Reserved addresses for P802.1AEcg

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

.../docs2015/ae-seaman-ede-interop-1115-v05.pdf

Latest draft P802.1AEcg D0.7

Mick Seaman

11/6/2015

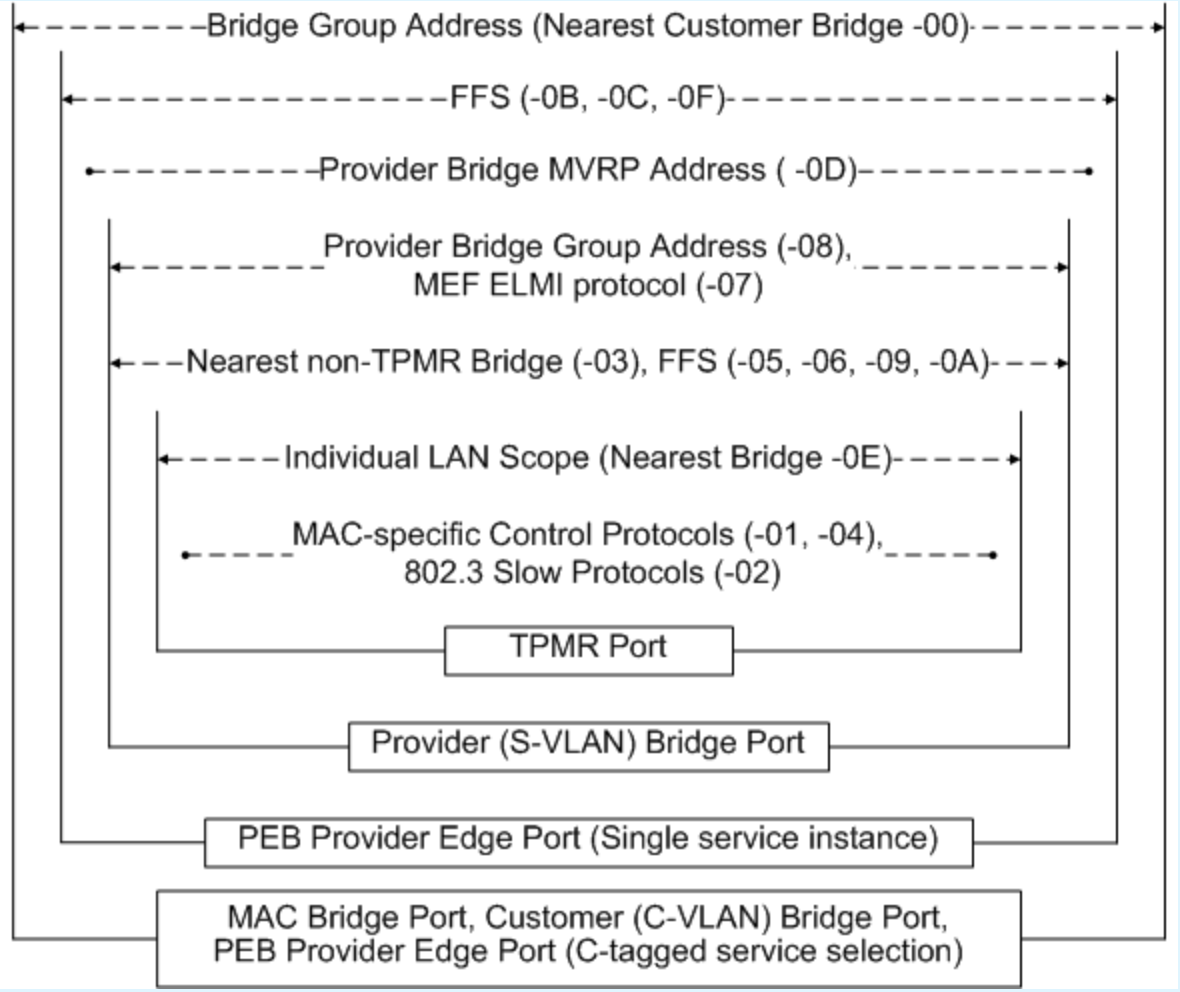
EDE specification objectives

- Maximal use of existing standards
- Minimal interference in unrelated issues
  - Could assemble an EDE out of existing bridges (except for address use by .1X)
- Integrated operation
  - Peering with existing spec MACsec-capable bridges
- And transparent operation
  - Add to, and secure, existing bridged network

Why allocate Reserved Addresses

- EAPOL frames (carrying EAP+MKA) currently use Reserved Addresses
- Prevents accidental/undesirable creation of multi-hop MACsec tunnels, blinding peers along path
- EDE ‘drop in’ requirement, don’t rely on rest of network to prevent undesirable behavior
- Why now – have to produce .1AEcg draft with address properties – limited choice of candidates so ‘allocate later’ not effective

