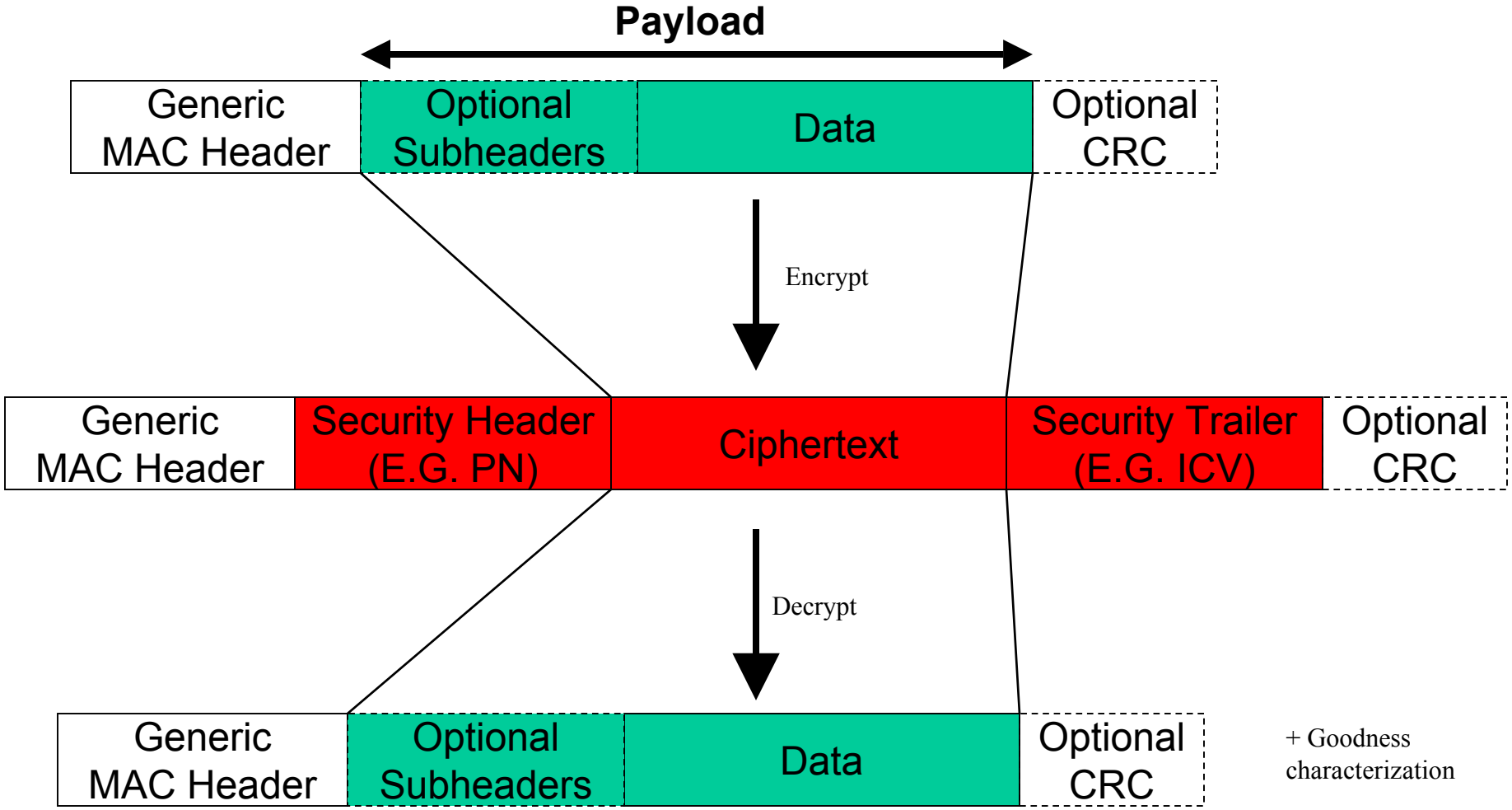
802.16 Packet CS and MacSec Leading to a Key Exchange Issue

