802.1AE-2018 SecY Delay
Richard Dubrawski
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted values</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecY transmit delay</td>
<td>&lt; Wire transmit time for maximum sized MPDU + (4 times wire transmit time for 64 octet MPDUs)</td>
</tr>
<tr>
<td>SecY transmit delay variance</td>
<td>&lt; SecY transmit delay</td>
</tr>
<tr>
<td>SecY receive delay</td>
<td>&lt; Wire transmit time for maximum sized MPDU + (4 times wire transmit time for 64 octet MPDUs)</td>
</tr>
<tr>
<td>SecY receive delay variance</td>
<td>&lt; SecY receive delay</td>
</tr>
<tr>
<td>SC and SA creation and control delay</td>
<td>&lt; 0.1 second</td>
</tr>
<tr>
<td>Transmit SAK install delay</td>
<td>&lt; 1 second (8.2.2)</td>
</tr>
<tr>
<td>Transmit SAK switch delay</td>
<td>&lt; Wire transmit time for 64 octet MPDU (8.2.2)</td>
</tr>
<tr>
<td>Receive SAK install delay</td>
<td>&lt; 1 second</td>
</tr>
<tr>
<td>Receive SAK switch delay</td>
<td>No frame loss</td>
</tr>
</tbody>
</table>

All times are in seconds.
## Allowed Latency vs Data Rate

<table>
<thead>
<tr>
<th>Wire Speed (bits per second)</th>
<th>Allowed Latency (sec)</th>
<th>Allowed Latency nano seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.00E+09</td>
<td>8.09E-05</td>
<td>80928.00</td>
</tr>
<tr>
<td>1.00E+10</td>
<td>8.09E-06</td>
<td>8092.80</td>
</tr>
<tr>
<td>1.00E+11</td>
<td>8.09E-07</td>
<td>809.28</td>
</tr>
<tr>
<td>4.00E+11</td>
<td>2.02E-07</td>
<td>202.32</td>
</tr>
<tr>
<td>1.00E+12</td>
<td>8.09E-08</td>
<td>80.93</td>
</tr>
</tbody>
</table>

8*Total Bytes / Wire Speed

<table>
<thead>
<tr>
<th>PT Size</th>
<th>64</th>
<th>9600</th>
</tr>
</thead>
<tbody>
<tr>
<td>Macsec Overhead</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>Ethernet Preamble</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Ethernet Inter-frame-gap</td>
<td>12</td>
<td>12</td>
</tr>
</tbody>
</table>

| 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.