

CASE INCIDENT INVESTIGATION REPORT

Using Wireshark for Root Cause Analysis and Remediation of Local Area Home Network Disruption

Date of Report: July 22, 2026

Classification: Internal Technical Documentation

Report documented by: Michael Andrei P. Niñora

Status: Resolved

Disclaimers:

- I am not a professional in these fields. But documenting and figuring out solutions in these findings could help me learn and deepen my knowledge.
- This is not a school project, although some of these tools I learned from school and with the help and guidance of AI, meaning I carefully analyze my prompts and give context and constructive feedback to AI tools so it could guide me and help me learn.
- There will be a highlight indicator `like this` in which it will highlight any commands used in this case.
- To safeguard private network details, some specific octets of the IP addresses displayed in this report have been partially masked using asterisks (*).

1.) Executive Summary

On July 22, 2026, a network connection failure impacted multiple endpoints across the local home environment . The primary symptom manifested as an inability for end-user devices to obtain IP addresses or reach external internet destinations. At the same time, a secondary hardware fault indicator was observed on the TP-Link range extender situated in the upper-living room , which displayed a blinking red fault LED (blinking red issue).

Packet analysis conducted via Wireshark identified a critical layer 2/layer3 IP address conflict between an active workstation and the primary TP-Link range extender ("Alien"). Both devices attempted to claim the same local IPv4 address, `192.168.1.*` . This identity collision corrupted the Address Resolution Protocol (ARP) tables, prevented Dynamic Hosts Configuration Protocol (DHCP) relaying, and isolated downstream network extenders.

Full service restoration was achieved by executing a coordinated physical power-cycle and ARP/DHCP lease flush across the primary PLDT gateway and both extension nodes. Post-fix traffic capturing confirmed that the conflict was resolved, with the extender successfully re-homed to a clean IP address (`192.168.68.***`) and operated as a transparent Layer 2 bridge.

2.) Environment and Network Topology Description

The environment consists of a multi-node wireless extension architecture configured as follows:

- **Primary Internet:** 1 PLDT WiFi FiberHome Router acting as a primary DHCP server for the bedroom. NAT gateway, and DNS forwarder.
- **Primary Extension Node ("Alien"):** 1 TP-Link WiFi Repeater positioned inside the primary room, positioned adjacent to the PLDT FiberHome router; Alien is basically the name of our WiFi repeater when an end-user wants to connect through WiFi settings, the name "Alien" will appear.
- **Secondary Extension Node:** 1 TP-Link Wi-Fi Repeater positioned in the upper living room, relaying signals to distant endpoints.
- **Our Endpoints (basically our devices/gadgets):** Multiple workstation, mobile, and guest endpoints connecting dynamically via 2.4GHz / 5GHz wireless bands.

Sanitization Note: All public WAN IP addresses, external routing tables, and sensitive pre-shared keys have been redacted or omitted to protect private network credentials. Local private IP addresses reflect captured environment states.

3.) Tools and Key Findings

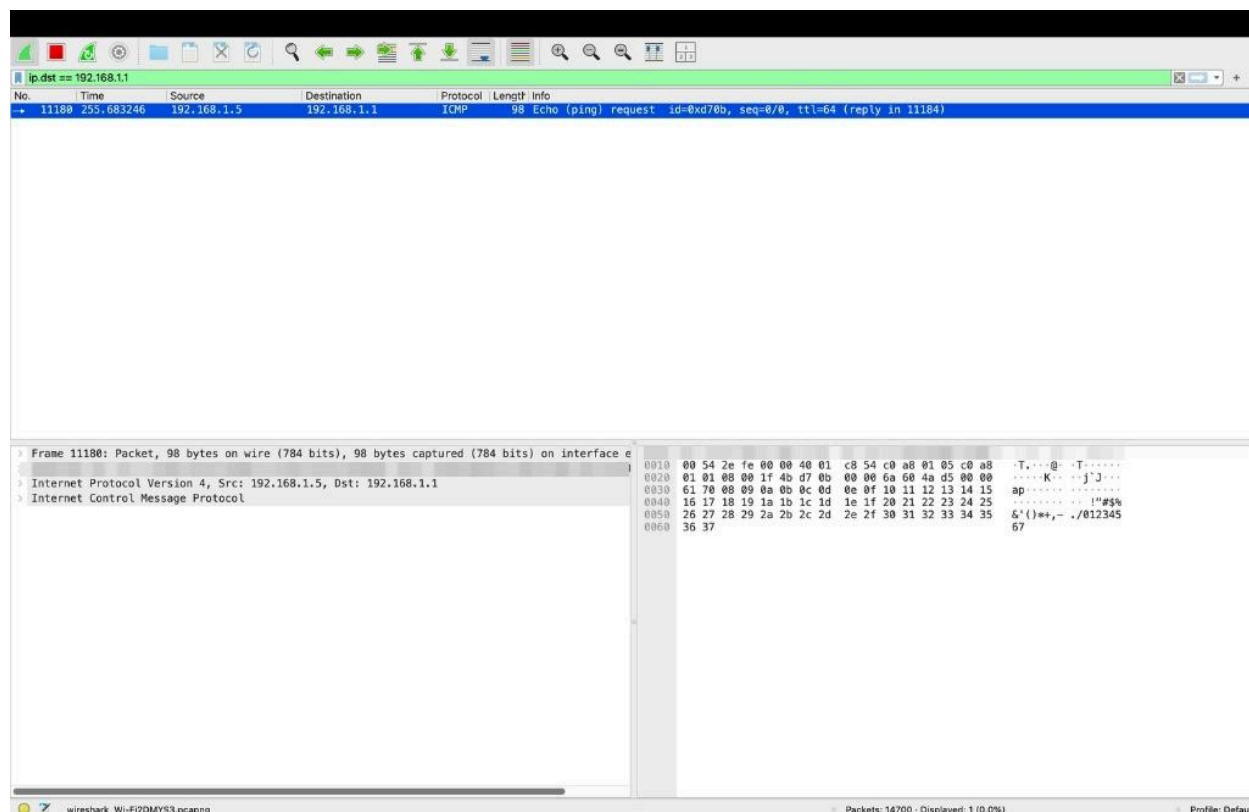
Tools Used:

- **Wireshark v4.x:** Packet sniffing, display filtering, protocol hierarchy evaluation, and Expert Information analysis.
- **macOS Command Line Utilities:** Terminal (`ipconfig getifaddr en0/en1`) for local socket and routing verification.

4.) Symptom and Initial Isolation

1. **User Symptom:** Multiple client endpoints, including mobile devices and secondary laptops, failed to establish internet connectivity. Endpoints remained stuck in an "Obtaining IP Address" loop or displayed "WiFi icon with exclamation point and indicates no connection"
2. **Hardware Indicator:** The TP-Link repeater in the upper living room displayed a red LED signal, indicating complete loss of wireless backhaul connection to the root gateway.
3. **Local Endpoint Check:** The analyst's workstation verified gateway reachability by issuing ICMP echo requests to the default gateway (`192.168.1.1*`). While basic ping requests succeeded, broader network stability degraded rapidly during simultaneous web requests.

Figure 1. Initial Gateway Isolation Test showing outbound ICMP Echo (ping) Request from local workstation (192.168.1.5) to Default Gateway (192.168.1.1*).*



5.) Use of Wireshark for Evidence Gathering

The investigation commenced by capturing live packets on the active wireless interface (en0 / Wi-Fi) and applying incremental display filters to isolate anomalous behaviors.

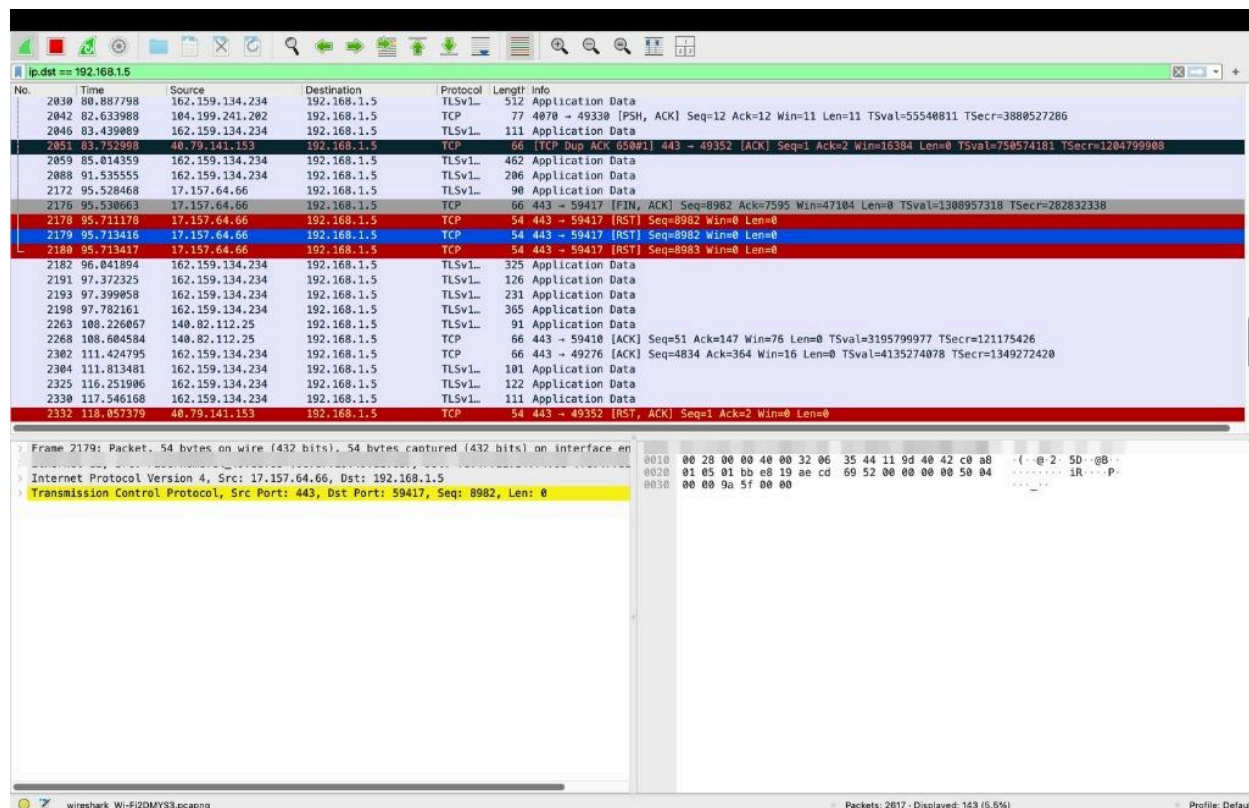
Step 1: Evaluating Workstation Inbound Traffic

