SET-D
Answer all the Questions
(2 x 25 = 50 Marks)

Instructions: Answer the questions

Ql. No	Question	Marks
1	ABC Ltd. has its headquarters in Delhi along with regional branch offices in Mumbai, Chennai, Kolkata and Bangalore. The Delhi headquarters has 2500 employees, Mumbai - 1500 employees, Chennai - 1000 employees, Kolkata - 800 employees and Bangalore - 600 employees. Each office has various departments like Sales, Marketing, IT, Accounts, HR etc. Answer the following Questions: **a. Design an efficient IPv6 addressing plan to allocate addresses to various departments in each office location. Explain your strategy.** • Use a /48 prefix for the entire organization • Divide into /56 subnets for each office location • Further divide /56 into /64 subnetworks for each department in that office • This allows 256 subnets per office location, enough for current departments and future growth • Keeps prefixes aggregatable for efficient routing • Use IP address management tool to allocate and track addresses	15
	b. The organization has existing IPv4 infrastructure and networking devices. Recommend a suitable transition mechanism to migrate to IPv6 while keeping existing IPv4 communication intact. Explain how your recommended mechanism works. • Use dual-stack approach - run IPv4 and IPv6 in parallel • Configure devices as dual-stack to support both protocols • Tunnel IPv6 traffic over existing IPv4 network using techniques like 6in4, 6to4 etc. • This allows direct IPv6 communication between dual-stack devices on local networks • Tunneling encapsulates IPv6 packets over IPv4 between offices across WAN • Gradually expand IPv6 deployment as devices and apps become compatible	5
	c. The Bangalore office uses NAT for IPv4 address conservation. Explain how NAT64 can help translate IPv4 and IPv6 addresses during the transition phase. • NAT64 allows IPv6 only clients to connect with IPv4 servers • It translates IPv6 addresses to IPv4 and vice versa for end to end communication	5

	• Bangalore office can deploy NAT64 gateway device • Internal network remains IPv6, external communication gets translated • DNS64 resolves IPv4 addresses and NAT64 converts them to IPv6 • Gradual phase out of NAT64 as migration completes over time.	
	(OR)	
2.	XYZ Corp is a large multinational organization that has recently deployed IPv6 addressing for its enterprise network. As a network engineer at XYZ Corp, design and implement mobility solutions over the IPv6 infrastructure. Answer the following Questions: **a. XYZ Corp wants seamless mobility for employees moving across different networks and locations. Recommend which IPv6 mobility protocol would work best and justify your recommendation.** • PMIPv6 provides network-based mobility management without host involvement • The mobile node retain its IP address while moving across networks • Local Proxy Mobility Agent manages mobility on behalf of mobile node • Centralized control, no specialized client software required on hosts • Suited for large enterprise networks like XYZ Corp	10
	b. Demonstrate the working of Proxy Mobile IPv6 by explaining the sequence of steps involved when an employee moves from office WiFi to cellular LTE network. • Mobile node connected to home network, assigned IP home address • MN moves and attaches to visited network. LMA notified. • LMA assigns IP care-of-address to MN and updates binding cache. • Bi-directional tunnel established between LMA and MAG. • Packets redirected between LMA and MAG transparently using tunnel. • MN uses same IP home address despite network change. • Process repeats seamlessly as MN moves across different networks.	10
	c. Discuss two additional mechanisms like Multihoming and Site Multihoming proxy (SMPY) that can enhance mobility support in an enterprise IPv6 network. • Multihoming - host configured with multiple IP addresses for reliability • If one interface fails, session continues on other interface • SMPY - Local proxy agents manage mobility between sites • Load balancing, optimizes paths between distributed sites • Enhances enterprise mobility across multiple locations	5

