

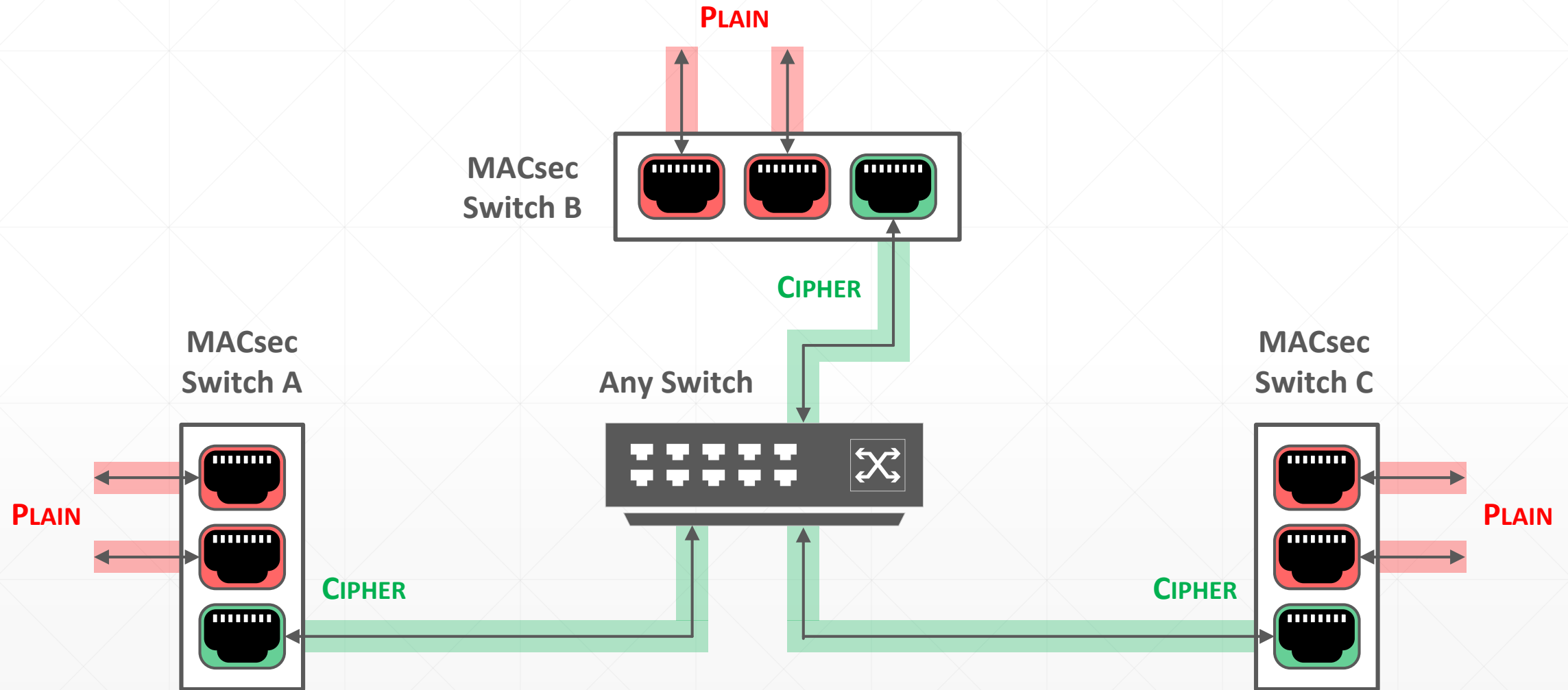
LAN Security mit MACsec

Referat von Peter Voser

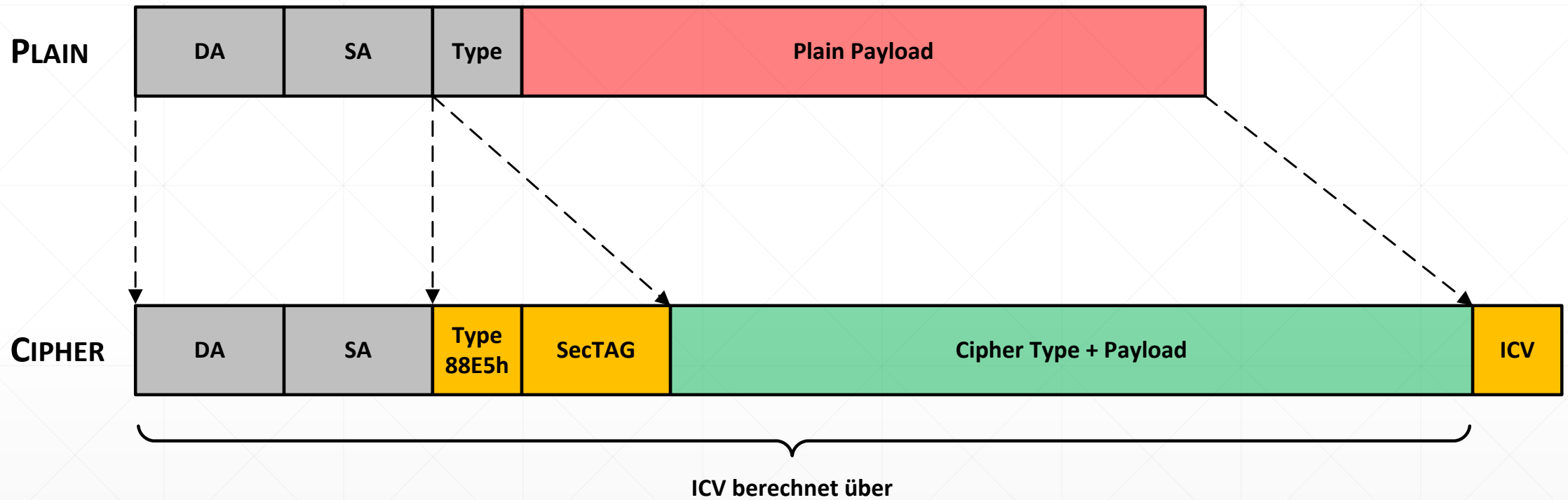
Agenda

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

Ein LAN mit MACsec

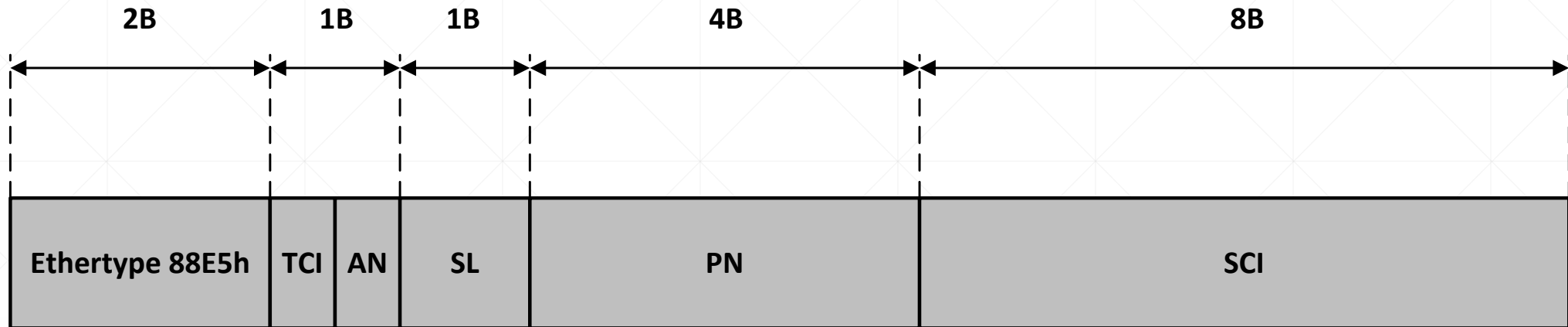


Layer 2 Frames



