Optimizing BFD Authentication

draft-mahesh-bfd-authentication-00

Mahesh Jethanandani, Ashesh Mishra
Manav Bhatia, Ankur Saxena

Problem

- Authentication is computationally intensive process
- Limits scale and stability of BFD sessions
- Soon, MD5 and SHA1 will no longer be adequately secure

Solution

- Authenticate only a small subset of BFD frames
  - All frames that are intended for triggering a change in the BFD session
    - Down, Admin_Down, Init, P-F sequence
  - Periodic BFD frames when the session state is UP
    - Once frame every 10 seconds?

Benefits

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

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

Open Issues

- There is a small window for man-in-the-middle attack between two authenticated BFD frames when the session is in state UP.
  - The rate of BFD-UP frame authentication can be increased (up to the negotiated Tx interval) to minimize such window (or eliminate it by authenticating every frame). Not a solution we prefer because of the performance degradation.

Open Issues

- Requires change in the BFD frame handling logic.
  - Simple change in software-only BFD implementations
  - May be complex to implement in certain hardware engines (particularly when using 3rd party ASICs)
  - Simple change in hybrid implementations where only frame Tx/Rx is hardware accelerated.

Open Issues

- Method for negotiating “optimized BFD authentication” capability between BFD peers requires further discussion.
  - Using the Auth-bit may not be adequate if some frames have the bit set and the others do not.

Open Issues

- System is open to DoS attacks if attacker injects auth frames.
  - Rate-limiting auth frames is an option (no more than 2-3 auth frames per-session per-second are expected)
  - Other ideas?

Open Issues

- When many sessions change state from UP to DOWN around the same time, the auth system load will be large
  - No larger than the load expected in full auth methods
  - Session establishment can be rate-limited to prevent clogging the CPU

Open Issues

- Why not cache the last well-known auth frame and compare new auth frames with the cached copy?
  - Can’t use sequence numbers in auth-tlv
  - Not a major security upgrade over the proposed method

Questions / Comments ?

mjethanandani@gmail.com

mishra.ashesh@outlook.com

manav@ionosnetworks.com

Saxena (ankurpsaxena@gmail.com