Extended BFD

draft-mirmin-bfd-extended

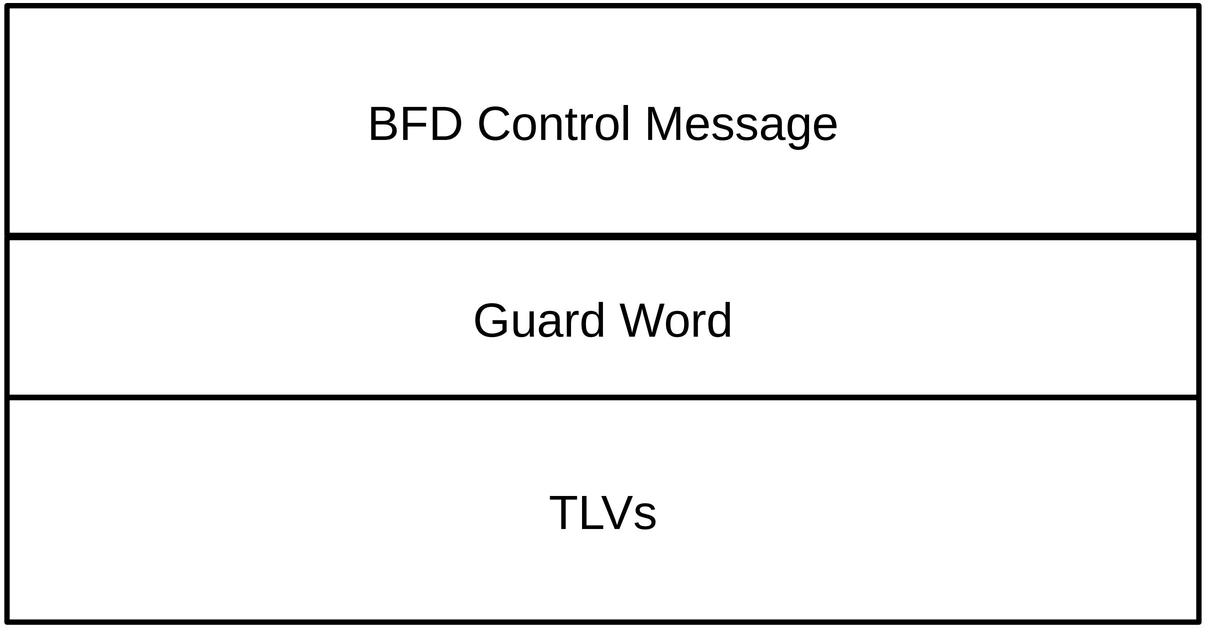
Greg Mirsky
Xiao Min

IETF-105 July 2019, Montreal

Motivation

- Observed proposals to monitor:
  - quality of a BFD session;
  - performance;
  - path MTU
- Extend BFD beyond continuity checking/connectivity verification to:
  - ensure backward compatibility;
  - Extensibility
- Intermittent authentication for a BFD session

Extended BFD Control Message Format



BFD Control Message

Guard Word

TLVs

- BFD Control Message as defined in RFC 5880
- Guard Word – unique four octets long word to identify Sender and Responder
- TLVs – optional
- Use Length field in UDP header to detect if a BFD packet includes a TLV, i.e, is an Extended BFD packet

Capability Negotiation

- No Extended BFD by default
- Capability negotiation using the Poll sequence and the Capability TLV

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

L	D	M	A	Reserved

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

- If LM or DM are proposed in the Periodic mode, e.g., Asynchronous, the standard timer negotiation procedures, as defined in RFC 5880, may be used by the remote BFD system

