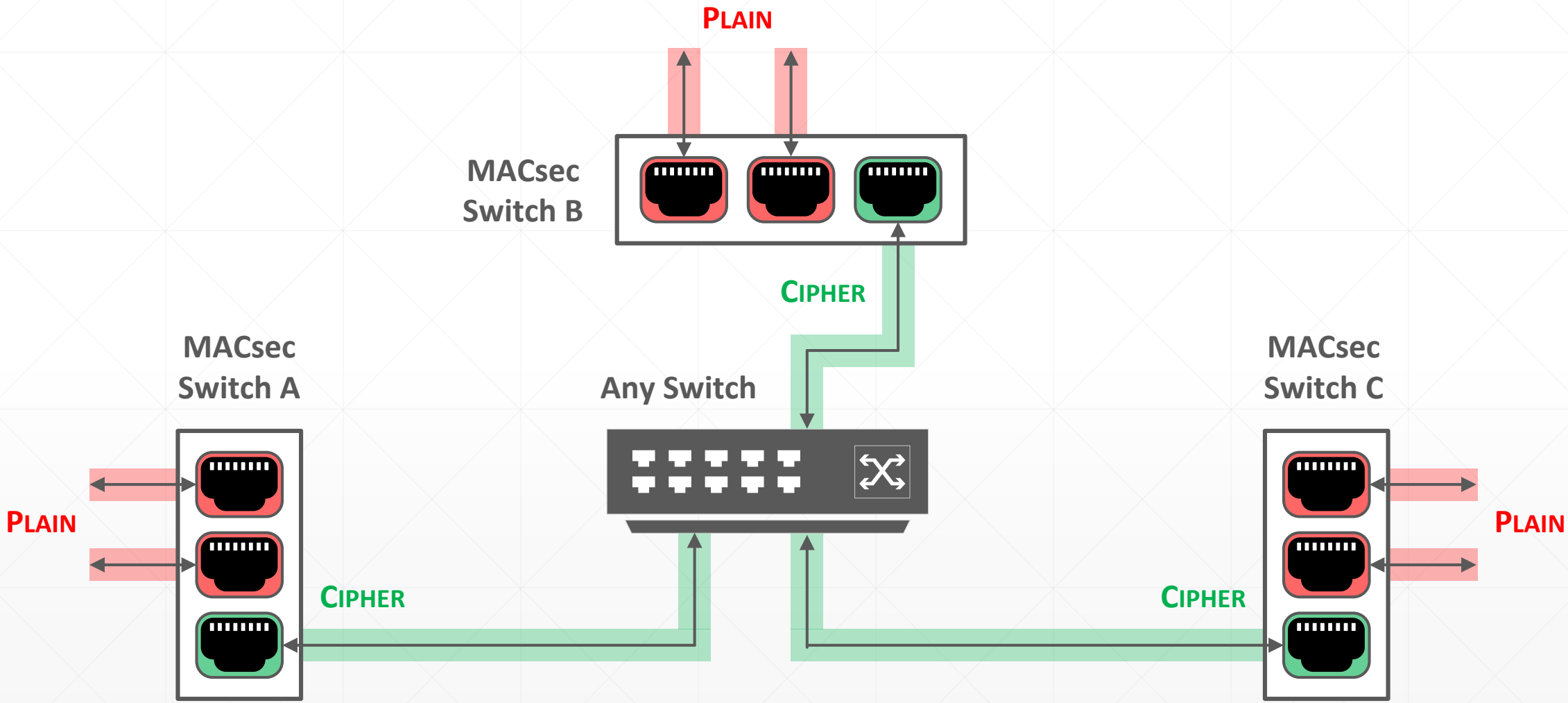
LAN Security mit MACsec

Referat von Peter Voser

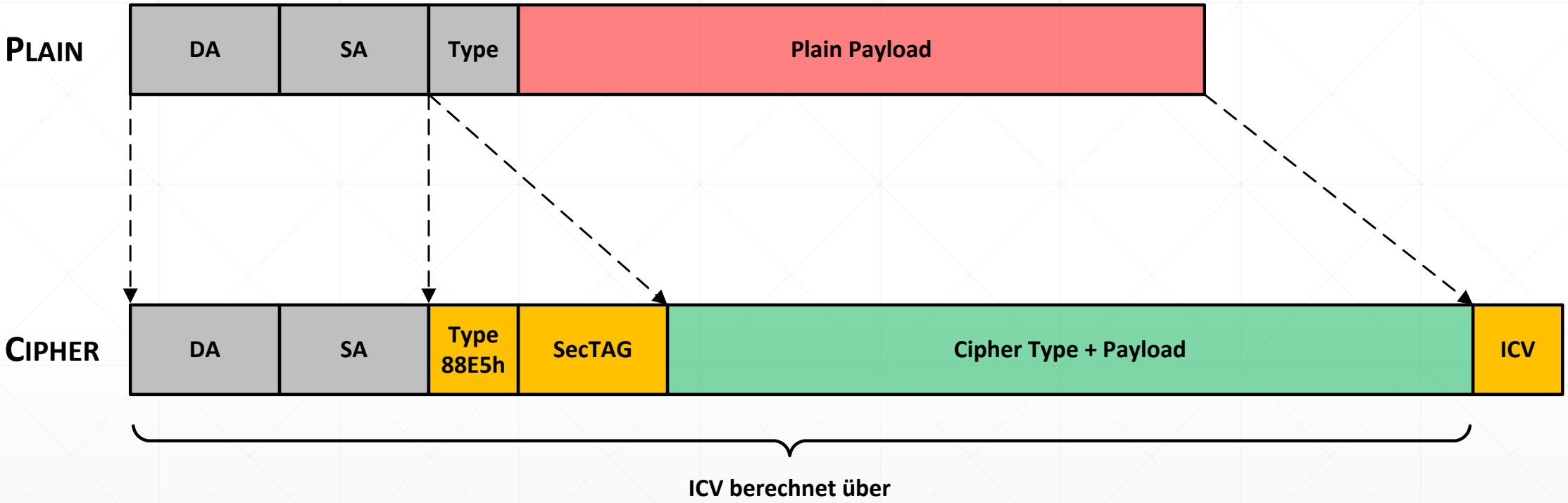
Agenda

- MACsec ist ein IEEE Standard
- Protokollaufbau
- Kryptografische Funktionen
- MACsec Implementierungen in Hardware oder Software
- Beispiele und Demo

