TRILL Link Security

Donald E. Eastlake, 3rd

<d3e3e3@gmail.com>

TRILL Link Security

- There is a partial draft:
  - draft-eastlake-trill-link-security-02.txt
- Goals of that draft are to do three things:
  - Establish strong security policies and defaults for TRILL link security.
  - Specify link security more precisely and provide defaults for Ethernet [RFC6325], PPP [RFC6361], and Pseudowire [RFC7173] links.
  - Specify edge-to-edge security.

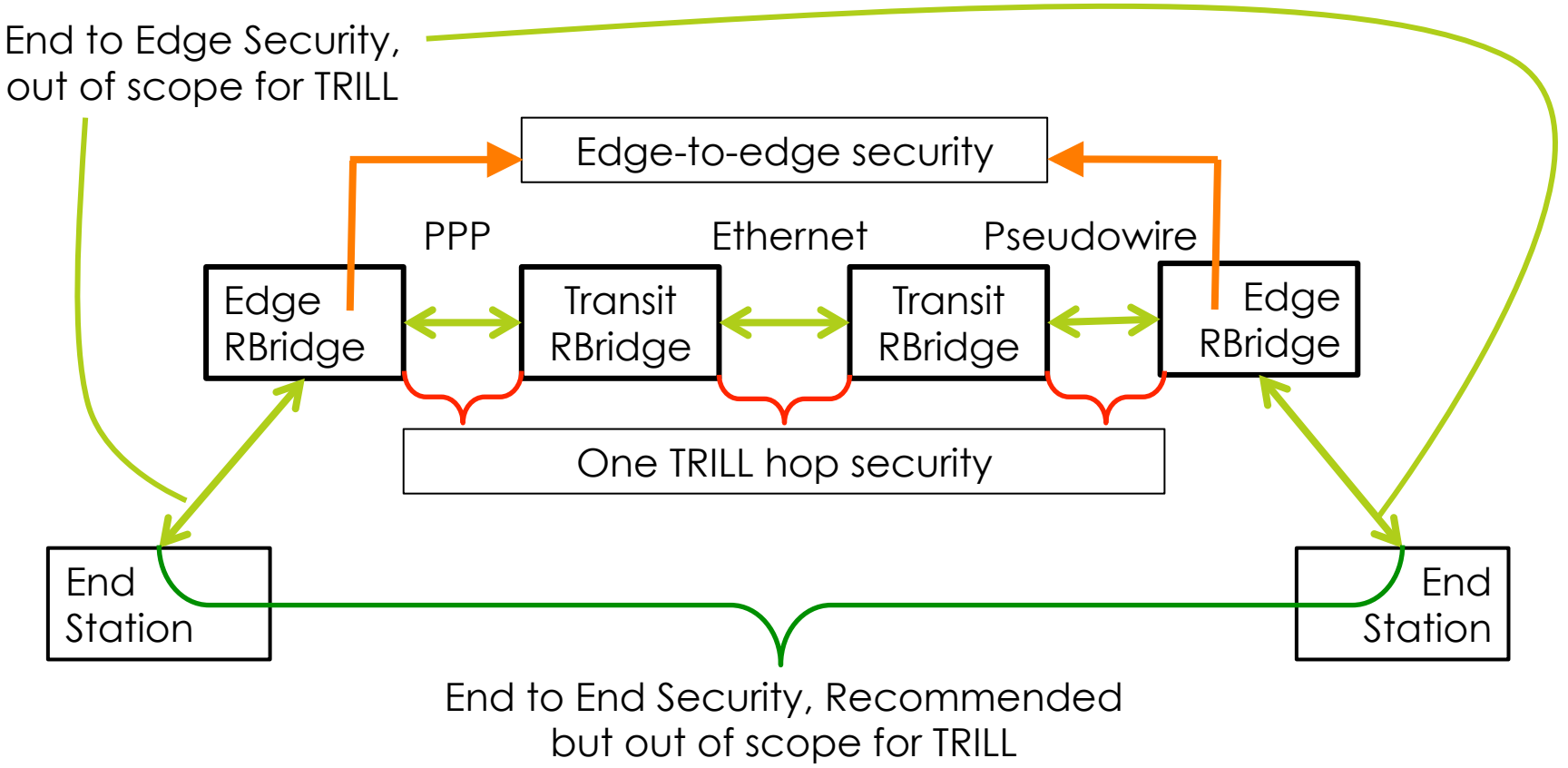
TRILL Link Security Policies

- Proposed policies:
  - **TRILL communication between TRILL switch ports that support encryption and authentication at line speed, MUST default to using security.**
  - **Security MUST be implemented even if a TRILL switch port is not capable of performing encryption and authentication at line speed.**
  - **When authentication is not available, opportunistic security [RFC7435] SHOULD be supported.**

