Ethernet Data Encryptors (EDEs)

Two port 802.1Q, 802.1AE, 802.1X devices providing ‘hop-specific’ frame integrity and data confidentiality. ‘Red side’ port rx/tx unprotected, ‘black side’ protected by MACsec. Protected `hop’ can be TPMR to TPMR, Provider Bridge to Provider Bridge, Customer to Provider, Customer Bridge to Customer Bridge.

.../docs2013/ae-seaman-ede-ppt-0913-v01.pdf

.../docs2013/ae-seaman-ede-0713-v02.pdf

.../docs2013/ae-seaman-macsec-hops-0626-v03.pdf

Some desired functionality is not obvious from existing standards. This presentation suggests some solutions, solicits feedback and help in identifying problems and issues.

Mick Seaman

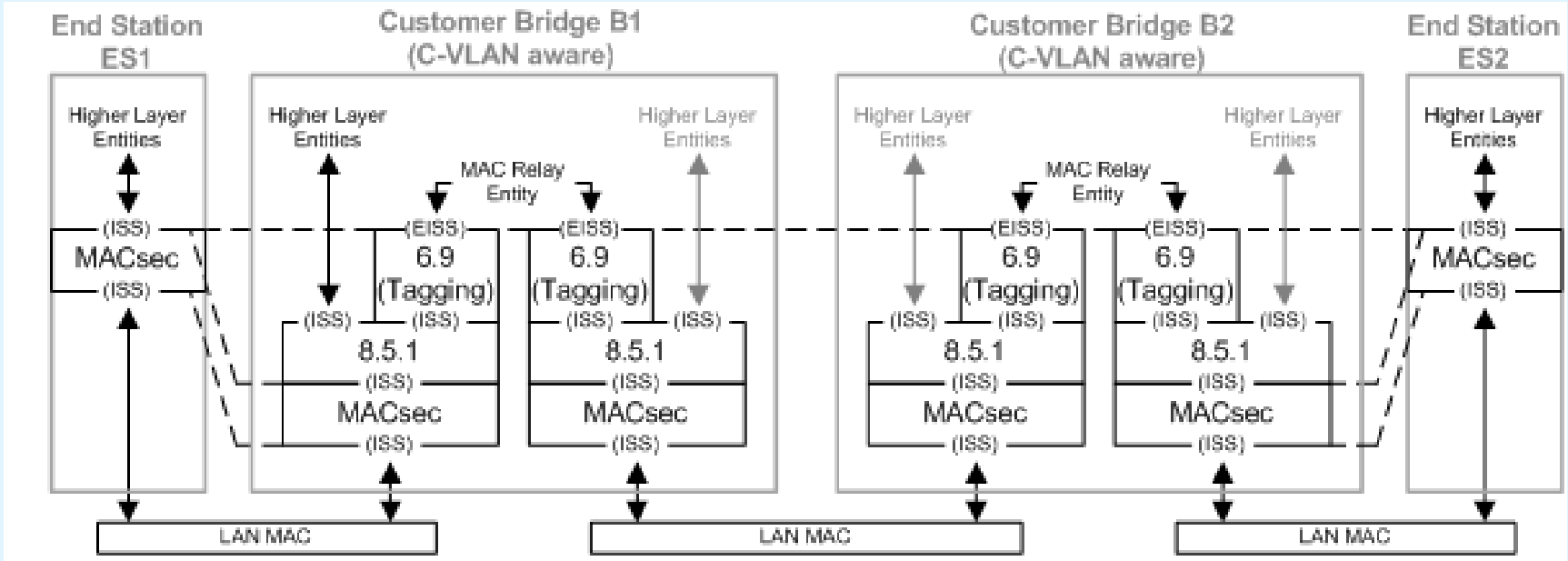
EDE specification objectives

- Maximal use of existing standards
- Minimal interference in unrelated issues
- Cover all the use cases
  - In network, across network, to network
  - C-DA, C-SA confidentiality w/ MAC-in-MAC
- Integrated operation
  - Peering with existing spec MACsec bridges
- And transparent operation
  - Add to existing bridged network

