WIRESHARK EDUCATION DAY – Olten CH 2026

# MACsec

## Überblick über MACsec und Analyse mit Wireshark

Benjamin Pfister

# Über mich

- Benjamin Pfister
- Leiter Netze & Telekommunikation
- IT-Consultant / Trainer
- Freier Autor
- Vater von BabyShark


# Inhalt

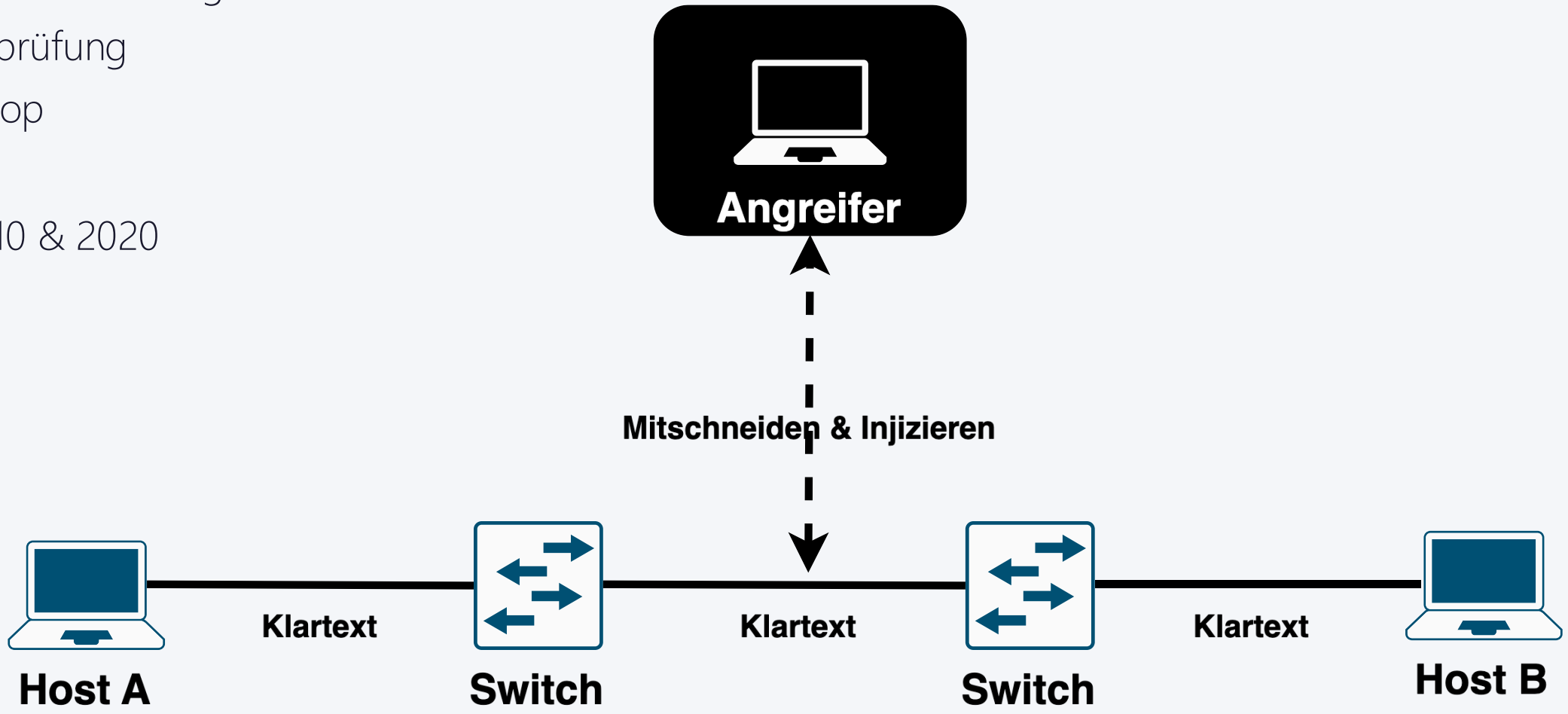


- Was ist MACsec?
- Anwendungsszenarien
- Frame-Aufbau
- Schlüsselverteilung & Analyse

