Group Keying

draft-ietf-trill-over-ip-05.txt
draft-ietf-trill-channel-tunnel-08.txt

IETF 95, Buenos Aires
Margaret Cullen margaret@painless-security.com
Mingui Zhang, Donald Eastlake, Dacheng Zhang.
Two Drafts

• The “TRILL over IP” draft treats an IP network as a link connecting TRILL switch ports, thus providing a method to connected TRILL sites into a single TRILL campus over IP.
  – Specifies encapsulation, security, and transport considerations including congestion, MTU, fat flows, QoS, middleboxes, and more.

• The “Channel Tunnel” draft extends the RBridge Channel [RFC 7178] facility for sending typed messages between RBridges by adding security.
Group Keying Need

• Both of these drafts cover multi-destination packets and may need encrypted & authenticated group transmission. This can be done in two ways:
  – Serial Unicast: Just use point-to-point security.
  – Group Keying and Multi-destination transmission.
  • TRILL over IP: This would apply if native IP multicast is supported on the IP link/network.
  • Channel Tunnel: Applies to group transmissions on the virtual link connecting all Rbridges that have expressed interest in a Data Label (VLAN or Fine-Grained Label).
Group Keying Problem

• There does not seem to be a good general specification for how to do group keying. This was delaying both drafts
  – draft-ietf-trill-channel-tunnel-08.txt is in Publication Requested state
  – draft-ietf-trill-over-ip-05.txt is a WG Draft
Group Keying Solution

• Three steps:

  1. For draft-ietf-trill-channel-tunnel, group transmission and keying removed. Draft says they will be covered in a separate draft. – Raised on mailing list without objection, Completed.

  2. Create draft-ietf-trill-group-keying that (a) specifies a generic group keying method and (b) provides a profile of that method for channel-tunnel. – Was not completed before IETF.

  3. Reference and use this “Group Keying” draft in “TRILL over IP”. – Was not completed before IETF.
Group Keying Solution

- draft-ietf-trill-channel-tunnel
  - Group Keying and transmission
  - Publication Requested

- draft-ietf-trill-group-keying
  - Generic Group Keying
  - New Draft

- draft-ietf-trill-over-ip
  - Group Keying and transmission
  - Reference

- WG Draft

- Move

- Reference
Next Steps

• Draft-ietf-trill-channel-tunnel can proceed normally

• Finish and post draft-ietf-trill-group-keying-00
  – Estimate: within a few weeks after IETF

• Finish and post revisions of TRILL over IP
  – Estimate: within 5-6 week after IETF

• WG Last Call for Group Keying and TRILL over IP drafts
Feedback? Questions?
Back up Slides
Security

• TRILL over IP draft specifies IPsec ESP (Encapsulating Security Protocol) in Tunnel Mode.
  – Uses IKEv2 to derived pairwise keys.
  – Use of ESP Tunnel Mode supports use of IPsec appliances separate from the actual RBridge port hardware.

• Proposal for IP multicast security keying:
  – By default, TRILL links have a Designated RBridge (DRB) on the link.
  – The DRB sends a key to the RBridges on the link that it recognizes using established pair-wise security.
IPsec ESP in Tunnel Mode

Without security

With security

April 2016

TRILL Group Keying