Network Capture Troubleshooting Report

`slow-app-server-lab.pcap`

Report ID	`PCAI-2026-1106-BBMG`
Version	1 (Sample)
Generated	2026-11-06 11:18:48 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 **6**
4.1 F01: 198.51.100.20 (erp.example.com):80 takes 2574 ms to answer requests (network RTT 19 ms) 6
4.2 F02: 198.51.100.20 (erp.example.com):80 answers HTTP requests in 2537 ms (median) . . . 6

5 Remediation roadmap **6**
5.1 Within 24 hours . . . 6
5.2 Strategic . . . 7

6 Coverage: checked and clean **7**

7 Assets and communications **7**
7.1 Asset inventory . . . 7
7.2 External destinations . . . 8
7.3 Other conversations . . . 8

8 Capture quality and mode metrics **8**
8.1 Services . . . 9
8.2 Endpoints with problems . . . 9

9 Next capture guidance **9**

A Appendices **9**
A.1 Protocol breakdown . . . 9
A.2 Methodology and scoring . . . 9
A.3 Vocabulary . . . 10

SAMPLE

Executive summary

slow-app-server-lab.pcap
5 Nov 2026 · 09:30:00–09:30:54 UTC · 54.3 s

Medium | High confidence

A HTTP (TCP/80) server answers slowly

Median time from request to first response byte is 2574 ms while the network round trip is only 19 ms, so about 2555 ms is spent inside the server. 1 more finding: section 3.

Affected: 198.51.100.20

NETWORK IMPACT

48 /100 **Degraded**

0 40 75 90

FINDINGS · 2

Critical 0 | High 0 | Medium 2 | Low 0 | Info 0

COVERAGE · 11 AREAS

2 with findings | 6 pass | 3 not assessed

Not assessed: no DHCP exchanges in...

978	15	4	2	2	74
frames	flows	hosts	protocols	destinations	checks run

The fault lies with the server 198.51.100.20:80

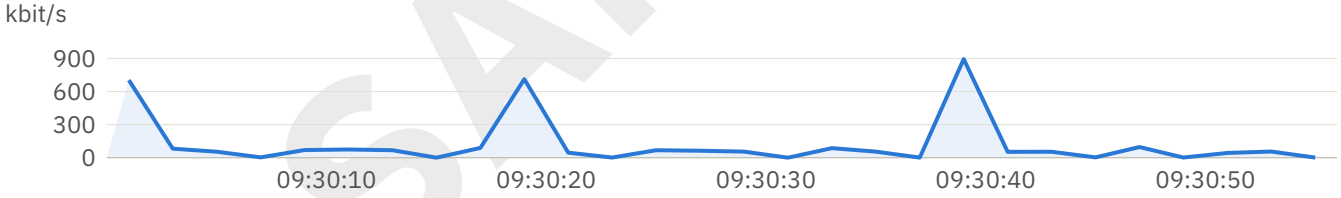
Figure 1 · section 4.1

Where the fault lies



Traffic ranged from 0.0 to 895 kbit/s

Figure 2 · UTC



Recommended actions

Within 24 hours	The network delivers requests quickly but 198.51.100.20...	Application Owner
Within 24 hours	Check slow back-end dependencies of the service on port...	Application Owner
Strategic	Capture again and re-run the analysis	Network Operations

Capture point: uplink (high). Figures use all 978 frames. Limitations: section 2.3.

SAMPLE

2 Scope, evidence and limitations

The analysis covers slow-app-server-lab.pcap (873.1 kB, 978 frames) from 2026-11-05 09:30:00.000 UTC to 2026-11-05 09:30:54.271 UTC (54.3 s).

2.1 Evidence integrity

File	`slow-app-server-lab.pcap`
Size	873.1 kB
SHA-256	`41556151c0d6f5998ec1e60debbf929d115ae6bb46e5c8978346e2458bc54de9`
Format	pcap
Link types	ethernet
Snapshot length	262,144
Frames	978
Capture point	Uplink, high confidence
First packet	2026-11-05 09:30:00.000 UTC
Last packet	2026-11-05 09:30:54.271 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 was taken on an uplink: traffic that stays behind the switch, between local hosts, is not in it.
- 3 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	198.51.100.20 (erp.example.com):80 takes 2574 ms to answer requests (network RTT 19 ms)	Medium	High	Affected `198.51.100.20`		Open
F02	198.51.100.20 (erp.example.com):80 answers HTTP requests in 2537 ms (median)	Medium	Medium	Affected `198.51.100.20`		Open

SAMPLE

4 Detailed findings

4.1 F01: 198.51.100.20 (erp.example.com):80 takes 2574 ms to answer requests (network RTT 19 ms)

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

Median time from request to first response byte is 2574 ms while the network round trip is only 19 ms, so about 2555 ms is spent inside the server.

Affected	`198.51.100.20` · `erp.example.com` · port 80

Evidence

- When the handshake is fast but answers are slow, the delay is server processing: CPU, disk, locks or a slow back end, not the network.
- Server response median 2574 ms over 6 connections
- Handshake RTT median 19 ms

Remediation: A01 (Within 24 hours, Application Owner); A02 (Within 24 hours, Application Owner); A04 (Strategic, Network Operations)

4.2 F02: 198.51.100.20 (erp.example.com):80 answers HTTP requests in 2537 ms (median)

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

Median time to first byte over 18 requests is 2537 ms.

Key facts for F02: as under F01.

Evidence

- Time to first byte measures server work per request; slow pages point at application code, database queries or upstream calls.

