Network Traffic Analysis Report

Executive Summary

Executive Summary of Network Traffic Analysis 1. Overview: - Total Packets: 691 - Duration: 1566.59 seconds - Average Packet Rate: 0.44 packets/second 2. Traffic Distribution: - Top Source IP: 192.168.1.2 (428 packets, 61.94% of total) - Top Destination IP: 192.168.1.1 (260 packets, 37.63% of total) - Most Active Port: 53 (299 occurrences) 3. Protocol Analysis: - Primary Protocol: 17 - Protocol Distribution: 17:542, 6:55, 170:6 4. Packet Size Statistics: - Average: 150.83 bytes - Median: 86.00 bytes - Std Dev: 172.22 bytes 5. Security Concerns: High traffic on unusual ports: 137, 5060 6. Key Recommendations: Review and potentially restrict traffic on identified unusual ports. This summary provides a high-level overview of the network traffic captured in the PCAP file. For detailed analysis and visualizations, please refer to the full report.

Detailed Analysis

Protocol Distribution:

- 17: 542 packets (78.44%)
- 6: 55 packets (7.96%)
- 170: 6 packets (0.87%)
- 0: 3 packets (0.43%)
- 37: 2 packets (0.29%)

Top 5 Source IP Addresses:

- 192.168.1.2: 428 packets (61.94%)
- 192.168.1.1: 49 packets (7.09%)
- 212.242.33.35: 30 packets (4.34%)
- 147.234.1.253: 25 packets (3.62%)
- 192.168.1.41: 13 packets (1.88%)

Top 5 Destination IP Addresses:

- 192.168.1.1: 260 packets (37.63%)
- 192.168.1.2: 104 packets (15.05%)
- 192.168.1.255: 102 packets (14.76%)
- 212.242.33.35: 43 packets (6.22%)
- 147.234.1.253: 20 packets (2.89%)

Top 10 Ports:

- Port 53: 299 packets (43.27%)
- Port 137: 196 packets (28.36%)
- Port 5060: 166 packets (24.02%)
- Port 21: 39 packets (5.64%)
- Port 2720: 37 packets (5.35%)
- Port 43690: 15 packets (2.17%)
- Port 138: 13 packets (1.88%)
- Port 30000: 9 packets (1.30%)
- Port 40392: 9 packets (1.30%)
- Port 2722: 6 packets (0.87%)

Packet Size Statistics:

- Average: 150.83 bytes

- Median: 86.00 bytes

- Standard Deviation: 172.22 bytes

TCP Flags Distribution:

- PA: 26 (48.15%)

- A: 12 (22.22%)

- S: 9 (16.67%)

- FA: 3 (5.56%)

- SA: 2 (3.70%)

- SPAUE: 1 (1.85%)

- SPUC: 1 (1.85%)

Traffic Distribution by Hour:

- Hour 15: 613 packets (88.71%)

Top 5 Conversations:

- 192.168.1.2 <-> 192.168.1.1: 235 packets (34.01%)

- 192.168.1.2 <-> 192.168.1.255: 84 packets (12.16%)

- 192.168.1.1 <-> 192.168.1.2: 45 packets (6.51%)

- 192.168.1.2 <-> 212.242.33.35: 39 packets (5.64%)

- 212.242.33.35 <-> 192.168.1.2: 29 packets (4.20%)

Average TTL: 115.39

Top 5 DNS Queries:

- _sip._udp.sip.cybercity.dk.: 107 times

- 1.0.0.127.in-addr.arpa.: 22 times

- .: 11 times

- sip.cybercity.dk.: 9 times

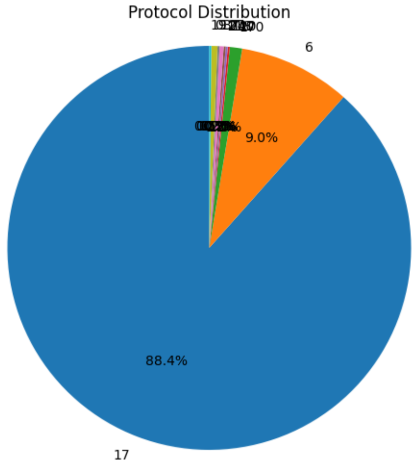
- _sip._udp.voip.brujula.net.: 6 times

Average TCP Window Size: 20971.30 bytes

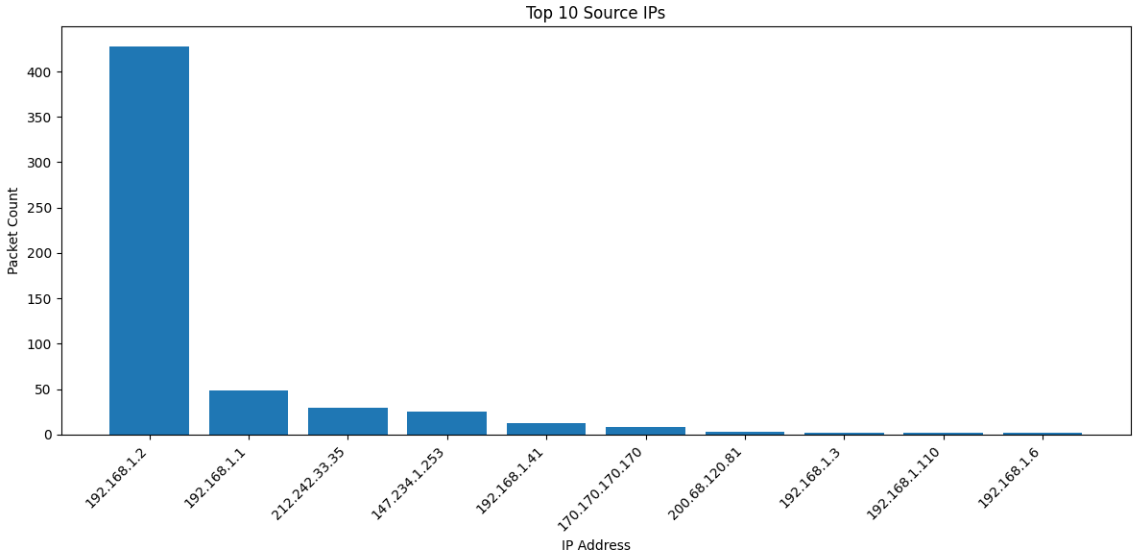
Average UDP Datagram Length: 1175.20 bytes