Ein LAN mit MACsec

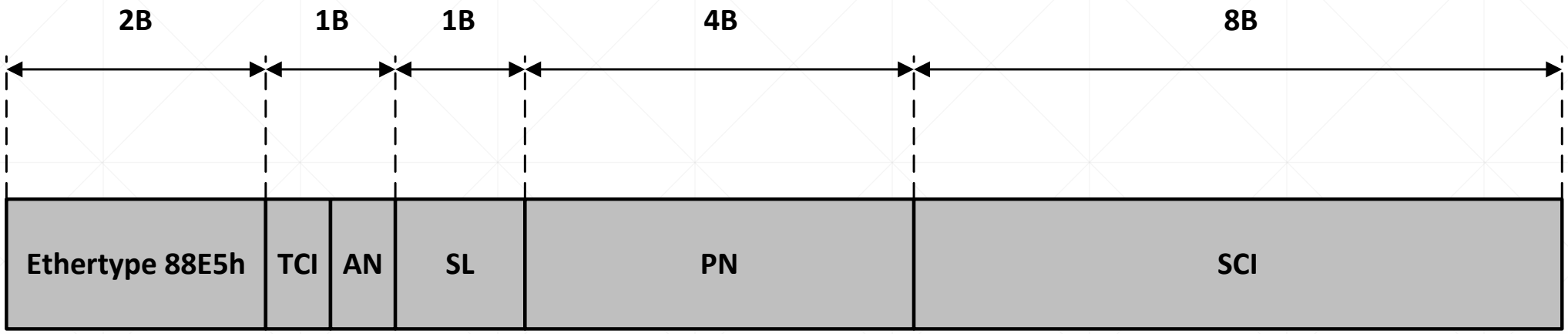


Layer 2 Frames



DA	*Destination Address*
SA	*Source Address*
SecTAG	*Security TAG*
ICV	*Integrity Check Value*

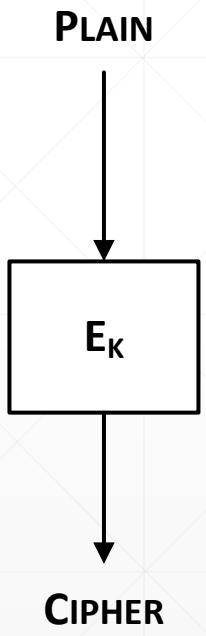
802.1AE Security Tag (Header)



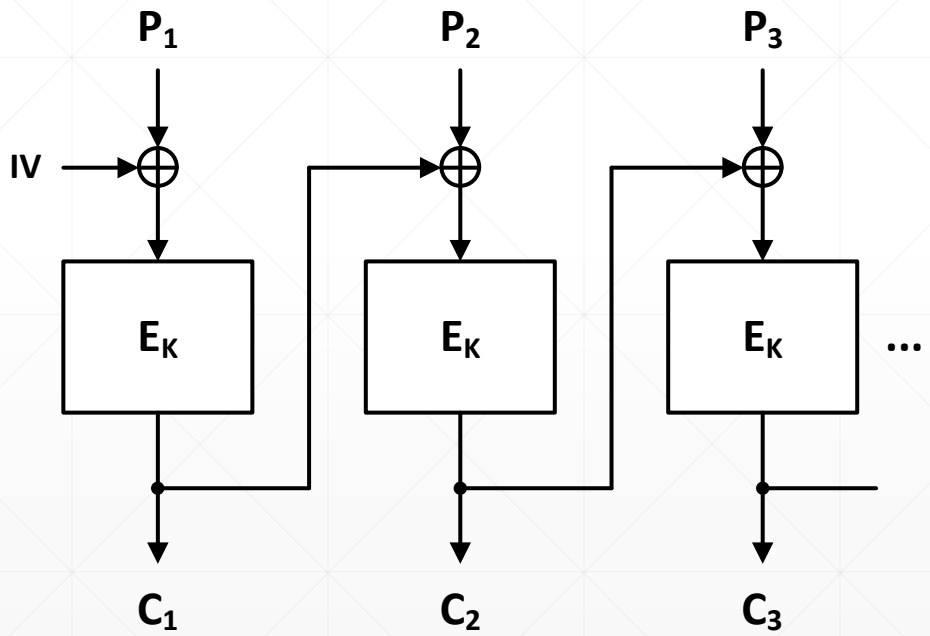
TCI *Tag Control Information*
AN *Association Number*
SL *Short Length*
PN *Packet Number*
SCI *Secure Channel Identifier*

AES Betriebsarten

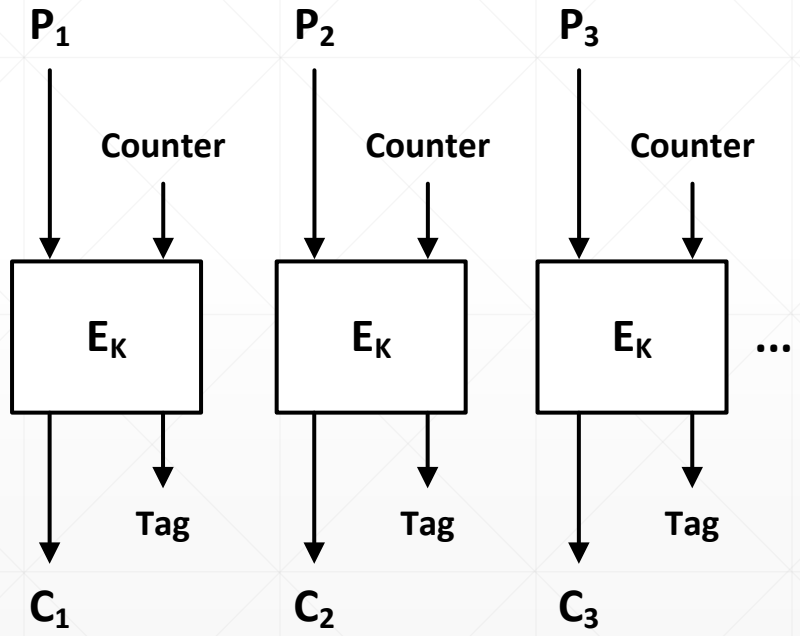
1. ECB
(ELECTRONIC CODE BOOK)



