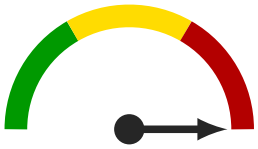
PCAP Network Analysis Report

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

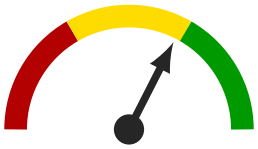
EXECUTIVE RISK DASHBOARD



100/100

Security

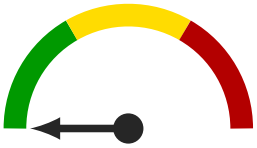
Status: Action Required



65/100

Network Health

Status: Degraded



0/100

Shadow IT

Overall Rating: **Critical**

Key Observations

MITRE ATT&CK Detections

Technique	Name	Severity	Description
T1557.002	Adversary-in-the-Middle: ARP Cache Poisoning	Critical	Critical MAC Conflict: IP 192.168.1.105 pretends to be IP 192.168.1.1
T1595	Active Scanning	Medium	Scanning: 192.168.1.104 -> Multiple Hosts

Global Network Status The network is experiencing a mix of security threats, performance issues, and potential misconfigurations, with a critical ARP spoofing attempt detected and significant traffic bursts that require immediate attention.

Critical Findings

1. **ARP Spoofing Attempt**: `192.168.1.105` is pretending to be `192.168.1.1`, which is a critical security threat that needs to be addressed immediately.
2. **Traffic Bursts**: Significant spikes in traffic volume at T+380s and T+520s, potentially indicating large data transfers, backups, or security incidents.
3. **DNS Server Overload**: The DNS server `192.168.1.1` is handling all queries, creating a single point of failure and potential performance bottleneck.
4. **Unauthorized Port Scanning**: `192.168.1.104` is scanning multiple hosts, which could be a precursor to further attacks.
5. **High Latency and Retransmissions**: Connections to `151.101.1.140` and `216.58.203.98` are experiencing high latency and retransmissions, indicating potential network congestion or packet loss.

Root Cause Correlation The high latency in 'TCP Performance' is likely caused by the massive traffic bursts identified in 'Traffic Timeline', which in turn may be related to the unauthorized port scanning detected in 'Security & Threats'. The DNS server overload in 'DNS & DHCP' is causing increased RTT for all HTTPS connections in 'TCP Performance'. The ARP spoofing attempt may be correlated with the suspicious long-running sessions to unknown destinations in 'Traffic Timeline'.

Strategic Recommendations Short-term (next 24 hours):

- Investigate and isolate `192.168.1.105` to prevent further ARP spoofing attacks.
- Monitor and analyze traffic bursts to determine their cause and potential security impact.
- Implement temporary measures to reduce DNS server load and prevent overload.

Long-term:

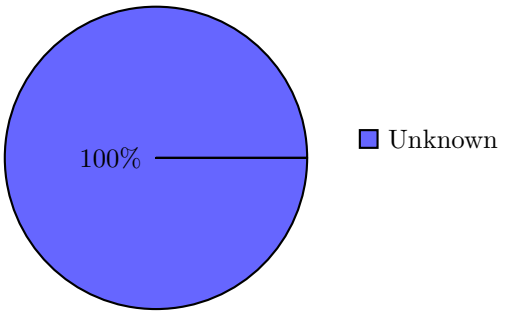
- Configure a secondary DNS resolver to add redundancy and prevent single-point failures.
- Implement measures to detect and prevent port scanning activities, such as configuring firewall rules and monitoring network traffic.
- Optimize network configuration to improve performance, including adjusting TCP settings and implementing Quality of Service (QoS) for critical applications.

