SYS-207 – Networks (Assessment Only)
00050 - Understand how addressing interface, routing, hierarchical address assignment and hierarchical routing, network-layer error reporting, network address translation address issues of the Network Layer

Name: Thanawin Pattanaphol **ID: 01324096**

Objective

Capture a traffic trace with Wireshark and identify where three Network-Layer techniques appear in the trace, then, interpret one of those techniques in detail using the official protocol standards.

Captured Trace

The trace was captured on the eno1 interface, in this context, the Wi-Fi card; shown in Figure 1.

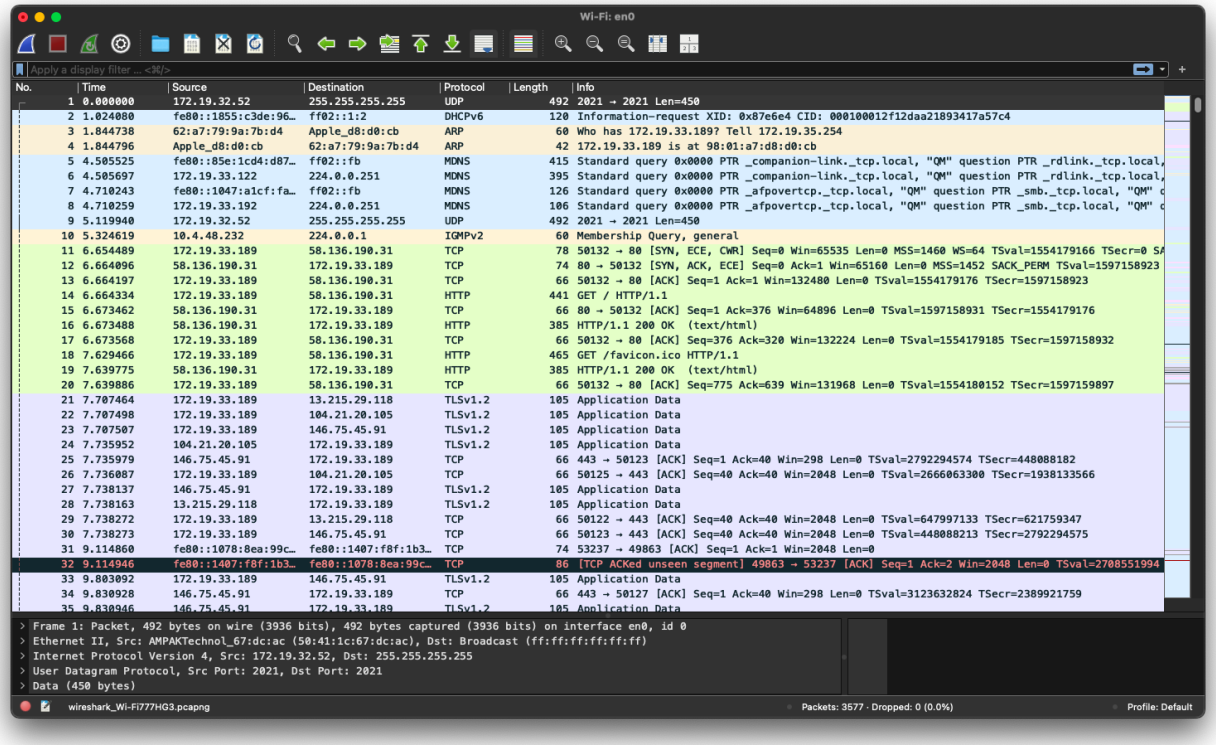

Figure 1

Network-Layer Techniques

To demonstrate the different Network-Layer techniques shown in the Wireshark trace, this report will display three different techniques that can be found in this trace.

Addressing

The figure below shows the Internet Protocol Version 4 (IPv4) section with its respective source and destination addresses. This demonstrates the Network-Layer technique of addressing of the RFC 791 Internet Protocol Standard of the DARPA Internet Program. [1]

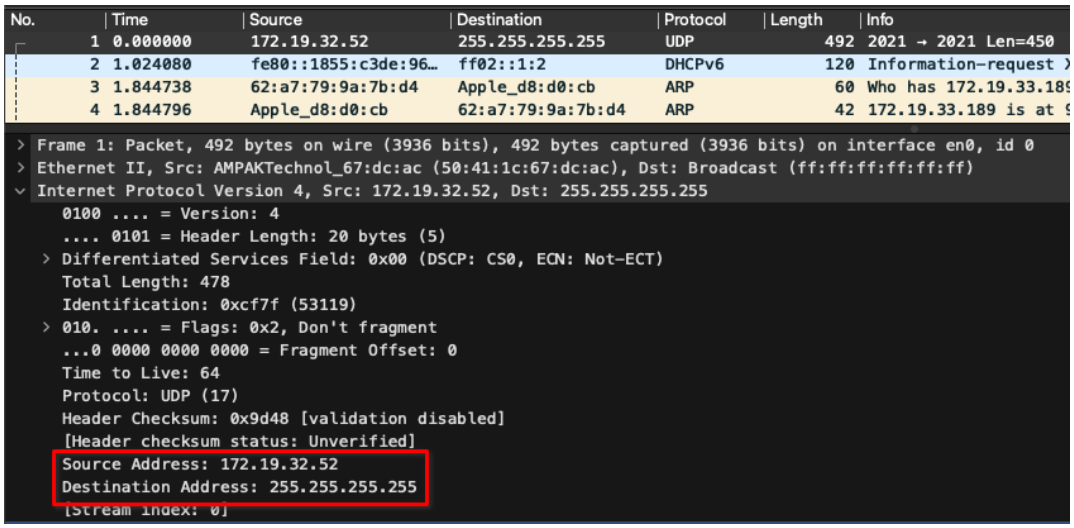

Figure 2

As seen above, RFC 791 defines the IPv4 header files, i.e. Address, TTL (Time to Live), header checksum, in which is a type of "addressing" technique in the Network Layer.

