THOUGHTS ON TSN SECURITY

Contributed by

Philippe Klein, PhD (philippe@broadcom.com)

METWORK SECURITY PROTOCOLS

		Description	Complexity	Performance
Layer 4..7	**SSL / TLS,…**	▪ Application layer encryption ▪ Client server mode	▪ Security built into the application ▪ Phased deployment difficult ▪ Client initiated ▪ Uses TCP connection oriented protocol	▪ Assumes medium to low performance
Layer 3	**IPsec**	▪ Layer 3 “Network” security ▪ End to End ”tunnels” ▪ Peer to peer Protocol	▪ Complex protocol suite, many options ▪ Key management using IKE protocol and PKI for authentication	▪ Ranges from low to high ▪ Significant header expansion
Layer 2	**MACsec**	▪ **Layer 2 security** ▪ **Hop by hop** ▪ **Peer to peer protocol**	▪ **Relatively simple to implement** ▪ **Phased deployment possible** ▪ **Key management (MKA via 802.1X-2010)**	▪ **Designed for high throughput** ▪ **Minimal header expansion**

MACsec SCOPE

- **IEEE Std 802.1AE (aka MACsec) Media Access Control (MAC) Security**
- **“MAC Security (MACsec) allows authorized systems that attach to and interconnect LANs in a network to maintain confidentiality of transmitted data and to take measures against frames transmitted or modified by unauthorized devices.”**
- **Relationship between IEEE Std 802.1AE and other IEEE 802 standards**
  - IEEE Std 802.1X specifies Port-based Network Access Control, and provides a means of authenticating and authorizing devices attached to a LAN.

WHAT IS MACsec?

- **Hop-to-hop Layer 2 Security**
  - Protects communication between trusted components of the network infrastructure
    - All frames exchanged between the two elements (called SecY) are authenticated and optionally encrypted
  - Controls access to the network when combined with 802.1X
  - Provides source authentication, integrity, and confidentiality using strong crypto (AES-GCM)
- **Secure LANs from attacks of:**
  - Wiretapping (confidentiality)
  - Impersonation (authentication)
  - Masquerading (MAC address spoofing)
  - Man-in-the-Middle attacks
  - Replay attack (authentication + anti-replay counter)
  - Denial-of-Service (DOS) attacks
- **Does not:**
  - Protect against attacks of trusted components themselves
  - Provide end-to-end security
  - Replace 802.11i

SECURE MAC SERVICE RELATIONSHIP

- **Connectivity Associations (CA)**
  - Set of stations that can securely communicate with each other using Secure Channels
- **Secure Channels (SC)**
  - An uni-directional channel identified by an SC Identifier in the packet header used to communicate between stations belonging to the same CA
- **Security Association (SA)**
  - An active key associated for each SC. Standard requires 2 active SAs per SC to support non-interrupting key swap

- **Usage Scenarios**
  - Point to Point LANs
  - Shared Media LANs
  - Provider Bridged Networks

