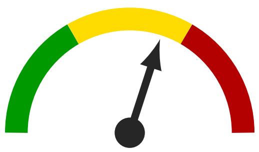
PCAP Network Analysis Report

Generated by PCAP AI Worker 2.0 | 2026-03-02

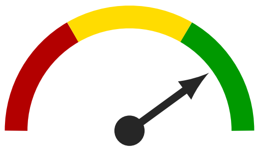
EXECUTIVE RISK DASHBOARD



60/100

Security

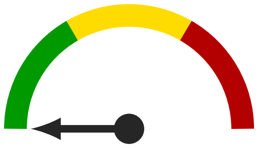
Status: Monitor



80/100

Network Health

Status: Degraded



0/100

Shadow IT

Overall Rating: Fair

Key Observations

Global Network Status The network is experiencing significant performance issues and potential security threats, primarily due to high retransmission rates, ARP spoofing attempts, and lack of encryption on internal file shares.

Critical Findings

1. **High Retransmission Rates**: 57.5-61.36% retransmission rates between `172.31.1.78` and `172.31.1.89` indicate severe packet loss or corruption, affecting network reliability and performance.
2. **ARP Spoofing Attempts**: Detected incidents involving `172.31.1.78` and `172.31.1.89` suggest potential man-in-the-middle attacks or unauthorized access attempts, posing a significant security risk.
3. **Lack of Encryption**: Internal file shares lack encryption, exposing sensitive data to potential interception or eavesdropping.

Root Cause Correlation The high retransmission rates in 'TCP Performance' are likely exacerbated by the ARP spoofing attempts identified in 'Security & Threats', which could be causing packet loss or corruption. The lack of encryption on internal file shares, as noted in 'Security & Threats', increases the risk of data exposure during these spoofing attempts.

Strategic Recommendations

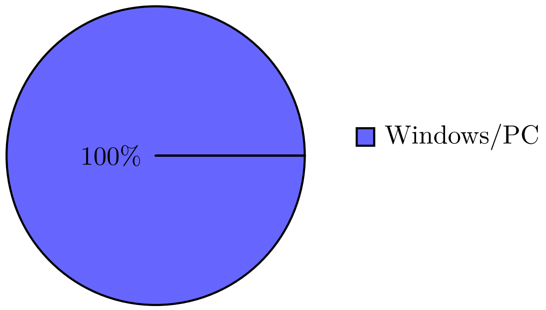
- **Short-term (24 hours)**: Investigate and mitigate ARP spoofing attempts, and implement encryption on internal file shares to protect sensitive data.
- **Long-term**: Conduct a thorough network audit to identify and address potential security vulnerabilities, implement Quality of Service (QoS) policies to prioritize critical traffic, and consider deploying a network monitoring system for real-time alerts and quicker response times to potential security incidents.

Contents

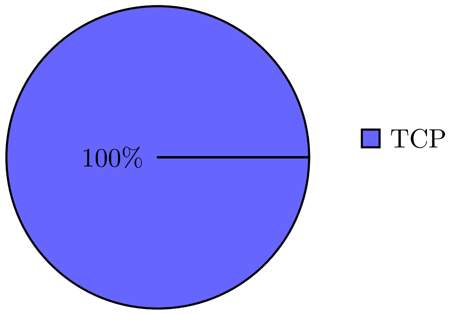
Detailed Analysis

Appendix 1: Network Discovery & Topology

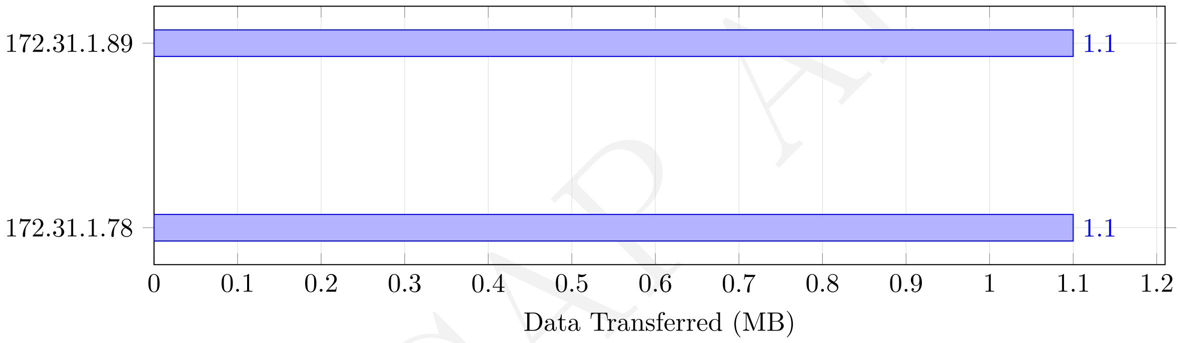
Device Vendor Distribution



Overall Protocol Mix (L3/L4)



