TRILL over IP

draft-ietf-trill-over-ip-01.txt

M. Wasserman
D. Eastlake
D. Zhang

IETF90 Toronto

Changes from -00

- Updated the reference list
- Added discussions of
  - Use of DTLS
  - Using IP Multicast

Use of DTLS (1)

- All RBridges that support TRILL over IP MUST implement DTLS and support the use of DTLS to secure both TRILL IS-IS and TRILL data packets.
- When there is IS-IS security provided, people may select to use IS-IS security to protect the IS-IS PDUs.
- If RBridges support certificates, they MUST support :
  - TLS_RSA_WITH_AES_128_CBC_SHA256
- If RBridges support pre-shared keys, they MUST support:
  - TLS_PSK_WITH_AES_128_CBC_SHA256

Use of DTLS (2)

- When IS-IS security [RFC5310] is deployed, there could be multiple keys identified with 16-bit key IDs. In this case, the Key ID of IS-IS-shared key is also used to identify the default derived keys used by DTLS.

Using IP Mulicast (1)

- Advantages of using an IP link that supports default multicast
  - Automatic discovery with zero or minimum configuration when an RBridge IP port come up.
  - More efficient link use for multi-destination traffic. (Unicast TRILL data packets still sent over unicast IP.)
  - Note: TRILL is already designed to support links with more than two RBridge ports attached.

Using IP Multicast (2)

- Disadvantages of trying to use multicast on an IP link
  - Multicast may not be available.
  - Unicast is typically more reliable. (This would only affect multi-destination TRILL data packets.)
  - Pairwise communications simplifies key management.

Using IP Mulicast (2)

- Changes from -00
  - When using IP multicast
    - IGMP or MLD packets need to be periodically transmitted so that the TRILL multicast IP traffic will be sent to the RBridge port.
  - When IP multicast is not supported
    - a TRILL over IP port may be configured to use serial unicast with a list of one or more unicast IP addresses of other TRILL over IP ports to which multi-destination packets are sent.

END