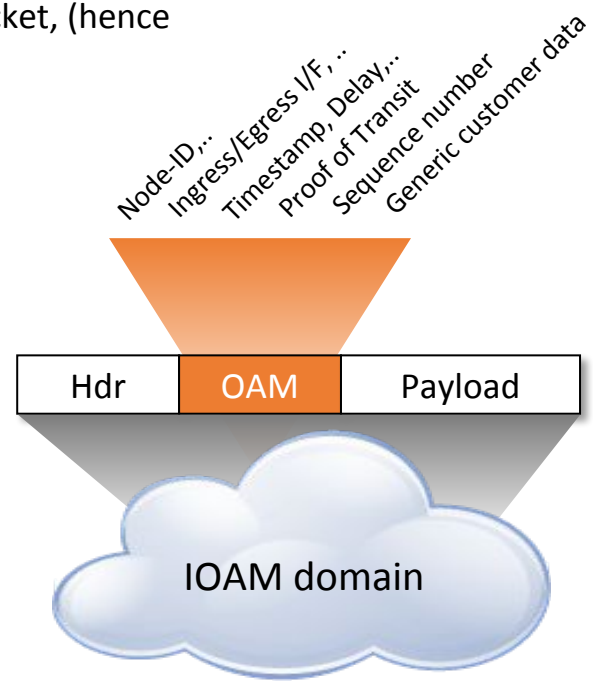
In-situ OAM (IOAM) in IPv6

6man

March 29th, 2019

In-situ OAM in a nutshell

- Gather telemetry and OAM information along the path within the data packet, (hence "in-situ OAM") as part of an existing/additional header
  - No extra probe-traffic (as with ping, trace, ..)
  - "Hybrid, Type-1 OAM" per RFC 7799
- Generic, Transport independent data-fields for IOAM
  - Scope: Per-hop, specific-hops only, end-to-end
  - Data fields include: Node IDs, interface IDs, timestamps, sequence numbers, ...
- Encapsulation
  - IOAM data fields can be embedded into a variety of transports, including: IPv6, SRv6, NSH, GRE, Geneve, VXLAN-GPE ...
- Main work on IOAM progressed in IPPM WG



Ask to 6man:

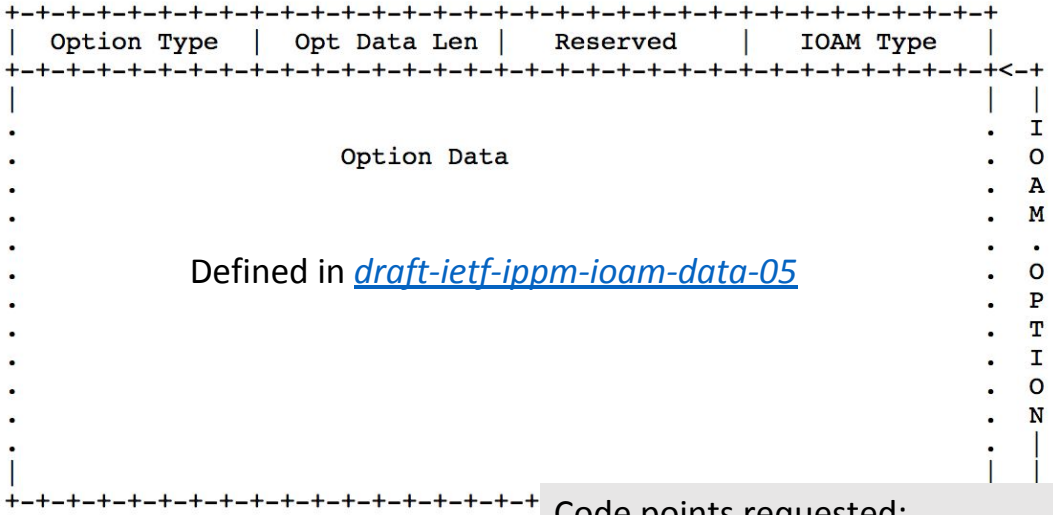
for IPv6 Option Type assignments to encapsulate IOAM data fields, so that work can progress further in IPPM.

