AK

TCP and UDP Packet Analysis Report

Prepared by: Abel Kolawole | Date: January 6, 2026

Subject: Transport Layer Protocol Comparison and Analysis

This document presents a technical analysis of TCP and UDP transport-layer protocols based on packet captures collected using Wireshark. The focus is on reliability, data integrity, and performance trade-offs observed in FTP and TFTP traffic.

Table of Contents

1. Objective 2. Lab Environment & Tools 3. Recreated Lab Topology 4. TCP Analysis 5. UDP Analysis 6. Comparison 7. Troubleshooting & Conclusion 8. References

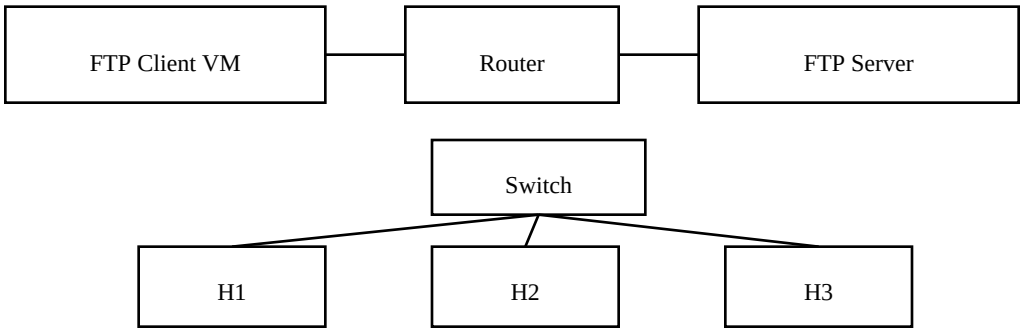
1. Objective

The goal of this project was to analyze and compare TCP and UDP transport-layer behavior by capturing and inspecting FTP (TCP) and TFTP (UDP) network traffic.

2. Lab Environment & Tools

Operating System: Linux (CyberOps Workstation VM). Tools: Wireshark, Mininet, FTP, TFTP. Protocols Analyzed: TCP (FTP) and UDP (TFTP).

3. Recreated Lab Topology



4. TCP Analysis (FTP Session)

The TCP three-way handshake (SYN, SYN-ACK, ACK) was observed during the FTP session, establishing a reliable connection prior to data transfer. Source IP: 10.0.2.15. Destination IP: 198.246.121.209. Source Port: 41026. Destination Port: 21 (FTP). Header Length: 40 bytes.

5. UDP Analysis (TFTP Session)

The TFTP transfer between Mininet hosts demonstrated UDP’s connectionless behavior. Source IP: 10.0.0.12. Destination IP: 10.0.0.11. Source Port: 45040. Destination Port: 69 (TFTP). UDP Length: 32.

6. TCP vs UDP Technical Comparison

Category	TCP (FTP)	UDP (TFTP)
Connection State	Connection-oriented	Connectionless
Reliability	Sequencing & retransmissions	Best-effort
Header Length	20 bytes	8 bytes
Lab Context	Secure, reliable transfer	Speed and simplicity

7. Troubleshooting & Conclusion

Root-owned packet captures caused permission issues, resolved using chown. UDP checksum offloading resulted in unverified checksum warnings in Wireshark. Overall, the analysis highlights TCP reliability versus UDP efficiency.

8. References

• Cisco Networking Academy: Lab – Using Wireshark to Examine TCP and UDP Captures. • Reddit Linux Community (r/Linux) for permission and chown best practices.