control (e.g., BBR) enables faster, bandwidth-aware adaptation rather than reacting only to loss.			

Unit- 4

Part A

<table>
<tr><th>Q.No</th><th>Questions</th><th>CO’s</th><th>Unit</th><th>Bloom’s Level</th></tr>
<tr><td>1.</td><td>A company's network faces two threats:
Threat 1: Eavesdropping on traffic without altering it.
Threat 2: Modifying data packets before they reach the destination.
Identify which is an Active Attack and which is a Passive Attack. Differentiate between them with examples.</td><td>CO4</td><td>4A</td><td>K2</td></tr>
<tr><td>1 Ans</td><td>
<table>
<tr><th>Active Attack</th><th>Passive Attack</th></tr>
<tr><td>1. An active attack modifies, interrupts, or destroys data in a system.</td><td>1. A passive attack only observes or monitors data without changing it.</td></tr>
<tr><td>2. It affects the integrity and availability of information.</td><td>2. It mainly affects the confidentiality of information.</td></tr>
<tr><td>3. The attacker actively participates in the communication.</td><td>3. The attacker secretly listens to the communication.</td></tr>
<tr><td>4. It is usually easier to detect because system behavior changes.</td><td>4. It is difficult to detect since no changes are made to the data.</td></tr>
<tr><td>5. Prevention requires authentication, access control, and integrity checks.</td><td>5. Prevention mainly relies on encryption and secure communication.</td></tr>
<tr><td>6. Example: Modifying bank transaction details, Denial-of-Service (DoS) attack, data tampering.</td><td>6. Example: Eavesdropping, packet sniffing, traffic analysis.</td></tr>
</table>
</td><td>CO4</td><td>4A</td><td>K2</td></tr>
<tr><td>2.</td><td>An attacker captures an authentication message during a video call and retransmits it later to gain unauthorized access to the system. What is a Replay Attack? How can it be prevented?</td><td>CO4</td><td>4A</td><td>K1</td></tr>
</table>

2 Ans	A Replay Attack is a type of cyberattack in which an attacker captures a valid data transmission, such as a login request or authentication message, and retransmits it later to gain unauthorized access or perform unauthorized actions. The attacker does not need to know the original message contents; they simply reuse the captured message. Example: An attacker records a user's online banking login request and replays it later to access the account without knowing the password. Countermeasures 1)Use Nonces 2) Use Timestamps, Use Session Tokens 3)Implement Challenge–Response Authentication 4)Use Secure Cryptographic Protocols:Protocols such as TLS/SSL help prevent replay attacks by protecting communication.	CO4	4A	K1
3.	A hacker positions themselves between a customer and their bank's website, intercepting all communication. The hacker captures the customer's login credentials and transaction details. Identify the MITM attack on data confidentiality.	CO4	4A	K2
3 Ans	A Man-in-the-Middle (MITM) attack occurs when an attacker secretly intercepts communication between two parties. This compromises data confidentiality because the attacker can read, capture, or steal sensitive information such as usernames, passwords, banking details, and personal data without the users' knowledge. Effects on Data Confidentiality: Unauthorized access to sensitive information. Theft of usernames, passwords, and financial data. Exposure of confidential personal or business information. Loss of privacy and trust in the communication system.	CO4	4A	K2
4.	A gaming server becomes unresponsive during a tournament due to a flood of requests from thousands of hijacked devices. State the purpose of a DDoS attack.	CO4	4A	K1
4 Ans	The purpose of a Distributed Denial-of-Service (DDoS) attack is to overload a target server, network, or website with a large volume of traffic from multiple compromised devices, making the service unavailable to legitimate users.	CO4	4A	K1
5.	Imagine your neighbor secretly listens to your phone calls and reads your messages. List any two types of information targeted in a MITM attack.	CO4	4A	K1
5 Ans	Any two of the following: Usernames and passwords Credit/Debit card or banking details Personal information (e.g., name, address, email) Session cookies or authentication tokens Confidential business data	CO4	4A	K1
6.	A company is configuring a VPN to connect remote offices. The network engineer needs to choose the appropriate IPsec	CO4	4A	K1

<table>
<tr><td></td><td>mode for securing the connection. Name the two operating modes of IPsec.</td><td></td><td></td><td></td></tr>
<tr><td>6 Ans</td><td><table>
<tr><td>Mode</td><td>Description</td><td>Use Case</td></tr>
<tr><td>Tunnel Mode</td><td>Encrypts the entire IP packet (header + payload) and adds a new IP header.</td><td>Gateway-to-Gateway VPNs, site-to-site VPNs.</td></tr>
<tr><td>Transport Mode</td><td>Encrypts only the payload (data) of the IP packet; original IP header is unchanged.</td><td>End-to-End communication (host-to-host).</td></tr>
</table></td><td>CO4</td><td>4A</td><td>K1</td></tr>
<tr><td>7.</td><td>A customer logs into their online banking account. The browser shows a padlock icon, indicating that TLS is securing the connection. Describe the role of encryption in TLS in protecting this communication.</td><td>CO4</td><td>4A</td><td>K2</td></tr>
<tr><td>7 Ans</td><td>Encryption converts plaintext into ciphertext, ensuring that only authorized users can read the transmitted data and protecting it from attackers.
TLS uses symmetric encryption (e.g., AES) to encrypt data after a secure handshake. The session keys are generated using asymmetric encryption (RSA/ECDHE) during the handshake.</td><td>CO4</td><td>4A</td><td>K2</td></tr>
<tr><td>8.</td><td>You are at a coffee shop using public Wi-Fi. You want to check your bank balance. The website uses HTTP for one site and HTTPS for another. Explore HTTPS site is more secure for your banking transaction.</td><td>CO4</td><td>4A</td><td>K2</td></tr>
<tr><td>8 Ans</td><td>HTTPS uses TLS/SSL to encrypt data exchanged between the client and server, protecting it from eavesdropping, tampering, and unauthorized access, whereas HTTP transmits data in plain text.</td><td>CO4</td><td>4A</td><td>K2</td></tr>
<tr><td>9.</td><td>An e-commerce platform processes thousands of transactions daily. It stores customer credit card details and personal information. The company must select a firewall to protect against both network-level and application-level attacks. Choose the appropriate firewall technique and justify your choice.</td><td>CO4</td><td>4A</td><td>K2</td></tr>
<tr><td>9 Ans</td><td>Stateful inspection is the appropriate choice because it monitors active sessions and allows only valid traffic, providing stronger protection than simple packet filtering.</td><td>CO4</td><td>4A</td><td>K2</td></tr>
</table>

<table>
<tr><td></td><td><table><tr><th>Recommendation</th><th>Justification</th></tr><tr><td>Web Application Firewall (WAF) + Next-Generation Firewall (NGFW)</td><td>A combined approach provides defense-in-depth — protecting against both network-layer and application-layer attacks.</td></tr></table></td><td></td><td></td><td></td></tr>
<tr><td>10.</td><td>A company wants to allow SSH access (port 22) only from its internal network (192.168.1.0/24) and block all other external SSH attempts. Summarize the use of packet filtering to restrict access to this service.</td><td>CO4</td><td>4A</td><td>K2</td></tr>
<tr><td>10 Ans</td><td>Configure firewall rules to allow only the required service port (e.g., Port 24 for SMTP) and deny other unnecessary ports.<table><tr><th>Criteria</th><th>Configuration</th></tr><tr><td>Service</td><td>SSH (port 22)</td></tr><tr><td>Allowed Source</td><td>192.168.1.0/24</td></tr><tr><td>Blocked Source</td><td>All other IPs</td></tr><tr><td>Action</td><td>ALLOW for internal; DROP for others</td></tr><tr><td>Purpose</td><td>Restrict SSH access to trusted network only</td></tr></table></td><td>CO4</td><td>4A</td><td>K2</td></tr>
<tr><td>11.</td><td>Imagine a security guard who checks your ID to ensure you are who you say you are (authentication). Another guard locks your bag (encryption) so no one can read your secrets. explore the role of AH and ESP in securing IP communication using this analogy.</td><td>CO4</td><td>4A</td><td>K1</td></tr>
<tr><td>11 Ans</td><td>AH verifies the authenticity and integrity of IP packets.
ESP encrypts data and also provides authentication and integrity, ensuring secure communication.</td><td>CO4</td><td>4A</td><td>K1</td></tr>
<tr><td>12.</td><td>A user wants to access multiple services (email, file server, database) without entering their password each time. who handles this using a central server. Give your justification.</td><td>CO4</td><td>4A</td><td>K1</td></tr>
<tr><td>12 Ans</td><td>KDC – Key Distribution Center. The Key Distribution Center (KDC) verifies the identity of users and provides Ticket Granting Tickets (TGTs) and service tickets, enabling secure authentication without transmitting passwords over the network.</td><td>CO4</td><td>4A</td><td>K1</td></tr>
<tr><td>13.</td><td>Employees working from home access the company network via VPN. The company must verify their identity, control access to sensitive data, and log their activities. Identify the behind concept of this.</td><td>CO4</td><td>4A</td><td>K2</td></tr>
</table>