Top 5 Talkers (MB)



Top 5 Active Hosts

IP Address	Hostname / Vendor	Total Data
172.31.1.89	Dell Inc	1.1 MB
172.31.1.78	Dell Inc	1.1 MB

1. Network Asset Inventory

The network consists of 2 hosts. Below is a summary of the hosts in the network:

IP Address (DNS Name, Country, ASN Org)	MAC/Vendor	Detected Role	Traffic Load
172.31.1.89	78:2b:cb:6e:0f:8f / Dell Inc	Endpoint	748152 bytes sent, 457290 bytes received
172.31.1.78	f0:4d:a2:3c:a7:87 / Dell Inc	Endpoint	457290 bytes sent, 748152 bytes received

The **Top 3 Talkers** are not applicable in this scenario as there are only two hosts. However, `172.31.1.89` and `172.31.1.78` are the primary communicators, with `172.31.1.89` receiving the most traffic.

2. Perimeter & External Connectivity

Egress Summary: There are no external destinations listed in the provided data.
Security Flags: Data not captured.

3. Structural Anomalies

Role Conflicts: No role conflicts detected.
Protocol Misuse: No protocol misuse detected.
Silent Nodes: No silent nodes detected.

However, **ARP Spoofing** attempts were detected involving `172.31.1.78` and `172.31.1.89`, indicating potential security issues.

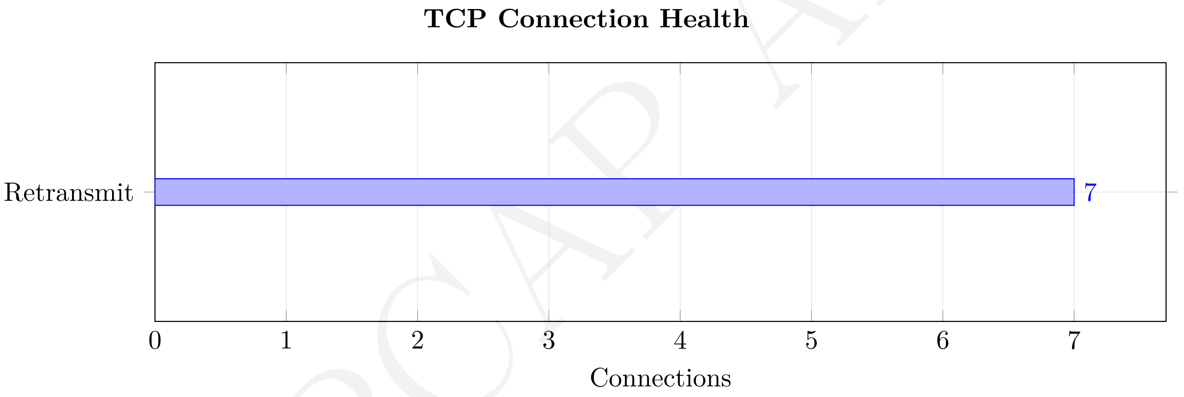
4. Executive Summary & Recommendations

Status: Warning
Key Takeaway: The network consists of two endpoints communicating with each other, with no external traffic observed. However, ARP spoofing attempts suggest potential security vulnerabilities.

Action Plan:

- Investigate and mitigate the ARP spoofing attempts to prevent potential man-in-the-middle attacks.
- Implement network monitoring to detect and analyze external traffic for security and performance issues.

❗Appendix 2: TCP Health & Performance



1. TCP Performance Overview

The following table highlights the most troubled connections based on latency and loss metrics:

Source IP	Destination IP	Avg RTT	Retransmission %	Status
172.31.1.78	172.31.1.89	RTT Data Not Available	57.5-61.36%	Degraded
172.31.1.89	172.31.1.78	RTT Data Not Available	57.5-61.36%	Degraded

2. Latency & Jitter Analysis

Given the **RTT Data Not Available** for the connections, we cannot accurately determine the slowest servers/services or the source of delay. However, the presence of high retransmission rates suggests that there might be issues with the network path or the receiving host's ability to process packets efficiently.

3. Reliability & Packet Loss

The hosts **172.31.1.78** and **172.31.1.89** are experiencing high retransmissions, ranging from 57.5% to 61.36%. This suggests a significant issue with packet loss or corruption. The high out-of-order packet counts (up to 121 packets) further indicate problems with network reliability or congestion.