2_STATION SC

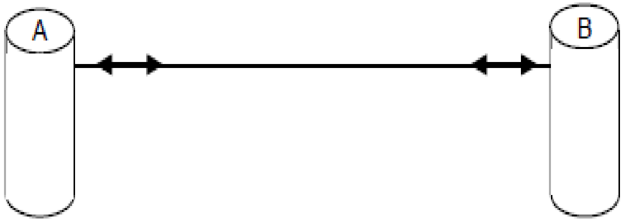


Figure 7-1—Two stations connected by a point-to-point LAN

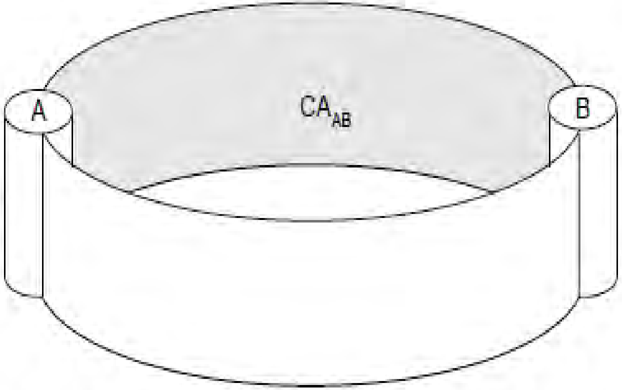


Figure 7-2—Two stations in a CA created by MACsec Key Agreement

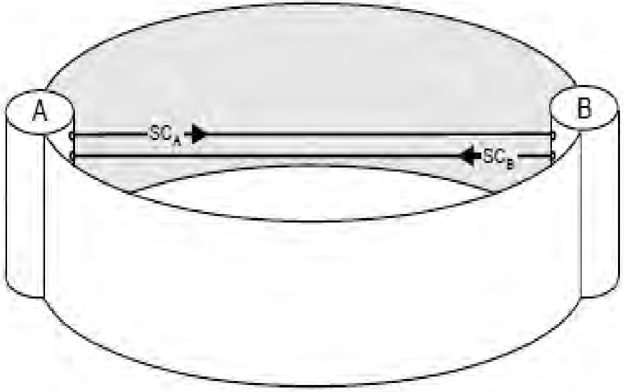


Figure 7-3—Secure communication between two stations

3_STATION SC

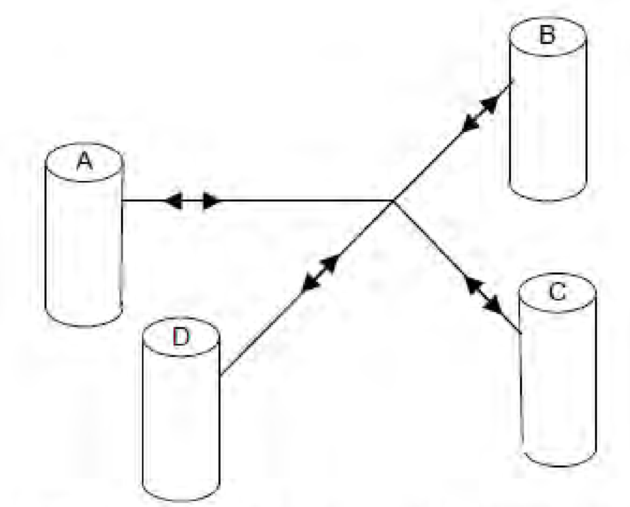


Figure 7-4—Four stations attached to a shared media LAN

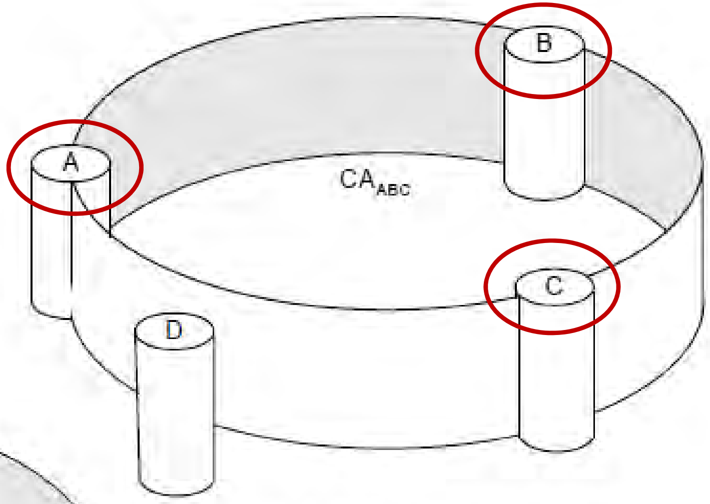


Figure 7-5—A CA including ports A, B, and C

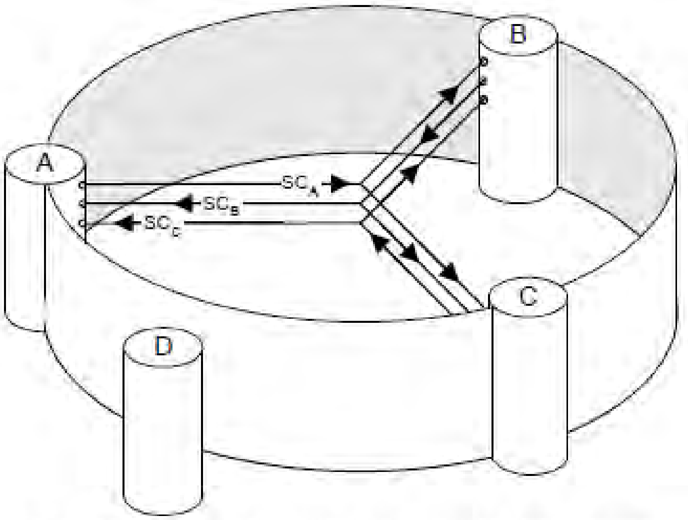
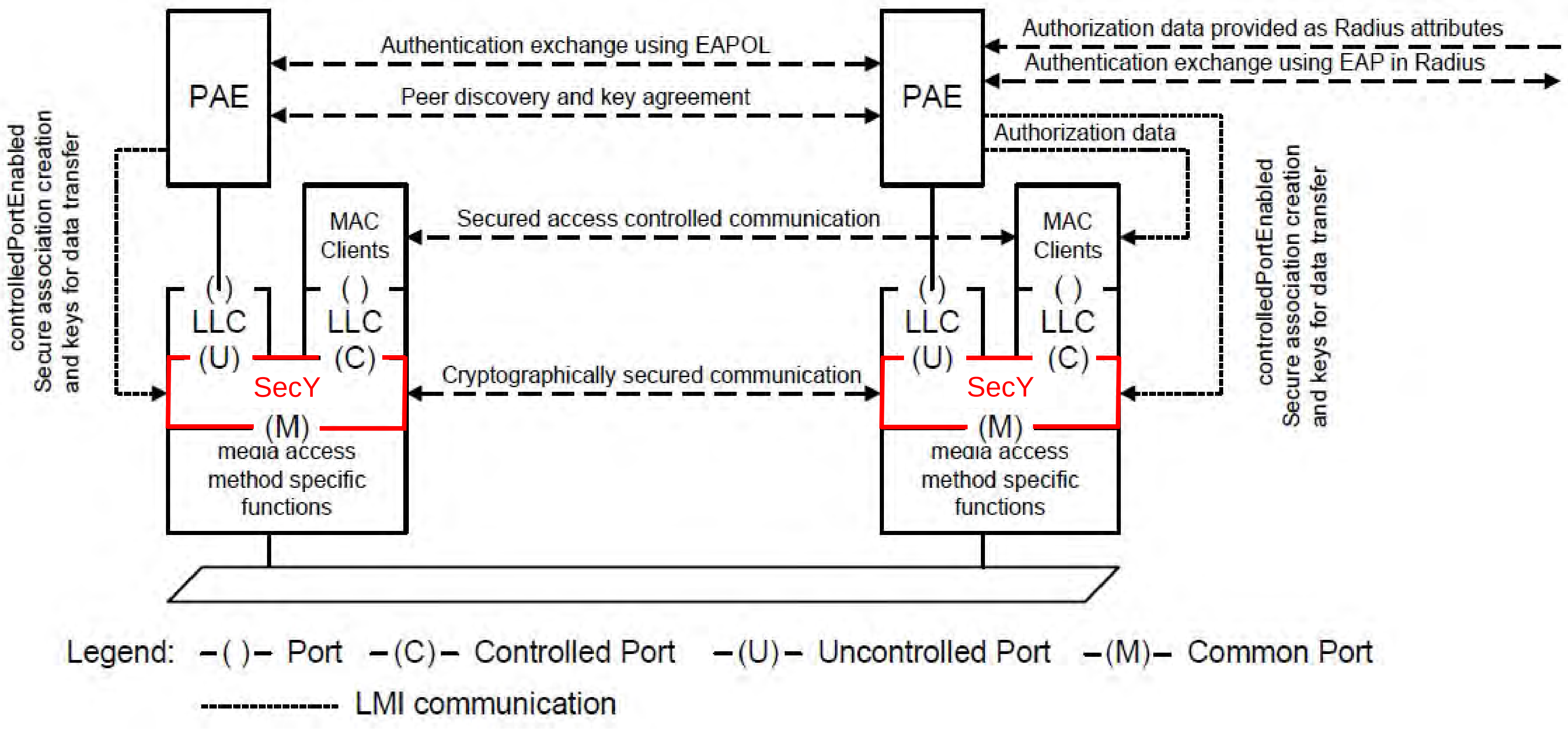