Visual Analysis

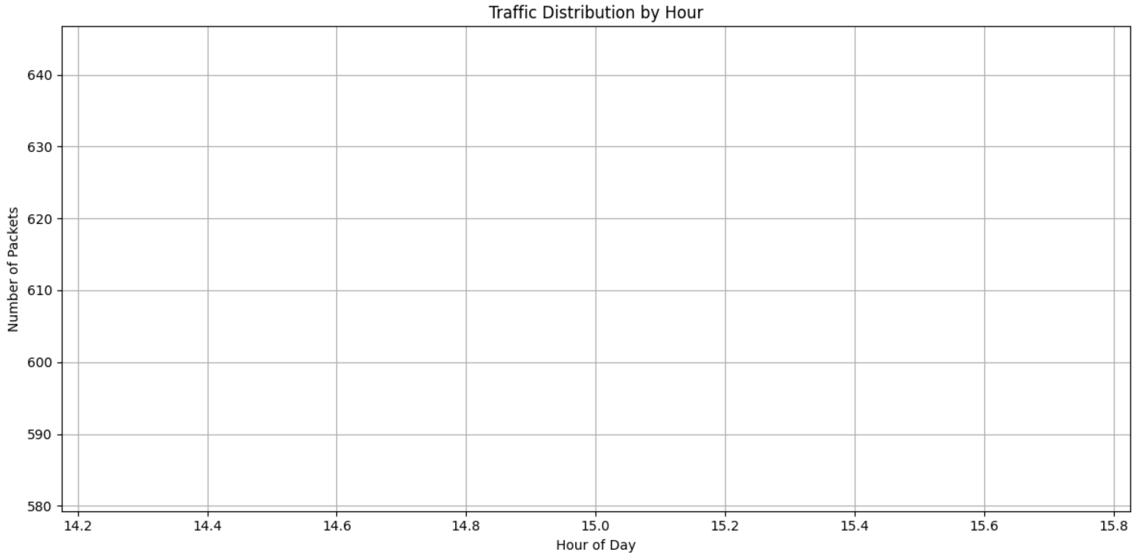
Protocol Distribution



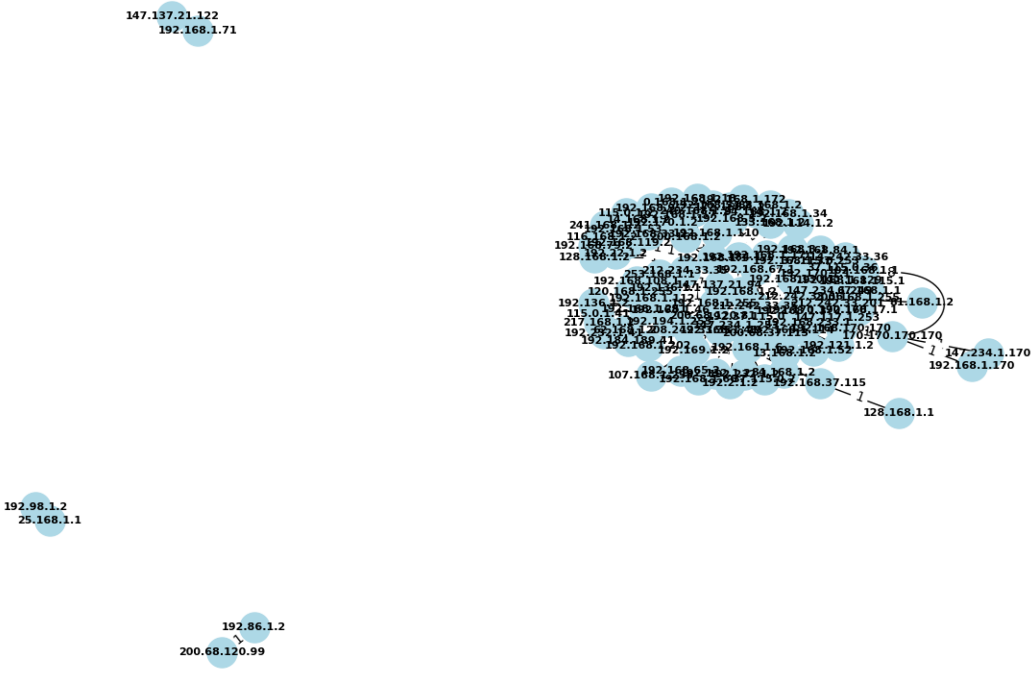
Top 10 Source IPs



Traffic Distribution by Hour



Network Communication Graph



Security Concerns

- High traffic on unusual ports: 137, 5060

Recommendations

- Review and potentially restrict traffic on identified unusual ports.