# Echo Request/Reply for Enabled In-situ OAM Capabilities

draft-ietf-ippm-ioam-conf-state-03

| | |
|---|---|
| Xiao Min | ZTE |
| Greg Mirsky | Ericsson |
| Lei Bo | China Telecom |

# Discussion Points after IETF 112

- Is this document still needed in a limited domain?
  - Yes, it’s still needed in a limited domain.
  - Updates have been made in the Introduction section to clarify its usage.
- May this document be obsoleted by a YANG model?
  - No, it has nothing to do with YANG.
  - Suggestion on using ICMP to carry YANG model is not accepted.
- Are more requirements than recommendations needed for security?
  - Yes, the requirements are specific to ICMPv6 etc.
  - Clarifications have been made in the Security Considerations section.

# More details on discussion point 1

## Is this document still needed in a limited domain?

- In a limited domain [RFC8799], this document is not needed if both prerequisites exist:
  - A control entity that has control over every IOAM device is deployed
  - A strict explicit path for the IOAM packets is provisioned by the control entity that has control over every IOAM device

- The takeaway from the discussion is that if neither of the above prerequisites can be confirmed, then this document is still needed in a limited domain

# More details on discussion point 2

## May this document be obsoleted by a YANG model?

- This document has nothing to do with YANG
  - There was an older suggestion during the first WG AP on using NETCONF between the IOAM encapsulating node and the IOAM transit/decapsulating nodes. One paragraph was added into the Introduction section explaining why it’s not a preferred approach.
  - There was a later suggestion to use ICMP to carry the informational elements derived from the YANG model. Echo Request/Reply is not a Management protocol like NETCONF or RESTCONF. ICMP doesn’t seem suitable for carrying informational elements derived from the YANG model. This latest suggestion is not accepted.

# More details on discussion point 3

Are more requirements than recommendations needed for security?

- The specific security requirements for ICMPv6 are defined in draft-xiao-6man-icmpv6-ioam-conf-state:
  - Use IP Authentication Header or IP Encapsulating Security Payload Header to provide integrity protection for IOAM Capabilities information
  - Use IP Encapsulating Security Payload Header to provide privacy protection for IOAM Capabilities information
  - Network operators establish policies that restrict access to ICMPv6 IOAM Echo functionality
    - Enable/disable ICMPv6 IOAM Echo functionality
    - Define enabled Namespace-IDs
    - For each enabled Namespace-ID, define the prefixes from which ICMPv6 IOAM Echo Request messages are acceptable
  - Rate-limit incoming ICMPv6 IOAM Echo Request messages

# Other updates since IETF 112

- In the IOAM Tracing Capabilities Objects
  - Egress_MTU and Egress_if_id are substituted by Ingress_MTU and Ingress_if_id, because ICMPv6 Echo Request is destined for the responding node itself
- In the IOAM Proof-of-Transit Capabilities Object
  - P bit is removed to align with the latest draft-ietf-ippm-ioam-data
- In the IOAM Edge-to-Edge Capabilities Object
  - TSL is removed to align with the latest draft-ietf-ippm-ioam-data

# Next step

- WGLC?

Thank you!