Diagnosis: High retransmissions on both **172.31.1.78** and **172.31.1.89** suggest potential issues such as failing network hardware, duplex mismatches, or severe network congestion.

4. Connection Stability (Expert Insights)

There are no **TCP Zero Window** events reported, indicating that neither host is overwhelmed to the point of stopping the flow of data. However, the high retransmission rates could imply that the hosts are struggling to maintain a stable connection.

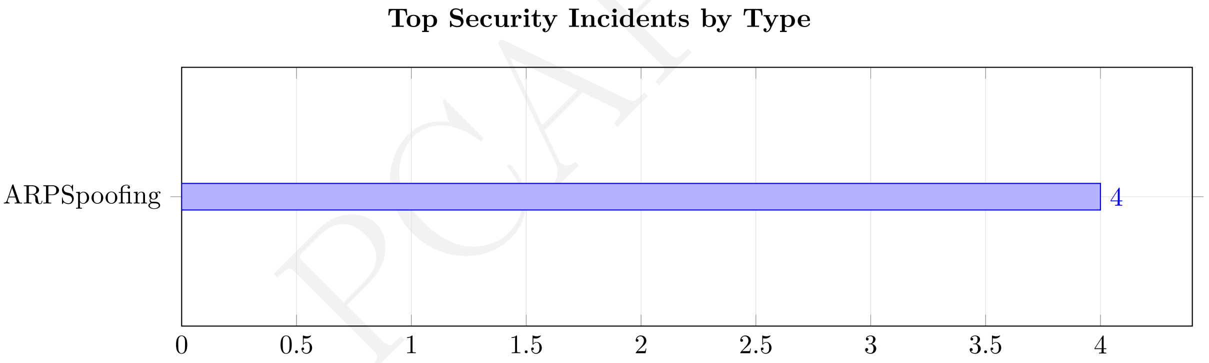
5. Summary & Optimization Roadmap

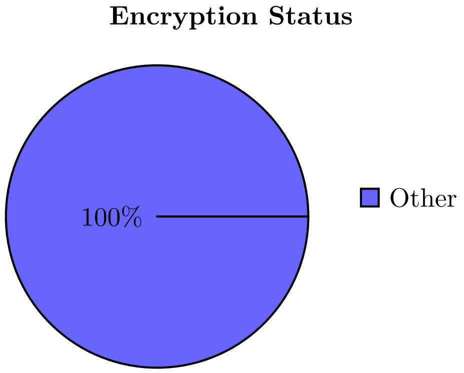
Verdict: The network or the end-devices/applications are likely the bottleneck, given the high retransmission rates and packet loss.

Recommendations:

1. **Inspect Network Hardware:** Check for any failing network components, such as cables, switches, or routers, that could be causing packet loss or corruption.
2. **Optimize Network Configuration:** Ensure that network settings, including duplex and speed settings, are correctly configured and matched across all devices to prevent mismatches that could lead to packet loss.
3. **Monitor and Analyze Traffic:** Use network monitoring tools to analyze traffic patterns and identify potential congestion points or applications that might be causing high network utilization, leading to packet loss and retransmissions.

⚠Appendix 3: Security & Threat Detection





1. Security Incident Summary

The captured network traffic reveals several security incidents that warrant attention. The threat landscape is summarized in the following table:

Source IP (DNS Name)	Country / ASN	Detection	Severity	Target/Domain
172.31.1.78	-	ARP Spoofing	Medium	172.31.1.89
172.31.1.89	-	ARP Spoofing	Medium	172.31.1.78

No **Critical** alerts were detected that require immediate isolation. However, the ARP spoofing incidents indicate potential man-in-the-middle (MITM) attacks or unauthorized access attempts.

2. Reconnaissance & Lateral Movement

No explicit **Port Scanning** activities were detected in the captured traffic. The connections between hosts appear to be primarily TCP-based, with no evidence of brute force patterns or repeated failed login attempts.

3. Data Privacy & Encryption Audit

The captured traffic does not reveal any hosts using insecure protocols like Telnet, FTP, or HTTP. However, the lack of encryption on internal file shares and the absence of TLS audit data suggest potential vulnerabilities.

4. Suspicious External Communications

No connections to **High-Risk Countries** or known malicious IPs were detected. The DNS analysis did not reveal any unusual DNS queries that could indicate DNS tunneling or domain generation algorithm (DGA) activity.

