TE – IT – Computer Network and Security Laboratory

ORAL / VIVA QUESITON BANK

Group A: Computer Network

Assignment 1: Router Configuration and Network Address Translation

1. What is the function of a router in a network?
2. How do you configure a router using CLI commands?
3. What is the purpose of the Routing Information Protocol (RIP)?
4. What are the differences between RIP version 1 and RIP version 2?
5. What is an Access Control List (ACL), and why is it used?
6. Explain the differences between Standard and Extended ACLs.
7. How does Network Address Translation (NAT) work?
8. What are the different types of NAT?
9. Explain Static NAT with an example.
10. What is Dynamic NAT, and how does it work?
11. What is Port Address Translation (PAT), and why is it useful?
12. How do ACLs enhance network security?
13. What commands are used to configure an ACL on a router?
14. How do you verify the ACL configuration?
15. What are the limitations of RIP?
16. Why is subnetting important in router configuration?
17. How can you check active routes in a router?
18. What are the differences between a static and a dynamic route?
19. What are some alternative routing protocols to RIP?
20. What happens if a router has multiple routes to the same destination?
21. What are the advantages of using a router over a switch?
22. What is route summarization?
23. What is the administrative distance in routing?
24. How does a router decide which route to use when multiple routes are available?
25. What is the function of a default route?
26. What is the impact of incorrectly configured ACLs?
27. How does NAT help in conserving IPv4 addresses?

28. What are the security risks of using NAT?
29. What is the difference between NAT and Proxy?
30. How do you troubleshoot common router configuration issues?

Assignment 2: Routing Protocols & WLAN Configuration

1. What is a routing protocol?
2. What is the difference between static and dynamic routing?
3. How does Enhanced Interior Gateway Routing Protocol (EIGRP) work?
4. What are the key parameters of EIGRP?
5. How does EIGRP calculate the best path?
6. What are K-values in EIGRP?
7. What is an OSPF Neighbor?
8. What are the different OSPF states?
9. How does OSPF calculate the shortest path?
10. What is the purpose of an OSPF Area?
11. What is the role of a Designated Router (DR) in OSPF?
12. What are the advantages of using OSPF over RIP?
13. What is link-state routing?
14. How does MAC filtering enhance WLAN security?
15. How does DHCP work in WLAN networks?
16. What are the advantages of using static IP addressing over DHCP?
17. What are the disadvantages of using DHCP in a secure network?
18. How do you configure a DHCP server on a router?
19. How does MAC address filtering work?
20. What security measures can be implemented in WLANs?
21. What is the function of a wireless access point?
22. What is WPA3, and how does it improve WLAN security?
23. What are the key differences between EIGRP and OSPF?
24. How do you troubleshoot WLAN connectivity issues?
25. What is the difference between infrastructure mode and ad-hoc mode in WLAN?
26. What is SSID, and how can it affect WLAN security?
27. What is a VLAN, and how is it implemented in wireless networks?

28. What is the role of a gateway in WLAN networking?
29. What tools can be used to analyze WLAN traffic?
30. What are some best practices for securing a wireless network?

Assignment 3: Socket Programming in C/C++

1. What is socket programming?
2. What is the difference between TCP and UDP sockets?
3. How do you create a socket in C/C++?
4. What is the function of the bind() system call?
5. What is the role of listen() in TCP socket programming?
6. How does accept() work in a TCP server?
7. What is the difference between blocking and non-blocking sockets?
8. What is the purpose of connect() in a TCP client?
9. What is the role of send() and recv() in socket programming?
10. How does a UDP socket differ from a TCP socket?
11. What are the advantages of UDP over TCP?
12. How does TCP ensure reliable data transmission?
13. How do you handle multiple clients in a TCP server?
14. What is the difference between an IP address and a port number?
15. What is the significance of the select() function in socket programming?
16. How do you close a socket in C/C++?
17. What is the purpose of getsockopt() and setsockopt()?
18. What is the role of threading in socket programming?
19. What is a socket descriptor?
20. What are the different types of sockets?
21. What is the use of the inet_pton() and inet_ntop() functions?
22. How does a client discover a server in a network?
23. What is a raw socket?
24. What security concerns exist in socket programming?
25. How do you detect and handle socket errors?
26. What is the difference between an IPv4 and IPv6 socket?
27. What are the benefits of using asynchronous sockets?

28. How do you implement secure socket communication?
29. What are common debugging techniques in socket programming?
30. What is the role of socket buffers?

Assignment 4: Server Administration

1. What is server administration?
2. What are common server administration commands?
3. What is an FTP server, and how does it work?
4. What are the advantages of using FTP over HTTP for file transfers?
5. How do you configure an FTP server?
6. What are the different FTP modes?
7. What security risks exist with FTP?
8. What is an SFTP server?
9. How do you configure a web server?
10. What is the difference between Apache and Nginx?
11. What is the function of a web server?
12. How does a DNS server relate to web hosting?
13. What is virtual hosting in web servers?
14. What is a reverse proxy?
15. What are the advantages of HTTPS over HTTP?
16. What is the role of SSL/TLS in web servers?
17. What are common server security best practices?
18. What is load balancing, and why is it important?
19. How do you monitor server performance?
20. What is a firewall, and how does it protect a server?
21. What is the difference between a dedicated and shared server?
22. How do you handle server crashes?
23. What is logging in server administration?
24. What are system services in Linux?
25. What is a cron job, and how is it used in servers?
26. How do you restart a service in Linux?
27. How do you check open ports on a server?

28. What is the role of the .htaccess file in web servers?
29. How do you troubleshoot server connectivity issues?
30. What tools are used for server security auditing?