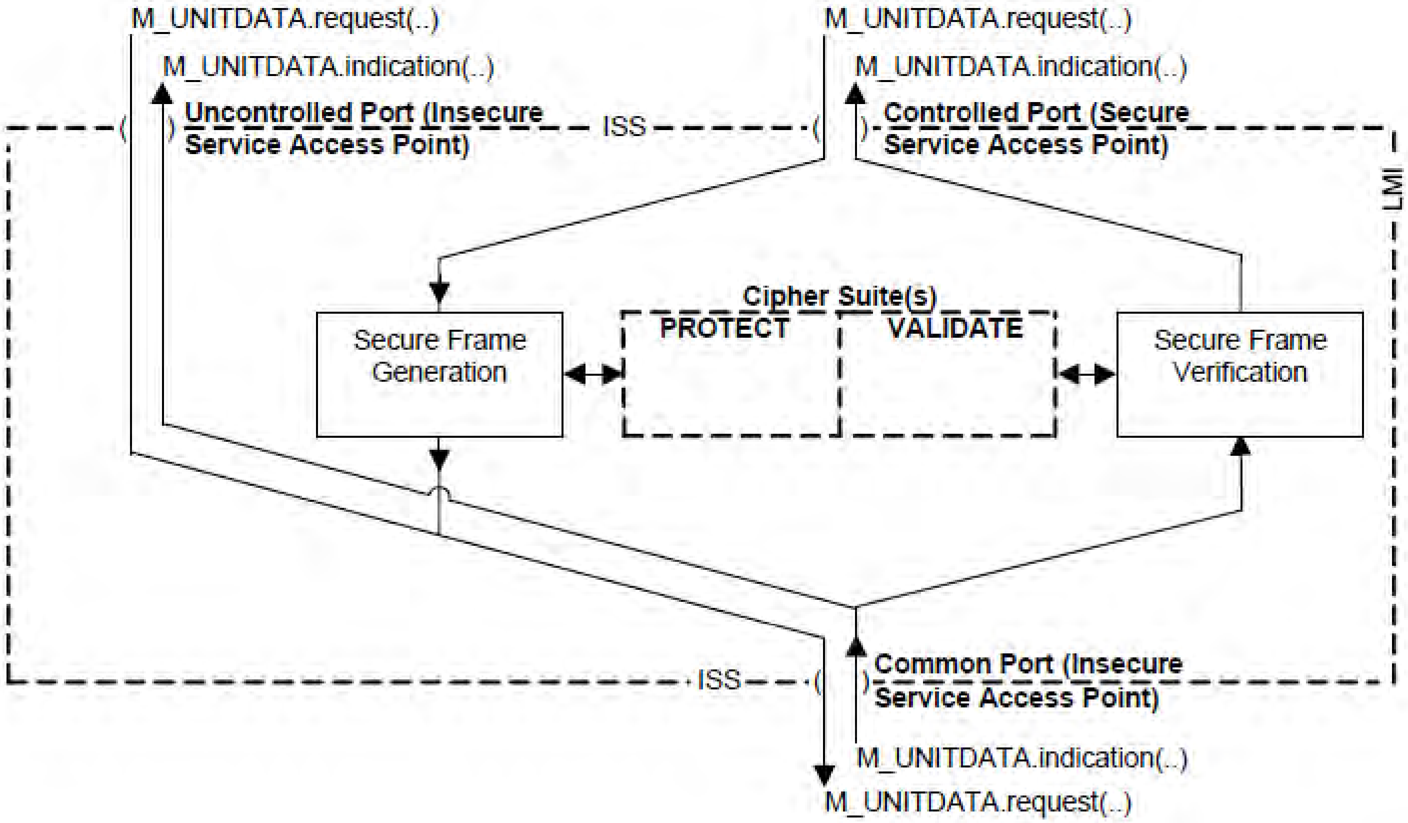
Figure 7-6—Secure communication between three stations

