OAM in Overlay Networks:
OAM Header
Echo Request and Echo Reply

draft-ooamdt-rtgwg-ooam-header-03
draft-ooamdt-rtgwg-demand-cc-cv-03

Greg Mirsky
Nagendra Kumar
Deepak Kumar

Mach Chen
Yizhou Li
David Dolson

IETF-98. March, 2017

Objective

The draft-ooamdt-rtgwg-ooam-header introduces Overlay Operations, Administration, and Maintenance (OOAM) Header to be used in overlay networks. OOAM Header creates Overlay Associated Channel (OAC) to ensure that OOAM control packets are in-band with user traffic and de-multiplex OOAM protocols.

Overlay Associated Channel

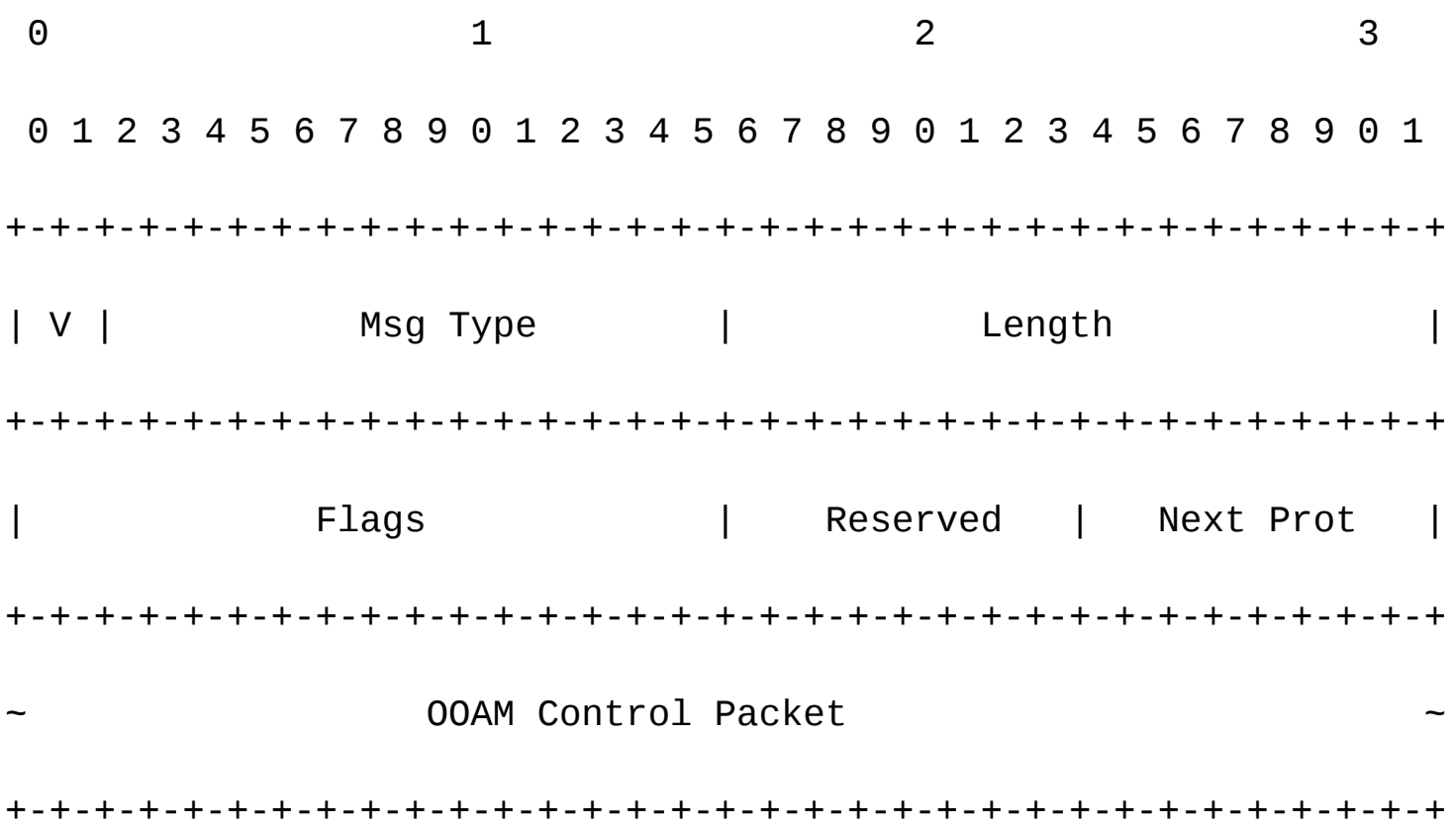
Associated Channel (OAC) in the overlay network is the channel that is in-band with user traffic through:

- using the same encapsulation as user traffic;
- following the same path through the underlay network as user traffic.

