Overlay OAM Design Team Report

Greg Mirsky gregory.mirsky@ericsson.com
Carlos Pignataro cpignata@cisco.com
Nagendra Kumar naikumar@cisco.com
Deepak Kumar dekumar@cisco.com
Erik Nordmark nordmark@acm.org
David Mozes davidm@mellanox.com
Mach Chen mach.chen@huawei.com
Yizhou Li liyizhou@huawei.com

IETF-96 July, 2016

Changes since IETF-95

- Li Yuzhou joined OOAM DT
- Santosh Pallagatti had to leave
- Updates to:
  - OOAM Requirements (many thanks to Ron Bonica and Tal Mizrahi for their reviews)
  - OOAM Gap Analysis (many thanks to Tal Mizrahi for the review)
- New documents:
  - OOAM Header
  - OOAM Echo Request/Reply, a.k.a. Ping

Overlay OAM Requirements

draft-ooamdt-rtgwg-ooam-requirement-01

Extended definitions

- Centralized Controller: An external standalone or virtual entity with topology awareness and with an ability to interact with network devices for OAM functionality.
- Overlay nodes: Network nodes participating in the Overlay network.
- Overlay Network or Overlay Layer: A network layer that is built on top another network layer. VxLAN-GPE over IP network is an example for Overlay layer.
- Underlay Network or Underlay Layer: The network that provides connectivity between the Overlay nodes. MPLS network providing LSP connectivity between BIER nodes is an example for underlay layer.
  - Terms “underlay network/layer” and “transport network/layer” are being used interchangeably in discussions and the documents.

New Requirements

REQ#8: Overlay OAM MUST support Path Maximum Transmission Unit (MTU) Discovery from the overlay layer over any transport layer.

REQ#13: Overlay OAM MAY support fault localization of Loss of Continuity check at transport layer.

OOAM Passive PM vs. RFC 7799

Section 3.4 and Section 3.5 of RFC 7799 provide the definitions for Active and Passive modes of Performance Measurement (PM) methods. OOAM DT interpretation of what Passive PM is

> A measurement method that should not modify the actual data packet processing behavior on underlay and overlay network.

Accordingly, it should be supported by the Overlay nodes.

Security Considerations

OAM requirements for various Overlay encapsulations may have security implications. For example, if proactive Fault Management (FM) is required, the security implication is that a passive eavesdropper can know when the session is down. Or, proactive FM may be used either to launch DoS or to highjack session and impact state, e.g. cause protection switchover. These security implications are natural results of the requirements, and do not depend on the particular implementation. Whether existing security mechanisms of existing protocols proposed to be re-used in OAM for overlay networks are adequate or require enhancements is for further study. New OAM protocols for overlay networks must consider their security mechanism to on per-solution basis.

Overlay OAM: Gap Analysis

draft-ooamdt-rtgwg-oam-gap-analysis-02

Updated and Extended

- The encapsulation of an overlay network uses one of methods discussed in draft-ietf-rtgwg-dt-encap to distinctly identify the payload as OAM, i.e. non-user, packet
- All Overlay OAM protocols share the common Overlay OAM Header