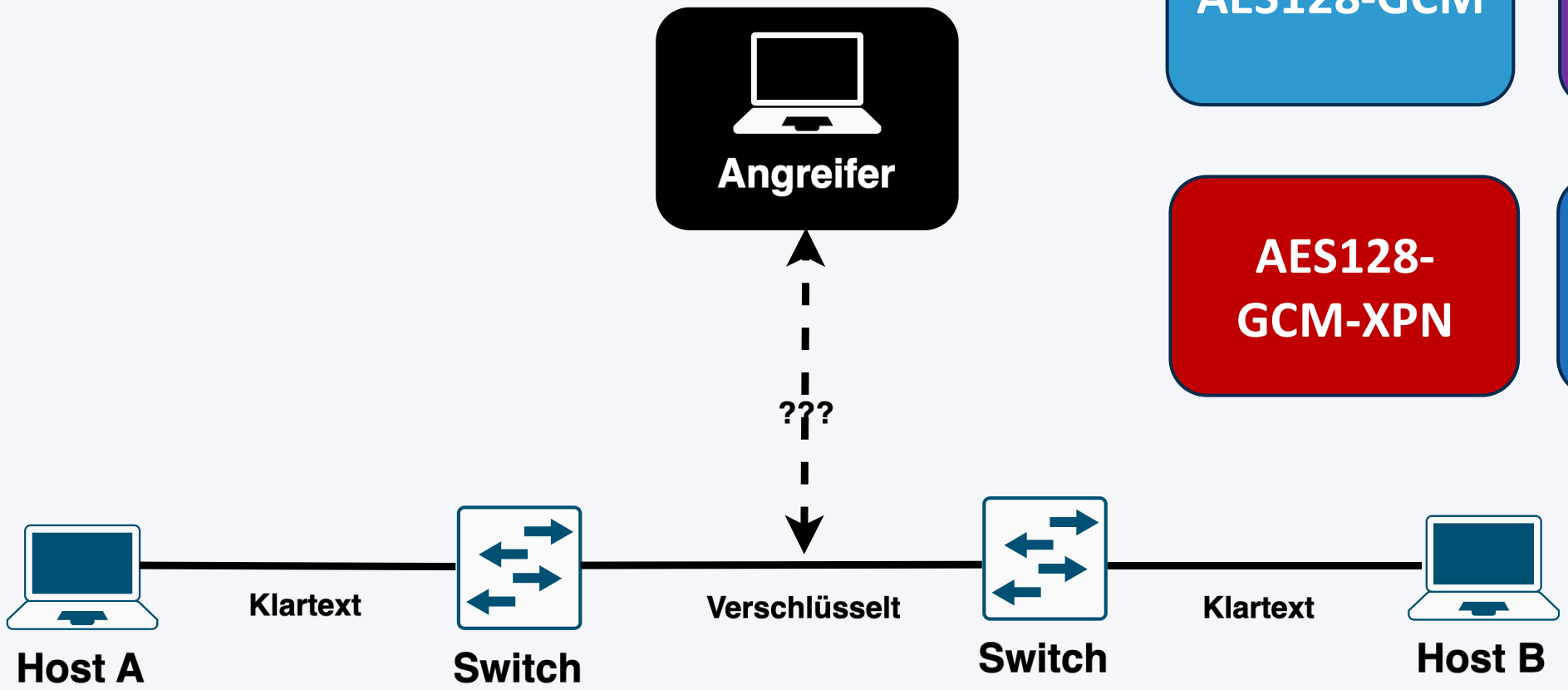
# Was ist MACsec?

# Was ist MACsec?

- Layer 2 Verschlüsselung
- Integritätsprüfung
- Hop-by-Hop
- 802.1AE
- 802.1X-2010 & 2020



