



SNS COLLEGE OF TECHNOLOGY

(An Autonomous Institution)

Approved by AICTE, New Delhi, Affiliated to Anna University, Chennai

Accredited by NAAC-UGC with 'A++' Grade (Cycle III) &

Accredited by NBA (B.E - CSE, EEE, ECE, Mech & B.Tech.IT)

COIMBATORE-641 035, TAMIL NADU



DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

QUESTION BANK

Computer Networks and Security (23AMT302)

1 Unit I: Introduction and Application Layer

1.1 Two-Mark Questions

1. Define data communication and list its key components.
2. What is a computer network? Give one example.
3. Differentiate between LAN and WAN with examples.
4. What is protocol layering? State its importance.
5. Name the four layers of the TCP/IP protocol suite.
6. What is the purpose of the OSI model?
7. List two differences between the OSI and TCP/IP models.
8. Define a socket in network programming.
9. What is the role of HTTP in the application layer?
10. Explain the purpose of FTP in networking.
11. What is SMTP? State its primary function.
12. Differentiate between POP3 and IMAP protocols.
13. What is MIME in email communication?
14. Define DNS and its primary function.
15. What is SNMP used for in network management?
16. Explain the term "client-server model" with an example.
17. What is the significance of packet switching in networks?
18. Name two application layer protocols used for email.
19. What is a protocol? Give one example.
20. Define network topology and name one type.

1.2 Sixteen-Mark Questions

1. Explain the TCP/IP protocol suite in detail, including the functions of each layer. Illustrate with an example of data transmission over the Internet.
2. Compare and contrast the OSI model with the TCP/IP model, highlighting their advantages and limitations in modern networking.

3. Describe the process of HTTP communication between a client and server. Discuss its role in web browsing with a real-world example.
4. Explain the working of DNS in resolving domain names to IP addresses. Analyze its hierarchical structure and importance in networking.
5. Discuss the functionalities of FTP and its two modes of operation. Evaluate its relevance in modern file transfer applications.
6. Elaborate on email protocols (SMTP, POP3, IMAP, MIME) and their roles in email communication. Provide a scenario of email transmission.
7. Analyze the role of SNMP in network management. Discuss how it monitors and controls network devices with examples.
8. Explain the concept of protocol layering and its significance in network design. Illustrate with the TCP/IP model.
9. Discuss the evolution of network types (LAN, WAN, MAN, PAN) and their applications in different scenarios.
10. Design a simple client-server application using sockets. Explain the steps involved in establishing communication.

2 Unit II: Transport and Network Layer

2.1 Two-Mark Questions

1. Define the transport layer and its primary function.
2. What is the key difference between TCP and UDP?
3. Explain the purpose of connection management in TCP.
4. What is flow control in the transport layer?
5. Define congestion control in TCP.
6. What is the role of SCTP in networking?
7. Explain the term "Quality of Service" (QoS).
8. What is packet switching? Give one advantage.
9. Define IPv4 and its address format.
10. What is subnetting in IP addressing?
11. Explain the purpose of IPv6 over IPv4.
12. What is the role of ARP in the network layer?
13. Define ICMP and its primary function.
14. What is DHCP used for in networking?
15. Differentiate between RARP and ARP.
16. What is meant by congestion avoidance?

17. Name two congestion avoidance techniques.
18. What is the significance of the three-way handshake in TCP?
19. Define port numbers in the transport layer.
20. What is the purpose of the network layer in the TCP/IP model?

2.2 Sixteen-Mark Questions

1. Explain TCP connection management in detail, including the three-way handshake and connection termination. Illustrate with a diagram.
2. Analyze the role of TCP congestion control mechanisms (slow start, congestion avoidance, fast retransmit). Discuss their impact on network performance.
3. Compare and contrast TCP and UDP protocols in terms of reliability, speed, and application scenarios.
4. Discuss the concept of subnetting in IPv4. Design a subnet for a network with 100 hosts, showing calculations and IP assignments.
5. Explain the structure and advantages of IPv6 over IPv4. Analyze its role in addressing modern network challenges.
6. Describe the working of DHCP in dynamic IP address allocation. Discuss its benefits and potential issues in large networks.
7. Analyze the role of ICMP in network troubleshooting. Provide examples of ICMP messages and their uses.
8. Discuss the Quality of Service (QoS) parameters and techniques for improving network performance in real-time applications.
9. Explain the process of packet switching in the network layer. Compare it with circuit switching, highlighting advantages and limitations.
10. Design a network scenario where SCTP is used instead of TCP or UDP. Justify its suitability with a detailed explanation.

3 Unit III: Data Link and Physical Layer

3.1 Two-Mark Questions

1. Define the data link layer and its primary function.
2. What is framing in the data link layer?
3. Explain flow control in the data link layer.
4. What is error control in networking?
5. Name two data link layer protocols.
6. Define HDLC and its primary use.
7. What is the role of PPP in networking?

