IPv6 Query for Enabled In-situ OAM Capabilities

draft-ietf-6man-icmpv6-ioam-conf-state-02

Xiao Min ZTE
Greg Mirsky Ericsson
Recap of this draft

• This draft defines ICMPv6 extensions to achieve IOAM Capabilities Discovery in IPv6 Networks
  – A companion document of RFC 9359
  – Use RFC 4620 “IPv6 Node Information Queries” as basis
  – For this Query mechanism, five IOAM Capabilities Objects are defined in this document:
    • IOAM Tracing Capabilities Object
    • IOAM Proof of Transit Capabilities Object
    • IOAM Edge-to-Edge Capabilities Object
    • IOAM DEX Capabilities Object
    • IOAM End-of-Domain Object
Update since last IETF

• This draft was presented at IETF 117, David Lamparter raised good comments regarding amplification attack threat, a resolution to address David’s comments was incorporated

• Some editorial changes were also incorporated
  – Revised Abstract to make a stronger connection between RFC 9359 and this document
  – Changed the terms from “Node IOAM Information Query” to “Node IOAM Request”, from “Node IOAM Information Reply” to “Node IOAM Reply”
  – Changed the reference to [I-D.ietf-ippm-ioam-ipv6-options] that has been published as RFC 9486
Update since last IETF (Cont.1)

• New text in Security Considerations:

  – An implementation that supports this specification MUST support an option of padding a Node IOAM Request packet to the Path MTU or the minimum IPv6 MTU [RFC8200], which can ensure that the Node IOAM Reply packet would not be larger than the invoking Node IOAM Request packet.

  – The network operators can choose to enforce the padding option or not in their networks.
• New text in Abstract:

– This document describes the application of the mechanism of discovering IOAM capabilities, described in RFC 9359 "Ping Enabled IOAM Capabilities", in IPv6 networks.
Next steps

• Ask for more reviews and comments
• Revise this draft to improve it
• WGLC on it

Thank you!