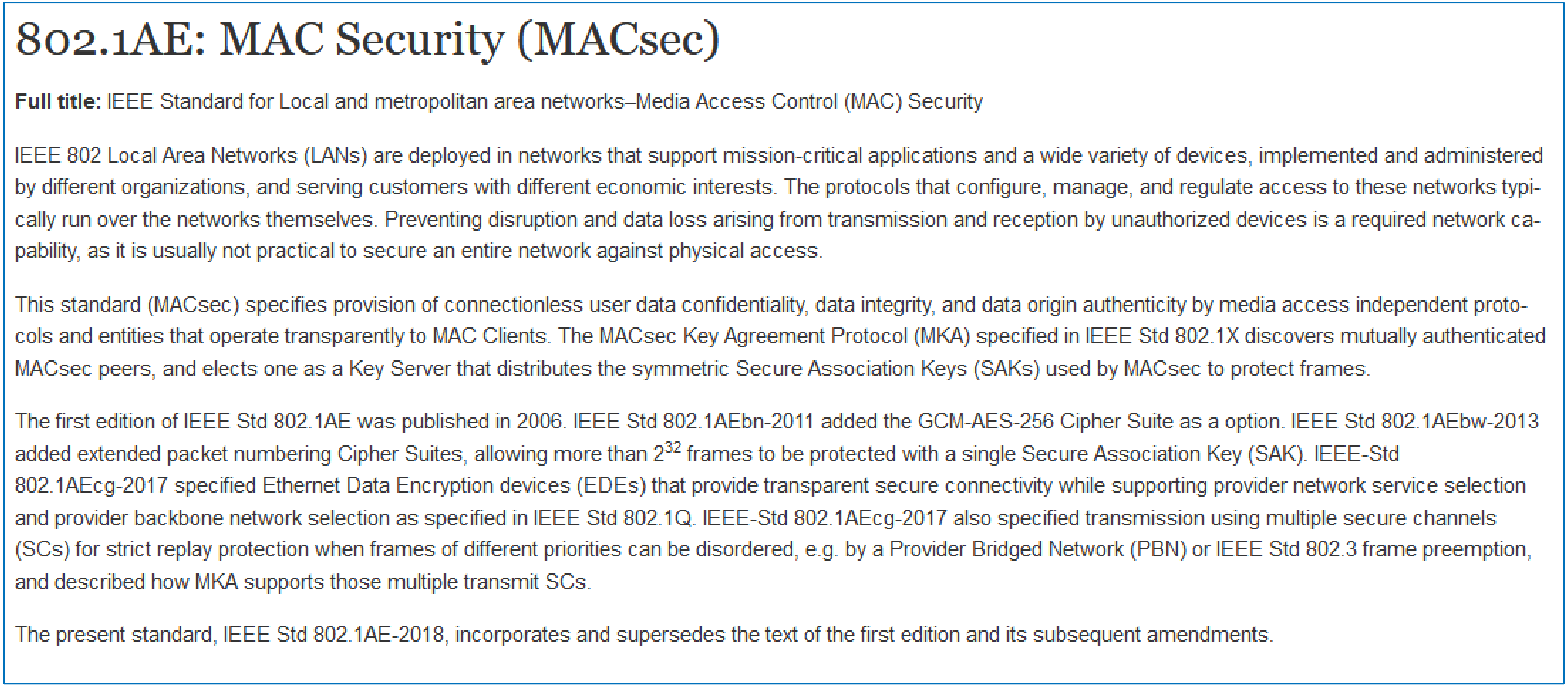
802.3 SPMD SG: MACsec & SPMD

Peter Jones - Cisco

Goals

- Review MACsec/802.1X basics including support for shared media
- Outline options for MACsec on SPMD

MACsec Basics



802.1AE: MAC Security (MACsec)

Full title: IEEE Standard for Local and metropolitan area networks–Media Access Control (MAC) Security

IEEE 802 Local Area Networks (LANs) are deployed in networks that support mission-critical applications and a wide variety of devices, implemented and administered by different organizations, and serving customers with different economic interests. The protocols that configure, manage, and regulate access to these networks typically run over the networks themselves. Preventing disruption and data loss arising from transmission and reception by unauthorized devices is a required network capability, as it is usually not practical to secure an entire network against physical access.

