Analysis of an IPv6 Packet in Wireshark

Aayush Adhikari, Roshan Tiwari, Shishir Sharma Rijal, Sudip Acharya

July 18, 2024

Overview

This document provides a detailed analysis of an IPv6 packet captured in Wireshark. The specific packet in question is Frame 5757, which consists of 144 bytes and contains various protocol layers.

1 Frame Summary

- **Frame Number:** 5757
- **Frame Length:** 144 bytes (1152 bits)
- **Capture Length:** 144 bytes (1152 bits)
- **Protocols in Frame:** Ethernet, IPv6, UDP, mDNS

2 Detailed Breakdown of the Packet

2.1 Frame Information

- **Frame Number:** 5757
  The unique identifier for this specific frame captured in the packet trace.
- **Frame Length:** 144 bytes
  The total size of the packet, including headers and payload.
- **Capture Length:** 144 bytes
  The amount of data captured for this packet. In this case, it matches the frame length, indicating no truncation.
- **Protocols in Frame:** eth:ethertype:ipv6:udp:mdns
  A list of protocols encapsulated within this frame, indicating the hierarchy from Ethernet to the application layer.

2.2 Ethernet II Header

- **Source MAC Address:** 6a:b0:ce:c1:62:dd
  The hardware address of the sender's network interface.
- **Destination MAC Address:** IPv6mcast_fb (33:33:00:00:00:fb)
  Indicates that the packet is sent to a multicast address reserved for IPv6.
- **Type:** IPv6 (0x86dd)
  Specifies the protocol type carried in the Ethernet frame, indicating that the payload is an IPv6 packet.

2.3 Internet Protocol Version 6 (IPv6) Header

- **Version:** 6
  Indicates that this is an IPv6 packet.
- **Traffic Class:** 0x00
  Represents the Differentiated Services Code Point (DSCP) and Explicit Congestion Notification (ECN). A value of 0 indicates the default traffic class.
- **Flow Label:** 0x90400
  A 20-bit field used to identify packets that belong to the same flow, facilitating quality of service.
- **Payload Length:** 90
  The length of the payload (UDP header + data) in bytes.
- **Next Header:** UDP (17)
  Indicates the next header protocol; in this case, it specifies that the next layer is UDP.
- **Hop Limit:** 255
  Similar to TTL in IPv4, this field limits the number of hops a packet can take. A value of 255 indicates that the packet can traverse the maximum number of hops before being discarded.
- **Source Address:** fe80::8a4:9b9d:993a:128d
  The IPv6 address of the packet's sender, indicating it is a link-local address.
- **Destination Address:** ff02::fb
  The IPv6 multicast address to which the packet is sent, specifically for mDNS queries.

IP Header Data in Byte Format

Offset	Value (Hex)	Description
0000	33 33 ff 3a 12 8d	Destination MAC Address
0006	6c b1 33 9d 0f ce	Source MAC Address
000c	86 dd	EtherType (IPv6)
000e	60	Version (6)
000f	00	Traffic Class
0010	00	Traffic Class
0011	00	Flow Label
0012	00 20	Payload Length (32 bytes)
0014	3a	Next Header (ICMPv6)
0015	ff	Hop Limit (255)
0016	fe 80	Source Address (fe80::)
0018	00 00 00 00	Source Address
001c	18 6d 46 61	Source Address
0020	98 f0 c6 d9	Source Address
0024	ff 02	Destination Address (ff02::)
0026	00 00 00 00	Destination Address
002a	00 00 00 00	Destination Address
002e	00 01	Destination Address
0030	ff 3a 12 8d	Destination Address
0034	87	ICMPv6 Type (Neighbor Solicitation)
0035	00	ICMPv6 Code
0036	ab 17	Checksum
0038	00 00 00 00	Reserved
003c	fe 80	Target Address
0040	00 00 00 00	Target Address
0044	00 00	Target Address
0046	08 a4 9b 9d	Target Address
004a	99 3a 12 8d	Target Address
004e	01	ICMPv6 Option Type
004f	01	ICMPv6 Option Length
0050	6c b1 33 9d 0f ce	Link-layer Address

2.4 User Datagram Protocol (UDP) Header

- **Source Port:** 5353
  The port from which the packet is sent. Port 5353 is commonly used for mDNS (Multicast DNS).

- **Destination Port:** 5353
  The port to which the packet is directed. This matches the source port, indicating a typical behavior in multicast communications.

- **Length:** 90
  The total length of the UDP packet, including both the header and the payload.

- **Checksum:** 0xa6f2 [unverified]
  A checksum used for error-checking the packet. The status ”unverified” indicates that the checksum has not been validated.

2.5 UDP Payload

- **Payload Size:** 82 bytes
  This indicates the size of the data carried in the UDP packet, which consists of mDNS query data.

2.6 Multicast Domain Name System (mDNS) Query

- **Transaction ID:** 0x0000
  A unique identifier for the query, allowing the sender to match responses with requests.
- **Flags:** 0x0000
  Indicates that this is a standard query with no additional options set.
- **Questions:** 3
  The number of questions included in the query.
- **Answer RRs:** 0
  Indicates that there are no resource records in the answer section yet.
- **Authority RRs:** 0
  Indicates that there are no authority records in the response.
- **Additional RRs:** 0
  Indicates that there are no additional resource records.

3 Conclusion

This analysis illustrates the structure and content of an IPv6 packet as captured in Wireshark. Understanding each field helps in diagnosing network issues, implementing security measures, and enhancing network protocols.