Group – B : Security

Assignment 1: Implement a Client and a Server on Different Computers Using Python and RSA Cryptosystem for Communication

1. What is the RSA cryptosystem, and how does it work for secure communication?
2. How do you generate the public and private keys in RSA encryption?
3. What are the primary advantages of using RSA for communication?
4. How do the client and server communicate securely using RSA in this assignment?
5. What role does the public key play in the RSA algorithm?
6. How does the private key ensure the security of the communication?
7. Describe the encryption and decryption process in RSA.
8. How do you implement RSA encryption and decryption in Python?
9. How do you exchange the public keys between the client and server securely?
10. What would happen if someone intercepts the public key in RSA communication?
11. Can RSA be used to encrypt large messages directly? Why or why not?
12. What is padding, and why is it necessary in RSA encryption?
13. How would you implement the RSA algorithm in Python using libraries like pycryptodome?
14. What are the common issues when implementing RSA in a real-world communication system?
15. How do you handle message integrity in RSA encrypted communication?
16. What is the role of the modulus in the RSA encryption scheme?
17. Explain how to ensure the authenticity of a message in RSA communication.
18. How can RSA encryption be used in an asymmetric key encryption system?
19. What are the computational costs of RSA, and how do they affect performance in large-scale systems?
20. How does the key length (e.g., 1024-bit, 2048-bit) affect the security of RSA encryption?
21. How do you verify that the RSA decryption process is successful in Python?
22. What are the limitations of RSA encryption in terms of speed and efficiency?
23. Can RSA be used for both encryption and digital signatures? If yes, how?
24. How would you implement the key exchange between the client and server in a network environment?

25. What potential vulnerabilities exist in RSA, and how can they be mitigated?
26. How does RSA ensure confidentiality during communication between client and server?
27. How would you handle key storage and management in the RSA algorithm?
28. How does Python's ssl library help secure communication using RSA?
29. What challenges would you face if RSA was used in a mobile or embedded environment with limited resources?
30. How do you ensure that RSA encryption provides confidentiality, integrity, and authenticity?

Assignment 2: Implement a Client and a Server on Different Computers Using Python and RSA Digital Signature Cryptosystem for Authentication

1. What is the purpose of digital signatures in the RSA cryptosystem?
2. How does RSA digital signature authentication differ from traditional encryption?
3. How do you generate a digital signature using RSA?
4. What role does hashing play in digital signatures?
5. How does the server authenticate the client using the RSA digital signature?
6. What is the process of verifying a digital signature in RSA?
7. Why is it necessary for the client to sign the message with their private key?
8. What happens if the client's private key is compromised in an RSA digital signature system?
9. How does the server verify the authenticity of the client's signature?
10. What is the difference between encryption and signing in RSA?
11. How do you implement digital signatures in Python using the pycryptodome library?
12. How is a message hash used in the process of digital signature creation and verification?
13. What are the steps involved in digitally signing a message and verifying it?
14. How do you ensure the integrity of the message during transmission when using RSA digital signatures?
15. What would happen if the message was altered after it was signed by the client?
16. Can RSA digital signatures be used to achieve non-repudiation? How?
17. How does RSA ensure the authenticity of the sender in a network communication system?
18. How do you implement RSA signing and verification functions in Python?
19. What are the challenges of implementing digital signature schemes in client-server communication?
20. How does the client ensure that no one else can forge their signature?
21. What is the significance of the public key in verifying a digital signature?
22. How does the RSA digital signature mechanism enhance trust between the client and server?

23. How would you handle errors during the signature verification process in a Python implementation?
24. What are the security risks of using RSA digital signatures, and how can they be mitigated?
25. How would you address the problem of key revocation in an RSA digital signature system?
26. What impact does the length of the RSA keys have on the security and performance of digital signatures?
27. How can RSA digital signatures be used to verify non-repudiation in transactions?
28. What is the difference between RSA encryption/decryption and RSA digital signing/verifying?
29. How do you test the validity of a digital signature in a client-server setup?
30. How can you secure the storage of private keys in a digital signature system?

Assignment 3: Implement a Client and a Server on Different Computers Using Python to Perform Encryption of Messages Using DES and Key Exchange via Diffie-Hellman

1. What is the Data Encryption Standard (DES), and how does it work for message encryption?
2. Why is Diffie-Hellman key exchange used in this assignment, and how does it work?
3. How do you implement the DES algorithm in Python for encrypting and decrypting messages?
4. Explain how the Diffie-Hellman method helps securely exchange keys between the client and server.
5. What is the purpose of DES in this assignment? How does it ensure message confidentiality?
6. How is the DES key generated and exchanged between the client and server?
7. What is the role of the Diffie-Hellman key exchange protocol in ensuring the security of the communication?
8. How does Diffie-Hellman solve the problem of securely sharing a key over an insecure channel?
9. How does DES handle block cipher encryption? What are the block sizes used in DES?
10. Why is DES considered less secure compared to modern encryption algorithms like AES?
11. How do you implement the key exchange using Diffie-Hellman in Python?
12. What are the security considerations when using Diffie-Hellman key exchange in a real-world application?
13. How does the client encrypt a message with the DES algorithm after exchanging keys using Diffie-Hellman?
14. What is the importance of key size in the security of the DES algorithm?
15. How is the DES key used to encrypt a message, and how is it decrypted by the receiver?
16. How does DES handle the encryption of large messages or data streams?
17. What are some vulnerabilities in DES that make it unsuitable for modern applications?

18. How does Python's pycryptodome library help implement DES encryption and Diffie-Hellman key exchange?
19. How do the client and server ensure that the exchanged keys via Diffie-Hellman are secret and unique?
20. How do you handle padding in DES encryption when the plaintext is not a multiple of the block size?
21. What would happen if an attacker intercepts the key exchange process in Diffie-Hellman?
22. How would you ensure secure key generation and key exchange between the client and server?
23. How do you prevent replay attacks in the Diffie-Hellman key exchange?
24. How is the DES key securely derived and stored after the key exchange process?
25. How does DES perform encryption and decryption using the same key, and why is this symmetric?
26. How would you implement message authentication after encryption using DES?
27. What challenges do you face when implementing DES and Diffie-Hellman in Python in terms of performance and security?
28. How would you address security weaknesses when using DES for message encryption in a production system?
29. How does Diffie-Hellman prevent the sharing of sensitive information between the client and server?
30. How does the key exchange process in Diffie-Hellman protect against man-in-the-middle attacks?

