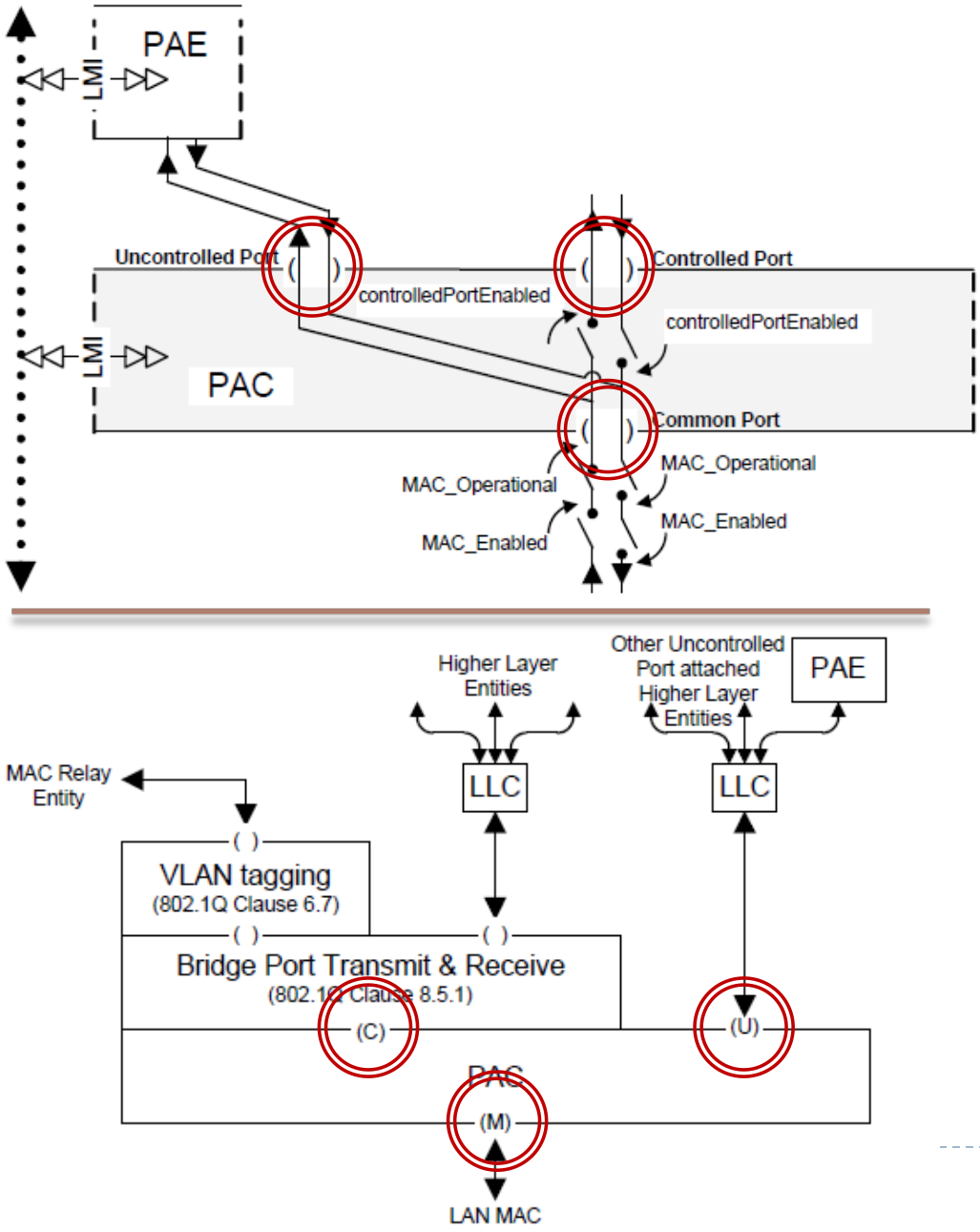
802.1X Entity Interfaces

IEEE 802.1 YANG Data Model
Marc Holness
May 2015

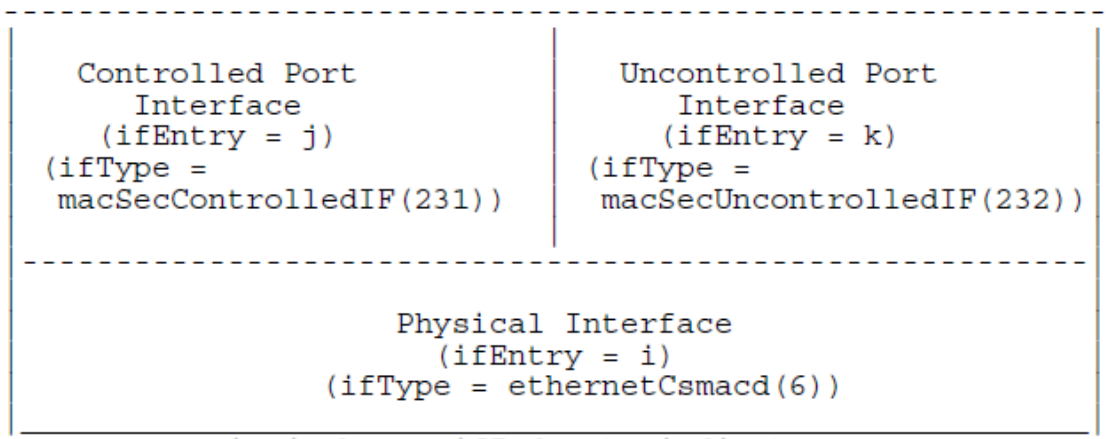
Port access entity and Port access controller



