Encryption method for 25G-EPON and 50G-EPON

Glen Kramer, Broadcom

PON-specific encryption requirements

- Encryption is established only between the OLT and ONUs
  - Encryption is needed to protect each ONU's traffic from being snooped by other ONUs (a problem created by broadcasting nature of PON medium)
  - Encryption must protect user traffic as well as PON control traffic between the OLT and ONUs (MPCPDUs, CCPDUs, OAMPDUs)
  - Generally, once encryption between the OLT and an ONU is stablished, it remains active until the ONU is reset/rebooted (i.e., months to years). Encryption sessions do not need to be re-negotiated every time a key is exchanged.
- Multicast groups must be encrypted to prevent non-members from snooping the multicast traffic
  - All ONU that are members of a given multicast group use the same encryption key. The key must be generated centrally (typically by the NMS or the OLT) and distributed to all member ONUs.
- Operators should be able to selectively enable/disable encryption per ONU or per multicast group for troubleshooting purposes

Issues with MACsec

- Significant overhead
  - ≈ 5% in the downstream. Higher in the upstream.
- MACsec only considers point-to-point LANs and multi-access LANs. Doesn’t take into account P2MP architecture and PON-specific features.
  - In PON, operators authenticate physical devices connected to the network (ONUs). Virtual ports (LLIDs) are created and deleted as needed (could be based on user behavior, similar to dynamic provisioning of service flows in DOCSIS). Performing authentication for every virtual port is impractical and may affect services.
  - Unclear how MKA can support single-copy multicast in PON

MACsec Group host access vs. PON multicast

- MACsec group host access is designed to allow direct communications between multiple hosts on a shared LAN.
- Prior to distributing the group CAK, each host goes through a pair-wise mutual authentication with the network access point (acting as EAP Authenticator)

- PON multicast is designed to deliver a copy of a frame from a single source (OLT) to a subset of ONUs. ONUs that are not group members shall not be able to "see" the frame
- A frame is replicated in the P2MP medium resulting in identical copies delivered to each group member.
- Multicast flows are unidirectional: Group members are not allowed to transmit any data upstream.
- ONUs are not allowed to communicate with other group members. (The asymmetry of P2MP medium facilitates the enforcement of this requirement.)
- Multicast groups can be static (permanent) or dynamic (created as needed for specific session/flow and destroyed afterwards).

MACsec and multicast LLID

- IEEE 802.1X does not explain how to support single-copy multicast.
- In this figure, a separate secure channel is established between the multicast source (Network Access Point/Authenticator) and each member of the multicast group (Host/Supplicant).
- Each Supplicant has to authenticate with the Authenticator before being able to join the group.
- Each Supplicant gets a separate decryption key.
- This makes single-copy multicast impossible.

7.5.2 System configuration and operation

The processes and entities that support this application are illustrated in Figure 7-12.