Assignment 4: Use Snort Intrusion Detection Package to Analyze Traffic and Create a Signature to Identify Problem Traffic

1. What is Snort, and how does it function as an intrusion detection system?
2. What are the differences between a signature-based and anomaly-based intrusion detection system?
3. How do you configure Snort to analyze network traffic?
4. How do you create custom signatures in Snort to detect specific types of malicious traffic?
5. What is the significance of network traffic analysis in detecting intrusions?
6. How can Snort detect DDoS (Distributed Denial of Service) attacks?
7. What is the role of a rule in Snort, and how is it used to identify malicious traffic?
8. How do you write a signature to detect an IP-based attack in Snort?
9. How do you analyze Snort logs to identify potential security threats?
10. What is the difference between "alert" and "log" in Snort's rule configuration?

11. How does Snort detect port scanning activities in the network?
12. How can Snort be integrated with other security tools for enhanced intrusion detection?
13. What are the main components of a Snort rule, and how are they structured?
14. How can Snort be configured to analyze HTTP traffic for potential web attacks?
15. What is the role of Snort in network monitoring and security?
16. How can you adjust Snort's configuration to reduce false positives during intrusion detection?
17. How does Snort handle traffic that matches a known attack signature?
18. How can Snort be used to detect SQL injection or cross-site scripting (XSS) attacks?
19. How do you test Snort signatures for accuracy in detecting intrusion attempts?
20. What is the process of creating a custom Snort signature for detecting a specific type of traffic?
21. How can Snort help in identifying network reconnaissance activities such as ARP spoofing?
22. What tools or interfaces can be used to interact with Snort for traffic analysis?
23. How can you use Snort in combination with other intrusion prevention systems (IPS)?
24. What is the importance of regularly updating Snort’s signature database?
25. How do you ensure that Snort can efficiently handle high-volume network traffic?
26. How would you use Snort to detect a specific malware signature in network traffic?
27. What are the best practices for deploying Snort in a large enterprise network?
28. How do you manage Snort's rules and signatures to keep up with evolving security threats?
29. How does Snort help in real-time monitoring of network traffic?
30. How would you configure Snort to detect a specific protocol anomaly or misuse?

Oral / Viva Questions from Theory Subject – BCN & CNS

Unit 1: Data Communication & Network Models

1. Define Shannon's Theorem.
2. What is the significance of Nyquist's theorem?
3. Differentiate between Analog and Digital signals.
4. Explain different types of noise in data communication.
5. What are the advantages of multiplexing?
6. Describe different network topologies.
7. What is bandwidth utilization?
8. Explain A/D, D/A, A/A, D/D signal conversion methods.
9. How does Shannon Hartley Theorem determine channel capacity?
10. What is the difference between simplex, half-duplex, and full-duplex communication?
11. How does Nyquist theorem determine the data rate?
12. Explain different types of signal encoding methods.
13. What is the difference between baseband and broadband transmission?
14. Define bit rate and baud rate.
15. Explain the concept of signal-to-noise ratio.
16. Differentiate between guided and unguided transmission media.
17. What is the importance of the Shannon limit?
18. Explain the concept of channel bandwidth.
19. Discuss the role of repeaters and amplifiers in communication.
20. How does bandwidth affect data transfer speed?
21. What is the impact of attenuation on signal transmission?
22. Compare frequency division multiplexing and time division multiplexing.
23. How do modulation techniques affect communication?
24. Explain phase shift keying (PSK) and amplitude shift keying (ASK).
25. What is quadrature amplitude modulation (QAM)?
26. What are the advantages of fiber-optic cables over copper cables?
27. Explain the working of different transmission impairments.
28. What is the role of error detection in data transmission?
29. How does interference affect communication systems?

30. Explain the importance of synchronization in digital communication.
31. What is meant by inter-symbol interference?
32. Describe the differences between synchronous and asynchronous transmission.
33. What are the key components of a communication system?
34. Explain the difference between narrowband and broadband signals.
35. What is pulse code modulation (PCM)?
36. How does adaptive modulation improve network efficiency?
37. Define channel coding and its role in communication.
38. What is forward error correction?
39. How do satellite communication systems transmit signals?
40. Explain the role of antennas in wireless communication.
41. Discuss the use of OFDM in modern communication systems.
42. What is the purpose of cyclic redundancy check (CRC)?
43. How does MIMO technology improve wireless networks?
44. Explain the role of a modem in communication.
45. What is frequency hopping in wireless networks?
46. Compare circuit switching, packet switching, and message switching.
47. How does latency affect real-time communication?
48. What is the function of an equalizer in communication systems?
49. Explain how error correction improves communication reliability.
50. How does spectrum management enhance wireless communication?

Unit 2: Error Detection, Correction & Data Link Control

1. What is error detection in data transmission?
2. Explain different error detection techniques.
3. Define Hamming distance and its significance.
4. What is a parity bit?
5. Explain how cyclic redundancy check (CRC) works.
6. What is the advantage of using checksum in error detection?
7. How does the Hamming code correct errors?
8. Differentiate between error detection and error correction.
9. What are the limitations of parity checking?

10. Describe the working principle of the Internet checksum method.
11. What is meant by flow control in networking?
12. Explain stop-and-wait protocol.
13. Differentiate between go-back-n ARQ and selective repeat ARQ.
14. What is piggybacking in flow control?
15. How does automatic repeat request (ARQ) help in reliable transmission?
16. What is the role of retransmission in error control?
17. Explain sliding window protocol.
18. Compare selective repeat ARQ and stop-and-wait ARQ.
19. What are the advantages of cyclic redundancy check?
20. How does bit stuffing work in framing?
21. What are the different types of framing techniques?
22. Explain the concept of data link layer services.
23. What is the importance of MAC layer in data communication?
24. Define the concept of simple parity checking.
25. How do link layer protocols handle error control?
26. What is the role of frame synchronization?
27. Explain bit-oriented and character-oriented framing.
28. What is an acknowledgment frame in networking?
29. How does sequence numbering help in reliable transmission?
30. Discuss the importance of HDLC protocol.
31. How do Ethernet frames differ from wireless frames?
32. What is the impact of error rates on network performance?
33. What is the significance of frame check sequence (FCS)?
34. Compare synchronous and asynchronous transmission modes.
35. How does error detection affect network latency?
36. Explain forward error correction (FEC).
37. Describe the main features of PPP protocol.
38. What are the limitations of stop-and-wait ARQ?
39. Why is error detection necessary in data communication?
40. How does adaptive error control work in networks?
41. Explain the role of acknowledgments in error control.