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

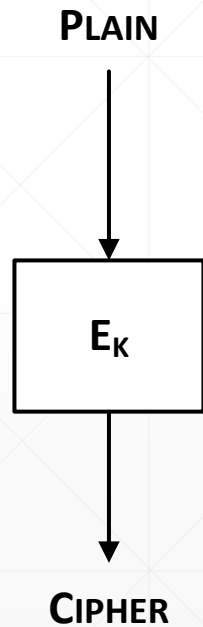
802.1AE Security Tag (Header)



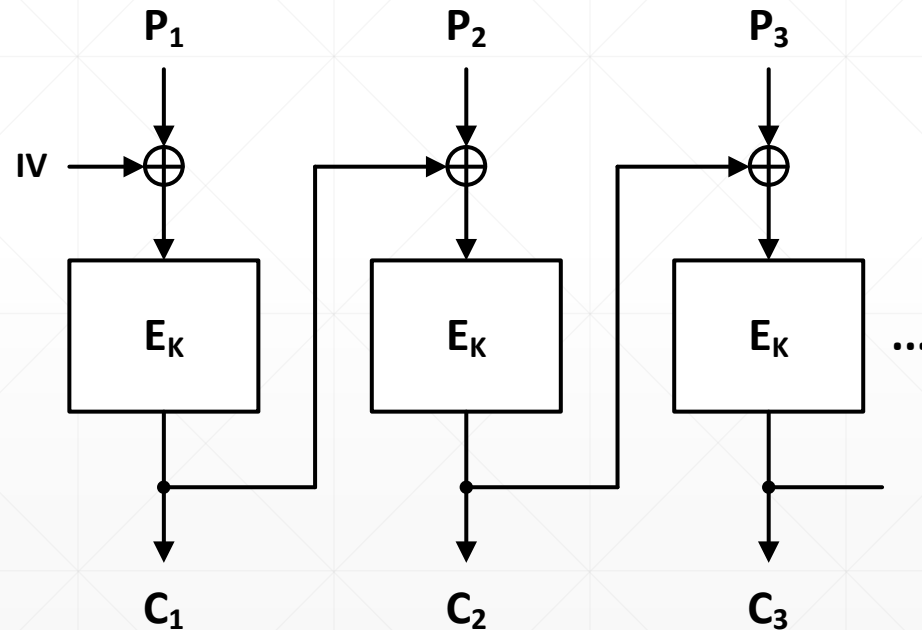
TCI *Tag Control Information*
AN *Association Number*
SL *Short Length*
PN *Packet Number*
SCI *Secure Channel Identifier*