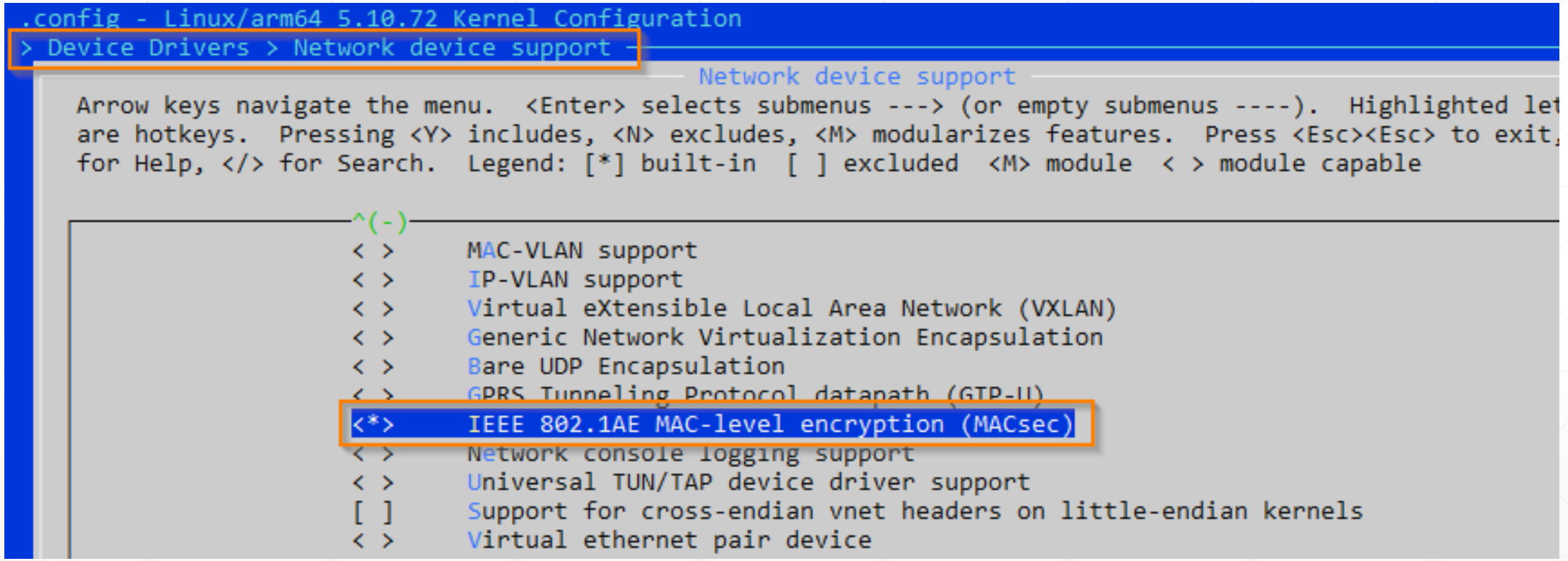
2. CBC
(CIPHER BLOCK CHAIN)