# Was ist MACsec?



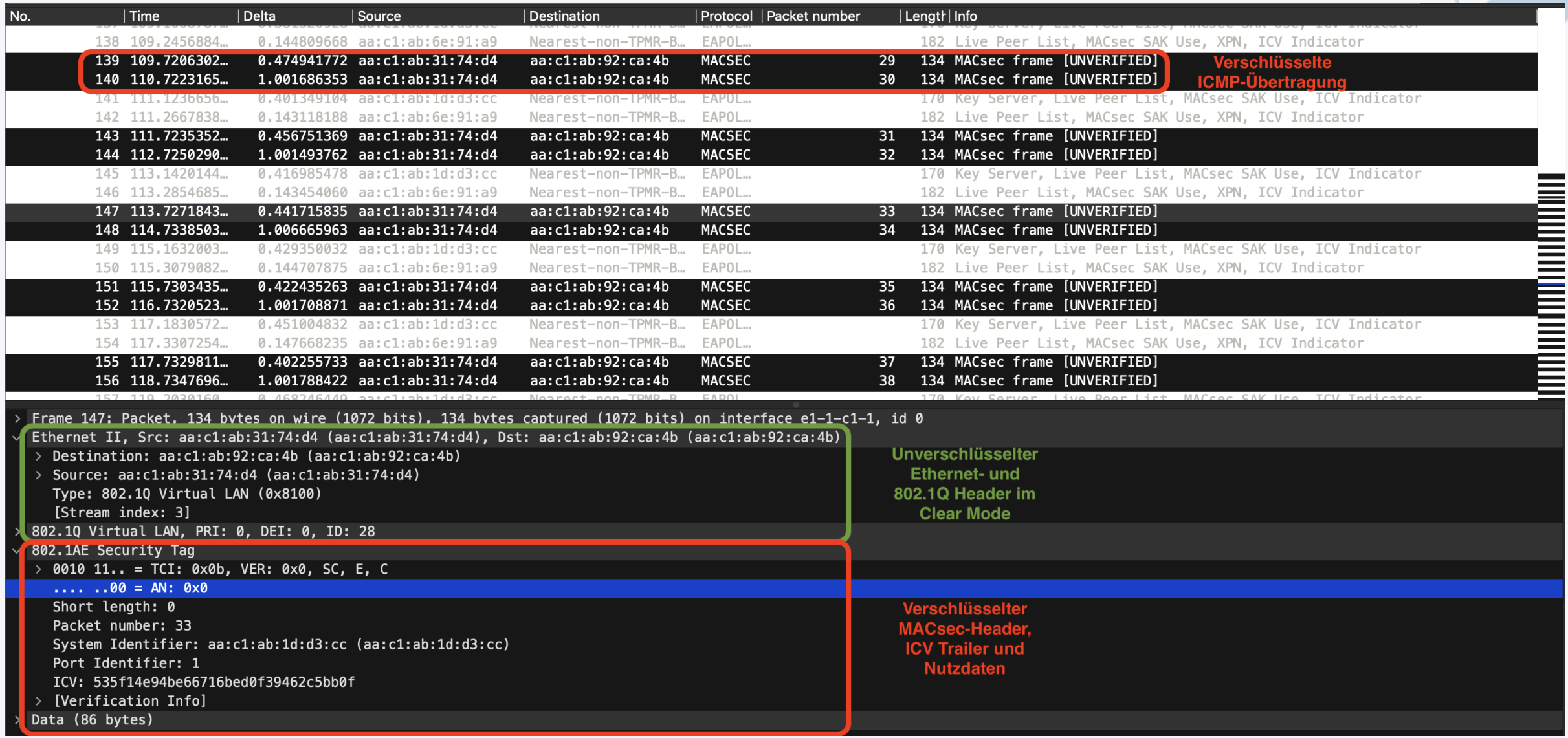

AES128-GCM

AES256-GCM

AES128-GCM-XPN

AES256-GCM-XPN

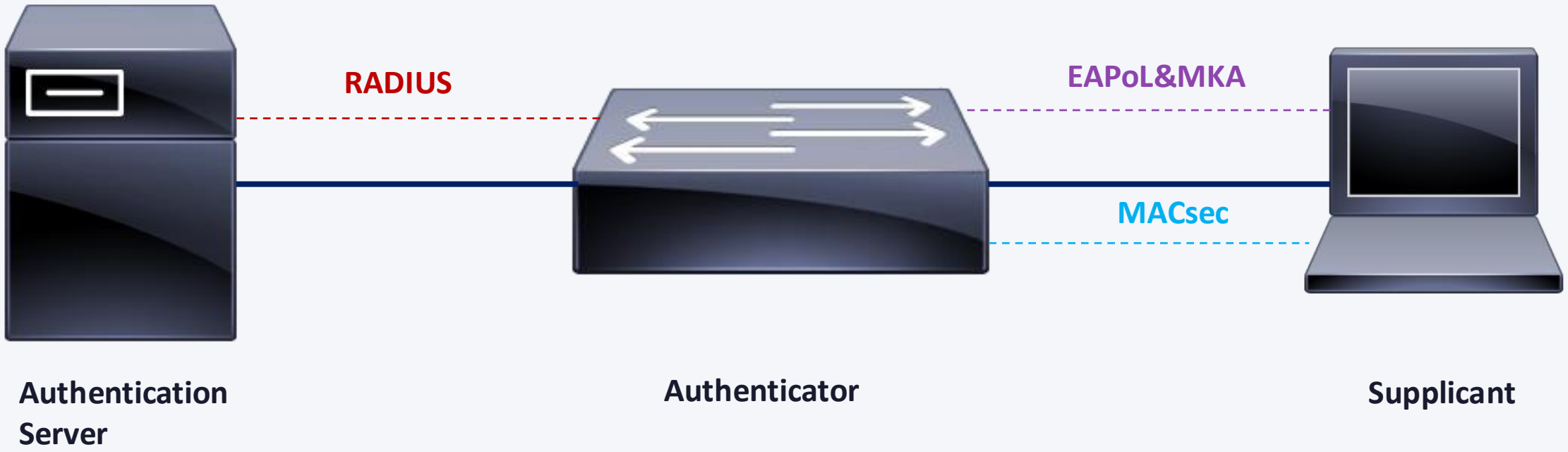
# Was ist MACsec?



