802.1AE

DA | SA
---|---
**UNI Tag (Vlan/MPLS)** | Inner Vlan Tag | User Data

Unencrypted

DA | SA
---|---
Integrity Protected

Secure Vlan Tag, User Data

ICV | FEC

Confidential

Unencrypted

Secure

Plain Text
MIXED SCENARIO

Node1

MACsec Enabled UNI-C port

EDE-M?

Node2

MACsec Enabled UNI-C port

Switched Network

Node3

MACsec Enabled UNI-C port

**Table: Secure VLAN Tag, User Data**

<table>
<thead>
<tr>
<th>DA</th>
<th>SA</th>
<th>Inner VLAN Tag</th>
<th>User Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>A</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>S</td>
<td>A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Diagram:**

- Node1 to Node3
- EDE-CC and EDE-M
- Switched Network
- UNI-N
- MACsec Enabled UNI-C port
- Secure VLAN Tag, User Data
802.1AEcg

Required functionality:
- Backward compatibility
- EDE-CC and EDE-M embedded in the ports.

Node1:
- Egress packets secured by MACsec should inter-op with both Node2 which could support 802.1aecg & Node3 which only supports 802.1AE-2006
- This could be solved by configuring EDE-CC in SCs that talk to Node2 and EDE-M in SCs that talk to Node3
- Is it possible as per .1AEcg?