

The Disappearing 'DORA'

—Deep-Dive Troubleshooting of DHCP Acquisition Failures in
Enterprise Wi-Fi Networks

1 Introduction

In enterprise WLAN operations, one of the most frequently encountered issues is the classic scenario where a client device shows a strong Wi-Fi signal but becomes stuck while obtaining an IP address.

Under the OpenWiFi / AsterAPNOS architecture, the Campus Controller and Access Points operate in a fully decoupled control-plane and data-plane model. The controller handles only control traffic—such as configuration provisioning, status monitoring, and telemetry collection—without processing, forwarding, or participating in any client data traffic. All user traffic, including DHCP broadcast and unicast exchanges, is handled locally at the AP edge through the Local Data Plane.

Within this architecture, when IP address assignment fails, the controller is not directly involved in packet forwarding. However, its integrated network-wide visibility—including Associated Link topology mapping, Trend Matrix analytics, and Key Event correlation—provides a powerful “single pane of glass” view into underlying data-plane failures.

By leveraging these multidimensional visual dashboards, engineers can move systematically from symptoms to root cause, narrowing the troubleshooting scope from a network-wide perspective down to the exact DHCP failure point. This article demonstrates how to use these capabilities to rapidly identify and isolate DHCP-related issues in enterprise wireless networks.

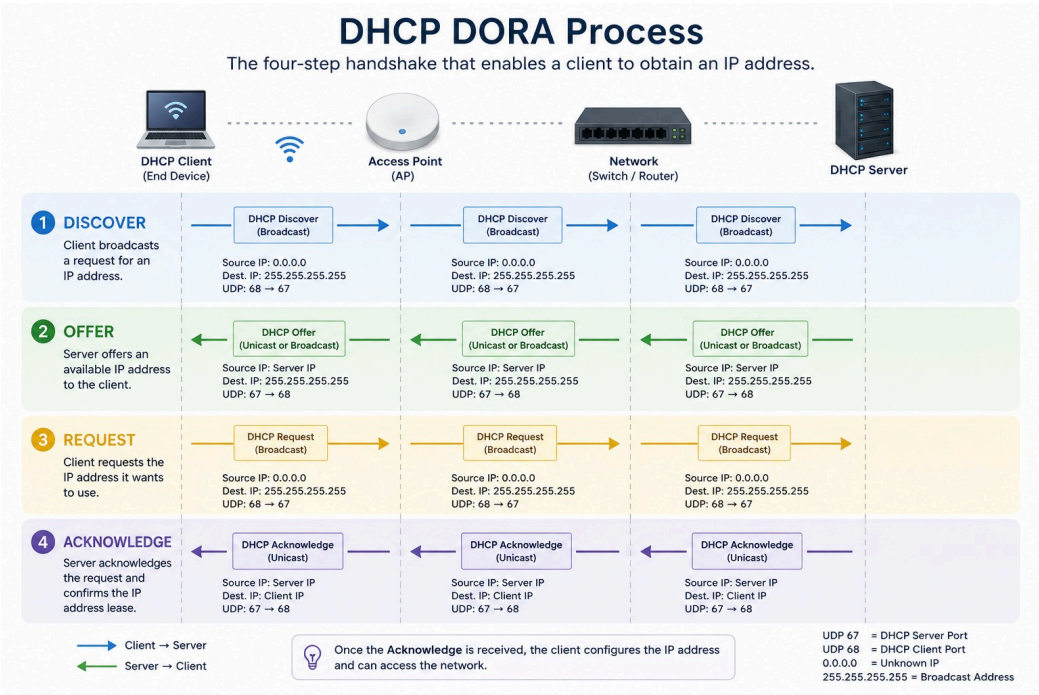


Figure 1 DHCP DORA

2 Macro-Level Troubleshooting: Using the Overview Dashboard for a Three-Dimensional Rapid Assessment

When a user reports that a device is unable to obtain an IP address—or when the controller raises a DHCP-related alert—the investigation should begin with the **Client Overview Dashboard**.