# Anwendungsszenarien

# Anwendungsszenarien

- Switch <-> Endgerät



# Anwendungsszenarien

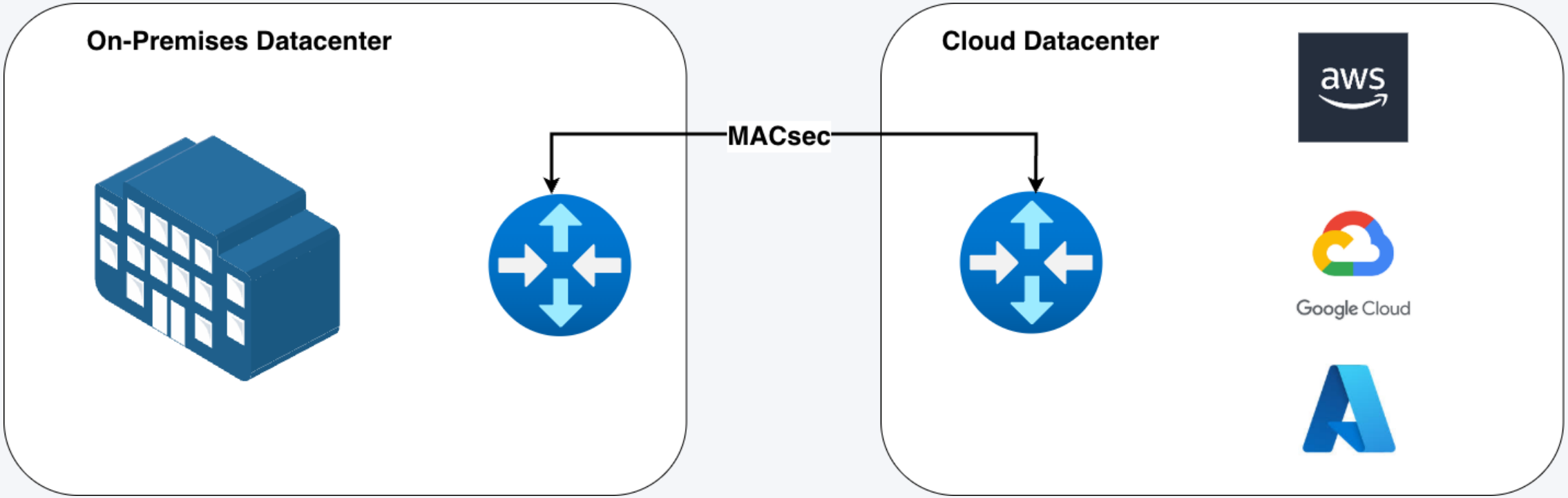
- Switch <-> Switch

**Authentifizierung über PSK**


**Verschlüsselung der Nutzdaten**

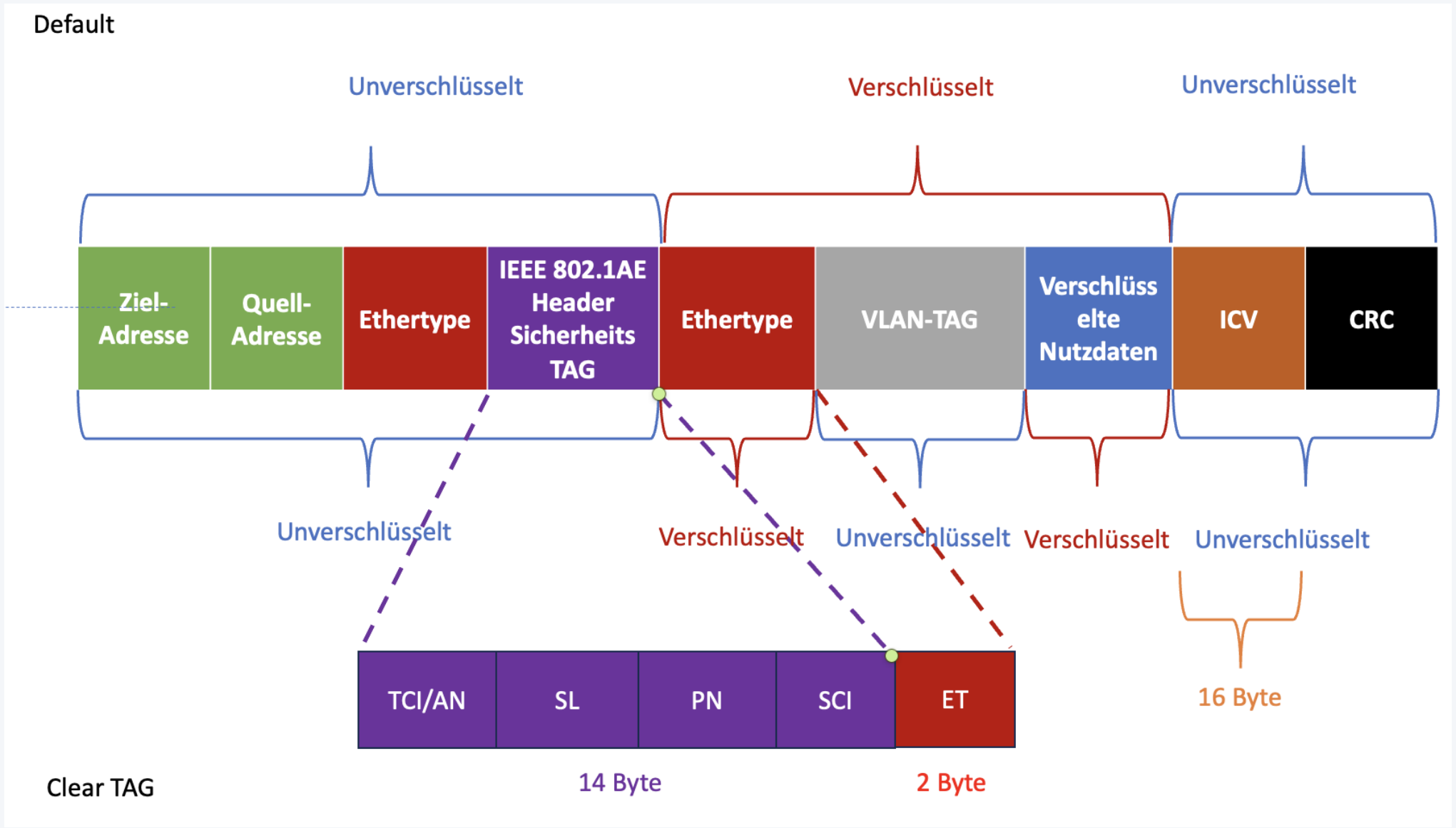
# Anwendungsszenarien

- Anbindung Cloud-Provider



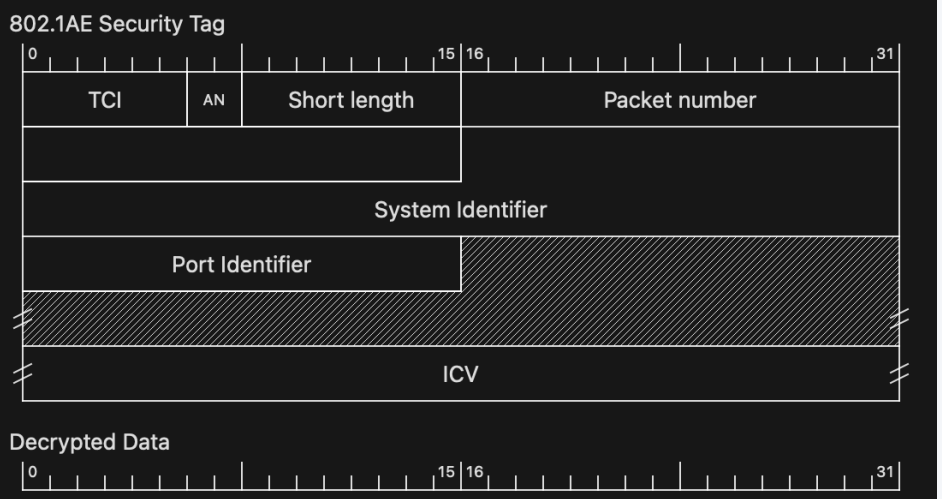
# Frame-Aufbau

# Frame-Aufbau



# Frame-Aufbau

```
> Frame 103: Packet, 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface
> Ethernet II, Src: aa:c1:ab:31:74:d4 (aa:c1:ab:31:74:d4), Dst: aa:c1:ab:92:ca:4b (aa:c1:ab:92:
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 28
v 802.1AE Security Tag
  > 0010 11.. = TCI: 0x0b, VER: 0x0, SC, E, C
    .... ..00 = AN: 0x0
    Short length: 0
    Packet number: 11
    System Identifier: aa:c1:ab:1d:d3:cc (aa:c1:ab:1d:d3:cc)
    Port Identifier: 1
    Ethertype: IPv4 (0x0800)
    ICV: 0e79bda1a54cb43961971292ac83ae16
  > [Verification Info]
  Decrypted Data: 08004500005483450000400 19b3eac110202ac1102010000d898000b000755a8bd69000000005
> Internet Protocol Version 4, Src: 172.17.2.2, Dst: 172.17.2.1
> Internet Control Message Protocol
```



# Wichtige Begrifflichkeiten

| Begrifflichkeit | Beschreibung |
|---|---|
| MKA | MACsec Key Agreement: Schlüsseleinigungsprotokoll, um MACsec Peers aufzufinden, Schlüssel zu generieren, zu erneuern und auszutauschen. |