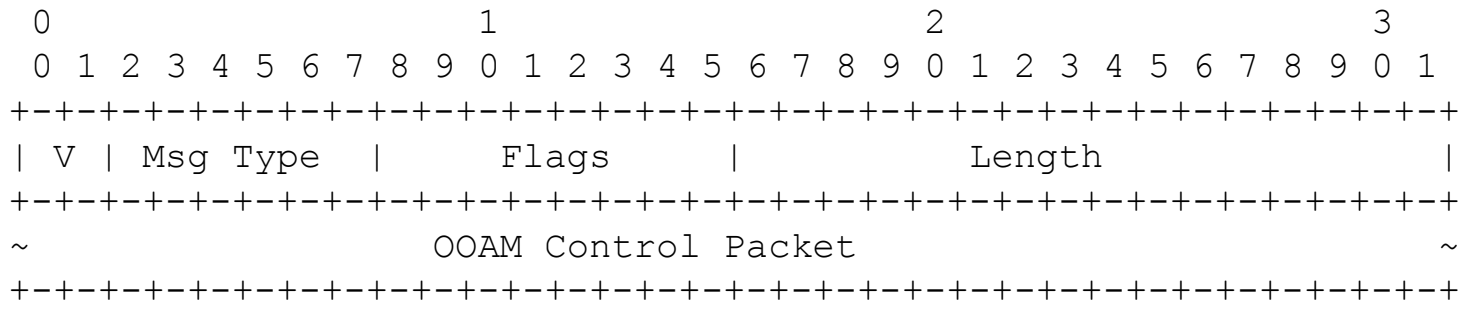
Performance Measurement OAM

- Active:
  - Loss and Delay Measurement in MPLS networks, RFC 6374
  - One/Two-way Active Performance Measurement Protocol(s), RFC 4656/RFC 5357
- Passive:
  - Alternate Marking Method
- Conclusions:
  - RFC 6374 can be used as foundation of active PM OAM in overlay networks. The YANG data model of the packet loss and delay measurement based on RFC 6374 can improve control and increase operational value of active performance measurement in overlay networks.
  - Alternate Marking Method being proposed as Passive OAM in BIER and can be used in NVO3 and SFC, given supported by overlay network encapsulation

OAM Header for use in Overlay Networks

draft-ooamdt-rtgwg-ooam-header-00

Overlay OAM Header

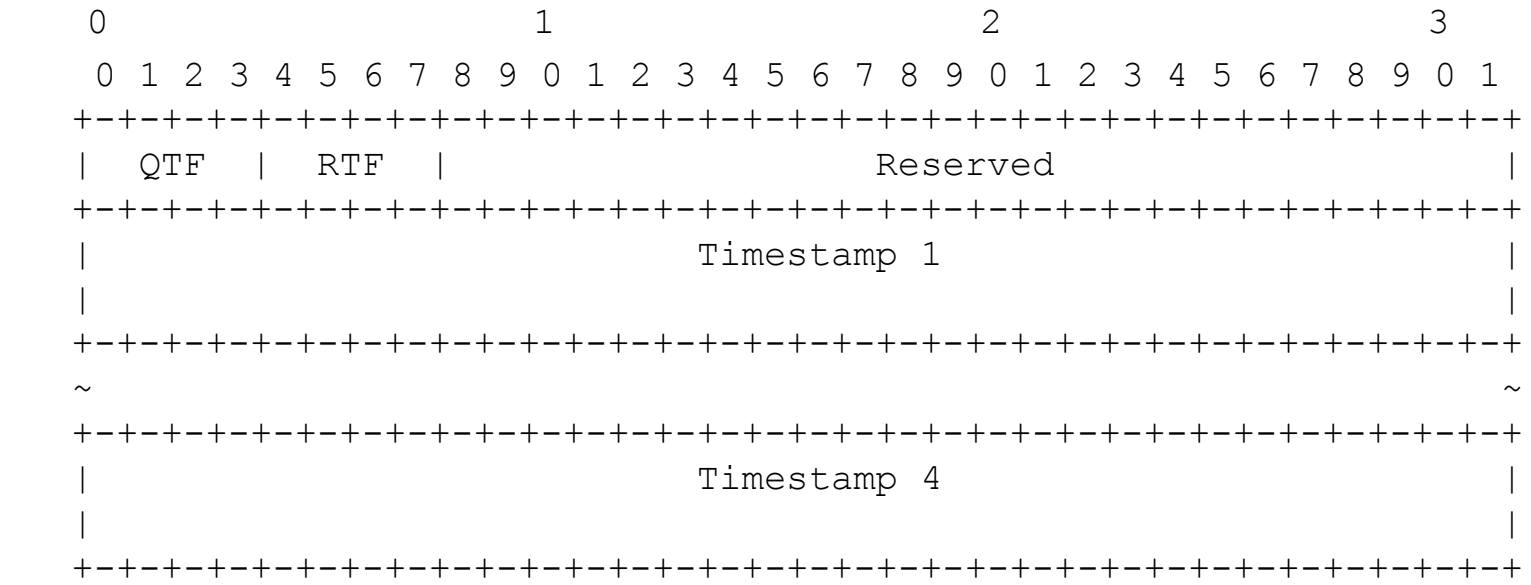


where:

- V - two bits long field indicates the current version of the Overlay OAM Header. The current value is 0
- Msg Type - six bits long field identifies OAM protocol, e.g. Ping or BFD
- Flags - eight bits long field carries bit flags that define optional capability and thus processing of the OOAM control packet, e.g. optional timestamping
- Length - two octets long field that is length of the OOAM control packet in octets

