Wireshark Report: Network Layer and IP Header Analysis

Rohan Baral
PAS077BCT029

July 1, 2024

1 Introduction

In modern networking, the network layer plays a crucial role in enabling effective data routing across interconnected systems. The Internet Protocol (IP) essentially specifies how packets are addressed and routed between devices. The network layer analysis covered in this study primarily looks at the structure and importance of IP headers. Captured packets are examined using Wireshark to learn more about IP header elements and how they contribute to dependable data transfer. This study is essential for network administrators and engineers alike since it improves our capacity to identify problems with networks and maximize performance.

2 Network Layer Overview

Anything that has to do with inter-network connections takes place at the network layer. This includes setting up the routes for data packets to take, checking to see if a server in another network is up and running, and addressing and receiving IP packets from other networks. This last process is perhaps the most important, as the vast majority of Internet traffic is sent over IP.

3 IP Header Analysis

3.1 Structure of the IP Header

IPv4, or Internet Protocol Version 4, is a foundational protocol used in packet-switched networks, offering connectionless communication across various types of networks since its implementation in ARPANET in 1983. It utilizes 32-bit addresses expressed in decimal form, facilitating logical connections between devices through identification.

3.1.1 Key Characteristics

- IPv4 addresses are 32-bit integers in decimal dotted notation (e.g., 192.168.1.5), classified into five classes (A, B, C, D, E) for different network and host configurations.
- The protocol supports unicast, broadcast, and multicast addressing.
- IPv4 allows for Variable Length Subnet Masking (VLSM) and uses Address Resolution Protocol (ARP) to map IP addresses to MAC addresses.

3.1.2 IPv4 Datagram Header

The IPv4 datagram header includes the following fields:

Version (4 bits): Identifies the IP protocol version (always 4 for IPv4).

Header Length (4 bits): Specifies the length of the header in 32-bit words (ranges from 5 to 15 words).

Type of Service (8 bits): Defines quality of service parameters such as low delay, high throughput, and reliability.

Total Length (16 bits): Indicates the total length of the datagram including header and data (ranging from 20 to 65,535 bytes).

Flags and Fragmentation Offset: Control flags for fragmentation and reassembly of packets.

Time to Live (8 bits): Limits the lifespan of the packet to prevent indefinite looping in the network.

Protocol (8 bits): Specifies the protocol used in the data portion of the datagram (e.g., TCP, UDP).

Header Checksum (16 bits): Ensures data integrity by verifying the header contents.

Source & Destination IP Addresses (32 bits each): Identify the sender and intended recipient of the datagram.

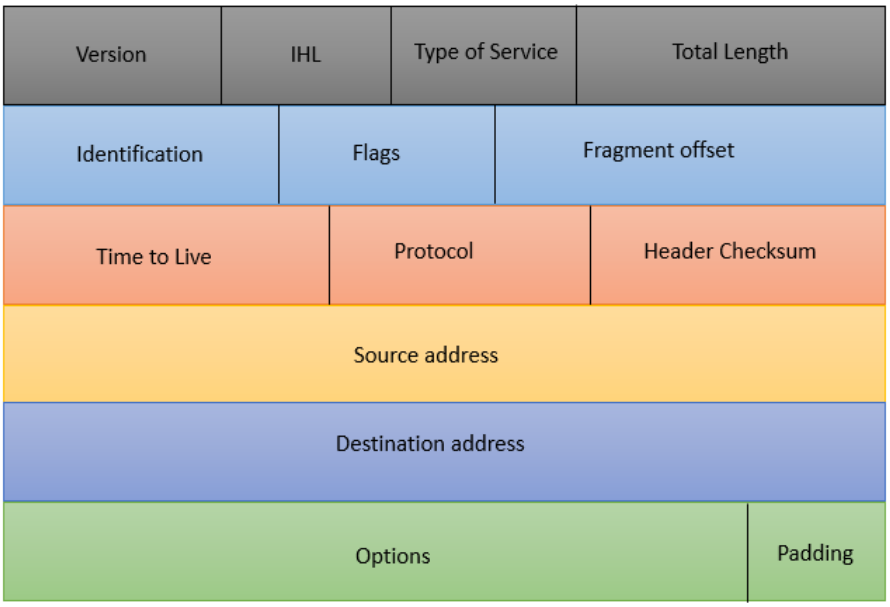

Figure 1: The IPV4 Header

3.2 Example Packet Analysis

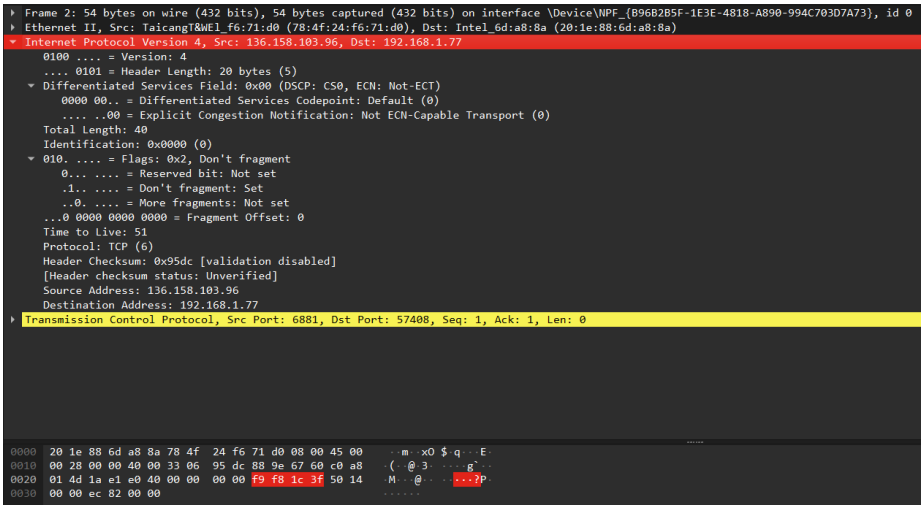

Figure 2: Wireshark Packet Example

- **Version:** IPv4 (Version 4).

- **Header Length:** 20 bytes, indicating the size of the IPv4 header.
- **Differentiated Services Field:** Default (CS0), with Explicit Congestion Notification (ECN) not enabled.
- **Total Length:** 40 bytes, including both header and data.
- **Identification:** Packet identification number is 0x0000.
- **Flags:** "Don't fragment" flag (DF) is set, ensuring the packet is not fragmented.
- **Fragment Offset:** 0, indicating this packet is not part of a fragmented set.
- **Time to Live:** 51, limiting the packet's lifespan to prevent looping in the network.
- **Protocol:** TCP (6), specifying the protocol for data handling.
- **Header Checksum:** 0x95dc, used for error detection (not verified in this capture).
- **Source Address:** 136.158.103.96, identifying the sender of the packet.
- **Destination Address:** 192.168.1.77, identifying the intended recipient of the packet.

4 Conclusion

The IPv4 datagram header, which includes essential details such as version, header length, kind of service, and checksum for dependable communication, is critical for data delivery and routing across networks. Knowing these headers is essential for network administration, as network traffic is captured and analyzed by programs like Wireshark. In-depth information about header fields is provided by Wireshark, which helps with troubleshooting and network speed optimization. In general, network professionals are better equipped to maintain safe and effective networks by being knowledgeable with IPv4 headers and Wireshark.