TRILL over IP

draft-ietf-trill-over-ip-03.txt

IETF 93, Prague

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

Document 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, and more.

Changes from -02 to -03

- Encapsulation: Important to use encapsulation with fast path support.
  - Hooks added for signaling support for and selecting encapsulation method.
  - Current draft supports simple UDP encapsulation and VXLAN encapsulation.
- QoS: Specify mapping of priority to DSCP code points.
- Specify mandatory to implement IPsec algorithms.

Encapsulation

- There are a number of factors that influence choice of TRILL over IP encapsulation. One size is unlikely to fit all.
  - Fast path support: For high speed applications, this is critical.
  - Ease of multi-pathing: Exposure of field(s) that can be used for multi-pathing internal to the IP path between TRILL switches.
  - Fragmentation and robust fragment ID.
  - Checksum strength: May be important depending on circumstances. (Integrity check can be provided by IPsec.)

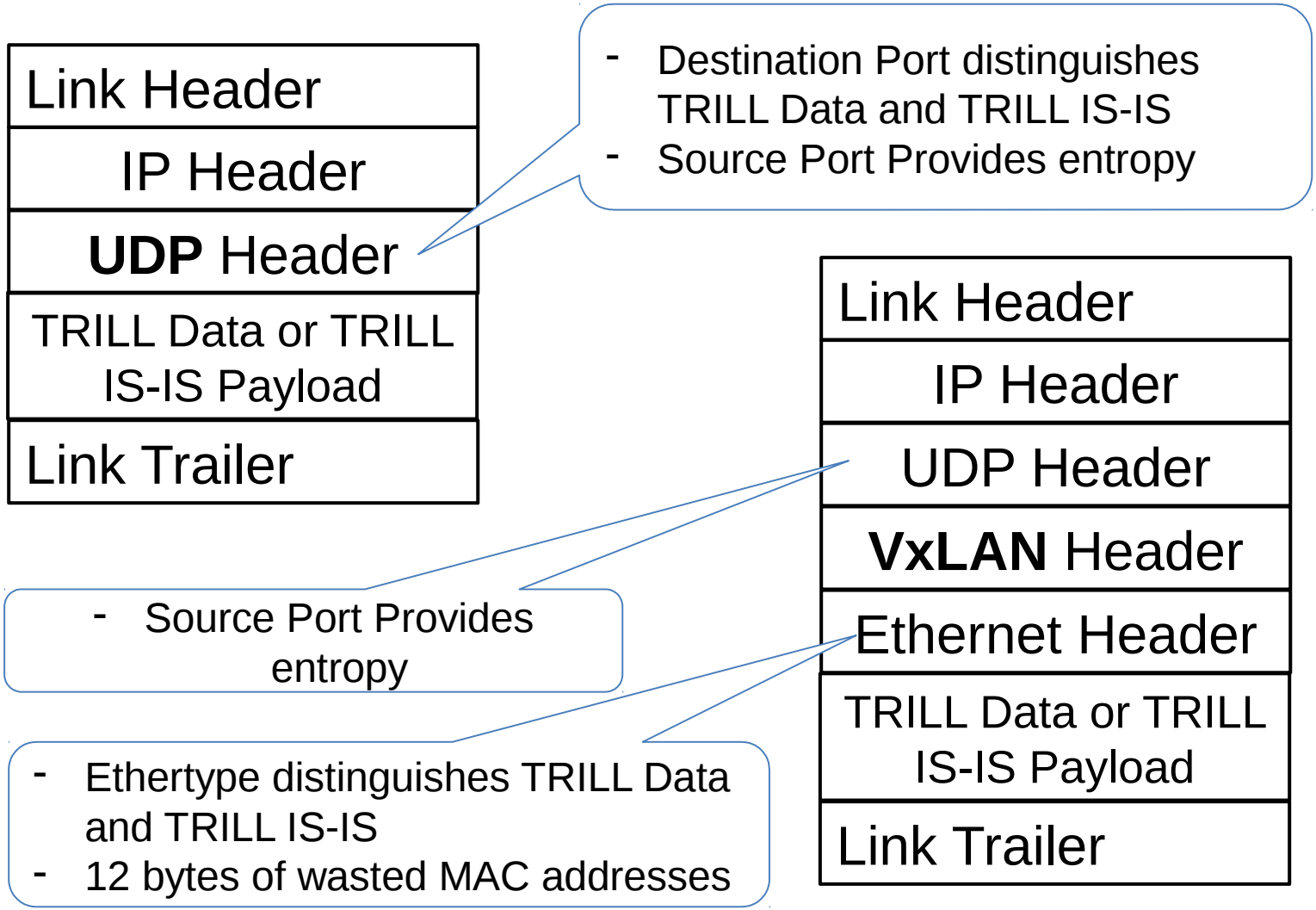
Encapsulation

- Simple UDP encapsulation MUST be implemented.
- Two modes of operation for TRILL over IP port:
  - **Dynamic:** All TRILL IS-IS Hellos are sent using UDP encapsulation and include a bit map of what encapsulations are fully supported. Data adjacencies are formed and LSPs sent on the IP link only if there is an encapsulation in common.
  - **Static:** Port is configured to always use a particular encapsulation for all TRILL data and IS-IS packets.

Encapsulation

- The current draft specifies two encapsulations:
  - UDP encapsulation (“native encapsulation”, really TRILL over UDP over IP). TRILL data versus IS-IS is indicated by destination UDP socket.
  - “VxLAN encapsulation” with current VxLAN [RFC7348] which has widespread fast path support (TRILL over Ethernet over VxLAN over UDP over IP). TRILL data versus IS-IS is indicated by EtherType but an extra source and destination MAC address are included which wastes 12 bytes.