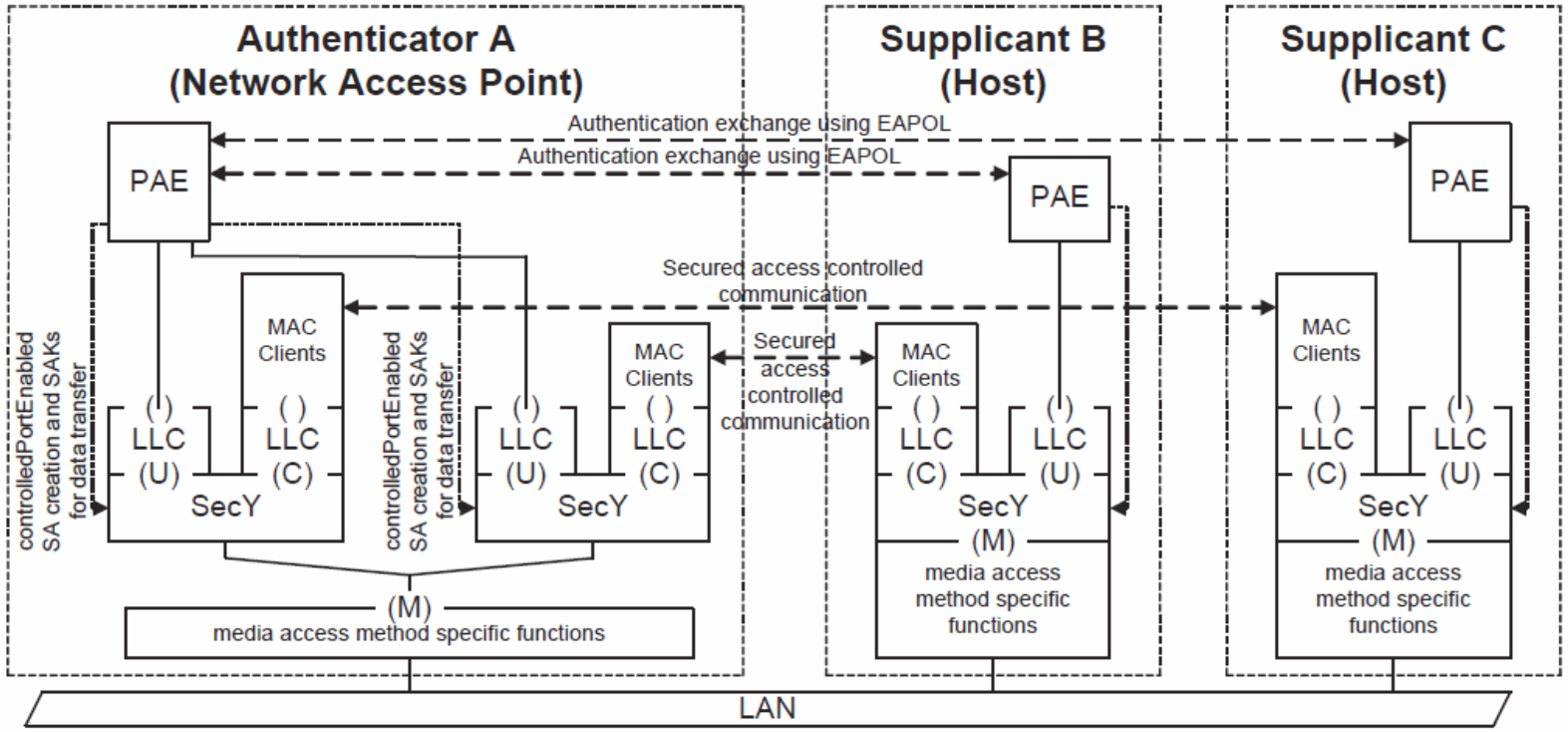


Figure 7-12—Network access control with MACsec and a multi-access LAN

802.1X, 7.6 Group host access with MACsec

While a multi-access LAN (7.5) provides independent and separate access for a number of hosts through a single network access point, there are application scenarios where direct communication between the hosts is also desirable. Access to a network is often enforced in a wiring closet per desktop LAN, while there can be two or more LAN stations per desk. The combination of a PC and an IP phone, interconnected by repeater-like functionality is typical. Communication between the PC and phone for computer assisted telephony, for example, is direct and does not pass through the network access point, while data from both PC and phone goes directly to the network. See Figure 7-14.

The use of MACsec to support a group CA in this scenario secures all the data communication described and does not require the instantiation of multiple virtual ports per physical port at the network access point, or bridging between those ports at the access point or within the secured network. Pairwise mutual authentication takes place between the network access point (acting as an EAP Authenticator) and each host (acting as an EAP Supplicant) prior to the network access point distributing the CAK for the group CA to the host. The network access point dynamically creates PAE instances to support each pairwise authentication as required.

It is possible to combine the use of group host access with point-to-point access over the same individual shared media LAN, first authenticating each host and then allocating it to an appropriate group on the basis of that authentication. Such a combined scenario allows, for example, a group of systems under the control of a single user to communicate directly, while requiring communication with another group to occur through the network access point.