42. What is burst error in data communication?
43. Define the concept of retransmission timer.
44. How does delay impact flow control mechanisms?
45. What is the significance of HDLC frame structure?
46. Explain the working principle of Go-Back-N ARQ.
47. Describe the difference between FEC and ARQ.
48. What is the difference between TCP and UDP error control?
49. How does bit interleaving reduce error rates?
50. What is the function of a link-layer switch in error control?

Unit III: Multi-Access Mechanism and Ethernet Standards

1. What is a random access technique? Explain CSMA.
2. Describe the difference between CSMA/CD and CSMA/CA.
3. What are the main differences between CSMA/CD and CSMA/CA in terms of collision handling?
4. How does CSMA/CD work in Ethernet networks?
5. What is the principle of CSMA? How does it ensure efficient use of the communication medium?
6. Explain the concept of Collision Detection in CSMA/CD.
7. What are the advantages and limitations of CSMA/CA in wireless networks?
8. Describe the concept of controlled access in networking.
9. What is the reservation technique in controlled access?
10. Explain how polling works in controlled access.
11. What is the principle of token passing in controlled access mechanisms?
12. Describe the channelization techniques in networking.
13. How does FDMA (Frequency Division Multiple Access) work?
14. Explain how TDMA (Time Division Multiple Access) differs from FDMA.
15. What are the advantages of TDMA over FDMA in network communication?
16. Define CDMA (Code Division Multiple Access) and explain its working.
17. What is the role of the MAC (Medium Access Control) layer in Ethernet?
18. How does Standard Ethernet (IEEE 802.3) work?
19. What are the differences between Standard Ethernet and Fast Ethernet in terms of speed and technology?

20. What is the maximum transmission speed of Gigabit Ethernet?
21. What are the main features of IEEE 802.4 (Token Bus)?
22. Explain the differences between IEEE 802.3, 802.4, and 802.5 in terms of topology and access methods.
23. What is IEEE 802.5 (Token Ring) and how does it differ from Ethernet?
24. How does Ethernet work in a wired network environment?
25. What are the components of an Ethernet frame?
26. Explain the significance of the Physical Layer in Ethernet standards.
27. How does the Media Access Control (MAC) address work in Ethernet networks?
28. Describe the process of collision detection and its importance in Ethernet networks.
29. What are the different types of Ethernet cabling and connectors?
30. What role does the Physical Layer play in Ethernet networks?
31. Describe the process of link aggregation in Ethernet networks.
32. Explain how Gigabit Ethernet differs from Fast Ethernet in terms of MAC and Physical Layer specifications.
33. What is the purpose of the Ethernet Frame Check Sequence (FCS)?
34. Describe the significance of the backoff algorithm in CSMA/CD.
35. How does Full-Duplex Ethernet differ from Half-Duplex Ethernet?
36. What are the benefits of using Ethernet in modern networking?
37. Explain how Ethernet addresses operate in a network.
38. What are the IEEE 802 standards for Ethernet?
39. Describe the process of signal encoding in Ethernet.
40. How does Fast Ethernet differ in terms of MAC layer from standard Ethernet?
41. Explain the concept of Ethernet switching.
42. What is a VLAN, and how does it relate to Ethernet networks?
43. How does Ethernet handle network congestion?
44. What is the role of the Ethernet hub in a network?
45. How does Ethernet differ from Wi-Fi in terms of access mechanisms?
46. How do Ethernet switches improve network efficiency?
47. Describe the key features of an Ethernet switch.
48. What is the purpose of the MTU (Maximum Transmission Unit) in Ethernet?
49. How does Ethernet handle network segmentation?
50. What are the different modes of operation in Ethernet?

Unit IV: Network Layer: Services and Addressing

1. What are the main services provided by the Network Layer?
2. Explain the concept of IP addressing in the Network Layer.
3. What is the difference between IPv4 and IPv6 addressing?
4. What are static and dynamic IP address configurations?
5. Describe the concept of classful addressing in IPv4.
6. What is classless addressing, and how does it improve IP addressing?
7. What are the different classes of IPv4 addresses?
8. What is a special IP address, and what is its significance?
9. Explain the concept of Network Address Translation (NAT).
10. How does NAT help with IPv4 address exhaustion?
11. What is the difference between static and dynamic NAT?
12. What is subnetting, and why is it necessary in IPv4?
13. Explain the process of subnetting and how it works.
14. What is supernetting, and how does it differ from subnetting?
15. How does the network layer deliver an IP packet?
16. What is the role of a router in forwarding IP packets?
17. Explain the structure of an IPv4 datagram.
18. What is fragmentation in IPv4, and why is it needed?
19. How is an IPv4 packet fragmented?
20. What is the role of the checksum in IPv4?
21. How is the checksum calculated in an IPv4 packet?
22. What are the fields in an IPv4 header?
23. What is the purpose of the TTL (Time to Live) field in IPv4?
24. Explain the transition process from IPv4 to IPv6.
25. What are the differences between IPv4 and IPv6 packet formats?
26. What are the key features of IPv6 addressing?
27. Describe the IPv6 address space.
28. How is IPv6 addressing structured?
29. What is the significance of the "::" notation in IPv6?
30. Explain the concept of anycast addressing in IPv6.