MACsec - ENCRYPTION

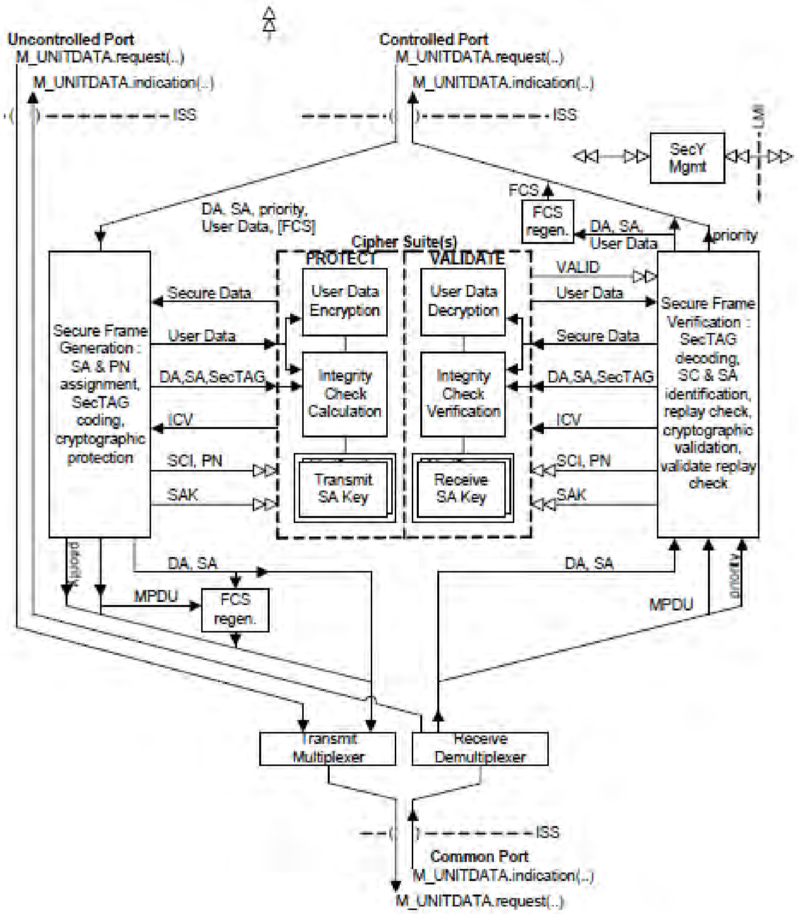
MACsec MODEL


controlledPortEnabled
Secure association creation
and keys for data transfer
PAE
Authentication exchange using EAPOL
Peer discovery and key agreement
PAE
Authorization data provided as Radius attributes
Authentication exchange using EAP in Radius
Authorization data
MAC Clients
Secured access controlled communication
MAC Clients
( )
LLC
(U)
( )
LLC
(C)
SecY
(M)
media access method specific functions
Cryptographically secured communication
( )
LLC
(U)
( )
LLC
(C)
SecY
(M)
media access method specific functions
controlledPortEnabled
Secure association creation
and keys for data transfer
Legend:
–( )– Port
–(C)– Controlled Port
–(U)– Uncontrolled Port
–(M)– Common Port
LMI communication

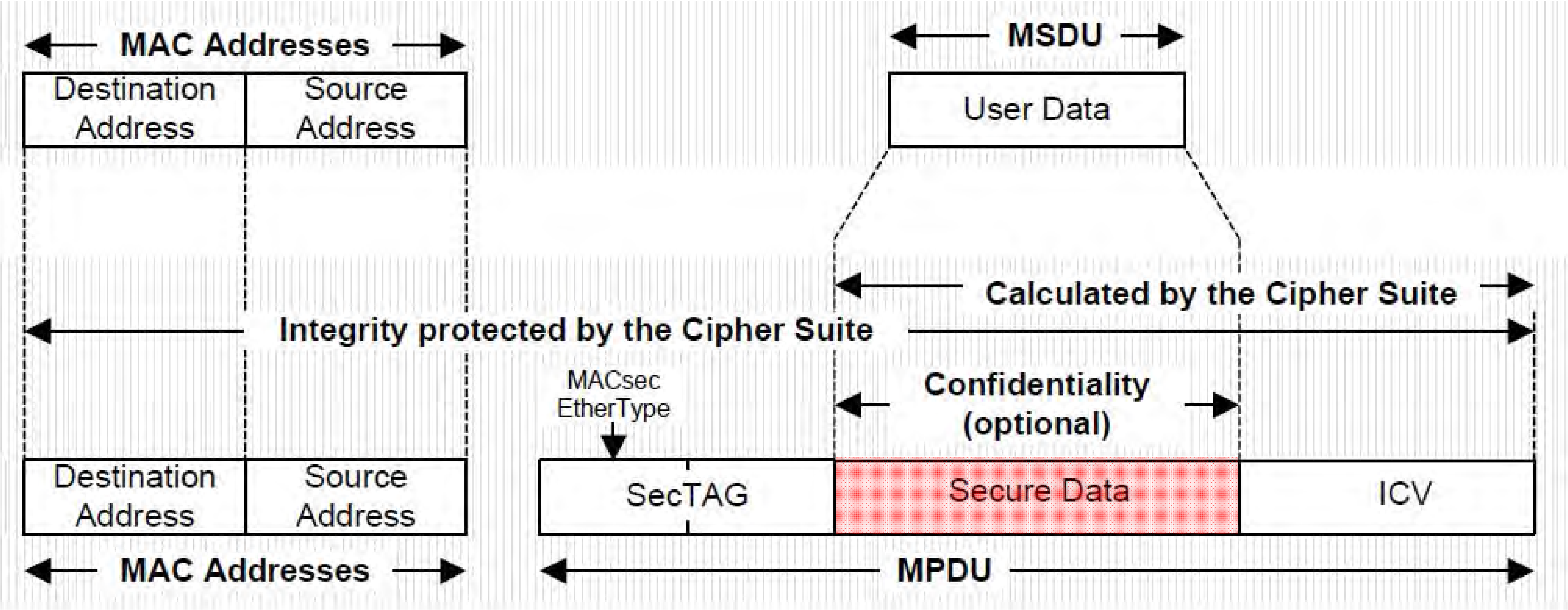
SecY – MAC Security Entity


M_UNITDATA.request(..)
M_UNITDATA.indication(..)
Uncontrolled Port (Insecure Service Access Point)
ISS
M_UNITDATA.request(..)
M_UNITDATA.indication(..)
Controlled Port (Secure Service Access Point)
LMI
Cipher Suite(s)
PROTECT
VALIDATE
Secure Frame Generation
Secure Frame Verification
ISS
Common Port (Insecure Service Access Point)
M_UNITDATA.indication(..)
M_UNITDATA.request(..)