(similar to what was done for PDM Dest-Option, RFC8250)

IOAM over IPv6

(draft-ioametal-ippm-6man-ioam-ipv6-options)

IPv6 Option format for carrying in-situ OAM data fields:



Defined in *draft-ietf-ippm-ioam-data-05*

IOAM Option	IPv6 Option type
Pre-allocated Tracing Option	HbH Option
Incremental Tracing Option	HbH Option
Proof of Transit Option	HbH Option
Edge to Edge Option	Destination Option

Code points requested:

Hex Value	Binary Value act chg rest	Description
TBD_1_0	00 0 TBD_1	IOAM Destination Option
TBD_1_1	00 1 TBD_1	IOAM HbH Option

Considerations for IOAM deployment in IPv6 networks

draft-ioametal-ippm-6man-ioam-ipv6-deployment

	Considerations
C1	Packet forwarding behaviour or decisions should not change due to presence of IOAM
C2	Addition of IOAM should not exceed PMTU
C3	ICMP errors due to addition of IOAM should be delivered to the source adding IOAM
C4	IOAM domains should provide a mechanism to prevent data leaks or be able to assure that upon leak network elements outside the domain are notaffected
C5	The source of that inserted and leaked the IOAM data must be easy to identify
C6	Compliance with [RFC8200] would require OAM data to be encapsulated instead of header/option insertion directly into in-flight packets using the original IPv6 header.

Deployment options

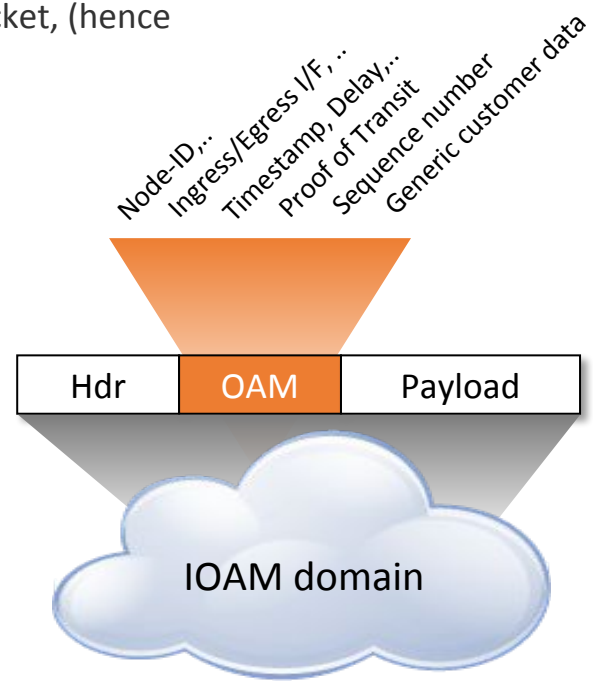
draft-ioametal-ippm-6man-ioam-ipv6-deployment

1. Source initiated IOAM
   a. Using extension headers to carry IOAM, per draft-ioametal-ippm-6man-ioam-ipv6-options
2. Transit networks - Use of encapsulation, avoiding header/option insertion into the original packets:
   a. IPv6-in-IPv6 encapsulation -
      using extension headers to carry IOAM (see above)
   b. IP-in-IPv6 encapsulation with ULA
      using extension headers to carry IOAM (see above)
   c. x-in-IPv6 encapsulation
      using “parent protocol”, e.g. Geneve-in-IPv6

BACKUP

In-situ OAM in a nutshell

- Gather telemetry and OAM information along the path within the data packet, (hence "in-situ OAM") as part of an existing/additional header
  - No extra probe-traffic (as with ping, trace, ..)
  - "Hybrid, Type-1 OAM" per RFC 7799
- Generic, Transport independent data-fields for IOAM
  - Scope: Per-hop, specific-hops only, end-to-end
  - Data fields include: Node IDs, interface IDs, timestamps, sequence numbers, ...
- Encapsulation
  - IOAM data fields can be embedded into a variety of transports, including: IPv6, SRv6, SR, NSH, GRE, Geneve, VXLAN-GPE ...
- Main work on IOAM progressed in IPPM WG



Deployment considerations

draft-ioametal-ippm-6man-ioam-ipv6-deployment-00

Considerations for IOAM deployment in IPv6 networks

	Considerations
C1	Packet forwarding behaviour or decisions should not change due to presence of IOAM
C2	Addition of IOAM should not exceed PMTU
C3	ICMP errors due to addition of IOAM should be delivered to the source adding IOAM
C4	IOAM domains should provide a mechanism to prevent data leaks or be able to assurethat upon leak network elements outside the domain are not affected
C5	The source of that inserted and leaked the IOAM data must be easy to identify
C6	Compliance with [RFC8200] would require OAM data to be encapsulated instead of header/option insertion directly into in-flight packets using the original IPv6 header.