Link Type Specific Link Security

- Summary by Link Type:
  - **Ethernet:** Specifies use of IEEE Std 802.1AE (MACSEC) Security, keys negotiated by 802.1X.
  - **PPP:**
    - For true PPP over HDLC links, does the best in it can.
    - In other cases, recommends using lower layer security such as Ethernet security for PPP over Ethernet.
  - **Pseudowire:** Pseudowires have no native security. Security for lower layer carrying pseudowire MUST be used.
  - (**IP:** IP link security is covered in the TRILL over IP draft.)

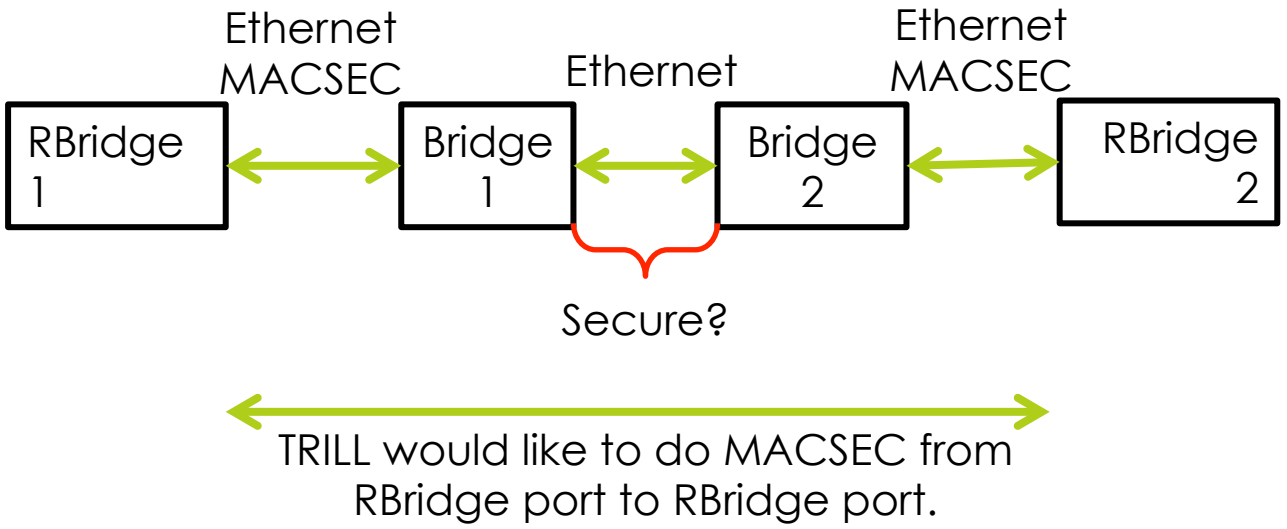
Overview


End to Edge Security,
out of scope for TRILL
Edge-to-edge security
PPP
Ethernet
Pseudowire
Edge
RBridge
Transit
RBridge
Transit
RBridge
Edge
RBridge
One TRILL hop security
End
Station
End
Station
End to End Security, Recommended
but out of scope for TRILL