AES Betriebsarten

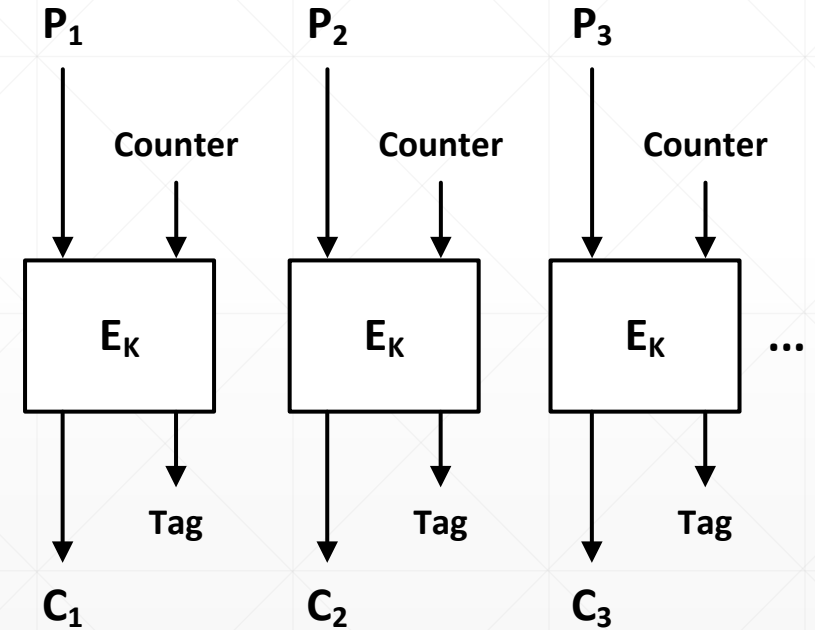
1. ECB (ELECTRONIC CODE BOOK)



2. CBC (CIPHER BLOCK CHAIN)



3. CM (COUNTER MODE)



Linux MACsec Kernelmodul

```
.config - Linux/arm64 5.10.72 Kernel Configuration
> Device Drivers > Network device support -
Network device support
Arrow keys navigate the menu. <Enter> selects submenus ---> (or empty submenus ----). Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes, <M> modularizes features. Press <Esc><Esc> to exit, <F1> for Help, </> for Search. Legend: [*] built-in [ ] excluded <M> module < > module capable

^(-)
< > MAC-VLAN support
< > IP-VLAN support
< > Virtual eXtensible Local Area Network (VXLAN)
< > Generic Network Virtualization Encapsulation
< > Bare UDP Encapsulation
< > GPRS Tunneling Protocol datapath (GTP-U)
<*> IEEE 802.1AE MAC-level encryption (MACsec)
< > Network console logging support
< > Universal TUN/TAP device driver support
[ ] Support for cross-endian vnet headers on little-endian kernels
< > Virtual ethernet pair device
```

Linux MACsec als *virtual device*

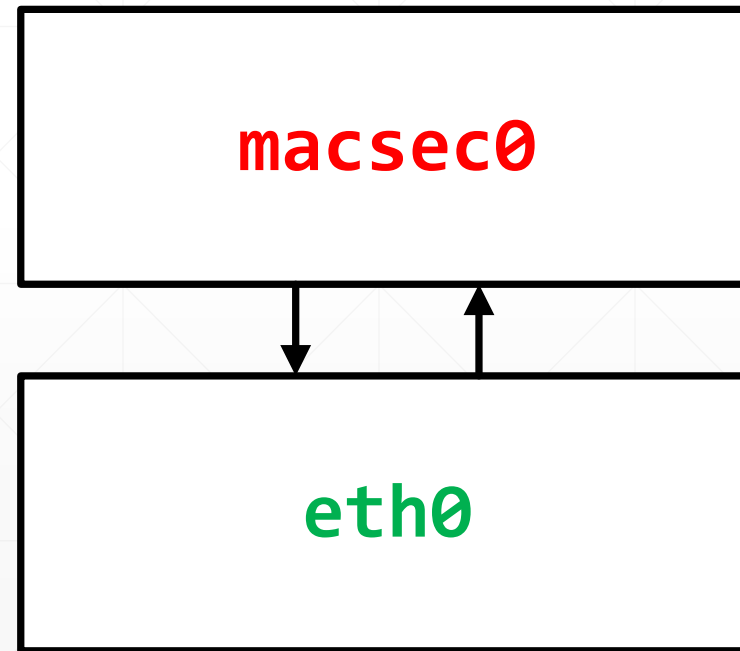
```
ip link add link eth0 macsec0 type macsec sci 000000000000A0001 cipher gcm-aes-256 encrypt on
```