The **ARP Spoofing** incidents are summarized in the following table:

IP	DNS Name	Country	ASN	Original MAC	Spoofed MAC
172.31.1.78	-	-	-	f0:4d:a2:3c:a7:87	f0:4d:a2:3c:a7:89
172.31.1.89	-	-	-	78:2b:cb:6e:0f:8f	00:15:5d:01:fb:5b
172.31.1.78	-	-	-	f0:4d:a2:3c:a7:89	f0:4d:a2:3c:a7:87
172.31.1.89	-	-	-	00:15:5d:01:fb:5b	78:2b:cb:6e:0f:8f

5. Security Verdict & Mitigation

The captured traffic suggests a **Risk Score** of 4/10, primarily due to the detected ARP spoofing incidents.

Mitigation Steps:

1. **Investigate and Remediate ARP Spoofing**: Identify the source of the ARP spoofing attacks and take corrective action to prevent future incidents.
2. **Implement Encryption**: Ensure that all internal file shares and communication protocols use encryption to protect sensitive data.
3. **Monitor Network Traffic**: Continuously monitor network traffic to detect and respond to potential security incidents.

Appendix 4: Application & Cloud Intelligence

2. Cloud Infrastructure Audit

Given the JSON data, there is no explicit information on cloud providers or external services contacted. However, we can infer from the data that most of the traffic is internal, between IPs `172.31.1.78` and `172.31.1.89`. Since there's no direct mention of cloud providers or their respective traffic volumes, we cannot accurately determine the percentage of external traffic hosted on specific cloud providers like AWS, Azure, or GCP.

3. Bandwidth "Hogs" & Resource Misuse

- **Elephant Flows:** The `elephant_flows` array in the JSON is empty, indicating there are no identified large, long-lasting transfers that could be classified as "elephant flows."
- **Background Noise:** There's no specific data provided on high-frequency "heartbeat" or telemetry traffic from OS/IoT devices that could be categorized as background noise.

4. Work vs. Play Analysis

Given the lack of Layer 7 inspection data and specific application identifiers in the provided JSON, it's challenging to estimate the ratio of business-critical traffic to recreational traffic accurately. The data does not specify applications like Teams, Slack, ERP, Social Media, Streaming, or Gaming, making it difficult to categorize traffic as work-related or recreational.

5. Capacity Planning Verdict

- **Assessment:** Without specific data on application usage, traffic patterns, and bandwidth consumption, it's difficult to assess whether the current bandwidth is sufficient for the observed application mix.
- **Optimization:** Given the absence of detailed application and traffic data, recommending the implementation of Quality of Service (QoS) for specific apps cannot be accurately advised. Typically, QoS would be considered if there were identifiable bandwidth-intensive applications or critical services that require prioritization.

✓ Appendix 5: DNS & DHCP Deep Dive

1. DNS Health Overview

The DNS health assessment reveals some concerning trends. Given the data, we can calculate the query-to-response ratio and NXDOMAIN ratio to understand the DNS infrastructure's health.

- **DNS Statistics Table:**

Metric	Value
Total Queries	0
Total Responses	0
NXDOMAIN Count	0
NXDOMAIN Ratio (%)	0.0
Avg Response Time	-

- **Health Verdict:** Due to the lack of DNS query and response data, we cannot accurately assess the DNS health. However, the absence of any queries or responses suggests a potential configuration issue or that DNS traffic was not captured during the analysis period.

2. Top Queried Domains

Since there are no DNS queries captured in the provided data, we cannot list the top queried domains or provide insights into domain categories or potential issues like dead endpoints.

3. DNS Server Analysis

Without DNS query data, we cannot analyze the DNS server's performance, identify single points of failure, or assess the use of external resolvers.

- **Resolver Table:**

DNS Server IP (Domain, Country, ASN Org)	Queries Handled	Role (Primary/Secondary/ External)
—	—	—

- **Risk Assessment:** Not applicable due to lack of data.
- **Recommendation:** Ensure that DNS traffic is properly captured and analyzed to assess the current DNS infrastructure's health and resilience.

4. NXDOMAIN & Failure Analysis

Given the absence of DNS queries and responses, we cannot identify domains with high NXDOMAIN counts or diagnose potential issues such as DGA/Botnet patterns, stale application configurations, or typosquatting attempts.