Authentication Capability

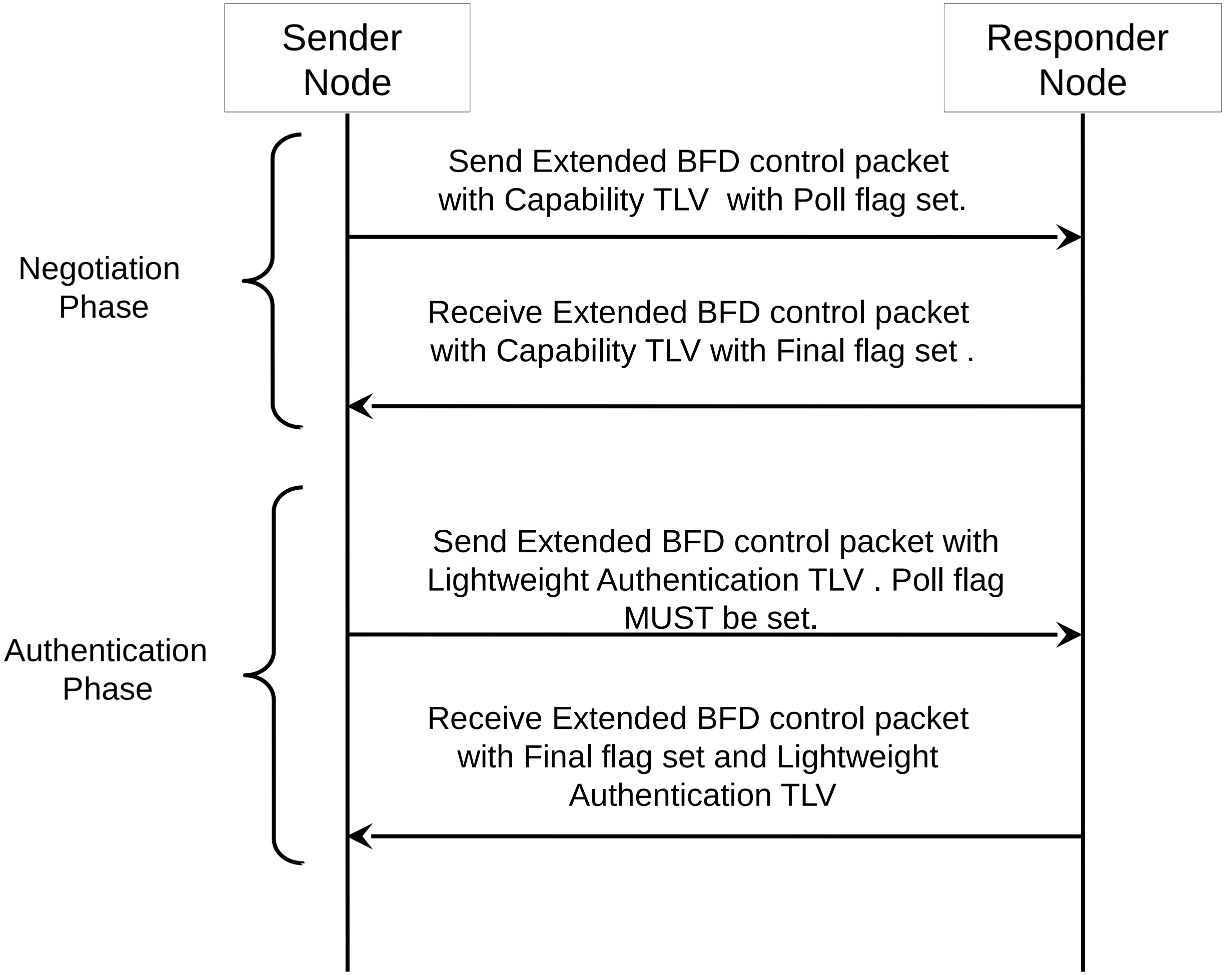
```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Len  | AuthL |    Authentication Mode         ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- 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 BFD system is capable of supporting for any of the methods advertised in the Authentication Mode field.
- Authentication Mode - variable-length field. It is a bit-coded field that a BFD system uses to list modes of lightweight authentication it supports.

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

Lightweight Authentication

Lightweight Authentication is on-demand authentication of a BFD session using the Poll sequence mechanism



Sender Node

Responder Node

Negotiation Phase

Send Extended BFD control packet with Capability TLV with Poll flag set.

Receive Extended BFD control packet with Capability TLV with Final flag set .

Authentication Phase

Send Extended BFD control packet with Lightweight Authentication TLV . Poll flag MUST be set.

Receive Extended BFD control packet with Final flag set and Lightweight Authentication TLV

Lightweight Authentication

Type = Lightweight Authentication	Length
HMAC = Variable number of four octets-long words	

Type - allocated by IANA
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 Extended BFD control packet data.

Value	Description	Reference
0	None	This document
1	One or more TLVs was not understood	This document
2	Lightweight Authentication failed	This document

Next Steps

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