David Johnston

david.johnston@ieee.org

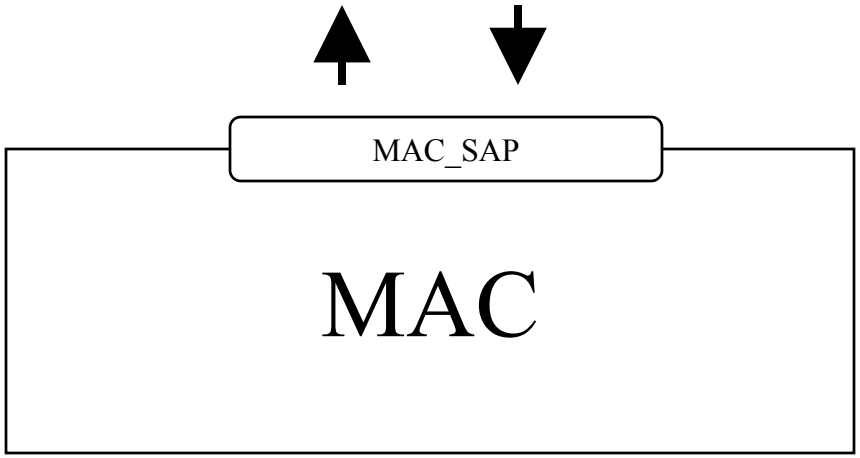
dj.johnston@intel.com

An 802.16 Packet



The 802.16 MAC SAP

- CREATE_CONNECTION
- CHANGE_CONNECTION
- TERMINATE_CONNECTION
- MAC_DATA(CID, Length, data, discard-eligible-flag, encryption)



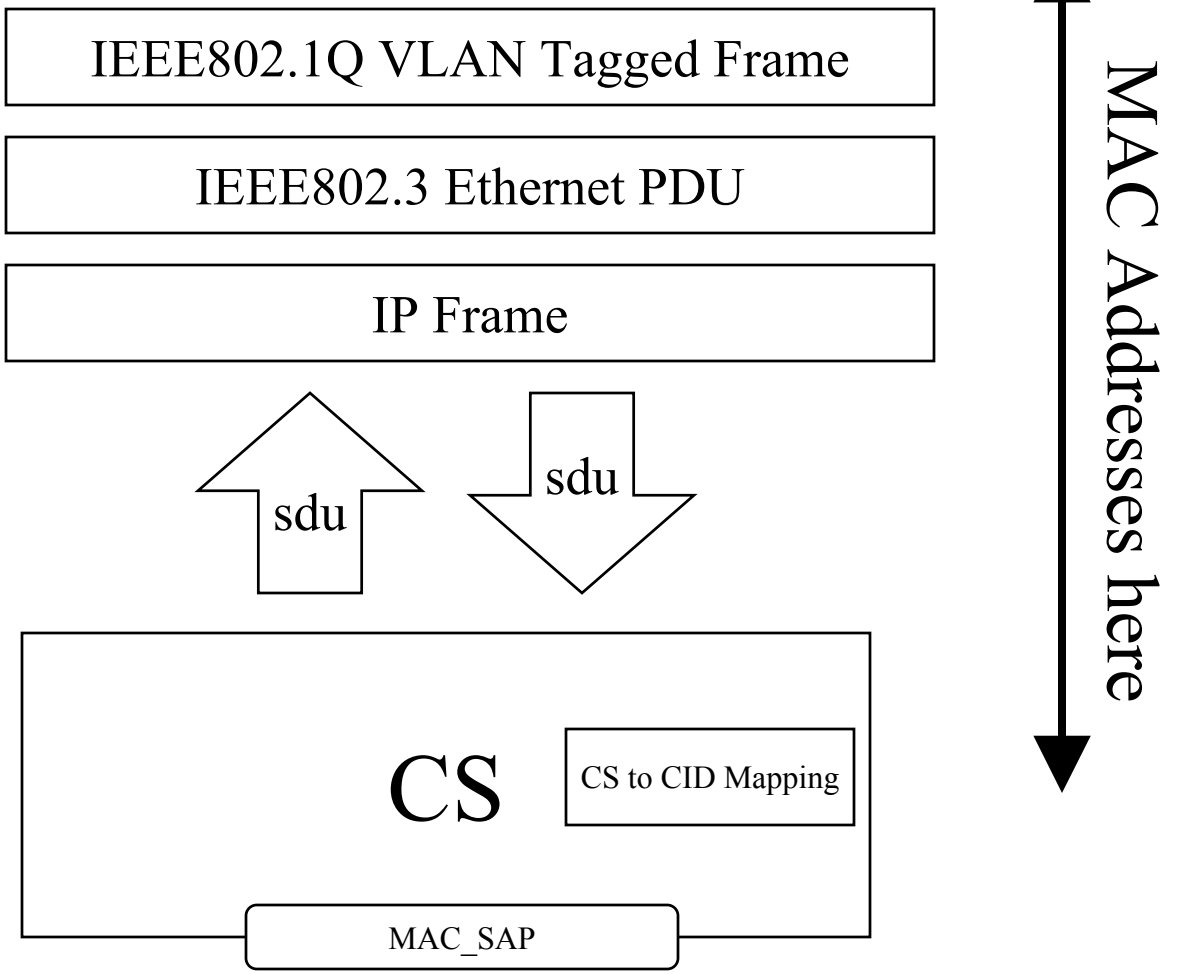
NO MAC Addresses here!

