

ARPGuard Quiz and Answer Key

ARPGuard Quiz and Answer Key (with Justification)

Instructions:

- Unless otherwise stated, answers should be 1–3 sentences.
 - Where applicable, learners should justify the answer by referencing observable ARP behavior in a capture.
- Q1) (Conceptual) What problem does ARP solve on an IPv4 Ethernet LAN?

Answer:

ARP resolves an IPv4 address to a link-layer (MAC) address on the local network segment.

Justification:

An Ethernet frame needs a destination MAC; ARP provides the mapping needed to send IP packets to a next hop [1].

Q2) (Conceptual) In the TCP/IP model, ARP is most closely associated with which boundary?

- A) Application layer
- B) Transport layer
- C) Network-to-Link boundary (local delivery)
- D) Physical layer

Correct Answer: C

Justification:

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

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

Answer:

arp

Justification:

Wireshark's protocol filter "arp" matches ARP packets and excludes other Ethernet/IP traffic.

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

Answer:

An IP→MAC conflict: the same IPv4 address is observed mapping to different MAC addresses over time.

Justification:

ARP poisoning relies on convincing a victim to associate a trusted IP (often the gateway) with an attacker's MAC.

A mapping change for the same IP is a direct symptom of that attack pattern.

Q5) (Applied) 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 for the host?

Answer:

The host may update its ARP cache so that packets intended for the gateway IP are sent to the attacker's MAC,

enabling traffic interception (MITM) or disruption (DoS).

Justification:

On a LAN, the host uses the ARP cache to choose the destination MAC for traffic to the gateway; poisoning redirects those frames to the attacker.

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

Answer:

IP_MAC_CONFLICT

Justification:

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

Q7) (Reasoning) Why can ARP spoofing work even if the attacker cannot break cryptography (e.g., TLS)?

Answer:

ARP spoofing can still redirect traffic at the link layer; without additional controls, the attacker can position itself as a man-in-the-middle or cause denial-of-service regardless of application-layer encryption.

Justification:

ARP poisoning changes who receives Ethernet frames; TLS protects payload confidentiality/integrity, but it does

not prevent redirection or traffic disruption at L2.

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

Answer:

(Example 1) DHCP snooping + Dynamic ARP Inspection (DAI): the switch validates ARP replies against trusted

DHCP bindings and drops forged ARP packets.

(Example 2) Static ARP entries for critical hosts (e.g., gateway): the host does not accept unsolicited mapping

changes, reducing cache poisoning opportunities.

Justification:

Both mitigations reduce the attacker's ability to inject or propagate forged IP→MAC mappings.

Q9) (Limitations) Give one realistic reason ARPGuard might produce a false positive.

Answer:

Gratuitous ARP or legitimate IP/MAC changes (e.g., failover, NIC replacement, VM migration) can cause a real

mapping change that looks like an IP→MAC conflict.

Justification:

ARPGuard uses heuristic signals; legitimate network events can resemble poisoning unless contextualized.

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

Answer:

The capture does not contain ARP mapping inconsistencies that match ARPGuard's heuristics; it does not prove

that the network is attack-free.

Justification:

Absence of detected anomalies is not proof of absence; ARPGuard is limited by what is present in the capture

and by the detector's rule set.

References

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