SecY ARCHITECTURE & OPERATION

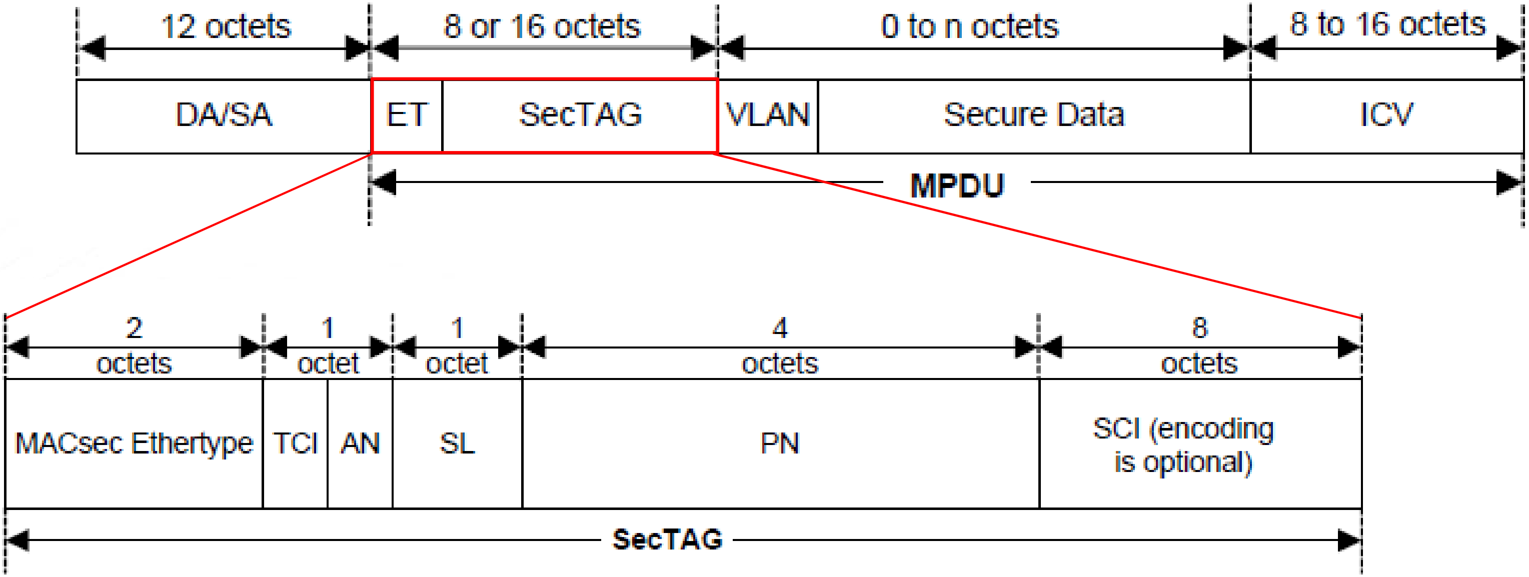


MACsec ENCRYPTION



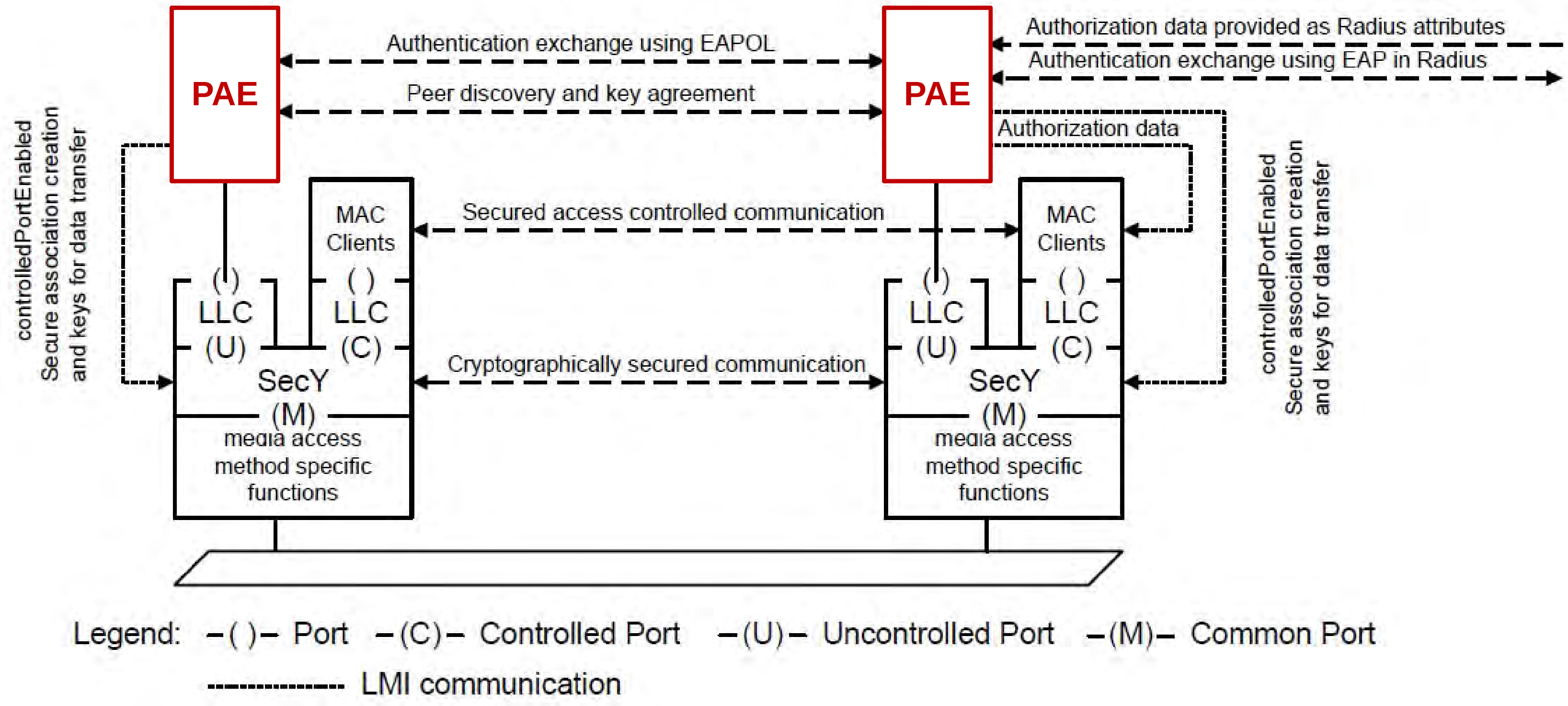
- **Cypher Suite: 128 or 256 AES-GCM (Galois/Counter Mode)**

SecTAG


12 octets
8 or 16 octets
0 to n octets
8 to 16 octets
DA/SA
ET
SecTAG
VLAN
Secure Data
ICV
MPDU
2 octets
1 octet
1 octet
4 octets
8 octets
MACsec Ethertype
TCI
AN
SL
PN
SCI (encoding is optional)
SecTAG