<table>
<tr><td>13 Ans</td><td>AAA ensures secure network access by verifying the user's identity (Authentication), determining access permissions (Authorization), and recording user activities (Accounting).</td><td>CO4</td><td>4A</td><td>K2</td></tr>
<tr><td>14.</td><td>Your 80-year-old grandma just bought a laptop and calls you saying, "Dear pappu, this website is asking for SSL! Is that a new type of pickle? Or should I restart the router?"</td><td>CO4</td><td>4A</td><td>K1</td></tr>
<tr><td>14 Ans</td><td>Don't restart the router, Grandma! And no, it's not a pickle. It’s an SSL.
SSL stands for Secure Sockets Layer.
It is a cryptographic security protocol developed to establish a secure communication channel between a client and a server over a network. SSL provides:
Confidentiality by encrypting data during transmission.
Authentication by verifying the identity
Data Integrity by ensuring that the transmitted data is not altered during communication.</td><td>CO4</td><td>4A</td><td>K1</td></tr>
<tr><td>15.</td><td>An e-commerce website uses two security tools: one that alerts administrators about attacks, and another that automatically blocks malicious traffic. Who does what and classify it.</td><td>CO4</td><td>4A</td><td>K1</td></tr>
<tr><td>15 Ans</td><td>E-commerce websites commonly use both IDS (alerts) and IPS (automatically blocks) for defense-in-depth.
<table>
<tr><td>Intrusion Detection System (IDS)</td><td>Intrusion Prevention System (IPS)</td></tr>
<tr><td>Monitors network or system activities for suspicious behavior.</td><td>Monitors and actively blocks malicious traffic.</td></tr>
<tr><td>Detects and generates alerts about security threats.</td><td>Detects, prevents, and stops attacks automatically.</td></tr>
<tr><td>Functions as a detection mechanism.</td><td>Functions as a prevention mechanism.</td></tr>
</table></td><td>CO4</td><td>4A</td><td>K1</td></tr>
</table>

Part- B

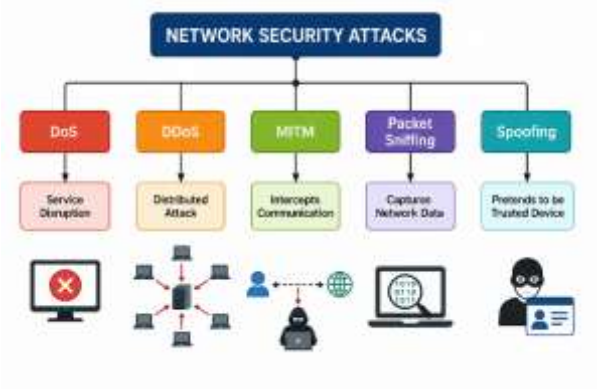
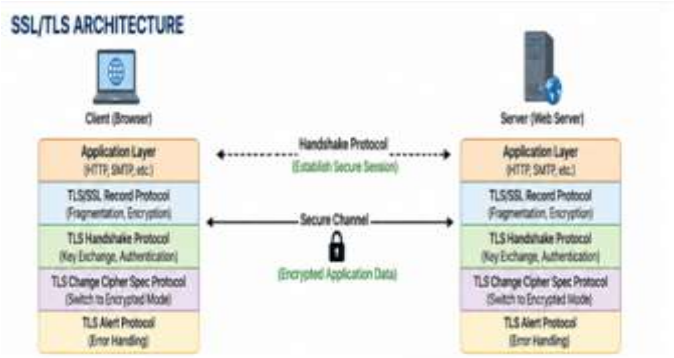
Q.No	Questions	CO’s	Unit	Bloom’s Level
1.	ShopFast, an e-commerce platform, experiences frequent network attacks. Customers complain about slow loading times, unauthorized transactions, and suspicious login attempts. Being a security expert investigates and identifies threats. Also justify of each category	CO4	4B	K3
1 Ans	Definition & working of DoS, DDOs, MITM, Packet sniffing and spoofing attacks (5 Marks) DoS (Denial of Service)- Exhaust server or network resources with excessive traffic or requests. DDoS (Distributed Denial of Service)- Overload the target using multiple compromised devices (Botnet) Man-in-the-Middle (MITM)- Intercept and alters communication between two parties	CO4	4B	K3

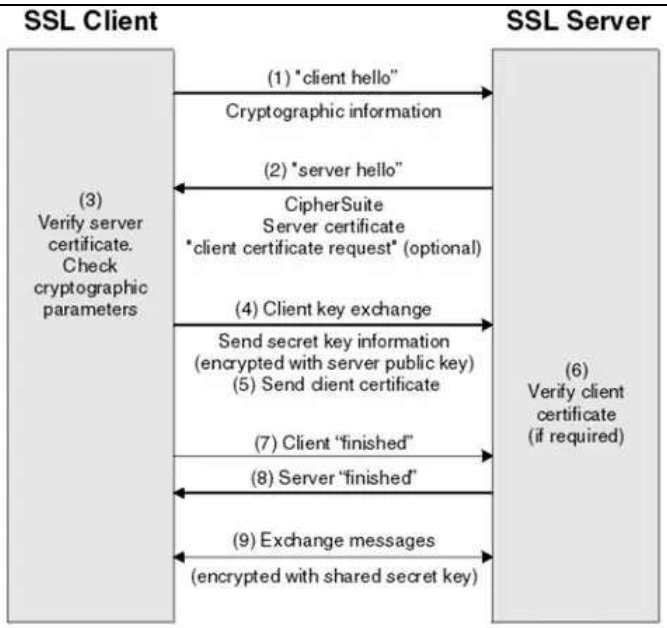
Packet Sniffing- Capture and analyze network packets to obtain sensitive information Spoofing- Impersonate a trusted user, device, or service

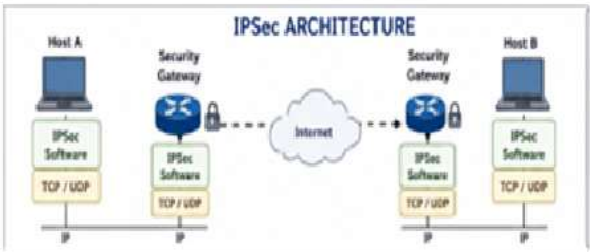
Impact on Network Analysis & preventive measures (5 Marks)

Attack	Impact on Network Security	Preventive Measures
DoS (Denial of Service)	Makes services unavailable to legitimate users, causing downtime and loss of productivity.	Firewall, Rate Limiting, IDS, Traffic Filtering, Load Balancing
DDoS (Distributed Denial of Service)	Causes large-scale service disruption, bandwidth exhaustion, and financial losses.	CDN, Load Balancer, DDoS Protection Services, Anycast Routing, Traffic Monitoring
MITM (Man-in-the-Middle)	Leads to data theft, credential compromise, identity theft, and unauthorized access.	HTTPS, SSL/TLS Encryption, VPN, MFA, Certificate Validation
Packet Sniffing	Compromises confidentiality by exposing usernames, passwords, emails, and financial data.	End-to-End Encryption, HTTPS, SSH, VPN, WPA3 Wi-Fi Security, Network Segmentation
Spoofing	Enables unauthorized access, phishing, malware distribution, and session hijacking.	SPF, DKIM, DMARC, DNSSEC, Strong Authentication, ARP Inspection, Network Monitoring

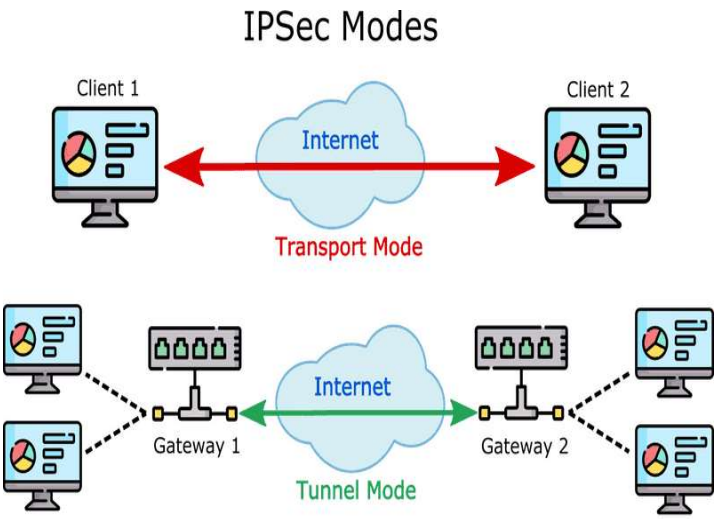
Examples with diagram (3 Marks)

				
2.	A powerful quantum computer has been developed that can break RSA encryption in seconds. A global financial network must migrate to post-quantum TLS to protect transactions. You are the security architect responsible for designing a new TLS handshake that resists quantum attacks. Illustrate the SSL/TLS architecture and explain how it can support quantum-resistant key exchange algorithms also demonstrate the TLS handshake process with a diagram.	CO4	4B	K4
2 Ans	**SSL/TLS Architecture with diagram (5 marks)** **SSL (Secure Sockets Layer)** and **TLS (Transport Layer Security)** are cryptographic protocols used to provide **secure communication over computer networks**. TLS is the improved and more secure version of SSL.  **Components of SSL/TLS Architecture** 1. Handshake Protocol 2. Change Cipher Spec Protocol 3. Alert Protocol 4. Record Protocol **TLS Handshake Process (5 marks)** The TLS handshake establishes a secure connection before actual data transfer.	CO4	4B	K4

	 TLS Handshake Steps Step 1: ClientHello Step 2: ServerHello Step 3: Server Authentication Step 4: Key Exchange Step 5: ChangeCipherSpec Step 6: Finished Message Step 7: Secure Communication **Establishing secure Communication: (3 marks)** 1. The client and server negotiate the strongest mutually supported TLS version and cipher suite. 2. The server proves its identity using a trusted digital certificate. 3. A secure key exchange establishes shared session keys. 4. Symmetric encryption protects data confidentiality. 5. Message authentication ensures integrity and detects tampering. 6. All subsequent communication is encrypted and authenticated through the TLS Record Protocol.			
3.	A multinational company has thousands of remote employees working from home. The employees connect to the corporate network via a VPN that uses IPSec. The company must ensure that all communication is secure and that employees can access internal resources. Analyze the IPSec architecture and explain how it secures VPN connections. Compare AH and ESP in Transport and Tunnel modes.find the best for the remote work VPN and why? Provide suitable diagrams.	CO4	4B	K3
3 Ans				