NOTE—The combined scenario described immediately above requires each group to be on a separate VLAN, with independent source address location learning between those VLANs, and connection between the VLANs being provided by routing, either within the network access point or elsewhere within the secured network.

No direct communication between ONUs is allowed

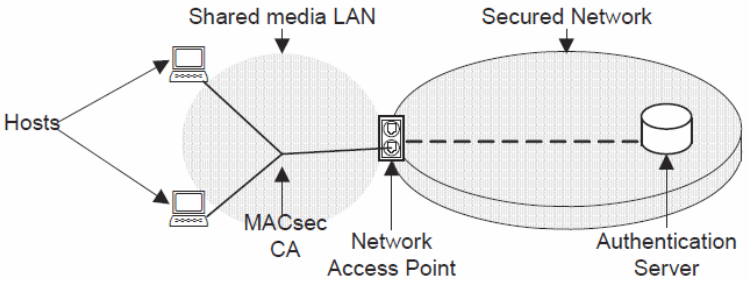


Figure 7-14—Group host access

An ONU may be a member of multiple multicast groups. It appears that ONU should authenticate each multicast LLID before it can obtain a shared CAK.

Multicast groups are distinguished by LLID tags (in envelope headers). Multicast groups are not required to use VLAN tags. Each client station connected to an ONU may receive multiple multicast flows (filtering may be configured by provisioning classification rules).