Virtual MACsec Device

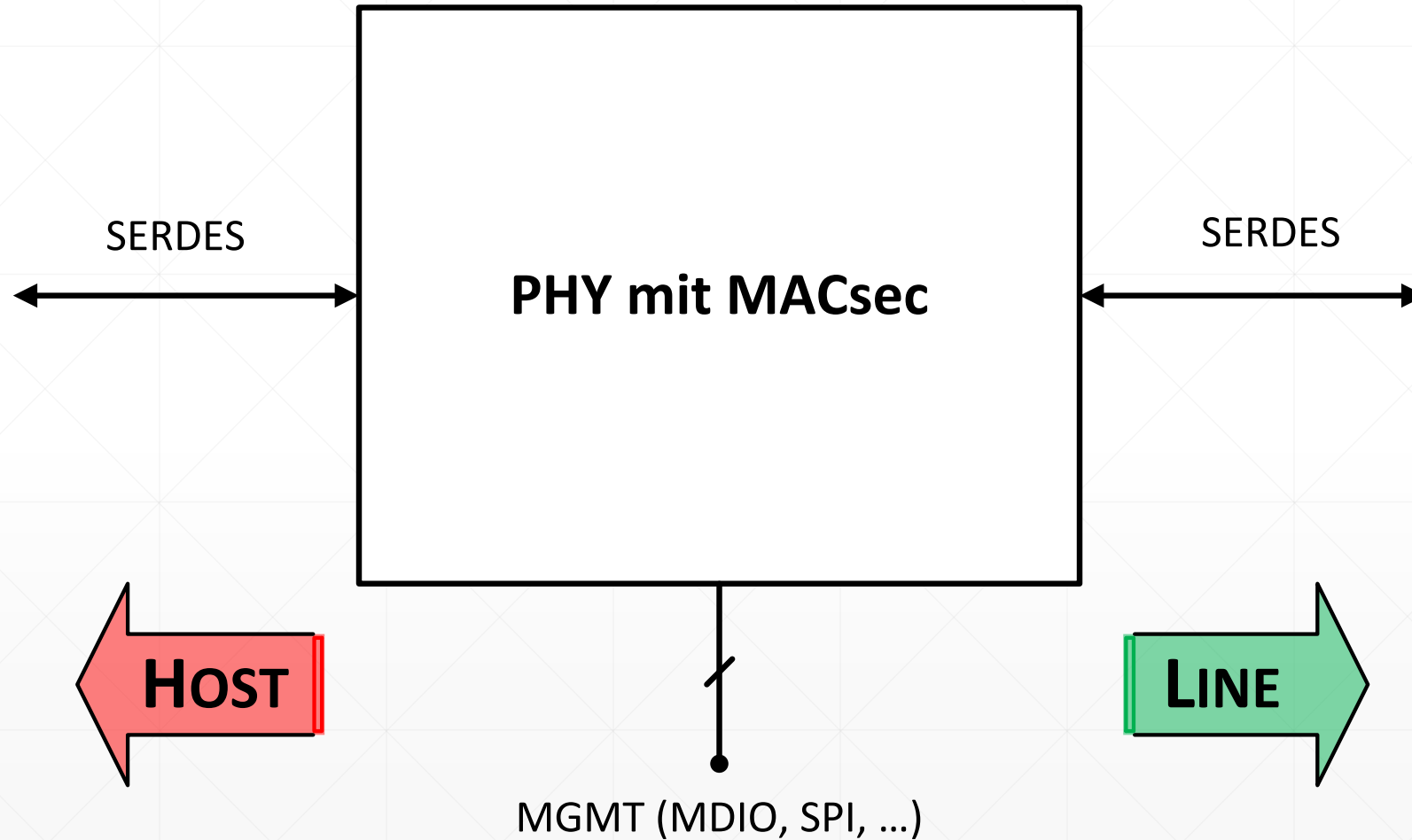
macsec0

Parent Device

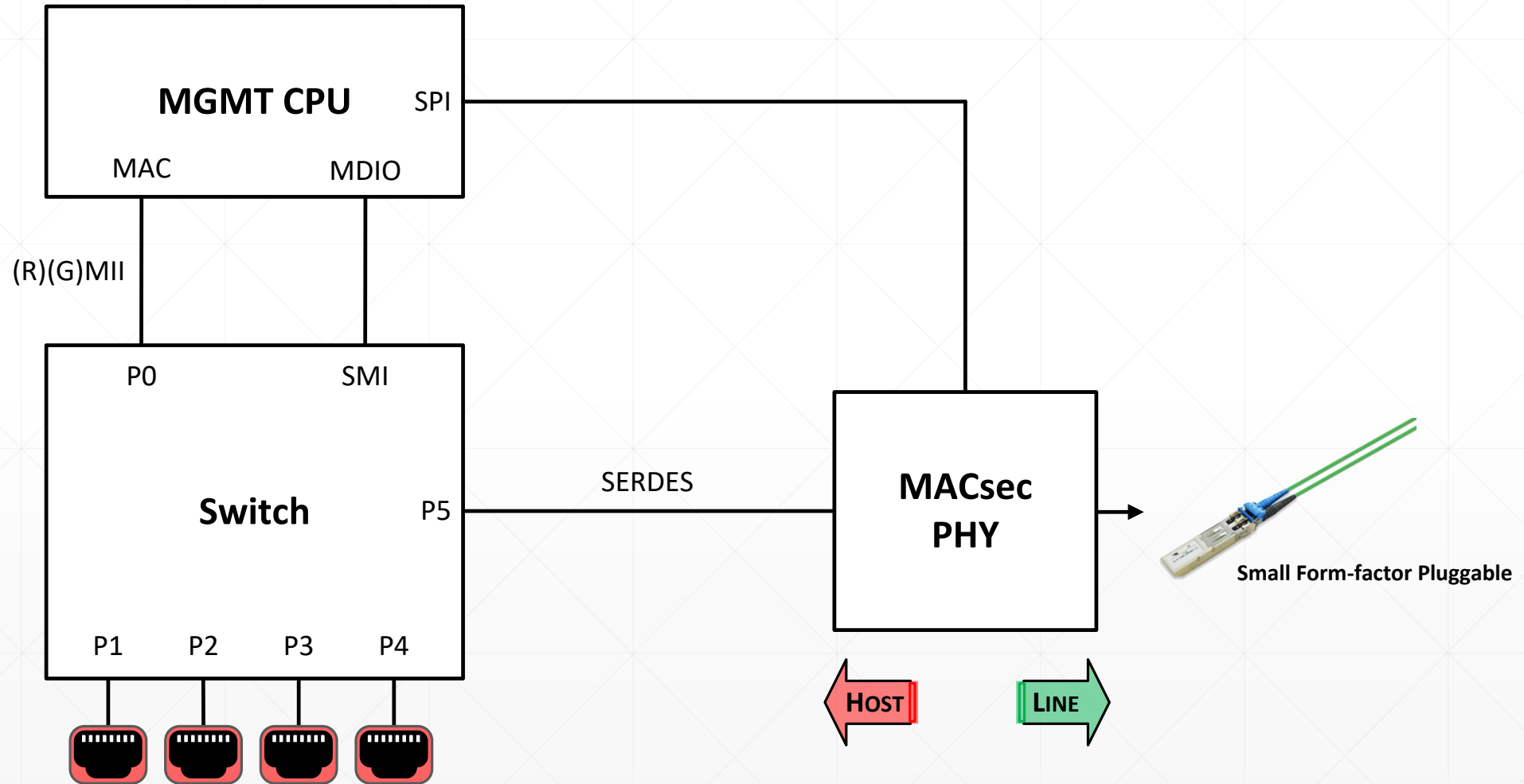
eth0