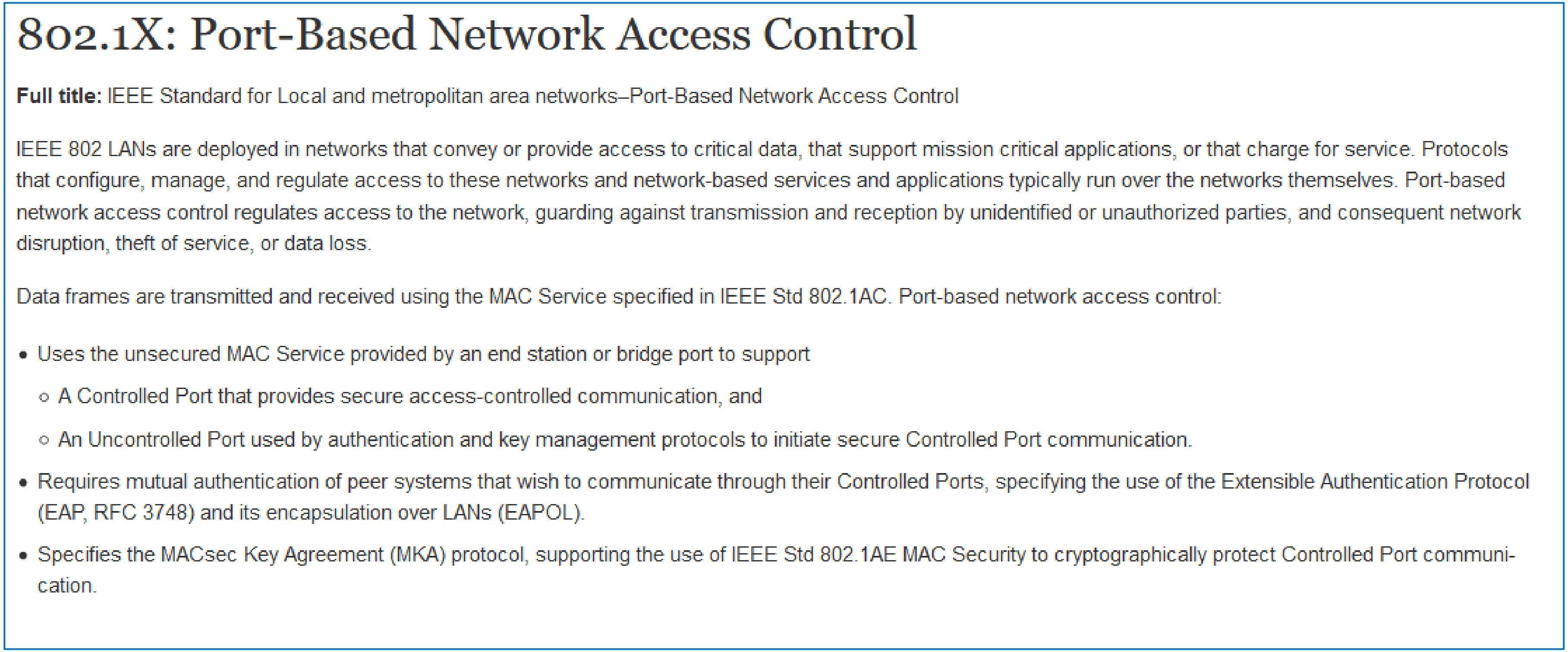
This standard (MACsec) specifies provision of connectionless user data confidentiality, data integrity, and data origin authenticity by media access independent protocols and entities that operate transparently to MAC Clients. The MACsec Key Agreement Protocol (MKA) specified in IEEE Std 802.1X discovers mutually authenticated MACsec peers, and elects one as a Key Server that distributes the symmetric Secure Association Keys (SAKs) used by MACsec to protect frames.

