802.1AE-2018 SecY Delay

Richard Dubrawski

Table 10-3—SecY performance requirements

Parameter	Permitted values
SecY transmit delay	< Wire transmit time for maximum sized MPDU + (4 times wire transmit time for 64 octet MPDUs)
SecY transmit delay variance	< SecY transmit delay
SecY receive delay	< Wire transmit time for maximum sized MPDU + (4 times wire transmit time for 64 octet MPDUs)
SecY receive delay variance	< SecY receive delay
SC and SA creation and control delay	< 0.1 second
Transmit SAK install delay	< 1 second (8.2.2)
Transmit SAK switch delay	< Wire transmit time for 64 octet MPDU (8.2.2)
Receive SAK install delay	< 1 second
Receive SAK switch delay	No frame loss

All times are in seconds.

Allowed Latency vs Data Rate

Wire Speed (bits per second)	Allowed Latency (sec)	Allowed Latency nano seconds
1.00E+09	8.09E-05	80928.00
1.00E+10	8.09E-06	8092.80
1.00E+11	8.09E-07	809.28
4.00E+11	2.02E-07	202.32
1.00E+12	8.09E-08	80.93
	8*Total Bytes / Wire Speed	

PT Size	64	9600
Macsec Overhead	32	32
Ethernet Preamble	8	8
Ethernet Inter-frame-gap	12	12
	116	9652
Number allowed	4	1
Total bytes on wire	10116	

Suggest dropping latency requirements

- Practical / Technological.
  - Current technologies (clock speeds) make achieving these requirements above 10Gbps unlikely.
  - Meeting these would require insecure design or gaming the system:
    - AES-GCM requires ICV check. Decrypted frame should not leave SecY until ICV check is validated. The requires buffering the frame in the SecY. Allowing the frame to move on and clawing it back if ICV check fails is bad security.
    - SecY is only 1 component in the implementation (either standalone EDE or in a bridge). Moving all buffers outside the SecY component does not reduce actual device latency, it just moves it.
    - Conformance could be claimed but only when operating in “pass through” mode. (No confidentiality and no integrity)
- Requirement not needed to provide MACSEC functionality and interoperability.
  - 100Gbps devices can successfully interoperate with 100Mbps devices, each having vastly different latency requirements.

Practicality

- Commercial vendors likely to ignore these requirements:
  - Customers care more about total device latency and not some arcane sub-component latency.
  - Not measurable directly, so hard to confirm.
  - Does not impact interoperability testing.
- 100Gbps+ implementations rely on parallel handling of frame data
  - Internal implementations use wide busses vs serial data streams.
  - Serial input data is buffered internally to allow parallel handling of the encrypt and decrypt operations.
- 200 nanoseconds is about the latency of 40 m of optical fiber.

What about TSN

- Actual latency through Bridge or EDE is bigger than the SecY.
- Does TSN need latency that scales with data rate?
  - Sub microsecond latency?
  - What does TSN really need?

Summarize

- SecY Latency requirements not realistically achievable at high data rates.
- Commercial vendors likely to ignore these requirements, weakening the spec.
- For low latency needs, this one component is insufficient.