31. What is the role of the network layer in error detection?
32. What are the primary functions of the router in a network?
33. How does routing in IPv4 differ from IPv6?
34. What are link-local addresses in IPv6?
35. What is an IPv6 global unicast address?
36. How are IPv6 addresses assigned to devices?
37. What is the role of the network layer in packet forwarding?
38. What is the difference between unicast, multicast, and broadcast in IPv4 and IPv6?
39. What are the advantages of IPv6 over IPv4?
40. How does IPv6 improve security in networking?
41. Explain how address autoconfiguration works in IPv6.
42. What are IPv6 types of addresses: unicast, multicast, and anycast?
43. What is the purpose of the ICMP (Internet Control Message Protocol) in the network layer?
44. How does IPv4 address resolution work?
45. What is the difference between IPv4 and IPv6 header formats?
46. What is the function of the ARP (Address Resolution Protocol)?
47. How does IP addressing impact routing decisions?
48. What is the role of DNS in IP addressing and resolution?
49. How does IPv6 handle address assignments differently from IPv4?
50. What challenges exist when transitioning from IPv4 to IPv6?

Unit V: Network Layer: Routing Protocols

1. What is the purpose of routing in a network?
2. Define a routing metric.
3. What is the difference between static and dynamic routing tables?
4. What are unicast routing protocols?
5. Explain the optimality principle in routing.
6. What is the difference between intra-domain and inter-domain routing?
7. What is shortest path routing?
8. What is flooding in the context of routing protocols?
9. How does distance vector routing work?
10. What is the Link State Routing protocol?

11. Explain how Path Vector Routing differs from other routing protocols.
12. What are the key features of the OSPF (Open Shortest Path First) protocol?
13. What is EIGRP (Enhanced Interior Gateway Routing Protocol)?
14. What is RIP (Routing Information Protocol), and how does it work?
15. How does the Bellman-Ford algorithm work in distance vector routing?
16. What are the advantages of link state routing over distance vector routing?
17. How does OSPF handle network topology changes?
18. What is the role of an Autonomous System (AS) in routing protocols?
19. Describe how the OSPF routing algorithm works.
20. What are the differences between OSPF and RIP?
21. How does BGP (Border Gateway Protocol) work in inter-domain routing?
22. What are the different types of BGP messages?
23. How does BGP handle routing between different ASes?
24. What is the purpose of the AS path attribute in BGP?
25. What are the key differences between interior and exterior gateway protocols?
26. Explain the concept of route summarization in OSPF.
27. What is the purpose of the hello protocol in OSPF?
28. How does BGP ensure path selection and loop prevention?
29. What is a routing loop, and how can it be prevented?
30. How does the split horizon rule help prevent routing loops in distance vector protocols?
31. What is the purpose of the TTL field in routing protocols?
32. Describe the concept of hierarchical routing in OSPF.
33. How does EIGRP use Diffusing Update Algorithm (DUAL) for routing decisions?
34. What are the key differences between OSPF and EIGRP?
35. What is the significance of metrics in routing protocols?
36. How does RIP handle the issue of count-to-infinity?
37. What are the types of OSPF routers in a network?
38. What are the limitations of RIP as a routing protocol?
39. How does OSPF ensure loop-free routing?
40. Explain the concept of interior and exterior routing.
41. What are the benefits of using a link-state routing protocol like OSPF?
42. What is the difference between a network prefix and a subnet in routing?

43. What is the role of an administrative distance in routing protocol selection?
44. How does OSPF handle multiple paths to a destination?
45. What is a virtual link in OSPF, and when is it used?
46. What are the key challenges in inter-domain routing?
47. How does the BGP protocol scale in large networks?
48. Explain the purpose of the "next-hop" attribute in BGP.
49. What is the function of the OSPF backbone area?
50. How do routing protocols ensure the most optimal path is chosen for data transmission?

Unit VI: Transport Layer – Services and Protocols

1. What are the key functions provided by the transport layer?
2. Explain the concept of transport layer services and its role in communication.
3. What is the purpose of flow control in the transport layer?
4. Define congestion control and explain its importance.
5. What is the difference between connection-oriented and connectionless services?
6. Describe the TCP (Transmission Control Protocol) and its key features.
7. What is the purpose of a TCP header, and what information does it contain?
8. Explain the process of TCP connection establishment (3-way handshake).
9. What are the three phases of the TCP connection termination process?
10. Describe the role of TCP segments in data transmission.
11. What is the purpose of the Leaky Bucket algorithm in congestion control?
12. Explain the Token Bucket algorithm and its significance in congestion control.
13. What is Quality of Service (QoS), and how does it relate to transport layer protocols?
14. How does TCP implement flow control using the sliding window mechanism?
15. What are the types of TCP timers, and what are their functions?
16. Describe the concept of TCP congestion control and its importance.
17. How does TCP handle congestion using the slow-start mechanism?
18. What are the key differences between TCP and UDP?
19. Explain the purpose of the UDP (User Datagram Protocol) header and its fields.
20. What is a UDP datagram, and how does it differ from TCP segments?
21. Describe the concept of connectionless communication in UDP.
22. What is a socket, and how is it used in networking applications?

23. What are the basic socket primitives used in TCP and UDP communication?
24. Explain the difference between a TCP socket and a UDP socket.
25. What is the role of the transport layer in end-to-end communication?
26. How does TCP ensure reliable data delivery?
27. What are the key differences between TCP and UDP in terms of reliability?
28. Explain the concept of flow control in TCP and how it prevents buffer overflow.
29. What are the advantages and disadvantages of using UDP over TCP?
30. How does TCP ensure the ordered delivery of data?
31. Describe how the TCP sliding window mechanism works.
32. What is congestion avoidance in TCP, and how is it implemented?
33. What is the function of the "sequence number" in a TCP header?
34. What are the functions of the acknowledgment number in the TCP header?
35. What is the role of the urgent pointer in TCP communication?
36. Explain the purpose of the "checksum" field in both TCP and UDP headers.
37. How does TCP handle retransmissions in case of packet loss?
38. What is the maximum segment size (MSS) in TCP, and how is it determined?
39. What is the difference between a segment and a packet in TCP?
40. How do the concepts of flow control and congestion control complement each other in TCP?
41. What are the applications of UDP in real-time communication?
42. How does TCP handle network congestion during data transmission?
43. Explain the concept of round-trip time (RTT) and its role in TCP flow control.
44. What is the role of a checksum in detecting errors in UDP and TCP communication?
45. What is the role of the "window size" in TCP flow control?
46. How does TCP manage multiple connections using ports?
47. Describe the process of error detection in TCP and UDP.
48. What is the maximum transmission unit (MTU) in TCP?
49. How does the transport layer handle retransmissions of lost packets?
50. What are the main characteristics of a reliable transport layer protocol like TCP?

