Analysis of IPV6 Packet in Wireshark

Introduction

This document provides a detailed analysis of an IPv6 packet captured in Wireshark. The specific packet captured is Frame 128, which consists of 86 bytes and contains various protocol layers.

Frame Summary

- **Frame Number:** 128
- **Frame Length:** 86 bytes (688 bits)
- **Capture Length:** 86 bytes (688 bits)
- **Protocols in Frame:** Ethernet, IPv6, ICMPV6

Detailed Breakdown of the Packet

Frame Information

- **Frame Number:** 128
  The unique identifier for this specific frame captured in the packet trace.
- **Frame Length:** 86 bytes
  The total size of the packet, including headers and payload.
- **Capture Length:** 86 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:icmpv6
  A list of protocols encapsulated within this frame, indicating the hierarchy from Ethernet to the application layer.

Ethernet II Header

- **Source MAC Address:** 5e:ba:2e:5e:ed:3c

  The hardware address of the sender's network interface.

- **Destination MAC Address:** IPv6mcast_01 (33:33:00:00:00:01)
  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.

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:** 0x00000
  A 20-bit field used to identify packets that belong to the same flow, facilitating quality of service.

- **Payload Length:** 32
  The length of the payload (UDP header + data) in bytes.

- **Next Header:** ICMPv6 (58)
  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::776e4:4d0b:2a8b:c6d1
  The IPv6 address of the packet's sender, indicating it is a link-local address.
- **Destination Address:** ff02::1
  The IPv6 multicast address to which the packet is sent.

IP Header Data in Byte Format

Offset	Value (Hex)	Description
0000	33 33 00 00 00 01	Destination MAC Address
0006	5e ba 2e 5e ed 3c	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	00 00 77 6e	Source Address
0020	4d 0b 2a 8b	Source Address
0026	ff 02	Destination Address (ff02::)
002	00 00 00 00	Destination Address
002a	00 00 00 00	Destination Address
002e	00 00	Destination Address
0030	00 00 00 01	Destination Address
0034	88	ICMPv6 Type (Neighbor Solicitation)
0035	00	ICMPv6 Code
0036	73 9b	Checksum
0038	20 00 00 00	Reserved
003c	fe 80	Target Address
0040	00 00 00 00	Target Address
0044	00 00	Target Address
0046	77 6e 4a 0b	Target Address
004a	2a 8b c6 d1	Target Address
004e	02	ICMPv6 Option Type
004f	01	ICMPv6 Option Length
0050	5e ba 2e 5e ed 3c	Link-layer Address

ICMPv6

- Type: Neighbor Advertisement (136)
- Checksum: 739b
- Target Address: fe80::776e:4d0b:2a8b:c6d1
- Flags: 20000000, override

Conclusion

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