| CKN | Connectivity Association Key Name: Dient als Rahmen für den CAK. Die Peers übertragen diesen untereinander zur Validierung im Klartext. |
| CAK | Connectivity Association Key: Schlüssel der Control-Plane, von dem der Sessionschlüssel abgeleitet wird. |
| SAK | Security Association Key: Sessionschlüssel, der vom CAK abgeleitet wurde und zur Verschlüsselung zwischen zwei MACsec Peers Verwendung findet. |
| MSK | Master Session Key: Wird innerhalb EAP-Austausch generiert. Supplicant- und Authentifizierungsserver verwenden MSK, um CAK zu generieren. |

# Schlüsselverteilung & Analyse

# Analyse mit Wireshark

- Was können wir allgemein analysieren?
  - Validieren ob verschlüsselt
  - Fehler im MKA
    - Fehler Übertragung EAPoL-Frames
    - Key Server-Auswahl
    - CAK-Namen
    - Confidentiality Offset
    - SAK-Verteilung
  - ICV-Fehler durch Manipulation oder Übertragungsfehler
  - Paketverlust anhand Paketnummer
  - Latenz mit Paketnummer

# Schlüsselverteilung

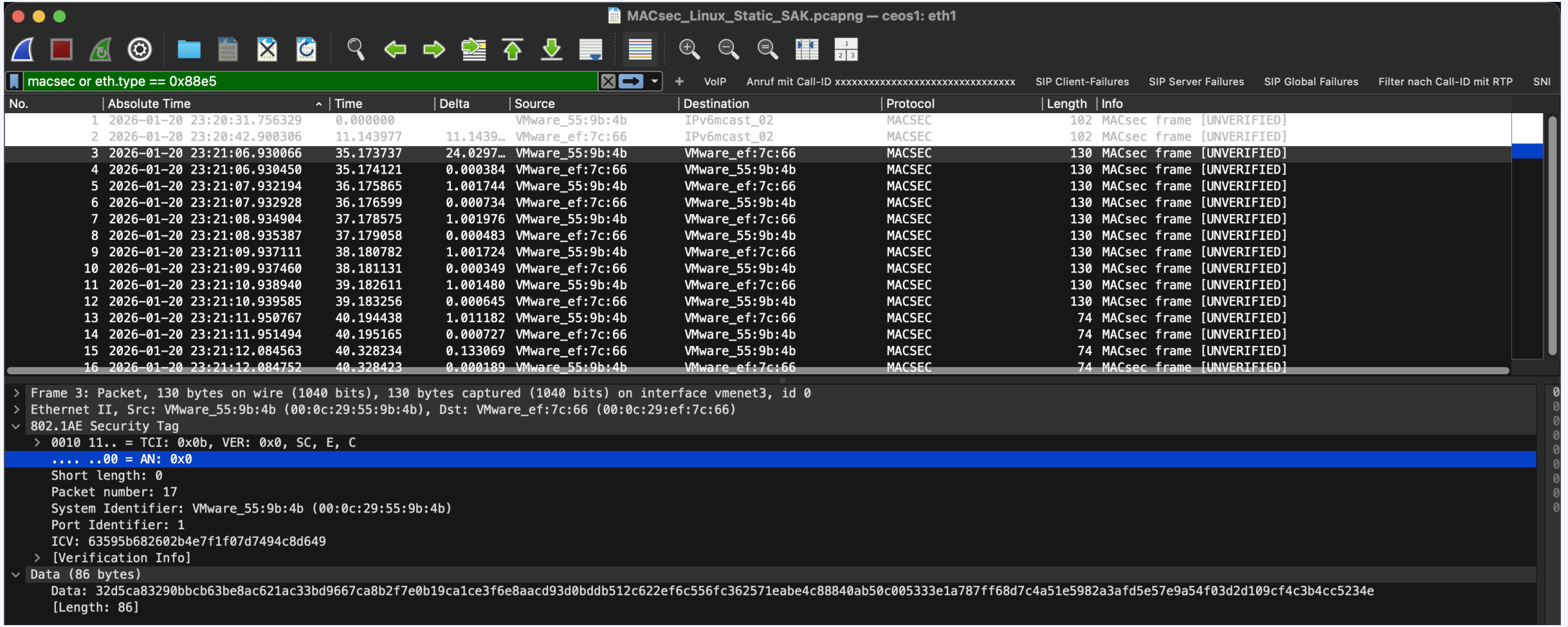
| Schlüsselaustausch | Beschreibung | Szenario |
|---|---|---|
| Statischer SAK | Manuelle Konfiguration des symmetrischen Sitzungsschlüssels | Switch-zu-Switch<br>Host-zu-Host |
| Statischer CAK | Manuelle Konfiguration des CAK und CKN und Nutzung MKA für Austausch SAK | Switch-zu-Switch |
| Dynamisch CAK MSK Verteilung via RADIUS und EAP-TLS | Nutzt dynamisches MKA und verteilt MSK im Rahmen von EAP-TLS um CAK zu ermitteln | Host-zu-Switch |