3. CM
(COUNTER MODE)

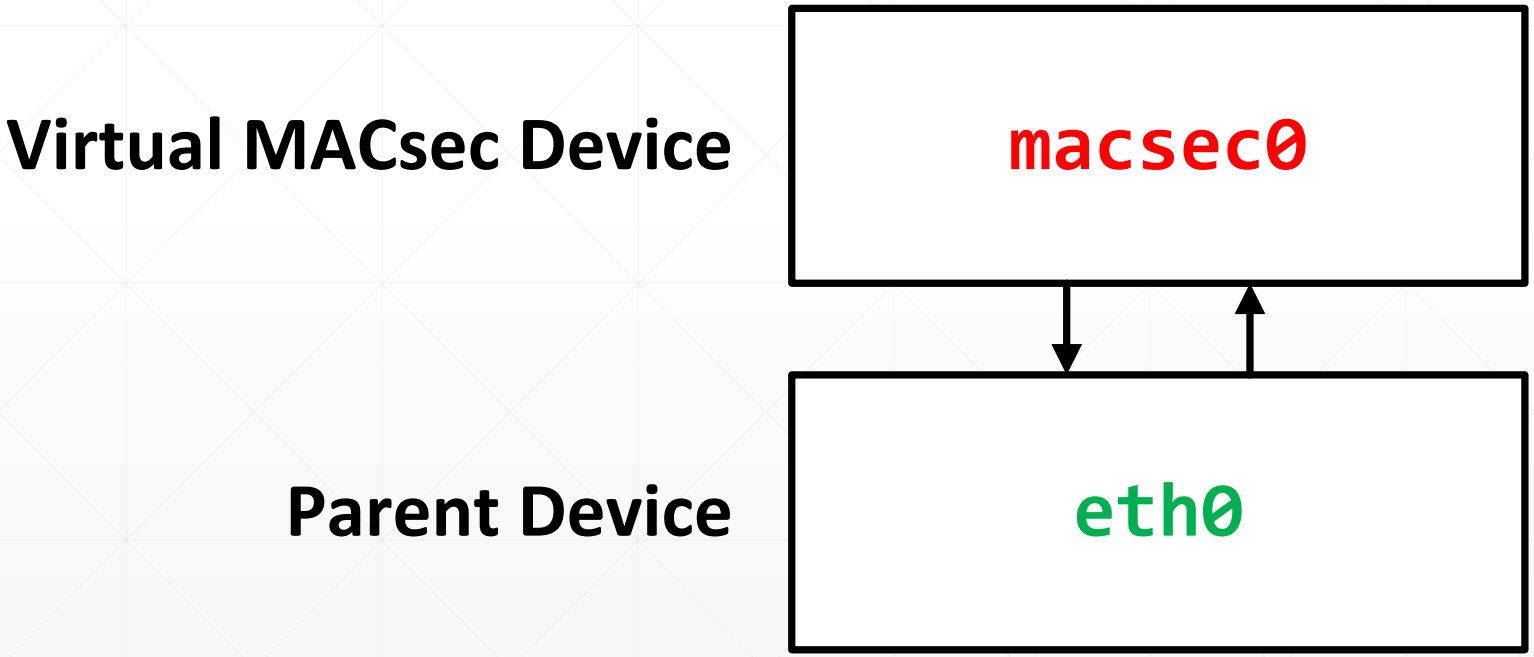


Linux MACsec Kernelmodul

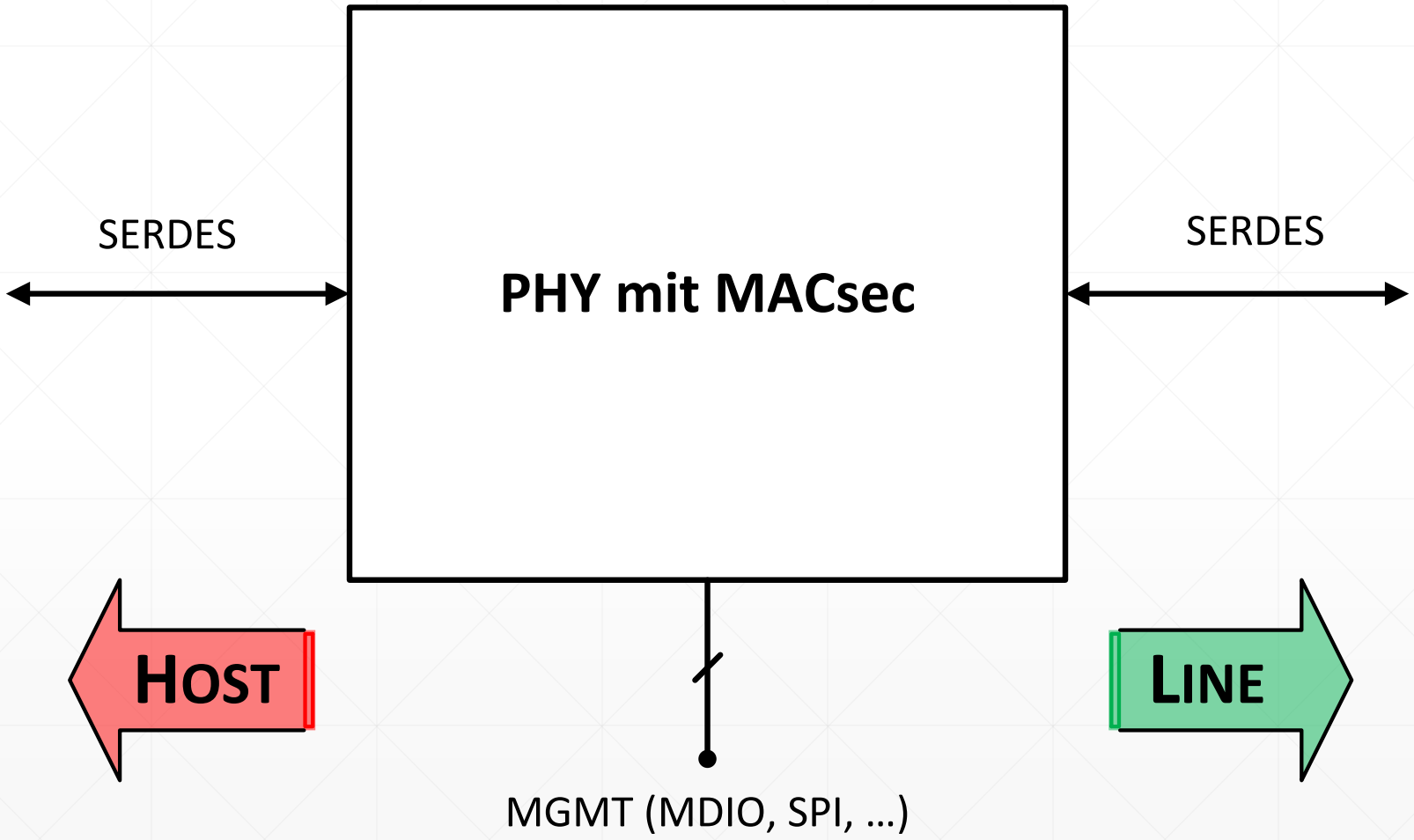


Linux MACsec als *virtual device*