The CS SAP

- SDUs go up and down

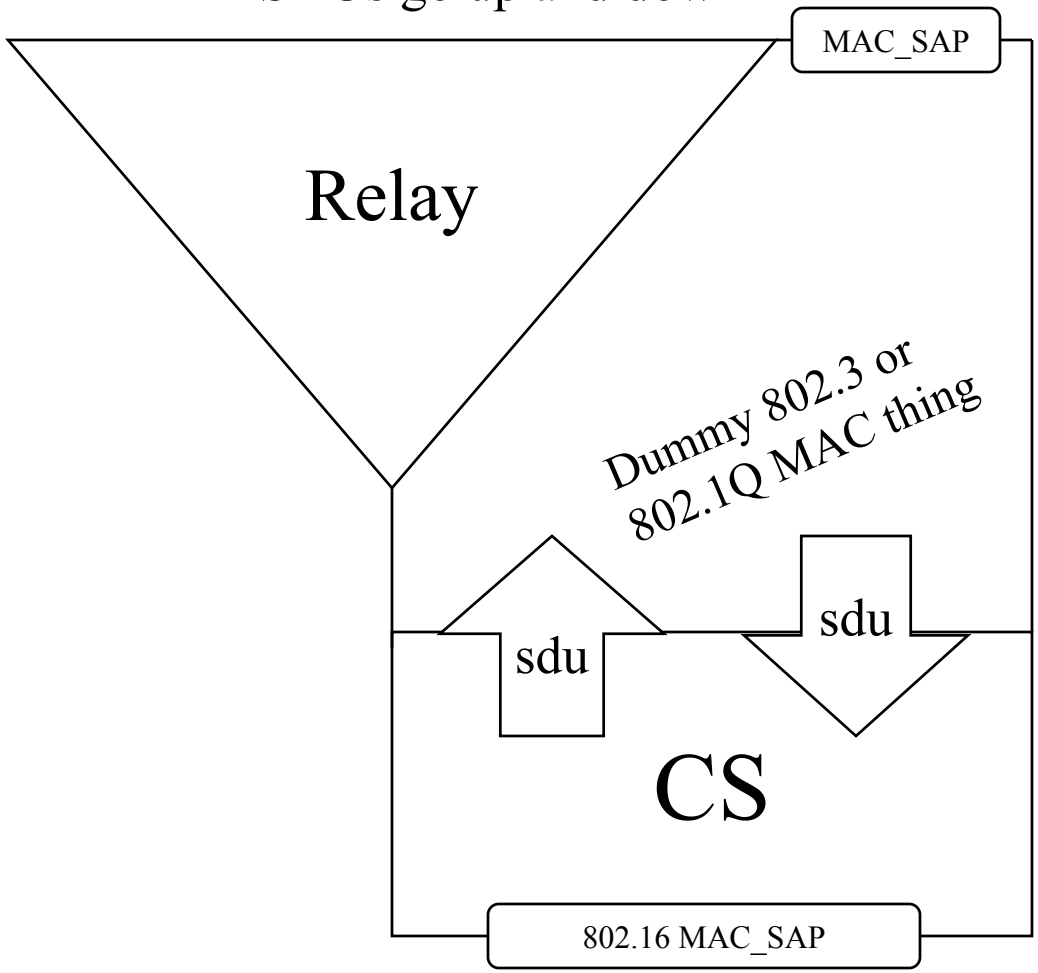
OR:

OR:

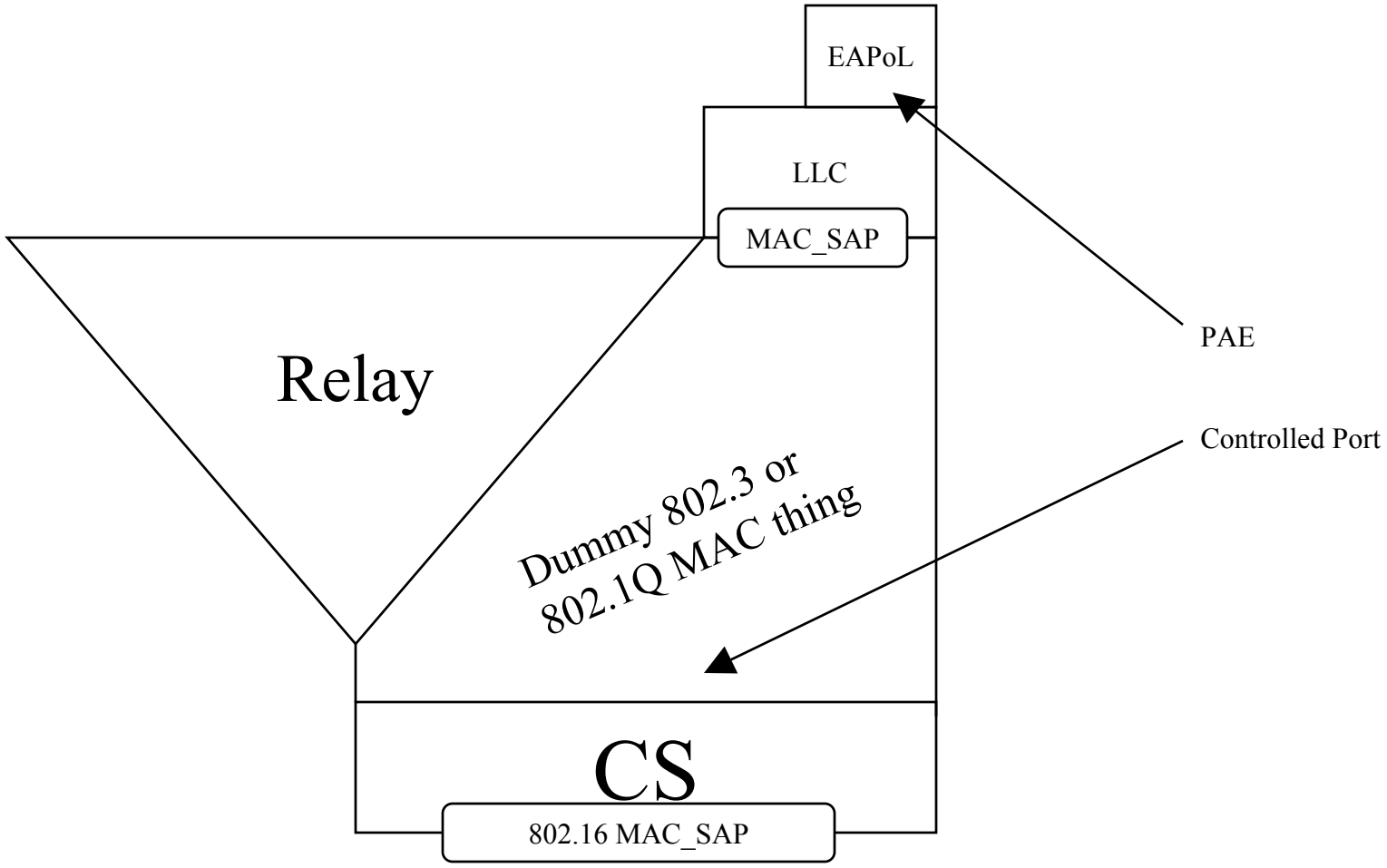


The CS SAP With 802.1 Bridging