Unit VII: Application Layer

1. What is the client-server communication model, and how does it work?
2. How does communication differ between TCP and UDP in client-server paradigms?
3. What is a peer-to-peer paradigm, and how does it differ from client-server communication?

4. Define DNS (Domain Name System) and explain its role in network communication.
5. What are the main functions of the DNS protocol?
6. How does DNS resolution work in the process of converting domain names to IP addresses?
7. What is the difference between FTP (File Transfer Protocol) and TFTP (Trivial File Transfer Protocol)?
8. Describe the working of the FTP protocol.
9. What is the difference between active and passive modes in FTP?
10. Explain the working of TFTP and its limitations compared to FTP.
11. What is HTTP (HyperText Transfer Protocol), and how does it facilitate web communication?
12. What are the various HTTP methods (GET, POST, PUT, DELETE)?
13. Explain the concept of HTTP status codes and their categories.
14. What is SMTP (Simple Mail Transfer Protocol), and how is it used in email communication?
15. How does SMTP differ from POP and IMAP in terms of email retrieval?
16. What is the role of POP (Post Office Protocol) in email communication?
17. How does IMAP (Internet Message Access Protocol) differ from POP in terms of email management?
18. Explain the concept of MIME (Multipurpose Internet Mail Extensions) and its role in email transmission.
19. What is DHCP (Dynamic Host Configuration Protocol), and how does it work in IP address assignment?
20. How does DHCP facilitate the management of IP addresses in a network?
21. What are the key differences between static and dynamic IP address allocation in DHCP?
22. How does the DHCP lease process work in a network?
23. What is TELNET, and how is it used for remote network management?
24. Explain the concept of the application layer in the OSI model.
25. How do application layer protocols interact with transport layer protocols?
26. What is the role of an application server in the client-server model?
27. What is a socket, and how is it used in application-layer communication?
28. What is the importance of port numbers in application-layer protocols?
29. Describe how web browsers use HTTP to retrieve web pages.
30. What is FTP passive mode, and why is it used?
31. How does SMTP ensure reliable email delivery?
32. How does an email client interact with POP and IMAP servers?
33. What is the significance of the MIME standard in email communication?

34. How does the client-server paradigm ensure data integrity and security?
35. What are the security concerns in using application-layer protocols like HTTP, FTP, and SMTP?
36. Explain the role of encryption in securing application-layer protocols.
37. How does DNS caching improve network efficiency?
38. What is the role of cookies in HTTP communication?
39. How does the HTTP/2 protocol improve upon HTTP/1.x?
40. What are the key differences between TCP and UDP in the context of application-layer protocols?
41. How do email protocols handle attachments?
42. What is the purpose of a DNS resolver in the DNS process?
43. What are the advantages of IMAP over POP for email management?
44. How does the concept of "state" work in HTTP and other application-layer protocols?
45. How does the client-server model scale in large distributed applications?
46. What are some common applications of FTP in enterprise environments?
47. What are the main advantages of using a peer-to-peer application model?
48. How does the DHCP Discover message work in the process of acquiring an IP address?
49. What is a URL, and how is it used in HTTP communication?
50. How does an email system differentiate between SMTP, POP, and IMAP during message delivery?

Unit VIII: Wireless Standards

1. What are the basic concepts of Wireless LANs (WLAN)?
2. Describe the design goals of a WLAN.
3. What are the key characteristics of WLAN networks?
4. Explain the architecture of a typical WLAN network.
5. What are the components of an IEEE 802.11 network?
6. Describe the physical layer in IEEE 802.11.
7. What are the different MAC sublayers in IEEE 802.11?
8. Explain the function of DCF (Distributed Coordination Function) in IEEE 802.11.
9. What is the role of PCF (Point Coordination Function) in IEEE 802.11?
10. What is the hidden station problem in wireless networking?
11. What is the exposed station problem in wireless networks, and how is it solved?
12. Describe the frame format in IEEE 802.11.

13. How does addressing work in IEEE 802.11 networks?
14. What is the function of the RTS/CTS mechanism in IEEE 802.11?
15. What are the advantages of IEEE 802.15.1 (Bluetooth) over IEEE 802.11 (WLAN)?
16. What is the architecture of Bluetooth, and what are its key components?
17. Explain the layers in the Bluetooth protocol stack.
18. What are the different operational states in Bluetooth communication?
19. How does Bluetooth perform device discovery?
20. What is the difference between Bluetooth Classic and Bluetooth Low Energy (BLE)?
21. What is IEEE 802.16 (WiMax), and how does it differ from WLAN and Bluetooth?
22. Describe the architecture and layers of the IEEE 802.16 protocol.
23. What are the main services provided by WiMax?
24. How does WiMax differ from WLAN in terms of coverage area and data rates?
25. Explain the role of base stations in WiMax networks.
26. How does WiMax handle mobility in its communication?
27. What are the key differences between Bluetooth, IEEE 802.11, and IEEE 802.16?
28. What is the role of the MAC layer in wireless networking standards?
29. How does WiMax achieve high-speed internet access in rural areas?
30. What is the concept of Quality of Service (QoS) in wireless standards like Bluetooth and WiMax?
31. Describe how the Bluetooth piconet operates.
32. What is a scatternet in Bluetooth, and how does it function?
33. What are the main differences in throughput between WiMax and WLAN?
34. How do the frequency ranges of WiMax and WLAN differ?
35. What are the advantages of IEEE 802.11ac over previous WLAN standards?
36. How does WiMax handle spectrum allocation?
37. Explain how WiMax supports broadband services for mobile users.
38. What is the role of security in WiMax networks?
39. How does IEEE 802.11 handle interference and congestion in wireless networks?
40. What is beamforming in WiMax, and how does it improve signal strength?
41. How does the IEEE 802.15.1 Bluetooth protocol achieve low power consumption?
42. What are the limitations of Bluetooth in terms of data rates and range?
43. What are the advantages of using WiMax for last-mile connectivity?
44. Describe the differences between Wi-Fi and WiMax in terms of network architecture.