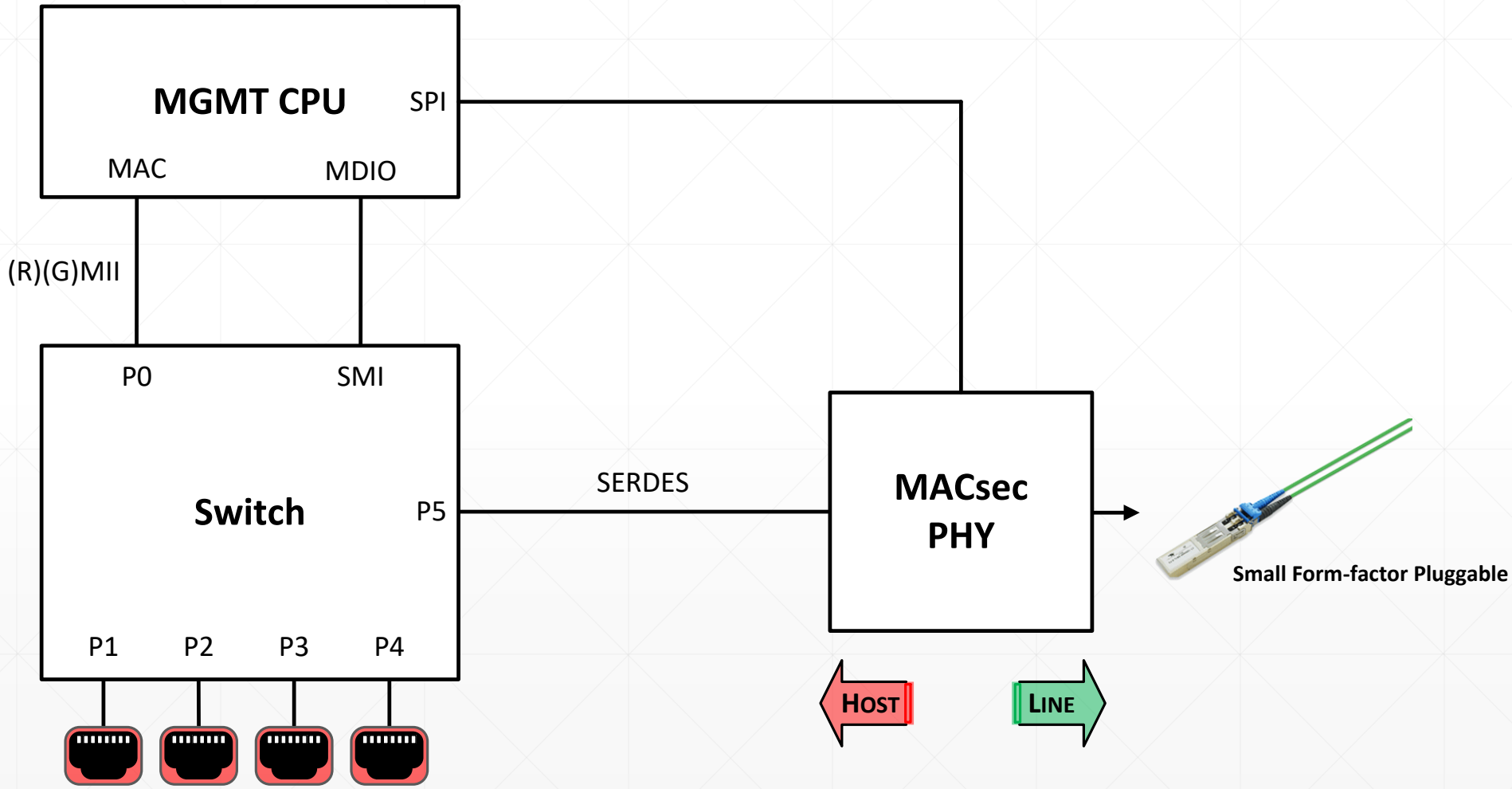
```
ip link add link eth0 macsec0 type macsec sci 0000000000A0001 cipher gcm-aes-256 encrypt on
```