3 .	Rahul is the principal network architect at Nexus Telecom that is upgrading from Frame Relay to modern broadband connectivity. The CEO has asked Rahul to submit a comprehensive technology migration report. **a. (i) Based on Nexus Telecom's needs to connect data centers and regional offices across long distances, recommend with justified arguments which broadband technology would be most suitable.** • Nexus has long distance connectivity needs between data centers and regional offices • Metro Ethernet provides high speed dedicated point-to-point connections up to 100 km • Offers scalable bandwidth from 1 Mbps to 10 Gbps based on needs • Provides secure Layer 2 connectivity over fiber avoiding public internet • Metro Ethernet meets enterprise grade WAN needs of Nexus Telecom **(ii) Investigate the role of PPPoE and PPPoA encapsulation protocols in transporting DSL traffic efficiently over Ethernet LAN infrastructure.** • PPPoE - Used for authenticating and transporting IP packets of DSL subscribers over Ethernet LAN. • Encapsulates PPP frames in Ethernet frames, allowing DSL transmission over Ethernet. • PPPoA - Used for ATM infrastructure, encapsulates PPP frames in ATM cells. • Provides authentication and transport of IP traffic from DSL modem to ISP access concentrator. • Crucial for carrying DSL traffic between subscriber and ISP over different media.	15
	b. Analyze if deployment of MLPPP can provide any significant benefits over standard PPP for provisioning real-time services like VoIP. Provide your expert judgement on its relevance for Nexus Telecom. • MLPPP or Multilink PPP bundles multiple PPP connections to increase bandwidth. • Useful when single PPP link is inadequate for high bandwidth applications. • But Metro Ethernet already provides sufficient high bandwidth connectivity. • MLPPP also does not provide QoS benefits for real-time traffic. • Modern QoS mechanisms like DSCP better for prioritizing VoIP traffic. • Hence MLPPP not very relevant for Nexus Telecom's needs.	10
	(OR)	

4	Imagine you are the head of a technology committee in a rapidly growing e-commerce company. The company is on the cusp of expanding its operations globally, and you are assigned with optimizing the existing network infrastructure to support this growth. Your recommendations will be instrumental in ensuring a seamless online shopping experience for customers worldwide, including secure transactions, fast loading times, and minimal downtime. **a. For global operations, how can you ensure secure data transmission and connectivity between remote offices, suppliers, and customers? Identify the technologies and strategies adapted for this expansion?** i. Virtual Private Networks (VPNs): Implement VPNs to encrypt data transmitted over the network, ensuring data confidentiality and integrity between remote offices, suppliers, and customers. ii. Multi-factor Authentication (MFA): Enforce MFA for user access to sensitive systems and data, enhancing security by requiring multiple forms of verification. iii. Secure Sockets Layer (SSL) and Transport Layer Security (TLS): Utilize SSL/TLS certificates to encrypt data during online transactions, providing a secure connection between customers and the e-commerce platform. iv. Content Delivery Networks (CDNs): Employ CDNs to distribute website content and resources globally, reducing latency and enhancing the loading times for customers worldwide. v. Intrusion Detection and Prevention Systems (IDPS): Implement IDPS to monitor network traffic and identify potential security threats, allowing for proactive threat mitigation. vi. Cloud-Based Security Solutions: Consider cloud-based security services for scalability and flexibility in securing network infrastructure. vii. Compliance with Data Protection Regulations: Ensure compliance with relevant data protection laws (e.g., GDPR, CCPA) to safeguard customer data.	10
	b. Discuss the network technologies that is used to provide a responsive and efficient online shopping experience in handling the increase of data transfer. It helps in reducing latency. Justify. i. Content Delivery Networks (CDNs): CDNs distribute content to edge servers globally, reducing the physical distance between users and the data source, which minimizes latency and speeds up page loading times. ii. Load Balancers: Load balancers distribute incoming network traffic across multiple servers, preventing server overload and ensuring a consistently responsive website.	10

		iii. Caching Mechanisms: Implement caching for frequently accessed content to reduce the need for repeated data transfer, improving page loading speeds. iv. Quality of Service (QoS): QoS mechanisms prioritize critical network traffic to ensure a responsive and efficient online shopping experience. v. High-Speed Internet Connectivity: Invest in high-speed internet connections and network infrastructure to accommodate increased data transfer demands.	
	c.	**In the era of global e-commerce, data security is paramount. How would you implement protocols and technologies to maintain the integrity and security of sensitive customer data during transactions?** i. Secure Socket Layer (SSL) and Transport Layer Security (TLS): Encrypt data transmitted during transactions to protect customer information from interception. ii. Tokenization: Replace sensitive data with tokens, reducing the risk of exposure during transactions. iii. Secure Payment Gateways: Implement trusted and secure payment gateways that comply with industry standards (e.g., Payment Card Industry Data Security Standard - PCI DSS). iv. End-to-End Encryption: Ensure that data is encrypted from the customer's device to the server and vice versa, safeguarding information throughout the transaction process. v. Regular Security Audits: Conduct regular security audits and vulnerability assessments to identify and address potential weaknesses in the e-commerce platform. vi. Data Access Controls: Enforce strict access controls to limit who can access sensitive customer data, ensuring that only authorized personnel can handle it. vii. Compliance with Data Security Standards: Adhere to industry-specific data security standards and regulations to maintain the highest level of data protection. viii. Incident Response Plan: Develop a comprehensive incident response plan to address and mitigate security breaches promptly.	5