Network Anomaly Connection Analysis Report

# Analysis Details

Source Analysis File: anomalies\_20250409\_145806.csv

Analysis Generated On: 2025-04-09 15:33:47

Analysis Model Used: hf.co/QuantFactory/Lily-Cybersecurity-7B-v0.2-GGUF:Q8\_0

Total Connection Groups Analyzed in Source: 4

# Analysis Metrics Summary

**Average Response Rate:** 16.25 words/second

**Average Sentence Length:** 16.41 words

**Average Vocabulary Richness:** 0.5588

**Average Word Length:** 6.72 characters

**Content Analysis:**

**Content Metrics:**

**Performance Metrics:**

**Top 5 Most Common Words:** devices (19), these (12), connections (11), connection (11), are (10)

**Total Character Count:** 8269

**Total Elapsed Time:** 76.13 seconds

**Total Sentence Count:** 75

**Total Word Count:** 1231

# Detailed Connection Group Analysis

## Connection Group 1 Analysis

### Analysis:  
  
#### Device Identification:  
The devices involved in this connection group are both identified as having an unknown manufacturer, denoted by "UNKNOWN" in the SRCMFG and DSTMFG columns. Their MAC addresses are also listed as "UNKOWN," further emphasizing their obscurity.  
  
#### Communication Details:  
The connections made between these devices utilize the TCP protocol. The source IP address, 192.168.68.68, is associated with both connections. Interestingly, the destination MAC addresses are identical for both connections (f0:09:0d:4d:83:00). However, the destination IP addresses differ slightly, which could indicate the existence of multiple devices behind that MAC address or a potential misconfiguration within the network.  
  
#### Traffic Volume:  
The CNT field indicates that each connection has had six and eight packets sent, respectively. While this traffic volume is not particularly alarming, it may be worth investigating further to determine if these connections represent legitimate communication or potentially malicious activities.  
  
#### Risk Assessment:  
Given the lack of information about the devices involved (unknown manufacturers) and their purpose within the network, it is challenging to assess the risk level accurately. However, using the available data, we can see that both devices are communicating using an unknown MAC address with a slightly different IP address as the destination. This anomaly could indicate unauthorized activity or potential security vulnerabilities.  
  
#### Recommendations:  
Due to the identified risks and the lack of clear context about the devices involved, it is recommended to prioritize further investigation into these connections. Specific actions for security personnel may include blocking the traffic temporarily to prevent any potential harm, closely monitoring the devices' behavior, or conducting a thorough examination of the network for any signs of intrusion or misconfiguration.

## Connection Group 2 Analysis

### Analysis Report for Anomalous Connection Group on 2025-04-09 at 14:58:06  
  
#### Device Identification:  
The devices involved in this anomalous connection group are both TP-Link Systems Inc devices, as indicated by their MAC addresses (f0:09:0d:4d:83:00) and the manufacturer name in the SRCMFG column. These devices have unique identifiers and operate under the TP-Link brand.  
  
#### Communication Details:  
The protocol used for these anomalous connections is TCP. The source IP address, SRCIP, is 35.186.224.46, with a source port of both EPH (Ephemeral Ports), as indicated by the SRCPORT value. The destination MAC addresses, DSTMAC, are c2:30:6b:75:12:d8, and the destination IP addresses, DSTIP, are 192.168.68.68. The destination ports, DSTPORT, are also indicated as EPH (Ephemeral Ports).  
  
#### Traffic Volume:  
The CNT field shows that both connections have a packet count of 4.0 for the first connection and 2.0 for the second connection. This information indicates the volume of traffic associated with each anomalous connection.  
  
#### Risk Assessment:  
Given the protocol used, TCP, and the involvement of unknown devices (UNKNOWN as SRCMFG), these connections pose a medium-level risk to our network environment. The use of ephemeral ports (EPH) on both ends further increases the potential for malicious activities, such as port scanning or unauthorized access attempts. However, it is important to note that the actual risk may depend on additional context and information about the specific devices and their intended purposes.  
  