- The PAE (Port Access Entity) is the protocol entity associated with a Port
  - It can support the protocol functionality associated with the Authenticator, the Supplicant, or both
- The PAE attaches to an UNCONTROLLED PORT, provided by the PAC to support the authentication exchange prior to authorizing use of the CONTROLLED PORT
- MAC_Operational for the UNCONTROLLED PORT is set True if and only if it is True for the COMMON PORT
- MAC_Operational for the CONTROLLED PORT is set True if and only if MAC_Operational for the COMMON PORT is True and controlledPortEnabled is set

Port access controller

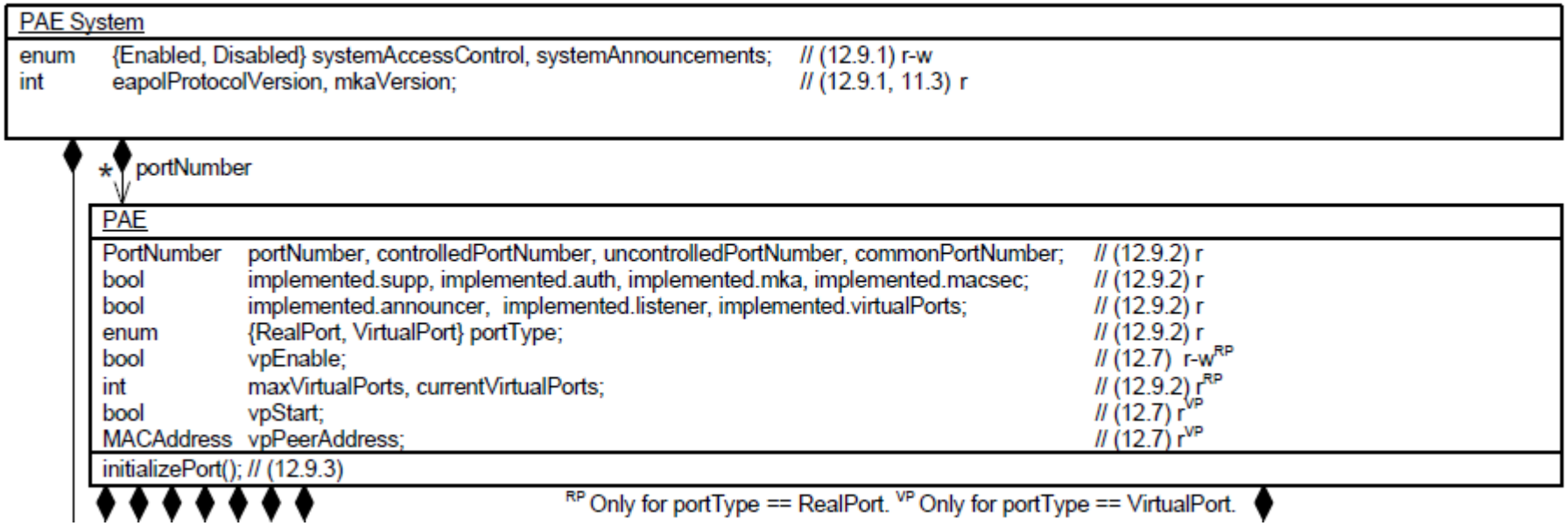
- The PAC (Port Access Controller), is a protocol-less shim that provides control over frame transmission and reception by clients attached to its CONTROLLED PORT, and uses the MAC Service provided by a COMMON PORT
- The access control decision is made by the PAE, typically taking into account the success or failure of mutual authentication and authorization of the PAE's peer(s), and is communicated by the PAE using the LMI to set the PAC's CONTROLLED PORT enabled/disable.
- The CONTROLLED PORT is the service point to provide one instance of the secure MAC service in a PAC
- The UNCONTROLLED PORT is the service point to provide one instance of the insecure MAC service in a PAC



i, j, k are ifIndex to indicate an interface stack in the ifTable.