The first edition of IEEE Std 802.1AE was published in 2006. IEEE Std 802.1AEbn-2011 added the GCM-AES-256 Cipher Suite as a option. IEEE Std 802.1AEbw-2013 added extended packet numbering Cipher Suites, allowing more than 2^{32} frames to be protected with a single Secure Association Key (SAK). IEEE-Std 802.1AEcg-2017 specified Ethernet Data Encryption devices (EDEs) that provide transparent secure connectivity while supporting provider network service selection and provider backbone network selection as specified in IEEE Std 802.1Q. IEEE-Std 802.1AEcg-2017 also specified transmission using multiple secure channels (SCs) for strict replay protection when frames of different priorities can be disordered, e.g. by a Provider Bridged Network (PBN) or IEEE Std 802.3 frame preemption, and described how MKA supports those multiple transmit SCs.

The present standard, IEEE Std 802.1AE-2018, incorporates and supersedes the text of the first edition and its subsequent amendments.

https://1.ieee802.org/security/802-1ae

802.1X Basics



802.1X: Port-Based Network Access Control

Full title: IEEE Standard for Local and metropolitan area networks–Port-Based Network Access Control

IEEE 802 LANs are deployed in networks that convey or provide access to critical data, that support mission critical applications, or that charge for service. Protocols that configure, manage, and regulate access to these networks and network-based services and applications typically run over the networks themselves. Port-based network access control regulates access to the network, guarding against transmission and reception by unidentified or unauthorized parties, and consequent network disruption, theft of service, or data loss.

Data frames are transmitted and received using the MAC Service specified in IEEE Std 802.1AC. Port-based network access control:

- Uses the unsecured MAC Service provided by an end station or bridge port to support
  - A Controlled Port that provides secure access-controlled communication, and
  - An Uncontrolled Port used by authentication and key management protocols to initiate secure Controlled Port communication.
- Requires mutual authentication of peer systems that wish to communicate through their Controlled Ports, specifying the use of the Extensible Authentication Protocol (EAP, RFC 3748) and its encapsulation over LANs (EAPOL).
- Specifies the MACsec Key Agreement (MKA) protocol, supporting the use of IEEE Std 802.1AE MAC Security to cryptographically protect Controlled Port communication.

https://1.ieee802.org/security/802-1x/

MACsec terms

- MAC Security Entity: SecY
- Key Agreement Entity: KaY
- Secure Association Identifier: SAI
- Connectivity Association: CA
- Secure Channel: SC
- Security Association: SA
- Secure Association Key: SAK