	Definition (2 Marks) IPSec (Internet Protocol Security) is a suite of security protocols that protects IP communications by providing authentication, integrity, confidentiality, and anti-replay protection at the Network Layer (Layer 3) of the OSI model. It is widely used in Virtual Private Networks (VPNs) for secure communication over untrusted networks such as the Internet. IPSec Architecture & Diagram (3 marks) IPSec consists of the following major components: • Authentication Header (AH) – Provides authentication, integrity, and anti-replay protection. • Encapsulating Security Payload (ESP) – Provides confidentiality (encryption), authentication, integrity, and anti-replay protection. • Internet Key Exchange (IKE) – Establishes Security Associations (SAs) and securely exchanges cryptographic keys. • Security Association (SA) – A logical connection that defines the security parameters for communication.  Modes of IPSec with diagram (4 marks) IPSec operates in two modes: 1. Transport Mode 2. Tunnel Mode	CO4	4B	K3

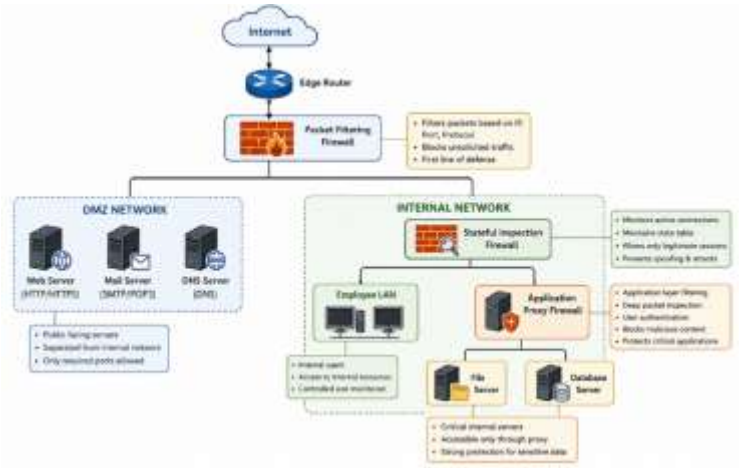
Feature	Transport Mode	Tunnel Mode
Protected Data	Payload only	Entire IP packet
Original IP Header	Visible	Hidden inside tunnel
New IP Header	Not Added	Added
Encryption Overhead	Low	Higher
Communication Type	Host-to-Host	Gateway-to-Gateway / Host-to-Gateway
Security Level	Moderate	High
VPN Support	Limited	Excellent



Comparison of Transport and Tunnel Modes (4 marks)

AH vs ESP in Transport and Tunnel Modes

Protocol	Transport Mode	Tunnel Mode
AH	Authenticates payload and immutable fields of the IP header; no encryption.	Authenticates the entire original IP packet; no encryption.

4.	A large enterprise network needs to protect its internal resources from external threats. The security team plans to deploy: Packet Filtering Firewall at the perimeter, Stateful Inspection Firewall between internal segments, Application Proxy Firewall in front of critical servers. Iluustrate a secure enterprise network using these firewall techniques and justify the appropriate firewall deployment.	CO4	4B	K4
4 Ans	Definition and types (2 marks) A Firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predefined security rules. In an enterprise network, multiple firewall technologies are deployed together to provide layered security (Defense in Depth) against cyber threats. The three commonly used firewall types are: • Packet Filtering Firewall • Stateful Inspection Firewall • Application Proxy Firewall Diagram to show secure enterprise nerwork (3 marks)  Enterprise Network Design The enterprise network consists of: • Internet • Edge Router • Packet Filtering Firewall • DMZ (Web, Mail, DNS Servers) • Stateful Inspection Firewall • Internal LAN	CO4	4B	K4

ESP	Encrypts and optionally authenticates the payload only.	Encrypts and optionally authenticates the entire original IP packet; adds a new outer IP header.

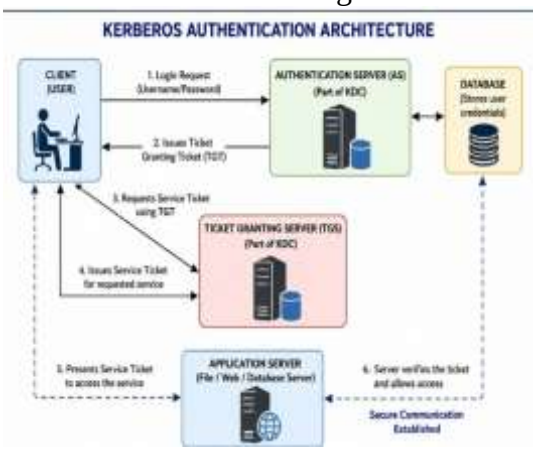
	• Application Proxy Firewall • Users and Internal Servers Types of Firewalls (5 marks) Packet Filtering Firewall Working Advantages Limitations Stateful Inspection Firewall Working Advantages Limitations Application Proxy Firewall Working Advantages Limitations Justification for appropriate firewall deployment. (3 marks) A secure enterprise network is best protected using a layered firewall architecture. A Packet Filtering Firewall at the network perimeter efficiently filters traffic based on basic rules, a Stateful Inspection Firewall verifies that packets belong to legitimate sessions before allowing access to the internal network, and an Application Proxy Firewall performs deep inspection and protects critical applications from advanced attacks. This multi-layered deployment provides strong confidentiality, integrity, availability, and comprehensive defense against modern cyber threats.			
5.	EduConnect University has 10,000 students and 1,000 faculty members. The university uses: Kerberos for single sign-on (SSO) to access email, LMS, and library services. RADIUS for Wi-Fi authentication (Eduroam) and VPN access. TACACS+ for network device administration. Analyze the working of Kerberos, RADIUS, and TACACS+. Compare their features for enterprise security. Justify why each protocol is used for its specific purpose.	CO4	4B	K4
5 Ans	Authentication protocols verify the identity of users and devices before granting access to network resources. Among the most widely used enterprise authentication protocols are Kerberos, RADIUS (Remote Authentication Dial-In User Service), and TACACS+ (Terminal Access Controller Access-Control System Plus). Each protocol has unique mechanisms, strengths, and deployment scenarios. Kerberos Authentication Protocol (4 marks) Definition Kerberos is a network authentication protocol that uses secret-key cryptography and a trusted third party called the Key Distribution Center (KDC) to provide secure authentication over insecure networks.	CO4	4B	K4

Components

- Client (User)
- Authentication Server (AS)
- Ticket Granting Server (TGS)
- Key Distribution Center (KDC = AS + TGS)
- Application Server (Service Server)

Step-by-Step Process

1. User enters username and password.
2. Client requests authentication from the Authentication Server (AS).
3. AS verifies credentials.
4. AS issues a Ticket Granting Ticket (TGT).
5. Client sends TGT to the Ticket Granting Server (TGS).
6. TGS verifies the TGT.
7. TGS provides a Service Ticket.
8. Client presents the Service Ticket to the application server.
9. Server validates the ticket.
10. Secure communication begins.



RADIUS Authentication Protocol (4 marks)

Definition

RADIUS is a centralized AAA (Authentication, Authorization, and Accounting) protocol commonly used for network access, VPNs, wireless LANs, and ISP authentication.

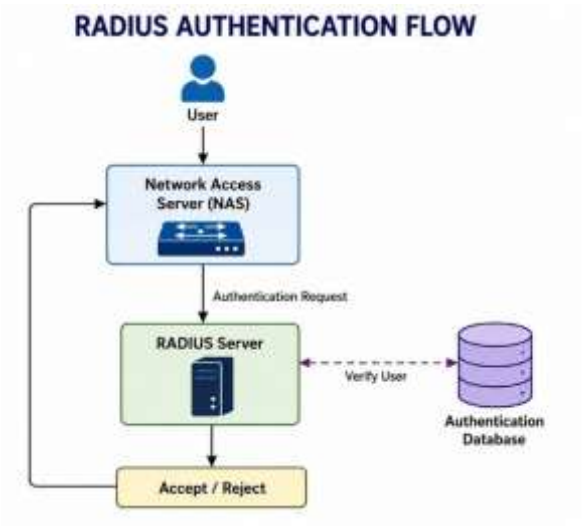
Components

- Client (Network Access Server)
- RADIUS Server
- Authentication Database

Step-by-Step Process

1. User requests network access.
2. NAS collects username and password.
3. NAS sends credentials to the RADIUS server.
4. RADIUS verifies credentials from the database.
5. Authentication decision is returned.

6. NAS grants or denies access.
7. Accounting information is logged.



TACACS+ Authentication Protocol (3 marks)

Definition

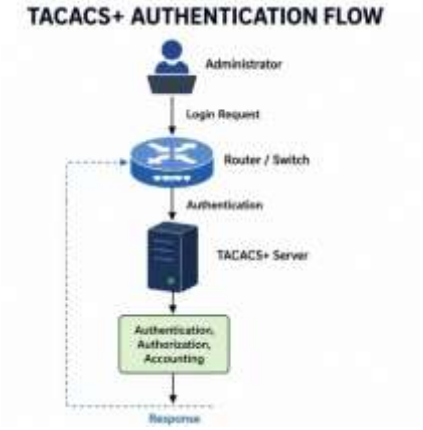
TACACS+ is a Cisco-developed AAA protocol primarily used for administrative access to routers, switches, and firewalls.

Components

- Administrator
- Network Device
- TACACS+ Server

Step-by-Step Process

1. Administrator logs into a network device.
2. Device forwards credentials to the TACACS+ server.
3. Server authenticates the administrator.
4. Authorization determines permitted commands.
5. Accounting logs all executed commands.
6. Access is granted based on privileges.