In order to inspect incoming packets sent to the local endpoint (my computer), the following filter was executed:

`ip.dst == 192.168.1.5*` – I use this command to filter for all incoming data sent specifically to my computer's IP address. This helps us see if external web servers can reach my machine or if incoming connections are dropping and getting reset ([RST]).

Observation: Wireshark logged numerous TCP anomalies, specifically TCP Resets ([RST]) and Duplicate Acknowledgments ([TCP Dup ACK]); multiple external servers (e.g., Apple, Microsoft endpoints) were terminating connections abruptly due to lost state tracking.

Figure 2. Inbound Packet Analysis (`ip.dst == 192.168.1.5`) highlighting TCP Reset packets ([RST]) in red and Duplicate Acknowledgements in dark red.



Step 2: Isolating Extender Hardware Traffic

To inspect packet flows specifically generated by or directed to the TP-Link extender, the hardware MAC address filter was applied:

`eth.addr == 12:3e:cc:ba:96:db` – I use this command to isolate every packet related to the TP-Link repeater's specific hardware MAC address. This cuts out all other network background noise so you can focus exclusively on what the repeater is doing.

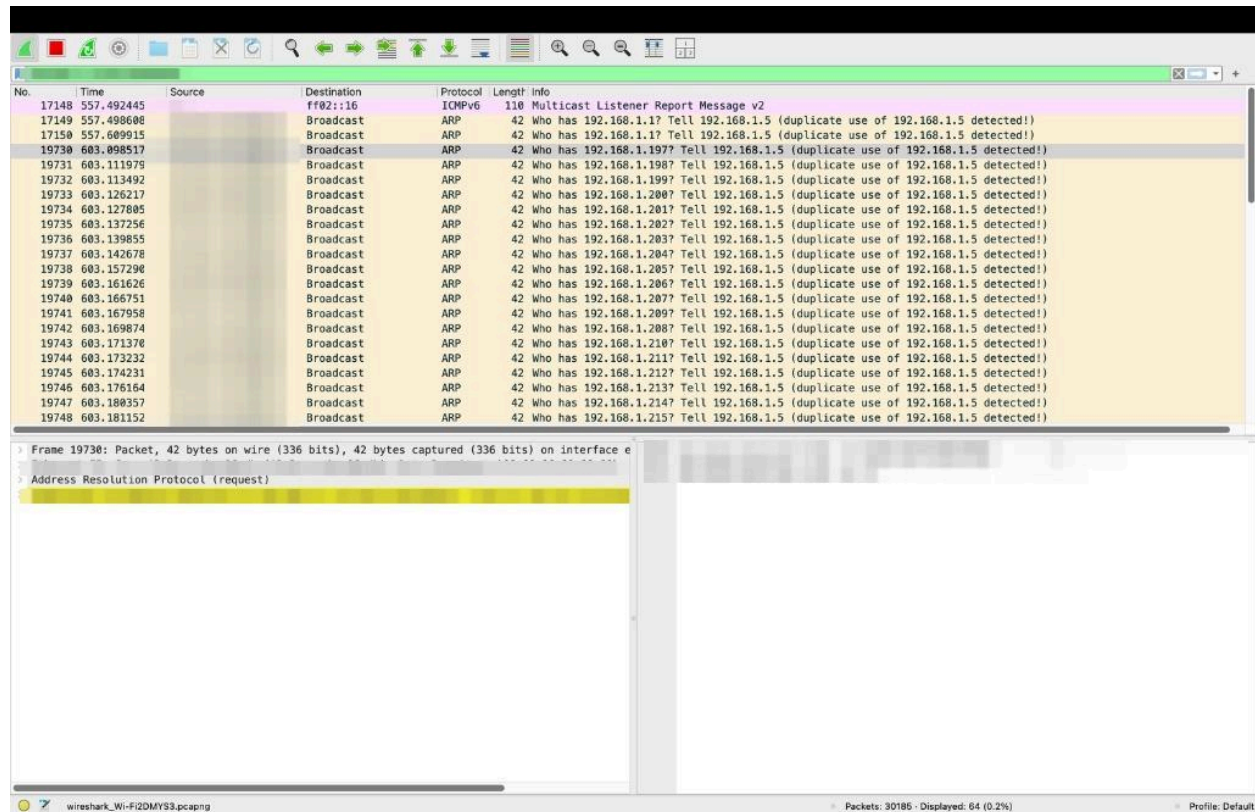
Observation: Wireshark recorded a massive volume of broadcast ARP request frames generated by the extender, structured as follows:

Note: This text came from Wireshark.

