802.1AEdk Status
Towards a first Draft

Don Fedyk (dfedyk@labn.net)
Outline

• Status
• Current state
• Some table of contents
• Relevant diagrams
  • Missing changes
Current MACsec draft.

• Clause 17 – MAC Privacy discussion Micks Updates _terminology
• Clause 18 – Privacy Protocol Needs work in some sections
  • Applicability ()
  • Privacy protection ()
  • Priority and traffic class support ()
  • Coexistence, interoperability and deployment () <- Here
• Clause 19 Encoding PDUs – Good Shape
• Clause 20 – MAC Privacy-protecting Entity (PrY) operation
  • Needs some diagram details see following.
• Clause 21 -MAC Privacy protection in Systems Needs a Pass through
• YANG – Pretty good shape.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.</td>
<td>MAC Privacy protection</td>
<td>18</td>
</tr>
<tr>
<td>17.1</td>
<td>The need for MAC privacy Protection</td>
<td>18</td>
</tr>
<tr>
<td>17.2</td>
<td>Protecting user data frames</td>
<td>19</td>
</tr>
<tr>
<td>17.3</td>
<td>Quality of Service Impact and mitigation</td>
<td>21</td>
</tr>
<tr>
<td>17.4</td>
<td>Interoperability and deployment</td>
<td>25</td>
</tr>
<tr>
<td>17.5</td>
<td>Network configuration</td>
<td>26</td>
</tr>
<tr>
<td>17.6</td>
<td>Security considerations</td>
<td>26</td>
</tr>
<tr>
<td>18.</td>
<td>MAC Privacy-protecting Protocol</td>
<td>27</td>
</tr>
<tr>
<td>18.1</td>
<td>Protocol design requirements</td>
<td>27</td>
</tr>
<tr>
<td>18.2</td>
<td>Protocol support requirements</td>
<td>29</td>
</tr>
<tr>
<td>19.</td>
<td>Encoding of MAC Privacy-protection Protocol Data Units</td>
<td>30</td>
</tr>
<tr>
<td>19.1</td>
<td>Structure, representation, and encoding</td>
<td>30</td>
</tr>
<tr>
<td>19.2</td>
<td>MMPDU components</td>
<td>30</td>
</tr>
<tr>
<td>19.3</td>
<td>MAC Privacy-protection EtherType</td>
<td>32</td>
</tr>
<tr>
<td>19.4</td>
<td>Protocol versions</td>
<td>32</td>
</tr>
<tr>
<td>19.5</td>
<td>Encapsulated User Frames</td>
<td>33</td>
</tr>
<tr>
<td>19.6</td>
<td>Trailing Pads</td>
<td>33</td>
</tr>
<tr>
<td>19.7</td>
<td>Explicit Pads</td>
<td>33</td>
</tr>
<tr>
<td>19.8</td>
<td>Encapsulated User Frame Fragments</td>
<td>33</td>
</tr>
<tr>
<td>19.9</td>
<td>Initial Frame Fragments</td>
<td>34</td>
</tr>
<tr>
<td>19.10</td>
<td>Final Frame Fragments</td>
<td>35</td>
</tr>
<tr>
<td>19.11</td>
<td>Express Bit</td>
<td>35</td>
</tr>
<tr>
<td>19.12</td>
<td>MPPDU generation</td>
<td>35</td>
</tr>
<tr>
<td>19.13</td>
<td>MPPDU validation</td>
<td>36</td>
</tr>
<tr>
<td>19.14</td>
<td>Bypass Port Frames</td>
<td>37</td>
</tr>
</tbody>
</table>
## Contents

20. MAC Privacy-protecting Entity (PrY) operation 39
   20.1 PrY overview 39
   20.2 SecY functions 41
   20.3 Model of operation 42
   20.4 PrY architecture 42
   20.5 Secure frame generation 43
   20.6 Secure frame verification 47
   20.7 SecY management 51
   20.8 Addressing 64
   20.9 Priority 64
   20.10 SecY performance requirements 65

21. MAC Privacy protection in Systems 66
   21.1 Privacy-protecting interface stacks 66
   21.2 Privacy protection for end station interfaces 67
   21.3 Privacy protection for bridge interfaces 67
   21.4 MACsec in VLAN-aware Bridges 69
   21.5 MACsec and Link Aggregation 70
   21.6 Link Layer Discovery Protocol (LLDP) 71
   21.7 MACsec in Provider Bridged Networks 72
   21.8 MACsec and multi-access LANs 74
Current Formats Clause 19

MPP element (general format)

- MPPDU element data
- MPP element (general format)
- Frame (DA, SA, MSDU)

Encapsulated Frame

- Padding to remainder of MPPDU (0 or more octets)
- Trailing Pad
- Explicit Pad

- Following length (msb)
- Following length (lsb)
- 0 or more 'following length' octets

- MPPCI Octet 1
- MPPCI Octet 2
- MPPCI Octet 3
- MPPCI Octet 4
- MPPCI Octet 5
- MPPCI Octet 6

- Following length (msb)
- Following length (lsb)
- Fragment number (24 bits)
- Encapsulated frame fragment

Reserved for future set to 0 and ignored on reception by this version of the protocol

- 1 if this is an urgent frame, 0 if this in non-urgent
- 1 if this is an final fragment of the frame, 0 otherwise
- 1 if this is an initial fragment of the frame, 0 otherwise
Clause 19
Clause 20
Clause 20
Clause 20 Stats

- `tx = transmitted frame`
- `Clear Port`
- `Bypass Port`
- `map userPriorityToPry to Channel or Frames`
- `add frame`
- `if (one channel)`
- `update outPadOctets`
- `add frames and fragments`
- `for (all frames) outUserFrames++`
- `for (all fragments) outUserFragments++`
- `update outPadOctets`
- `if nodata`
Clause 20 Management and YANG
Comments