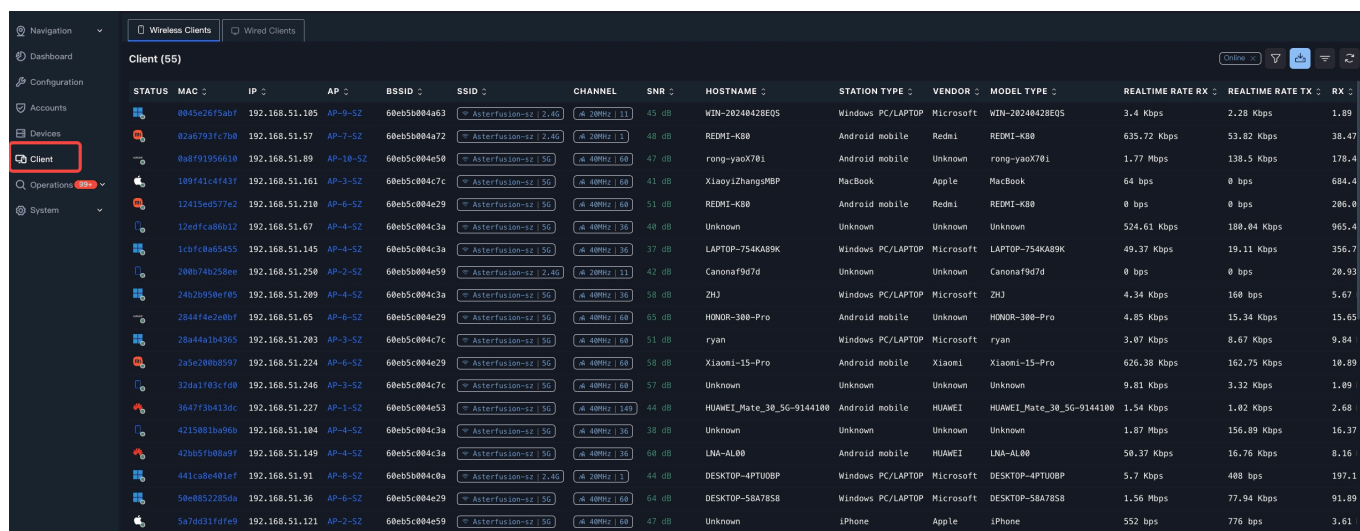
Rather than diving directly into packet captures, engineers should first leverage the controller’s global visibility to perform a rapid health assessment. The Overview Dashboard acts as a network-wide observability layer, providing immediate insight into client behavior, AP status, and network trends.

Through three key visualization components, engineers can quickly answer three critical questions:

-  **Is the issue isolated or widespread?**
-  **Is the problem client-related, AP-related, or network-related?**
-  **When did the failure begin, and is it still occurring?**

By answering these questions first, the troubleshooting scope can be dramatically reduced before moving into detailed packet-level analysis.

[Navigation: Site → Client]