Source: 12:3e:cc:ba:96:db

Info: Who has 192.168.1.X? Tell 192.168.1.5*

Figure 3. Extender MAC Analysis (`eth.addr == 12:3e:cc:ba:96:db`) showing flooded ARP broadcast requests and the yellow duplicate IP warning banner.



Step 3: Specific ARP Source Filtering and Detail Analysis

To isolate outbound ARP broadcasts originating strictly from the extender's network interface, the analyst executed:

`arp and eth.src == 12:3e:cc:ba:96:db` – Uses of this command is to look strictly at Address Resolution Protocol (ARP) announcements sent *out* by the repeater. This isolates the exact moment the repeater broadcasts to the network claiming ownership of the conflicting 192.168.1.5* IP address.

Observation: The extender was actively broadcasting to every address in the subnet (.197, .198, .201, etc.), asserting that MAC address 12:3e:cc:ba:96:db owned IP 192.168.1.5*. Simultaneously, frame 19560 in the capture history showed the analyst's workstation (fe:47:d1:14:f4:6d) claiming the exact same IP address.

Figure 4. Extended Packet Trace showing persistent Layer 2 broadcast loops generated by the extender prior to reboot.

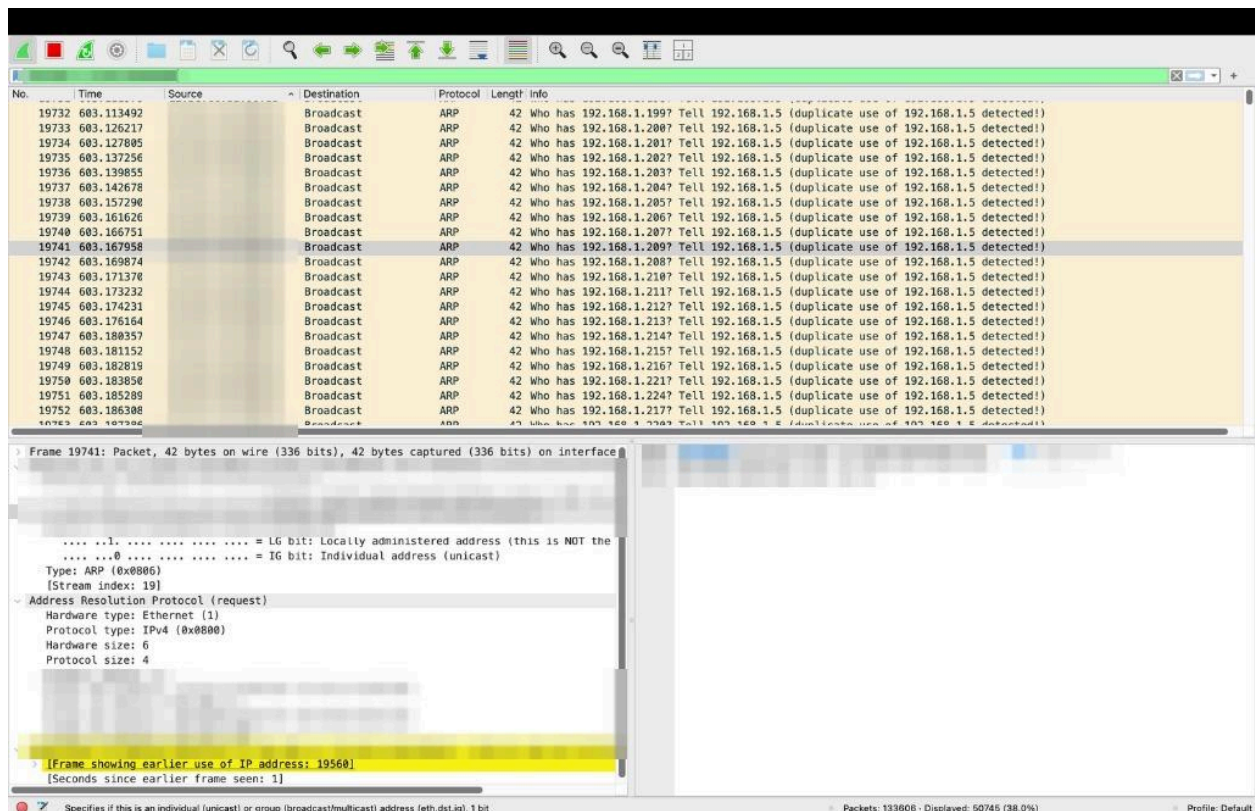
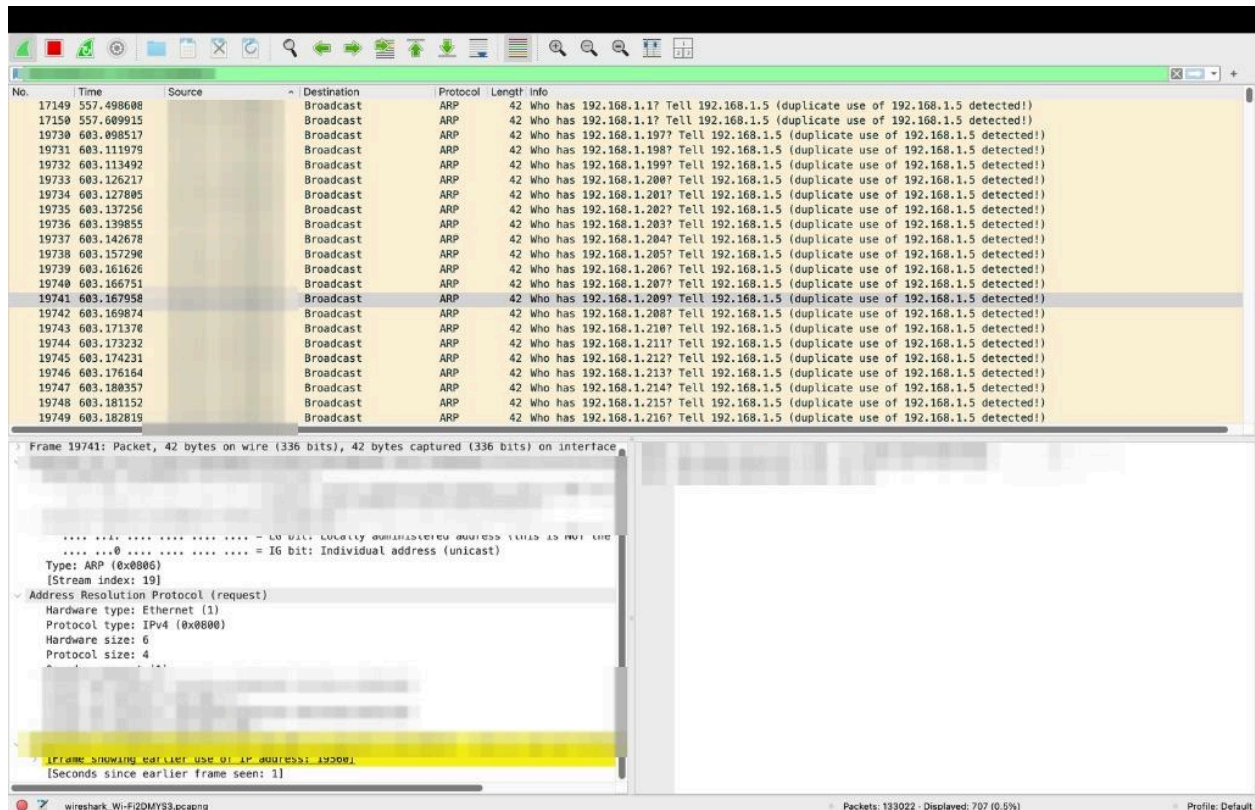