Authentication protocol

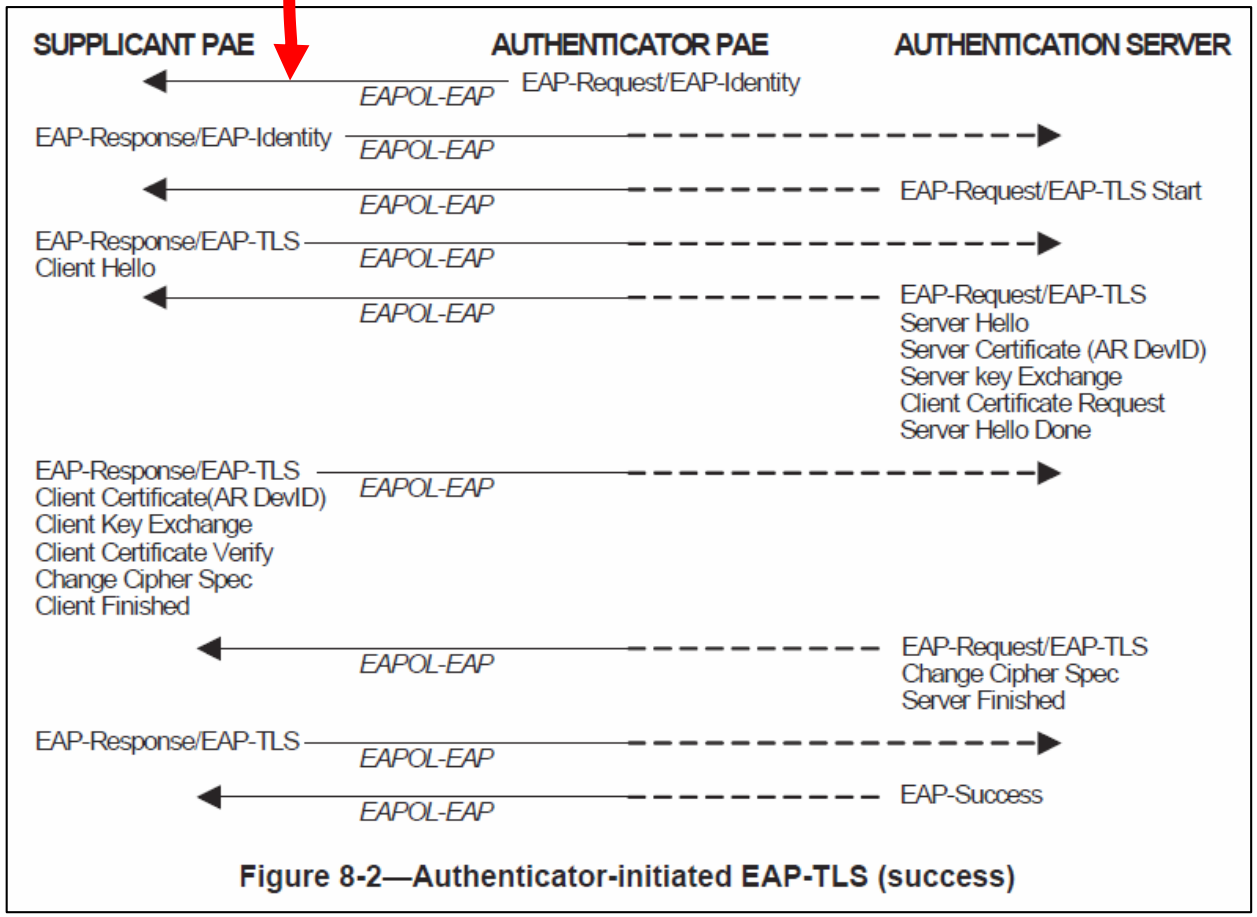


Figure 8-2—Authenticator-initiated EAP-TLS (success)

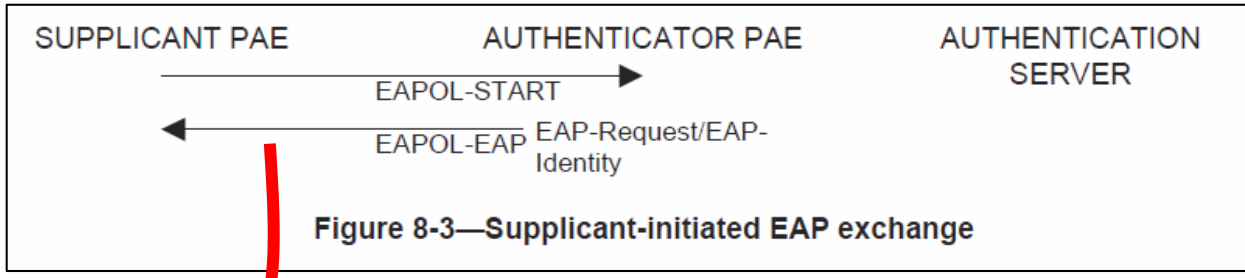


Figure 8-3—Supplicant-initiated EAP exchange

In supplicant-initiated EAP exchange, EAPOL-START is sent by the supplicant, followed by the entire EAP exchange shown on the left.

Performing host authentication every time a dynamic multicast group is created is impractical and will increase the delay associated with provisioning of such groups

Zero-overhead encryption method

- Designed specifically for EPON architecture
- Specified in DPoE and is referenced by SIEPON Package A.
- No security issues were identified in 10G-EPON deployments
- Identical methods to encrypt unicast and multicast links.
- For 25G- and 50G-EPON, zero-overhead method can be further optimized:
  - Reduce number of keys by having a secure association between ONU and OLT, rather than between each pair of virtual ports (i.e., per unicast LLID).
  - Rely on encrypted management channel (MLID) to deliver subsequent key(s)
  - The same TLV delivers either unicast or multicast key. One OAMPDU may carry multiple keys (one unicast key per ONU and multiple multicast keys - one for each multicast LLID configured in a given ONU).