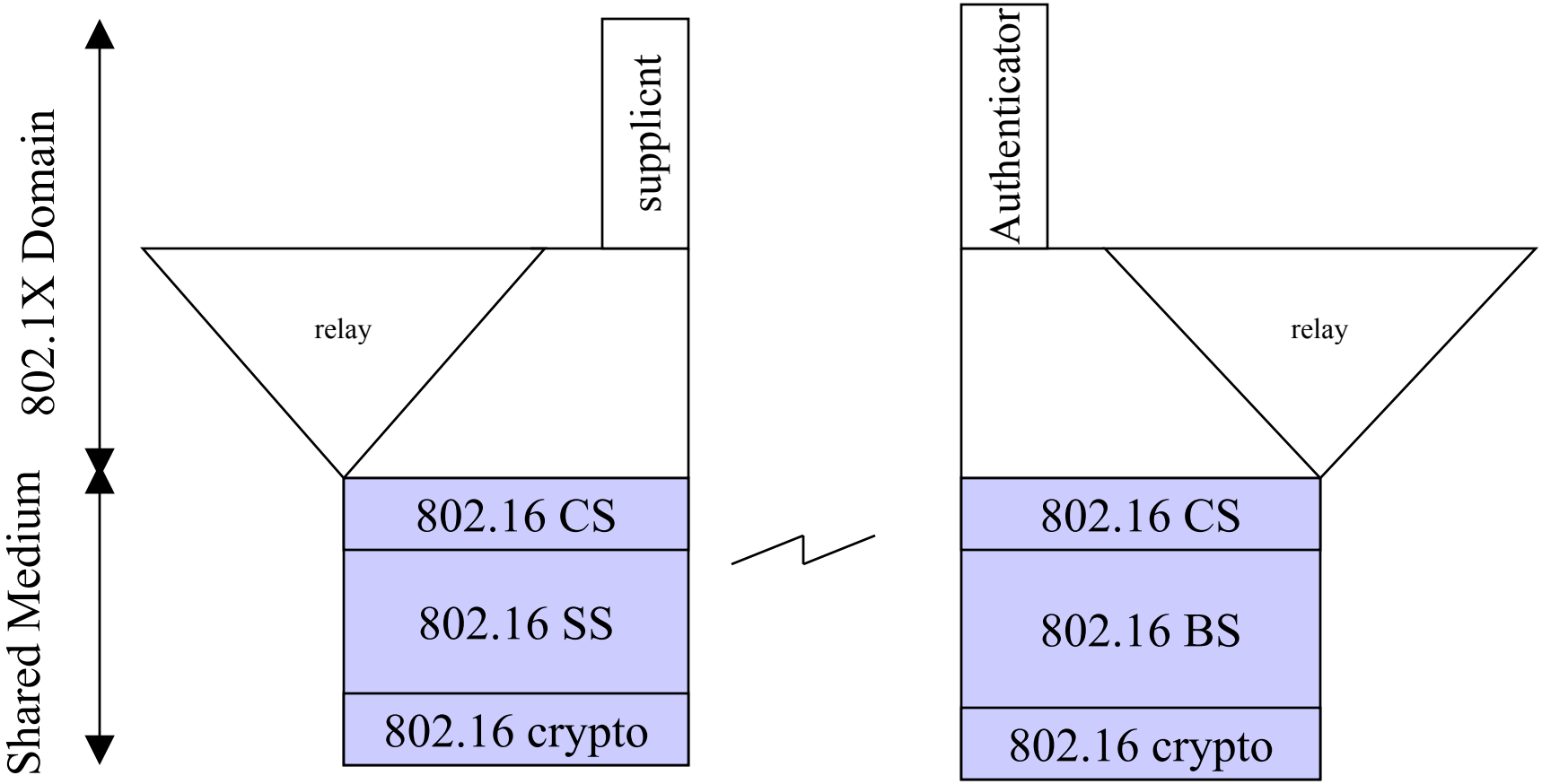
- SDUs go up and down



Where would 802.1aa go?