Figure : PAC Interface Stack

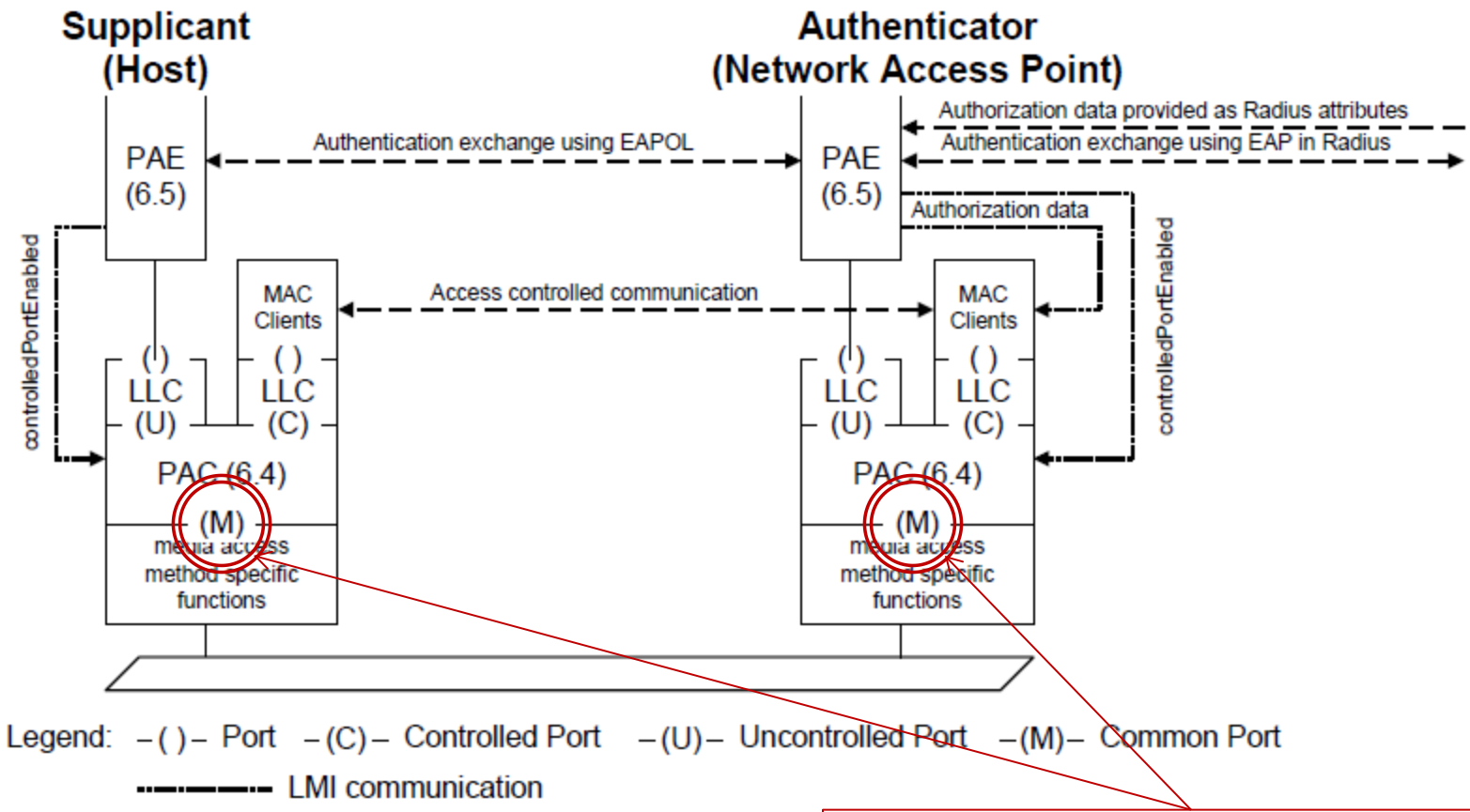
PAE identification



PortNumber:

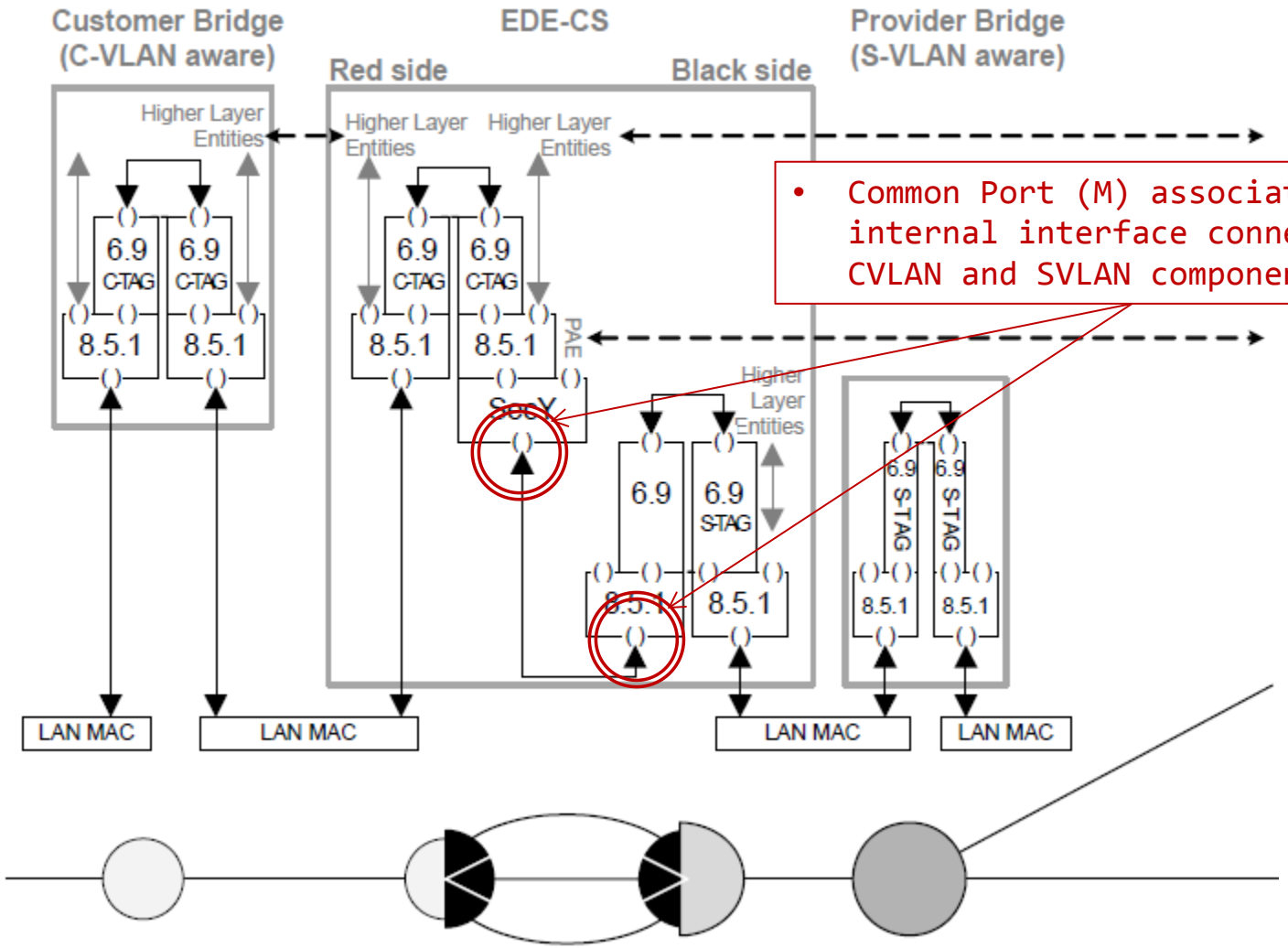
- Each PAE is uniquely identified by a port number
  - The port number used is unique amongst all port numbers for the system, and directly or indirectly identifies the UNCONTROLLED PORT that supports the PAE
- If the PAE has been dynamically instantiated to support an existing or potential virtual port, this *portNumber*, the *uncontrolledPortNumber* and the *controlledPortNumber* are allocated by the real port's PAE, and this *portNumber* is the *uncontrolledPortNumber*
- If the PAE supports a real port, this *portNumber* is the *commonPortNumber* for the associated PAC or SecY