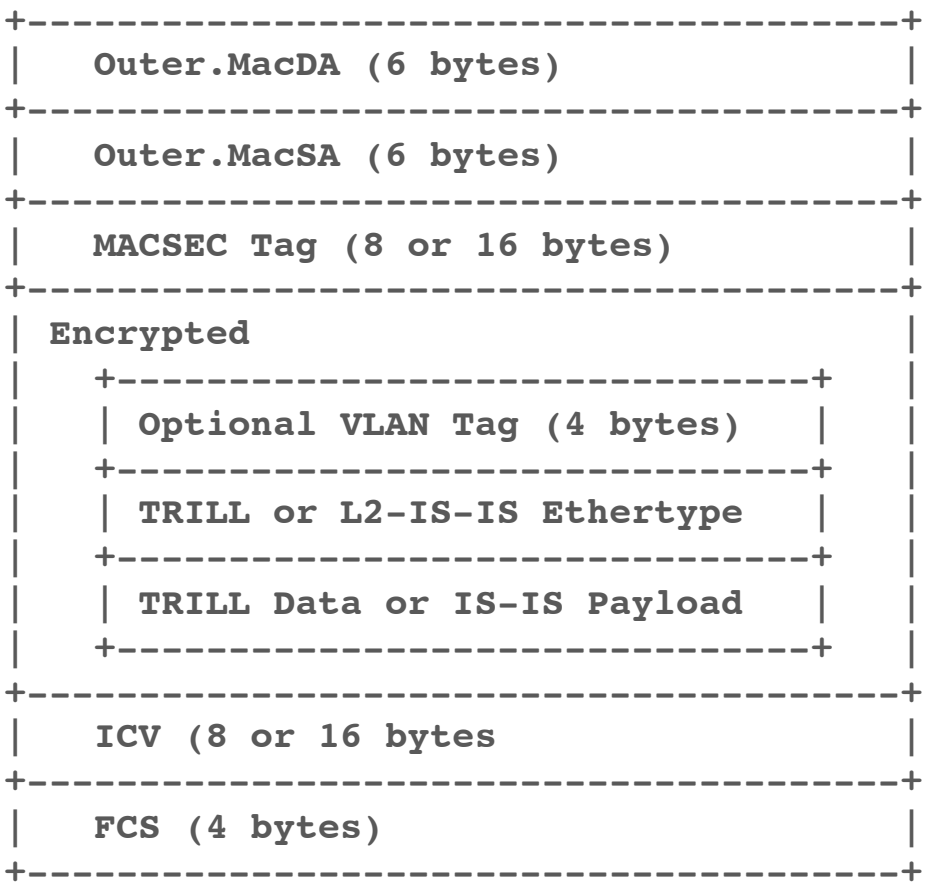
More on Ethernet Security

- MACSEC is straightforward for point to point Ethernet links.
  - In case of intervening customer bridges, those bridges have to be trusted/keyed or you need some more encapsulation.
- The draft has an appendix that touches on end station to end station MACSEC and MACSEC between an end stations and its edge TRILL switch, although algorithms and keying in those cases is out of scope for TRILL.

