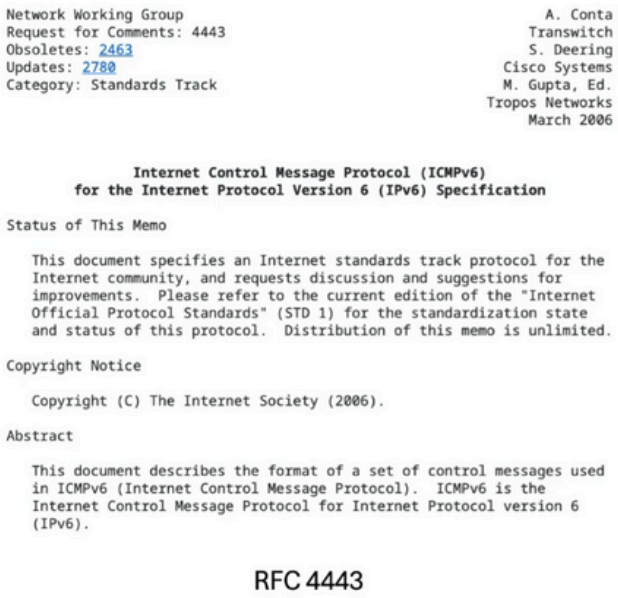
ICMPv6

- Internet Control Message Protocol Version 6 (ICMPv6) is responsible for sending control and error messages in IPv6 networks.
- Functionalities include:
  - Packet delivery errors
  - Redirections
  - Echo Request and Echo Reply
  - ...
- It serves as the foundation for the *Neighbor Discovery Protocol*.



Network Working Group
Request for Comments: 4443
Obsoletes: 2463
Updates: 2780
Category: Standards Track

A. Conta
Transwitch
S. Deering
Cisco Systems
M. Gupta, Ed.
Tropos Networks
March 2006

Internet Control Message Protocol (ICMPv6)
for the Internet Protocol Version 6 (IPv6) Specification

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This document describes the format of a set of control messages used in ICMPv6 (Internet Control Message Protocol). ICMPv6 is the Internet Control Message Protocol for Internet Protocol version 6 (IPv6).

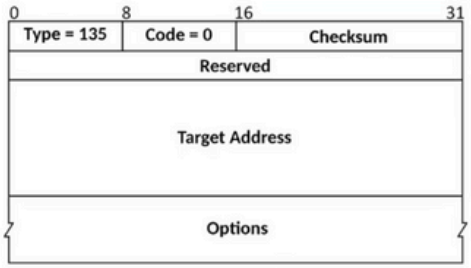
RFC 4443

Neighbor Discovery Protocol

- Allows nodes to discover other active nodes on the same local network.
- Facilitates the translation of layer 3 addresses to layer 2 addresses for efficient communication.
- Ensures there are no duplicate IP addresses on the same network, avoiding conflicts and ensuring connectivity.
- Fundamental for establishing connectivity and efficient communication between devices in IPv6 networks.

Neighbor Solicitation

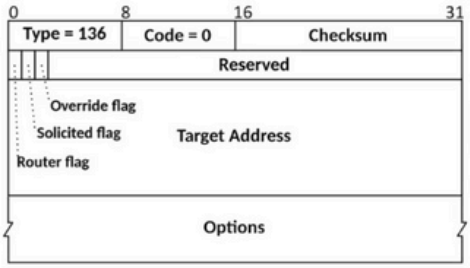
- They are sent by an IPv6 node to request the layer 2 address (MAC address) of another node on the same local network.
- They are used when a node needs to communicate with another node on the same local network and does not have the layer 2 address corresponding to the layer 3 address (IPv6 address) of the destination node in its neighbor cache.



Picture source: Neighbor Discovery Protocol (en.wikipedia.org)

Neighbor Advertisement

- They are sent by an IPv6 node in response to a Neighbor Solicitation (NS) message to announce its layer 2 address (MAC address).
- A node sends an NA message in response to an NS message directed to it, or it can send an NA message proactively to announce its presence on the network.



Picture source: Neighbor Discovery Protocol (en.wikipedia.org)

Neighbor Spoofing

- Attack technique in IPv6 networks.
- Impersonation of the identity of a legitimate node.
- Interception and manipulation of network traffic.
- Theft of confidential information.
- Possible launch of Denial of Service (DDoS) attacks.

Conclusion

- ICMPv6 is crucial for the administration and maintenance of IPv6 networks and essential for the proper functioning of NDP.
- The Neighbor Discovery Protocol facilitates key functions such as neighbor discovery and address resolution.
- Neighbor Solicitation and Neighbor Advertisement are essential components of NDP used to request the layer 2 address of a node (NS) and to respond and announce that address (NA).
- Neighbor Spoofing is a dangerous attack technique that compromises security by impersonating the identity of legitimate nodes.