45. How does Bluetooth ensure reliable data transmission in noisy environments?
46. What are the different types of WiMax equipment used for communication?
47. How does the IEEE 802.11 protocol handle encryption and security?
48. What are the factors that influence the range of wireless LANs?
49. How do wireless devices manage power consumption in Bluetooth and WiMax?
50. What are the emerging trends in wireless networking standards?

Unit IX: Adhoc & Wireless Sensor Networks (WSN)

1. What is the difference between infrastructure and infrastructure-less wireless networks?
2. Explain the main issues in Adhoc wireless networks.
3. What are the design issues in the MAC layer of an Adhoc network?
4. Define MACAW. How does it work in an Adhoc network?
5. What are the major challenges in designing the MAC layer of Adhoc networks?
6. Describe the classification of Adhoc network protocols.
7. What is the purpose of a routing protocol in Adhoc wireless networks?
8. Discuss the issues in designing a routing protocol for Adhoc wireless networks.
9. Compare and contrast the types of Adhoc network routing protocols.
10. Explain the working of DSDV protocol in Adhoc networks.
11. How does AODV differ from DSR in terms of routing protocol design?
12. What are the advantages and limitations of DSR routing protocol?
13. What are the applications of sensor networks in modern technology?
14. How are Adhoc wireless networks different from sensor networks?
15. What are the challenges in designing a sensor network?
16. Explain the architecture of a typical sensor node.
17. What are the key challenges faced by sensor networks in terms of scalability?
18. How do energy consumption and battery life impact sensor network design?
19. Define layered architecture in sensor networks.
20. What are the advantages of a clustered architecture in sensor networks?3

21. Describe the classification of sensor network protocols.
22. Explain the role of routing in sensor networks.
23. What are the challenges in sensor network localization?

24. How do sensor networks handle mobility in Adhoc scenarios?
25. What is the role of sensor data aggregation in energy optimization?
26. Discuss the various types of communication models in sensor networks.
27. What is the significance of the MAC layer in sensor networks?
28. How does the QoS (Quality of Service) affect sensor network performance?
29. What are the security challenges in wireless sensor networks?
30. How does a multi-hop communication model function in sensor networks?
31. Discuss the importance of scalability in sensor networks.
32. Explain the concept of routing in mobile Adhoc networks (MANETs).
33. What is the role of routing tables in Adhoc networks?
34. How do Adhoc networks handle dynamic topology?
35. What is the significance of TCP/UDP in Adhoc and sensor networks?
36. How do Adhoc networks support voice and video traffic?
37. Discuss the importance of load balancing in Adhoc networks.
38. What role does the physical layer play in wireless sensor networks?
39. How does interference impact sensor network communication?
40. Explain the concept of time synchronization in sensor networks.
41. What is the difference between proactive and reactive routing protocols?
42. Discuss the concept of hybrid routing protocols in wireless Adhoc networks.
43. How do Adhoc networks support large-scale communications?
44. What is the significance of delay tolerance in Adhoc networks?
45. Explain the concept of QoS in Adhoc networks.
46. How do Adhoc networks handle fault tolerance and reliability?
47. What is the significance of the Internet of Things (IoT) in sensor networks?
48. Discuss the importance of collaborative sensing in wireless sensor networks.
49. How do you handle congestion in Adhoc networks?
50. What are the potential uses of Adhoc and sensor networks in smart cities?

Unit X: Introduction to Network Security

1. Why is network security important in today's digital age?
2. Describe the two main categories of network attacks.
3. What are passive attacks, and how do they differ from active attacks?

4. Define unauthorized access in network security.
5. What is a Distributed Denial of Service (DDoS) attack, and how does it work?
6. Explain the concept of a Man-in-the-Middle (MitM) attack.
7. What is confidentiality in the context of network security?
8. How do authentication and authorization contribute to network security?
9. What is the principle of non-repudiation in network security?
10. Define access control and its significance in securing a network.
11. How do stream ciphers work in cryptography?
12. Compare monoalphabetic and polyalphabetic substitution ciphers.
13. What is the rail-fence cipher, and how is it used for encryption?
14. Explain the difference between block ciphers and stream ciphers.
15. What is the Electronic Code Book (ECB) mode in block ciphers?
16. How does Cipher Block Chaining (CBC) mode function in block ciphers?
17. What is Cipher Feedback (CFB) mode in block ciphers?
18. Explain Output Feedback (OFB) mode in block ciphers.
19. What are the common threats in network security?
20. Define and discuss the concept of integrity in network security.
21. How does encryption ensure confidentiality in data transmission?
22. What is the role of digital signatures in network security?
23. How does a public key infrastructure (PKI) work?
24. What is the significance of private key management in network security?
25. Describe the Diffie-Hellman key exchange algorithm.
26. What are the advantages of symmetric key encryption?
27. How does RSA encryption work?
28. What is the role of digital certificates in network security?
29. Explain the concept of hash functions in cryptography.
30. How are cryptographic algorithms applied in securing online communications?
31. Discuss the importance of multi-factor authentication in modern networks.
32. What are some common cryptographic protocols used in network security?
33. How can an attacker exploit the weaknesses in a cipher?
34. What is the role of firewalls in network security?
35. Define intrusion detection systems (IDS) and their use in network security.

