Exam (Solution)

The exam consists of multiple-choice questions (MCQs). The correct answer(s) to each question may include one, two, three, four, or five options, or possibly none.

- **Exercise 1: (2 pts)**

Question 1: Which statements about IPv4 and IPv6 are correct?
(a) ■ IPv6 addresses are 128 bits long.
(b) ■ IPv4 uses dotted-decimal notation; IPv6 uses hexadecimal colon-separated notation.
(c) ■ CIDR allows flexible subnetting in both IPv4 and IPv6.
(d) ■ IPv6 eliminates the need for NAT due to its vastly larger address space.
(e) □ IPv6 header size is variable and can exceed 64 bytes.

Question 2: Which of the following statements about the OSI and TCP/IP models are true?
(a) ■ The OSI model comprises seven layers; the TCP/IP model has four.
(b) ■ The OSI model is theoretical and protocol-agnostic; TCP/IP is practical and protocol-specific.
(c) ■ The TCP/IP Transport layer offers both connectionless (UDP) and connection-oriented (TCP) services.
(d) ■ The OSI Presentation layer handles data formatting, encryption, and compression.
(e) □ The TCP/IP model explicitly separates Session and Presentation layers.

- **Exercise 2: (3 pts)**

Question 1: Regarding the HTTPS (HTTP over TLS) handshake, which of the following are correct?
(a) ■ The client and server use asymmetric cryptography to authenticate the server's identity.
(b) □ A symmetric session key is generated before the server presents its digital certificate.
(c) ■ Digital certificates issued by Certificate Authorities are exchanged to validate public keys.
(d) ■ The handshake negotiates the cipher suite to be used for encryption.
(e) □ Encrypted application data is exchanged before the TLS session is fully established.

Question 2: Which of the following statements about DHCP and its DORA process are true?
(a) □ DHCPDISCOVER messages are sent as unicast to a specific DHCP server.
(b) ■ DHCPOFFER messages include network parameters such as subnet mask and DNS server.
(c) ■ The client sends a DHCPREQUEST message to accept a specific IP offer.
(d) □ DHCP uses TCP port 67 for data transfer.
(e) ■ DHCPACK finalizes the lease and may include the lease duration.

Question 3: In the DNS resolution process, which of the following statements are correct?
(a) ■ A recursive resolver queries root servers, TLD servers, and authoritative servers.
(b) ■ Iterative queries involve the resolver returning referrals to other DNS servers.
(c) □ CNAME records map domain names directly to IPv4 addresses.
(d) □ Authoritative name servers cache DNS responses received from higher-level servers.

- **Exercise 3: (4 pts)**

Question 1: Which of the following statements about MQTT Quality of Service (QoS) levels are correct?
(a) ■ QoS 0 messages are delivered at most once without confirmation and may be lost.
(b) ■ QoS 1 employs a two-step handshake (PUBLISH–PUBACK) and may result in duplicates.
(c) ■ QoS 2 guarantees exactly once delivery via a four-step handshake (PUBLISH–PUBREC–PUBREL–PUBCOMP).
(d) □ QoS 1 always prevents message duplication.
(e) ■ Higher QoS levels incur greater latency and resource overhead.

Question 2: Regarding the fixed-size CoAP header, which of the following are correct?
(a) ■ The Version field occupies 2 bits.
(b) □ The Type Code field occupies 4 bits.
(c) □ The Option Count field occupies 4 bits.
(d) ■ The Code field occupies 8 bits.
(e) ■ The Message ID occupies 16 bits.

Question 3: Which of the following statements about the Mosquitto and EMQX MQTT brokers are true?
(a) □ Mosquitto natively supports clustered deployments for high availability.
(b) ■ EMQX can handle up to 100 million concurrent connections per cluster.
(c) ■ Mosquitto's persistence mechanism is file-based only.
(d) □ EMQX lacks built-in support for horizontal scaling.
(e) □ Mosquitto supports role-based access control (RBAC) out of the box.

Question 4: Regarding MQTT session state and CoAP confirmable message reliability mechanisms, which of the following statements are correct?
(a) ■ Setting the MQTT clean-session flag to false instructs the broker to retain the client's subscriptions and undelivered messages.
(b) ■ MQTT session state comprises the client's subscription list, unacknowledged QoS 1/2 messages, and packet identifiers.
(c) ■ CoAP confirmable (CON) messages require the recipient to reply with either an ACK or RST.
(d) □ CoAP confirmable messages include sequence numbers to guarantee in-order delivery.
(e) □ Persistent MQTT sessions are supported only in MQTT v5.0 and later.

- **Exercise 4: (3 pts)**

Question 1: Regarding TCP's reliability and congestion-control mechanisms, which of the following statements are correct?
(a) ■ TCP uses a sliding-window mechanism to match the sender's rate to the receiver's buffer capacity.
(b) □ The Slow Start algorithm increases the congestion window linearly until it reaches the slow-start threshold (ssthresh).
(c) ■ Fast Retransmit is triggered after three duplicate ACKs are received for the same sequence number.
(d) ■ Upon detecting packet loss via timeout, TCP sets ssthresh to half of the current congestion window and resets the window to one MSS.
(e) ■ Congestion Avoidance phase employs additive increase and multiplicative decrease of the congestion window.