STATUS	MAC	IP	AP	BSSID	SSID	CHANNEL	SNR	HOSTNAME	STATION TYPE	VENDOR	MODEL TYPE	REALTIME RATE RX	REALTIME RATE TX	RX
Online	0045c26f5abf	192.168.51.105	AP-9-5Z	60eb5b004a63	Asterfusion-12 2.4G	40MHz 11	45 dB	WIN-20240428E05	Windows PC/LAPTOP	Microsoft	WIN-20240428E05	3.4 Kbps	2.28 Kbps	1.89
Online	82a6793fc7b0	192.168.51.57	AP-7-5Z	60eb5b004a72	Asterfusion-12 2.4G	40MHz 1	48 dB	REDMI-K80	Android mobile	Redmi	REDMI-K80	635.72 Kbps	53.82 Kbps	38.47
Online	0a8f191956610	192.168.51.89	AP-10-5Z	60eb5c004e50	Asterfusion-12 5G	40MHz 68	47 dB	rong-yaoX70i	Android mobile	Unknown	rong-yaoX70i	1.77 Mbps	138.5 Kbps	178.4
Online	189f43c4f43f	192.168.51.161	AP-3-5Z	60eb5c004c7c	Asterfusion-12 5G	40MHz 68	41 dB	XiaoyiZhangMBP	MacBook	Apple	MacBook	64 bps	0 bps	684.4
Online	12415ed577e2	192.168.51.210	AP-6-5Z	60eb5c004e29	Asterfusion-12 5G	40MHz 68	51 dB	REDMI-K80	Android mobile	Redmi	REDMI-K80	0 bps	0 bps	286.0
Online	12edfca86b12	192.168.51.67	AP-4-5Z	60eb5c004c3a	Asterfusion-12 5G	40MHz 38	48 dB	Unknown	Unknown	Unknown	Unknown	524.61 Kbps	188.84 Kbps	965.4
Online	1c0fc0a05455	192.168.51.145	AP-4-5Z	60eb5c004c3a	Asterfusion-12 5G	40MHz 38	37 dB	LAPTOP-754KAB9K	Windows PC/LAPTOP	Microsoft	LAPTOP-754KAB9K	49.37 Kbps	19.11 Kbps	356.7
Online	200b74b258ee	192.168.51.250	AP-2-5Z	60eb5b004e59	Asterfusion-12 2.4G	40MHz 11	42 dB	Canona9d7d	Unknown	Unknown	Canona9d7d	0 bps	0 bps	28.93
Online	2402b959ef05	192.168.51.289	AP-4-5Z	60eb5c004c3a	Asterfusion-12 5G	40MHz 38	58 dB	ZHJ	Windows PC/LAPTOP	Microsoft	ZHJ	4.34 Kbps	160 bps	5.67
Online	2844f4e2e0bf	192.168.51.65	AP-6-5Z	60eb5c004e29	Asterfusion-12 5G	40MHz 68	65 dB	HONOR-300-Pro	Android mobile	Unknown	HONOR-300-Pro	4.85 Kbps	15.34 Kbps	15.65
Online	28a44a1b4365	192.168.51.203	AP-3-5Z	60eb5c004c7c	Asterfusion-12 5G	40MHz 68	51 dB	ryan	Windows PC/LAPTOP	Microsoft	ryan	3.07 Kbps	8.67 Kbps	9.84
Online	2a5e20008597	192.168.51.224	AP-6-5Z	60eb5c004e29	Asterfusion-12 5G	40MHz 68	58 dB	Xiaomi-15-Pro	Android mobile	Xiaomi	Xiaomi-15-Pro	626.38 Kbps	102.75 Kbps	18.89
Online	32da1f03cf00	192.168.51.246	AP-3-5Z	60eb5c004c7c	Asterfusion-12 5G	40MHz 68	57 dB	Unknown	Unknown	Unknown	Unknown	9.81 Kbps	3.32 Kbps	1.09
Online	3647f30413dc	192.168.51.227	AP-1-5Z	60eb5c004e53	Asterfusion-12 5G	40MHz 148	44 dB	HUAWEI_Mate_30_5G-9144100	Android mobile	HUAWEI	HUAWEI_Mate_30_5G-9144100	1.54 Kbps	1.02 Kbps	2.68
Online	4215801ba90b	192.168.51.184	AP-4-5Z	60eb5c004c3a	Asterfusion-12 5G	40MHz 38	38 dB	Unknown	Unknown	Unknown	Unknown	1.87 Mbps	156.89 Kbps	16.37
Online	42b05f000a9f	192.168.51.149	AP-4-5Z	60eb5c004c3a	Asterfusion-12 5G	40MHz 38	68 dB	LNA-AL00	Android mobile	HUAWEI	LNA-AL00	58.37 Kbps	16.76 Kbps	8.16
Online	441ca0e081ef	192.168.51.91	AP-8-5Z	60eb5c004c0a	Asterfusion-12 2.4G	40MHz 1	44 dB	DESKTOP-4PTU0BP	Windows PC/LAPTOP	Microsoft	DESKTOP-4PTU0BP	5.7 Kbps	488 bps	197.1
Online	50a0852705da	192.168.51.36	AP-6-5Z	60eb5c004e29	Asterfusion-12 5G	40MHz 68	64 dB	DESKTOP-5BA7858	Windows PC/LAPTOP	Microsoft	DESKTOP-5BA7858	1.56 Mbps	77.94 Kbps	91.89
Online	5a7d031fdfe9	192.168.51.121	AP-2-5Z	60eb5c004e59	Asterfusion-12 5G	40MHz 68	47 dB	Unknown	iPhone	Apple	iPhone	552 bps	776 bps	3.61

