ARPGuard Project Overview

ARPGuard Project Overview
========================
1. Project Summary

ARPGuard is a compact instructional artifact that demonstrates how Address Resolution Protocol (ARP) behavior
can be observed and how ARP spoofing (ARP cache poisoning) can be detected using simple, explainable heuristics. The author developed ARPGuard to support a hands-on lab sequence that aligns with TCP/IP model
thinking and common network-defense concepts.
The project intentionally combines:
- Learner-facing instruction (lab handout),
- Instructor-facing guidance (facilitator notes),
- A brief assessment instrument (quiz + answer key with justification),
- A small, reproducible technical artifact (PCAPs, Python analyzer, and optional web dashboard).
2. Intended Audience and Scope

The project is designed for a cybersecurity networking course where learners have basic familiarity with:
- IPv4 addressing and subnetting,
- MAC addressing and Ethernet framing,
- Packet capture and inspection concepts (e.g., Wireshark filters).
It does not assume prior experience with ARP poisoning tooling or advanced switch security features.
3. Deliverables (High-Level)

- Lab handout: “Detecting ARP Spoofing with ARPGuard”
- Facilitator notes: timing, common misconceptions, troubleshooting
- Quiz + Answer Key: includes correct answers and justification
- Source code:
- arpguard_core.py (PCAP analyzer),
- arpguard_lab_tools.py (PCAP generation + demo),
- arpguard_web_dashboard.py (optional UI)
- Supporting artifacts:
- benign_arp.pcap
- arp_spoof_attack.pcap
- figure assets (topology + analysis snapshots)
4. Technical Approach (Detection Heuristics)

ARPGuard focuses on transparent indicators that learners can validate directly in a capture:
- IP→MAC conflict: the same IPv4 address is observed mapping to multiple MAC addresses over time.
This is a primary symptom of ARP cache poisoning in a local broadcast domain [1].
- Unsolicited ARP replies: ARP “is-at” replies observed without a recent “who-has” request.
This can indicate poisoning behavior, though legitimate gratuitous ARP exists; ARPGuard treats it as a softer
signal (lower severity).
- MAC fanout: a single MAC address claims a large number of IPv4 addresses (threshold-based), which can be
suspicious depending on context.
5. Safety and Ethics

ARP spoofing is a real attack technique. The project materials assume a controlled lab environment and either
(a) synthetic PCAPs, or (b) instructor-authorized isolated networks. Learners should not attempt spoofing on production or campus networks. The lab can be completed using the provided PCAPs without running any live
spoofing tools.
6. References

----
[1] D. C. Plummer, “An Ethernet Address Resolution Protocol,” RFC 826, Nov. 1982.
[2] Wireshark Foundation, “Address Resolution Protocol (ARP),” Wireshark User’s Guide, accessed 2025-12-14.
[3] Cisco Systems, “Dynamic ARP Inspection,” security configuration documentation, accessed 2025-12-14.
[4] IEEE, “IEEE 802.1X Port-Based Network Access Control,” standard overview, accessed 2025-12-14.