Network Capture Troubleshooting Report

dhcp-no-offer-lab.pcap

Report ID	PCAI-2026-1106-ZRQQ
Version	1 (Sample)
Generated	2026-11-06 11:18:57 UTC
Engine	PcapAI Analysis Engine 0.2.0 · ruleset 2026.10.1
Classification	TLP:CLEAR

SAMPLE

Document control

Version history

Version	Date	Change
1	2026-11-06	Initial report

Distribution

TLP:CLEAR Disclosure is not limited, subject to copyright.

Data handling

Captures and reports are stored in Amazon S3 in the us-west-2 region. Uploads without an account and their reports are deleted 24 hours after upload; account reports are kept for 30 days, or for as long as a Pro subscription lasts.

Support: info@pcapai.com

SAMPLE

Contents

1 Executive summary 4

2 Scope, evidence and limitations 5
- 2.1 Evidence integrity . . . 5
- 2.2 Versions . . . 5
- 2.3 Limitations . . . 5

3 Findings summary 5

4 Detailed findings 5
- 4.1 F01: 3 devices got no DHCP offer (21 DISCOVERs) . . . 5
- 4.2 F02: Self-assigned 169.254.x.x addresses on 3 hosts . . . 6

5 Remediation roadmap 6
- 5.1 Immediately . . . 6
- 5.2 Within 24 hours . . . 6
- 5.3 Strategic . . . 6

6 Coverage: checked and clean 7

7 Assets and communications 7
- 7.1 Asset inventory . . . 7
- 7.2 Other conversations . . . 7

8 Capture quality and mode metrics 8

9 Next capture guidance 8

A Appendices 8
- A.1 Event log . . . 8
- A.2 Protocol breakdown . . . 9
- A.3 Methodology and scoring . . . 9
- A.4 Vocabulary . . . 9

SAMPLE

Executive summary

dhcp-no-offer-lab.pcap
5 Nov 2026 · 09:30:00–09:31:30 UTC · 90.4 s

High | High confidence

3 devices got no DHCP offer (21 DISCOVERs)

Clients broadcast DHCP DISCOVER repeatedly without receiving any OFFER, so they cannot get an IP address. 1 more finding: section 3.

Affected: traffic in the capture

NETWORK IMPACT

82 /100 **Impaired**

0 40 75 90

FINDINGS · 2

Critical 0 | High 1 | Medium 1 | Low 0 | Info 0

COVERAGE · 11 AREAS

1 with a finding | 4 pass | 6 not assessed

Not assessed: no TCP connections in...

65	4	5	3	0	32
frames	flows	hosts	protocols	destinations	checks run

The fault lies with the server

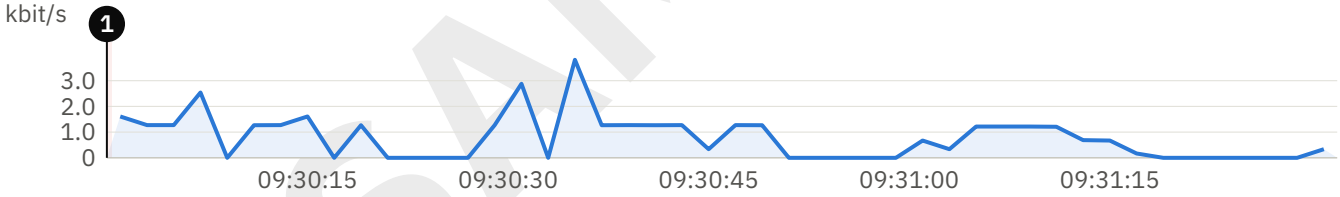
Figure 1 · section 4.1

Where the fault lies

Clients → Network → **Server**

Traffic ranged from 0.0 to 3.8 kbit/s

Figure 2 · UTC



1 09:30:00 DHCP | Devices get no answer from DHCP

Recommended actions

Immediately	No DHCP server answered	Application Owner
Within 24 hours	Hosts using 169.254.x.x addresses did not get a DHCP...	Endpoint / IT Operations
Strategic	Capture again and re-run the analysis	Network Operations

Capture point: not determined (low). Figures use all 65 frames. Limitations: section 2.3.