ITU-T G.9804.2 Security

- **ITU-T PON uses a method very similar to zero-overhead method.**
  - *"The default algorithm used for XGEM payload encryption is the AES-128 [NIST FIPS-197] cipher, used in Counter mode (AES-CTR), as described in [NIST SP800-38A]."*
  - *"Provisioning a non-default XGEM port for encryption does not imply the traffic is always encrypted. The encryption status of each individual XGEM frame is determined dynamically by the sender, within the explicitly configured or pre-defined capabilities of the associated XGEM port, and is indicated in the XGEM frame header."*
  - *"For each of the two key types (unicast and broadcast), both the OLT CT and the ONU maintain an indexed array of two data encryption key entries."*
- **Initialization Vector (IV) derivation is different, but the concept is the same**

DPoE 2.0

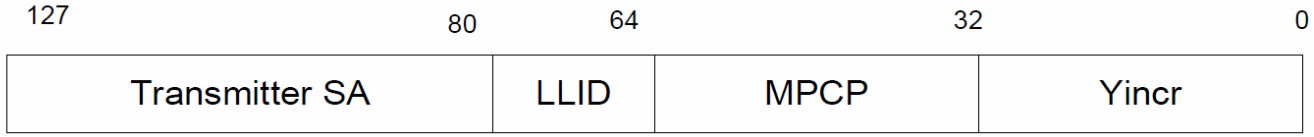
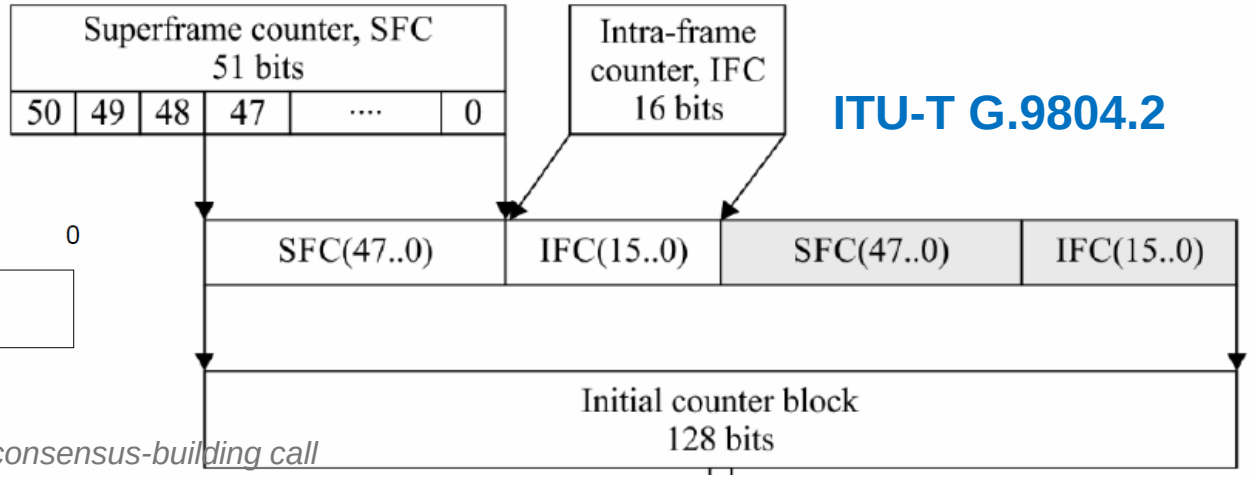


Figure 26 - Octet Order within the Initial Vector (10G)

ITU-T G.9804.2



Discussion points

MACsec		Zero-Overhead Encryption	
For	**Against**	**For**	**Against**
MH: *I do like the fact that MACSec solution has a larger security expert forum vetting the system and keeping it up to date.*	***MH:*** *I am not a fan of MACSec, especially in the upstream direction, where packet sizes are smaller and overhead will be higher.*	***JCM:*** *The one place where I see a difference is about performance and competitiveness. Having no overhead cost is definitely advantageous.*	

Straw Poll

- I prefer the following encryption method for IEEE 1904.4 (vote for one only)
  1. 802.1AE SecTag overhead ___0___
  2. Zero-overhead encryption ___6___

Motion #3

- IEEE 1904.4 should specify zero-overhead encryption method based on AES Counter mode.
  - Moved: Glen Kramer
  - Second: Mark Laubach
  - (Technical, required >= 2/3)
- Motion passed by voice vote without opposition

Thank you