TRILL Link Security

Donald E. Eastlake, 3rd

<d3e3e3@gmail.com>

TRILL Link Security

- There is an early, incomplete draft:
  - draft-eastlake-trill-link-security-01.txt
- It's main goal (when complete) is 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.

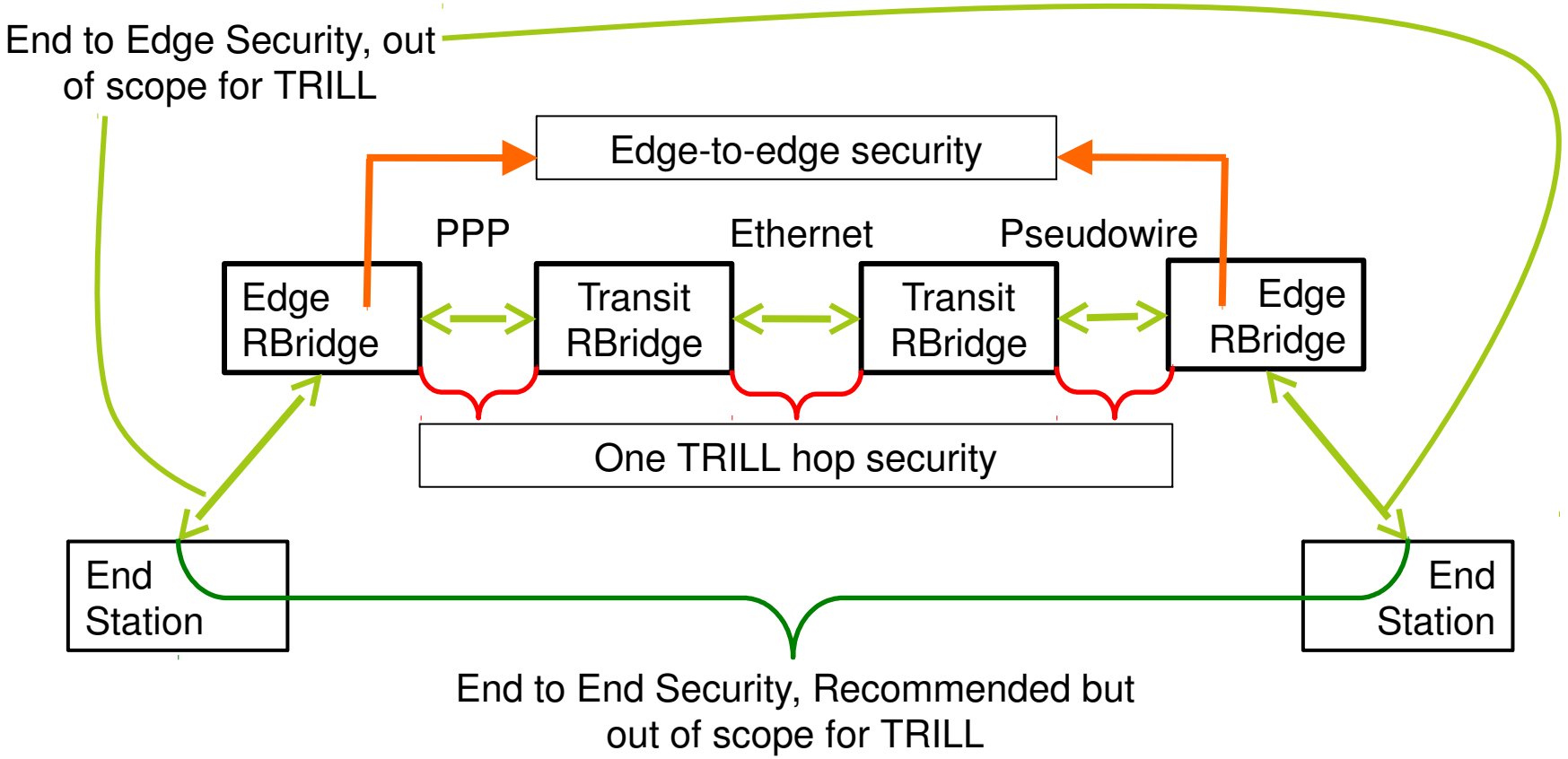
TRILL Link Security Policies

- 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
  - 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: Has no native security. Security for lower layer carrying pseudowire MUST be used.
  - (IP: Security covered in TRILL over IP draft.)

Example


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 also 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.

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.
  - Positive: Transit TRILL switches generally can't spy on the payload and higher bandwidth core links are not burdened with crypto.
  - The draft currently specifies MACSEC inside the TRILL Header.

Questions / Action

- Questions?

- Action: The draft needs more work. Comments welcome.

END

Donald E. Eastlake, 3rd

<d3e3e3@gmail.com>