# Schlüsselverteilung

- Statisch SAK
  - Statische Hinterlegung Schlüssel-ID und Schlüssel
  - Beispiel Ubuntu mit iproute2

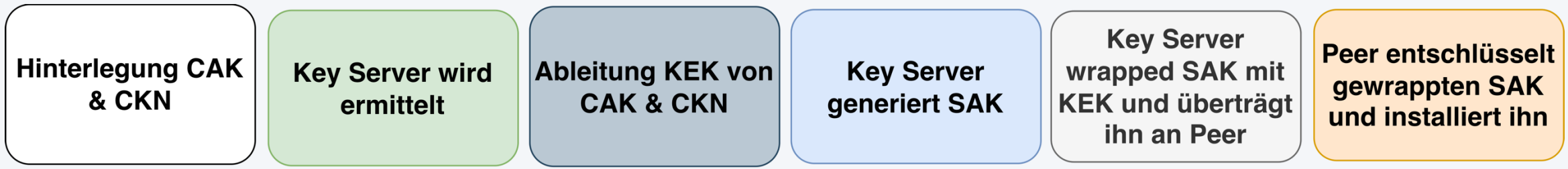
```
231  ip link set ens160 down
232  ip link add link ens160 macsec0 type macsec encrypt on
233  ip macsec add macsec0 tx sa 0 pn 1 on key AAAA 01234567012345670123456701234567
234  ip macsec add macsec0 rx address 00:0c:29:ef:7c:66 port 1
235  ip macsec add macsec0 rx address 00:0c:29:ef:7c:66 port 1 sa 0 pn 1 on key AAAA 01234567012345670123456701234567
236  ip addr add 192.168.203.2/24 dev macsec0
237  ip link set ens160 up
238  ip link set macsec0 up
```