Timestamp

The idea comes from work on Residence Time Measurement, interest in measuring Delay and Delay Variation in addition to other Active OAM measurements



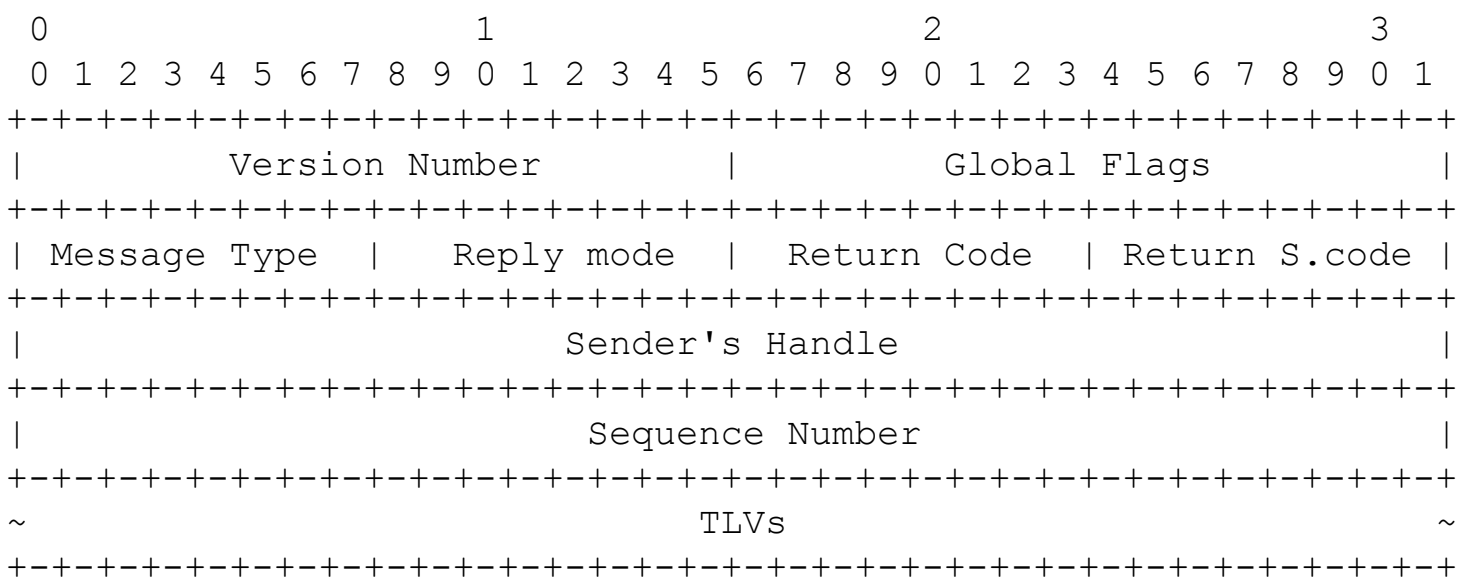
where:

- QTF - Querier timestamp format, e.g. NTP or IEEE-1588v2
- RTF - Responder timestamp format
- Timestamp 1-4 - 64-bit timestamp values

On-demand CC/CV for Overlay Networks

draft-ooamdt-rtgwg-demand-cc-cv-00

Overlay OAM Ping format



Overlay OAM Ping format (cont.)

Where:

- the Version reflects the current version
- the Global Flags is a bit vector field
- The Message Type filed reflects the type of the packet. Value TBA2 identifies Echo Request and TBA3 - Echo Reply
- the Reply Mode defines the type of the return path requested by the Sender of the Echo Request
- Return Codes and Subcodes can be used to inform the sender about result of processing its request
- the Sender's Handle is filled in by the sender, and returned unchanged by the receiver in the echo reply
- The Sequence Number is assigned by the sender and can be, for example, used to detect missed replies
- TLVs (Type-Length-Value tuples) have the two octets long Type field, two octets long Length field that is length of the Value field in octets

To be addressed

- Sender ID to be used for out-of-band, i.e. IP network, Echo Reply
- Source MEP ID (OOAM Domain ID + MEP ID) for Connectivity Verification
- Specification of Return Path Control Channel
- and more …

Conclusion

- We need your review and comments!