8. Explain the term "Media Access Control" (MAC).
9. What is CSMA/CD in Ethernet?
10. Define a Virtual LAN (VLAN).
11. What is the purpose of the 802.11 standard?
12. Explain the term "transmission media" with an example.
13. What is circuit switching? Give one example.
14. Define bandwidth in the physical layer.
15. What is meant by signal encoding?
16. Name two types of transmission media.
17. What is the role of the physical layer in networking?
18. Define jitter in network performance.
19. What is the significance of Ethernet in LANs?
20. Explain the term "data rate" in the physical layer.

3.2 Sixteen-Mark Questions

1. Explain the process of framing, flow control, and error control in the data link layer. Illustrate with examples.
2. Compare and contrast HDLC and PPP protocols, highlighting their applications and limitations.
3. Discuss the working of CSMA/CD in Ethernet networks. Analyze its effectiveness in modern LANs.
4. Explain the concept of Virtual LANs (VLANs) and their role in network segmentation. Provide a real-world implementation scenario.
5. Analyze the IEEE 802.11 standard for wireless LANs. Discuss its key features and challenges in deployment.
6. Describe the types of transmission media used in the physical layer. Evaluate their suitability for different network environments.
7. Explain the process of circuit switching and its applications. Compare it with packet switching in terms of performance.
8. Discuss the performance metrics of the physical layer (bandwidth, latency, jitter). Analyze their impact on network efficiency.
9. Design a network using Ethernet and VLANs for a small organization. Explain the configuration steps and benefits.
10. Analyze the role of error control mechanisms in the data link layer. Discuss techniques like CRC and their effectiveness.

4 Unit IV: Authentication and Security

4.1 Two-Mark Questions

1. Define authentication in network security.
2. What is an authentication protocol?
3. Explain the term "key establishment."
4. What is mediated key exchange?
5. Define user authentication with an example.
6. What is password-based authentication?
7. List two password security best practices.
8. Define a Certificate Authority (CA).
9. What is a digital signature?
10. Explain the purpose of digital certificates.
11. What is key management in security?
12. Name two authentication protocols.
13. Define mutual authentication.
14. What is the role of a public key in authentication?
15. Explain the term "session key."
16. What is a trusted third party in authentication?
17. Define single sign-on (SSO).
18. What is the significance of key exchange protocols?
19. Name two types of authentication factors.
20. Explain the term "non-repudiation" in security.

4.2 Sixteen-Mark Questions

1. Explain the process of authentication and key establishment in network security. Discuss the role of trusted third parties.
2. Analyze the working of password-based authentication systems. Discuss their vulnerabilities and mitigation strategies.
3. Describe the role of a Certificate Authority in managing digital certificates. Explain the certificate issuance process.
4. Discuss the concept of digital signatures and their role in ensuring data integrity and authenticity.
5. Explain the process of mediated key exchange with an example protocol (e.g., Kerberos). Analyze its security features.

6. Design a secure authentication system for an online banking application. Justify the choice of protocols and mechanisms.
7. Analyze the importance of key management in network security. Discuss best practices for secure key distribution.
8. Compare and contrast different authentication protocols (e.g., Kerberos, OAuth). Evaluate their suitability for cloud environments.
9. Discuss the challenges of user authentication in large-scale networks. Propose a multi-factor authentication solution.
10. Explain the concept of non-repudiation and its implementation using digital signatures and certificates.

5 Unit V: Public-Key Cryptography and Message Authentication

5.1 Two-Mark Questions

1. Define cryptography and its purpose.
2. What is a cryptographic hash function?
3. Differentiate between symmetric and public-key encryption.
4. Explain the term "public key cryptography."
5. Name two public-key cryptography algorithms.
6. What is a cipher block mode of operation?
7. Define the Secure Hash Algorithm (SHA).
8. What is HMAC in message authentication?
9. Explain the term "message integrity."
10. What is the role of a digital signature in cryptography?
11. Define a one-way hash function.
12. What is the purpose of key exchange in cryptography?
13. Explain the term "block cipher."
14. Name two applications of public-key cryptography.
15. What is the significance of message authentication?
16. Define the term "nonce" in cryptography.
17. What is the role of RSA in public-key cryptography?
18. Explain the term "key pair" in cryptography.
19. What is a message digest?
20. Define the term "cryptographic salt."

5.2 Sixteen-Mark Questions

1. Explain the principles of public-key cryptography. Discuss the RSA algorithm with an example of key generation and encryption.
2. Analyze the role of cryptographic hash functions in ensuring data integrity. Compare SHA-256 and MD5 in terms of security.
3. Discuss the working of HMAC in message authentication. Explain its advantages over simple hash functions.
4. Compare and contrast symmetric and public-key encryption. Provide scenarios where each is preferred.
5. Explain the different cipher block modes of operation (e.g., CBC, ECB). Analyze their security and performance trade-offs.
6. Design a secure communication system using public-key cryptography for a corporate email application. Justify your design choices.
7. Discuss the role of digital signatures in achieving non-repudiation. Explain the signing and verification process with an example.
8. Analyze the vulnerabilities of cryptographic systems. Propose strategies to mitigate attacks like man-in-the-middle.
9. Explain the Diffie-Hellman key exchange algorithm. Discuss its role in secure communication with an example.
10. Evaluate the importance of secure hash functions in network security. Discuss their applications in password storage and digital signatures.