University of Guelma | 12/06/2025
Department of Computer Science | Communication Protocols and Distributed Systems
Semester 2, Master 1 SIQ (2024/2025) - Time : 1h15 | Dr. Mohamed Amine Ferrag
First Name : ..... ; Last Name : .....; Group : .....

Resit Exam Solution

This exam consists of multiple-choice questions (MCQs).
Each question may have one, multiple, or no correct options.

Exercise 1 – IP Layer and Models

(1 pts) **Question 1:** Which of the following statements about IPv4 and IPv6 are correct?

(a) ☐ IPv4 uses a header checksum; IPv6 does not use one.
(b) ☐ IPv6 uses extension headers for fragmentation and routing.
(c) ☐ IPv4 natively supports multicast in the base protocol.
(d) ☐ IPv6 requires manual address configuration; IPv4 can use SLAAC.
(e) ☐ IPv6 includes a Flow Label field for QoS.

Solution: (a), (b), (c), (e)

(1 pts) **Question 2:** Which of the following statements about the OSI and TCP/IP models are true?

(a) ☐ The OSI model defines a separate Presentation layer.
(b) ☐ The TCP/IP model groups Session and Presentation into its Application layer.
(c) ☐ OSI's Network layer corresponds to IP in TCP/IP.
(d) ☐ The TCP/IP model has exactly five layers.
(e) ☐ OSI's Transport layer maps to TCP and UDP in TCP/IP.

Solution: (a), (b), (c), (e)

Exercise 2 – Security and Name Services

(1 pts) **Question 1:** Which of the following statements about the TLS handshake in HTTPS are correct?

(a) ☐ The server may request a client certificate for mutual authentication.
(b) ☐ The pre-master secret is encrypted with the server's public key.
(c) ☐ Cipher suite negotiation takes place after ChangeCipherSpec.
(d) ☐ The server sends its certificate before ServerHello.
(e) ☐ Finished messages confirm the integrity of the handshake.

Solution: (a), (b), (e)

(1 pts) **Question 2:** Which of the following statements about DHCP and the DORA process are true?

(a) ☐ DHCPDISCOVER is broadcast to 255.255.255.255.
(b) ☐ DHCPOFFER carries the offered IP and lease duration.
(c) ☐ DHCPREQUEST can be unicast to the selected server.
(d) ☐ DHCP uses UDP ports 68 (client) and 67 (server).
(e) ☐ DHCPINFORM is used when the client already has an IP.

Solution: (a), (b), (c), (d), (e)

(1 pts) **Question 3:** Which of the following statements about iterative DNS resolution are correct?

(a) ☐ The resolver queries root, then TLD, then authoritative servers.
(b) ☐ Glue records prevent extra lookups by providing delegation data.
(c) ☐ Negative caching avoids repeated NXDOMAIN queries.
(d) ☐ CNAME chains can increase resolution latency.
(e) ☐ Authoritative servers forward queries upstream.

Solution: (a), (b), (c), (d)

Exercise 3 – Publish/Subscribe and IoT Protocols

(1 pts) **Question 1:** Which of the following statements about MQTT QoS and features are correct?

(a) ☐ QoS 1 uses a two-step PUBLISH–PUBACK handshake.
(b) ☐ The RETAIN flag makes the broker store the last message on a topic.
(c) ☐ QoS 2 may deliver duplicates after reconnection.
(d) ☐ MQTT topics support the wildcards `+` and `#`.
(e) ☐ Clean session = false resumes previous subscriptions.

Solution: (a), (b), (d), (e)

(1 pts) **Question 2:** Which of the following statements about CoAP confirmable (CON) messages are correct?

(a) ☐ CON messages require an ACK or RST reply.
(b) ☐ The Token field identifies request-response pairs.
(c) ☐ CoAP default port is 5683 over UDP.
(d) ☐ Message ID helps detect duplicates, not replay protection.
(e) ☐ Non-confirmable messages still guarantee delivery.

Solution: (a), (b), (c), (d)

(1 pts) **Question 3:** Which of the following statements about MQTT brokers are correct?

(a) ☐ EMQX supports clustering with distributed metadata.
(b) ☐ Mosquitto natively supports HTTP bridging.
(c) ☐ HiveMQ offers MQTT over WebSockets out-of-the-box.

(d) ☐ EMQX enforces topic-level ACLs by default.
(e) ☐ Mosquitto requires external plugins for TLS.