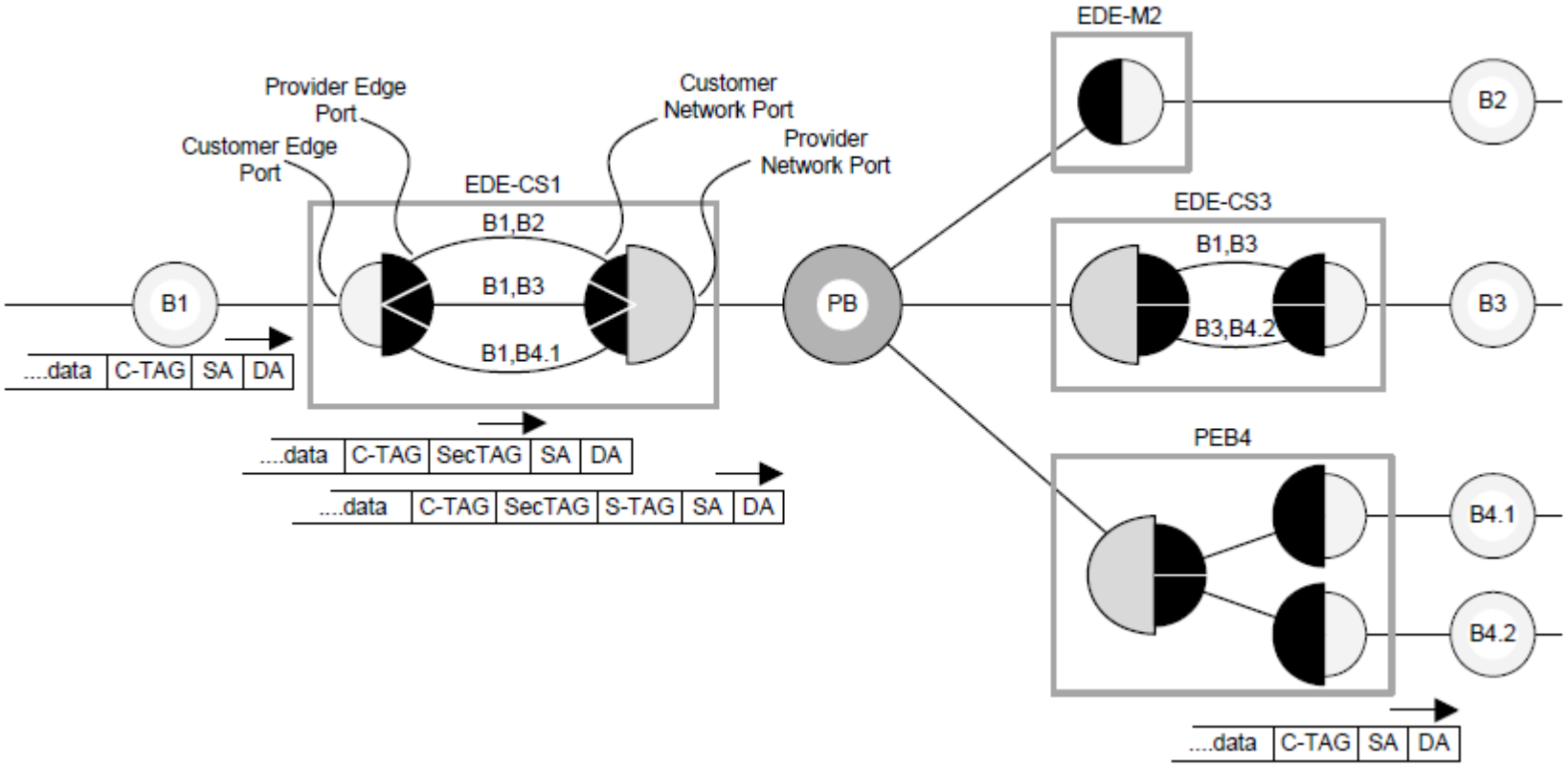
Network access control with a physically secure point-to-point LAN