SAMPLE

2 Scope, evidence and limitations

The analysis covers dhcp-no-offer-lab.pcap (10.0 kB, 65 frames) from 2026-11-05 09:30:00.000 UTC to 2026-11-05 09:31:30.401 UTC (90.4 s).

2.1 Evidence integrity

File	dhcp-no-offer-lab.pcap
Size	10.0 kB
SHA-256	5cd84dc73ca6e2735e818a340d294d736d7678eed4e79c4d24037a98dcaa54b3
Format	pcap
Link types	ethernet
Snapshot length	262,144
Frames	65
Capture point	Not determined
First packet	2026-11-05 09:30:00.000 UTC
Last packet	2026-11-05 09:31:30.401 UTC

2.2 Versions

Engine	PcapAI Analysis Engine 0.2.0 · ruleset 2026.10.1
Content	2026.10.1 (sha256:f246f84c4791dd30)
ATT&CK	19.2
Intelligence lists	service categories 2026-10-09.1; GeoLite2 Country 2026-02-17; GeoLite2 ASN 2024-07-29

2.3 Limitations

- The capture point could not be determined, so every check is read as if its frames were visible.
- 6 coverage areas were assessed partly or not at all; section 6 names the missing inputs.
- Host activity outside this capture (processes, logons, other network segments) is not visible.

3 Findings summary

ID	Title	Severity	Confidence	Roles	First seen	Status
F01	3 devices got no DHCP offer (21 DISCOVERs)	High	High		2026-11-05 09:30:00 UTC	Open
F02	Self-assigned 169.254.x.x addresses on 3 hosts	Medium	High	Affected 169.254.38.112; Affected 169.254.77.240; Affected 169.254.201.17		Open

4 Detailed findings

4.1 F01: 3 devices got no DHCP offer (21 DISCOVERs)

High Network problem · Open · Confidence: High · Reference PCAI-2026-1106-ZRQQ-F01

Clients broadcast DHCP DISCOVER repeatedly without receiving any OFFER, so they cannot get an IP address.

First seen	2026-11-05 09:30:00.000 UTC (T+0.000 s)
Last seen	2026-11-05 09:30:00.000 UTC (T+0.000 s)

Evidence

SAMPLE

- No OFFER means the DHCP server is down, its pool is exhausted, or the relay (ip helper) for this VLAN is missing or wrong.
- DISCOVERs without OFFER: 21
- Clients: `02:10:00:00:00:51`, `02:10:00:00:00:52`, `02:10:00:00:00:53`

Remediation: A01 (Immediately, Application Owner); A03 (Strategic, Network Operations)

4.2 F02: Self-assigned 169.254.x.x addresses on 3 hosts

Medium Network problem · Open · Confidence: High · Reference PCAI-2026-1106-ZRQQ-F02

These hosts did not get a DHCP lease and gave themselves a link-local address; they cannot reach other networks.

Affected	`169.254.38.112` · `02:10:00:00:00:51`
Affected	`169.254.77.240` · `02:10:00:00:00:53`
Affected	`169.254.201.17` · `02:10:00:00:00:52`

Evidence

- Windows and macOS self-assign `169.254.0.0/16` when DHCP fails; such hosts only talk to other self-assigned hosts.