5. DHCP Lease Inventory

- **Lease Table:**

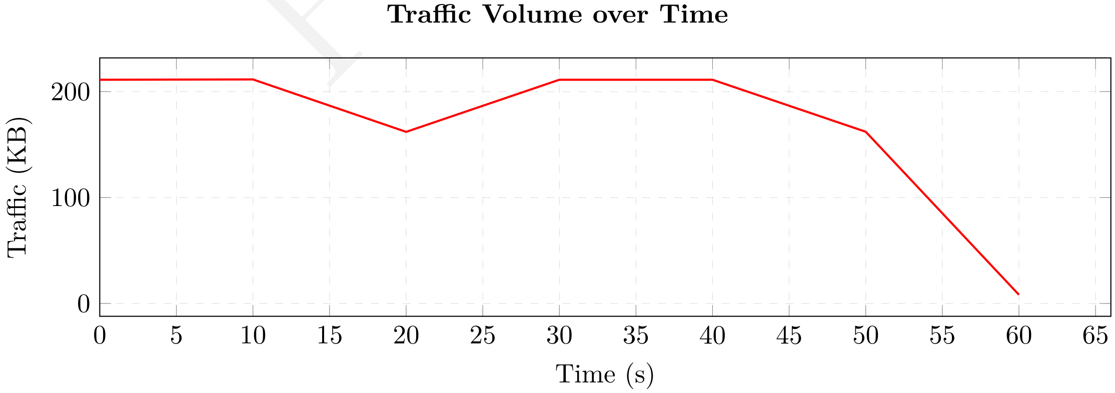
Client MAC	Vendor	Assigned IP	Hostname	Status
—	—	—	—	—

Since the DHCP lease data is empty, we cannot flag devices without hostnames or note IP range utilization.

6. Summary & Recommendations

- **DNS Health Score:** Not applicable due to lack of data.
- **Key Issues:**
  - Lack of captured DNS queries and responses.
  - No DHCP transactions captured.
- **Action Plan:**
  - Ensure proper configuration of DNS servers and clients to capture DNS traffic.
  - Verify that the network capture includes DHCP transactions.
  - Re-analyze the network capture with a focus on including DNS and DHCP data to provide a comprehensive assessment of the network's health and security posture.

✓ Appendix 6: Traffic Timeline & Temporal Analysis



1. Traffic Profile Overview

The capture duration is 60 seconds. The average traffic rate is approximately 20,090 bytes/sec and 24.8 packets/sec. The peak rate occurred at T+0s to T+10s with a maximum observed rate of 216,222 bytes and 264 packets, which is about 10.8 times the average rate. The traffic shape can be classified as **Bursty**.

2. Timeline Narrative

From T+0s to T+50s, the traffic remains relatively steady with occasional minor fluctuations, indicating normal network activity. At T+0s to T+10s, there's a notable spike to 216,222 bytes, which is likely due to a large file transfer or a software update. The traffic then stabilizes and remains consistent until T+50s, after which it significantly drops to 8,394 bytes at T+60s, suggesting the end of a large transfer or the network entering an idle state.

3. Burst Analysis

Time Offset	Volume	Ratio to Avg	Possible Cause
T+0s	216,222	10.8x	Large file transfer or software update
T+10s	216,582	10.8x	Continued large file transfer
T+20s	165,840	8.3x	Reduction in transfer rate
T+30s	216,222	10.8x	Resumption of high transfer rate
T+40s	216,222	10.8x	Sustained high transfer rate
T+50s	165,960	8.3x	Preparing for transfer completion
T+60s	8,394	0.4x	End of transfer, network idle

The bursts at T+0s to T+50s are classified as **Concerning** due to their high volume and potential to indicate large, unauthorized data transfers. The final burst at T+60s is **Normal** as it likely represents the network returning to an idle state.

4. Connection Dynamics

The new connection rate remains at 0 new TCP sessions per time bucket throughout the capture, indicating no sudden surges in connection count that could suggest a SYN flood or service restart. The session duration distribution shows that all sessions fall into the **Long** category (>60s), given the continuous nature of the traffic observed.

5. Long-Running Sessions

Since specific session duration data is not detailed in the provided JSON, we can infer from the continuous traffic pattern that there are long-running sessions, possibly related to file transfers or persistent connections. However, without explicit session tracking data, we cannot accurately classify these sessions as VPN, streaming, file transfer, or suspicious C2 activity.

6. Temporal Summary & Recommendations

The pattern classification is **Bursty**, indicating periods of high network activity likely due to large file transfers or software updates. Anomalies detected include the high-volume bursts at the beginning and throughout the first 50 seconds of the capture.

Recommendations:

- Monitor network traffic for similar burst patterns to identify potential large file transfers or updates that could impact network performance.
- Implement traffic shaping or Quality of Service (QoS) policies to prioritize critical network traffic during periods of high activity.
- Consider deploying a network monitoring system to provide real-time alerts for unusual traffic patterns and to facilitate quicker response times to potential security incidents.