Creating notion of the OAC in the overlay network ensures that packets of active OAM protocols carried in the OAC are in-band with user traffic. Additionally, OAC allows development of OAM tools that, from operational point of view, function in essentially the same manner in any type of overlay.

Overlay OAM Header

Header format:

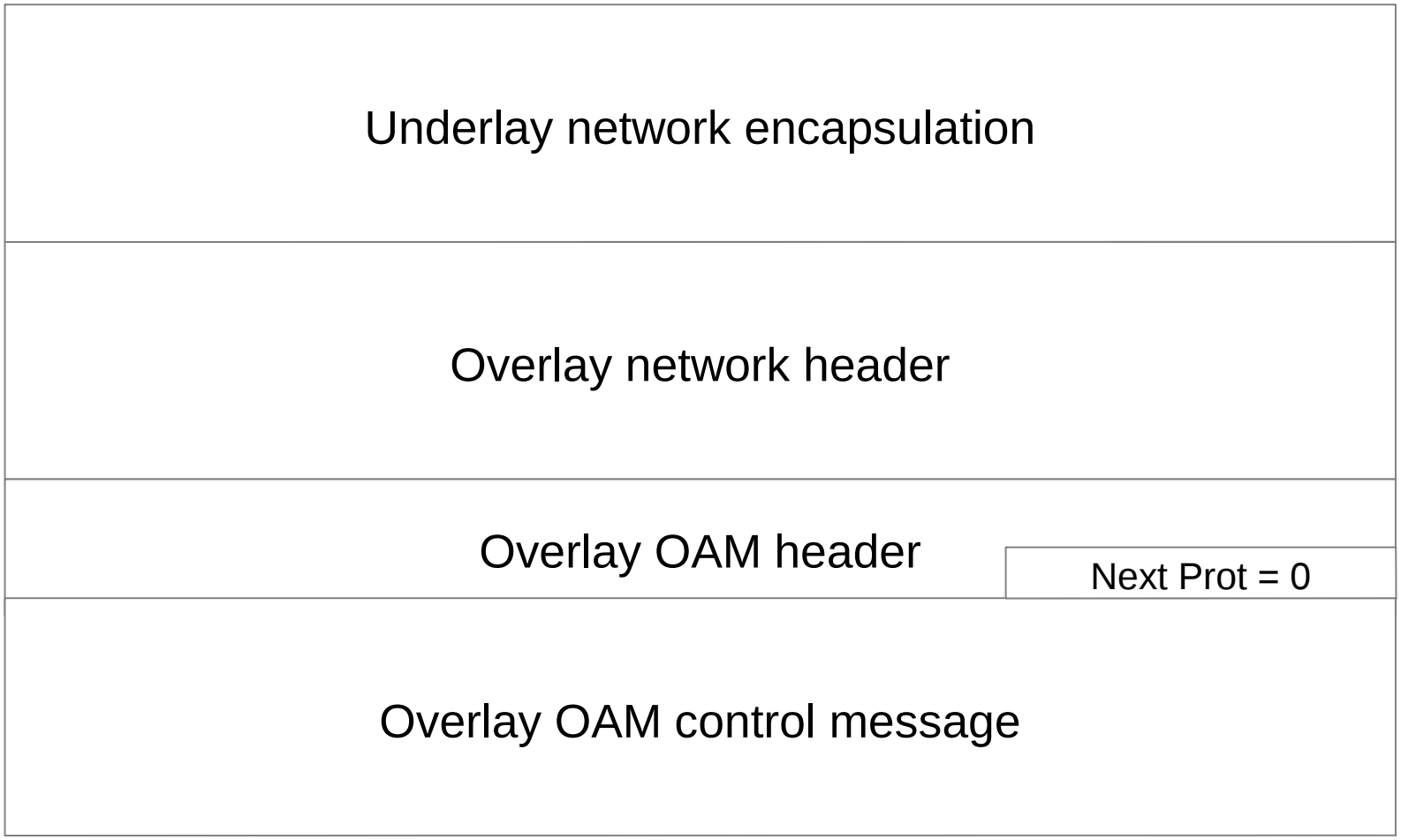


Requirements toward overlay encapsulation

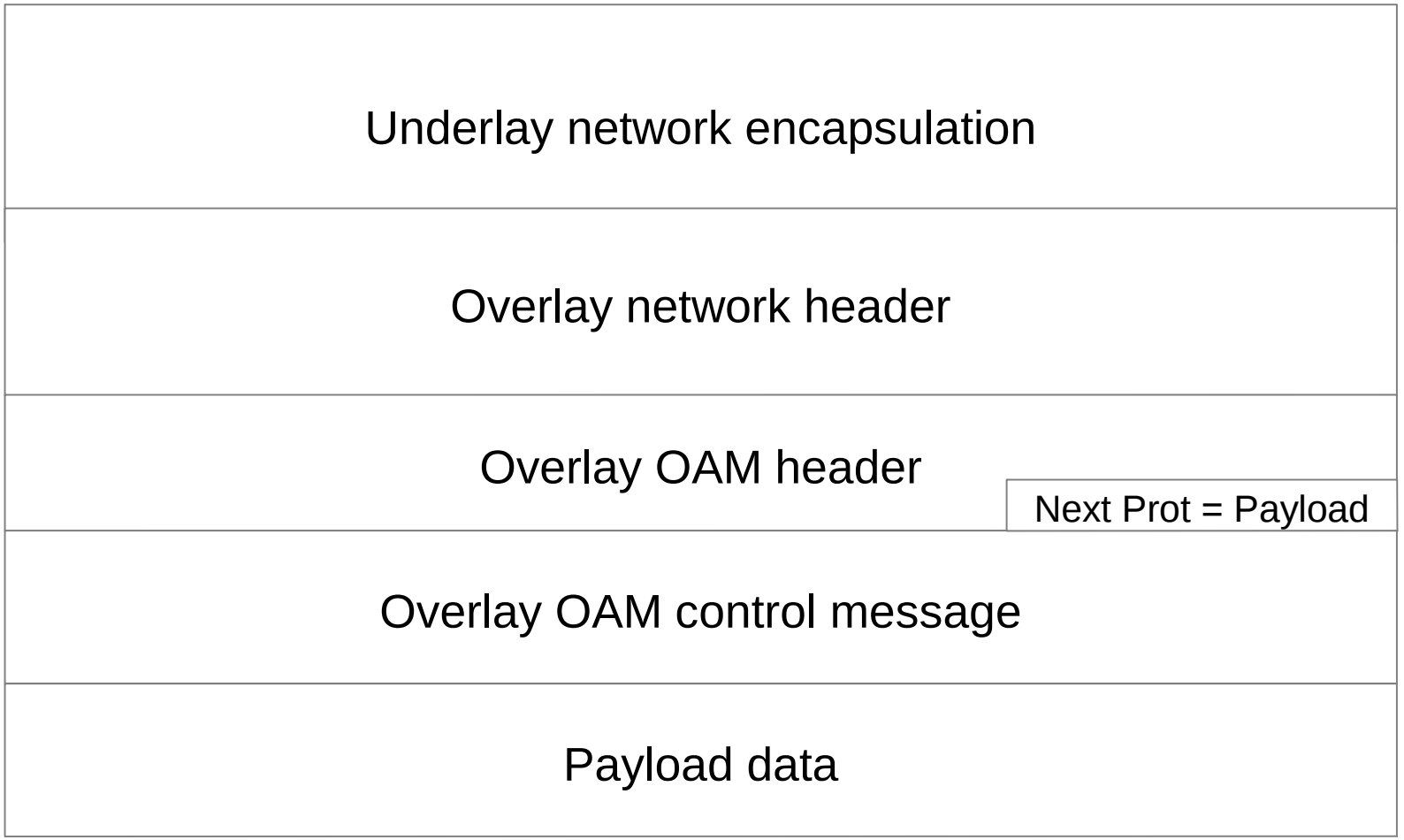
To ensure that active OAM control packets are in-band with the monitored data flow encapsulation layer MUST comply with the following requirements:

- encapsulation of OAM control message and data packets in underlay network MUST be indistinguishable from underlay network forwarding point of view;
- presence of OAM control message in overlay packet MUST be unambiguously identifiable;
- it MUST be possible to express entropy for underlay ECMP in overlay encapsulation in order to avoid using data packet content by underlay transient nodes.

Active OAM control packet encapsulation



Hybrid OAM control packet encapsulation



Recap

- Terminology:
  - switched from ping to “Echo Request” and “Echo Reply”
- Overlay Echo Request Transmission:
  - MUST use the appropriate encapsulation of the monitored overlay network;
  - Overlay network's header MUST be immediately followed by the Overlay OAM Header;
  - Message Type field in the Overlay OAM Header MUST be set to Overlay Echo Request value

Security Considerations

- Overlay EchoRequest/Replay operates within the domain of the overlay network and thus inherits any security considerations that apply to the use of that overlay technology and, consequently, underlay data plane.
- Possible approaches of attacking an overlay node using Overlay Echo Request/Reply:
  - send Overlay Echo Requests to overload the node, i.e. DoS;
  - tampering with Echo Request/Reply to misrepresent state of the overlay network;
  - unauthorized use of Echo Request/Reply to obtain information about overlay/underlay network.
- To mitigate risks:
  - throttle control packets to the control plane;
  - use Sendler’s Handle, Sequence Number and, possible, Timestamp block;
  - source address validation

Traceroute in Overlay

- What is traceroute in an Overlay Network?
- Does any overlay have TTL?
  - NSH introduced TTL in the latest update
- Or is traceroute expected to trace the underlay?

Next steps

- Welcome comments from the WG
- Asking WG to consider adoption of the drafts
- Thank you