MACsec & Shared Media

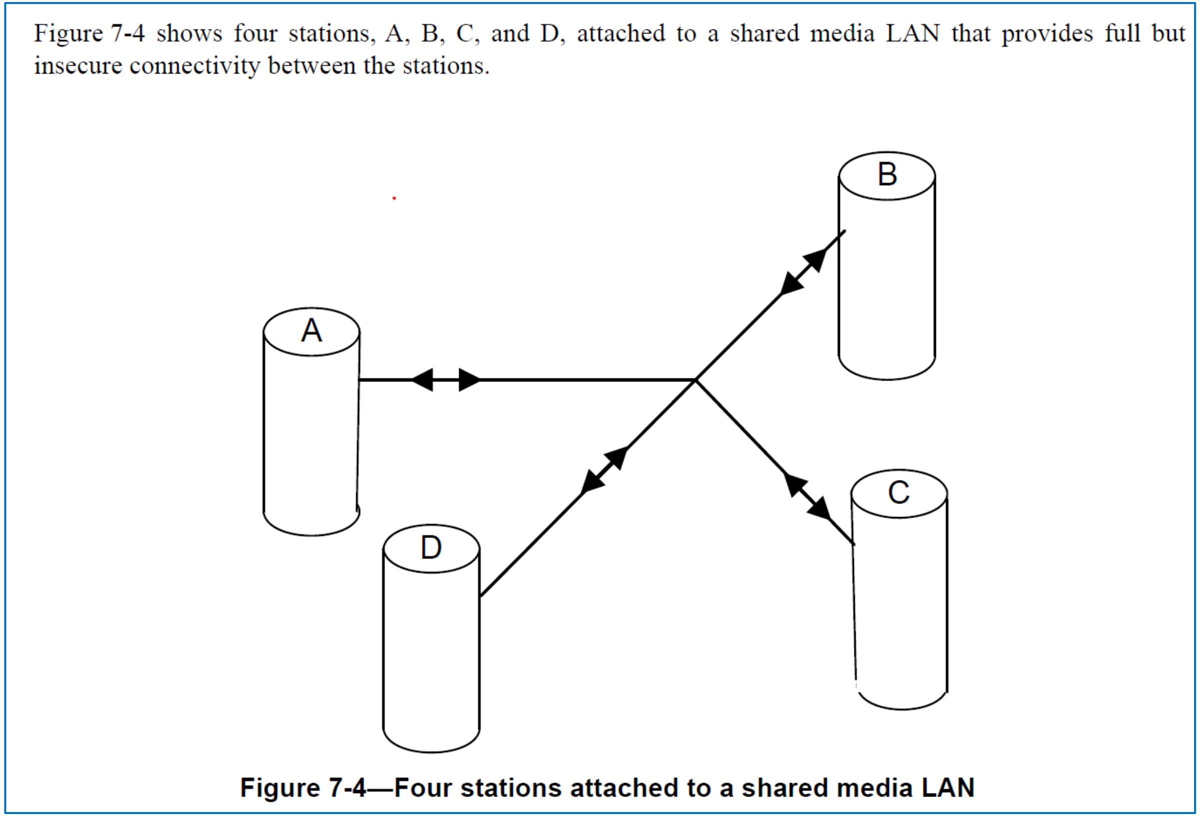


Figure 7-4 shows four stations, A, B, C, and D, attached to a shared media LAN that provides full but insecure connectivity between the stations.

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

From IEEE Std 802.1AE-2018

MACsec & Shared Media example

Figure 7-5 depicts a CA created by MACsec Key Agreement following mutual authentication and authorization of A, B, and C. The CA excludes D.

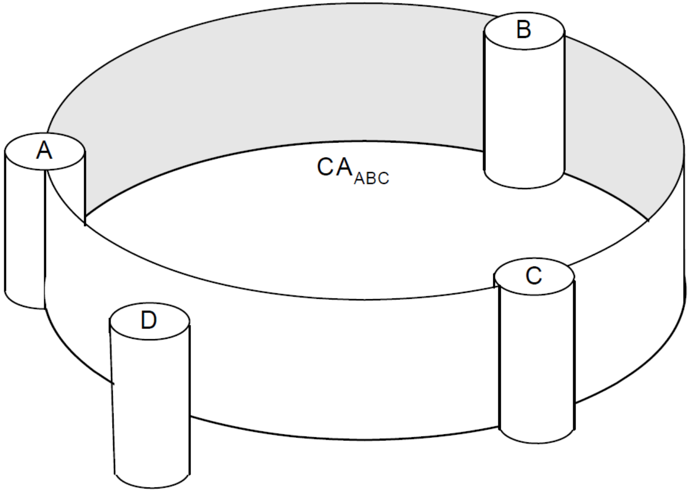


Figure 7-5—A CA including ports A, B, and C

Figure 7-6 shows the three SCs that support the CA, one for transmission by each of A, B, and C.