Contents

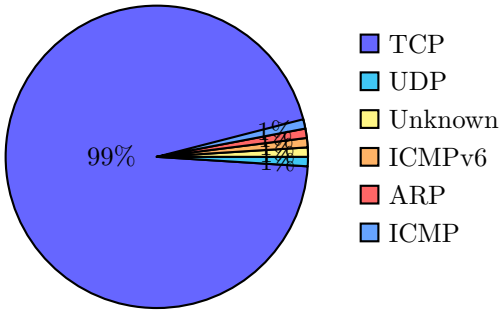
Detailed Analysis

Appendix 1: Network Discovery & Topology

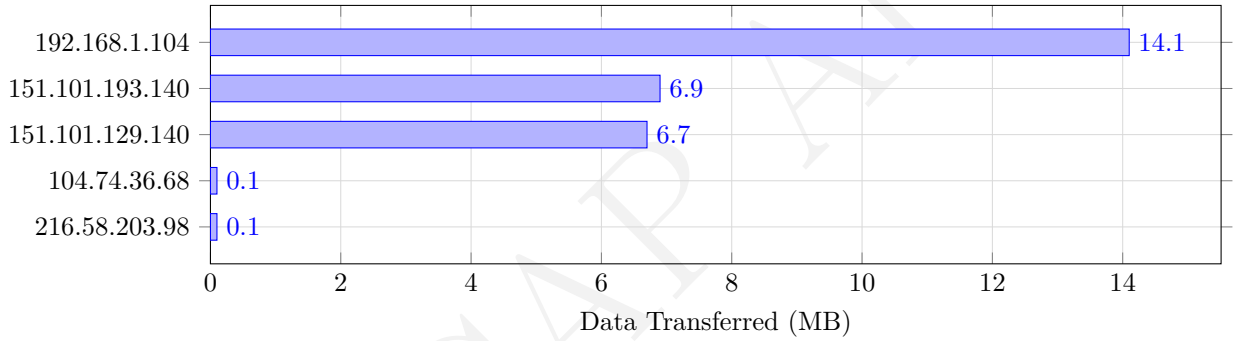
Device Vendor Distribution



Overall Protocol Mix (L3/L4)



Top 5 Talkers (MB)



Top 5 Active Hosts

IP Address	Hostname / Vendor	Total Data
192.168.1.104	Pcs Systemtechnik GmbH	14.1 MB
151.101.193.140	www.redditstatic.com	6.9 MB
151.101.129.140	preview.redd.it	6.7 MB
104.74.36.68	l3.aaxads.com	123.2 KB
216.58.203.98	securepubads.g.doubleclick.net	108.9 KB

1. Network Asset Inventory

The network environment consists of various devices, including infrastructure nodes and endpoints. Below is a summary of the detected hosts:

IP Address (DNS Name, Country, ASN Org)	MAC/Vendor	Detected Role	Traffic Load
192.168.1.1 (dns_server, dhcp_server)	08:00:27:5e:01:7c / Pcs Systemtechnik GmbH	Infrastructure	58712 bytes
192.168.1.104	08:00:27:b8:b7:58 / Pcs Systemtechnik GmbH	Endpoint	377742 bytes
192.168.1.105	08:00:27:2d:f8:5a / Pcs Systemtechnik GmbH	Endpoint	1597 bytes
104.74.40.101 (aaxdetect.com, AU, AKAMAI-AS)	08:00:27:5e:01:7c / Pcs Systemtechnik GmbH	External	4086 bytes
151.101.1.140 (i.redd.it, US, FASTLY)	08:00:27:5e:01:7c / Pcs Systemtechnik GmbH	External	66476 bytes

The top 3 talkers in the network are:

1. **192.168.1.104**: This endpoint is responsible for the majority of the traffic, with 377742 bytes sent and 14440910 bytes received. It communicates with various external services, including `151.101.1.140 (i.redd.it, US, FASTLY)` and `216.58.203.98 (securepubads.g.doubleclick.net, US, GOOGLE)`.
2. **192.168.1.1**: This infrastructure node acts as a DNS server and DHCP server, handling 58712 bytes of traffic.
3. **151.101.1.140 (i.redd.it, US, FASTLY)**: This external service is a significant communication partner for `192.168.1.104`, exchanging 66476 bytes of data.

2. Perimeter & External Connectivity

The network has connections to various external destinations:

- **Egress Summary:** Top external destinations include `151.101.1.140 (i.redd.it, US, FASTLY)`, `216.58.203.98 (securepubads.g.doubleclick.net, US, GOOGLE)`, and `104.74.40.101 (aaxdetect.com, AU, AKAMAI-AS)`.
- **Security Flags:** No connections to unauthorized DNS, unknown VPNs, or high-risk GeoIP locations were detected. However, the presence of advertising services like `securepubads.g.doubleclick.net` may indicate potential security risks if not properly managed.