Remediation: A02 (Within 24 hours, Endpoint / IT Operations); A03 (Strategic, Network Operations)

5 Remediation roadmap

5.1 Immediately

ID	Step	Owner	Effort	Verification	Findings
A01	No DHCP server answered: check that the DHCP server is up and has free leases, and that the relay on this VLAN (`ip helper-address`) points to it. Verify · Windows `ipconfig /renew` Verify · Linux `dhclient -v`	Application Owner	Small	A lease renewal gets an OFFER within 1 s.	F01

5.2 Within 24 hours

ID	Step	Owner	Effort	Verification	Findings
A02	Hosts using 169.254.x.x addresses did not get a DHCP lease: check the DHCP server, relay and VLAN for those hosts. Verify · Windows `ipconfig /renew`	Endpoint / IT Operations	Small	The hosts obtain normal addresses after a lease renewal.	F02

5.3 Strategic

ID	Step	Owner	Effort	Verification	Findings
A03	Capture again after applying the steps and re-run the analysis.	Network Operations	Small	The new capture shows none of these problems.	F01, F02

SAMPLE

6 Coverage: checked and clean

What this capture let the engine check:

- **Checks:** 32 of 100 checks ran, in 5 of 11 areas; the table below gives the reason for each one that could not run.
- **Decoded:** 1 protocol (ARP).
- **Hosts:** 5 hosts, 0 destinations outside the network (section 7).
- **Protocols:** 3 protocols; in cleartext: DHCP (UDP/67) and mDNS (UDP/5353).
- **Passwords:** no login exchange in the capture, and no credential was sent readable.
- **TLS:** no TLS handshake in the capture.

Area	Checks evaluated	Checks matched	Not run	Status	Reason
TCP connections	0	0	9	Not assessed	No TCP connections in the capture
Packet loss	0	0	8	Not assessed	Only 0 TCP data packets: too little to judge loss
Latency	0	0	4	Not assessed	No complete TCP handshakes to measure round-trip time
Receive windows	5	0	0	✓ Pass	
DNS	0	0	14	Not assessed	No DNS queries in the capture
DHCP	7	2	0	High F01, F02	
LAN (ARP, broadcast, switching)	13	0	0	✓ Pass	
Routing and MTU	2	0	0	✓ Pass	
TLS	0	0	6	Not assessed	No TLS handshakes in the capture
Applications and services	0	0	27	Not assessed	No application service endpoints identified
Capture quality	5	0	0	✓ Pass	

7 Assets and communications

The capture holds 4 flows (by addresses, ports and protocol) between 4 address pairs.

7.1 Asset inventory

5 internal hosts, from IP traffic, ARP, Ethernet senders and the entities of the findings.

IP	MAC	Hostname	Roles	Bytes sent	Bytes received	Risk
169.254.38.112	02:10:00:00:00:51	not observed	Affected	267 B	0 B	36
169.254.77.240	02:10:00:00:00:53	not observed	Affected	264 B	0 B	36
169.254.201.17	02:10:00:00:00:52	not observed	Affected	267 B	0 B	36
192.168.10.1	02:10:00:00:00:01	not observed		0 B	0 B	
192.168.10.5	02:10:00:00:00:05	not observed		0 B	0 B	

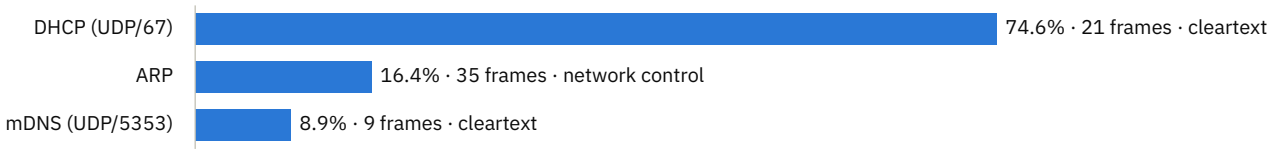
7.2 Other conversations

The 4 conversations the destinations table does not list, by bytes. Address A sent the first packet.

Address A	Address B	Ports at B	Protocol	Bytes A → B	Bytes B → A
0.0.0.0	255.255.255.255	67	DHCP (UDP/67)	6.7 kB	0 B
169.254.201.17	224.0.0.251	5353	mDNS (UDP/5353)	267 B	0 B
169.254.38.112	224.0.0.251	5353	mDNS (UDP/5353)	267 B	0 B
169.254.77.240	224.0.0.251	5353	mDNS (UDP/5353)	264 B	0 B

SAMPLE

Figure 3. Cleartext protocols carried 83.6% of the captured bytes



Share of captured bytes per protocol, with frames; 3 protocols in total. Source: all 65 frames, dhcp-no-offer-lab.pcap. Table: section A.2.

