Optimizing BFD Authentication

draft-mahesh-bfd-authentication-02

Mahesh Jethanandani, Ashesh Mishra
Manav Bhatia, Ankur Saxena

BFD Authentication

Problem

- Computationally intensive process
- Limits scale and stability
- Soon, MD5 and SHA1 will no longer be adequately secure

Solution

- Authenticate a sub-set of BFD frames
- Authenticate all state-changes
- Authenticate few BFD CC-UP frames periodically

Benefits

- Authenticating a smaller set of frames reduces the computational stress on the system

- Stronger hashing algorithms can be used in BFD authentication without significant performance degradation

Changes from v00 to v02

- Authentication map

Column = From Row = To	DOWN	INIT	UP	Poll	Demand
DOWN	NULL Auth	Auth	n/a	n/a	Auth
INIT	Auth	NULL Auth	Auth	Auth	Auth
UP	Auth	n/a	Null Auth with periodic Auth	Auth	Auth
Poll	Auth	n/a	Auth	Auth	Auth
Demand	Auth	Auth	Auth	Auth	Auth

Most frames are UP-to-UP

Changes from v00 to v02

- Use NULL-Auth TLV in all un-authenticated frames
  - Compatible with BFD-Stability draft
  - Maintains sequence numbers to prevent replay attacks

```
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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            TLV Type           |            TLV Len            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Sequence Number                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Sender Timestamp                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Questions / Comments /Adopt ?

Mahesh Jethanandani (mjethanandani@gmail.com)

Ashesh Mishra (mishra.ashesh@outlook.com)

Manav Bhatia (manav@ionosnetworks.com)

Ankur Saxena (ankurpsaxena@gmail.com)