MACsec - AUTHENTICATION

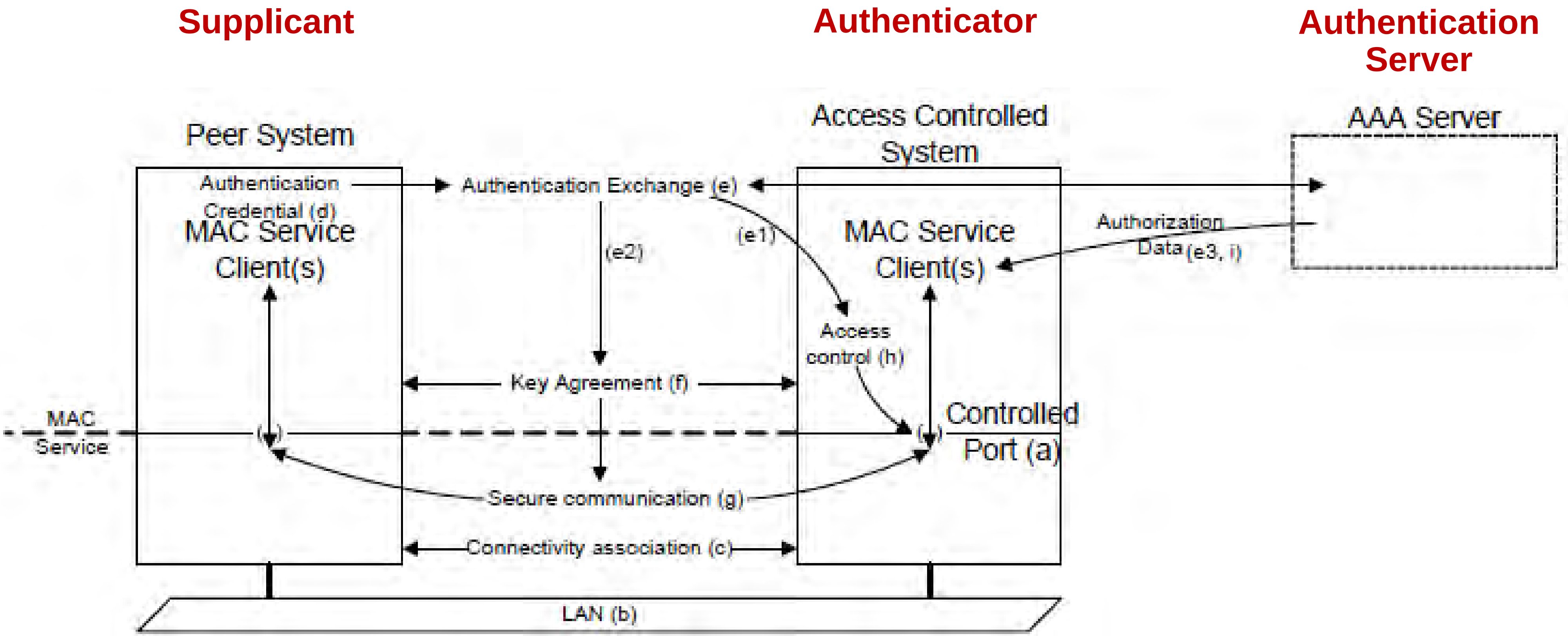
MACsec FRAME CRYPTOGRAPHIC PROTECTION



PAE
PAE
Authentication exchange using EAPOL
Peer discovery and key agreement
Authorization data provided as Radius attributes
Authentication exchange using EAP in Radius
Authorization data
controlledPortEnabled
Secure association creation
and keys for data transfer
MAC Clients
( )
LLC
(U)
LLC
(C)
SecY
(M)
media access method specific functions
Secured access controlled communication
Cryptographically secured communication
Legend: –( )– Port –(C)– Controlled Port –(U)– Uncontrolled Port –(M)– Common Port
LMI communication

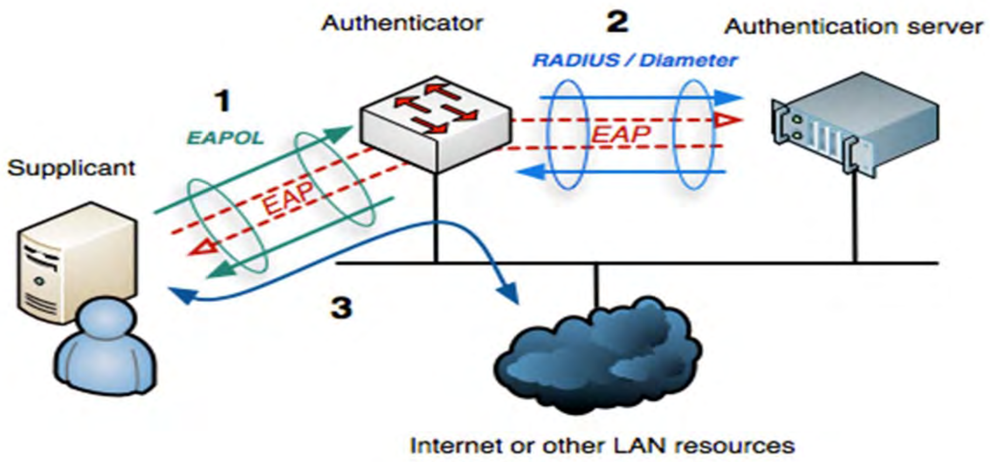
- 802.X authentication is used to authenticate end stations
- MKA (MACsec Key Agreement) Protocol is used to exchange session keys based on CA Key

IEEE Std 802.1X - PORT BASED NETWORK ACCESS CONTROL



IEEE 802.1 Plenary Meeting, Berlin, March 2015

802.1X EAP (EXTENSIBLE AUTHENTICATION PROTOCOL)



- **Define a frameset to allow different Authentication METHODs**
  - Pre shared keys,
  - Certificates,
  - Passwords,
  - SIM credentials,
  - Biometrics,….
- **AEPol/AEPoW : define container messages to carry the authentication protocol over wired and wireless links**

