Group Keying and TRILL Over IP

draft-ietf-trill-over-ip-06.txt
draft-eastlake-trill-group-keying-00.txt

IETF 96, Berlin

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

Two Communication Protocols

- There are two drafts that need to provide data security.
  - RBridge Channel: draft-ietf-trill-rbridge-channel-10
    - Supports typed control messages between RBridges
    - Almost through IESG (In 2nd IETF LC due to downref)
  - TRILL over IP: draft-ietf-trill-over-ip-06
    - Supports IP as a link technology between RBridges
    - WG Draft
- Both can do point-to-point in a straight forward way using a modern security protocol including key negotiation. TRILL over IP uses IPsec.

Group Keying Need

- Both drafts would like to support multi-destination traffic but need a good group key distribution protocol.
  - TRILL over IP: This would only apply if native IP multicast is supported on the IP link/network.
  - Channel Tunnel: Applies to group transmissions of control messages on the virtual link connecting all RBridges that have expressed interest in a Data Label (VLAN or Fine-Grained Label).
- Currently would have to use serial multi-cast for multi-destination messages, which is inefficient.

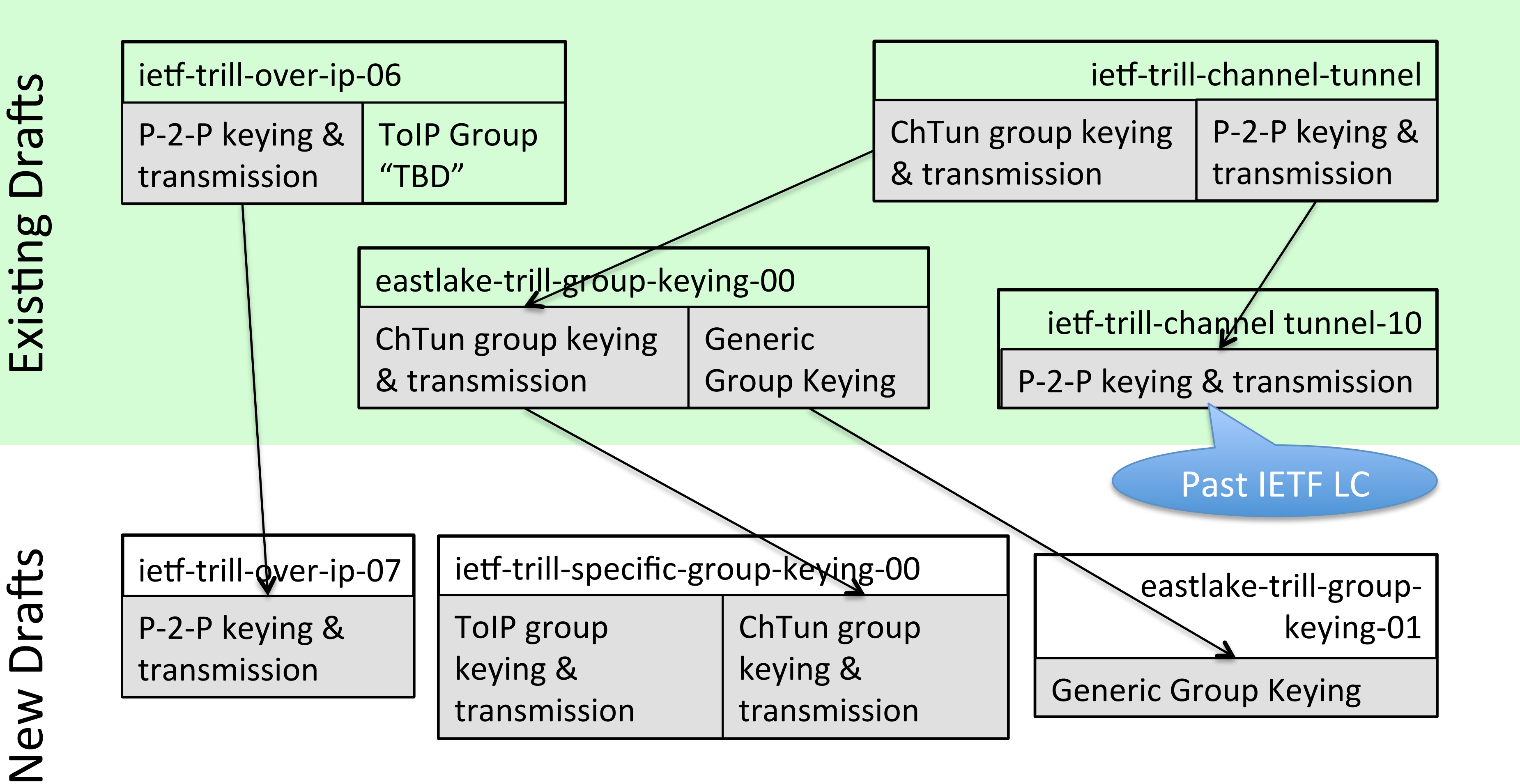
Group Keying Solution Technical

- A generic group keying protocol has been designed and is currently in draft-eastlake-trill-group keying-00.txt.
  - Securely distributes shared secret keys to the group members.
  - This provides keying for multicast/broadcast security but which group member originated a packet is not authenticated.
  - (If authentication of the source group member is required, use less efficient serial unicast.)