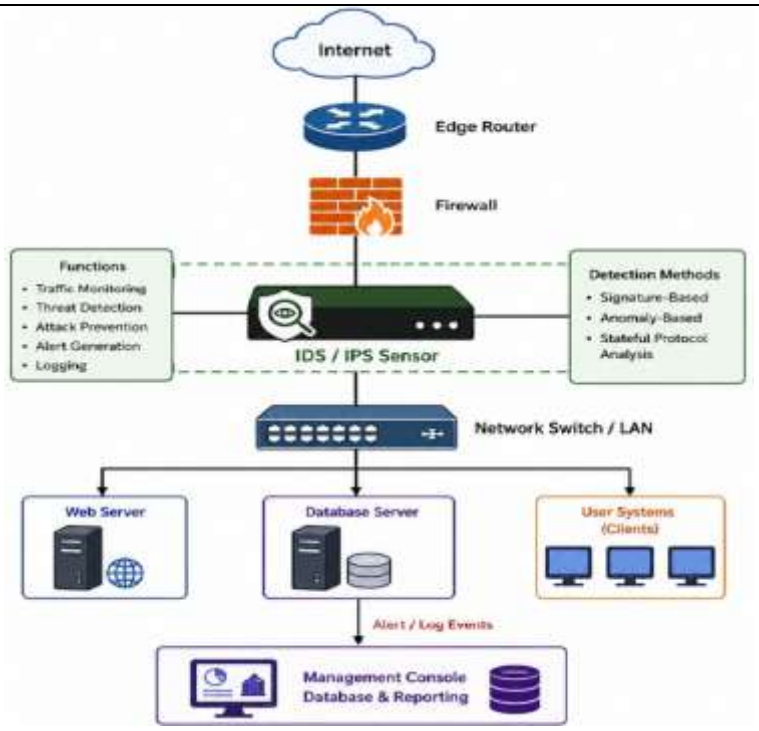
Enterprise Security Comparison (2 marks)

Aspect	Kerberos	RADIUS	TACACS+
Security Level	Very High	High	Very High
Ease of Deployment	Moderate	Easy	Moderate
Scalability	High	Very High	High
Administrative Control	Moderate	Moderate	Excellent
Wireless Authentication	No	Excellent	Limited
Device Management	Limited	Moderate	Excellent
Logging and Auditing	Moderate	Good	Excellent

6.	A metaverse company connects Physical Headquarters, Virtual Offices, and Remote Employees accessing via VR/AR. Sketch a VPN solution using MPLS VPN for Physical-Virtual office links, IPSec VPN for remote sites, and SSL VPN for employees and corporate partners. Justify your choices and provide an architecture diagram.	CO4	4B	K3
6 Ans	Need and diagram of secure VPN Architecture (3 marks) A Virtual Private Network (VPN) provides secure communication over public or private networks by ensuring confidentiality, integrity, authentication, and secure remote access. Large enterprises often use a combination of MPLS VPN, IPSec VPN, and SSL VPN to securely connect branch offices, data centers, cloud resources, and remote employees. Types of VPN (3 marks) MPLS VPN Purpose: Connects headquarters, branch offices, and data	CO4	4B	K3

	centers over a private service provider network. Features • Private WAN connectivity • High Quality of Service (QoS) • Low latency • Traffic isolation • Highly reliable IPSec VPN Purpose: Provides encrypted site-to-site communication over the public Internet. Features • AES encryption • Authentication using digital certificates or pre-shared keys • Data integrity using SHA • Tunnel mode • Anti-replay protection SSL VPN Purpose: Enables secure remote access for employees using web browsers or VPN clients. Features • Browser-based access • Multi-Factor Authentication (MFA) • TLS encryption • No dedicated hardware required on the client • Access control based on user roles Working of the Secure VPN Solution (3 Marks) Step 1: Branch Connectivity (MPLS VPN) • Branch offices connect to the service provider's MPLS cloud. • MPLS securely routes traffic between enterprise sites. • Business-critical applications receive prioritized bandwidth through QoS. Step 2: Site-to-Site Secure Communication (IPSec VPN) • IPSec gateways establish encrypted tunnels between enterprise locations over the Internet. • Data is encrypted, authenticated, and protected from interception. Step 3: Remote User Access (SSL VPN) • Remote employees connect securely to the SSL VPN gateway. • Users authenticate using credentials and MFA. • Encrypted TLS sessions provide secure access to enterprise applications. Step 4: Enterprise Firewall Protection • The firewall inspects incoming and outgoing traffic. • Access policies ensure only authorized users and devices can reach internal resources. Step 5: Secure Access to Data Center			

<table>
<tr>
<td></td>
<td>
<ul><li>Authenticated users access web, application, and database servers securely through the VPN infrastructure.</li></ul>
Comparison of VPN Technologies (2 mark)
<table>
<tr><th>Feature</th><th>MPLS VPN</th><th>IPSec VPN</th><th>SSL VPN</th></tr>
<tr><td>Network Type</td><td>Private WAN</td><td>Public Internet</td><td>Public Internet</td></tr>
<tr><td>Encryption</td><td>Optional</td><td>Strong</td><td>Strong</td></tr>
<tr><td>Remote Access</td><td>No</td><td>Limited</td><td>Yes</td></tr>
<tr><td>Site-to-Site Connectivity</td><td>Excellent</td><td>Excellent</td><td>Limited</td></tr>
<tr><td>Performance</td><td>Excellent</td><td>Good</td><td>Good</td></tr>
<tr><td>Quality of Service (QoS)</td><td>Excellent</td><td>Moderate</td><td>Moderate</td></tr>
<tr><td>Cost</td><td>High</td><td>Moderate</td><td>Low</td></tr>
<tr><td>Best Use</td><td>Branch-to-Branch Connectivity</td><td>Secure Site-to-Site Communication</td><td>Secure Remote User Access</td></tr>
</table>
Justification (2 Mark)
A hybrid VPN architecture combining MPLS VPN, IPSec VPN, and SSL VPN provides a comprehensive enterprise connectivity solution. This integrated design offers high security, scalability, performance, and flexibility, making it well suited for modern enterprise environments.
</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>Analyze the architecture and operation of Intrusion Detection and Prevention Systems (IDS/IPS) and evaluate their role in protecting modern networks.</td>
<td>CO4</td>
<td>4B</td>
<td>K4</td>
</tr>
<tr>
<td>7 Ans</td>
<td>Need for Intrusion Detection and Prevention Systems (IDS/IPS) and diagram (4 marks)
An Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS) are essential components of modern network security. They monitor network traffic and system activities to identify malicious behavior, unauthorized access, and security policy violations. While an IDS detects and alerts administrators about potential threats, an IPS detects, blocks, and prevents attacks in real time, providing proactive protection against cyber threats.</td>
<td>CO4</td>
<td>4B</td>
<td>K4</td>
</tr>
</table>



Components of IDS/IPS

1. Traffic Sensor

2. Analysis Engine

3. Signature Database

4. Management Console

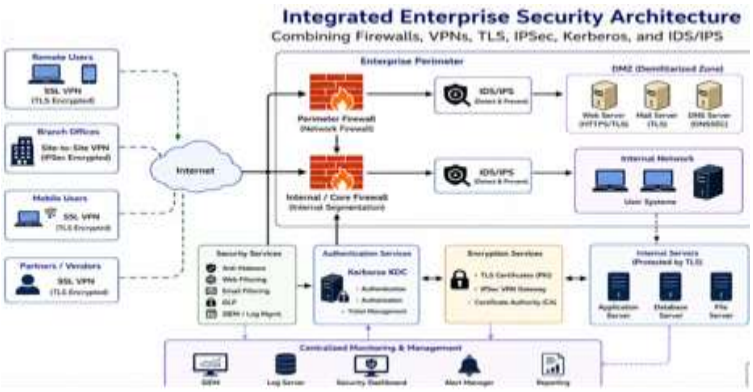
5. Response Module (IPS)

Operation of IDS (3 marks)

Working Process

1. Network traffic is mirrored to the IDS sensor.
2. IDS captures and analyzes packets.
3. Traffic is compared against attack signatures and anomaly profiles.
4. If suspicious activity is detected:
    - An alert is generated.
    - Logs are stored.
    - Security administrators are notified.
5. Legitimate traffic continues without interruption.

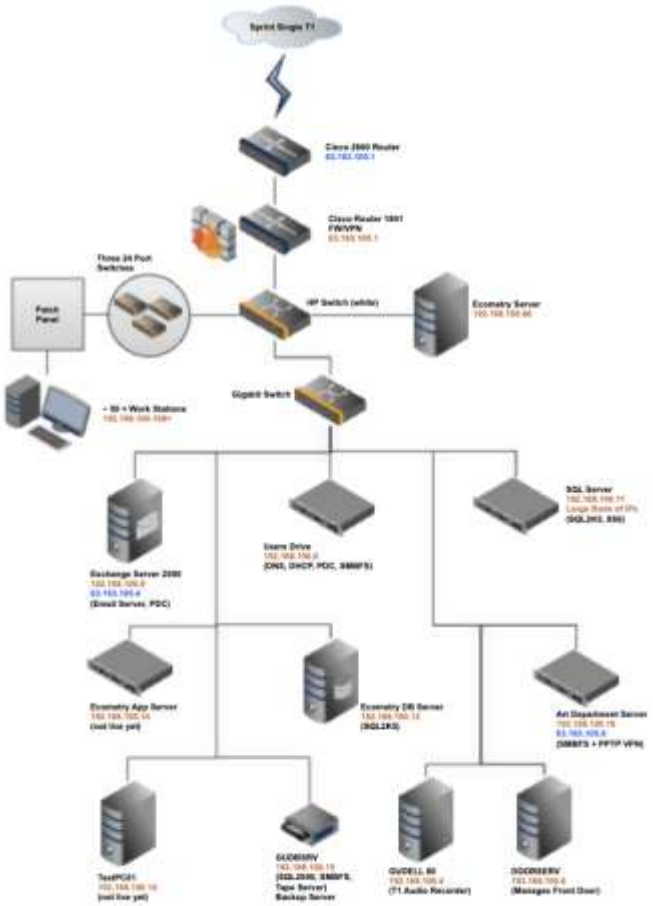
	Characteristics
	
	• Passive monitoring.
	• Does not block attacks.
	• Generates alerts for further investigation.
	