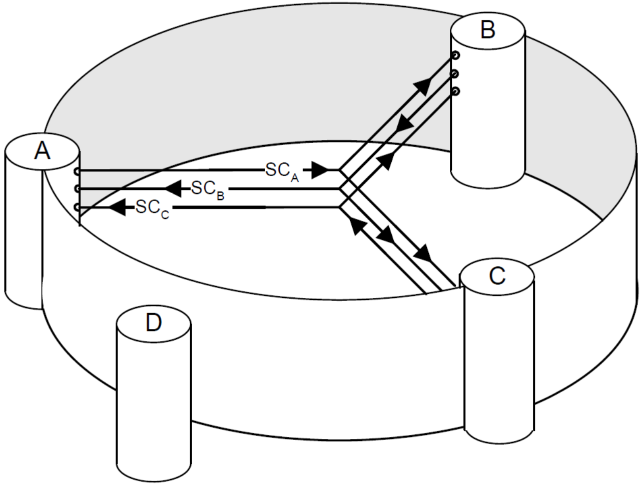
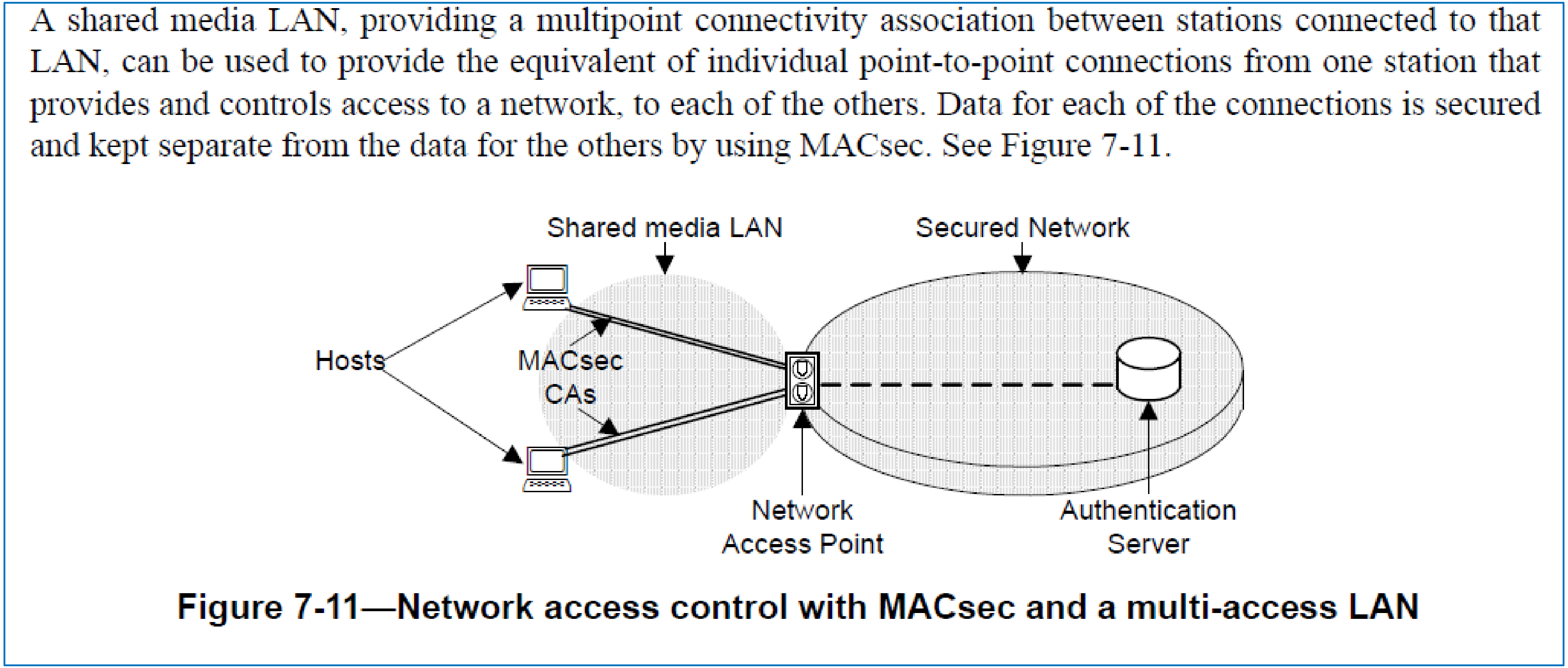


Figure 7-6—Secure communication between three stations

- 4 member LAN (e.g. SPMD mixing segment)
- Secure communications between 3 of the members
- Each SC provides unidirectional point-to-multipoint communication

From IEEE Std 802.1AE-2018

802.1X and Shared Media

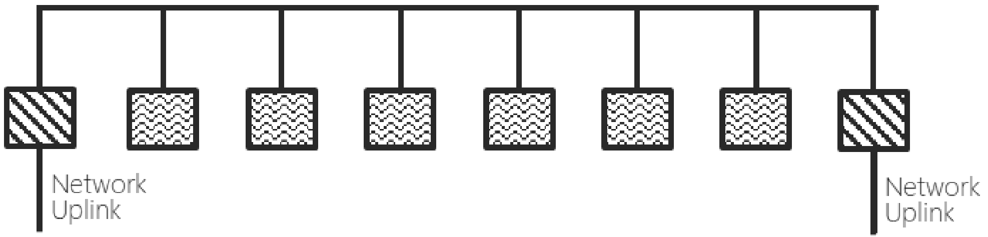


A shared media LAN, providing a multipoint connectivity association between stations connected to that LAN, can be used to provide the equivalent of individual point-to-point connections from one station that provides and controls access to a network, to each of the others. Data for each of the connections is secured and kept separate from the data for the others by using MACsec. See Figure 7-11.

