Integrated OAM

draft-mmm-rtgwg-integrated-oam

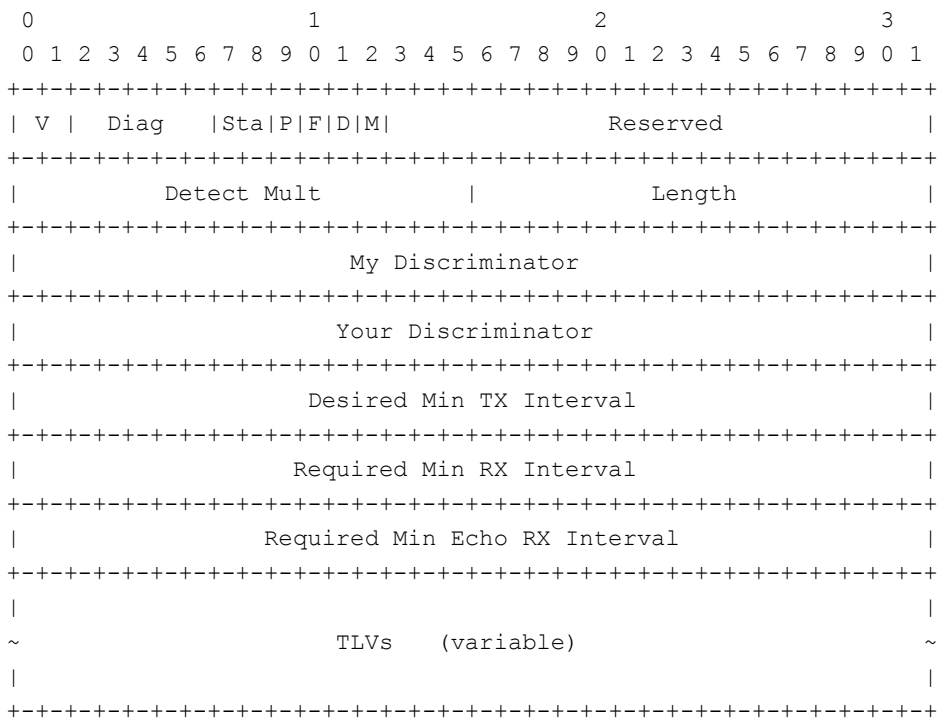
Greg Mirsky
Xiao Min
Gyan Mishra

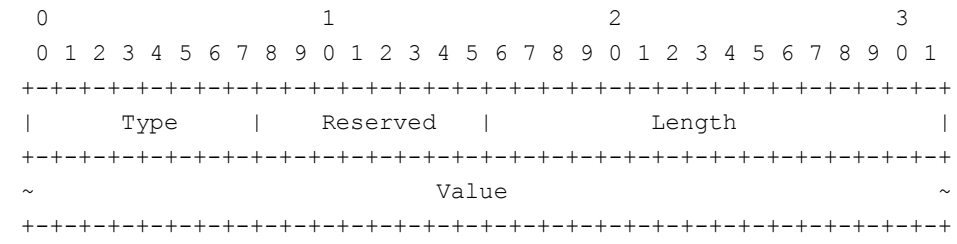
IETF-110 March 2021, Prague (virtual)

Motivation

- Lessons learned from BFD:
  - security is important but securing every test packet at 3.3 ms is way too expensive
  - protocol extensibility to extend its functionality
  - minimize the number of OAM protocols required to operate a network
- Lessons learned from an active PM OAM:
  - it is more about one-way measurement ,although the two-way is important
  - flexibility to measure packet loss and delay separately and in combination
  - security
  - extensibility
- Integrated OAM:
  - lightweight path continuity check
  - powerful and flexible performance monitoring
  - security
  - extensibility

Integrated OAM Control Message Format





Control Message:

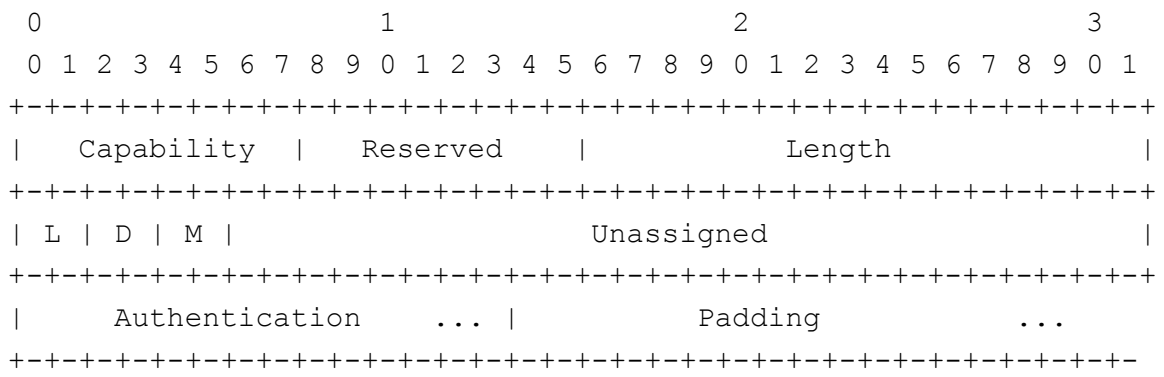
- Version
- Reserved
- Diagnostic
- Status
- Poll
- Final
- Demand
- Multicast
- Detect Multiplier
- Length
- My Discriminator
- Your Discriminator
- Desired Min TX Interval
- Required Min RX Interval
- Required Min Echo RX Interval

TLV:

- Type
- Reserved
- Length
- Value

Capability Negotiation

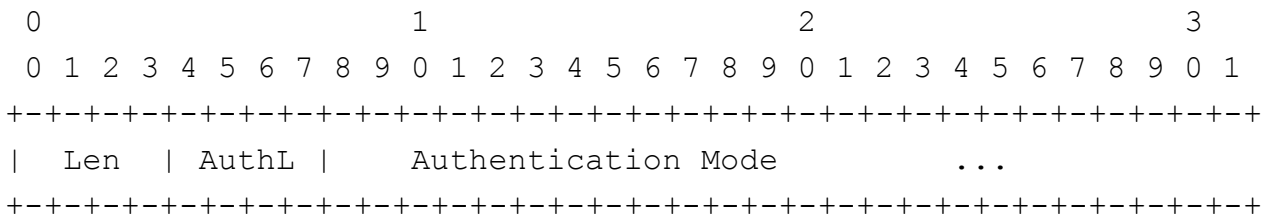
- Capability negotiation using the Poll sequence and the Capability TLV



L – Loss measurement, bit flags Periodic and Poll
D – Delay measurement, bit flags Periodic and Poll
M – Path MTU discovery/monitoring
A – Lightweight Authentication, variable length field

- Timer negotiation mechanism can be used separately for the loss and delay measurement using Desired Min TX Interval and Required Min RX Interval values in the Integrated OAM control message