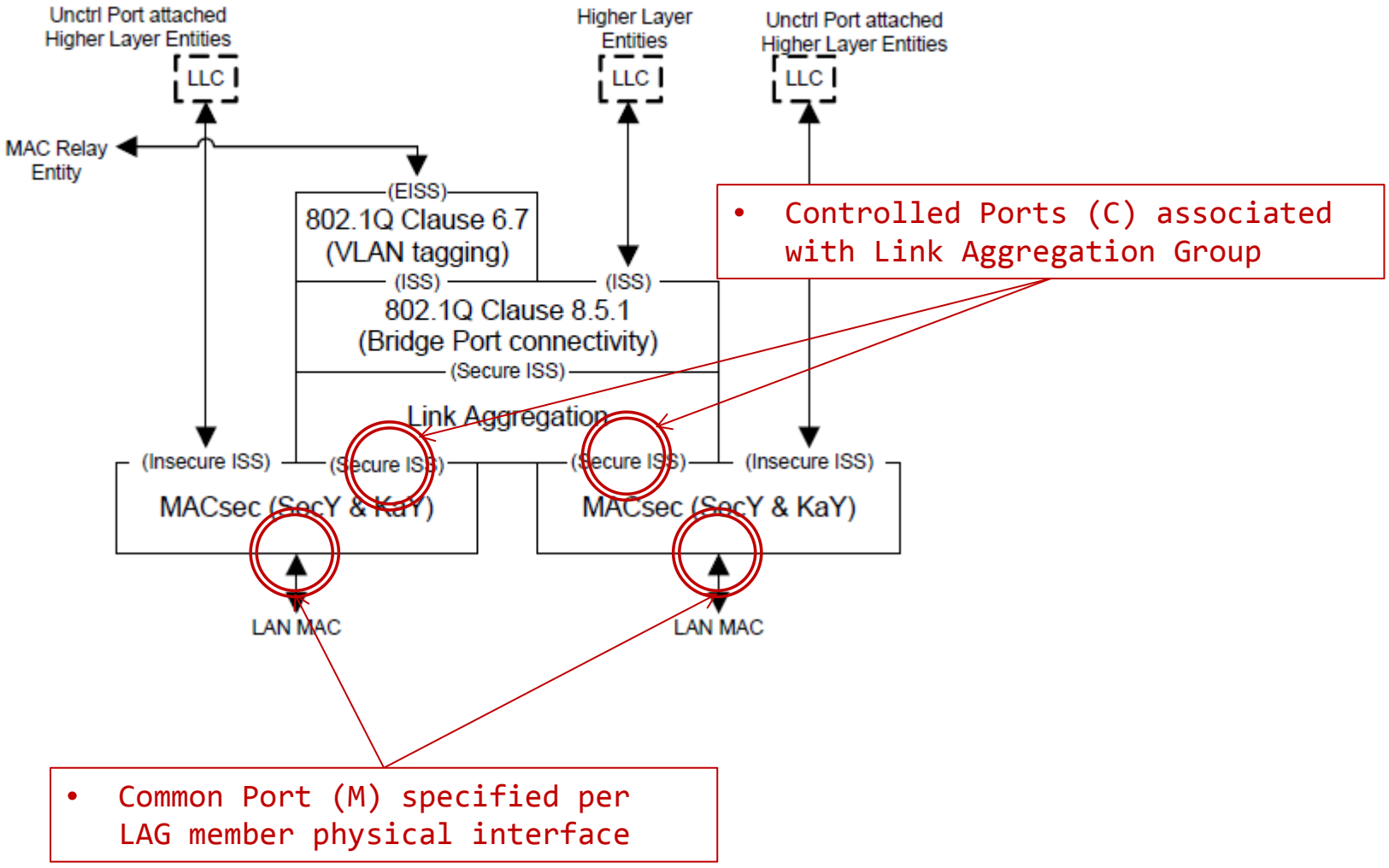
- Common Port (M) could be considered an augmentation of the Interface associated with the physical port.