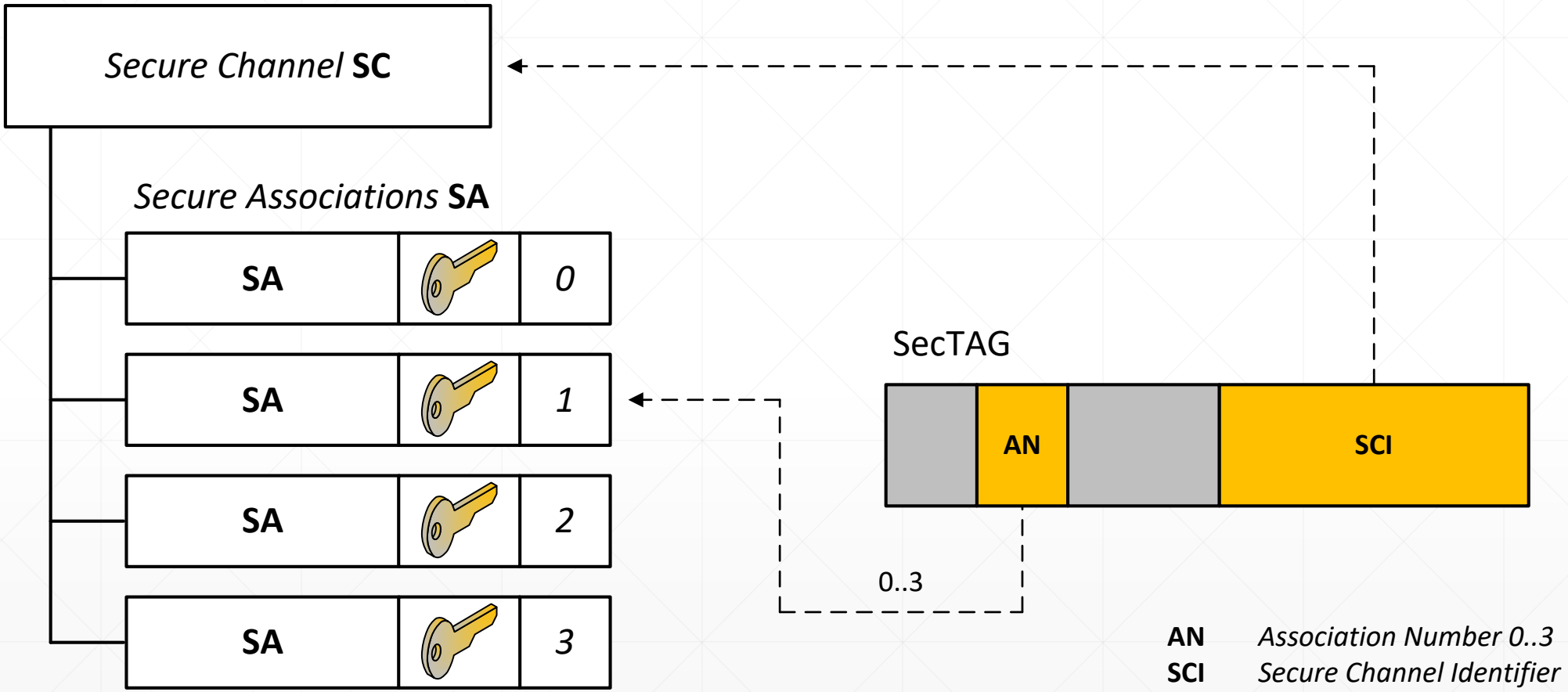
MACsec Hardware Implementierung mit PHY



Hardware Design Beispiel mit MACsec PHY

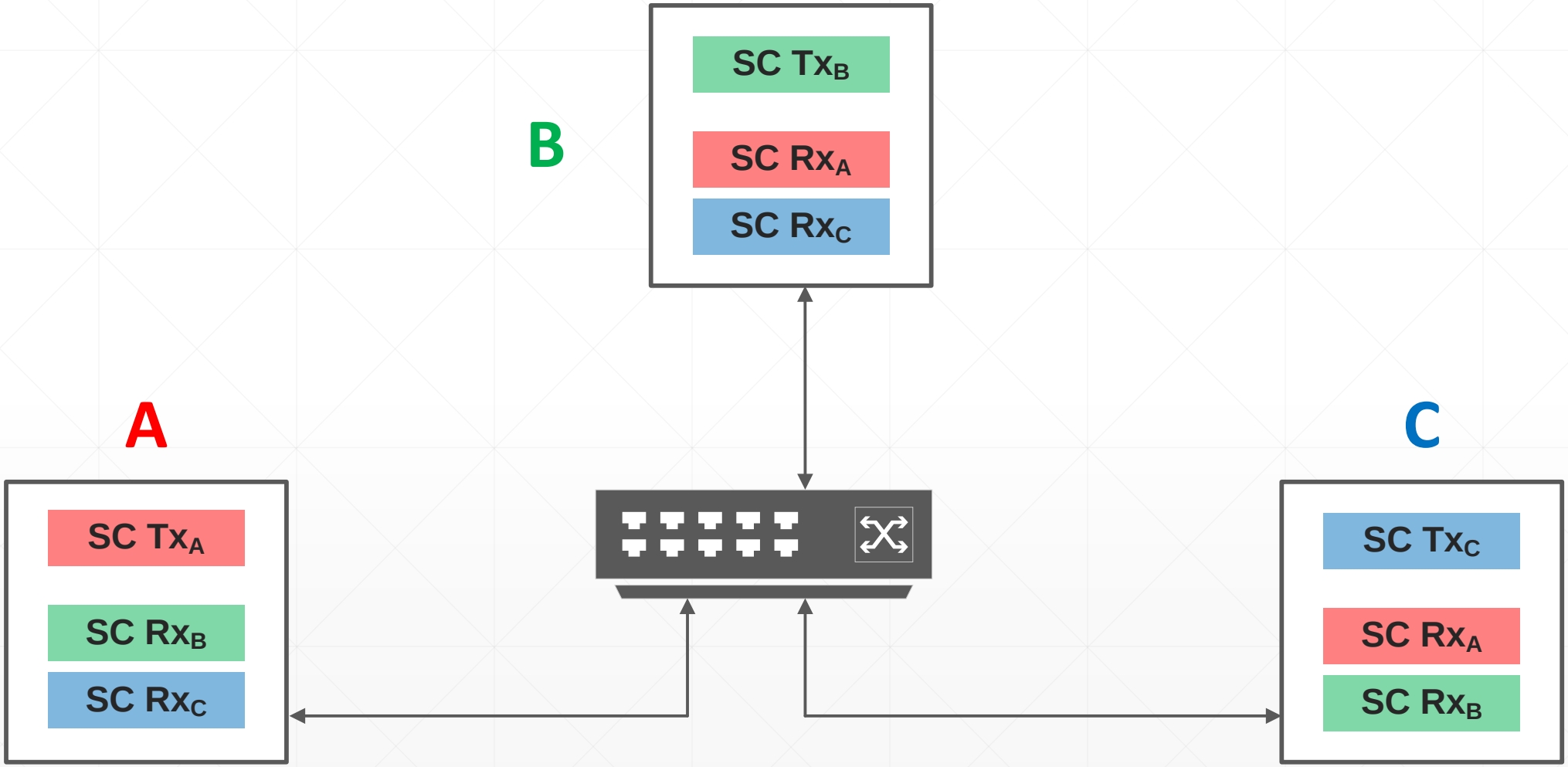


MACsec Struktur

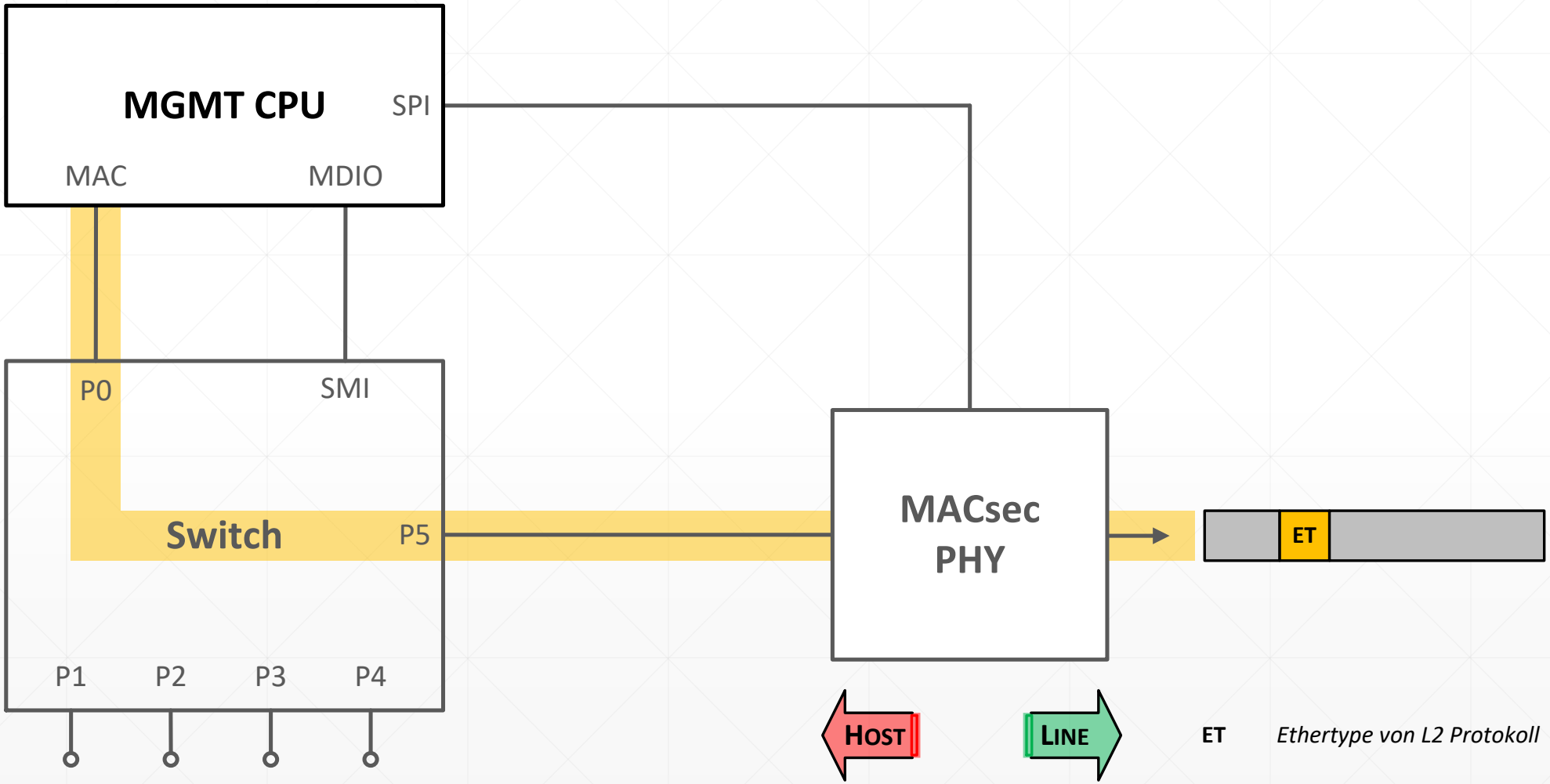


AN *Association Number 0..3*
