MACsec with Shared Media

James A. McIntosh – Microchip Technology, Inc.

v0.3 – July 12, 2023

Introduction

- The MACsec standard (IEEE 802.1AE-2018) describes both point-to-point and shared media LAN applications in Clause 7.
- The shared media use case is applicable to 10BASE-T1S.

- This topic was also discussed in TC17 in a presentation from Dr. Philip Axer of NXP in February 2023.
  - Look here for reference to that discussion: https://members.opensig.org/wg/TC17/document/8921

SCs between 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.

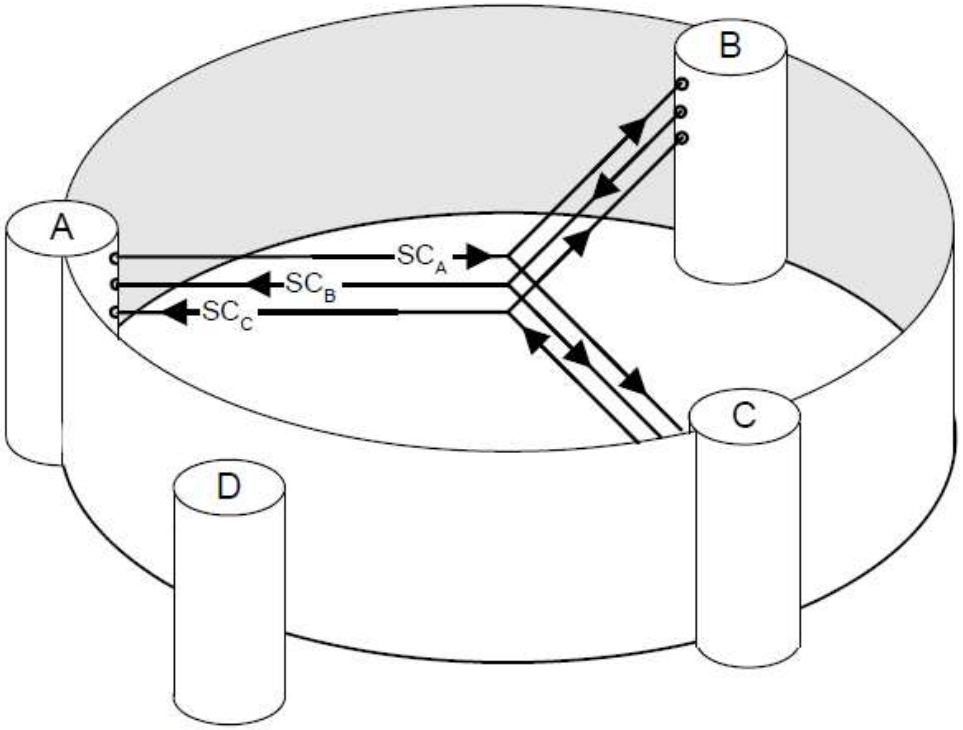


Figure 7-6—Secure communication between three stations

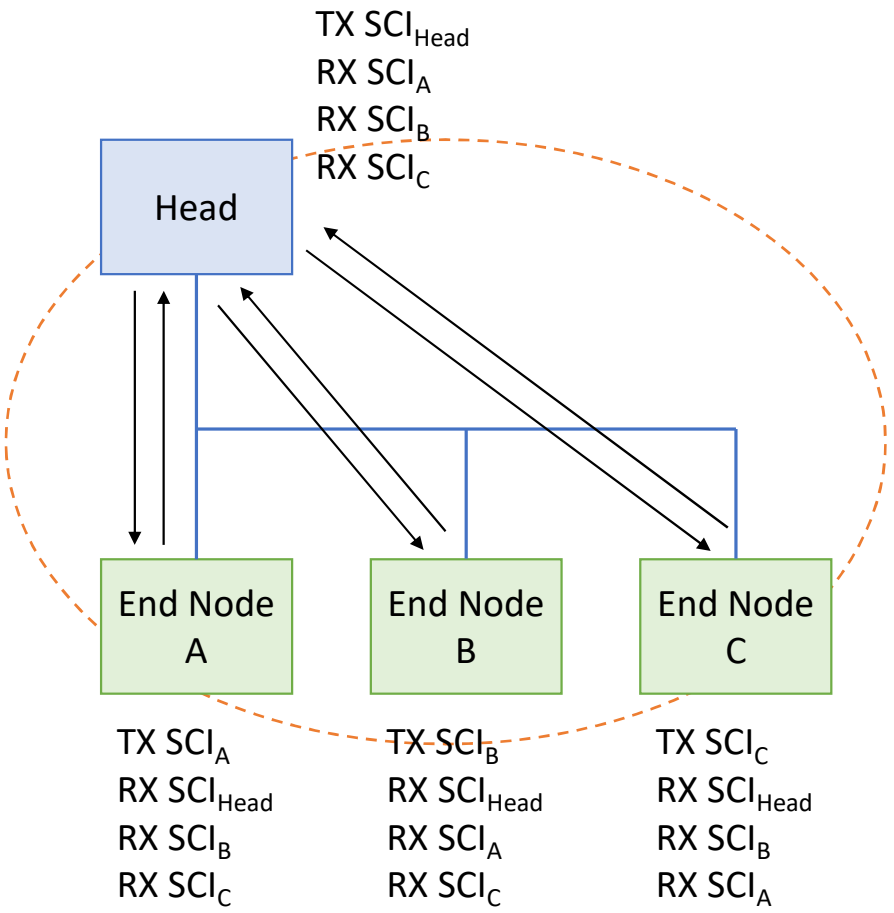
Scalability

- If there are *N* devices in a single CA, each device will need one transmit SC, but *N*-1 receive SCs.
- This leads to scalability issues for larger networks.