EDE-CS connected to a PBN S-tagged interface

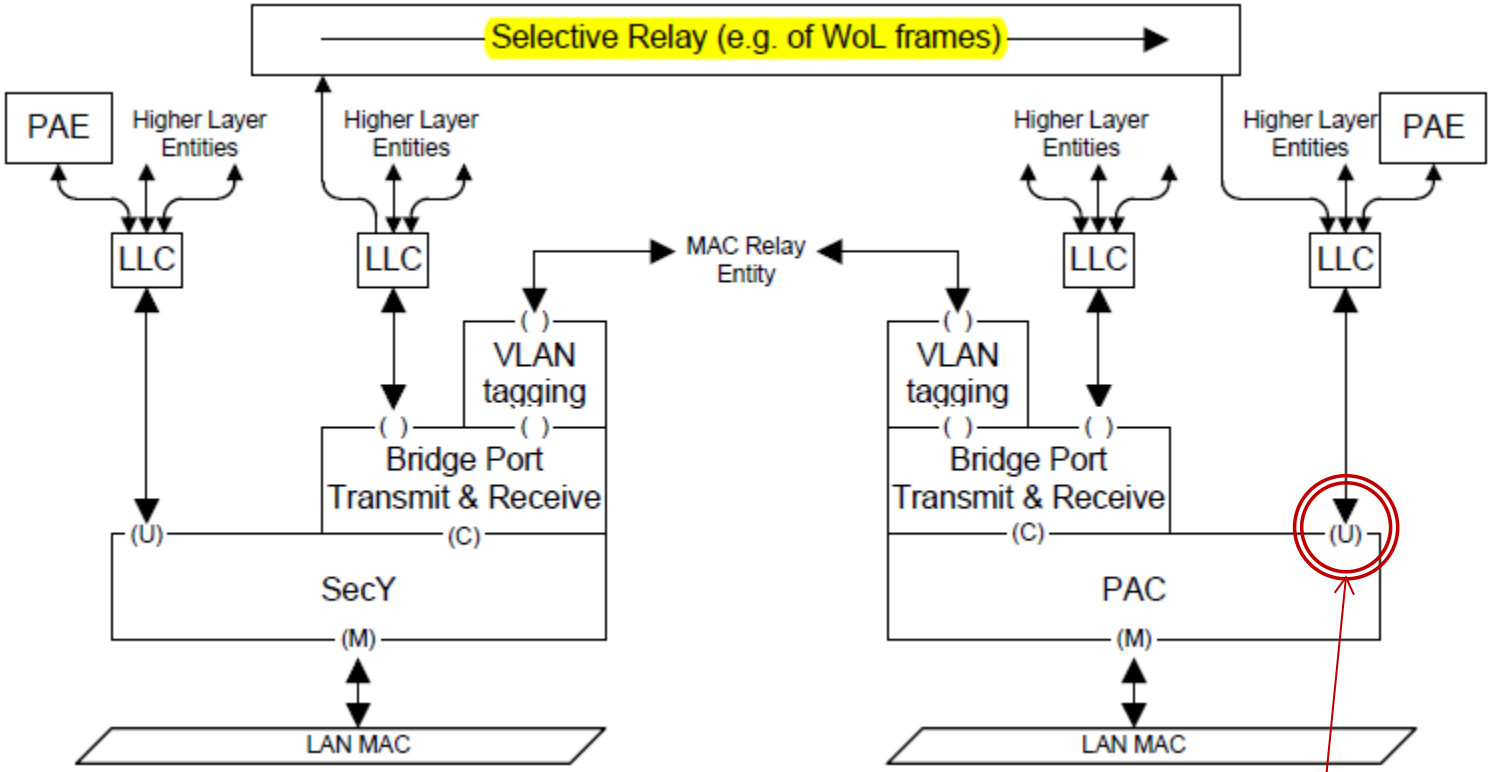



EDE-M2
B2
Provider Edge Port
Customer Edge Port
Customer Network Port
Provider Network Port
EDE-CS1
B1,B2
B1,B3
B1,B4.1
EDE-CS3
B1,B3
B3,B4.2
B1
PB
B3
PEB4
B4.1
B4.2
....data
C-TAG
SA
DA
....data
C-TAG
SecTAG
SA
DA
....data
C-TAG
SecTAG
S-TAG
SA
DA
....data
C-TAG
SA
DA