Solution: (a), (c)

Exercise 4 – Transport Layer Mechanics

(1 pts) **Question 1:** Which of the following statements about TCP congestion control are correct?

(a) ☐ Slow Start increases cwnd exponentially.
(b) ☐ Fast Recovery inflates cwnd using duplicate ACKs.
(c) ☐ Tahoe resets cwnd to one MSS on loss.
(d) ☐ CUBIC is Linux's default TCP algorithm.
(e) ☐ AIMD stands for Additive Increase, Multiplicative Decrease.

Solution: (a), (b), (c), (d), (e)

(1 pts) **Question 2:** Which of the following statements about TCP header fields are true?

(a) ☐ Window Size can be scaled via TCP options.
(b) ☐ PSH flag requests immediate delivery to application.
(c) ☐ Checksum covers pseudo-header, header, and payload.
(d) ☐ Urgent Pointer is valid only if URG=1.
(e) ☐ Sequence Number indicates byte offset, not packet count.

Solution: (a), (b), (c), (d), (e)

(1 pts) **Question 3:** Which of the following statements about UDP and its use are correct?

(a) ☐ IPv6 mandates a non-zero UDP checksum.
(b) ☐ UDP provides no retransmission on loss.
(c) ☐ DNS over UDP may fall back to TCP if >512 bytes.
(d) ☐ RTP typically uses UDP for real-time media.
(e) ☐ UDP header includes a length field.

Solution: (a), (b), (c), (d), (e)

Exercise 5 – VPN and IPsec

(1 pts) **Question 1:** Which of the following statements about Dynamic Multipoint VPN (DMVPN) are correct?

(a) ☐ DMVPN uses mGRE interfaces on hub and spokes.
(b) ☐ NHRP resolves dynamic spoke IPs for direct tunnels.
(c) ☐ IPsec transport mode encrypts only payload, not GRE.
(d) ☐ DMVPN spokes require static crypto maps.
(e) ☐ DMVPN supports on-demand spoke-to-spoke tunnels.

Solution: (a), (b), (e)

(1 pts) **Question 2:** Which of the following statements about IPsec protocols and Security Associations are correct?

(a) ☐ AH provides integrity/authentication but no encryption.
(b) ☐ ESP can provide confidentiality, integrity, and authentication.
(c) ☐ AH is used when encryption is mandatory.
(d) ☐ IPsec SA is unidirectional; two needed for bidirectional.
(e) ☐ IKEv2 establishes SAs in a single exchange.

Solution: (a), (b), (d)

(1 pts) **Question 3:** Which of the following statements about cryptographic primitives in IPsec are correct?

(a) ☐ DH Group 14 uses a 2048-bit MODP prime.
(b) ☐ ECC Group 21 offers similar security with shorter keys.
(c) ☐ AES-GCM provides combined confidentiality and integrity.
(d) ☐ 3DES uses two 112-bit keys.
(e) ☐ SHA-1 is secure for digital signatures.

Solution: (a), (b), (c)

Exercise 6 – Subnetting and ACLs

(2 pts) **Question 1:** You have network 172.16.0.0/20. Which of the following statements about subdividing it into four equal subnets are correct?

(a) ☐ Each subnet mask is /22.
(b) ☐ Each subnet contains 1024 addresses.
(c) ☐ The second subnet is 172.16.4.0/22.
(d) ☐ Broadcast of the third subnet is 172.16.8.0/22 => 172.16.11.255.
(e) ☐ A /21 mask yields two subnets.

Solution: (a), (b), (c), (d), (e)

(2 pts) **Question 2:** Which of the following IP addresses would match the ACL "deny 10.0.0.0 0.0.15.255"?

(a) ☐ 10.0.10.5
(b) ☐ 10.0.16.1

(c) ☐ 10.0.15.255
(d) ☐ 10.0.0.128
(e) ☐ 10.0.31.0

Solution: (a), (c), (d)

(2 pts) **Question 3:** Which of the following statements about summarizing contiguous /24 networks are correct?

(a) ☐ Two /24 networks aligned can summarize to /23.
(b) ☐ Four /24 on boundaries 0, 64, 128, 192 summarize to /22.
(c) ☐ A /21 summary starts at a multiple of 8 in the third octet.
(d) ☐ A /20 summary covers 16 contiguous /24s.
(e) ☐ A /19 summary covers 32 contiguous /24s.

Solution: (a), (c), (d), (e)