Question 2: Which of the following statements about TCP header fields are true?
(a) ■ The Sequence Number field indicates the byte offset of the first data byte in this segment.
(b) ■ The Acknowledgement Number field is valid only if the ACK control flag is set.

(c) ■ The Data Offset (Header Length) field is specified in 4-byte words and ranges from 5 to 15.
(d) ■ The Urgent Pointer field is interpreted only when the URG flag is set.
(e) □ The Checksum covers only the TCP header, not the payload or pseudo-header.
(f) ■ The Window Size field specifies how many bytes the sender of the segment is currently willing to receive.

Question 3: Concerning UDP characteristics and typical applications, which statements are correct?
(a) ■ UDP checksum is optional in IPv4 and may be set to zero to disable error checking.
(b) ■ UDP natively supports both unicast and multicast delivery without additional protocol overhead.
(c) □ UDP preserves message ordering across packet boundaries.
(d) ■ DNS and DHCP protocols both run over UDP by default.
(e) ■ Real-time applications like VoIP favor UDP to avoid retransmission delays and head-of-line blocking.
(f) ■ UDP uses 16-bit source and destination port numbers to multiplex applications at endpoints.

- **Exercise 5: (3 pts)**

Question 1: Regarding Dynamic Multipoint VPN (DMVPN), which of the following statements are correct?
(a) ■ DMVPN uses a multipoint GRE (mGRE) interface to support multiple IPsec tunnels on a single hub router.
(b) ■ DMVPN relies on the Next Hop Resolution Protocol (NHRP) to dynamically discover and establish spoke-to-spoke tunnels.
(c) □ DMVPN requires static, pre-configured IPsec policies for each spoke-to-spoke connection.
(d) ■ By default, DMVPN employs a hub-and-spoke topology but can build direct spoke-to-spoke tunnels on demand.
(e) □ DMVPN eliminates the need for any IPsec gateways at branch sites.

Question 2: Which of the following statements about IPsec protocol encapsulation and Security Associations (SAs) are true?
(a) □ The Authentication Header (AH) protocol provides both encryption and integrity protection.
(b) ■ The Encapsulating Security Payload (ESP) protocol can provide confidentiality, integrity, and authentication.
(c) ■ AH is appropriate when confidentiality is not required but integrity and origin authentication are needed.
(d) □ ESP encrypts the entire original IP header as well as its payload.
(e) ■ An IPsec SA is unidirectional, so two SAs are required for bidirectional traffic protection.

Question 3: Which of the following statements about cryptographic algorithms and Diffie-Hellman (DH) groups in IPsec are correct?
(a) ■ DH groups 1, 2, and 5 are deprecated due to insufficient key lengths.
(b) ■ DH group 14 uses a 2048-bit prime modulus for key exchange.
(c) ■ Elliptic Curve Cryptography (ECC) groups such as DH 19 and 20 offer equivalent security with shorter key sizes.
(d) □ AES supports key lengths of 112, 192, and 256 bits.
(e) ■ The 3DES algorithm uses three independent 56-bit keys to encrypt each 64-bit block.

- **Exercise 6: (5 pts)**

Question 1: You have the network 10.100.0.0/20 and must subdivide it into eight equal-sized subnets. Which of the following statements are correct?
(a) ■ Each subnet will use a /23 mask.
(b) ■ Each subnet contains 512 total addresses.
(c) ■ The third subnet's network address is 10.100.4.0.
(d) ■ The broadcast address of that third subnet is 10.100.5.255.
(e) □ A /22 mask would also yield eight subnets.

Question 2: An ACL uses the statement "permit 192.168.16.0 0.0.3.255". Which of the following are true about the matched address range?
(a) ■ It covers 192.168.16.0 through 192.168.19.255.
(b) □ It matches 192.168.20.0.
(c) □ The third-octet bits 0–3 are wildcarded.
(d) ■ It can be used to permit four contiguous /24 networks.
(e) ■ It matches 192.168.16.128.

Question 3: Which of the following statements about summarizing contiguous /24 networks are correct?
(a) ■ Summarizing two contiguous /24 networks aligned on a /23 boundary requires a /23 mask.
(b) ■ Summarizing four contiguous /24 networks aligned on a /22 boundary requires a /22 mask.
(c) ■ A /21 summary must start at a third-octet value divisible by 8.
(d) ■ A /20 summary must start at a third-octet value divisible by 16.
(e) ■ A /20 summary covers 16 contiguous /24 networks.

Question 4: You have 192.168.100.0/24 and need subnets for at least 60, 30, and 14 hosts (in that order). Which statements about your VLSM design are correct?
(a) ■ To support $\geq$ 60 hosts you must use a /26 mask.
(b) ■ A /27 mask supports up to 30 usable hosts.
(c) □ A /28 mask supports up to 30 usable hosts.
(d) ■ A /28 mask supports up to 14 usable hosts.
(e) ■ After the /26 block, the next subnet begins at 192.168.100.64.

Question 5: Given the network 192.168.96.0/20, which of these /24 subnets fall within its address range?
(a) ■ 192.168.96.0/24
(b) ■ 192.168.100.0/24
(c) ■ 192.168.103.0/24
(d) ■ 192.168.104.0/24
(e) □ 192.168.112.0/24