IEEE 802.1X MKA KEY DISTRIBUTION

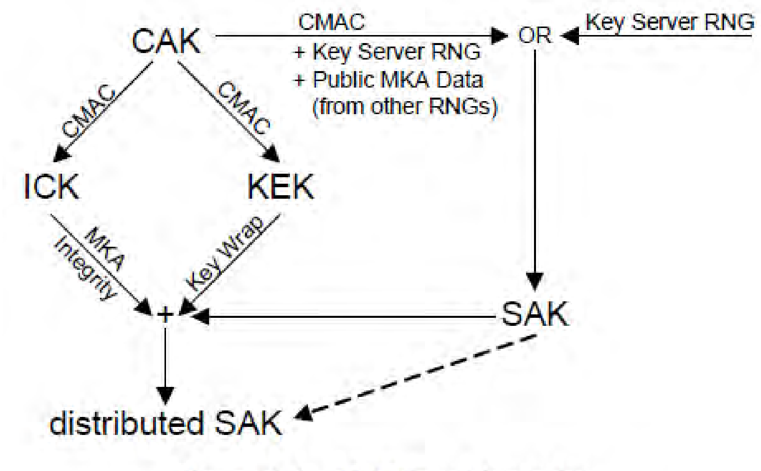


Figure 6-3—MKA key hierarchy

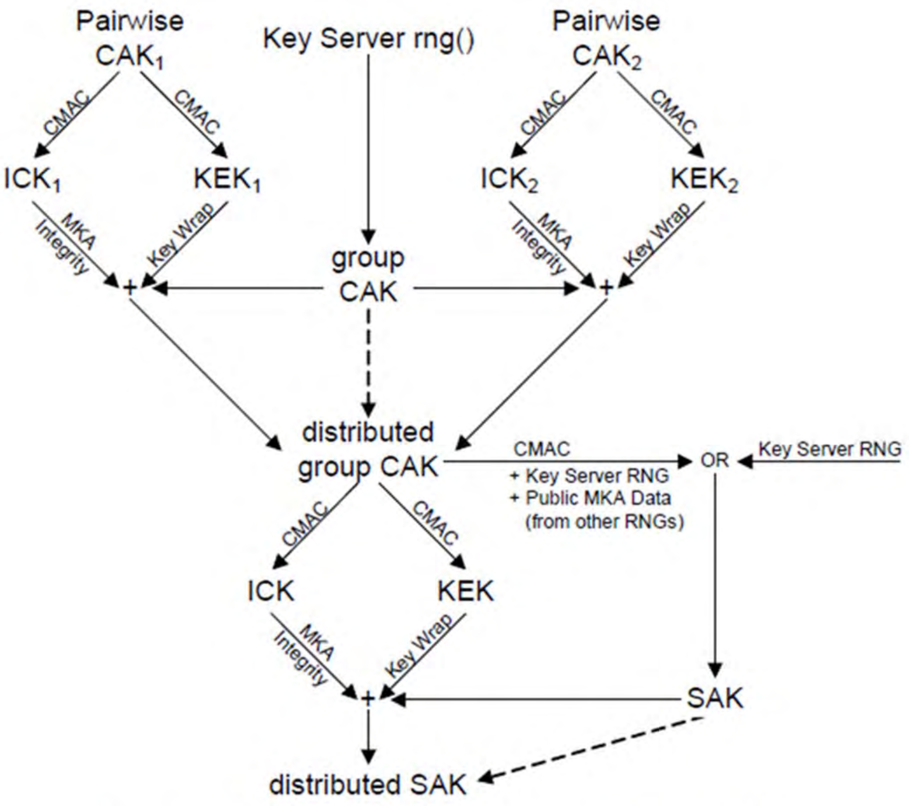


Figure 6-4—Use of pairwise CAKs to distribute group SAKs

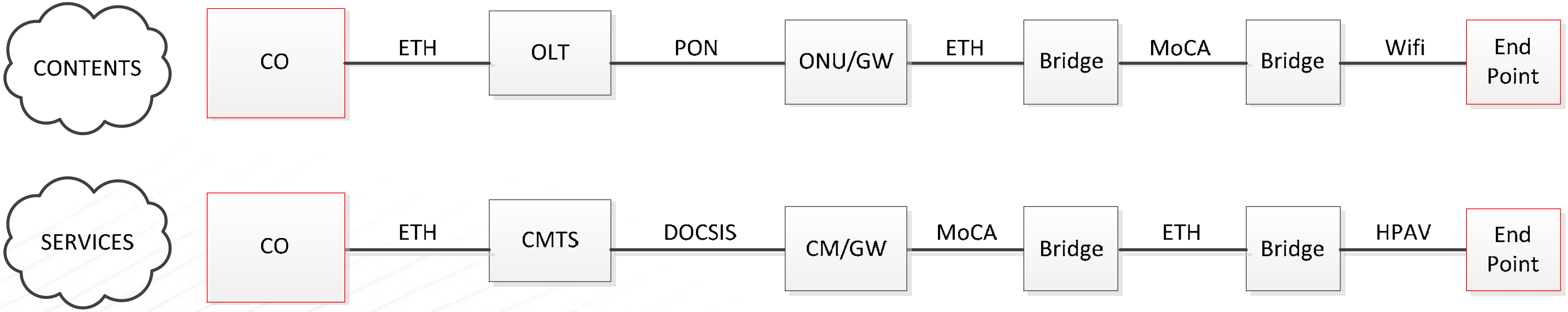
allows implementation of a policy of perfect forward security

CAK	Secure Connectivity Association Key
ICK	Integrity Check Value Key
KEK	Key Encrypting Key
SAK	Secure Association Key