Remediation: A03 (Within 24 hours, Application Owner); A04 (Strategic, Network Operations)

5 Remediation roadmap

5.1 Within 24 hours

ID	Step	Owner	Effort	Verification	Findings
A01	The network delivers requests quickly but `198.51.100.20` answers slowly: check CPU, memory, disk I/O and application logs on `198.51.100.20` at the capture time.	Application Owner	Small	Median response time on `198.51.100.20:80` drops below 500 ms in a new capture or in APM.	F01
A02	Check slow back-end dependencies of the service on port 80 (database, authentication, upstream APIs).	Application Owner	Small		F01
A03	Profile the slow endpoints on `198.51.100.20`: application-server thread pools, database queries and upstream calls.	Application Owner	Small	Median time to first byte on `198.51.100.20:80` is under 500 ms.	F02

SAMPLE

5.2 Strategic

ID	Step	Owner	Effort	Verification	Findings
A04	Capture again after applying the steps and re-run the analysis.	Network Operations	Small	The new capture shows none of these problems.	F01, F02

6 Coverage: checked and clean

What this capture let the engine check:

- **Checks:** 74 of 100 checks ran, in 8 of 11 areas; the table below gives the reason for each one that could not run.
- **Decoded:** 2 protocols (DNS and HTTP).
- **Hosts:** 4 hosts, 2 destinations outside the network (section 7).
- **Protocols:** 2 protocols; in cleartext: HTTP (TCP/80) and DNS (UDP/53).
- **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	9	0	0	✓ Pass	
Packet loss	8	0	0	✓ Pass	
Latency	4	1	0	Medium F01	
Receive windows	5	0	0	✓ Pass	
DNS	14	0	0	✓ Pass	
DHCP	0	0	7	Not assessed	No DHCP exchanges in the capture
LAN (ARP, broadcast, switching)	0	0	13	Not assessed	No broadcast or ARP traffic in the capture
Routing and MTU	2	0	0	✓ Pass	
TLS	0	0	6	Not assessed	No TLS handshakes in the capture
Applications and services	27	1	0	Medium F02	
Capture quality	5	0	0	✓ Pass	

7 Assets and communications

The capture holds 15 flows (by addresses, ports and protocol) between 9 address pairs.

7.1 Asset inventory

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

IP	MAC	Hostname	Roles	Bytes sent	Bytes received	Risk
192.168.10.1	02:10:00:00:00:01	not observed	DNS server	555 B	459 B	
192.168.10.23	02:10:00:00:00:23	not observed		8.3 kB	277.1 kB	
192.168.10.31	02:10:00:00:00:31	not observed		7.9 kB	263.6 kB	
192.168.10.45	02:10:00:00:00:45	not observed		8.6 kB	291.8 kB	

SAMPLE

7.2 External destinations

2 external destinations exchanged traffic with internal hosts, most bytes first. Bytes are summed over their conversations; out counts the bytes the internal hosts sent.

Names come from HTTP Host, TLS SNI and DNS answers, the network owner from the GeoLite databases and the reputation from the service-category lists; section 2.2 dates each source.

Destination	Network owner	Protocol	Internal hosts	Reputation	Bytes out (conversations)	Bytes in (conversations)
198.51.100.21 static.example.com		HTTP (TCP/80)	192.168.10.23, 192.168.10.31, 192.168.10.45	Not listed	13.7 kB	561.7 kB
198.51.100.20 erp.example.com		HTTP (TCP/80)	192.168.10.23, 192.168.10.31, 192.168.10.45	Not listed	10.7 kB	270.3 kB

7.3 Other conversations

The 3 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
192.168.10.23	192.168.10.1	53	DNS (UDP/53)	153 B	185 B
192.168.10.31	192.168.10.1	53	DNS (UDP/53)	153 B	185 B
192.168.10.45	192.168.10.1	53	DNS (UDP/53)	153 B	185 B

Figure 3. Cleartext protocols carried 100.0% of the captured bytes



Share of captured bytes per protocol, with frames; 2 protocols in total. Source: all 978 frames, slow-app-server-lab.pcap. Table: section A.1.

8 Capture quality and mode metrics

Capture point	Uplink, high confidence: 100% of the unicast IP frames go to or from the gateway MAC, across 4 hosts on the local network.
Position on the TCP paths	Near the client
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 9
Network health impact	48 of 100
Network issues found	2
TCP connection attempts	9
TCP connections established	9
TCP connection attempts that failed	0
TCP retransmissions	0
Estimated packet loss	0.0%
Handshake round trip, median	19 ms
Handshake round trip, 95th percentile	19 ms
Server response time, 95th percentile	2,823 ms
DNS queries	6
DNS queries without an answer	0
DNS answer time, 95th percentile	14 ms

SAMPLE

8.1 Services

Service	Server	Clients	Requests	Unanswered	Errors	95th percentile
HTTP	198.51.100.20 (erp.example.com):80	3	18	0	0	2,858 ms
HTTP	198.51.100.21 (static.example.com):80	3	12	0	0	30 ms

8.2 Endpoints with problems

Endpoint	field-role	Service	Failed connections	Retransmissions	Loss	Median RTT	Status
198.51.100.20 (erp.example.com):80	server	HTTP (TCP/80)	0 of 6	0	0.0%	19 ms	slow

9 Next capture guidance

Why a new capture would help

- The capture is shorter than 5 minutes.
- 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 Protocol breakdown

Protocol	Protection	Bytes	Share	Frames
HTTP (TCP/80)	cleartext	856.4 kB	99.9%	966
DNS (UDP/53)	cleartext	1.0 kB	0.1%	12

A.2 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.

SAMPLE

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.3 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