Agenda

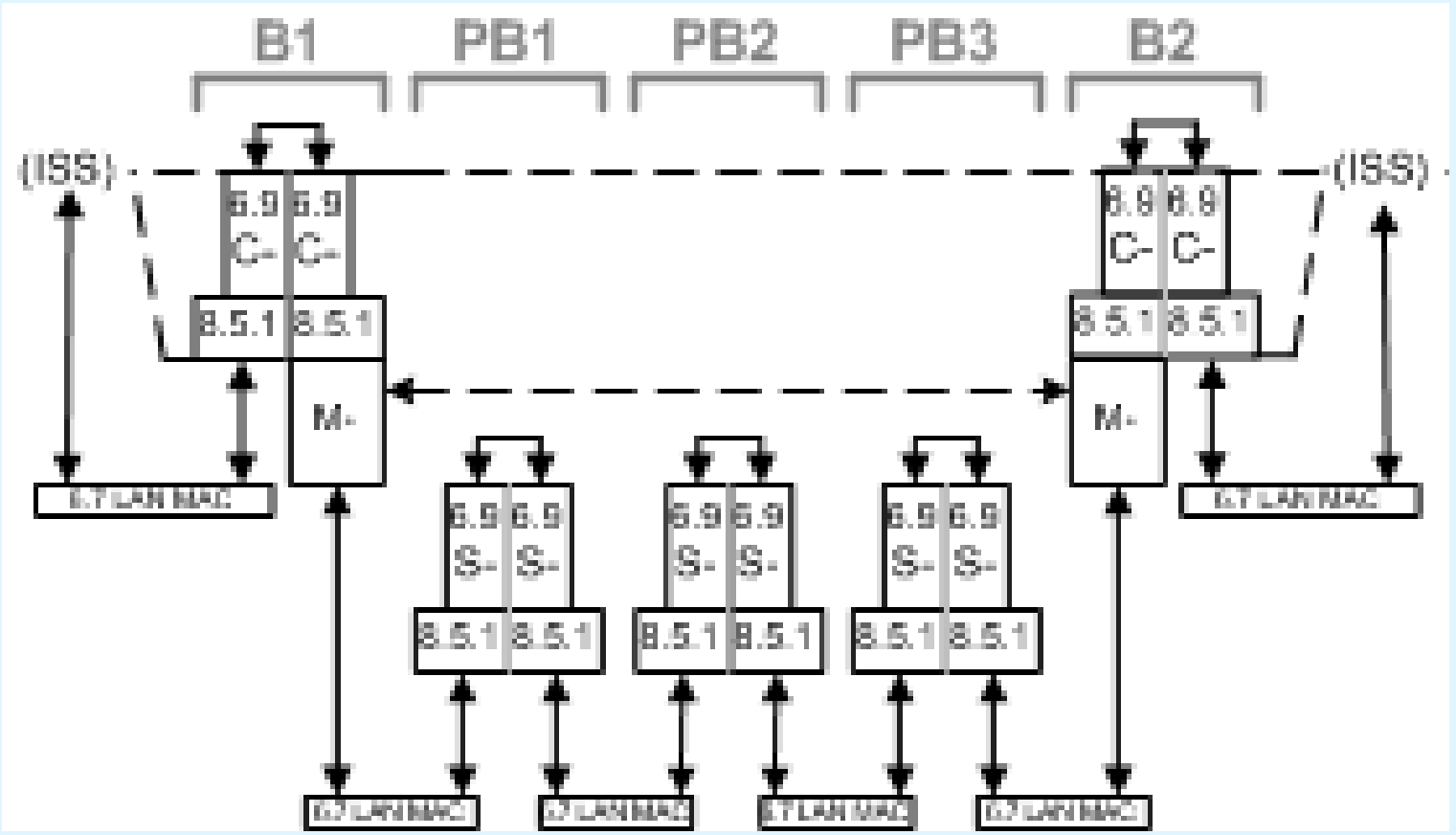
- EDE specification objectives
- MACsec basics (a crash course)
- Integrated operation
- Transparent operation
- An EDE classification scheme
- Addressing for transparent operation
- Missing interface(s) in .1Q ?
- A.O.B