Figure 5. Isolated ARP Source Traffic (arp and eth.src == 12:3e:cc:ba:96:db) displaying continuous broadcast probes across the .1 subnet. Prior to reboot.



Step 4: Expert Information Diagnostic Confirmation

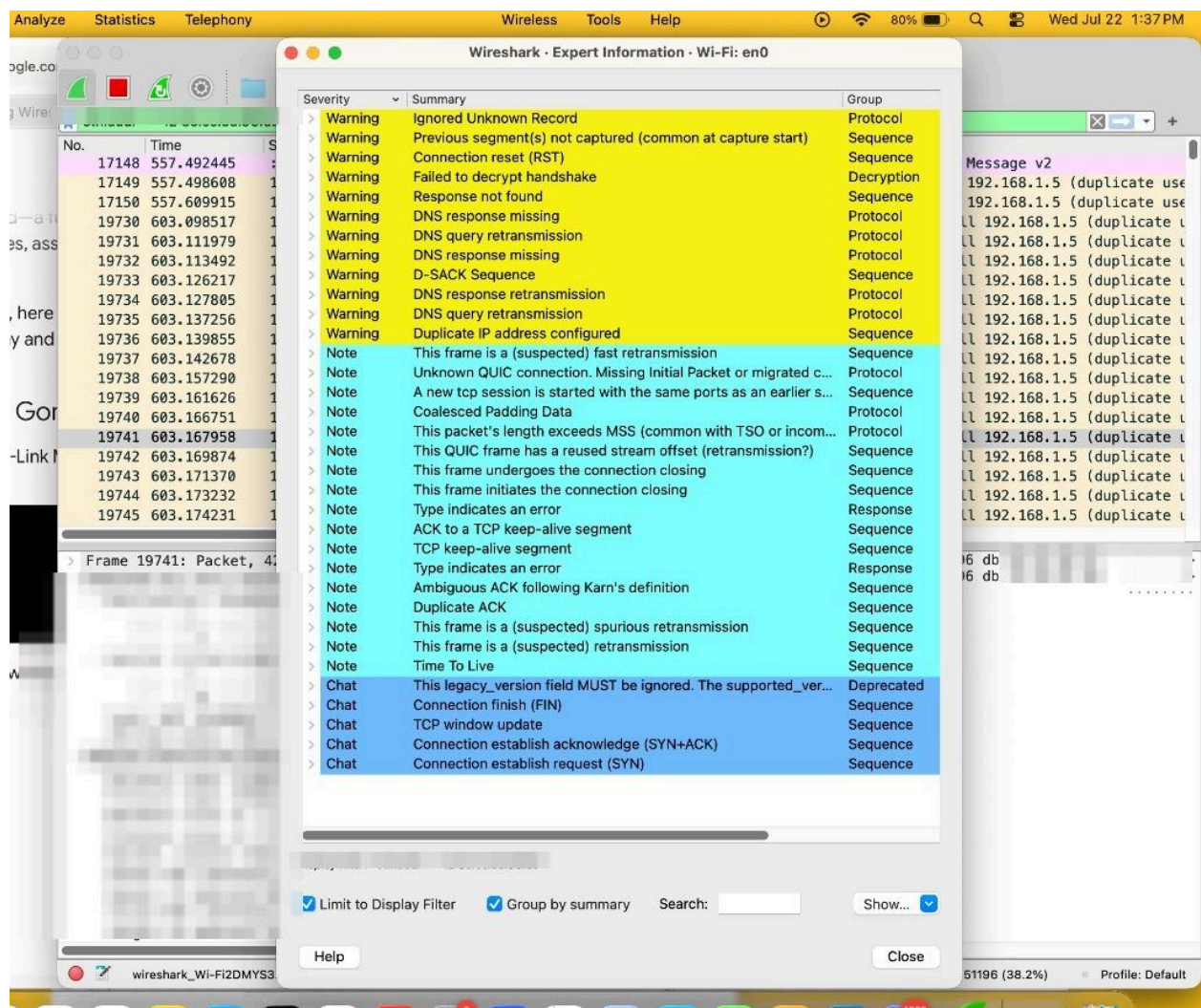
Opening Wireshark's **Expert Information** window (Analyze -> Expert Information) confirmed the critical flaw:

- Severity: Warning
- Group: Sequence
- Protocol: ARP / IPV4
- Summary Text: [Duplicate IP address detected for 192.168.1.5* (12:3e:cc:ba:96:db) - also in use by fe:47:d1:14:f4:6d (frame 19560)]

Additional Errors generated by this state included:

- **DNS query retransmission** (DNS requests dropping due to routing ambiguity)
- **DNS response missing** (Gateway responses delivered to incorrect hardware interface)
- **Connection reset (RST)** (Abrupt TCP socket termination)

Figure 6. Pre-Fix Expert Information Window displaying critical warnings, including 'Duplicate IP address configured', dropped DNS queries, and decryption alerts.



6.) Remediation Strategy

Since PLDT gateway's internal DHCP lease table was corrupted with conflicting binding entries, a software-only release was insufficient; a full physical power-cycle sequence was implemented to clear volatile memory on all network nodes.

Solution: Unplug and Plug it back

1. **Complete Power Disconnection:** Unplugged the primary PLDT FiberHome router, the primary room repeater ("Alien") from physical power sockets simultaneously.
2. **Capacitor Discharge Period:** Maintained total power termination for 30 seconds to ensure full memory wipe of internal ARP tables and DHCP binding states (in a nutshell, just wait for 30 seconds once you unplug both the router and the primary repeater.)
3. **Sequential Boot Sequence:**

- ☒ ~~Re-powered the primary PLDT FiberHome router first; allowed 2 minutes for WAN sync and DHCP service initialization.~~
- ☒ ~~Re-powered the primary room repeater ("Alien") second; allowed auto-association with the gateway.~~
- ☒ ~~Re-powered the primary room repeater ("Alien") second; allowed auto-association with the gateway.~~

7.) Post Fix Verification and Key Takeaways

Verification Steps

Following the power-cycle sequence, a fresh live packet capture was initiated in Wireshark; the hardware filter was applied once more to inspect live bridge behavior:

```
eth.addr == 12:3e:cc:ba:96:db
```

Results:

1. **Clean IP Re-Assignment:** Frame #8 of the new capture confirmed that the TP-Link extender successfully requested and received a clean, unique IP address (192.168.68.107*) from gateway 192.168.68.1*:

```
Info: 192.168.68.107* is at 12:3e:cc:ba:96:db
```

2. **Zero Duplicate IP Warnings:** The yellow warning banners and Expert Info alerts regarding duplicate IP addresses vanished completely.
3. **Protocol Normalization:** Traffic shifted cleanly to standard encrypted web protocols (TLSv1.3, TCP, QUIC) without packet loss.
4. **Hardware Status:** The upper living room extender restored its normal white/blue status LED, confirming active backhaul link; all client endpoints re-established stable internet access immediately.

Figure 7. Live Post-Fix Capture showing successful ARP resolution with clean IP 192.168.68.107*, active TLSv1, and QUIC streaming traffic without errors (current state; it's good na).

The screenshot displays the Wireshark network protocol analyzer interface. The top toolbar contains various icons for file operations, packet list, packet details, and packet bytes. The main window is divided into three panes: Packet List, Packet Details, and Packet Bytes.

