TRILL Link Security

Donald E. Eastlake, 3rd

<d3e3e3@gmail.com>

TRILL Link Security

- There is a very early, incomplete -00 draft:
  - draft-eastlake-trill-link-security-00.txt
- It's main goal (when complete) is to do two things:
  - Establish strong security policies and defaults for TRILL link security.
  - Specify link security more precisely and provide defaults for the following link types:
    - Ethernet [RFC6325], PPP [RFC6361], and Pseudowire [RFC7173].

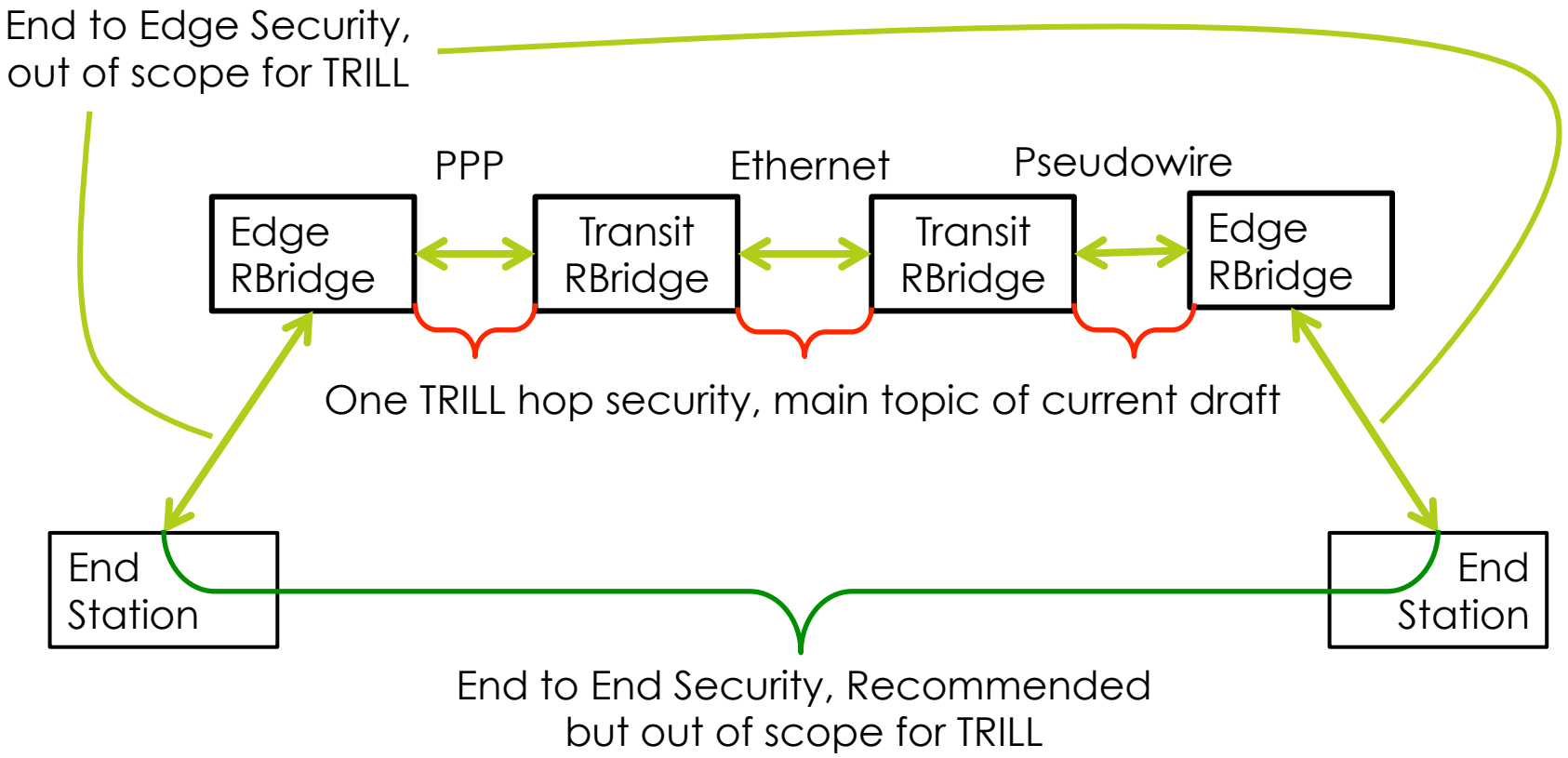
TRILL Link Security Policies

- Proposed new policies:
  - **TRILL communication between TRILL switch ports that support encryption and authentication at line speed, MUST default to using security.**
  - **Security MUST/SHOULD be implemented and available 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 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 to be covered in TRILL over IP draft.)

Example


End to Edge Security,
out of scope for TRILL
PPP
Ethernet
Pseudowire
Edge RBridge
Transit RBridge
Transit RBridge
Edge RBridge
One TRILL hop security, main topic of current draft
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, they 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.

Possible Addition

- Edge-to-Edge security between ingress TRILL switch and egress TRILL switch.
  - There are various possibilities including MACSEC inside the TRILL Header.

Questions / Action

- Questions?

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

END

Donald E. Eastlake, 3rd

<d3e3e3@gmail.com>