Deployment options

1. Source initiated IOAM
   a. See draft-ioametal-ippm-6man-ioam-ipv6-options
2. Transit networks - Use of encapsulation, avoiding header/option insertion into the original packets:
   a. IPv6-in-IPv6 encapsulation -
      using extension headers to carry IOAM (see above)
   b. IP-in-IPv6 encapsulation with ULA
      using extension headers to carry IOAM (see above)
   c. x-in-IPv6 encapsulation e.g. Geneve-in-IPv6

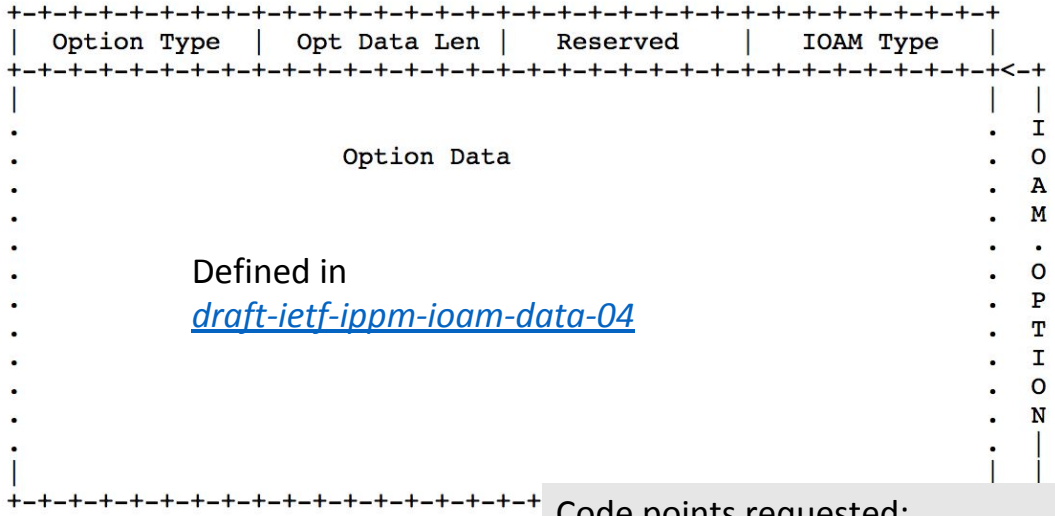
IOAM encapsulation in IPv6

draft-ioametal-ippm-6man-ioam-ipv6-options-01

IOAM over IPv6

(draft-ioametal-ippm-6man-ioam-ipv6-options-01)

IPv6 Option format for carrying in-situ OAM data fields:



IOAM Option	IPv6 Option type
Pre-allocated Tracing Option	HbH Option
Incremental Tracing Option	HbH Option
Proof of Transit Option	HbH Option
Edge to Edge Option	Destination Option

Code points requested:

Hex Value	Binary Value act chg rest	Description
TBD_1_0	00 0 TBD_1	IOAM Destination Option
TBD_1_1	00 1 TBD_1	IOAM HbH Option

Challenges

1. Limitations/Challenges of using encapsulation in transit network to carry IOAM

2. To support hardware friendly tracing option - Incremental Trace IOAM HbH Option: Changes Option Data Len en-route.
   a) Dealing with PMTU– Packet size changes can exceed PMTU.

1.Limitation/Challenges with encapsulation

1. Hard to ensure the encapsulated packet follows the same path with the same forwarding behaviour as original packet :
   a. IP-in-IPv6 encapsulation with ULA : “internal IPv6 forwarding topology using the IOAM domain's interior ULA address space that is parallel with the forwarding topology that exists with the non-IOAM address space” - Is an operational overhead

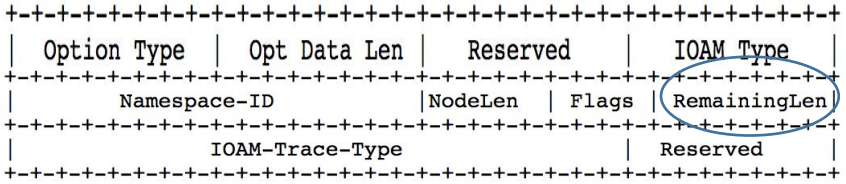
   b. If new IPv6 packet is created with encapsulating node as source(E) and the original destination (D) as the destination:
      1. Payload of this packet is the original IPv6 packet along with an extension header inserted inside.