8 Capture quality and mode metrics

Capture point	Not determined: The 0 frames of unicast IP traffic between local hosts are too few to tell.
Position on the TCP paths	Undetermined
Frames cut by the snapshot length	0
Packets dropped by the capture tool	not reported
Segments acknowledged but not captured	0
Duplicate frames (captured twice)	0
One-sided TCP sessions	0 of 0
Network health impact	82 of 100
Network issues found	2

9 Next capture guidance

Why a new capture would help

- The capture is shorter than 5 minutes.
- The capture point could not be determined.
- Some areas could not be assessed because their protocols were absent.

How to capture

- Capture on a SPAN port or TAP of the gateway uplink or the server segment.
- Capture for at least 15 minutes, ideally during business hours.
- Use the full snapshot length.
- Do not use capture filters that drop ARP, DNS or DHCP.

A Appendices

A.1 Event log

Time (UTC)	ID	Observation
2026-11-05 09:30:00.000 UTC T+0.000 s	F01	First seen: 3 devices got no DHCP offer (21 DISCOVERs)

SAMPLE

A.2 Protocol breakdown

Protocol	Protection	Bytes	Share	Frames
DHCP (UDP/67)	cleartext	6.7 kB	74.6%	21
ARP	network control	1.5 kB	16.4%	35
mDNS (UDP/5353)	cleartext	798 B	8.9%	9

A.3 Methodology and scoring

Detection rules inspect captured protocol data. Findings with the same rule and key entities are merged; the report lists them in order of severity, confidence and first appearance.

Confidence follows fixed rules. High: the primary signal, every required check passes, at least one strong check passes and no alternative remains open. Medium: the primary signal, no required check fails, and either no strong check passes or an alternative remains open. Low: a partial primary signal, or a required check could not be evaluated.

Each finding scores its severity weight (Critical 90, High 75, Medium 45, Low 20) times a confidence factor (High 100%, Medium 85%, Low 60%); exposures are capped at 75 and indicators at 40. Overall risk is the highest finding score plus at most 15 points for attack breadth across tactics, affected hosts and linked findings. Bands: Low 0-24, Guarded 25-49, Elevated 50-74, Severe 75-100.

A host's risk is the highest score of the findings that name it, weighted by its role (suspected source 100%, affected or impersonated 80%, client or server of an exposure 70%), plus 3 points for each further finding, at most 10, capped at 100.

Every observation lists the Wireshark frames it rests on and a display filter that selects them in the original capture.

Framework references list the controls to review for each finding. They do not state compliance or non-compliance; applicability depends on the organization's scope.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique, tactic and mitigation names come from ATT&CK 19.2, © The MITRE Corporation, used under its terms of use.

A.4 Vocabulary

- Threat: activity that indicates an attack in progress or completed.
- Exposure: a weakness that could be used against the network; no attack on it was observed.
- Indicator: a signal worth reviewing; on its own it is not evidence of an attack.
- Severity: Critical, High, Medium, Low or Info, set by the finding profile and its conditions.
- Confidence: High, Medium or Low, set by the automatic checks listed on each finding.
- Risk bands: Low 0–24, Guarded 25–49, Elevated 50–74, Severe 75–100.
- Frame: one captured packet, numbered as in Wireshark.
- Conversation: all traffic between two IP addresses, in both directions, as in the Wireshark IPv4 and IPv6 conversation statistics.
- TCP session: one TCP connection.
- Exchange: one request with its response.
- Observation: one evidence row of a finding, with its frames and display filter.
- Check: one detection rule evaluated on the capture. Area: the checks of one attack family.
- Host: an internal device of the asset inventory. Destination: an external address that exchanged traffic with internal hosts.
- Bytes: out is sent by the internal host and in is received by it. Request and response bytes count the application message; conversation bytes count whole frames.

SAMPLE