#### Recommendations:  
Based on the protocols used and the unknown devices involved, I would recommend further investigation into these anomalous connections. Blocking or restricting these connections temporarily may be a reasonable measure to minimize potential risks while gathering more information. It is crucial for security personnel to closely monitor any subsequent activity related to these devices to ensure the safety of our network environment.

## Connection Group 3 Analysis

### Anomalous Connection Analysis:  
  
##### Device Identification:  
The anomalous connection group involves a device with an unknown manufacturer named "UNKNOWN" and MAC address "c2:30:6b:75:12:d8". Based on the provided information, it appears that this device is communicating with another device from TP-Link Systems Inc. This connection has been flagged as anomalous due to the unknown manufacturer of the device initiating the connections.  
  
##### Communication Details:  
The communication between these devices occurs using the UDP protocol. The source IP address (192.168.68.68) is associated with an ephemeral port (EPH), ranging from 33950 to 46726. The destination IP address (68.105.28.15) is the same for all connections, while the source MAC address remains consistent with "f0:09:0d:4d:83:00".  
  
##### Traffic Volume:  
The CNT field indicates that there are multiple connections established between these devices, which can be observed by the repeated occurrence of the same IP addresses and ports. The specific number of packets exchanged for each connection is not provided in the given information.  
  
##### Risk Assessment:  
Given the context of this anomalous connection group, I would assess the risk level as Medium. While there are multiple connections established, it seems that these devices are communicating with a known manufacturer, TP-Link Systems Inc. However, having an unknown device involved adds an element of uncertainty and potential vulnerability. It is important for security personnel to investigate further and ensure that appropriate security measures are in place to mitigate any potential risks associated with this connection group.  
  
##### Recommendations:  
Based on the information provided, I recommend monitoring these connections closely. Investigating the unknown device "UNKNOWN" and its behavior within the network environment would be prudent. It is crucial for security personnel to gather more details about the device and its intended purpose before deciding whether to block or allow the connections. By conducting further analysis, potential threats can be identified and appropriate actions can be taken to safeguard the network infrastructure.

## Connection Group 4 Analysis

Device Identification:  
In this anomalous connection group, all devices involved are identified as TP-Link Systems Inc based on their manufacturer (MFG) names. However, the MAC addresses associated with these devices are marked as "UNKNOWN", which raises concern about their identification. It is important to note that without knowing the specific OUIs (Organizationally Unique Identifiers) of these devices, it becomes challenging to determine if they are part of our baseline or not.  
  
Communication Details:  
The protocol used in this communication group is UDP. The IP addresses involved are 68.105.28.15 (source) and 192.168.68.68 (destination). It appears that the source device initiates the connection from its ephemeral port (EPH), which could indicate various applications such as DNS, NTP, or a custom application using UDP protocol.  
  
Traffic Volume:  
The CNT field in this connection group shows a packet count of 1 for each connection. Since we are dealing with anomalous connections, the traffic volume might not be indicative of any malicious intent, but it is crucial to monitor and investigate further.  
  
Risk Assessment:  
Based on the provided information, I would assess the risk level as "Medium". The unknown devices and the usage of an uncommon protocol (UDP) warrant further investigation to ensure that these connections are not associated with any potential threats or vulnerabilities.  
  
Recommendations:  
Given the uncertainty regarding the devices involved due to their unknown OUIs, I would recommend taking a cautious approach. Initially, it may be prudent to block these connections until their exact nature and potential risks can be thoroughly assessed. Once more information is gathered, further actions such as monitoring or investigating these connections may become necessary based on the specific findings and context.  
  
It's important for security personnel to stay vigilant and continue monitoring network activities closely while conducting a comprehensive investigation into these anomalous connections. By doing so, we can ensure the safety and security of our network environment.