	Operation of IPS (3 Marks)
	
	Working Process
	
	1. Network traffic passes through the IPS.
	2. IPS inspects every packet in real time.
	3. Malicious traffic is detected using signatures, anomaly detection, or policy rules.
	4. IPS immediately:
	  o Drops malicious packets.
	  o Blocks attacker IP addresses.
	  o Terminates malicious sessions.
	  o Updates firewall rules if configured.
	5. Legitimate traffic is forwarded to the destination.
	
	Characteristics
	
	• Active protection.
	• Prevents attacks automatically.
	• Operates inline with network traffic.
	
	Detection Techniques
	
	1. Signature-Based Detection
	2. Anomaly-Based Detection
	3. Stateful Protocol Analysis
	Role of IDS/IPS in Protecting Modern Networks (3 marks)
	IDS and IPS play a vital role in securing enterprise networks by:
	
	• Detecting malware, ransomware, and advanced persistent threats (APTs).
	• Preventing unauthorized access and intrusion attempts.
	• Protecting web applications, cloud services, and data centers.
	• Supporting regulatory compliance through logging and auditing.
	• Monitoring internal and external network traffic.
	• Reducing the impact of Distributed Denial-of-Service (DDoS) attacks.
	• Providing real-time threat detection and automated response.			

	• Enhancing security in cloud, IoT, wireless, and hybrid network environments.			
8.	After Cyber-attack, survivors have a network with a Central Bunker, Camps, Mobile Units, Scouts, and Allies using solar-satellite links (intermittent, low bandwidth). Sketch a security architecture using Firewalls, VPNs, TLS, IPSec, Kerberos, and IDS/IPS to secure communication, authenticate users, and detect attacks. Justify each component's placement and explain how they work together.	CO4	4B	K4
8 Ans	Need for an Integrated Enterprise Security Architecture with diagram (4 marks) Integrated Enterprise Security Architecture combines multiple security technologies to provide defense-in-depth, ensuring confidentiality, integrity, authentication, availability, and continuous monitoring. By integrating Firewalls, VPNs, TLS, IPSec, Kerberos, and IDS/IPS, enterprises can protect users, applications, and data from both external and internal threats while enabling secure communication across distributed environments.  Components of the Architecture (4 Marks) 1. Perimeter Firewall 2. Virtual Private Network (VPN) 3. Transport Layer Security (TLS) 4. IPSec 5. Kerberos Authentication Server 6. Intrusion Detection and Prevention System (IDS/IPS) 7. DMZ (Demilitarized Zone) 8. Internal Enterprise Network 9. SIEM (Security Information and Event Management) Working of the Integrated Security Architecture (3 Marks)	CO4	4B	K4

	Step 1: Secure Remote Access • Remote users connect through an SSL VPN using encrypted TLS communication. Step 2: Secure Branch Connectivity • Branch offices establish secure IPSec VPN tunnels with headquarters for encrypted site-to-site communication. Step 3: Firewall Protection • The perimeter firewall filters and permits only authorized traffic. • Internal firewalls segment the enterprise network and restrict unauthorized lateral movement. Step 4: Threat Detection • IDS/IPS continuously inspects traffic. • Malicious packets are detected, logged, and blocked (IPS). Step 5: User Authentication • Users authenticate through the Kerberos Key Distribution Center (KDC). • Ticket-based authentication provides secure access and supports Single Sign-On (SSO). Step 6: Secure Communication • Internal and external application traffic is protected using TLS. • Site-to-site traffic remains encrypted using IPSec. Step 7: Monitoring and Incident Response • Logs from firewalls, VPNs, IDS/IPS, and servers are collected by the SIEM platform. • Security teams monitor alerts and respond to incidents in real time. Security Features (2 Marks) • Multi-layered (Defense-in-Depth) security. • Strong user authentication using Kerberos. • Encrypted remote access through SSL VPN. • Secure site-to-site communication using IPSec VPN. • TLS-secured application and web communication. • Network segmentation using firewalls. • Real-time intrusion detection and prevention. • Centralized logging, monitoring, and incident management.			

Part- C

Q.No	Questions	CO's	Unit	Bloom's Level
1.	MediLink is a global telemedicine platform that connects patients, doctors, hospitals, and diagnostic labs across 20 countries. The network handles sensitive medical data,	CO4	4C	K5

	including electronic health records (EHR), diagnostic images, and real-time video consultations. Analyze and evaluate the suitability of Kerberos, RADIUS, TACACS+, MPLS VPN, SSL VPN, IPSec VPN, and IDS/IPS. Design and justify a secure enterprise network architecture.			
1 Ans	1. Introduction (2 Marks) A multi-campus university requires a secure, scalable, and highly available network to support students, faculty, administrative staff, research laboratories, and remote learners. The network must ensure secure authentication, encrypted communication, role-based access control, and continuous monitoring against cyber threats. An integrated security architecture using authentication protocols, VPN technologies, and IDS/IPS provides a reliable solution. 2.Enterprise Network Architecture (4 Marks)  3..Authentication Protocols (3 Marks) Authentication protocols verify user identities before	CO4	4C	K5

<table>
<tr>
<td></td>
<td>granting access to university resources.

a) Kerberos,b) RADIUS,c) TACACS+

4.VPN Technologies (2 Marks)
a) MPLS VPN

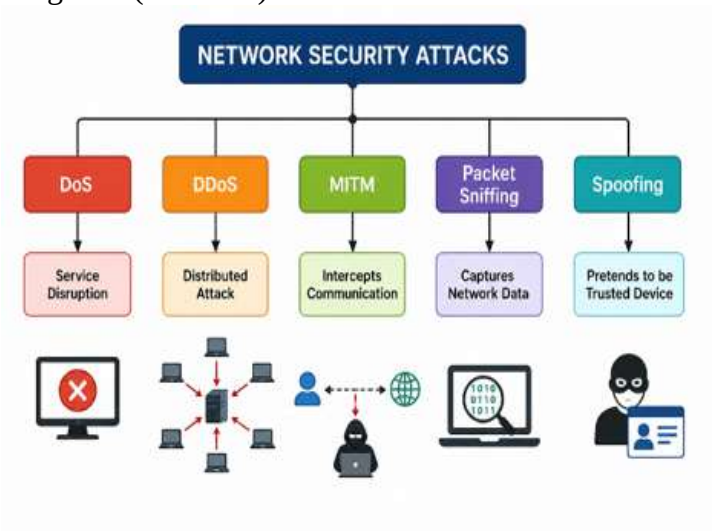
b) SSL VPN

c) IPSec VPN

5.Intrusion Detection and Prevention Systems (IDS/IPS) (2 Marks)
Intrusion Detection System (IDS)

Intrusion Prevention System (IPS)

6.Evaluation : (2 Marks)
<table>
<tr><td>Feature</td><td>MPLS VPN</td><td>SSL VPN</td><td>IPSec VPN</td></tr>
<tr><td>Connection Type</td><td>Site-to-Site</td><td>Remote Access</td><td>Site-to-Site & Remote Access</td></tr>
<tr><td>Security</td><td>Service-provider isolation</td><td>SSL/TLS encryption</td><td>IPSec encryption (AH & ESP)</td></tr>
<tr><td>Performance</td><td>Very High</td><td>Moderate</td><td>High</td></tr>
<tr><td>Browser Access</td><td>No</td><td>Yes</td><td>No (usually requires VPN client)</td></tr>
<tr><td>Best Application</td><td>Inter-campus connectivity</td><td>Remote students and faculty</td><td>Secure branch communication</td></tr>
<tr><td>Deployment Cost</td><td>High</td><td>Low</td><td>Moderate</td></tr>
</table>
</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Evaluate the effectiveness of modern network security mechanisms in protecting enterprise networks against cyber attacks. In your answer, analyze network attacks (DoS, DDoS, MITM, sniffing, and spoofing), secure transport protocols (TLS/SSL and IPSec), and firewall technologies (Packet Filtering, Stateful Inspection, and Application-layer Proxy Firewalls).</td>
<td>CO4</td>
<td>4C</td>
<td>K5</td>
</tr>
</table>

2 Ans	Importance of network security and enterprise threats (2 Marks) Network Attacks: DoS, DDoS, MITM, Sniffing, and Spoofing (working, impact) Diagrams (4 Marks)  Comparative Analysis of Security Mechanisms secure transport protocols (TLS/SSL and IPSec), and fire wall technologies (Packet Filtering, Stateful Inspection, and Application-layer Proxy Firewalls). (4 marks) **Evaluation of Effectiveness (3 marks)** Modern network security mechanisms are highly effective when implemented together as a **layered security architecture**. **TLS/SSL** secures application-layer communications, **IPSec** protects network-layer traffic and VPN connections, while **Packet Filtering**, **Stateful Inspection**, and **Application-layer Proxy Firewalls** provide complementary levels of traffic inspection and access control. Although advanced attacks such as **DDoS** and sophisticated **MITM** techniques still pose challenges, integrating these mechanisms with **Intrusion Detection/Prevention Systems (IDS/IPS), endpoint protection, strong authentication, and continuous monitoring** provides comprehensive protection for enterprise networks.	CO4	4C	K5