# Static SAK


MACsec_Linux_Static_SAK.pcapng — ceos1: eth1
macsec or eth.type == 0x88e5
VoIP
Anruf mit Call-ID xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
SIP Client-Failures
SIP Server Failures
SIP Global Failures
Filter nach Call-ID mit RTP
SNI
No. | Absolute Time | Time | Delta | Source | Destination | Protocol | Length | Info
1 2026-01-20 23:20:31.756329 0.000000 VMware_55:9b:4b IPv6mcast_02 MACSEC 102 MACsec frame [UNVERIFIED]
2 2026-01-20 23:20:42.900306 11.143977 11.1439… VMware_ef:7c:66 IPv6mcast_02 MACSEC 102 MACsec frame [UNVERIFIED]
3 2026-01-20 23:21:06.930066 35.173737 24.0297… VMware_55:9b:4b VMware_ef:7c:66 MACSEC 130 MACsec frame [UNVERIFIED]
4 2026-01-20 23:21:06.930450 35.174121 0.000384 VMware_ef:7c:66 VMware_55:9b:4b MACSEC 130 MACsec frame [UNVERIFIED]
5 2026-01-20 23:21:07.932194 36.175865 1.001744 VMware_55:9b:4b VMware_ef:7c:66 MACSEC 130 MACsec frame [UNVERIFIED]
6 2026-01-20 23:21:07.932928 36.176599 0.000734 VMware_ef:7c:66 VMware_55:9b:4b MACSEC 130 MACsec frame [UNVERIFIED]
7 2026-01-20 23:21:08.934904 37.178575 1.001976 VMware_55:9b:4b VMware_ef:7c:66 MACSEC 130 MACsec frame [UNVERIFIED]
8 2026-01-20 23:21:08.935387 37.179058 0.000483 VMware_ef:7c:66 VMware_55:9b:4b MACSEC 130 MACsec frame [UNVERIFIED]
9 2026-01-20 23:21:09.937111 38.180782 1.001724 VMware_55:9b:4b VMware_ef:7c:66 MACSEC 130 MACsec frame [UNVERIFIED]
10 2026-01-20 23:21:09.937460 38.181131 0.000349 VMware_ef:7c:66 VMware_55:9b:4b MACSEC 130 MACsec frame [UNVERIFIED]
11 2026-01-20 23:21:10.938940 39.182611 1.001480 VMware_55:9b:4b VMware_ef:7c:66 MACSEC 130 MACsec frame [UNVERIFIED]
12 2026-01-20 23:21:10.939585 39.183256 0.000645 VMware_ef:7c:66 VMware_55:9b:4b MACSEC 130 MACsec frame [UNVERIFIED]
13 2026-01-20 23:21:11.950767 40.194438 1.011182 VMware_55:9b:4b VMware_ef:7c:66 MACSEC 74 MACsec frame [UNVERIFIED]
14 2026-01-20 23:21:11.951494 40.195165 0.000727 VMware_ef:7c:66 VMware_55:9b:4b MACSEC 74 MACsec frame [UNVERIFIED]
15 2026-01-20 23:21:12.084563 40.328234 0.133069 VMware_ef:7c:66 VMware_55:9b:4b MACSEC 74 MACsec frame [UNVERIFIED]
16 2026-01-20 23:21:12.084752 40.328423 0.000189 VMware_55:9b:4b VMware_ef:7c:66 MACSEC 74 MACsec frame [UNVERIFIED]
Frame 3: Packet, 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface vmenet3, id 0
Ethernet II, Src: VMware_55:9b:4b (00:0c:29:55:9b:4b), Dst: VMware_ef:7c:66 (00:0c:29:ef:7c:66)
802.1AE Security Tag
0010 11.. = TCI: 0x0b, VER: 0x0, SC, E, C
.... ..00 = AN: 0x0
Short length: 0
Packet number: 17
System Identifier: VMware_55:9b:4b (00:0c:29:55:9b:4b)
Port Identifier: 1
ICV: 63595b682602b4e7f1f07d7494c8d649
[Verification Info]
Data (86 bytes)
Data: 32d5ca83290bbcb63be8ac621ac33bd9667ca8b2f7e0b19ca1ce3f6e8aacd93d0bddb512c622ef6c556fc362571eabe4c88840ab50c005333e1a787ff68d7c4a51e5982a3afd5e57e9a54f03d2d109cf4c3b4cc5234e
[Length: 86]

# Schlüsselverteilung

## Statisch CAK



# Schlüsselverteilung



- Statisch CAK
  - Hinterlegung CKN und CAK
  - Key-Server

```
ceos1#sh run | sec mac security
mac security
   profile mka
      cipher aes256-gcm
      key 020202020202020202020202020202020202020202020202020202020202020202 7 075F731C1C594B55454259
5C567A79747A6367724157445353060B0801045C534A460B080503000506 5B0956550805544156560B59565D711E1E5B495
747405B5E
      mka key-server priority 15
      mka session rekey-period 600
      traffic unprotected drop
interface Ethernet1
   mac security profile mka
```

# Static CAK

## EAPoL MKA

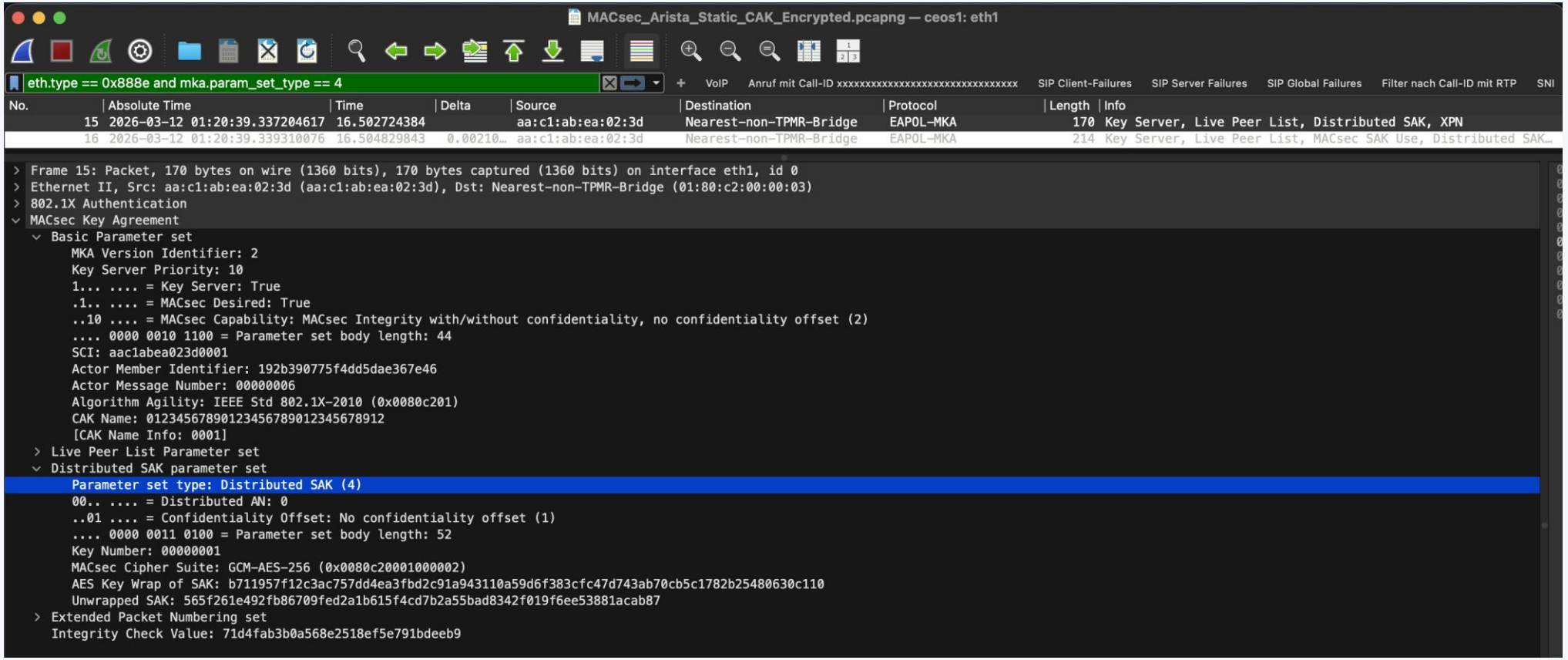
| No. | Time | Delta | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|---|
| 8 | 9.686986667s | | aa:c1:ab:ea:02:3d | Nearest-non-TPM… | EAPOL-MKA | 94 | Key Server, XPN |
| 9 | 10.501125324s | 0.… | aa:c1:ab:03:d3:81 | Nearest-non-TPM… | EAPOL-MKA | 114 | Key Server, Potential Peer List, XPN |
| 10 | 11.793064591s | 1.… | aa:c1:ab:ea:02:3d | Nearest-non-TPM… | EAPOL-MKA | 114 | Key Server, Live Peer List, XPN |
| 11 | 12.599381955s | 0.… | aa:c1:ab:03:d3:81 | Nearest-non-TPM… | EAPOL-MKA | 114 | Live Peer List, XPN |
| 15 | 16.502724384s | 3.… | aa:c1:ab:ea:02:3d | Nearest-non-TPM… | EAPOL-MKA | 170 | Key Server, Live Peer List, Distributed SAK, XPN |
| 16 | 16.504829843s | 0.… | aa:c1:ab:ea:02:3d | Nearest-non-TPM… | EAPOL-MKA | 214 | Key Server, Live Peer List, MACsec SAK Use, Distributed SAK, XPN |