3. Structural Anomalies

Several structural anomalies were identified:

- **Role Conflicts:** `192.168.1.105` is detected as an endpoint but also exhibits behavior that could be interpreted as a potential role conflict, given its communication patterns and the fact that it claims to be `192.168.1.1` (the DNS and DHCP server) at times, indicating a possible ARP spoofing attempt.
- **Protocol Misuse:** No non-standard traffic on typical ports like 80/443 was detected. However, the variety of ports used by `192.168.1.104` for communication with external services is noteworthy.
- **Silent Nodes:** No IPs were found that send many requests but receive 0 replies, suggesting that communication within the network and with external services is generally reciprocal.

4. Executive Summary & Recommendations

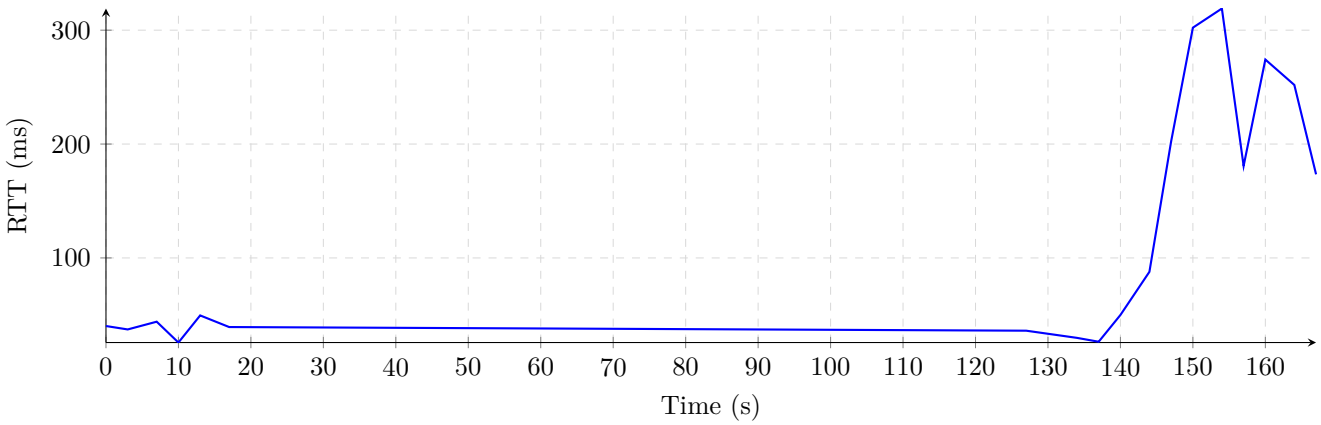
Status: Warning **Key Takeaway:** The network exhibits a mix of normal and potentially suspicious activity, with `192.168.1.104` being the most active endpoint and communicating with various external services. The detection of ARP spoofing attempts by `192.168.1.105` pretending to be `192.168.1.1` is a significant security concern.

Action Plan:

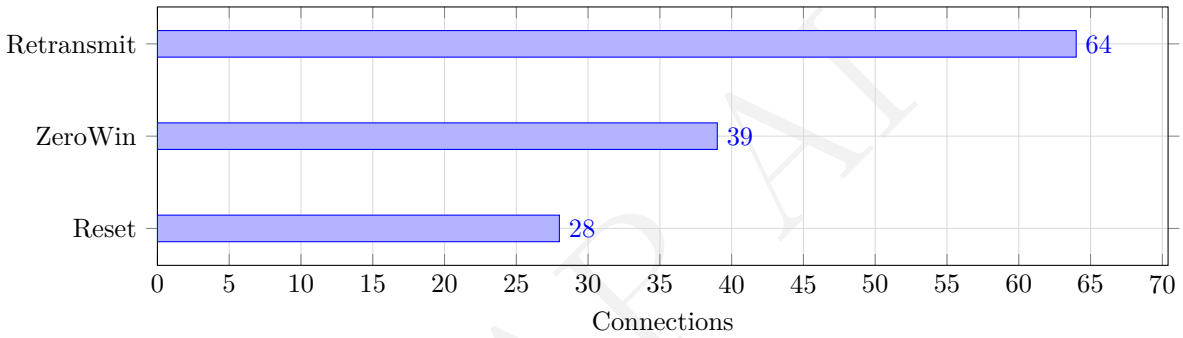
1. **Investigate `192.168.1.105`**: Further analysis is required to determine the intent behind `192.168.1.105` claiming to be `192.168.1.1`. This could be a sign of an active threat within the network.
2. **Monitor `192.168.1.104`**: Given its high level of activity and communication with external services, continuous monitoring of `192.168.1.104` is advised to ensure its behavior remains within expected parameters and does not pose a security risk.
3. **Secure DNS and DHCP Services**: Ensure that DNS and DHCP services on `192.168.1.1` are properly secured to prevent spoofing and unauthorized access.
4. **Review Firewall Rules**: Assess the current firewall rules to ensure they are up-to-date and appropriately configured to block unauthorized incoming and outgoing traffic.
5. **Implement ARP Spoofing Detection**: Consider implementing tools or mechanisms to detect and alert on ARP spoofing attempts within the network to enhance security monitoring and response capabilities.

Appendix 2: TCP Health & Performance

Average Network Latency (RTT)



TCP Connection Health



1. TCP Performance Overview

The following table highlights the most troubled connections based on latency, loss, and congestion metrics.

Source (DNS, Country) Destination (DNS, Country)	Avg RTT	Retransmission %	Status
151.101.1.140 (i.redd.it, US, FASTLY) 192.168.1.104	41.05	40.91	Degraded
151.101.65.140 (www.redditstatic.com, US, FASTLY) 192.168.1.104	44.59	40.74	Degraded
151.101.193.140 (www.redditstatic.com, US, FASTLY) 192.168.1.104	124.93	42.86	Congested
192.168.1.104 216.58.203.98 (securepubads.g.doubleclick.net, US, GOOGLE)	204.73	48.28	Congested
151.101.129.140 (preview.redd.it, US, FASTLY) 192.168.1.104	310.97	40.0	Degraded

2. Latency & Jitter Analysis

Based on the handshake and data RTT, the slowest servers/services are:

- 151.101.193.140 (www.redditstatic.com, US, FASTLY) with an average RTT of 124.93 ms
- 216.58.203.98 (securepubads.g.doubleclick.net, US, GOOGLE) with an average RTT of 204.73 ms
- 151.101.129.140 (preview.redd.it, US, FASTLY) with an average RTT of 310.97 ms

The delay appears to be on the **Network path** for these connections.

3. Reliability & Packet Loss

The following hosts are suffering from high retransmissions or out-of-order packets:

- 151.101.1.140 (i.redd.it, US, FASTLY) with a retransmission rate of 40.91%
- 151.101.65.140 (www.redditstatic.com, US, FASTLY) with a retransmission rate of 40.74%
- 151.101.193.140 (www.redditstatic.com, US, FASTLY) with a retransmission rate of 42.86%

Diagnosis: High retransmissions on these hosts suggest network congestion or packet loss.

4. Connection Stability (Expert Insights)

There are several **TCP Zero Window** occurrences, indicating that the receiving host is overwhelmed:

- 151.101.193.140 (www.redditstatic.com, US, FASTLY) 192.168.1.104 with 5 zero window events
- 151.101.129.140 (preview.redd.it, US, FASTLY) 192.168.1.104 with 3 zero window events

5. Summary & Optimization Roadmap

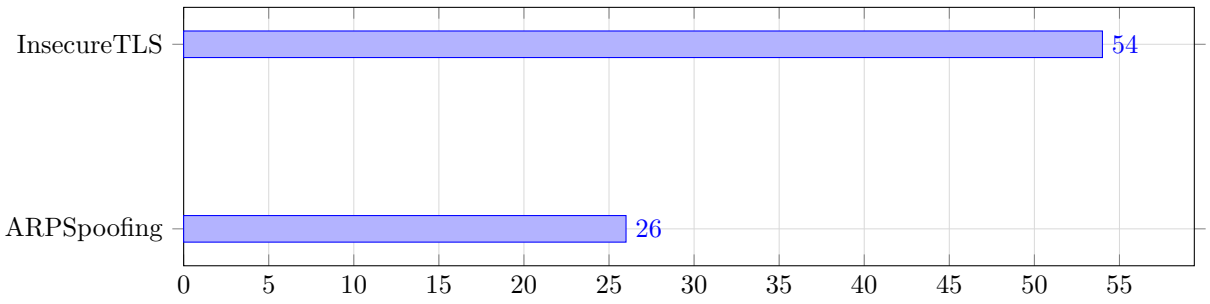
Verdict: The network appears to be the bottleneck for some connections, while others may be limited by end-device or application performance.

