ARPGuard Quiz and Answer Key

Assessment aligned to lab objectives (includes brief justification for each answer)

Instructions

- Unless the instructor specifies otherwise, responses should be 1–3 sentences.
- Where applicable, justify answers by referencing observable ARP behavior (fields, sequence, mapping stability/conflict).
- Total suggested points: 20.

Part A — Questions

Q1 (2 pts): What problem does ARP solve on an IPv4 Ethernet LAN?

Q2 (2 pts): In the TCP/IP model, ARP is most closely associated with which boundary? (A) Application (B) Transport (C) Network-to-Link boundary (D) Physical

Q3 (1 pt): Which Wireshark display filter shows only ARP traffic?

Q4 (3 pts): What is the strongest single indicator of ARP spoofing in a capture?

Q5 (3 pts): A host first learns “192.168.1.1 is-at 00:aa:bb:cc:dd:01” and later sees “192.168.1.1 is-at de:ad:be:ef:00:66”. What risk does this create?

Q6 (2 pts): Which ARPGuard alert corresponds to the situation in Q5?

Q7 (2 pts): Why can ARP spoofing still be harmful even if application traffic uses TLS?

Q8 (3 pts): Name two mitigations and briefly explain how each reduces ARP spoofing risk.

Q9 (1 pt): Give one realistic reason ARPGuard might produce a false positive.

Q10 (1 pt): If ARPGuard reports 0 alerts on a benign capture, what conclusion is most defensible?

Part B — Answer Key (Correct Answer + Justification)

Q1 — Answer: ARP resolves an IPv4 address to a link-layer (MAC) address on the local segment.

Justification: Ethernet delivery requires a destination MAC; ARP provides that mapping for local delivery [1].

Q2 — Answer: C (Network-to-Link boundary).

Justification: ARP maps a network-layer identifier (IP) to a link-layer identifier (MAC) for local broadcast domain delivery; it is not an end-to-end transport mechanism.

Q3 — Answer: arp

Justification: Wireshark's protocol filter "arp" matches ARP packets and excludes other protocols.

Q4 — Answer: An IP-to-MAC conflict: the same IPv4 address mapping to different MAC addresses over time.

Justification: Poisoning relies on convincing a host to associate a trusted IP (often the gateway) with an attacker MAC; a mapping change is the direct symptom.

Q5 — Answer: The host may update its ARP cache so frames intended for the gateway IP are sent to the attacker MAC, enabling interception (MITM) or disruption (DoS).

Justification: On a LAN, the ARP cache determines which MAC receives frames for the gateway; poisoning redirects those frames to the attacker.

Q6 — Answer: IP_MAC_CONFLICT

Justification: ARPGuard raises IP_MAC_CONFLICT when it observes the same IP associated with multiple MAC addresses over time.

Q7 — Answer: ARP spoofing can still redirect or disrupt traffic at L2 even if payloads are encrypted; TLS does not prevent link-layer redirection or DoS.

Justification: Encryption protects payload confidentiality/integrity, but it does not stop an attacker from positioning as an on-path forwarder or causing local delivery failures.

Q8 — Answer: (Example 1) DHCP snooping + Dynamic ARP Inspection: the switch validates ARP replies against trusted bindings and drops forged ARP packets. (Example 2) Static ARP entries for critical hosts: the host does not accept unsolicited mapping changes for those entries.

Justification: Both reduce the attacker's ability to inject or propagate forged IP-to-MAC mappings; DAI enforces consistency centrally while static ARP enforces it locally.

Q9 — Answer: Legitimate IP/MAC changes (failover, VM migration, NIC replacement) or gratuitous ARP can look like an IP-to-MAC conflict.

Justification: Heuristic signals can match benign operational events unless the evaluator adds context and network change awareness.

Q10 — Answer: The capture does not contain mapping inconsistencies that match ARPGuard’s heuristics; it does not prove the network is attack-free.

Justification: Absence of detected anomalies is not proof of absence; the detector is limited by capture visibility and rule coverage.

References

[1] D. C. Plummer, “An Ethernet Address Resolution Protocol,” RFC 826, IETF, Nov. 1982.