Figure 2 Client Overview Dashboard

2.1 Client Baseline — Eliminating RF and Protocol-Level Factors

The controller provides real-time physical-layer metadata for the client:

[Wi-Fi 7] [5 GHz | -50 dBm] [SNR: 49 dB] [VLAN: 403] [IP: 192.168.20.129]

[Navigation: Site → Client → Select client]

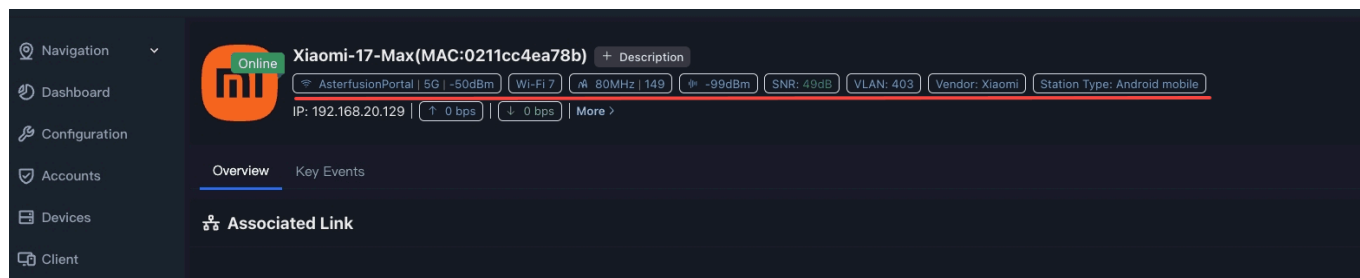


Figure 3 Client for Xiaomi-17-Max

➤ Diagnostic Value

An SNR of **49 dB** indicates an exceptionally strong RF environment, while the **Wi-Fi 7** protocol confirms that the client is operating with the latest wireless capabilities. These metrics allow engineers to quickly rule out packet loss caused by weak signal strength, excessive interference, or poor wireless conditions. When the physical layer is performing optimally, troubleshooting efforts should shift entirely toward the wired infrastructure, DHCP services, and the AP's local bridging and forwarding functions.

➤ Status Assessment

Pay close attention to the IP address assigned to the client.

Check the client's assigned IP address. If no IP address is displayed, the wireless Layer 2 connection has already been established successfully. However, the DHCP exchange has failed to complete due to a lack of response from the upstream network or DHCP server. The client will typically self-assign a Link-Local Address (169.254.x.x), which can be confirmed from the client's network settings.

This observation immediately narrows the troubleshooting scope to the DHCP path, including the AP data plane, VLAN forwarding, DHCP relay functions, and the DHCP server itself.

2.2 Associated Link Topology — Aligning with the Wired Physical

Architecture in Seconds

The dashboard clearly visualizes the complete forwarding path from the wireless client through the AP and into the wired fabric network, providing an end-to-end view of the client's network attachment point

and upstream connectivity.



Figure 4 Associated Link

➤ Diagnostic Value

The Associated Link topology provides immediate visibility into the service VLAN used by the affected client—in this case, **VLAN 403**. Using the end-to-end forwarding path, engineers can rapidly validate both downstream Leaf switches and upstream Spine switches without manually tracing the network.

In distributed gateway deployments, the primary objective is to verify that **VLAN 403** is properly carried across the entire fabric and that the corresponding **Anycast Gateway** is configured with the correct **DHCP relay (ip helper-address)** parameters. Any missing VLAN configuration or DHCP relay misconfiguration along the path can interrupt the DHCP DORA exchange and prevent successful IP address assignment.

