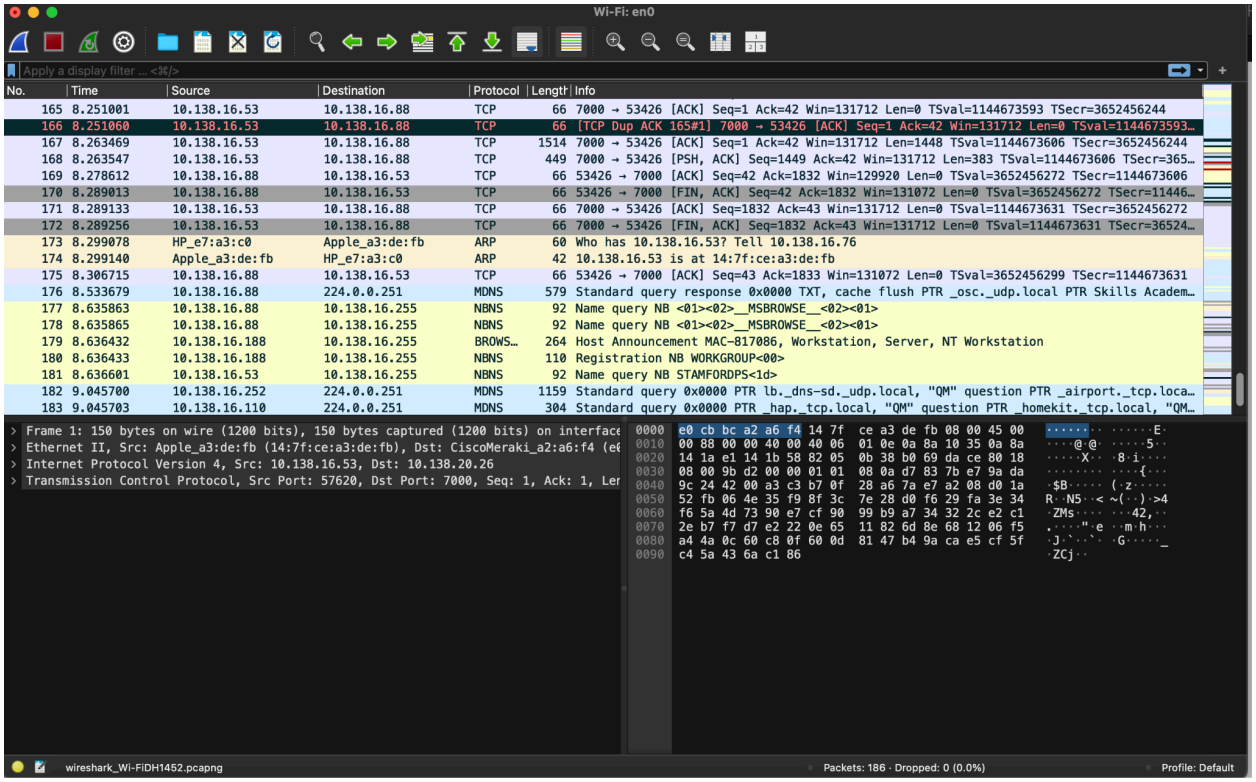

Network Protocol & Traffic Analysis Project Report

---

1. Packet Capture & Protocol Identification

Screenshot Reference: Screenshot 2025-05-07 at 3.57.12 PM

Identified Protocols:

- **TCP (Transmission Control Protocol)**
  Example: Packet No. 165, 166
  - Reliable, connection-oriented protocol used for data exchange.
- **ARP (Address Resolution Protocol)**
  Example: Packet No. 173, 174
  - Resolves IP addresses to MAC addresses for local network communication.
- **MDNS (Multicast DNS)** and **NBNS (NetBIOS Name Service)**
  Example: Packet No. 176–183
  - Used for name resolution on local networks without a centralized DNS server.

These protocols are commonly seen in internal network traffic. TCP handles actual communication, while ARP, MDNS, and NBNS assist with addressing and name resolution.

---

2. Vulnerability Assessment of ARP

Target Protocol: ARP

Packets Referenced: 173, 174

Description:

- ARP does not have any form of authentication or verification.
- Anyone on the network can send a fake ARP reply.

Example Vulnerability: ARP Spoofing / Man-in-the-Middle (MITM)

- A malicious actor can send a fake ARP reply associating their MAC address with a victim's IP.
- This allows interception or redirection of traffic.

Conclusion:

- ARP is vulnerable by design and should be monitored closely.
- Mitigation strategies: dynamic ARP inspection, static ARP entries, and network segmentation.

---

3. Network Performance Metrics (Security Perspective)

Observed Metrics in Wireshark:

- **Sequence Numbers & Acknowledgments:** Indicates packet delivery and tracking.
- **TCP Window Sizes:** Reflects available buffer size; anomalies might hint at resource exhaustion.
- **Dropped Packets:** 0.0% drop rate observed (indicating good health during capture).
- **Timing:** Timestamp analysis shows consistent and timely packet flow.

Security Insight:

- No retransmissions or delays = no DoS or packet loss during this session.
- Consistent flow and no strange retransmits suggest clean performance.

---

4. Traffic Pattern Analysis

Normal Traffic:

- TCP communication between internal IPs (e.g., 10.138.16.53 ↔ 10.138.16.88).
- ARP request/reply sequences are typical for MAC resolution.

Suspicious Traffic:

- High volume of NBNS and MDNS packets (e.g., Packets 176–183):
    - Repetitive queries to multicast addresses.
    - Might indicate broadcast storm, misconfigured client, or network reconnaissance.

Conclusion:

- Monitor broadcast/multicast services.
- Apply traffic filters (e.g., `udp.port == 5353`) to isolate and audit such traffic.

---

5. Conclusion

This packet capture reveals:

- Standard use of TCP, ARP, MDNS, and NBNS.
- Vulnerability in ARP that can lead to MITM attacks.
- Performance metrics indicate a healthy connection.
- Slight anomaly detected in the frequency of name resolution protocols, which may warrant further investigation.