SCI *Secure Channel Identifier*
SC *Secure Channel*
SA *Secure Association*

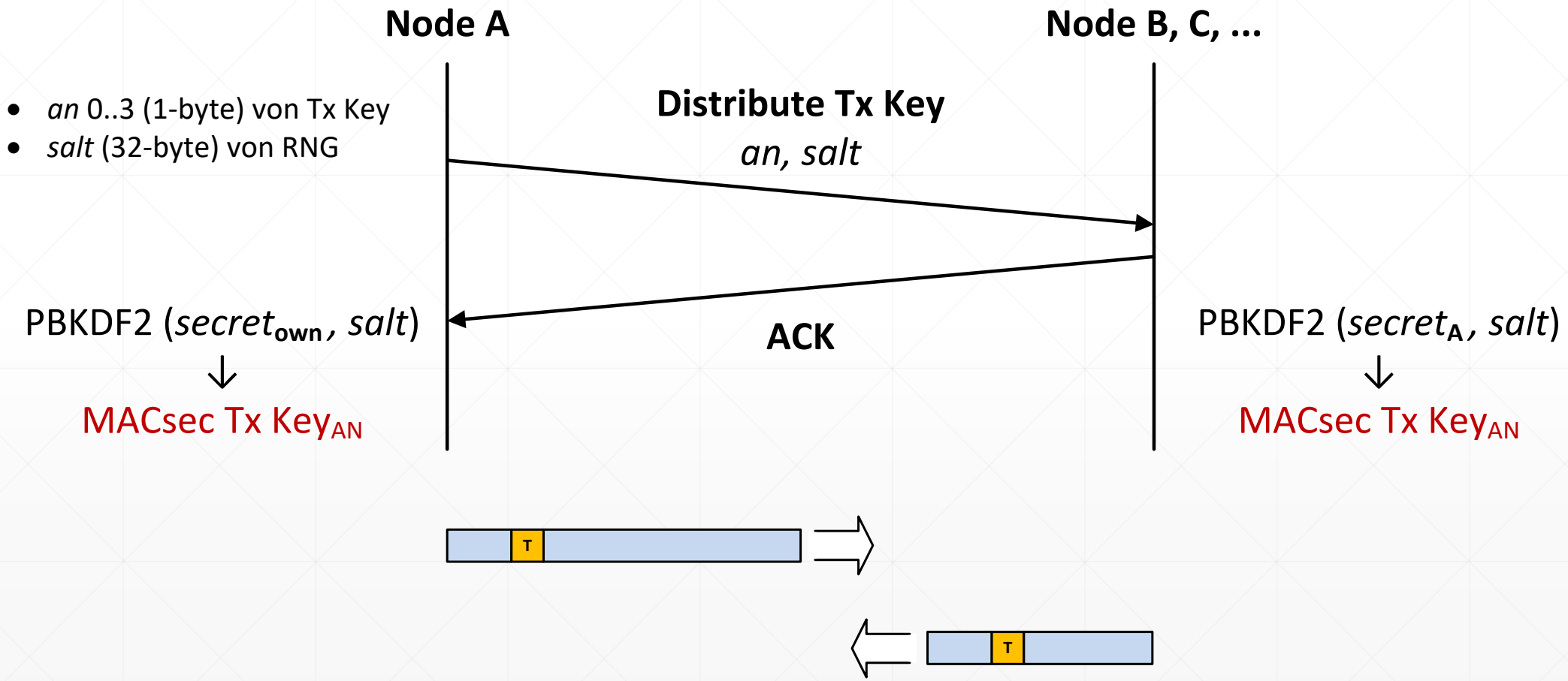
MACsec Schlüssel ist Tx basiert



MGMT CPU für Key Exchange über Layer 2



Test Key Exchange



Wie schnell ist eine Security Association verbraucht?