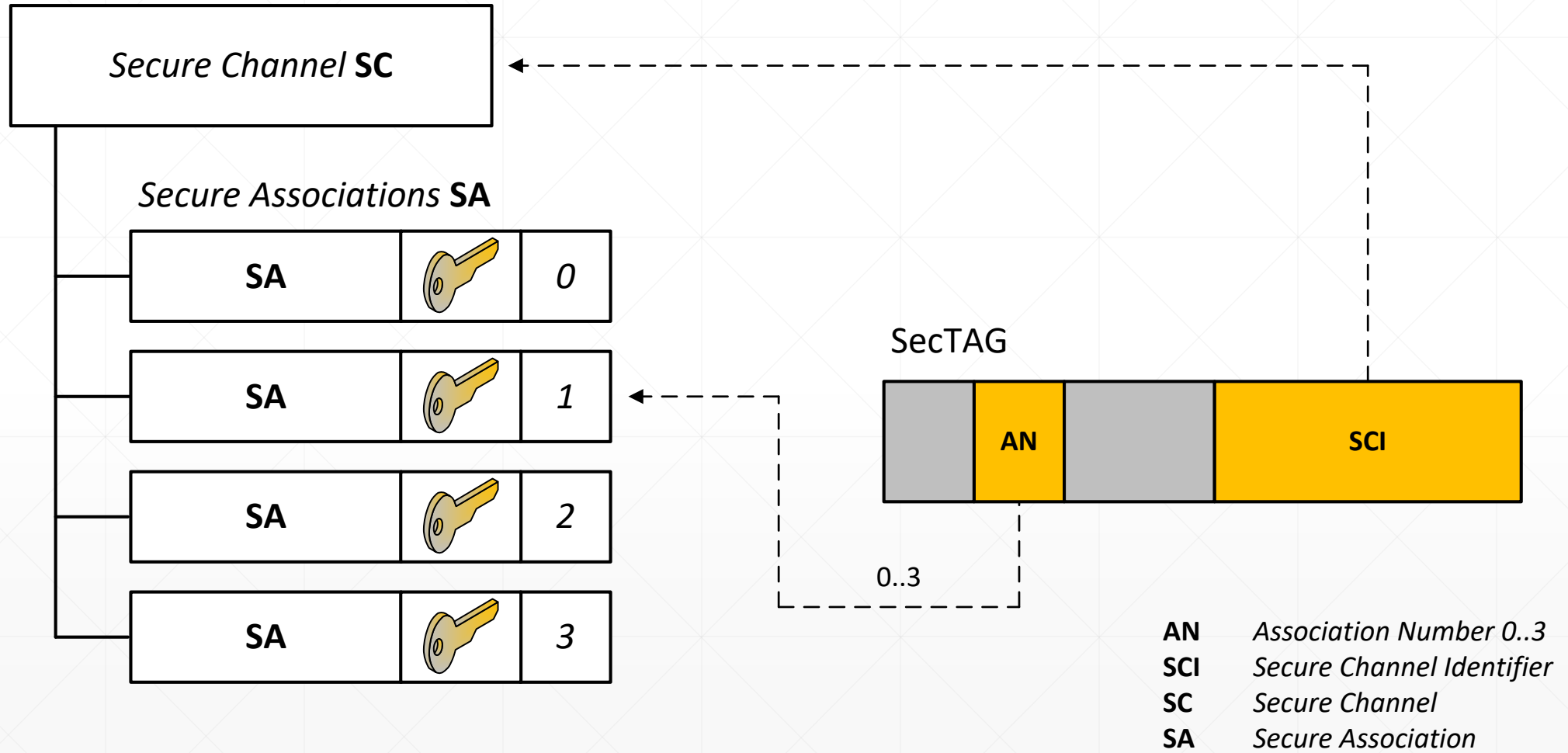
MACsec Hardware Implementierung mit PHY



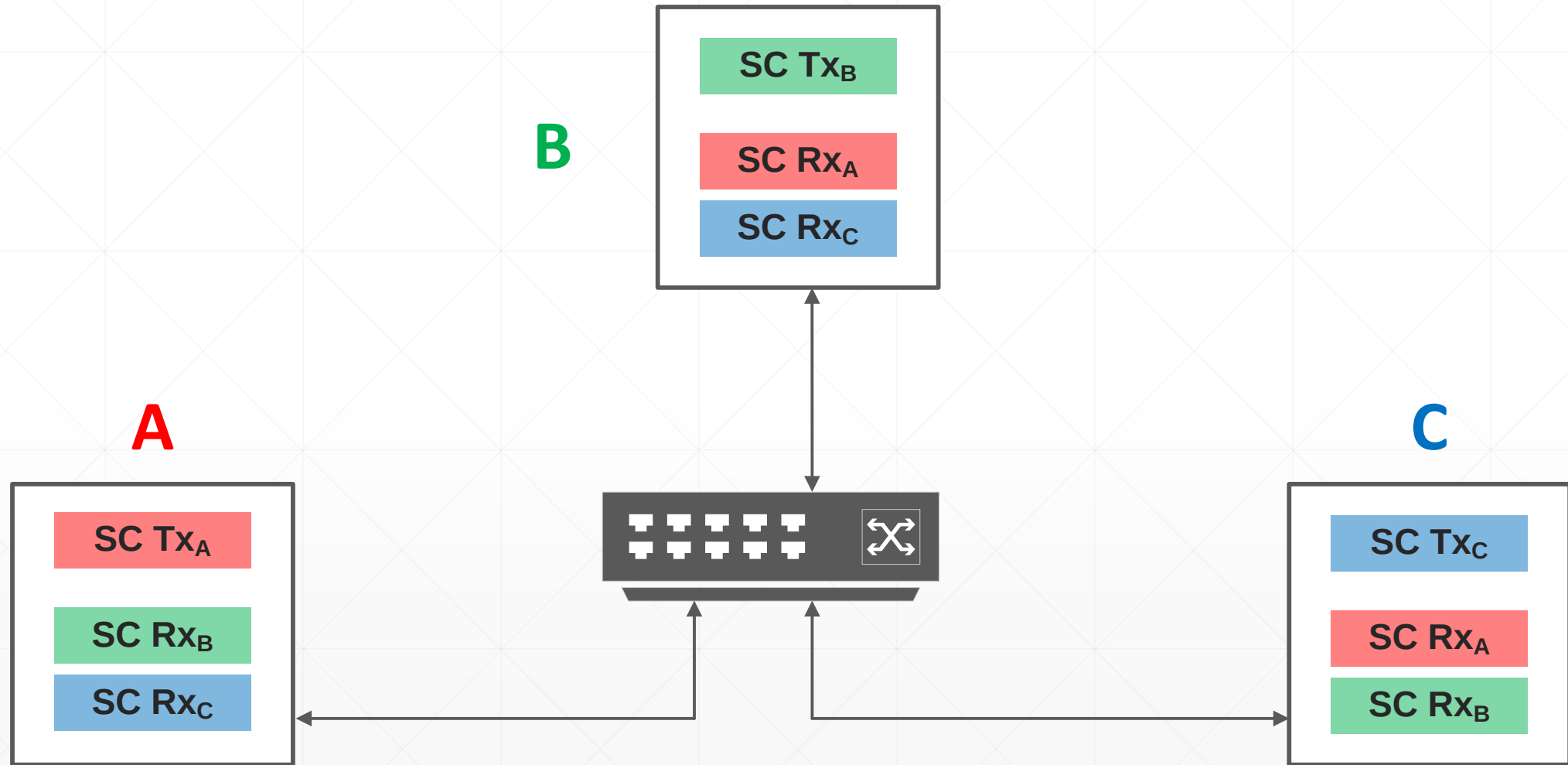
Hardware Design Beispiel mit MACsec PHY