Unit- 5

Part A

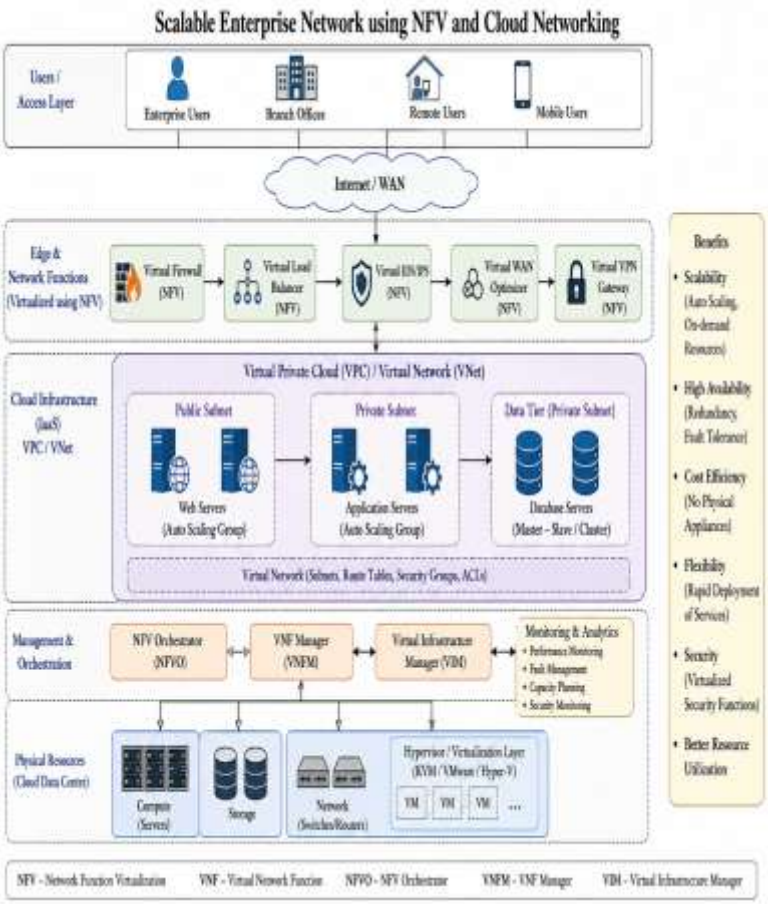
Q.No	Questions	CO's	Unit	Bloom's Level
1.	A telecom company wants to replace its expensive hardware-based network devices with virtualized software	CO5	5A	K1

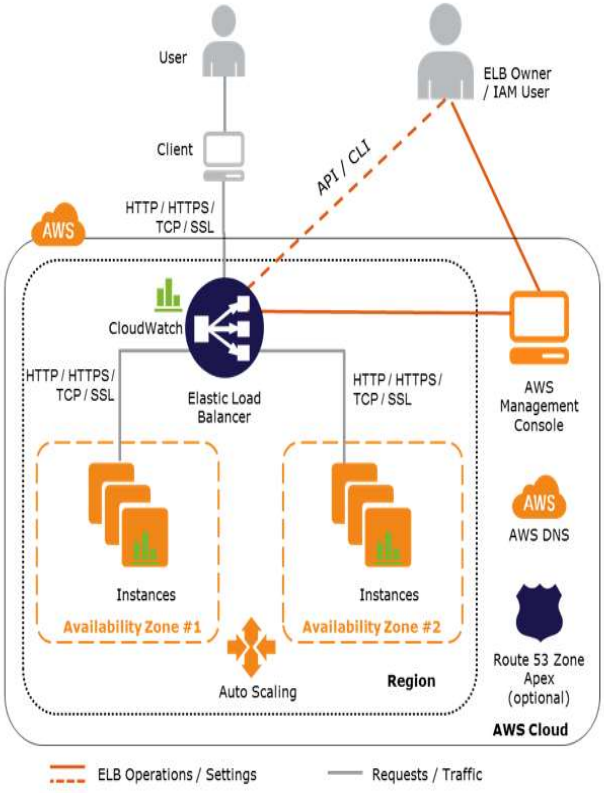
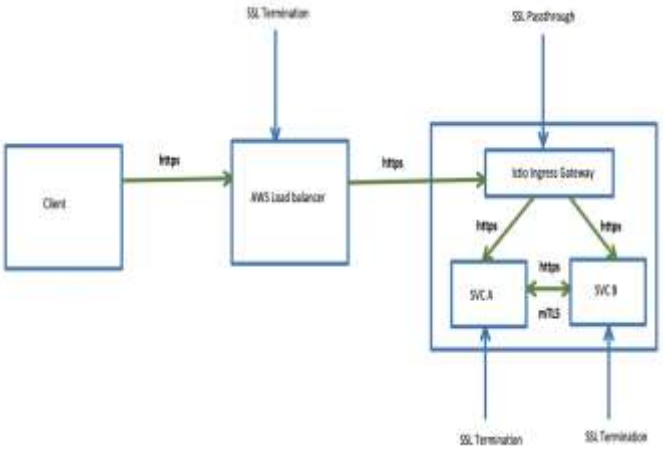
	running on standard servers. How will you achieve.			
1 Ans	NFV virtualizes network services such as firewalls and routers to run on software instead of dedicated hardware.	CO5	5A	K1
2.	A company is migrating its IT infrastructure from on-premises data centers to the cloud. The network team needs to understand how networking works in the cloud. State which network to follow.	CO5	5A	K1
2 Ans	Cloud networking is the use of cloud infrastructure to deliver and manage network services over the internet.	CO5	5A	K1
3.	Distinguish between load balancing and auto-scaling in cloud environments. Explain how they differ in purpose and function.	CO5	5A	K1
3 Ans	Load balancing distributes traffic across servers, while auto-scaling adjusts the number of servers based on demand.	CO5	5A	K1
4.	A company is migrating from traditional hardware-based networking to virtual networking. The network team needs to present the benefits to management. List any five benefits of virtual networking.	CO5	5A	K1
4 Ans	Scalability, cost efficiency, resource optimization, fast recovery and flexibility.	CO5	5A	K1
5.	Interpret the role of network slicing in 5G — what it is and why it is important.	CO5	5A	K2
5 Ans	It enables multiple virtual networks to run on a single physical infrastructure for different applications.	CO5	5A	K2
6.	An e-commerce website experiences high traffic during flash sales. To prevent servers from crashing, the company uses a load balancer .Describe its function.	CO5	5A	K1
6 Ans	To distribute traffic evenly across servers to improve performance and reliability.	CO5	5A	K1
7.	Describe the function of auto-scaling — why is it used in cloud environments?	CO5	5A	K1
7 Ans	Auto-scaling automatically increases or decreases computing resources based on workload demand.	CO5	5A	K1
8.	Name any two platforms that support cloud networking and state their purpose.	CO5	5A	K1
8 Ans	AWS and Microsoft Azure are cloud computing platforms that provide virtual networking services, allowing users to build, manage, and scale network infrastructure over the internet.	CO5	5A	K1
9.	Summarize the key features of 5G architecture — what are its main characteristics?	CO5	5A	K1
9 Ans	5G architecture supports high-speed, low-latency communication and massive connectivity.	CO5	5A	K1
10.	List any two advantages of Network Function Virtualization (NFV) and briefly explain each.	CO5	5A	K1

10 Ans	• Reduced hardware cost – Minimizes dependency on dedicated network devices. • Scalability – Network functions can be easily scaled based on demand.	CO5	5A	K1
11.	Classify the cloud deployment models — what are the different types of cloud deployment and how do they differ?	CO5	5A	K1
11 Ans	Public cloud, Private cloud, Hybrid cloud.	CO5	5A	K1
12.	State the main goal of virtual networking and briefly explain its purpose.	CO5	5A	K1
12 Ans	To create network resources using software instead of physical hardware.	CO5	5A	K1
13.	How does load balancing work in cloud networking? Briefly explain its function.	CO5	5A	K1
13 Ans	The process of distributing incoming network traffic across multiple servers (or resources) to ensure no single server is overwhelmed, improving performance, availability, and reliability.	CO5	5A	K1
14.	Mention any two features of 5G networks and briefly explain each.	CO5	5A	K1
14 Ans	High data speed – Enables ultra-fast data transmission. Low latency – Provides very minimal delay in communication.	CO5	5A	K1
15.	A large telecommunications company needs to find the most efficient routes for data packets across its complex network. Traditional routing algorithms struggle with the network's size and dynamic conditions. How do genetic algorithms help find optimal routes in this scenario?	CO5	5A	K2
15 Ans	They optimize routing paths using evolutionary techniques to find efficient solutions.	CO5	5A	K2

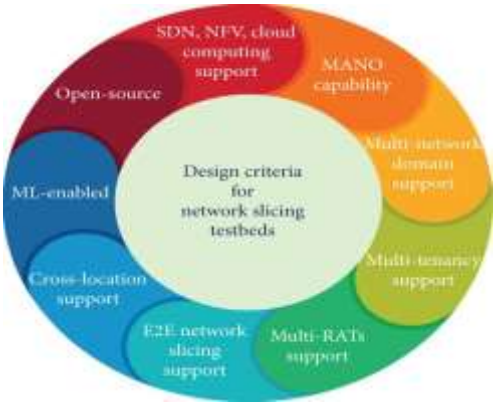
Part B

Q.No	Questions	CO's	Unit	Bloom's Level
1	A growing enterprise with unpredictable traffic patterns wants to migrate from hardware-based networking to NFV and cloud networking to achieve scalability, cost savings, and agility. Devise a scalable enterprise network using NFV and cloud networking concepts. Justify your choices.	CO5	5B	K4
1.ans	Basics (2 Marks) Definition of Network Function Virtualization (NFV) Definition of Cloud Networking Need for scalable enterprise networks	CO5	5B	K4