2.3 Trend Matrix — Using Temporal Correlation to Identify the Root Cause

The **Online Trend** and **Association Trend** panels at the bottom of the dashboard form a time-based correlation matrix, allowing engineers to analyze client connectivity events in the context of roaming and network behavior.

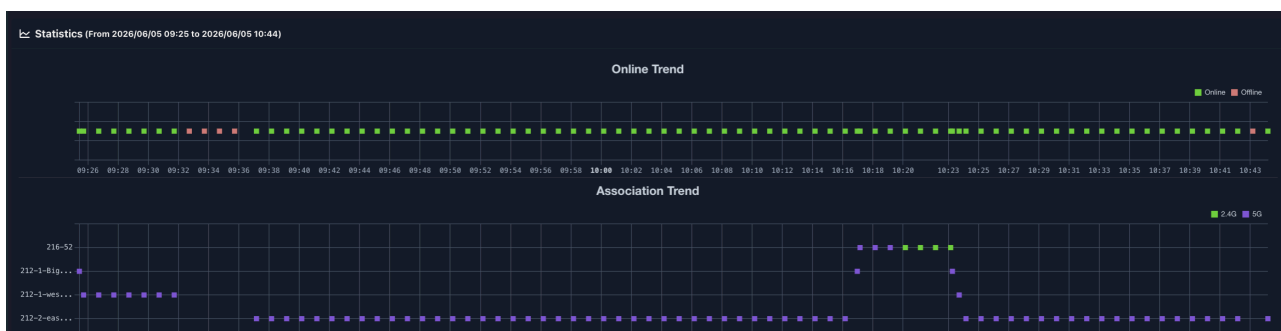


Figure 5 Online Trend

➤ **Failure Scenario: Roaming-Induced DHCP Failure**

Suppose the Online Trend suddenly changes from green to red, indicating a loss of connectivity or a DHCP timeout event. By correlating this timestamp with the Association Trend, engineers discover that the client performed a roaming transition from 212-1-west to 212-2-east at exactly the same moment.

➤ **Diagnostic Conclusion**

If the client remains online and healthy while connected to a single AP, but consistently loses connectivity immediately after roaming, the DHCP server can largely be ruled out as the root cause.

In this scenario, the issue is more likely located between the network segments serving the source AP and the destination AP. Common causes include:

-  The service VLAN is not fully extended across the Layer 2 domain between the two AP locations.
-  VLAN configuration inconsistencies exist along the wired forwarding path.
-  The returning unicast DHCP Offer packet is forwarded toward the old AP location and fails to reach the client's new attachment point.

By correlating connectivity status with roaming events on a common timeline, engineers can rapidly determine whether the DHCP failure is associated with wireless mobility rather than the DHCP server itself, significantly reducing the troubleshooting scope.

3 Micro-Level Analysis: Tracing the DORA Breakpoint Through the Key Events Protocol Stack

Once the macro-level dashboards have narrowed down the probable fault domain, the next step is to switch to the Key Events view.

The Key Events panel records the Layer 2 and Layer 3 state-machine transitions reported in real time by the AP's local data plane to the controller. It serves as a protocol-level "stethoscope," allowing engineers to pinpoint exactly where a network handshake breaks down.

Under normal operating conditions, the DHCP DORA process—Discover, Offer, Request, and Acknowledge—should occur in rapid succession, with each stage separated by only a few milliseconds.

Standard Healthy DORA Exchange Sequence:



Figure 6 Healthy DORA

The figure illustrates a normal client onboarding process in which a wireless device successfully joins the network and obtains an IP address. From the Key Events timeline, it is evident that the DHCP DORA exchange is completed successfully without any timeout, retransmission, or protocol interruption.

The client first completes the standard **802.11 Authentication (Auth)** and **Association (Associated)** procedures and successfully connects to AP **212-2-east-52**. The recorded RSSI ranges from **-33 dBm to -40 dBm**, indicating an excellent RF environment with no signs of weak coverage or wireless interference.