Frame Grösse	Frames / Sekunde @ 10 mbps
64	**14´880**
146	7´530
530	2´272
1538	812

worst case

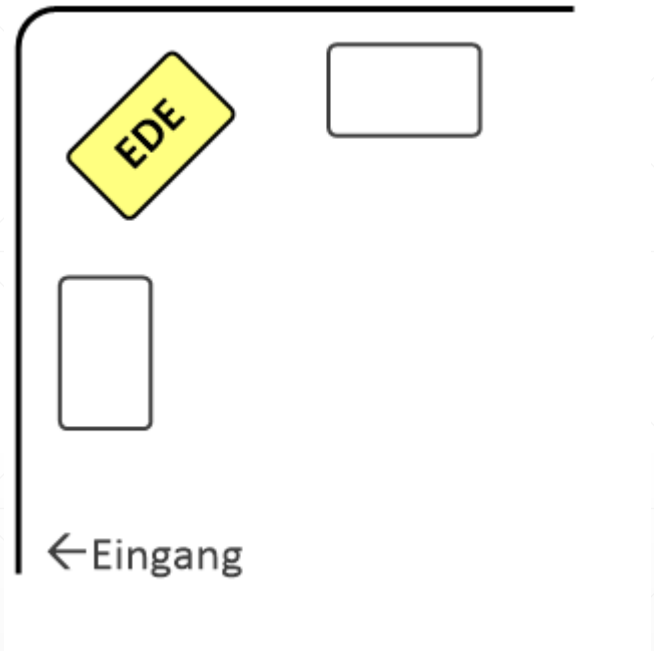
Bei Speed 10G : $\frac{2^{32}-1}{14´880´000}$ = PN in **289 s** verbraucht

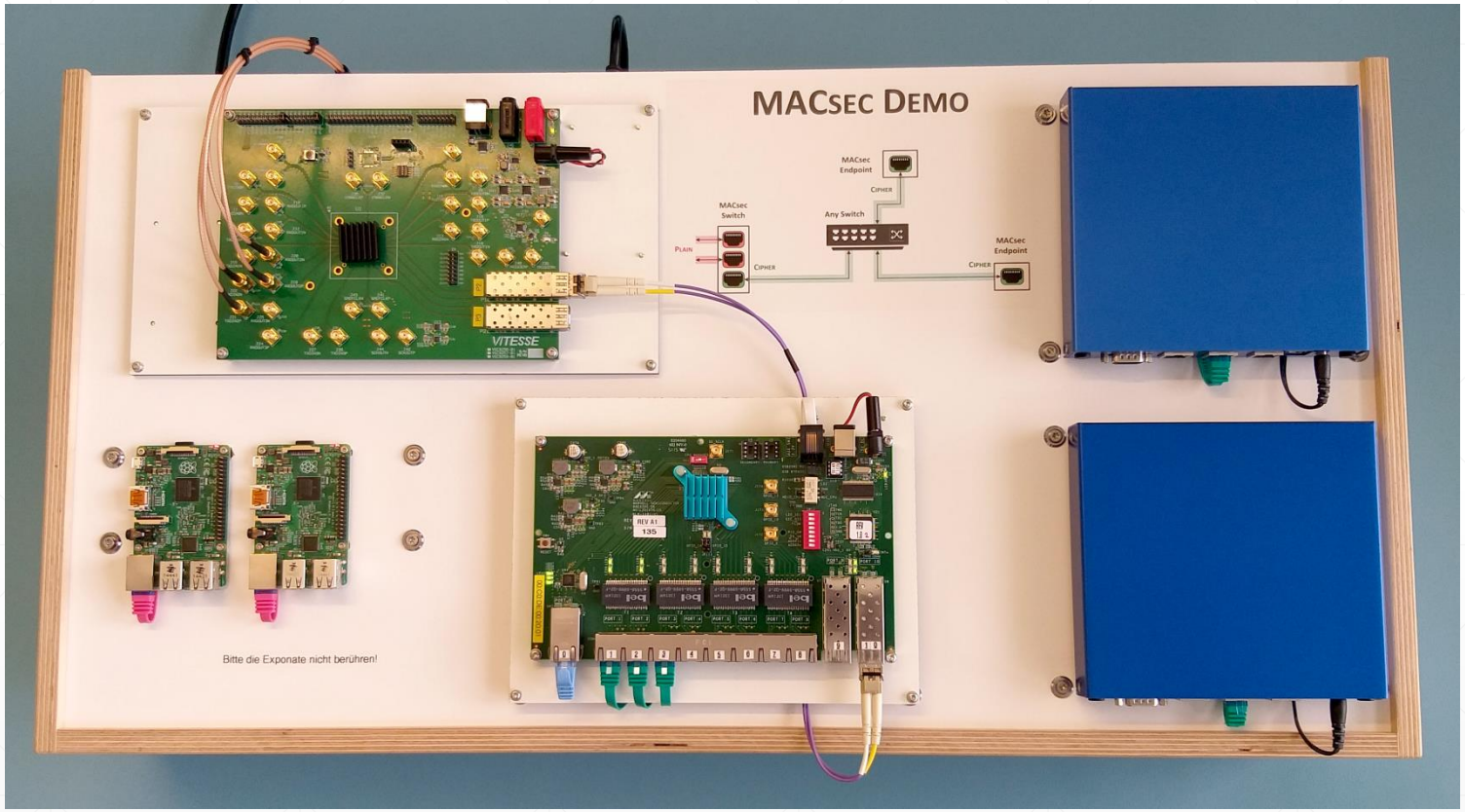
Übersicht MACsec IEEE-Standards

- 802.1AE (2006)
- Änderung: 802.1AEbn (2011) mit *AES/GCM-256*
- Änderung: 802.1AEbw (2013) mit *XPN (64-bit PN)*
- 802.1AE (2018)

- Weiterführende Standards: 802.1X (MKA)

Demo Time


EDE
←Eingang


MACsec Demo
MACsec Endpoint
Cipher
MACsec Switch
Any Switch
Plain
Cipher
MACsec Endpoint
Cipher
VITESSE
Bitte die Exponate nicht berühren!

Fragen?

Embedded Development GmbH

www.embedded-development.ch

Peter Voser

077 405 70 05 Mobile

peter.voser@voser-development.ch