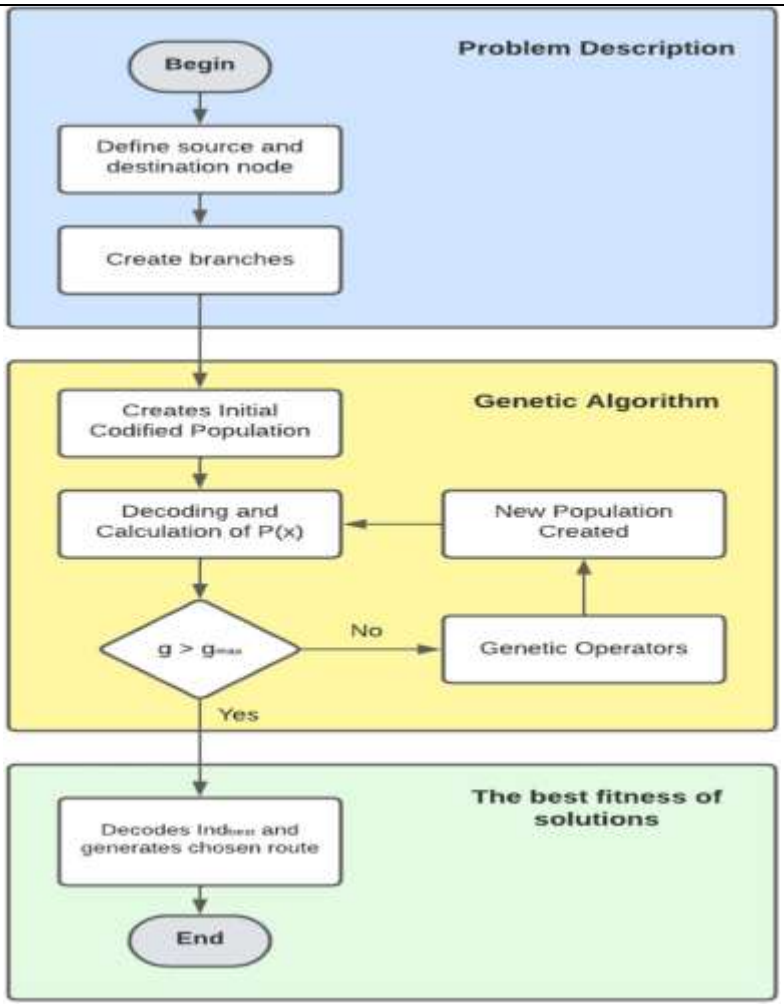
	Diagram (5 Marks)  **Explanation (4 Marks)** • NFV virtualizes routers, firewalls and gateways. • Cloud networking hosts VNFs in virtual machines. • Auto Scaling adds/removes servers automatically. • Load Balancer distributes traffic evenly. • VPC isolates enterprise resources. • SDN controller manages virtual resources. **Justification (2 Marks)** • Reduces hardware cost. • High scalability and availability. • Faster deployment. • Efficient resource utilization.			
2	"FinSecure" is a financial services company that processes thousands of transactions per second. The application uses: AWS Virtual Networking for secure, isolated network environments.	CO5	5B	K3

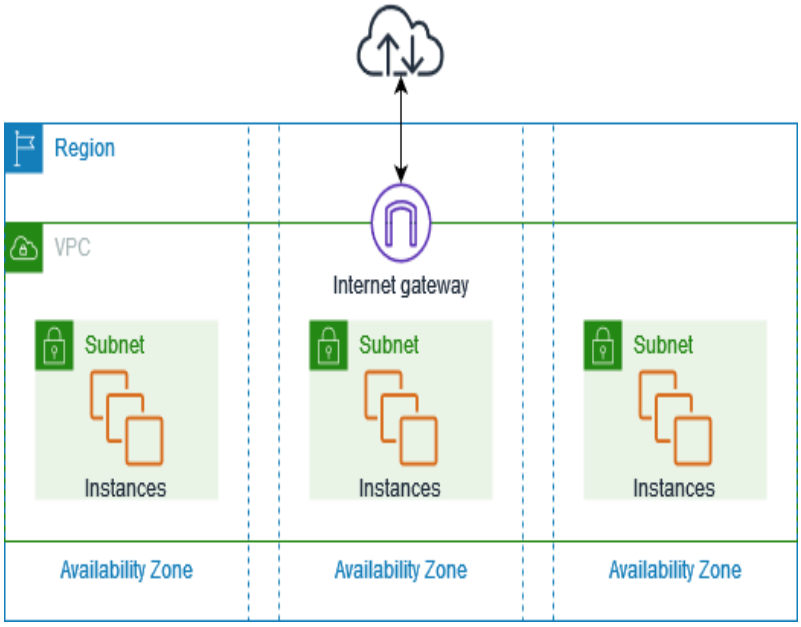
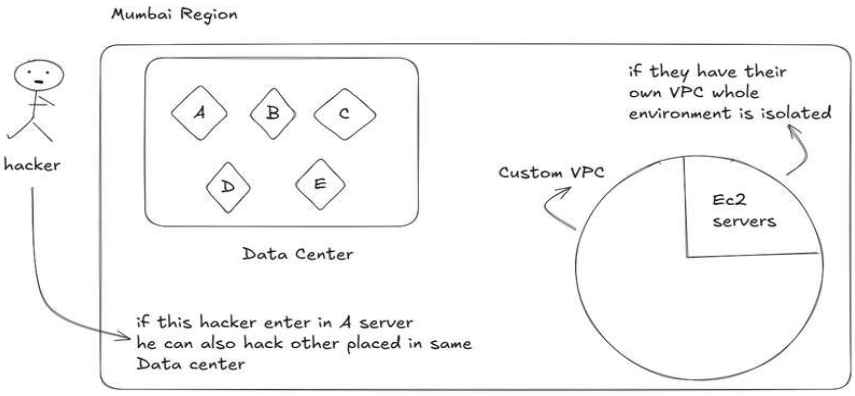
	Azure Load Balancing for global traffic distribution and failover. Analyze the role of AWS Virtual Networking and Azure Load Balancing in FinSecure's cloud infrastructure. How do they ensure low latency, security, and high availability?			
2.Ans	**A. Basics (2 Marks)** • AWS Virtual Private Cloud (VPC) • Azure Load Balancer • Purpose of cloud networking **B. Diagram (5 Marks)**   	CO5	5B	K3

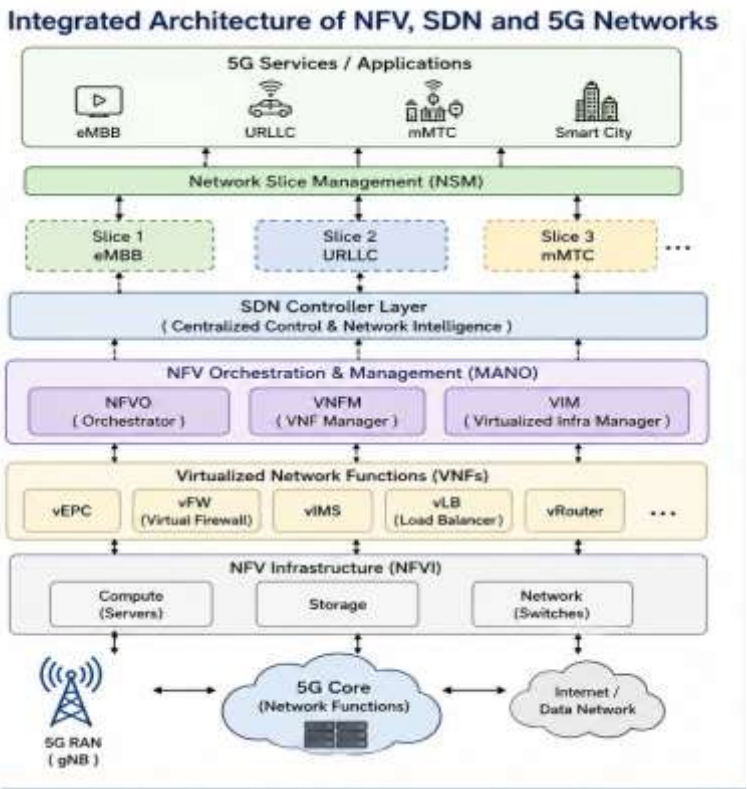
	C. Explanation (4 Marks) • VPC provides network isolation. • Public/private subnet implementation. • Route tables manage packet forwarding. • Security Groups secure resources. • Azure Load Balancer distributes traffic. • Health probes detect server failures. **D. Justification (2 Marks)** • Improved availability. • Better security. • High fault tolerance. • Efficient workload distribution.			
3	A telecom operator uses 5G, NFV, and Network Slicing to offer differentiated services: eMBB (high bandwidth), URLLC (ultra-low latency), mMTC (massive IoT). Sketch a 5G-enabled cloud architecture integrating NFV and Network Slicing. Justify your design choices.	CO5	5B	K3
3.Ans	A. Basics (2 Marks) 5G architecture NFV Network slicing B. Diagram (4 Marks)	CO5	5B	K3

	   **C. Explanation (5 Marks)** i. RAN connects users. ii. 5G Core manages sessions. iii. NFV virtualizes network functions. iv. SDN controls routing. v. Network slicing creates logical networks. vi. Edge computing reduces latency. **D. Justification (2 Marks)** i. Low latency. ii. Flexible resource allocation. iii. Supports multiple applications. iv. Better QoS.			
4.	Analyze the Effectiveness of Genetic Algorithm-Based Routing Compared to Conventional Routing Protocols	CO5	5B	K4

<table>
<tr>
<td>4.Ans</td>
<td>
1. Mechanisms: (3 marks)
<ul>
<li>How Routing Protocols Operate
<ol>
<li>Conventional Routing Protocols</li>
<li>GA-Based Routing</li>
</ol>
</li>
<li>Selection</li>
<li>Crossover</li>
<li>Mutation</li>
</ul>
2. Comparative Analysis:
GA vs. Conventional Protocols (3 Marks)
<table>
<tr><th>Genetic Algorithm</th><th>Conventional Routing</th></tr>
<tr><td>Evolution-based</td><td>Fixed algorithms</td></tr>
<tr><td>Global optimization</td><td>Local optimization</td></tr>
<tr><td>Better load balancing</td><td>Limited optimization</td></tr>
<tr><td>Computationally intensive</td><td>Faster execution</td></tr>
</table>
3.Diagram (3m)
</td>
<td>CO5</td>
<td>5B</td>
<td>K4</td>
</tr>
</table>