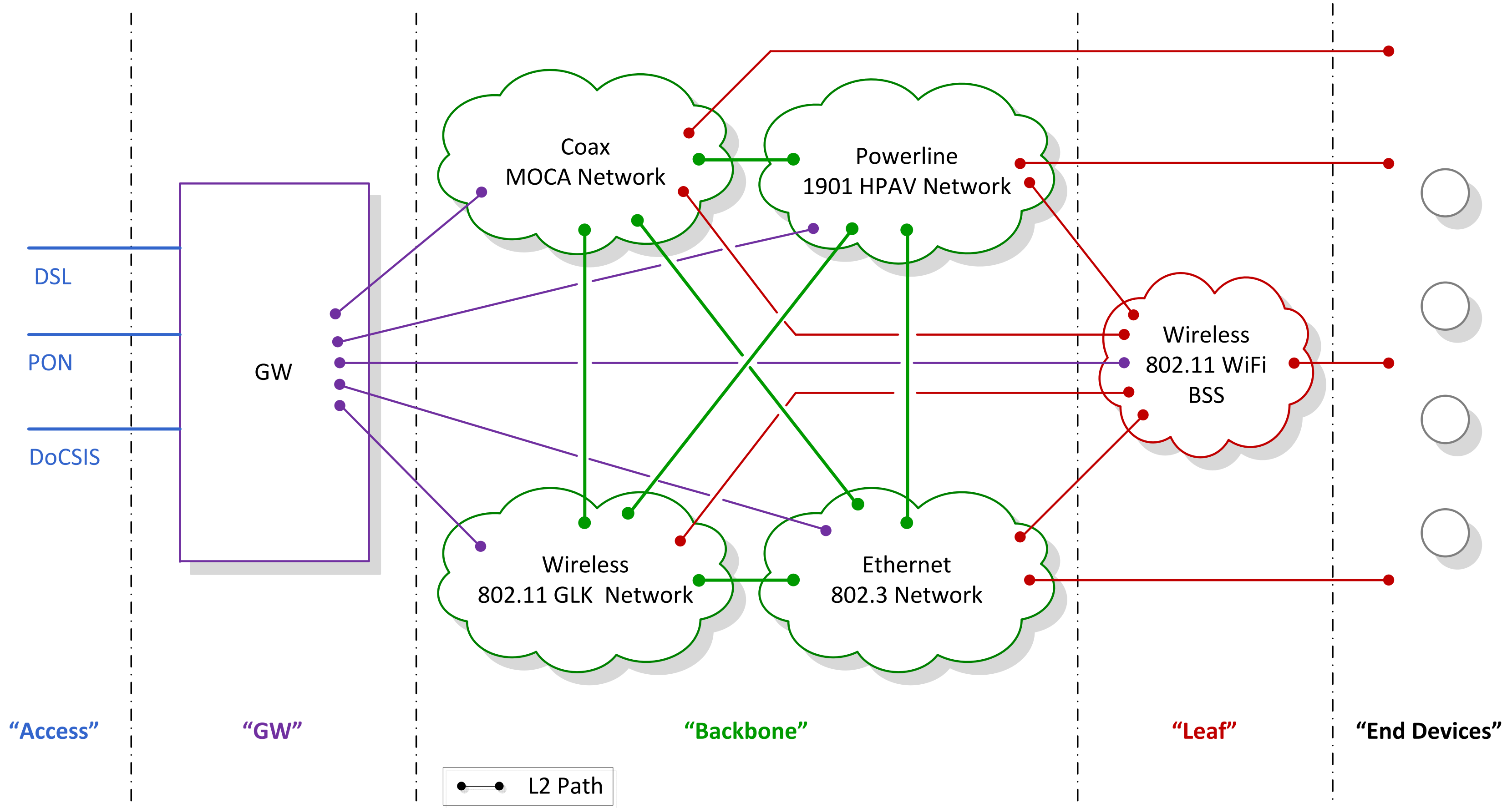
MACsec - CHALLENGES

END TO END FOR SERVICE PROVIDERS

- **Examples of End to End Hybrid Networks for Service Providers**



HYBRID HOME NETWORK CONNECTIVITY



NATIVE L2 SECURITY SCHEMES

Technology	Authentication	Encryption	Comments
Ethernet / IEEE 802.3	EAP	**AES-128 GCM**	IEEE 802.1AE (MACsec), 802.1X
MoCA	Proprietary (dynamic) PSKs	DES AES-128 CBC	The whole MPDU is encrypted in the PHY (including the Eth MAC header)
HomePlug AV2 / IEEE 1901	Proprietary (dynamic) PSKs	AES-128 CBC	
WiFi / IEEE 802.11	EAP	AES-128 CCMP	802.1X, **AES-GCM for 802.11ad**
DoCSIS	Proprietary PSK	DES AES-128 CBC	http://www.cablelabs.com/specification/docsis-3-1-security-specification DPoE Security and Certificate Specification includes EAP http://www.cablelabs.com/wp-content/uploads/specdocs/DPoE-SP-SECv1.0-I05-140327.pdf
EPON	EAP	**AES-128 GCM**	IEEE 802.1AE (MACsec) , 802.1X
ADSL	PAP/CHAP	none	L3 encryption

EAP = Extendable Authentication Protocol (RFC 3748)
GCM = Galois/Counter Mode
PSK = Private Shared Key
DPoE = DOCSIS Provisioning of EPON Specifications

DEVIL'S ADVOCATE (NO FLAME PLEEEEASE)

- **Hop to hop "limitation"**
  - Packet need to decrypted to access the inner VLAN tag
  - Key "explosion" – Let be realistic – Key management was and still is the main roadblock to security deployment…
- **802.1AEcg (aims to Provider bridges)**
  - VLAN is copied outside the encrypted fields
- **What if:**
  - Same key could now be OPTIONALLY reused if the Authentication Method and credentials are the same on 2 links…
    - If the SA is the same on Ingress and Egress , could the encrypted packets be forwarded as is ?
    - Better performance ?
    - Better transit protection ?
    - Retain network synchronization accuracy ?
    - Optional link or path authentication

    Notice that this scheme was already presented at the Ethernet Summit in 2014 by Vitesse Semiconductors
- **Q: What about IEEE 1588 Annex K ?**

MY (HUMBLE) CONCLUSIONS

- IEEE 802.1AE (MACsec) is a robust solution for network wide security at the link layer but …
- More effort should be made to address the “low end” (SMB ? / SOHO / Home) market
- Hard to promote as many “customers” are foreseeing the need for security
- Seen as expensive and cumbersome
- Must be actively promoted beyond Ethernet Core Networks
- MUST BE INTEGRATED UP FRONT IN ARCHITECTURE DESIGN

Thank you