Project 4 - Traceroute Implementation Report

Student 1: Brian Zhang (bz271) **Student 2:** Christopher Doss (cad407)

Part B: Wireshark Analysis

Destination used: www.princeton.edu

1. What is the value of the protocol field in the IP layer? Which protocol does it indicate?

(Answer with reference to first request and response packet in your trace)

Answer:

- **Request (Probe):** Protocol field = 17, Protocol = UDP
- **Response (ICMP):** Protocol field = 1, Protocol = ICMP

2. How many IP headers do you observe in the ICMP response packet?

Answer: 2 IP headers. *(Explanation: The outer IP header (Router -> You) and the inner IP header (You -> Destination) that is embedded in the ICMP payload as the "quoted" original packet)*

3. What is the value of the type field and code field in the ICMP packet received from the router?

(Answer with reference to first request and response packet in your trace)

Answer:

- **Type:** 11 (Time Exceeded)
- **Code:** 0 (TTL exceeded in transit)

4. What is the value of the type field and code field in the ICMP packet received from the destination?

Answer:

- **Type:** (Not Reached) - In your specific trace, the destination (Princeton/Cloudflare) filtered the final packets, so no Type 3 Code 3 was received.
- **Code:** (Not Reached) *(Note: standard traceroutes usually end with Type 3 Code 3, but modern firewalls often block this. Your trace ended at hop 11 without reaching final destination)*

5. How many routers were present in the path to the destination?

Answer: 11 routers were visible in the trace (trace stopped at hop 11). *(Cloudflare firewall prevented seeing the final hop)*

6. What is the TTL in the packet delivered to the destination?

Answer: 11 *(This corresponds to the max TTL reached in your specific trace before it stopped)*

7. How does source and destination IP in different layers of IP in ICMP packet relate to your machine (ilab), your destination machine and intermediate router?

Answer:

- **Outer IP Header:**
  - Source IP: The Router's IP (e.g., 172.24.48.1 for the first hop)
  - Destination IP: My Machine's IP (172.24.52.159)
- **Inner IP Header (inside ICMP payload):**
  - Source IP: My Machine's IP (172.24.52.159)
  - Destination IP: Destination Machine's IP (104.18.4.101)