Reserved address use today



EDE-M PAE addressing choices

- .1X PAE Address (-03, aka nearest non-TPMR)
  - ✓ Interoperates with existing MACsec-capable Customer and Provider Bridges, and EDE-Ms on same LAN
  - ✓ Interoperates with PEB port for i/f access protection
- Nearest Customer Bridge address (-00)
  - ✓ Interoperates with existing MACsec-capable Customer Bridges and EDE-Ms over PBN single service instance
  - ✓ Interoperates with EDE-CS hub over PBN
- EDE-CC PAE address (see slide 6)
  - ✓ Interoperates with EDE-CC hub over PBN
- Allow configuration (-03, -00, or EDE-CC address)

EDE-CS PEP addressing choices

- Nearest Customer Bridge address (-00)
  - Interoperates with other EDE-CSs
  - Interoperates with MACsec Customer Bridges attached to untagged PBN port i/f's or single service instance
- EDE-CC PEP Address (see slide 6)
  - Interoperates with EDE-CCs (single VLAN/service)

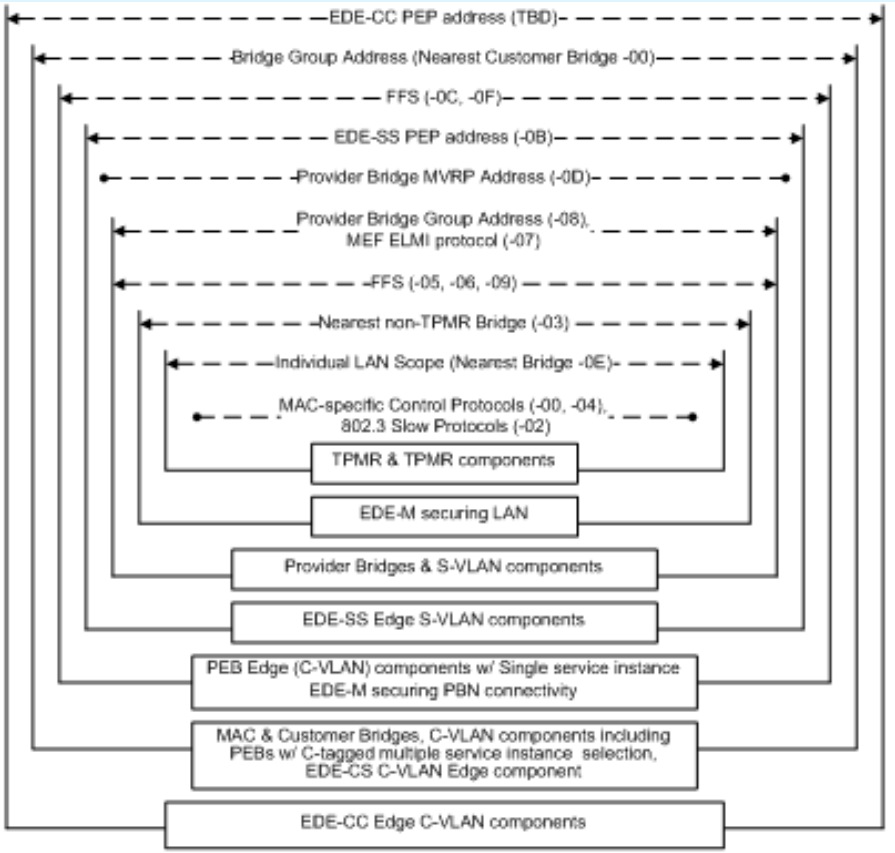
EDE-CC PEP addressing choices

- New standard group address
  - Not Reserved Address, PEBs need to forward
  - Changing PEBs to forward existing address impractical
  - Configuring bridges in Customer Network to filter would help prevent misconfiguration, though not essential
- One PEP might secure mgt connectivity to PEB i/f
  - Would require explicit PEB support, -03 address suitable
  - Specify -07 (ELMI) forwarding by EDE components

Address requirements – EDE-SS's

- New allocation (-0B)
  - Needs to pass through Provider Bridges
  - Needs to be filtered by C-VLAN components/Bridges
  - Needs to be different from EDE-CS and EDE-CC PAE addresses

Reserved addresses with EDEs



802.1Q Reserved addresses are the block of 16 beginning 01-80-C2-00-00-00

Addresses (inc. -07) are not assigned for the exclusive use of particular protocols, EtherTypes are required, as other protocols can use each address, with possible constraints (e.g. for -02).

The Provider Bridge MVRP Address (-0D) is filtered by S-VLAN components using MVRP as well as by C-VLAN components, so may not reach the latter.

EDE's also enforce frame scoping—discarding all frames that are not sent by CA participants, both when connectivity is secured and when not (unless unsecured connectivity is permitted).