After the client passes **Station Authentication**, it is granted access to the service network. The DHCP state machine then proceeds through the standard DORA sequence:

- ✧ **DHCP Discover** – The client broadcasts a request for an available IP address.
- ✧ **DHCP Offer** – The DHCP server responds with a proposed IP address lease.
- ✧ **DHCP Request** – The client requests to use the offered address.
- ✧ **DHCP Ack** – The DHCP server acknowledges the request and finalizes the lease assignment.

As shown in the event log, the client is successfully assigned the IP address **192.168.20.129**, and every stage of the DHCP process is marked as **Success**.

This event sequence confirms that:

- Wireless authentication is functioning correctly.
- Client association is successful.
- AP local bridging and forwarding are operating normally.
- VLAN forwarding is functioning as expected.

- DHCP relay services (if deployed) are working properly.
- The DHCP server is reachable and responding correctly.
- The client has successfully obtained a valid IP address.

This timeline serves as a **Golden Baseline** for DHCP troubleshooting. Any abnormal DHCP behavior can be compared against this healthy sequence to quickly determine where the DORA process is interrupted and identify the corresponding failure domain.

4 Deep-Dive Investigation in a Decoupled Architecture

Since user traffic never traverses the controller in the OpenWiFi / AsterAPNOS architecture, a Key Events sequence showing “**DHCP Discover – Success**” but no corresponding **DHCP Offer** confirms that the AP has successfully forwarded the client’s DHCP request into the wired network.

At this stage, troubleshooting should move entirely away from the wireless domain and focus on two critical areas: the **wired switching fabric** and the **backend DHCP infrastructure**.

4.1 Wired Fabric Layer: VLAN Mismatches, Roaming Topology Issues, and DHCP Relay Failures

Once the packet leaves the AP’s Ethernet interface, it enters the wired switching infrastructure (such as traditional Access/Aggregation networks or modern Leaf-Spine fabrics). Common failure points at this stage include:

- **VLAN Propagation and PVID Mismatches**

Use the **Associated Link** topology view to trace the forwarding path.

The AP tags the DHCP Discover packet with **VLAN 403** and forwards it toward the wired network. If the switch port connected to the AP does not permit VLAN 403, or if an incorrect PVID configuration causes the packet to be re-tagged unexpectedly, the DHCP Discover broadcast will be dropped at the very first hop of the access network.

```
User-Leaf-2# show vlan summary
```

VLAN ID	IP Address	Ports	Port Tagging	DHCP Helper Address
400	192.168.16.254/32	Ethernet5	untagged	172.16.1.2
		Ethernet13	untagged	172.16.1.1
		Ethernet25	untagged	
		Ethernet40	untagged	
		Ethernet47	untagged	
401	192.168.17.254/32	Ethernet5	tagged	172.16.1.2
		Ethernet13	tagged	172.16.1.1
		Ethernet25	tagged	
		Ethernet40	tagged	
		Ethernet47	tagged	
402	192.168.18.254/32	Ethernet1-4	untagged	172.16.1.2
		Ethernet6-12	untagged	172.16.1.1
		Ethernet14-24	untagged	
		Ethernet26-39	untagged	
		Ethernet41-46	untagged	
		Ethernet48	untagged	
403	192.168.20.254/32	Ethernet5	tagged	172.16.1.2
		Ethernet13	tagged	172.16.1.1
		Ethernet25	tagged	
		Ethernet40	tagged	
		Ethernet47	tagged	
		Ethernet53	tagged	
404	192.168.21.254/32	Ethernet5	tagged	172.16.1.1
		Ethernet13	tagged	172.16.1.2
		Ethernet25	tagged	
		Ethernet40	tagged	
		Ethernet47	tagged	
406	192.168.46.254/32	Ethernet5	tagged	172.16.1.1
		Ethernet13	tagged	172.16.1.2
		Ethernet25	tagged	
		Ethernet40	tagged	
		Ethernet47	tagged	
		Ethernet53	tagged	

Figure 7 VLAN Config on Switch

➤ DHCP Relay Not Configured or Malfunctioning

Verify the **ip helper-address** configuration on the Layer 3 gateway interface, typically located on a Leaf or Spine switch.