IEEE 802.1Q VLAN-aware Bridge Port (LAG) with MACsec

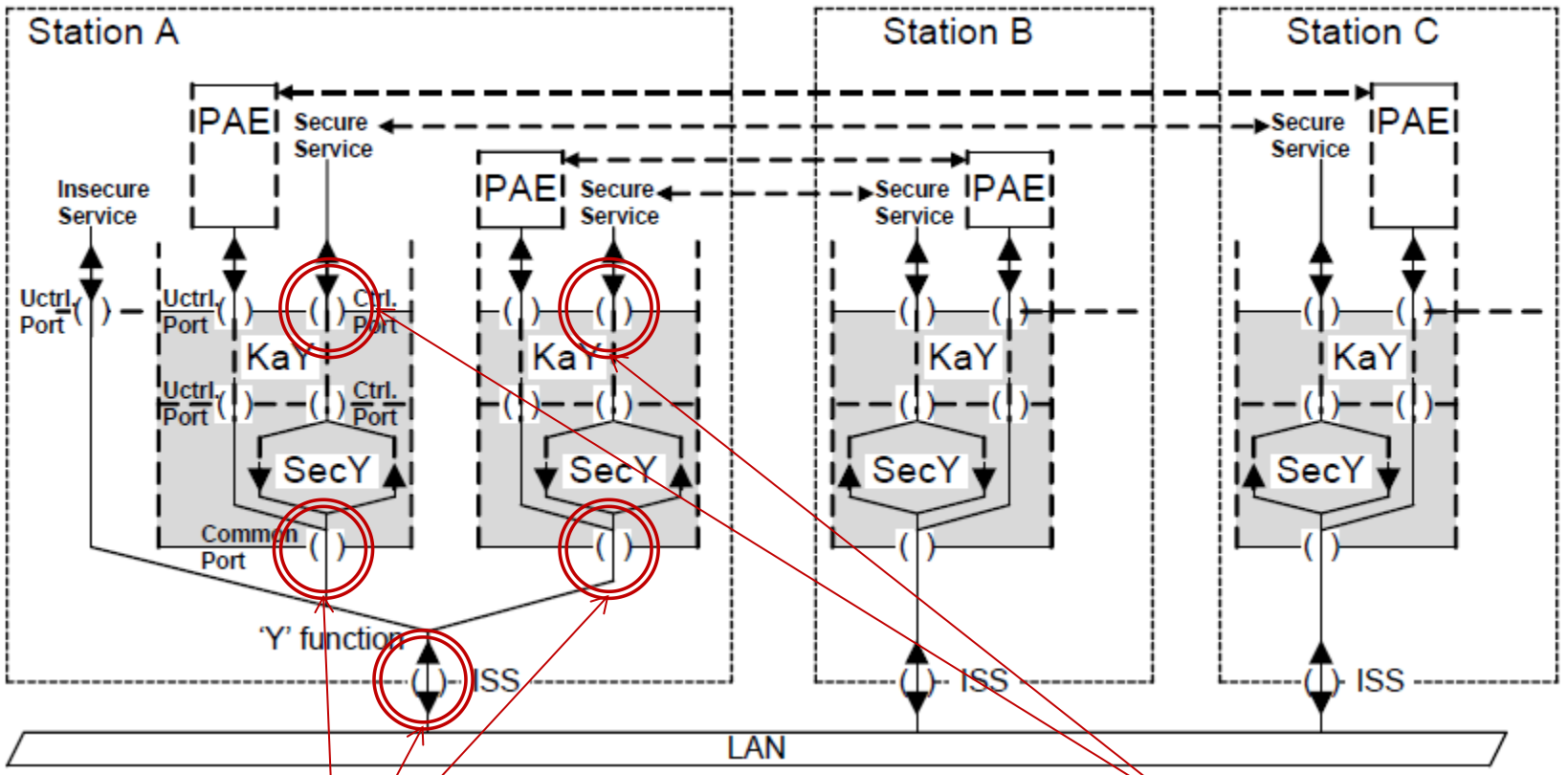


Selective relay to a physically secured unauthenticated port



- Uncontrolled Port (U) could be associated with a PAE or another application (e.g., Wake-on-LAN)