	 **4.Advantages (2 m)** • Reduced congestion • Better QoS • Adaptive routing • Multiple path discovery **5.Limitations (2 M)** • Higher computation time Complex implementation			
5	Develope a cloud-based network using AWS VPC and Azure Load Balancer to ensure high availability, fault tolerance, and scalability. Analyze how your design handles: Traffic distribution, Failover and disaster recovery, Security and compliance, Justify your architectural choices.	CO5	5B	K4

5.Ans	1.Definition (2 Marks) 2.Diagram (4 marks) The following diagram shows an example VPC. The VPC has one subnet in each of the Availability Zones in the Region, EC2 instances in each subnet, and an internet gateway to allow communication between the resources in your VPC and the internet.  3.Steps to Configure the Azure Standard Load Balancer (5 Marks) Step 1: Design the AWS Core Network Infrastructure. Step 2: Establish Cross-Cloud Private Connectivity Step 3: Deploy Load Balancer. 4.Example Diagram (2 Marks)  	CO5	5B	K4

6	Analyse the integrated architecture of NFV, SDN, and 5G networks, and evaluate their roles in enabling intelligent, programmable, and scalable next-generation communication systems with a suitable diagram.	CO5	5B	K4
6.Ans	• Basics (2 Marks) NFV, SDN, and 5G networks • Comparison Diagram (4 Marks)  • **Explanation (2 Marks)** **Comparison of NFV, SDN, and 5G Architecture (5 Marks)**	CO5	5B	K4

Parameter	**NFV (Network Function Virtualization)**	**SDN (Software Defined Networking)**	**5G Architecture**
1. Primary Objective	Virtualizes network functions	Centralizes network control	Provides next-generation mobile communicatio

				n
2. Main Function	Replaces hardware appliances with Virtual Network Functions (VNFs)	Separates the control plane from the data plane	Delivers high-speed, low-latency, and massive connectivity
3. Core Component	VNFs, NFVI, MANO	SDN Controller, OpenFlow-enabled switches	5G Core (5GC), gNB, Network Slicing
4. Resource Manageme nt	Virtualizes and allocates computing resources	Dynamicall y controls traffic flow	Allocates resources through network slices
5. Scalability	Supports rapid scaling of virtual network functions	Enables flexible network expansion through centralized control	Supports millions of connected devices and services
6. Cost Efficiency	Reduces hardware and operational costs	Simplifies network managemen t and reduces maintenanc e costs	Improves spectrum and infrastructure utilization
7. Quality of Service (QoS)	Optimizes service deployment and resource utilization	Enables intelligent traffic engineering and policy control	Provides customized QoS for eMBB, URLLC, and mMTC services

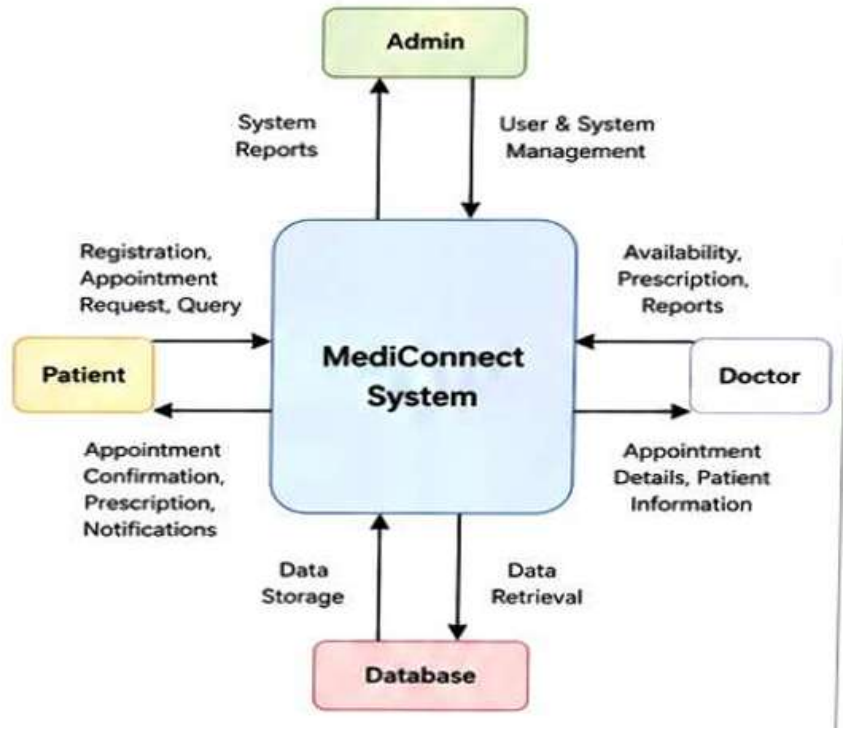
	8. Role in Integrated Architecture	Virtualizes network services	Controls and manages network traffic	Combines NFV and SDN to deliver intelligent, scalable, and low-latency communication services			
7	Articulate a congestion control mechanism for a cloud data center network using Genetic Algorithm optimization. Explain each phase of the Genetic Algorithm and analyse how it minimizes congestion, improves load balancing, enhances bandwidth utilization, and reduces packet delay with a suitable architecture diagram.				CO5	5B	K3
7.Ans	**A. Introduction (2 Marks)** • A **Genetic Algorithm (GA)** is a bio-inspired optimization technique based on Darwin's theory of natural selection. • In cloud data center networks, GA is used to identify the **optimal routing path** by minimizing congestion and maximizing network resource utilization. • It continuously searches for the best route using evolutionary operations such as **selection, crossover, and mutation**. B. Architecture Diagram (4 Marks) C. Phases of Genetic Algorithm (5 Marks) a. Population Initialization b. Fitness Evaluation c. Selection d. Crossover e. Mutation f. Termination and Best Route Selection **D. Performance Analysis and Advantages (2 Marks)** **Congestion Reduction** • Distributes traffic over multiple paths. • Prevents bottlenecks and network overload.				CO5	5B	K3

	Load Balancing • Evenly allocates traffic across servers and network links. • Improves utilization of available resources. **Bandwidth Utilization** • Selects routes with higher available bandwidth. • Reduces idle network resources. **Packet Delay Reduction** • Chooses the shortest and least congested paths. • Minimizes end-to-end transmission delay. **QoS Improvement** • Enhances throughput. • Increases Packet Delivery Ratio (PDR). • Reduces packet loss and jitter.			
8	"MediConnect" is a telemedicine platform offering: Remote surgery, Video consultations, Patient monitoring. The platform uses NFV to virtualize network functions and Network Slicing to create dedicated slices for each service. Discover a 5G-enabled cloud architecture integrating NFV and Network Slicing for "MediConnect". Explain how your design meets the diverse requirements of remote surgery, video consultations, and patient monitoring.	CO5	5B	K3
8.Ans	Overview of Key Concepts: (4 Marks)			

Concept	Description			
5G	Fifth-generation mobile network offering high data rates (20 Gbps), ultra-low latency (1 ms), and massive connectivity (1M devices/km²) .	CO5	5B	K3
NFV (Network Function Virtualization)	Virtualizes network functions (firewalls, routers, load balancers) as software (VNFs) running on standard servers — enabling flexibility, cost savings, and rapid deployment.			
Network	Creates multiple virtual networks (slices) on a shared physical 5G			

Slicing	infrastructure — each slice optimized for specific service requirements (e.g., low latency, high bandwidth, massive connectivity).				
Cloud Architecture	Uses cloud resources (AWS/Azure/GCP) for compute, storage, and networking — integrated with 5G RAN (Radio Access Network) and core network.				

Design diagram for MediConnect: (4 Marks)



How NFV and Network Slicing Work Together (5 Marks)

Step	NFV Role	Network Slicing Role
1. Resource Pooling	NFV virtualizes hardware resources (compute, storage, networking).	Slices are created on the shared NFV infrastructure.
2. Service Creation	VNFs (firewalls, routers, LBs) are deployed as software.	Each slice gets dedicated VNFs and resources.

	3. Isolation	NFV provides resource isolation.	Slices are logically isolated — traffic from one slice does not affect others.			
	4. Scaling	VNFs are scaled up/down based on demand.	Slices can be scaled independently.			
	5. Manageme nt	NFV MANO (Management and Orchestration) manages VNFs.	Network slicing management defines and manages slices.			

Part C

Q.No	**Questions**	**CO's**	**Unit**	**Bloom's Level**
1.	Evaluate the role of Network Function Virtualization (NFV) in modern network infrastructure. Compare it with traditional hardware-based networking in terms of scalability, cost, flexibility, and performance.	CO5	5C	K5
1.Ans	Overview of Network Function Virtualization (2 Marks) Network Function Virtualization Architecture (3 Marks) Components of NFV and working (4 marks) ● NFVI (Network Functions Virtualization Infrastructure) ● VNFs (Virtual Network Functions) ● MANO (Management and Orchestration) Comparison – NFV with Traditional Hardware-based networking(5 marks)	CO5	5C	K5
2.	Evaluate and compare the Spine-Leaf architecture with the traditional Three-Tier Data Center architecture. Which architecture is more suitable for cloud data centers? Justify.	CO5	5C	K5
2 Ans	Overview of Spine-Leaf Architecture (3 Marks) ● Definition of Data Center Network Architecture ● Traditional Three-Tier Architecture ● Spine-Leaf Architecture	CO5	5C	K5

	● Performance Comparison ● Cloud Data Center Suitability Spine -Leaf Architecture (2 Marks) Three-Tier Data Center Architecture (2 Marks) Comparison (5 Marks) Justification (2 Marks)			