Routing – Decreasing TTL values across packets

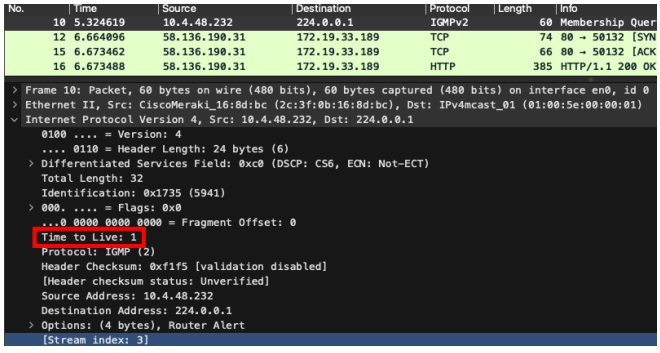

Figure 3

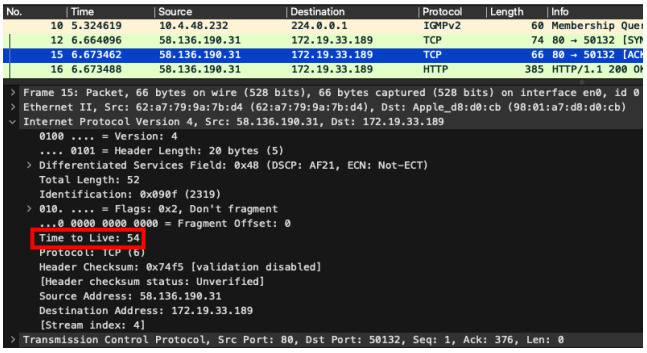

Figure 4

Figure 3 & 4 displays two different packets that were filtered using ip.ttl < 64. This is to display the TTL or Time-To-Live values in that they are below the initial TTL values of 64 or 128. As specified in RFC 791, every router decrements TTL by at least one before forwarding a packet [3], therefore, the TTL values of the packets display that multiple routing hops were involved, demonstrating active network-layer routing behavior.

Network-layer error reporting

Figure 5 displays the ICMP section, in which, shows its type to be 3 or "Destination Unreachable". This is specified in RFC 792 where it defines Type 3 and codes, returned internet header + 64 bits to allow the sender to match the error to an originating process. [2]

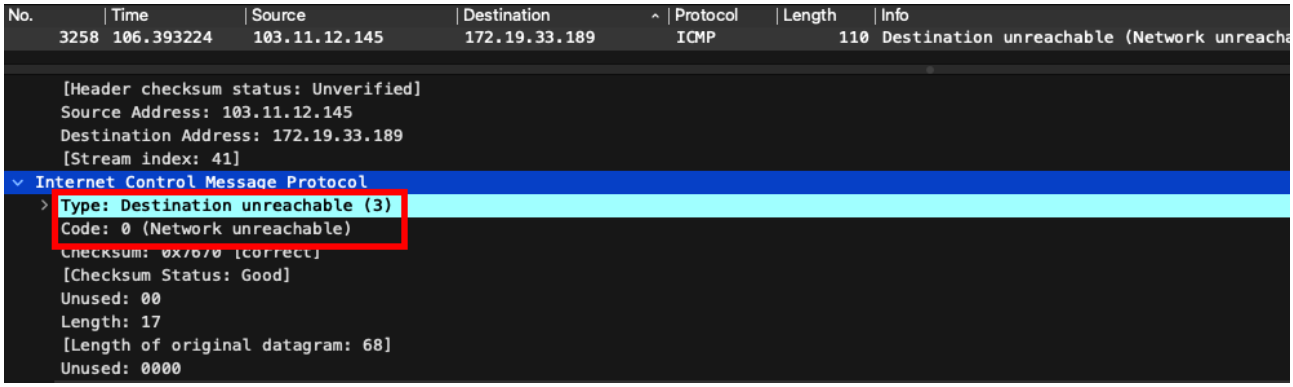

Figure 5

References

[1] J. Postel, **Internet Protocol**, RFC 791, Sep. 1981. (See *§1.4 Operation*, *§2.3 Addressing*, pp. 1–6 for addressing, TTL, fragmentation).

[2] J. Postel, **Internet Control Message Protocol**, RFC 792, Sep. 1981. (See *"Destination Unreachable Message"* and *"Time Exceeded Message"*, pp. 4–6 — packet formats, Type/Code meanings, and the requirement to include the original IP header + 64 bits.)

[3] J. Postel, **Internet Protocol**, RFC 791, Sep. 1981. (See §3.2.1 Time to Live, pp. 14–15 — TTL decrement by each router; packet lifetime limitation; hop-by-hop forwarding behavior.)