MACSEC is port to port



TRILL Ethernet Link Security

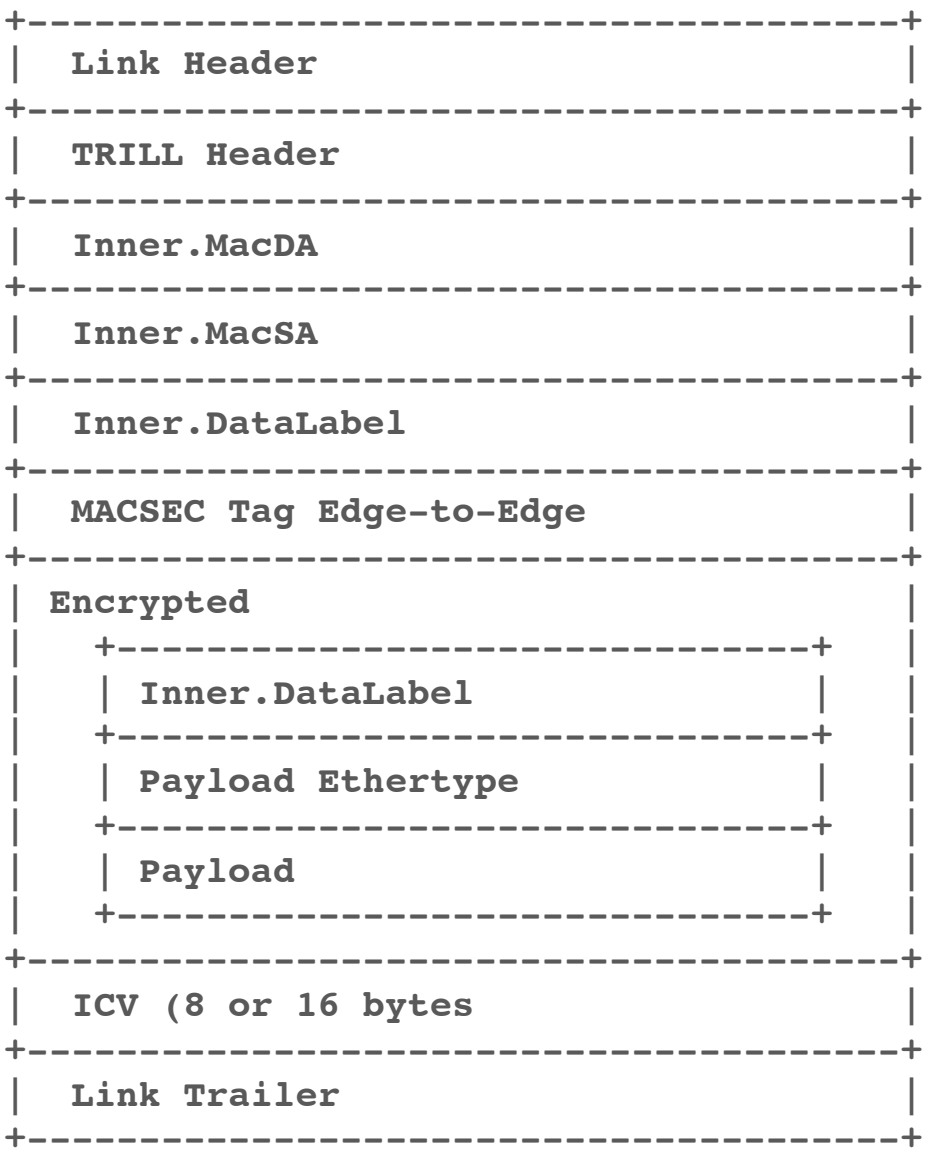


Edge-to-Edge Secuirty

- Edge-to-Edge security is between the ingress TRILL switch and the egress TRILL switch.
  - Negative: While one TRILL hop link security can protect the TRILL header, edge-to-edge security can only protect the inner payload. The TRILL header must be visible for TRILL switches to route correctly. And the inner Data Label (VLAN or FGL) must be visible for pruning.
  - Positive: Transit TRILL switches generally can't spy on the payload. Provides a reasonable amount of security without burdening transit TRILL switches with crypto.

Edge-to-Edge Secuirty

- Edge-to-Edge security has some difficulties. The obvious candidates are:
  - MACSEC, IPsec, and DTLS.
  - MACSEC and IPsec have better hardware support.
  - MACSEC would probably be more popular than IPsec.
- Draft currently says MACSEC but the structure of the TRILL Data packet makes it a bit hard to put MACSEC inside the TRILL Header and still expose the VLAN / FGL for pruning multi-destination distribution.



What you might want for TRILL edge-to-edge MACSEC.

Questions / Action

- Questions?

- Actions:
  - After a bit more work on the draft, a call for WG adoption should be done on the draft on link security.

END

Donald E. Eastlake, 3rd

<d3e3e3@gmail.com>