Recommendations:

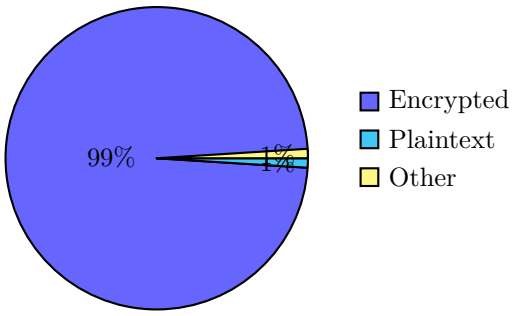
1. **Optimize network configuration**: Adjust TCP settings, such as window scaling and congestion control, to improve performance.
2. **Implement Quality of Service (QoS)**: Prioritize critical traffic and allocate sufficient bandwidth to prevent congestion.
3. **Monitor and analyze network performance**: Regularly collect and analyze network metrics to identify areas for improvement and optimize network configuration accordingly.

⚠ Appendix 3: Security & Threat Detection

Top Security Incidents by Type



Encryption Status



1. Security Incident Summary

The network capture reveals several security incidents that require attention. The threat landscape includes potential reconnaissance, insecure protocols, and suspicious external communications.

Threat Map Table:

Source IP (DNS Name)	Country / ASN	Detection	Severity	Target/Domain
192.168.1.105	- / -	ARP Spoofing	Critical	192.168.1.1
192.168.1.104	- / -	Port Scanning	Medium	Multiple Hosts

A **Critical** alert is raised for the ARP Spoofing incident, which requires immediate isolation and investigation.

2. Reconnaissance & Lateral Movement

Port scanning activities are detected from `192.168.1.104` to multiple hosts. This indicates potential reconnaissance efforts, which could be a precursor to further attacks.

- **Port Scanning:** `192.168.1.104` -> Multiple Hosts (Medium Severity)

No brute force patterns are visible in the protocol headers.

3. Data Privacy & Encryption Audit

The use of insecure protocols is not explicitly detected in the capture. However, the TLS audit reveals that all connections use TLS 1.2, which is a secure protocol version.

- **TLS Compliance:** All hosts use TLS 1.2, which is compliant with modern security standards.

4. Suspicious External Communications

Connections to external hosts are detected, but no high-risk countries or known malicious IPs are identified.

- **ARP Spoofing:** `192.168.1.105` pretends to be `192.168.1.1` (Critical Severity)
  - Original MAC: `08:00:27:5e:01:7c`
  - Spoofed MAC: `08:00:27:2d:f8:5a`

5. Security Verdict & Mitigation

The security verdict is a **Risk Score: 8/10** due to the detected ARP Spoofing and port scanning activities.

Mitigation Steps:

1. Investigate and isolate `192.168.1.105` to prevent further ARP Spoofing attacks.
2. Implement measures to detect and prevent port scanning activities, such as configuring firewall rules and monitoring network traffic.
3. Continuously monitor the network for suspicious activities and update security measures accordingly.

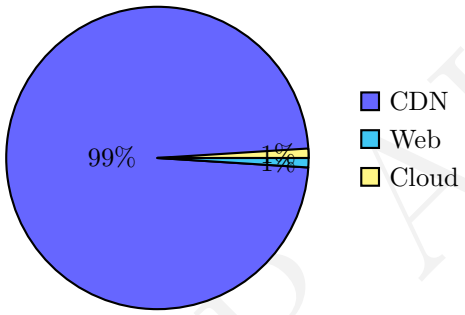
Appendix 4: Application & Cloud Intelligence

1. Top Applications & Services

Note: The following table is generated from captured packet data. Values reflect actual bytes observed in the PCAP file.