Key Server Aushandlung & Peer Discovery

Aushandlung Verschlüsselungsparameter und Verteilung Session Key

# Static CAK

## EAPoL MKA

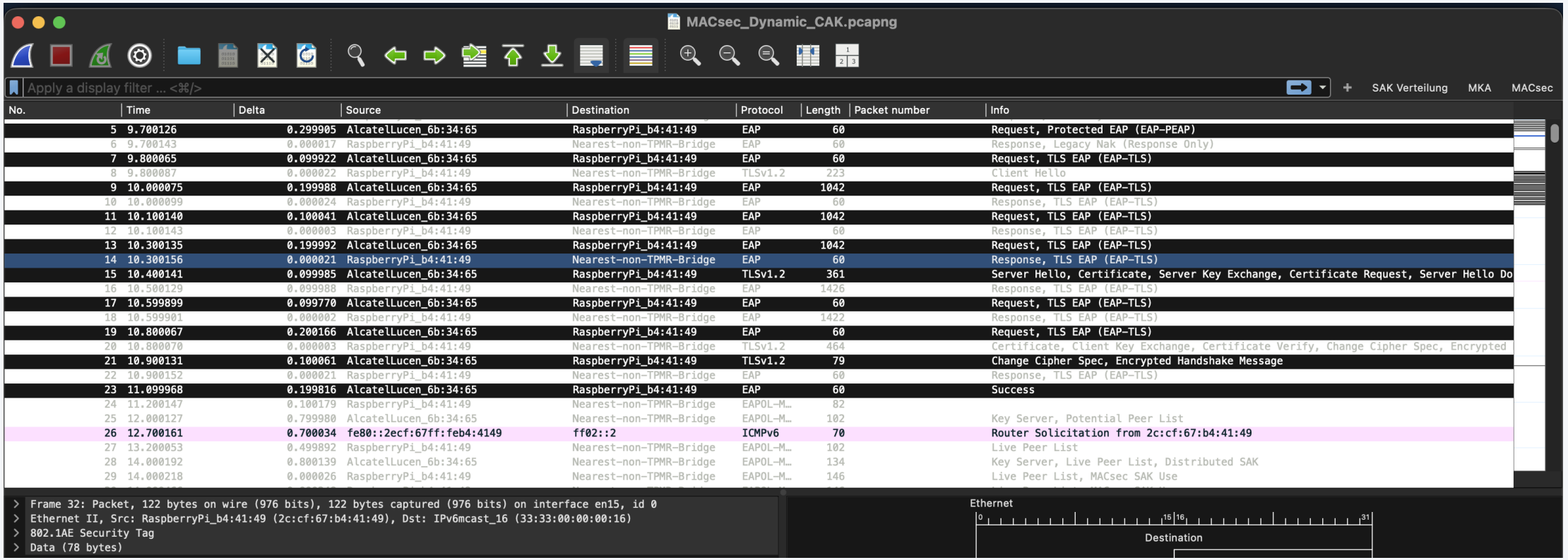


# Schlüsselverteilung

## Dynamic CAK

# Schlüsselverteilung

## Dynamic CAK



# Bildquellen



- Pexels https://www.pexels.com/de-de/
- Unsplash https://unsplash.com/de

# Vielen Dank!

WIRESHARK


## Benjamin Pfister

linkedin.com/in/benjamin-pfister-90136b298