Group Keying Solution Process

- Three steps:
  1. Put through the two drafts with provision only for point-to-point saying true multi-destination will be covered elsewhere.
  2. Put through a generic group key distribution mechanism.
  3. Put through a draft covering specifics of how to use group keying in the two drafts along with the generic group keying draft.

Plan Going Forward



Existing Drafts

ietf-trill-over-ip-06

P-2-P keying & transmission

TolP Group “TBD”

ietf-trill-channel-tunnel

ChTun group keying & transmission

P-2-P keying & transmission

eastlake-trill-group-keying-00

ChTun group keying & transmission

Generic Group Keying

ietf-trill-channel tunnel-10

P-2-P keying & transmission

Past IETF LC

New Drafts

ietf-trill-over-ip-07

P-2-P keying & transmission

ietf-trill-specific-group-keying-00

TolP group keying & transmission

ChTun group keying & transmission

eastlake-trill-group-keying-01

Generic Group Keying

Next Steps

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

1. Revise/create new drafts as on previous page
   - Estimate, 4-5 weeks after IETF meeting
2. WG Last Call on TRILL over IP draft
3. WG Adoption of (generic) Group Keying draft

- Later: WG Last Call on (generic) group keying draft and specific group keying draft

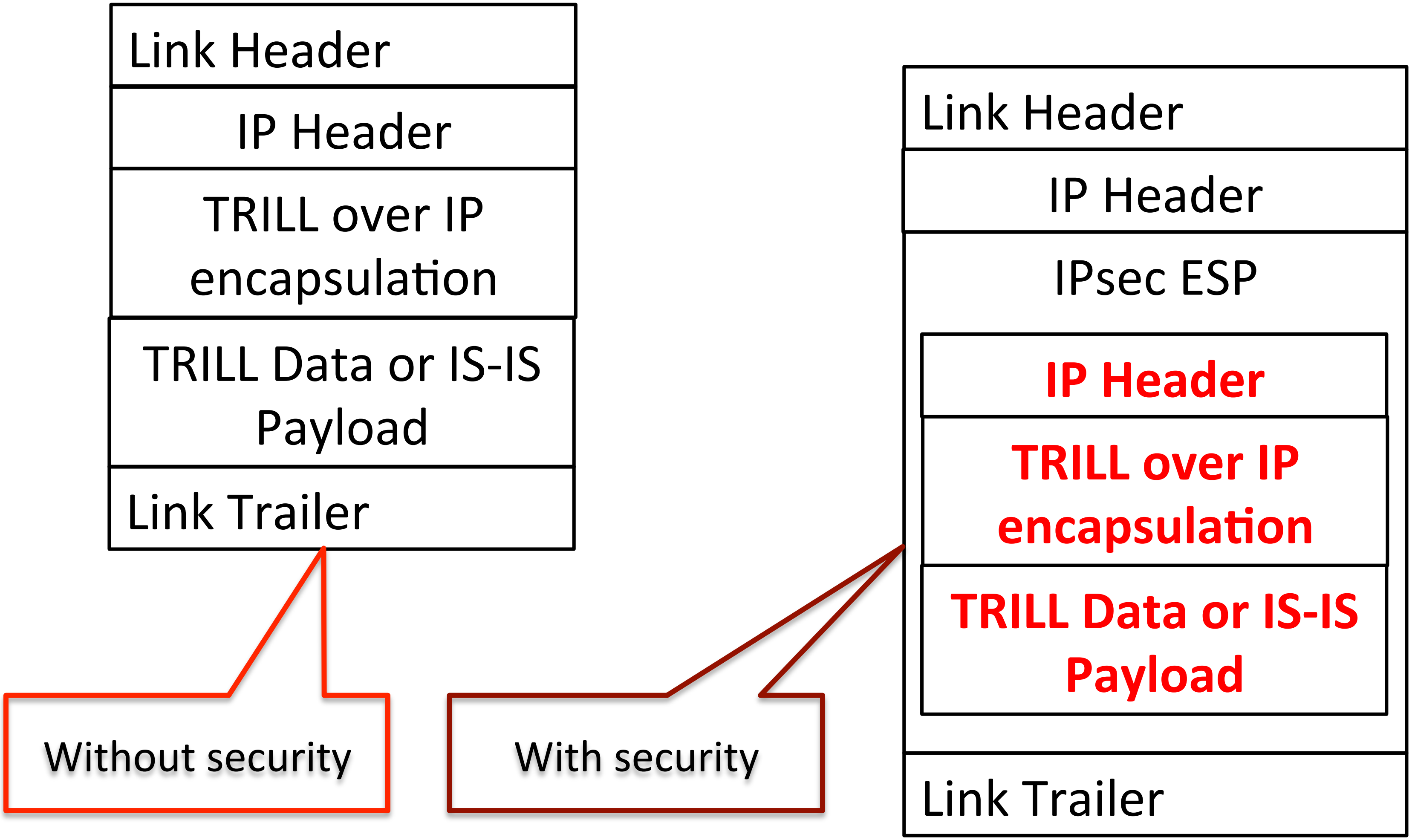
Feedback? Questions?

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.
- 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 as per the group key distribution protocol that has been designed.

IPsec ESP in Tunnel Mode



Link Header

IP Header

TRILL over IP encapsulation

TRILL Data or IS-IS Payload

Link Trailer

Without security

With security

Link Header

IP Header

IPsec ESP

IP Header

TRILL over IP encapsulation

TRILL Data or IS-IS Payload

Link Trailer