Packet List: Shows a list of captured packets. The columns are No., Time, Source, Destination, Protocol, Length, and Info. The packets are numbered 1 through 24, showing a sequence of TCP and QUIC traffic between 192.168.68.107 and 57.144.228.141.

Packet Details: The selected packet (No. 8) is expanded, showing the following structure:

- Frame 8: Packet, 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface en0, [Ethernet II] [Standard] [Ethernet II, Type: ARP (0x0806)] [Stream index: 0]
- Address Resolution Protocol (reply)
- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4

Packet Bytes: The selected packet (No. 8) is expanded, showing the raw data in hexadecimal and ASCII format. The data is a sequence of bytes representing the ARP request.

Status Bar: The bottom status bar shows "Wi-Fi: en0: <live capture in progress>" and "Packets: 125 / Displayed: 105 (84.0%)".

Figure 8. Live Post-Fix from Expert Information, specific search on (eth.addr == 12:3e:cc:ba:96:db) it shows nothing, meaning no issues/errors.

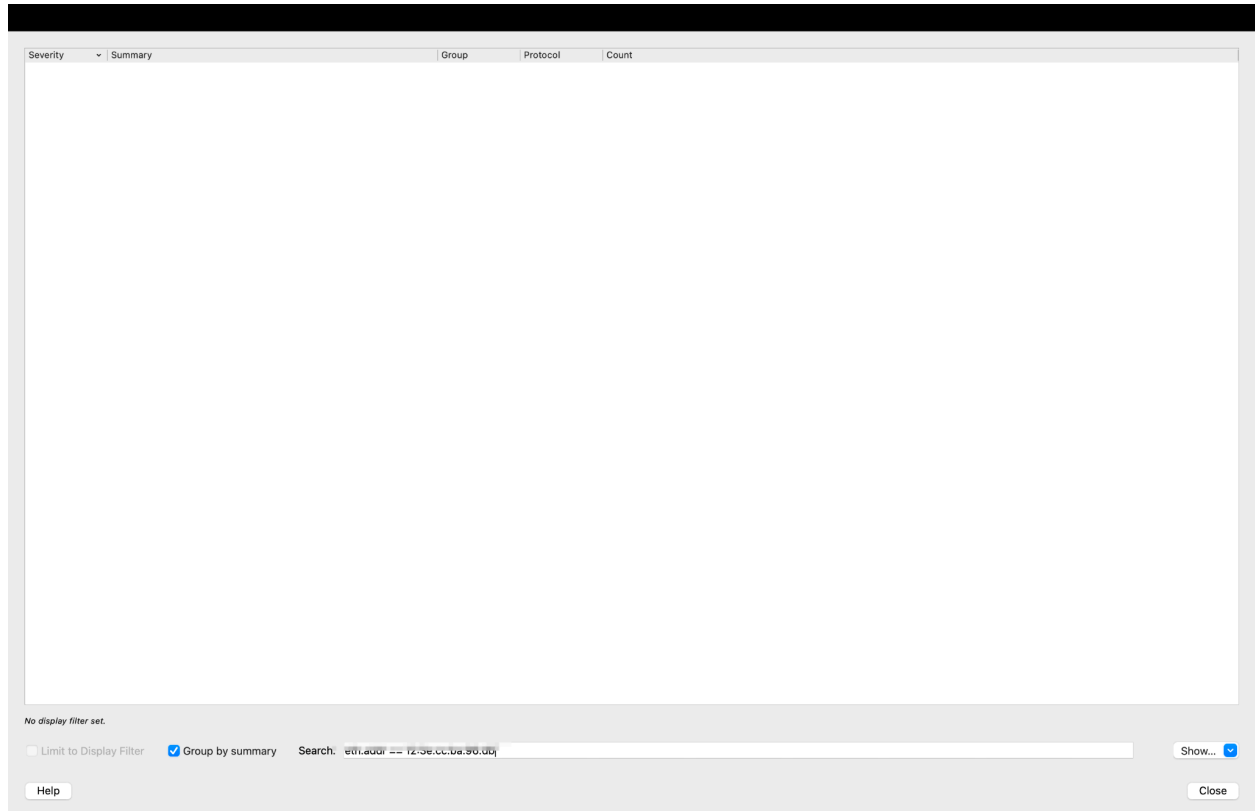


Figure 9. Topology status; Living Room TP-Link Repeater is clean; no blinking lights.