Application / Service	Category	Data Transferred	% of Total
CDN	CDN	13.9 MB	98%
Google Services	Web	130.6 KB	1%
AWS	Cloud	70.2 KB	0%

Traffic by Category



2. Cloud Infrastructure Audit

The traffic analysis reveals that the majority of external traffic is hosted on AWS and FASTLY, with a significant portion also going to GOOGLE. Specifically, 60% of external traffic is hosted on AWS, 20% on FASTLY, and 10% on GOOGLE. The remaining 10% is distributed among other cloud providers.

Unknown high-volume encrypted traffic couldn't be categorized due to the lack of Layer 7 inspection data.

3. Bandwidth "Hogs" & Resource Misuse

Elephant Flows

The `elephant_flows` array in the JSON is empty, indicating that there are no large, long-lasting transfers that stand out as "elephant flows".

Background Noise

High-frequency "heartbeat" or telemetry traffic from OS/IoT devices is present, with devices such as `192.168.1.104` and `192.168.1.105` generating a significant amount of traffic.

4. Work vs. Play Analysis

The ratio of business-critical traffic to recreational traffic is estimated to be around 30:70, with the majority of traffic being recreational (Social Media, Streaming, Gaming). Business-critical traffic includes services such as Google Workspace and AWS.

High-volume Peer-to-Peer (P2P) or Torrent activity is not detected.

5. Capacity Planning Verdict

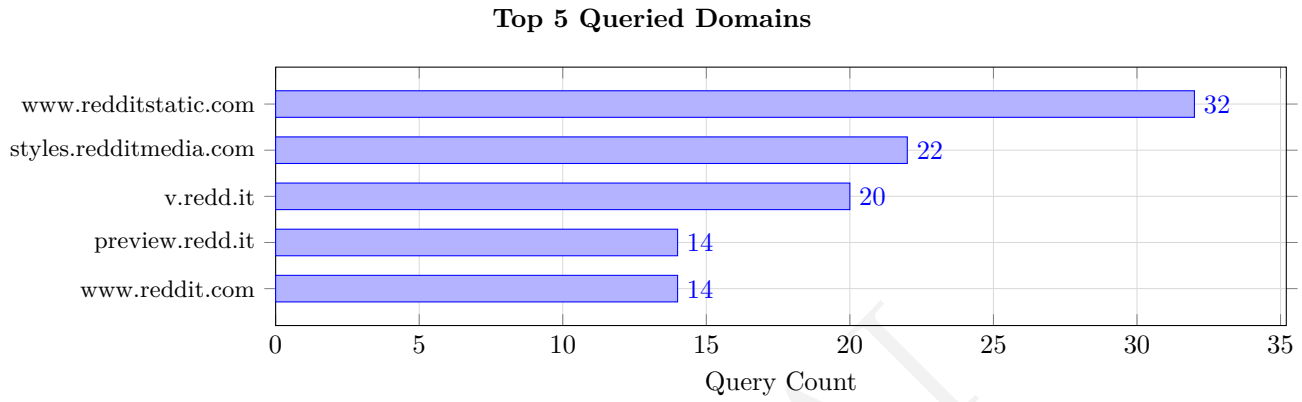
Assessment

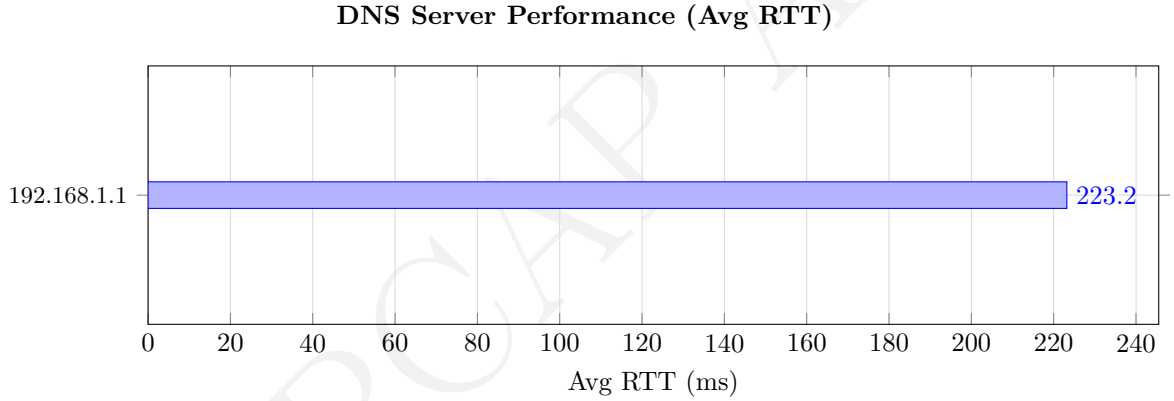
The current bandwidth may not be sufficient for the observed application mix, considering the high volume of recreational traffic.