Figure 7-11—Network access control with MACsec and a multi-access LAN

From IEEE Std 802.1X-2020

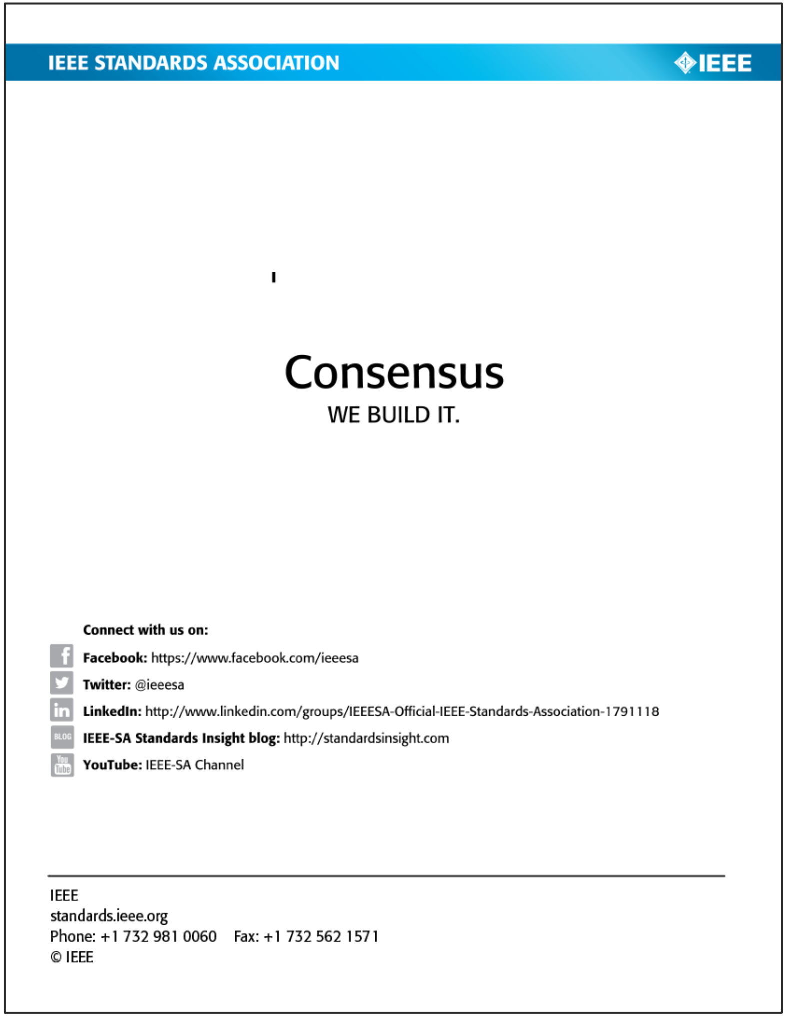
MACsec & SPMD



- MACsec/802.1X natively support multidrop
- Options on how to model communications
  - Any to any (Single CA with per node point to multipoint SCs)
  - Point to point switch to end device and point to multipoint switch to end devices for multicast/broadcast

Conclusion

- MACsec can be used to provide secure communications on multidrop networks such as 802.3da
- 802.3da does not need anything extra to support MACsec
- Multiple options available for modelling communication.



IEEE STANDARDS ASSOCIATION

Consensus

WE BUILD IT.

Connect with us on:

Facebook: https://www.facebook.com/ieeesa

Twitter: @ieeesa

LinkedIn: http://www.linkedin.com/groups/IEEESA-Official-IEEE-Standards-Association-1791118

IEEE-SA Standards Insight blog: http://standardsinsight.com

YouTube: IEEE-SA Channel

IEEE
standards.ieee.org
Phone: +1 732 981 0060   Fax: +1 732 562 1571