Authentication Capability

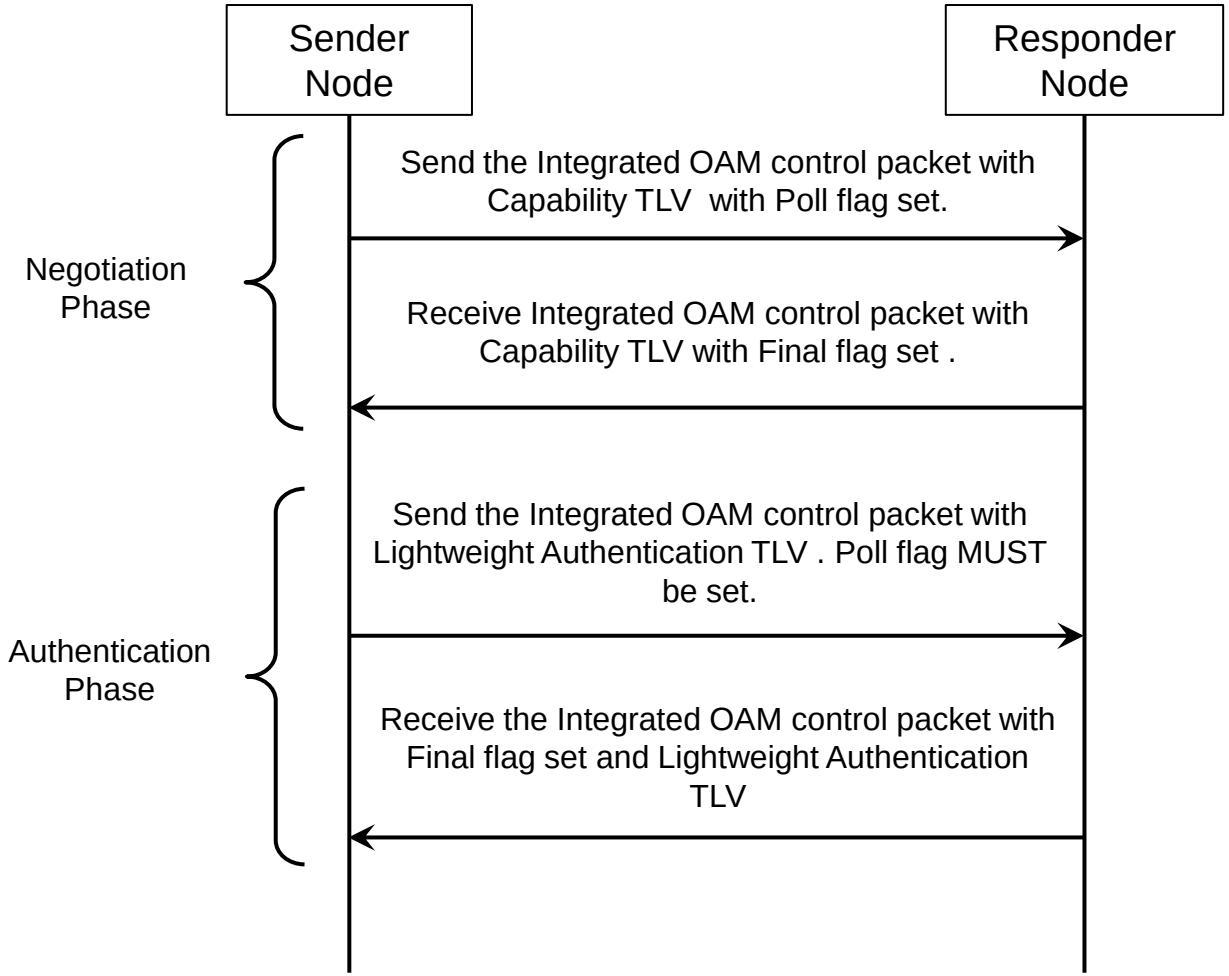


- Len (Length) - four-bits long field. The value of the Length field is equal to the length of the Authentication field, including the Length, in octets.
- AuthL (Authentication Length) – four bits size field. The value of the field is, in four octets long words, the longest authentication signature the Integrated OAM system is capable of supporting for any of the methods advertised in the Authentication Mo de field. In other words, the longest digest – 60 octets.
- Authentication Mode - variable-length field. It is a bit-coded field that an Integrated O OAM system uses to list modes of lightweight authentication it supports.

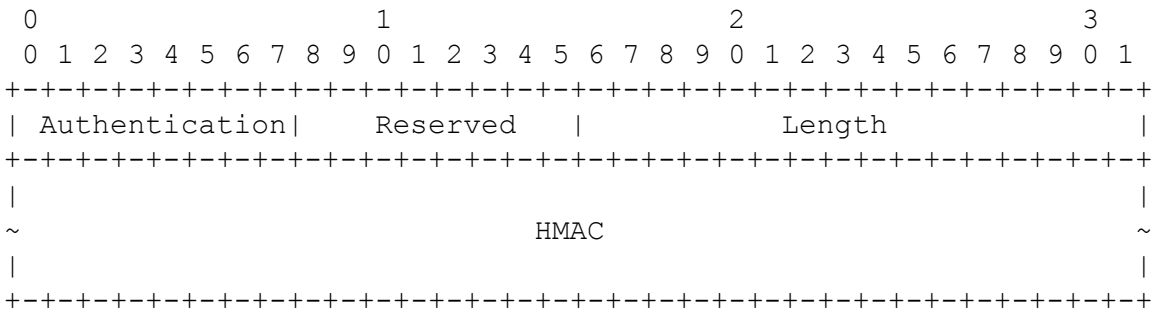
Bit Position	Value	Description	Reference	
0	0x1	Keyed SHA-1	This document	- BFD legacy
1	0x2	Meticulous Keyed SHA-1	This document	- BFD legacy
2	0x4	SHA-256	This document	

Lightweight Authentication

Lightweight Authentication is on-demand authentication of an Integrated OAM session using the Poll sequence mechanism



Lightweight Authentication



Type - allocated by IANA
Reserved – zeroed on the transmission and ignored on receipt (explicitly identify the authentication mode and the length?)
Length - two octets long field equals length on the HMAC (Hashed Message Authentication Code) field in octets. The value of the Length field MUST be a multiple of 4.
HMAC (Hashed Message Authentication Code) - the hash value calculated on the preceding Integrated OAM control packet data.

Performance Monitoring in the Integrated OAM

- Use RFC 6374 constructs
- Packet Loss
  - synthetic one-way
  - synthetic two-way
  - direct loss measurement
- Packet Delay
  - one-way
  - two-way
- Addition:
  - Packet MTU discovery

Next Steps

- Continue adding details (PMTU Monitoring operation)
- Discuss, discuss, discuss
- Welcome comments, suggestions, and cooperation
- WG adoption?

Thank you