MACsec in a customer network

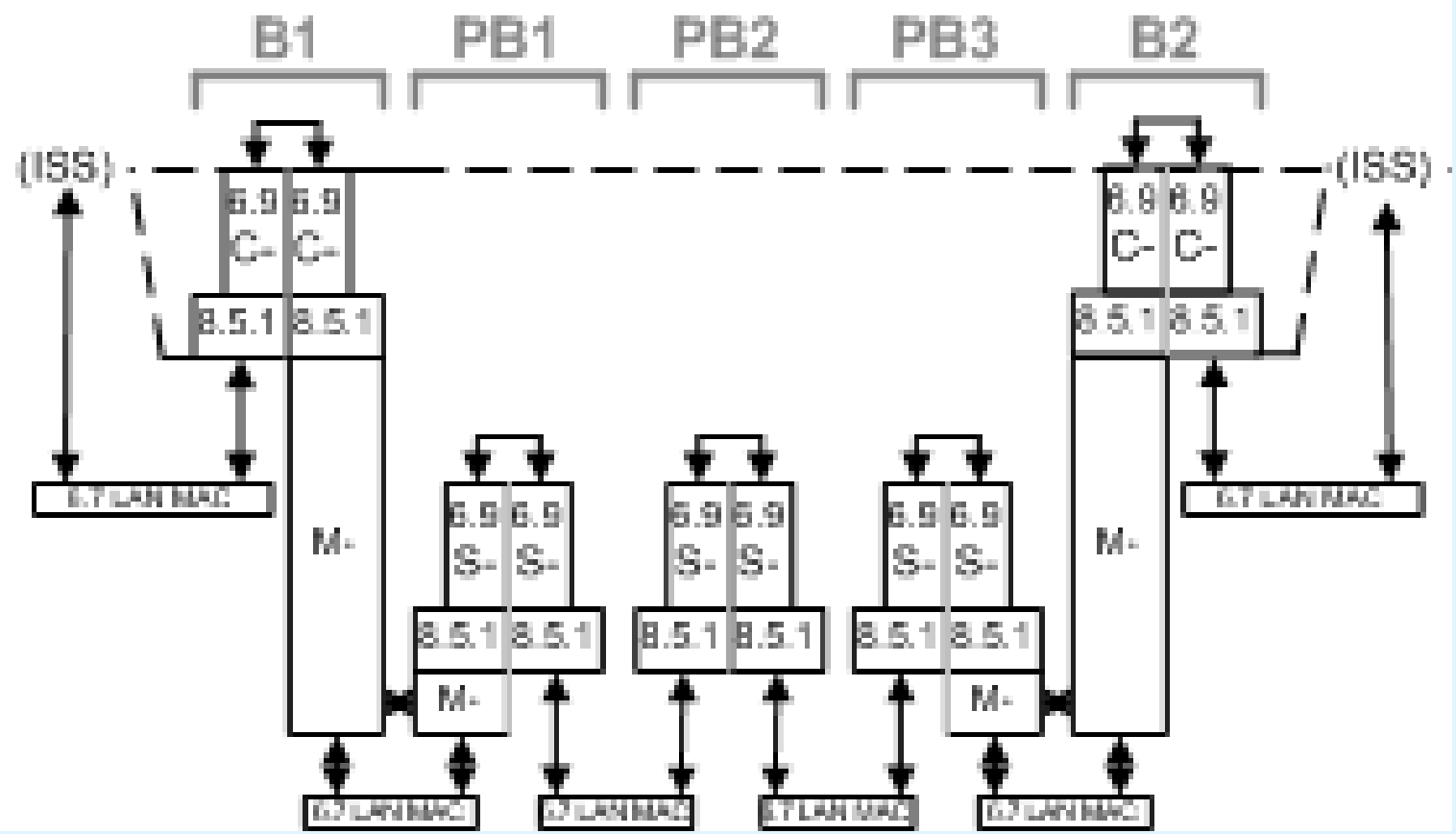


NOTE—This figure has been simplified to show the addition of MACsec functionality as a single shim, comprising both the MAC Security Entity(SecY) that carries out the frame protection and validation operations, and the associated PAE and KaY (see 802.1X-2010) that facilitate authentication and key agreement. The latter make use of an Uncontrolled Port provided by the SecY. This figure and similar figures in this note show only each SecY's Common Port (below MACsec) and its Controlled Port (above MACsec) and allows communication between peer PAEs and KaYs to be shown as communication between peer MACsec entities.