36. What is an intrusion prevention system (IPS)?
37. Explain the role of VPNs in network security.
38. How does public-key cryptography differ from symmetric-key cryptography?
39. What is the role of the secure sockets layer (SSL) in encryption?
40. How do access control lists (ACLs) work in securing a network?
41. What are some methods used to prevent SQL injection attacks?
42. Explain the concept of malware and how it impacts network security.
43. What is phishing, and how can users protect themselves?
44. How can businesses defend against DDoS attacks?
45. What are the security measures used in wireless networks?
46. How does a Digital Certificate Authority (CA) operate?
47. Explain the importance of patch management in network security.
48. What are the challenges in securing mobile networks?
49. How do zero-trust security models work?
50. What are the ethical concerns related to network security?

Unit XI: Cryptographic Algorithms

1. What are the basic mathematical preliminaries used in cryptography?
2. How are groups, rings, and fields used in cryptographic algorithms?
3. What is the role of prime numbers in cryptography?
4. Explain the working of the Data Encryption Standard (DES).
5. What is the Advanced Encryption Standard (AES)?
6. How does the RSA algorithm work for public-key encryption?
7. What are the advantages of RSA over DES?
8. Explain the concept of a hash function in cryptography.
9. What is a digital signature, and how does it work?
10. What are digital certificates, and what role do they play in encryption?
11. Define the Public Key Infrastructure (PKI) and explain its importance.
12. How does the Diffie-Hellman key exchange algorithm work?
13. What is the PKIX model in cryptographic systems?
14. Explain the concept of asymmetric encryption.
15. How does symmetric encryption differ from asymmetric encryption?

16. What are elliptic curve cryptosystems (ECC)?
17. What are the security considerations when choosing a cryptographic algorithm?
18. What is the purpose of key management in cryptographic systems?
19. How is AES used in securing data communication?
20. What are the applications of cryptography in modern networks?
21. What are the limitations of the DES algorithm?
22. How is a public key used in RSA encryption?
23. What is the importance of padding in block cipher algorithms?
24. What is the relationship between encryption and authentication?
25. Explain the concept of key exchange in cryptography.
26. How do hybrid cryptosystems work?
27. Discuss the impact of quantum computing on current cryptographic algorithms.
28. What is the role of a cipher suite in secure communication?
29. How is cryptographic strength measured?
30. What are some common attacks on cryptographic systems?
31. How do you secure private key storage in a public-key cryptosystem?
32. Explain the use of hash functions in verifying data integrity.
33. What is a salt, and how does it enhance security in hashing?
34. What are the differences between HMAC and normal hashing algorithms?
35. How is RSA used for digital signatures?
36. What is the importance of key size in cryptographic algorithms?
37. What are the challenges associated with implementing AES?
38. What is the role of the blockchain in modern cryptography?
39. Explain the concept of homomorphic encryption.
40. What is a cryptographic nonce, and how is it used?
41. How does the ElGamal encryption algorithm work?
42. What is the purpose of a cryptographic random number generator?
43. How does a cipher block chaining (CBC) mode enhance data security?
44. What is the significance of key stretching in cryptography?
45. Discuss the role of cryptography in securing cloud services.
46. How do you prevent side-channel attacks in cryptographic systems?
47. What is the use of XOR operations in cryptography?

48. Explain the role of certificates in HTTPS.
49. How does a cipher text feedback (CFB) mode function in encryption?
50. Discuss the role of cryptography in securing mobile applications.

Unit XII: Introduction to Cyber Security

1. What is cyber security, and why is it essential in today's world?
2. Define the layers of security in cyber systems.
3. What is the difference between vulnerability and a threat in cyber security?
4. What are the common harmful acts in cyber security?
5. Define malware and provide examples.
6. What is phishing, and how can individuals protect themselves from it?
7. What is a Man-in-the-Middle (MIM) attack?
8. How do Denial of Service (DoS) attacks affect networks?
9. Explain SQL injection and how to prevent it.
10. What is cyber warfare, and how does it differ from cyber crime?
11. Describe cyber stalking and the threats it poses to individuals.
12. What is cyber terrorism, and what are its potential impacts?
13. How do software attacks differ from hardware attacks?
14. What is the role of internet governance in cyber security?
15. What motivates attackers in cyber crimes?
16. How does cyber espionage pose a threat to national security?
17. What are the key components of a comprehensive cyber security policy?
18. Explain the importance of patch management in cyber security.
19. How does encryption protect against cyber threats?
20. What is two-factor authentication, and why is it important?
21. What role does machine learning play in detecting cyber threats?
22. How do firewalls help in cyber security?
23. What is an intrusion detection system (IDS)?
24. Explain the role of access control in securing networks.
25. What is the significance of an incident response plan in cyber security?
26. How do vulnerabilities in IoT devices pose a cyber threat?
27. What is the concept of zero-trust security in cyber defense?

28. How do DDoS attacks differ from regular DoS attacks?
29. What are the ethical concerns related to hacking?
30. How can businesses protect their data from cyber threats?
31. What is the role of encryption in securing online banking transactions?
32. What is the importance of digital certificates in ensuring secure communications?
33. How do hackers exploit software vulnerabilities in cyber attacks?
34. What is the difference between a hacker and a cracker?
35. How can businesses mitigate the risk of ransomware attacks?
36. What is the role of monitoring in cyber threat detection?
37. How can organizations prevent data breaches?
38. What is the significance of network segmentation in cyber security?
39. How do botnets contribute to cyber attacks?
40. What are the challenges in securing cloud computing environments?
41. How do phishing scams affect both individuals and organizations?
42. What is the role of cyber insurance in mitigating cyber risks?
43. How do you handle insider threats in a corporate environment?
44. What is the impact of GDPR on cyber security policies?
45. How does biometric authentication contribute to cyber security?
46. How do cyber attacks on critical infrastructure affect national security?
47. What is the significance of cyber security training for employees?
48. What is the role of artificial intelligence in cyber defense?
49. What is the importance of regular system updates in cyber security?
50. What strategies can governments adopt to protect against cyber terrorism?