      2. *The original packet is restored by removing the outer IPv6 header and the inner extension header by a node at the domain boundary.*
      3. *Modified packet may still leak – but will only confuse the destination node.*
      4. *ECMP computation needs to be reworked.*
      5. *Complex/costly implementation in HW & SW.*

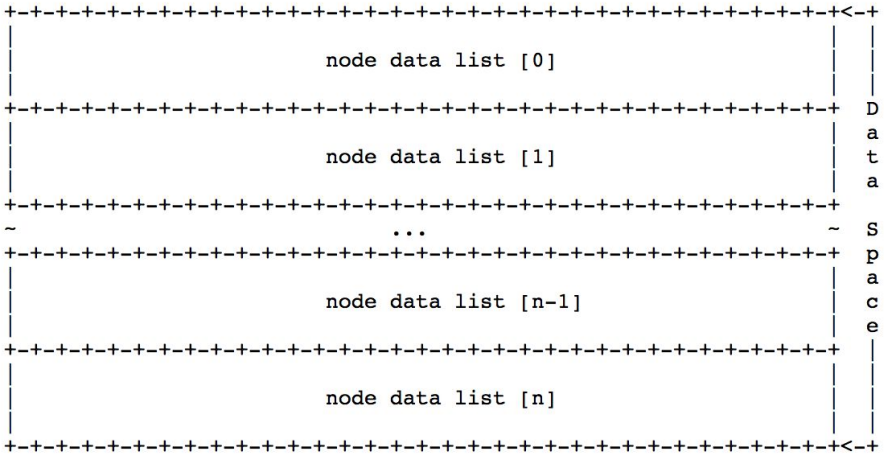
2. Incremental Trace IOAM HbH Option

- Possible Solutions

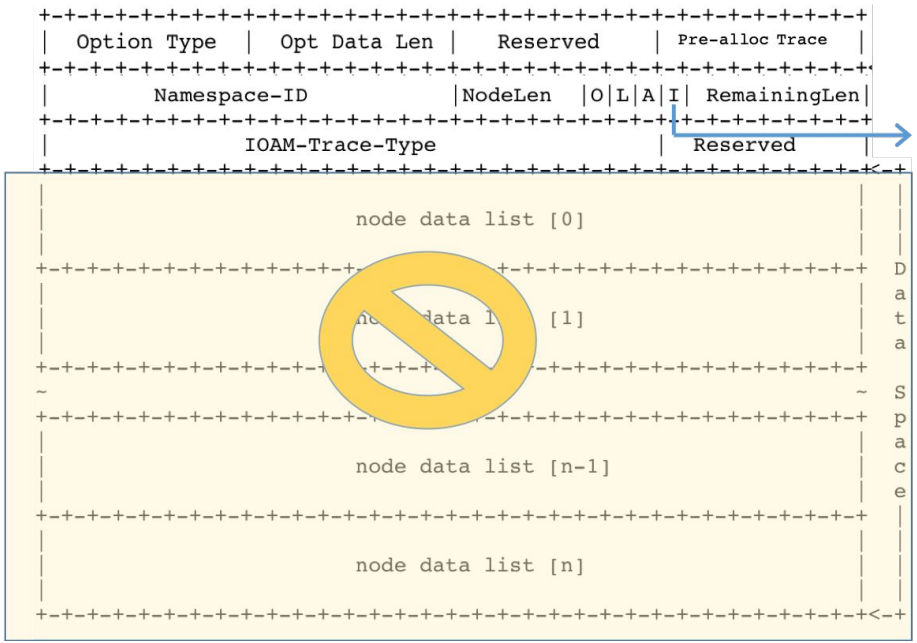
1. Use PMTU to determine max possible Incremental Trace IOAM Option length
2. Do not support Incremental Trace IOAM Option in IPv6?



The trace option data MUST be 4-octet aligned:



Another approach: Immediate export



Immediate export mode

- To export IOAM data fields immediately at every IOAM supported network node, instead of adding the IOAM data fields to the packet traversing the network.

Next steps

- IOAM data fields definition - draft-ietf-ippm-ioam-data - Progressing in IPPM WG.
- Please review draft-ioametal-ippm-6man-ioam-ipv6-options
- Should draft-ioametal-ippm-6man-ioam-ipv6-options progress in IPPM or 6man?