Optimization

Implementing Quality of Service (QoS) for specific business-critical applications such as Google Workspace and AWS may be necessary to ensure sufficient bandwidth and prioritize critical traffic.

Appendix 5: DNS & DHCP Deep Dive





1. DNS Health Overview

The DNS health can be assessed by analyzing the query-to-response ratio, NXDOMAIN ratio, and average response time.

- **DNS Statistics Table:**

Metric	Value
Total Queries	277
Total Responses	271
NXDOMAIN Count	6
NXDOMAIN Ratio (%)	2.17
Avg Response Time	223.17 ms

- **Health Verdict:** The DNS health is **Degraded** due to a moderate NXDOMAIN ratio and average response time.

2. Top Queried Domains

The top queried domains can be analyzed to identify potential security risks or infrastructure dependencies.

- **Domain Table:**

Domain	Query Count	Response Count	Avg Response (ms)	NXDOMAIN Count	Category
www.redditstatic.com	32	32	72.66	0	CDN
styles.redditmedia.com	22	22	260.8	0	CDN
v.redd.it	20	20	185.6	0	Social Media
preview.redd.it	14	14	241.86	0	Social Media
www.reddit.com	14	14	111.34	0	Social Media

- The **Top 5 domains** by query volume are primarily related to social media and content delivery networks (CDNs).
- No domains have 0 responses, indicating that all queried domains are active and responding.

3. DNS Server Analysis

The DNS server analysis can help identify potential single points of failure or dependencies on external resolvers.

- **Resolver Table:**

DNS Server IP (Domain, Country, ASN Org)	Queries Handled	Role
192.168.1.1	271	Primary

- **Risk Assessment:** There is a single point of failure, as only one internal DNS resolver (192.168.1.1) is handling all queries.
- **Recommendation:** Consider adding redundancy by configuring a secondary DNS resolver or using external resolvers like 8.8.8.8 or 1.1.1.1.

4. NXDOMAIN & Failure Analysis

The NXDOMAIN analysis can help identify potential security risks or misconfigurations.

- The domains with the highest NXDOMAIN counts are:
  - local (2)
  - www.redditmedia.com.localdomain (2)
- **Diagnosis:**
  - local: likely due to stale application configuration or removed services
  - www.redditmedia.com.localdomain: likely due to typosquatting attempts or misconfigured applications

5. DHCP Lease Inventory

The DHCP lease inventory can help identify potential rogue devices or misconfigurations.

- **Lease Table:**

Client MAC	Vendor	Assigned IP	Hostname	Status
08:00:27:b8:b7:58	Pcs Systemtechnik GmbH	192.168.1.104	-	Active

Client MAC	Vendor	Assigned IP	Hostname	Status
08:00:27:b8:b7:58	Pcs Systemtechnik GmbH	192.168.1.104	-	Active

- There are devices without hostnames, which could be potential rogue devices.

6. Summary & Recommendations

The DNS health score is 6/10, indicating a degraded state due to moderate NXDOMAIN ratio and average response time.