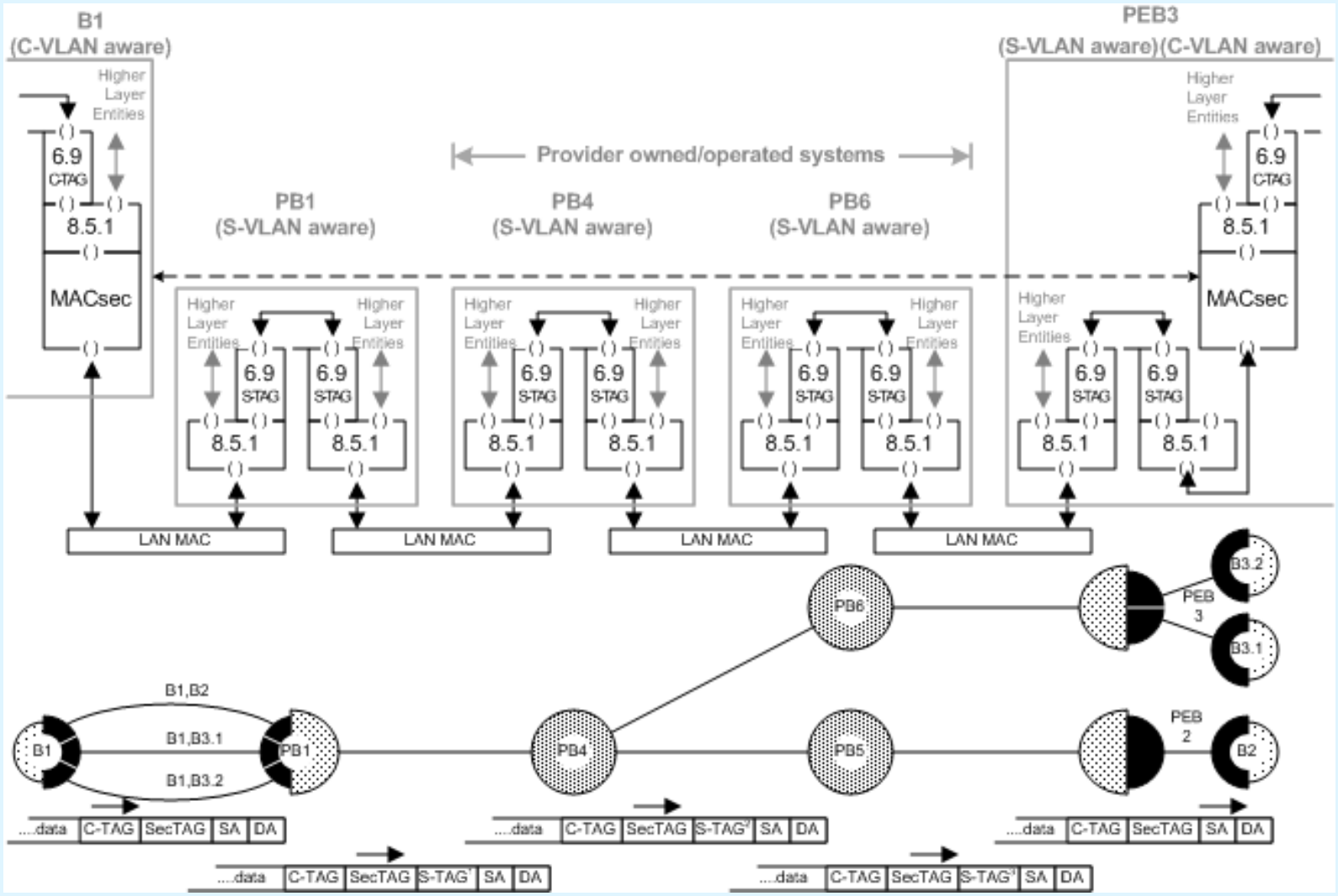
Protection across a provider network



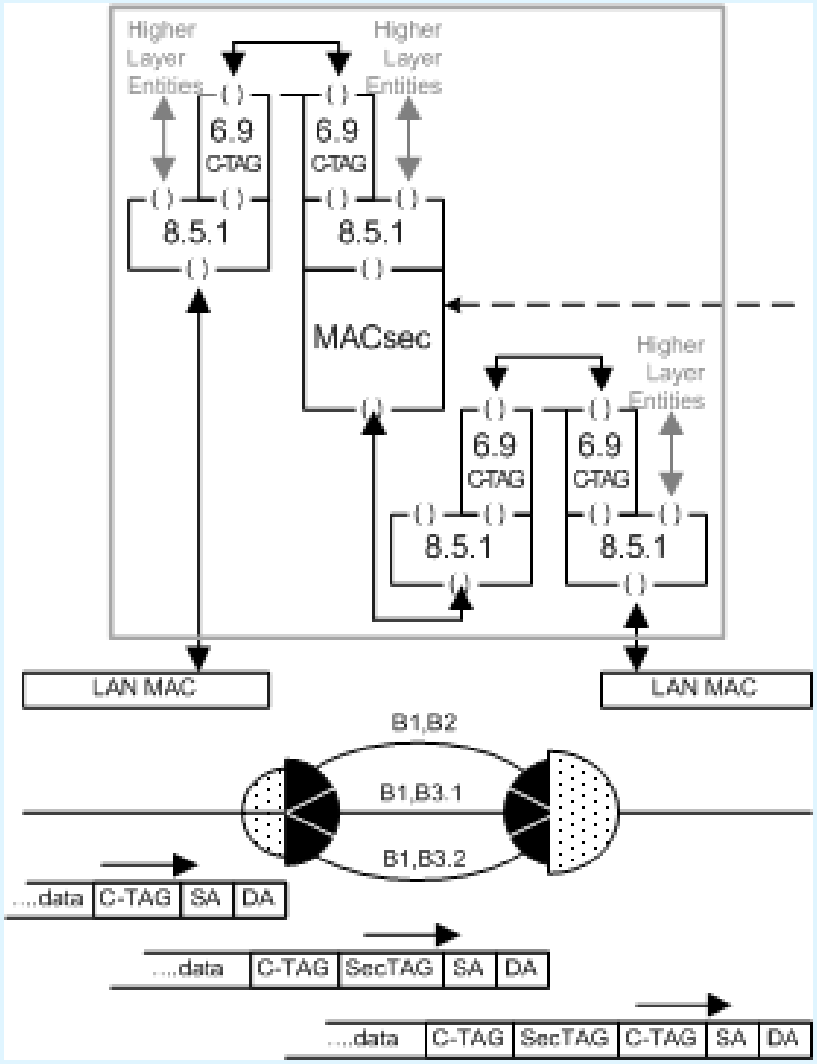
Protecting access to a provider network



Integrated Operation (example)



Transparent operation (example)



An EDE classification scheme

- EDE-<red-side VLAN TAG><black-side VLAN tag>

For example:

- EDE-CS

Customer service selection via C-TAG, MACsec added, then S-TAG to select provider service

- EDE-CC

Customer service selection via C-TAG, MACsec added, then C-TAG to select provider service

- EDE-BC

Customer BEB added I & B-TAG, B-TAG service selection, MACsec provides confidentiality of original C-DA, C-SA, then C-TAG selects provider service

- EDE-T

A TPMR with black-side MACsec, no VLAN TAG processing

Addressing for transparent operation

- EAPOL frames (carrying EAP+MKA) currently use Reserved Addresses
- Prevents accidental/undesirable creation of multi-hop MACsec tunnels
- Demand for additional Reserved Addresses for transparent EDE pairs undesirable
- Transparent EDEs always two-port red/black, discarding self-addressed EAPOL frames received on red-side
- Makes additional reserved addresses unnecessary, but standard allocation still desirable
- Specify with care : May be enough rope for some to shoot themselves in the foot

Missing interface(s) in .1Q ?

- PBBN specifies S-tagged interface, but leaves C-tagged i/f to readers imagination
- Is there any other guidance we should be providing about PBN or PBBN use?
- Integrated operation
- T

A.O.B

- ?