Encapsulation



Encapsulation

- Other encapsulations are being developed in other working groups. Examples:
  - VxLAN GPE – eliminates 12 wasted bytes.
  - GUE (Generic UDP Encapsulation).
  - GENEVE
  - … there are more …

- TRILL over IP can be extended by future documents to support additional encapsulations.

Encapsulation

- Miscellaneous points:
  - Encapsulation support indicated by re-purposing support indication for a range of RBridge Channel protocol numbers. This is an efficient encoding already provided for in Hellos.
  - Encapsulation support could differ between ports on the same TRILL switch as it might depend on port hardware.
  - If TRILL over IP ports P1 and P2 have IP connectivity and both ports support encapsulations X and Y, then P1 might send to P2 using X and P2 might send to P1 using Y.

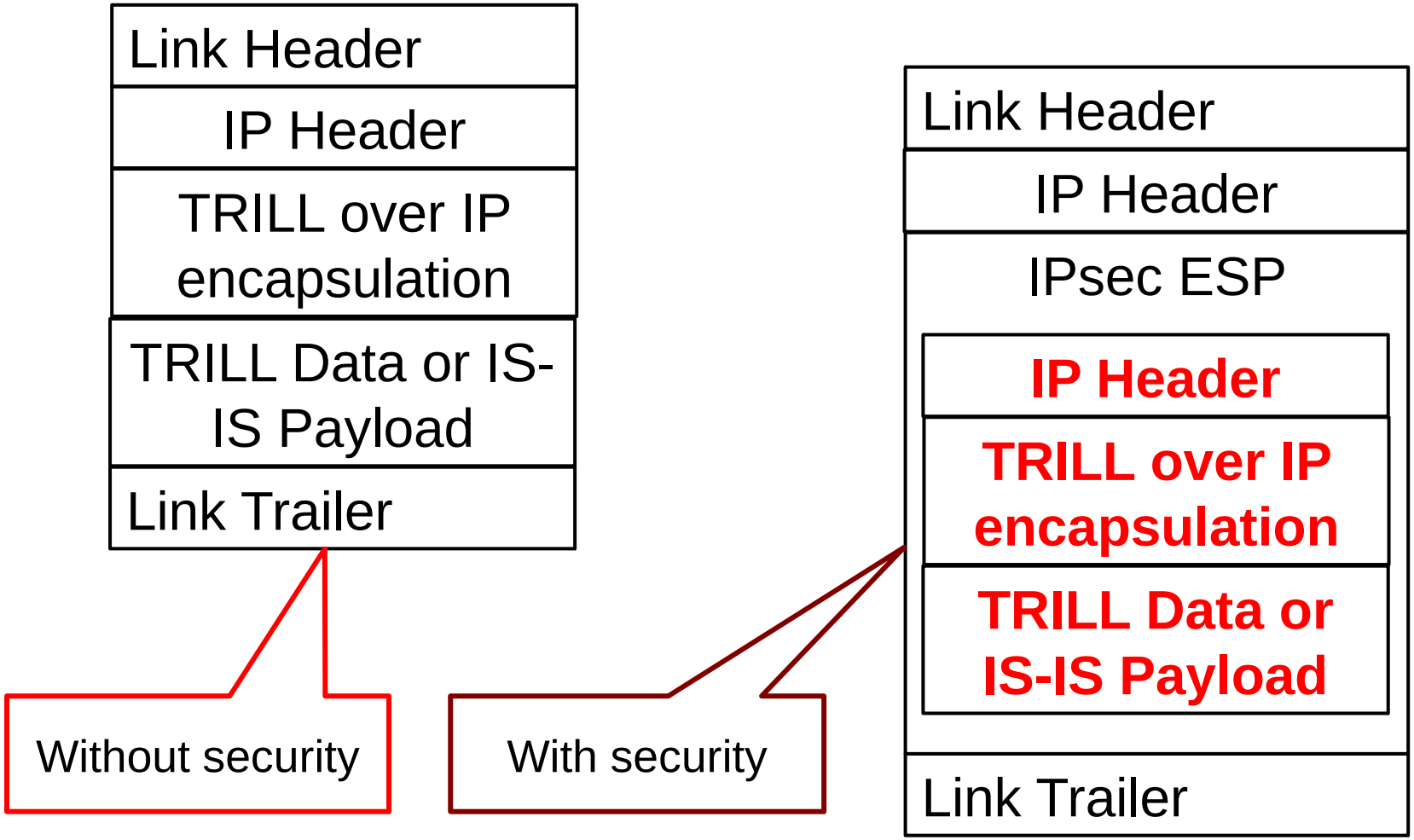
QoS

- TRILL uses 8 priority levels to give priority to critical control traffic and provide for relative priority of data.
- The -03 draft includes a default mapping of priority to DSCP codepoints and provides for configuration of that mapping.

Security

- Draft now specifies IPsec ESP (Encapsulating Security Protocol) in Tunnel Mode.
  - By default uses keys derived from TRILL IS-IS keys. Could add key negotiation support.
  - Use of ESP Tunnel Mode supports use of IPsec appliances separate from the actual RBridge port hardware.

IPsec ESP in Tunnel Mode



Work Remaining

- Work remaining includes:
  - Improve IPsec use. Add material on security configuration.
  - Middle Box Considerations section is empty.
  - Currently draft grew organically with material on a topic sometimes split between different parts of the draft. Needs some reorganization.

Feedback? Questions?