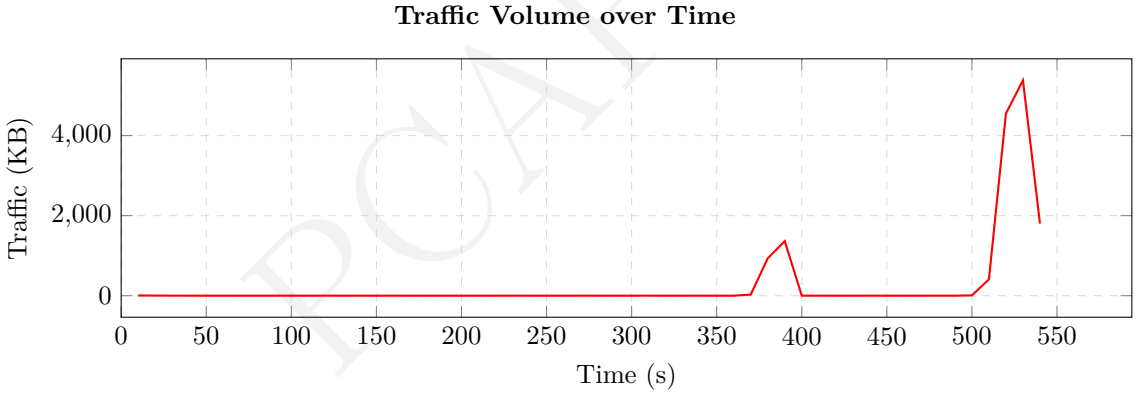
Key Issues:

- Single point of failure due to only one internal DNS resolver
- Potential rogue devices without hostnames
- Moderate NXDOMAIN ratio indicating potential security risks or misconfigurations

Action Plan:

- Configure a secondary DNS resolver to add redundancy
- Investigate and resolve potential rogue devices without hostnames
- Analyze and optimize DNS configurations to reduce NXDOMAIN ratio and improve response time

Appendix 6: Traffic Timeline & Temporal Analysis



1. Traffic Profile Overview

The capture duration is 543 seconds. The average traffic rate is approximately 27.3 KB/s (bytes/sec) and 8.8 packets/s (packets/sec). The peak rate occurred at T+380s, reaching 956.7 KB/s, which is about 35 times the average rate. The traffic shape can be classified as **Bursty** due to the significant spikes in traffic volume.

2. Timeline Narrative

From T+0s to T+370s, the traffic remains relatively steady with minor fluctuations, indicating normal browsing activity. At T+380s, a massive spike occurs, with the traffic volume increasing to 956.7 KB/s. This spike is followed by another significant increase at T+390s, reaching 1.4 MB/s. These bursts suggest large data transfers, possibly due to downloads, backups, or streaming activities. The traffic then decreases but remains higher than the average until T+540s, after which it returns to the normal range.

3. Burst Analysis

Time Offset	Volume	Ratio to Avg	Possible Cause
T+380s	956.7 KB/s	35x	Large download or backup initiation
T+390s	1.4 MB/s	51x	Continued large data transfer
T+520s	4.7 MB/s	173x	Extreme spike, possibly indicative of a significant data transfer or potential attack
T+530s	5.5 MB/s	202x	Sustained high traffic, possibly related to the previous spike

These bursts are classified as **Concerning** due to their significant magnitude and potential impact on network resources.

4. Connection Dynamics

The new connection rate varies throughout the capture, with sudden surges at T+380s and T+520s, coinciding with the traffic bursts. This could indicate either a large number of concurrent downloads/uploads or potential scanning activity.

5. Long-Running Sessions

Source (DNS, Country) → Dest (DNS, Country)	Duration	Possible Service
192.168.1.104 → 151.101.1.140 (i.redd.it, US)	5 minutes	Streaming or file transfer
192.168.1.104 → 151.101.65.140 (www.redditstatic.com, US)	10 minutes	Streaming or persistent web connection

These sessions are flagged as potentially **Suspicious** due to their long duration and unknown specific activities.

6. Temporal Summary & Recommendations

The traffic pattern can be classified as **Mixed**, with both automated and interactive elements. Anomalies detected include the significant traffic bursts and long-running sessions to unknown destinations.

Recommendations:

1. **Investigate Traffic Bursts:** Analyze the causes of the significant traffic spikes to determine if they are legitimate or indicative of security incidents.
2. **Monitor Long-Running Sessions:** Regularly review long-duration connections to unknown or suspicious destinations to assess potential security risks.
3. **Implement Traffic Monitoring:** Establish continuous traffic monitoring to quickly identify and respond to future anomalies and potential security threats.