**ICMPv6 Packet Analysis Report**

**\* - Almustapha Wakili**

**\* - Amuda Kamorudeen**

**\* - Binkam Deepak**

**\* - Ciana Hoggard**

**Introduction**

This detailed report provides an analysis of ICMPv6 packets captured during a network monitoring session as part of Task 1 for the COSC 650 course project, conducted by the Amuda Group. This task aims to dissect and understand the function and structure of ICMPv6 packets which are pivotal in IPv6 networking, specifically focusing on their roles in error reporting and informational messaging.

**Objectives**

* To capture live network traffic containing ICMPv6 packets using Wireshark.
* To select and analyze a specific ICMPv6 packet, focusing on the IPv6 and ICMPv6 headers.
* To explain the significance of the extracted fields and their roles in network communication.

**Methodology**

Setup and Packet Capture

1. \*\*Environment Preparation:\*\* Configure Wireshark on a local machine connected to an IPv6-capable network. Ensure the network interface is configured to accept IPv6 traffic.

2. \*\*Capturing Packets:\*\* Start Wireshark and initiate packet capture on the selected network interface. Execute a `ping -6 fe80::1` command from a terminal or command prompt to generate ICMPv6 traffic, targeting the link-local IPv6 address. Allow Wireshark to run during the ICMPv6 transaction to capture inbound and outbound packets.

Packet Selection and Analysis

1. \*\*Selection Criteria:\*\* Identify and select a packet that clearly represents ICMPv6 communication (e.g., Router Advertisement, Echo Request/Reply). Choose Frame Number 27 for this report due to its completeness and relevance.

2. \*\*Analysis Procedure:\*\* Extract and document key fields from both the IPv6 and ICMPv6 headers. Use protocol specifications from IETF RFCs and other technical resources to interpret field values and their implications.

**Results and Analysis**

**Frame Number**

**27**

**IPv6 Header Fields**

- \*\*Version\*\*: 6. Indicates the protocol version, confirming the packet is using IPv6.

- \*\*Traffic Class\*\*: 0x00. Typically used for Differentiated Services (DiffServ), here indicates default handling.

- \*\*Flow Label\*\*: 0x2dbac. Helps label packets belonging to the same flow; used in managing packet sequencing and Quality of Service (QoS).

- \*\*Payload Length\*\*: 120. The length in bytes of the ICMPv6 payload.

- \*\*Next Header\*\*: 58. Specifies that the next header is an ICMPv6 header, dictating the type of payload encapsulated.

- \*\*Hop Limit\*\*: 255. Maximum hops allowed for the packet, often set to 255 for local subnet communications.

- \*\*Source Address\*\*: `fe80::fad2:acff:fe78:b83f`. Link-local address of the sender, used within a single network segment.

- \*\*Destination Address\*\*: `ff02::1`. Multicast address that targets all nodes on the local link.

**ICMPv6 Header Fields**

- \*\*Type\*\*: 134 (Router Advertisement). Indicates the packet's purpose in the communication.

- \*\*Code\*\*: 0. Additional specification for the Type field; here indicates a general message.

- \*\*Checksum\*\*: 0xc677. Validates the integrity of the ICMPv6 message, ensuring no corruption occurred during transit.

- \*\*Flags\*\*: 0xc0. Bits representing various configuration flags (e.g., Managed Address Configuration).

- \*\*Router Lifetime\*\*: 180 seconds. Indicates the duration the router is considered as default.

- \*\*Reachable Time\*\*: 0 milliseconds. Specifies the time a node is considered reachable after a confirmation.

- \*\*Retrans Timer\*\*: 0 milliseconds. Time between retransmitted Neighbor Solicitation messages.

**Additional Frame Information**  
- ICMPv6 Option (Recursive DNS Servers): Lists recursive DNS servers for IPv6 addresses, such as 2001:558:feed::1 and 2001:558:feed::2.  
- ICMPv6 Option (Prefix Information): Provides prefix-related details like length (32 bytes), prefix (2601:155:400:ca50::/64), and flags for on-link and autonomous address configuration.  
- ICMPv6 Option (Route Information): Contains routing information with route lifetime (180 seconds) and route preference.  
- ICMPv6 Option (Source Link-Layer Address): Provides the MAC address of the source, such as f8:d2:ac:78:b8:3f.

**Conclusion**

The ICMPv6 packet analysis performed provides in-depth insights into IPv6 operations and the roles of ICMPv6 messages in maintaining robust and efficient network communications. The detailed examination of the packet headers underscores their importance in network configuration, diagnostics, and management.

**Appendix**