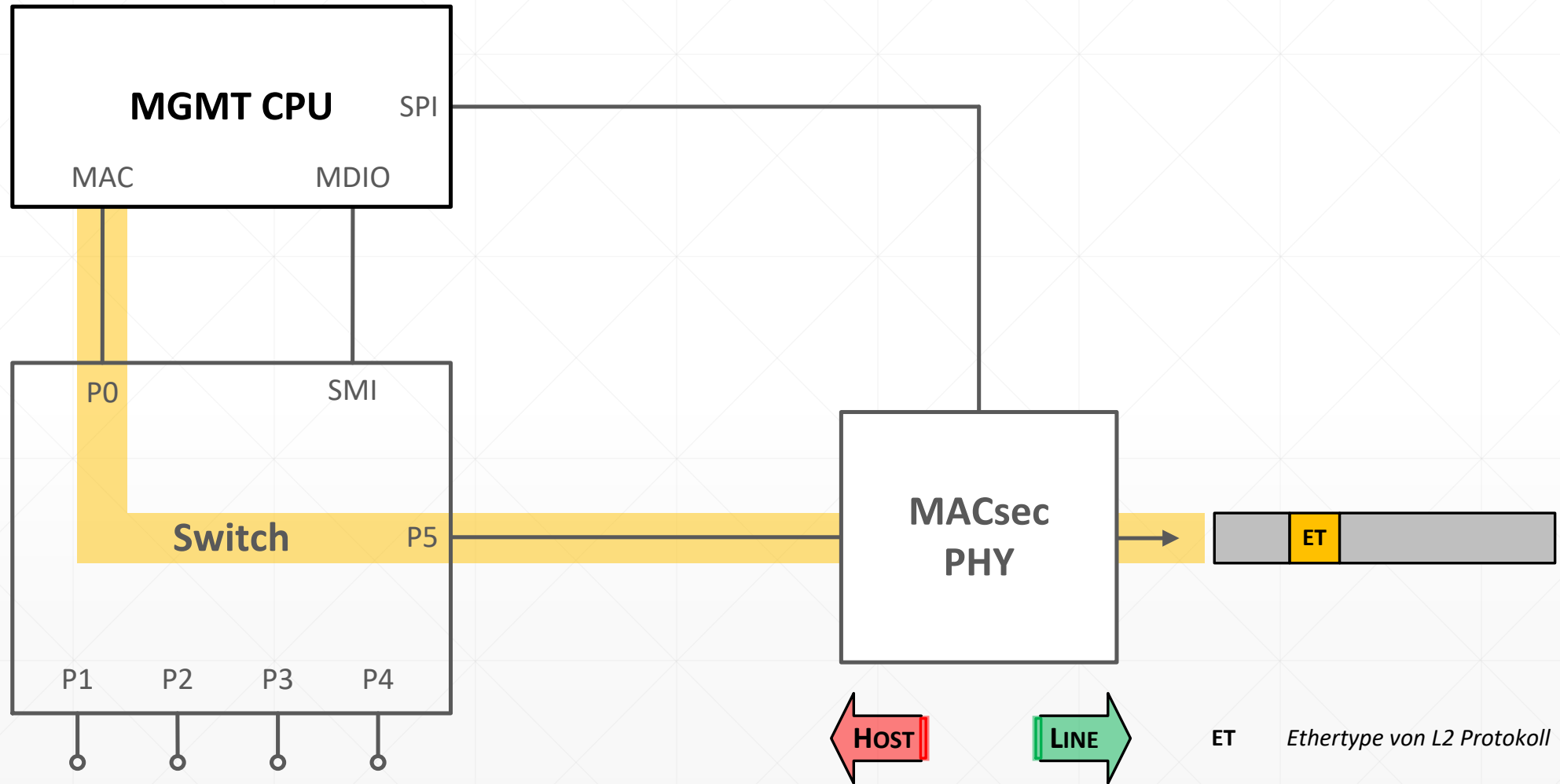
MACsec Struktur



MACsec Schlüssel ist Tx basiert

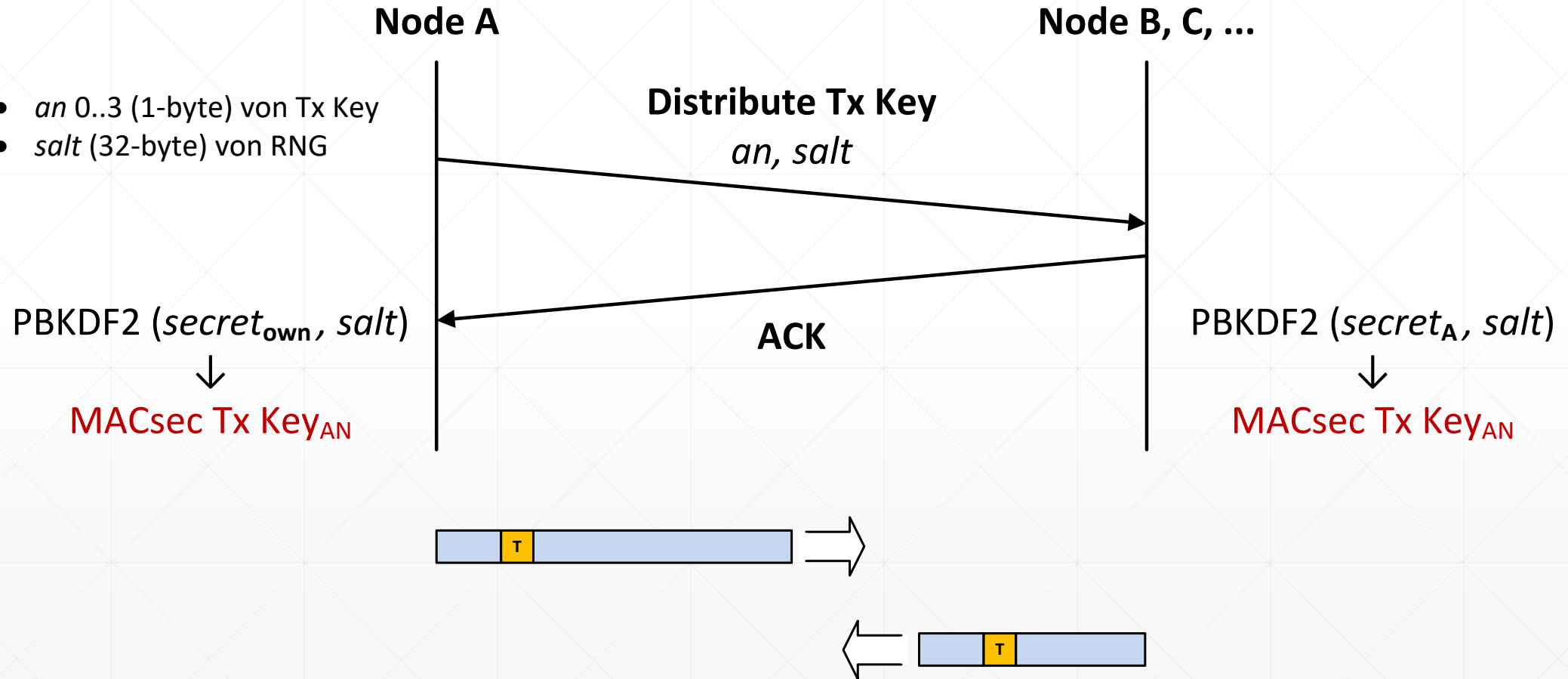


MGMT CPU für Key Exchange über Layer 2



Test Key Exchange

- an 0..3 (1-byte) von Tx Key
- $salt$ (32-byte) von RNG



Wie schnell ist eine Security Association verbraucht?