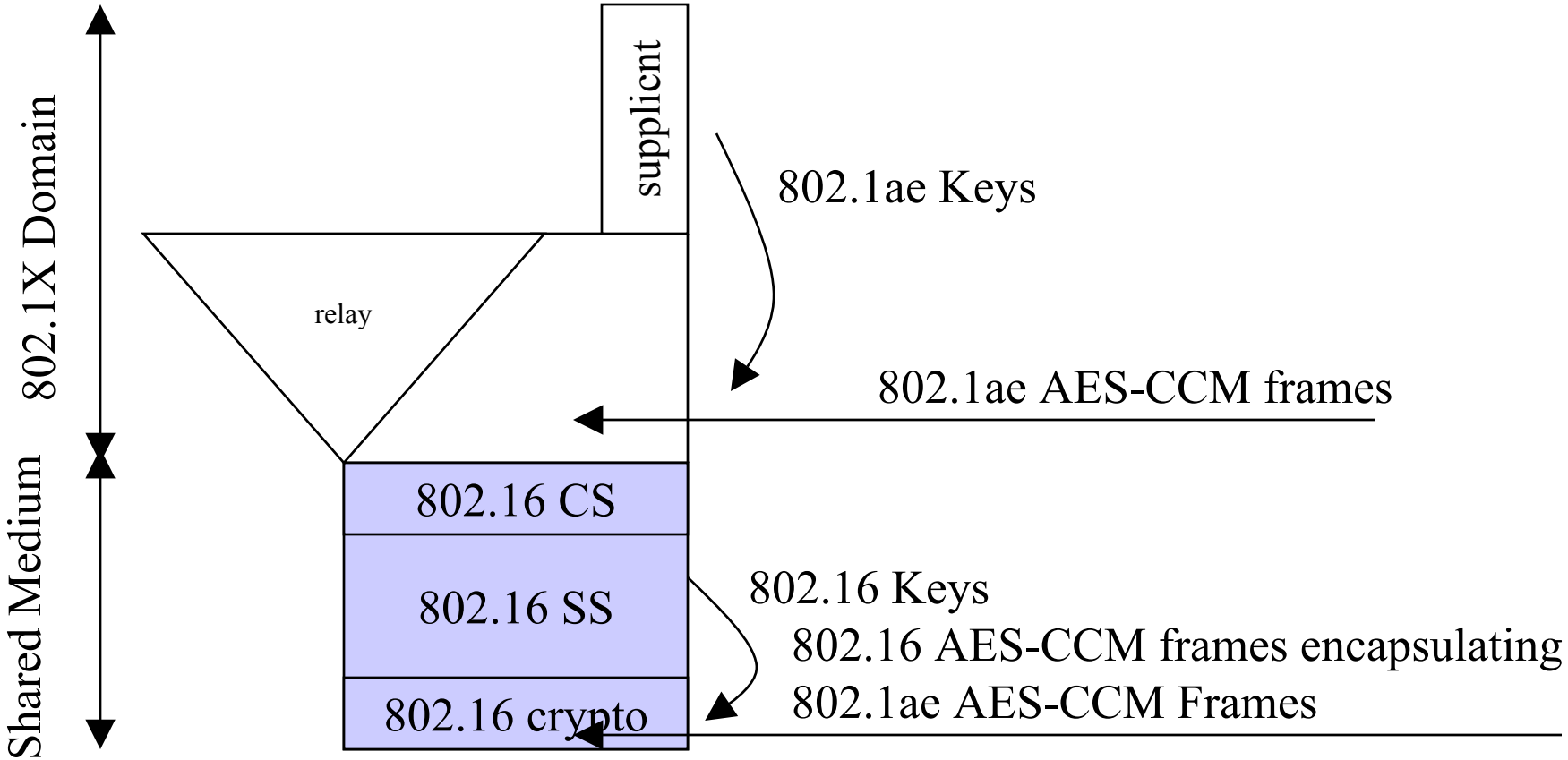


802.16 SS-BS bridged connection

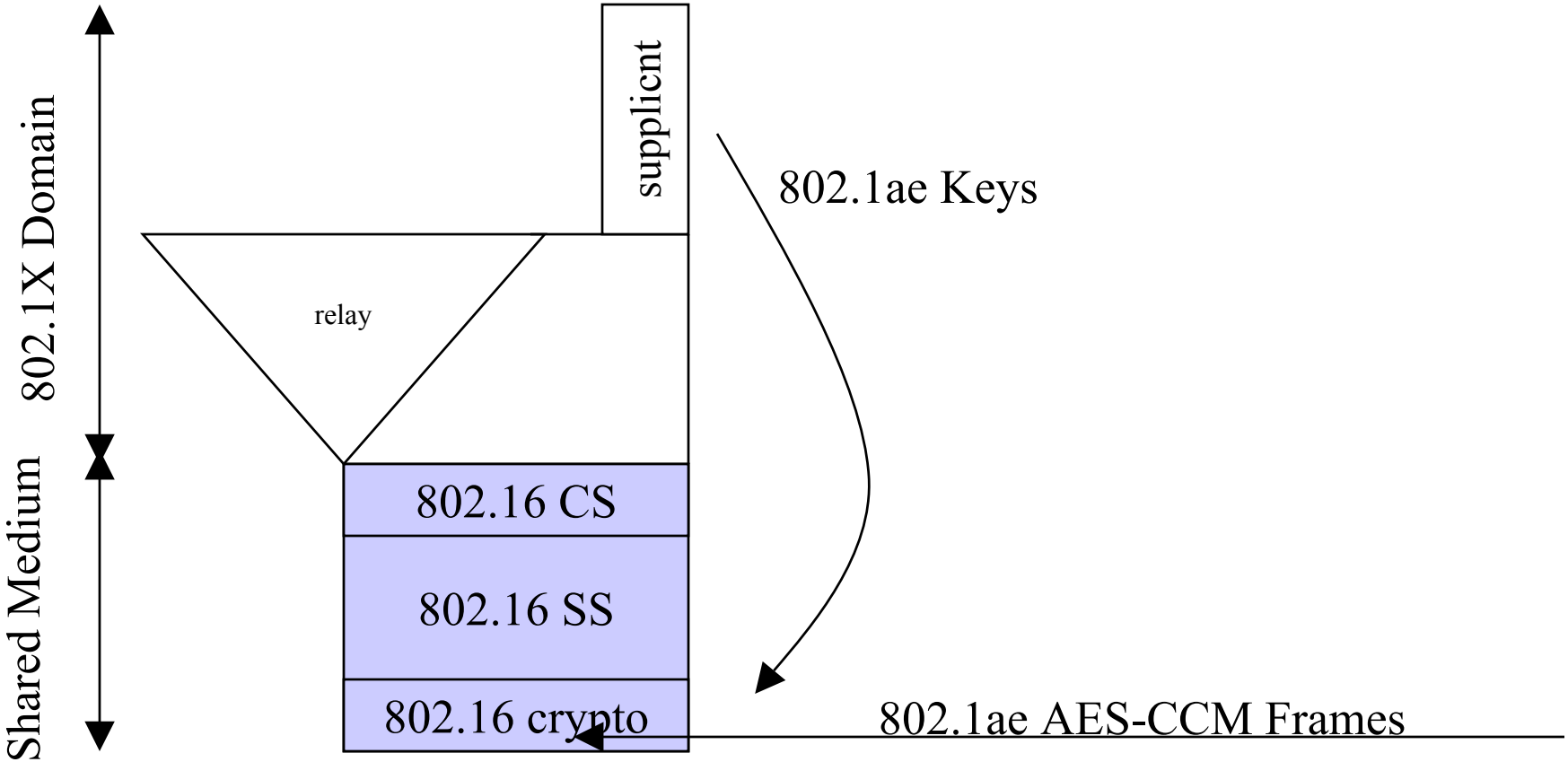


802.16 is an anonymous blob, isolated by a convergence service

Overloaded Crypto



Cutting the link?



Question

- Is it a sane/desirable/useful goal to decouple keying from MacSec such that keying can be useful to lower down ciphers?
- Leading to:
  - Controlled port above the lowest MAC
  - Cipher at bottom of lowest MAC
  - Keys provided from above
    - Port status and key availability synchronized
    - Efficiency (no overloaded crypto on broken 802 architectures)

Implications on Requirements

- If the previous idea is sound then:
- Key Exchange should allow lower cipher to propagate keying parameters upwards..
  - Amount of keying required (E.G. 128, 256 bits, etc)