TRILL over IP

draft-ietf-trill-over-ip-05.txt

IETF 94, Yokohama

Margaret Cullen margaret@painless-security.com
Mingui Zhang, Donald Eastlake, Dacheng Zhang.

Basic Summary

- “TRILL over IP” treats an IP network as a link connecting TRILL switch ports, thus providing a method to connected TRILL sites into a single TRILL campus.
- Two Scenarios are described in the draft
  - Remote Office Scenario
  - IP Backbone Scenario
- Specifies encapsulation, security, and transport considerations including congestion, MTU, fat flows, QoS, middleboxes, and more.

Changes from -04 to -05

1. Add use of IKEv2 for pairwise key agreement / management.
2. Addition of middlebox material.
   - There is some conflict between using IP source port for entropy to improve handling of fat flows and maintenance of flow state by NAT/NAPT boxes.
3. QoS material improved. (Maps internal TRILL packet priorities into DSCP code points.)

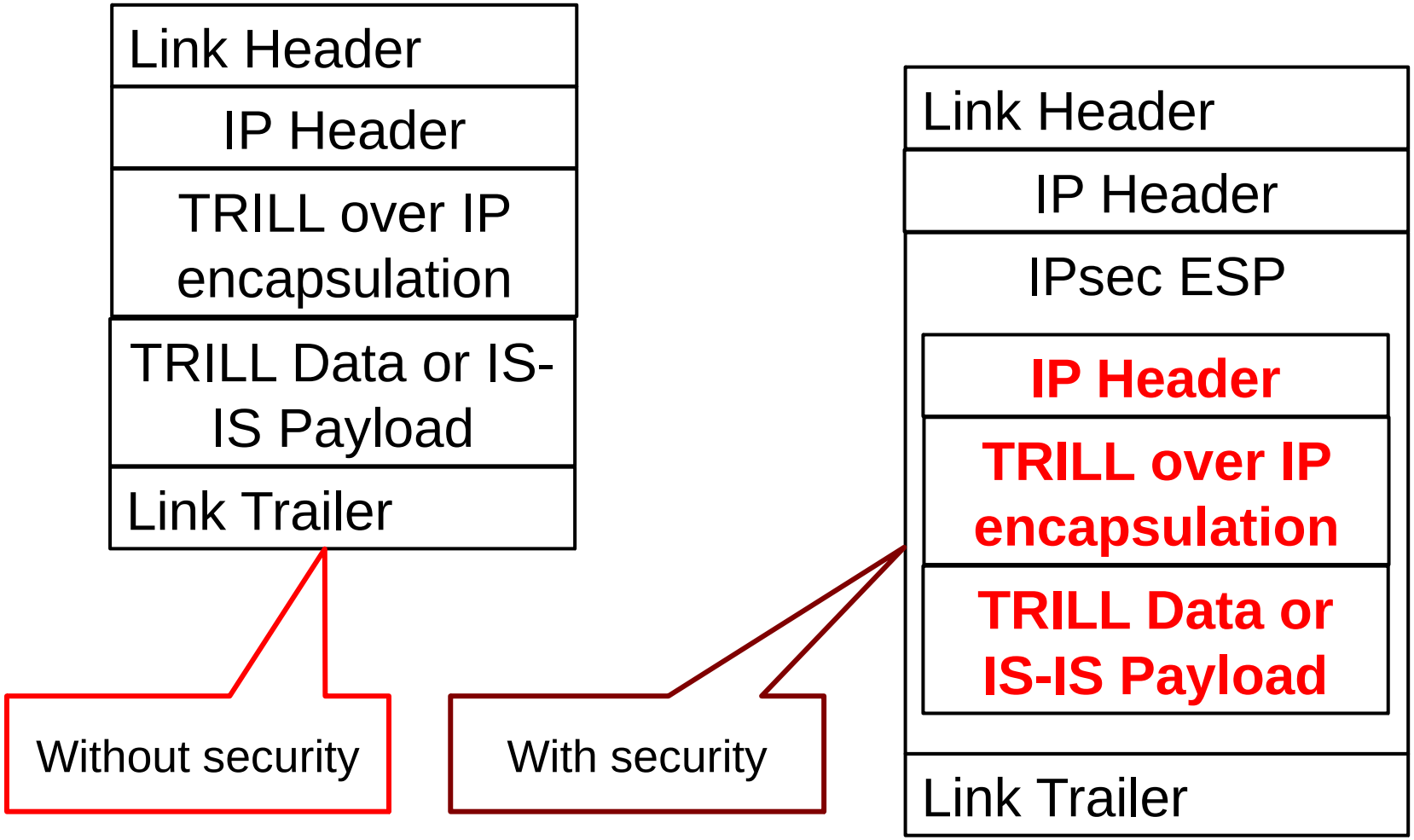
More Changes from -04 to -06

4. Encourage use of IPv6 to avoid fragment ID weaknesses of IPv4 unless the network is engineered so no IP fragmentation can happen.
6. Major re-organization of the draft sections / sub-sections to bring related material together and provide a more logical flow to the document.
   - Some expansion and re-writing without technical change for clarity.

Security

- 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 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



Work Remaining

- Work remaining includes:
  - Complete security section for multicast keying.
  - Complete material in TRILL IP Port configuration section, particularly as it relates to security configuration.

Feedback? Questions?