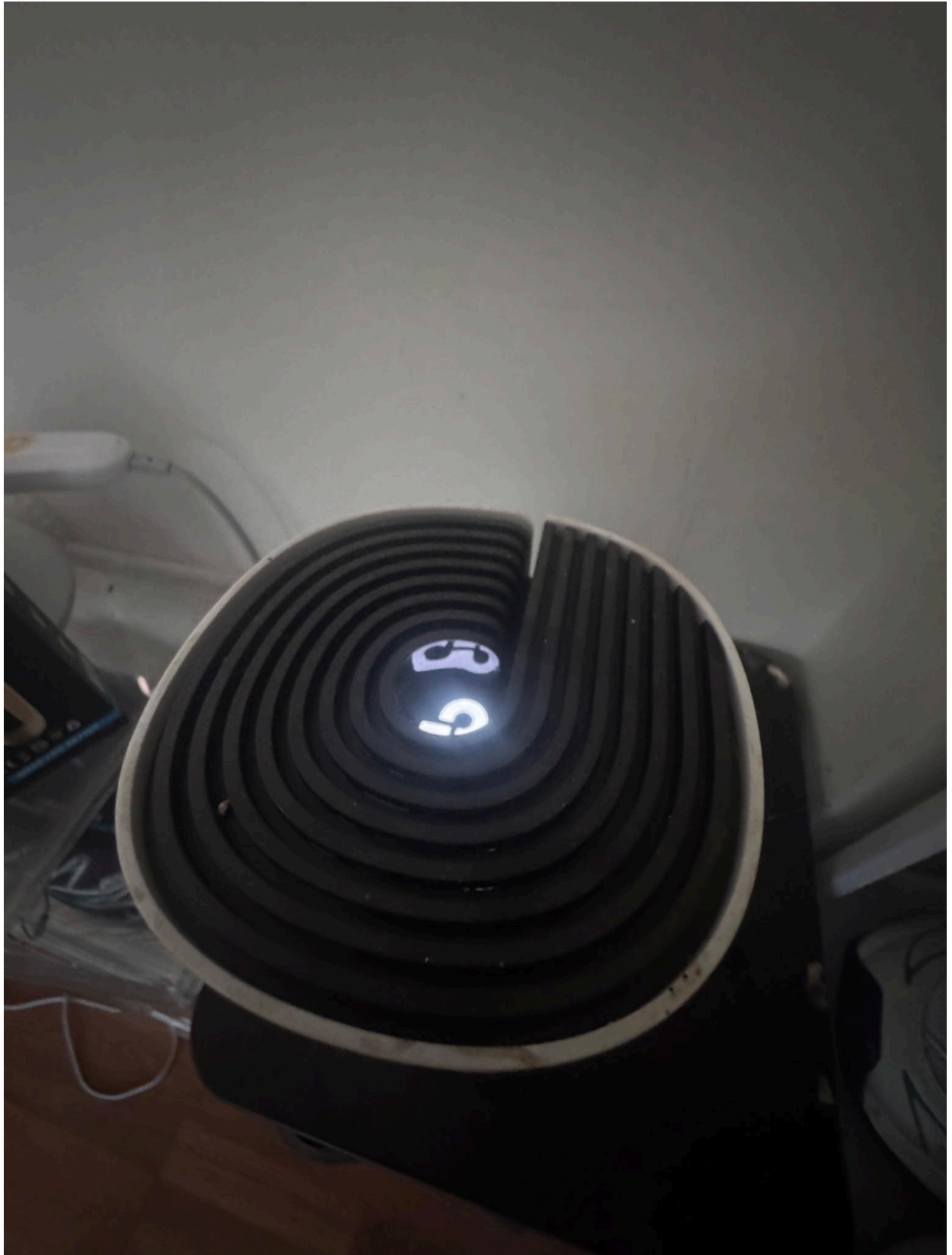


Figure 10. Topology status; PLDT WiFi Router in Main Room clean; no issues.



Figure 11. Topology status; TP-Link Primary WiFi Repeater inside main room clean; no issues



Documented Wireshark Commands Reference Table

Filter Command	Purpose	Finding / Result
<code>ip.dst == 192.168.1.5*</code>	Inspects inbound traffic targeting the workstation	Revealed TCP resets and dropped ACKs
<code>ip.addr == 192.168.1.1*</code>	Monitors bi-directional traffic with default gateway	Confirmed baseline gateway ICMP status
<code>eth.addr == 12:3e:cc:ba:96:db</code>	Filters all frames involving the TP-Link MAC address	Isolated extender behavior from general noise
<code>arp and eth.src == 12:3e:cc:ba:96:db</code>	Filters ARP requests specifically sent by the extender	Uncovered continuous ARP broadcasts claiming .5*
<code>dns</code>	Scans for Domain Name System queries	Identified dropped lookup requests during outage

Key Takeaways

(1) How Extender Conflicts Cause Outages: Wi-Fi extenders pass internet traffic back and forth to your main router. If an extender accidentally claims the same IP address as your laptop or phone, the router gets confused, which cuts off internet access for all devices connected through that extender.

(2) Looking Beyond Warning Lights: A red blinking light on a repeater only tells you that the connection is broken, but it won't tell you why. Using packet analysis tools like Wireshark lets you look "under the hood" to find the exact root cause of the problem.

(3) How a Healthy Extender Behaves: A working extender acts like a silent middleman; it passes your internet traffic through without making extra noise on the network. Seeing very little direct background traffic from the repeater itself during active browsing is proof that it is working perfectly.

(4) Importance of Wireshark: With the use of PCAP tools such as Wireshark able to guide and help me for deep analysis of packets and network traffics applied into this case.

~end of document