Task 5 - Network Traffic Analysis Report

# 1. TCP Traffic Analysis

Captured Packets Range: Frame Numbers 100–115  
Observed Protocols: TCP, TLSv1.2  
Key Findings:  
- A TCP three-way handshake was successfully completed between 192.168.1.15 and 23.55.106.34 on port 443.  
- TLS handshake initiated (Client Hello observed).  
- Several TCP Dup ACKs, out-of-order packets, and fast retransmissions were recorded.  
- TLS errors such as "Previous segment not captured" and "Ignored Unknown Record" indicate packet loss.  
Conclusion:  
Connection establishment was successful, but network performance was degraded due to retransmissions and loss.

# 2. ICMPv6 Traffic Analysis

Captured Packets Range: Frame Numbers 65–99  
Observed Protocol: ICMPv6  
Key Findings:  
- Detected frequent Neighbor Solicitation messages using ICMPv6 from link-local IPv6 sources.  
- Also observed Multicast Listener Report messages, a normal part of IPv6 operation.  
Conclusion:  
ICMPv6 behavior is consistent with IPv6 Neighbor Discovery Protocol (NDP); no anomalies found.

# 3. mDNS Traffic Analysis

Captured Packets Range: Frame Numbers 80–133  
Observed Protocol: mDNS (Multicast DNS)  
Key Findings:  
- Detected mDNS queries and responses including '\_googlecast.\_tcp.local' and '\_ipp.\_tcp.local' indicating the presence of Chromecast and printer services.  
- Multicast IPs used: 224.0.0.251 (IPv4) and ff02:fb (IPv6).  
Conclusion:  
Standard LAN service discovery traffic observed. Network contains Google Cast and printer-capable devices.

# 4. Overall Summary

|  |  |  |
| --- | --- | --- |
| Protocol | Key Activity | Remarks |
| TCP | TLS Handshake, Packet Loss | Connection stable but degraded due to packet loss |
| ICMPv6 | Neighbor Discovery | Expected IPv6 activity, no issues |
| mDNS | Service Discovery | Google Cast, IPP detected on LAN |