- I will discuss three possible configurations in the following slides.

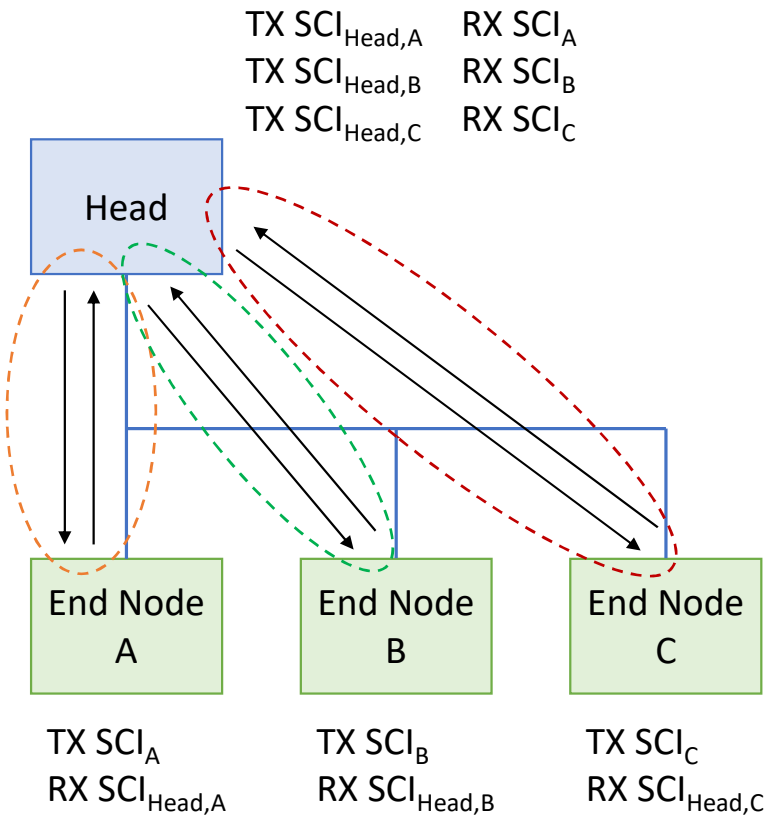
Configuration 1 – Single CA

- This case assumes:
  - All nodes communicate with each other.
  - All nodes require complete privacy and authentication.
- All nodes require 1 TX key and *N*-1 RX keys



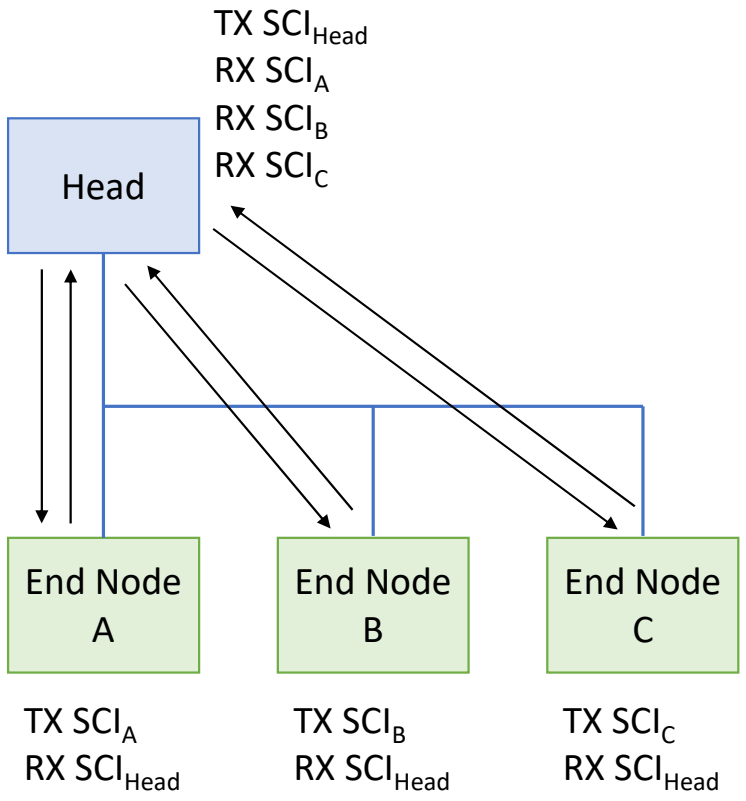
Configuration 2 – Multiple CAs

- This case assumes:
  - End nodes only communicate with the Head node.
  - They still require complete privacy and authentication.
- Head node requires *N*-1 TX keys.
- End nodes only require one RX key each.



Configuration 3 – Partial Multiple CAs

- This case assumes:
  - End nodes only communicate with the Head node.
  - Head node is "broadcasting" to the end nodes.
- Blend of configurations 1 & 2 above.
  - Head node has 1 TX key and *N*-1 RX keys (same as configuration 1)
  - End nodes have only 1 TX key and 1 RX key (same as configuration 2)



Thank you!

Thoughts?