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



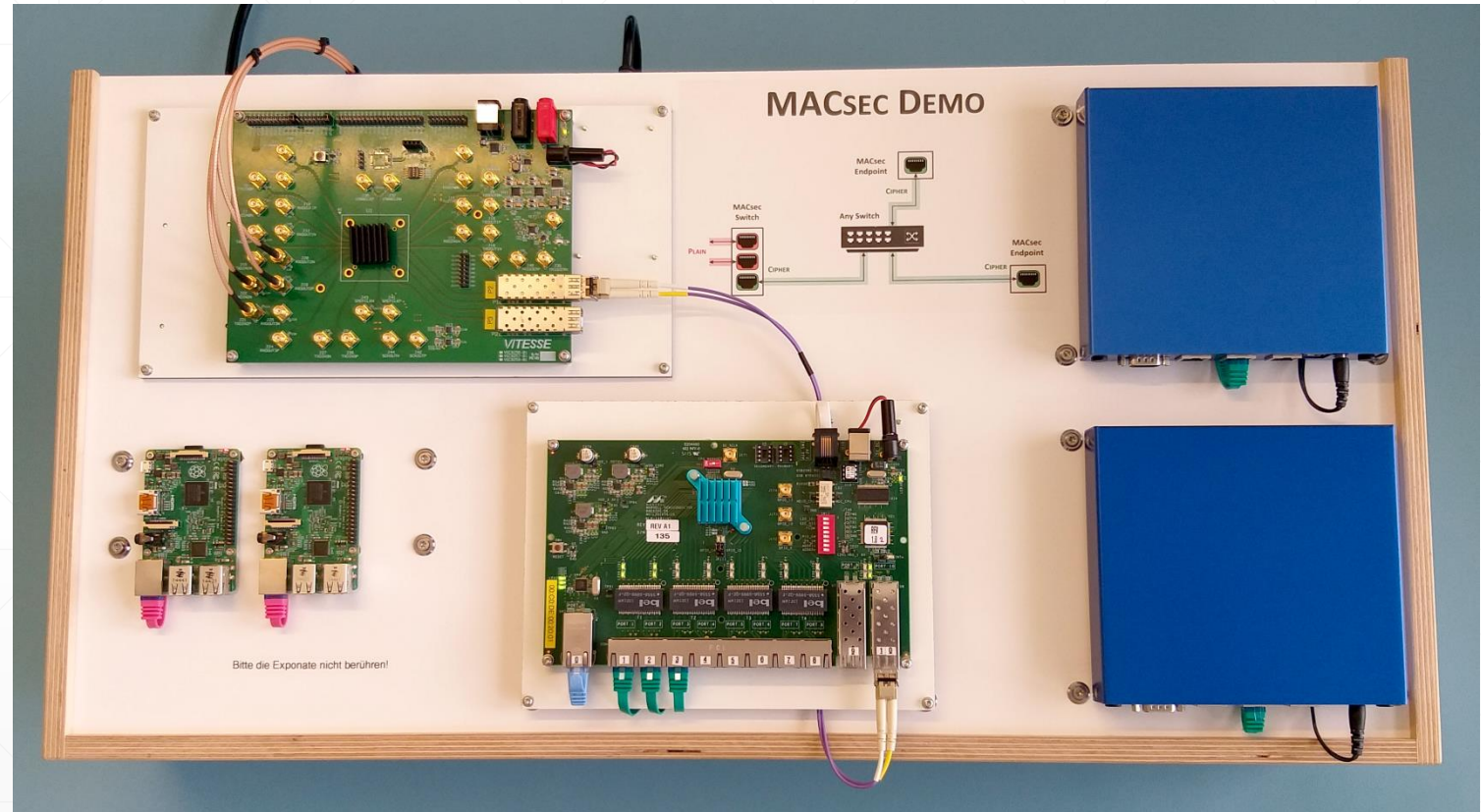
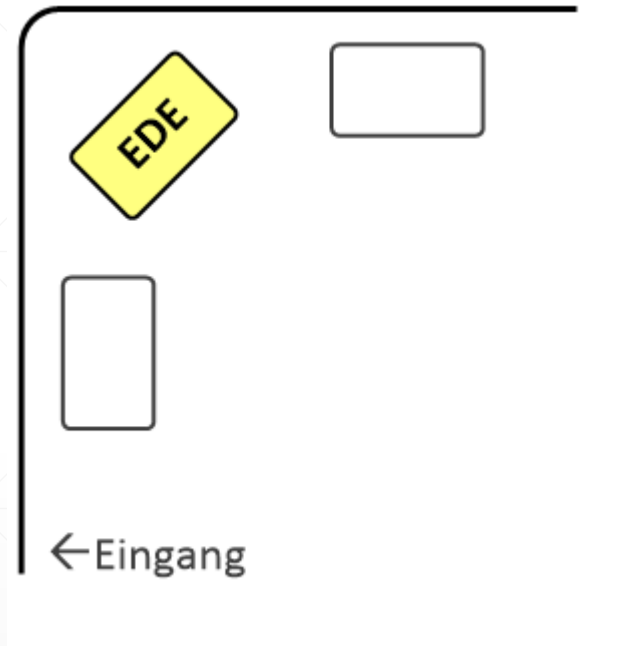
worst case

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

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



Fragen?

Embedded Development GmbH
www.embedded-development.ch

Peter Voser
077 405 70 05 Mobile
peter.voser@vosser-development.ch