Ensure that the gateway correctly converts the Layer 2 DHCP Discover broadcast into a Layer 3 unicast packet and forwards it to the designated DHCP server. Missing, incorrect, or non-functional DHCP relay configurations are among the most common causes of DHCP failures in enterprise networks.

4.2 Backend DHCP Infrastructure: Policy Conflicts, Routing Issues, and Address Pool Exhaustion

If the wired fabric is forwarding traffic correctly and the DHCP Discover packet successfully reaches the backend network, attention should shift to the DHCP server itself (such as Linux ISC DHCP, Kea DHCP, or Microsoft DHCP Server).

➤ Option 82 Compatibility Issues

Some networks insert **DHCP Option 82** information when forwarding DHCP requests. This metadata may include details such as the AP MAC address, SSID, switch port, or circuit identifier.

If the DHCP server is configured with strict relay-agent validation policies and cannot properly interpret the Option 82 format, it may silently discard the request without generating a DHCP Offer. From the controller's perspective, this manifests as a classic **"Discover Success, Offer Missing"** failure pattern.

➤ Address Pool Exhaustion

Check the status of the corresponding DHCP scope or address pool.

In high-density enterprise environments with large numbers of transient users, excessively long lease times can cause address pools to become saturated with stale leases from devices that are no longer connected. In this scenario, the DHCP Discover packet reaches the server successfully, but the server is unable to allocate an available address and therefore does not return a valid DHCP Offer.

➤ DHCP Failover Synchronization Failures

In DHCP failover deployments, synchronization issues between primary and secondary DHCP servers may prevent either server from responding to client requests.

If lease databases become inconsistent or failover state information becomes corrupted, the DHCP servers may intentionally suppress DHCP responses to avoid issuing conflicting leases. As a result, clients experience DHCP timeouts even though the Discover packet successfully reaches the backend infrastructure.

```

class      client      failover      option-group pool      relay
sonic# show dhcp failover info
-----
Failover-name      : test
Local-address      : 3.3.3.2
Peer-address       : 3.3.3.1
Role               : primary
Max_response_delay : 60
Heartbeat_interval : 20
Local-state        : communications-interrupted
Peer-state         : normal
Split              : 50%

sonic# 4

```

Figure 8 DHCP not sync

5 Conclusion

In modern wireless network architectures where the control plane and data plane are completely decoupled, the controller does not participate in forwarding user traffic. Instead, it serves as an efficient observer and recorder, continuously capturing the critical events occurring throughout the network.

When the controller shows a successful DHCP Discover event, followed by complete silence in the subsequent stages, the solution is not to blindly reboot the AP or restart the controller. Instead, engineers should trust the evidence provided by the event timeline itself.

Based on the available information, the wireless access layer has already fulfilled its role. The real issue is likely hidden elsewhere in the network.

At this point, troubleshooting efforts should focus on the upstream wired infrastructure and backend services:

-  **Verify that the service VLAN is correctly propagated across the switching fabric.**
-  **Review DHCP server policies related to Option 82, DHCP Relay Agent, and other access-control mechanisms.**
-  **Examine whether DHCP packets are being dropped or blocked by forwarding policies, ACLs, security features, or routing anomalies along the request and return paths.**
-  **Verify that the DHCP Failover peers are operating normally and that lease databases and failover states are properly synchronized.**

Rather than relying on a trial-and-error approach of “reboot and hope,” engineers should follow the actual path taken by the DHCP packets. Only by validating each hop along the forwarding path can the true root cause be identified and one of the most common—and most challenging—enterprise WLAN onboarding issues be resolved efficiently.

Ultimately, successful DHCP troubleshooting is not about finding where the client failed to connect; it is about identifying exactly where the DORA exchange stopped moving.