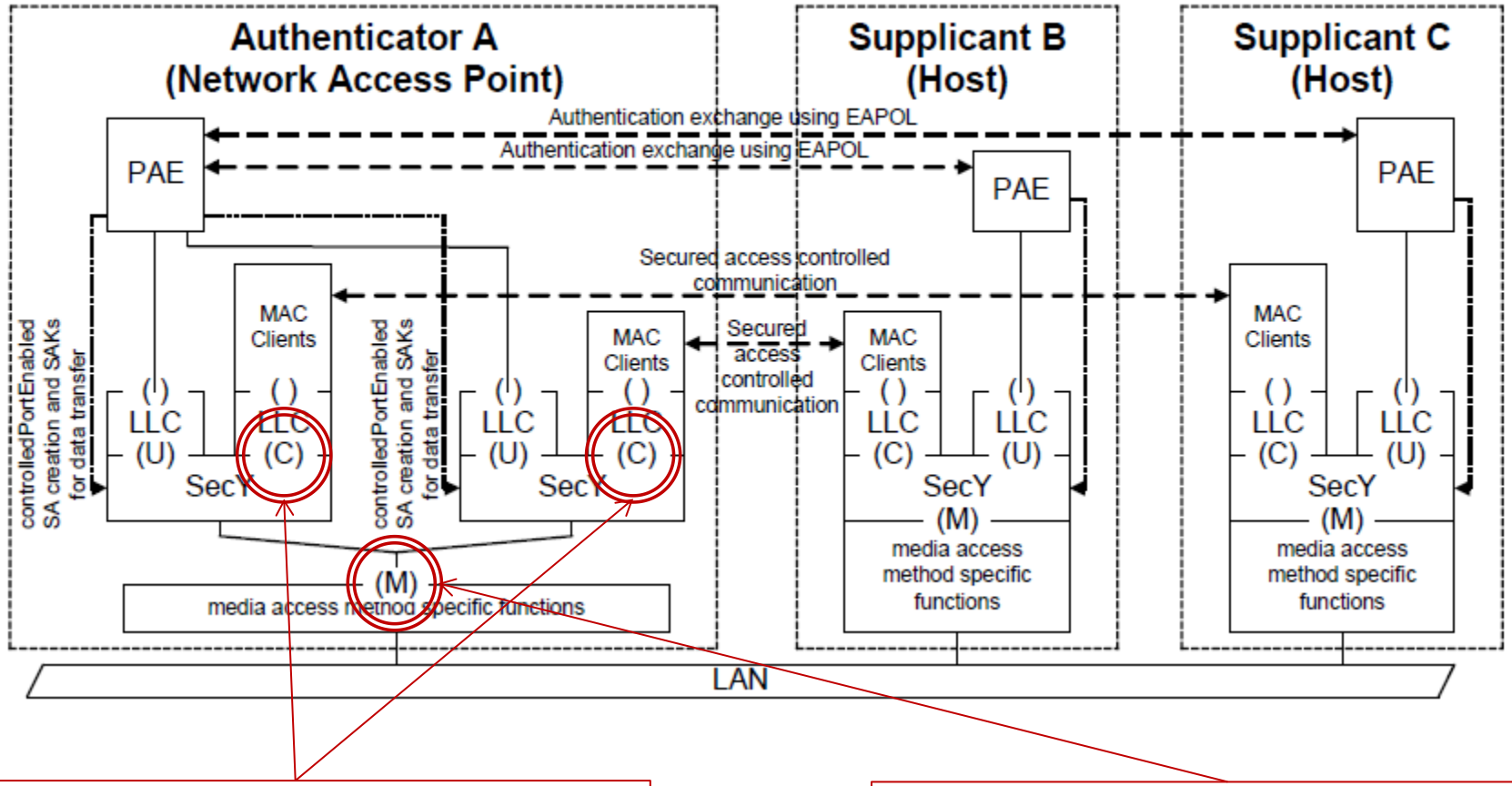
An example multi-access LAN



- Essentially, a single COMMON PORT (M) used by each instance over the LAN

- Multiple CONTROLLED PORTS (C) defined. Essentially, a (C) per virtual port

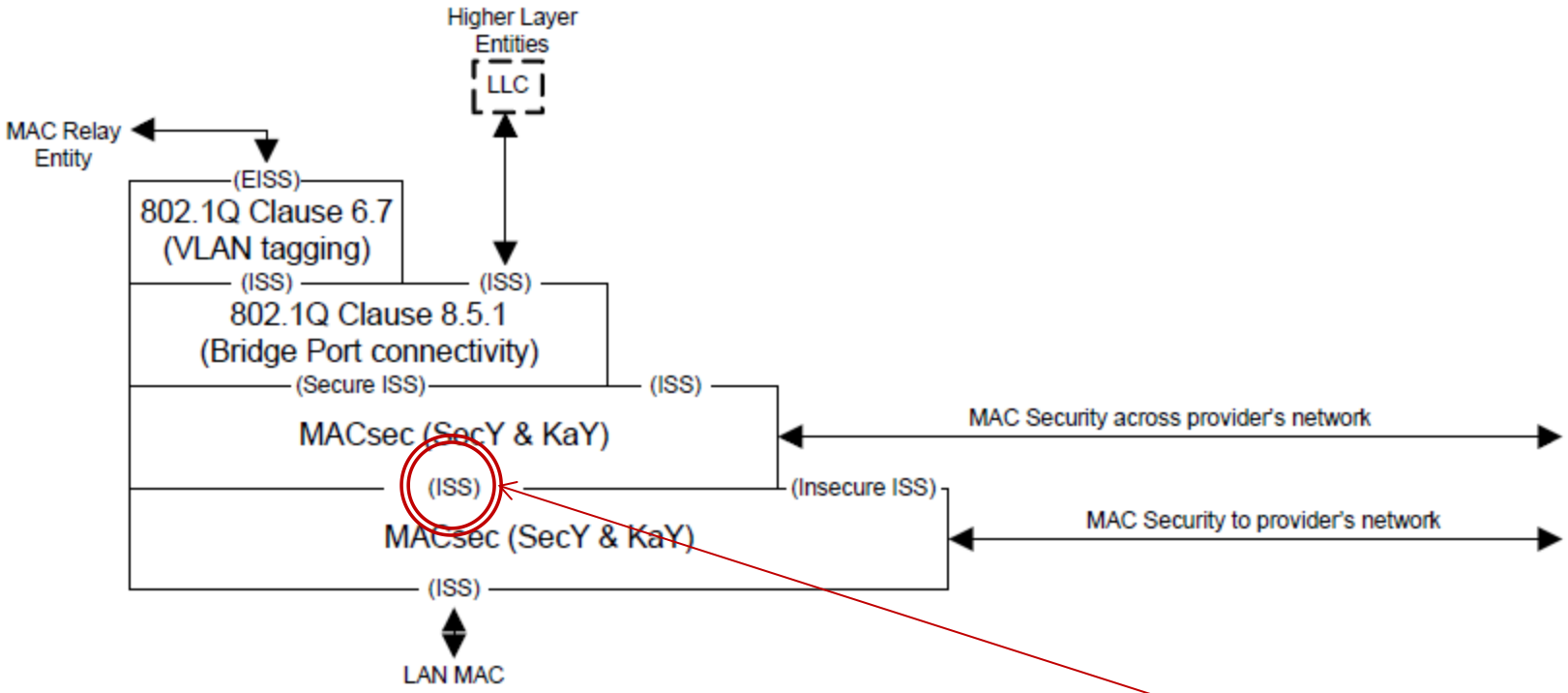
Network access control with MACsec and a multi-access LAN



- Multiple Controlled Ports (C) defined. Essentially, a (C) per virtual port

- Single Common Port (M) supported via the LAN connection

Interface stack for MAC Security to and across provider's network



- The upper layer COMMON PORT (M) is associated with the lower layer CONTROLLED PORT (C)

Secure PBN transit and access with priority selection