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 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

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

<table>
<thead>
<tr>
<th>Bit Position</th>
<th>Value</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0x1</td>
<td>Keyed SHA-1</td>
<td>This document</td>
</tr>
<tr>
<td>1</td>
<td>0x2</td>
<td>Meticulous Keyed SHA-1</td>
<td>This document</td>
</tr>
<tr>
<td>2</td>
<td>0x4</td>
<td>SHA-256</td>
<td>This document</td>
</tr>
</tbody>
</table>
Lightweight Authentication

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

**Negotiation Phase**
- Sender Node: Send Extended BFD control packet with Capability TLV with Poll flag set.
- Responder Node: Receive Extended BFD control packet with Capability TLV with Final flag set.

**Authentication Phase**
- Sender Node: Send Extended BFD control packet with Lightweight Authentication TLV. Poll flag MUST be set.
- Responder Node: Receive Extended BFD control packet with Final flag set and Lightweight Authentication TLV.
# Lightweight Authentication

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.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>None</td>
<td>This document</td>
</tr>
<tr>
<td>1</td>
<td>One or more TLVs was not understood</td>
<td>This document</td>
</tr>
<tr>
<td>2</td>
<td>Lightweight Authentication failed</td>
<td>This document</td>
</tr>
</tbody>
</table>
Next Steps

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