

SharkFest'26 Europe

MACsec

An overview of MACsec and analysis using Wireshark

Benjamin Pfister

Sponsored by:
PROFITAP DEEP NETWORK OBSERVABILITY
cPacket
TCP/IP training
endace Record. Respond.

About Me

- Benjamin Pfister
- Head of Network & Telecommunication
- IT-Consultant / Trainer
- Freelance Author
- Baby Shark's dad





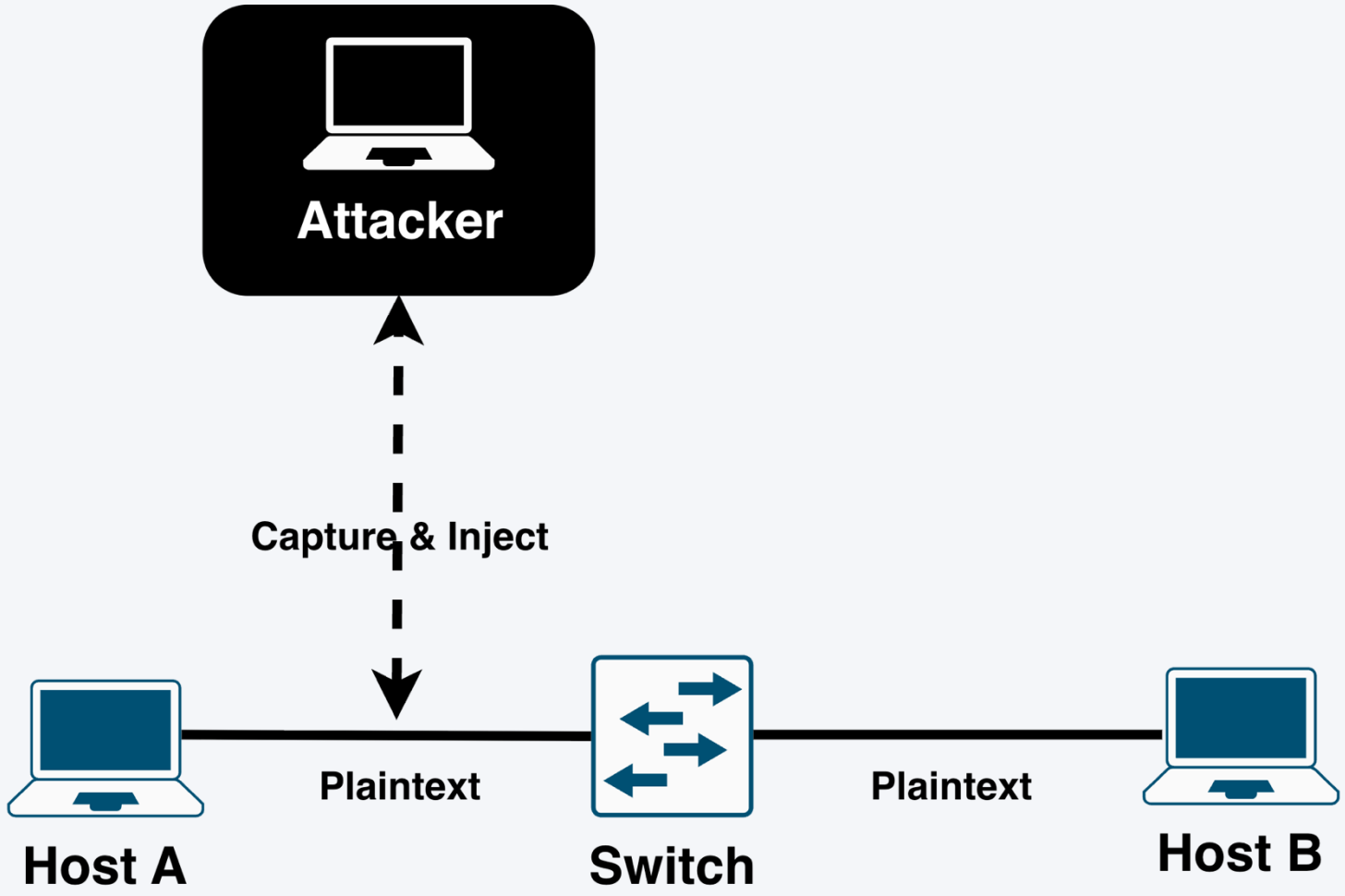
Agenda

- What is MACsec?
- Scenarios
- Frame
- Key-Distribution & Analysis

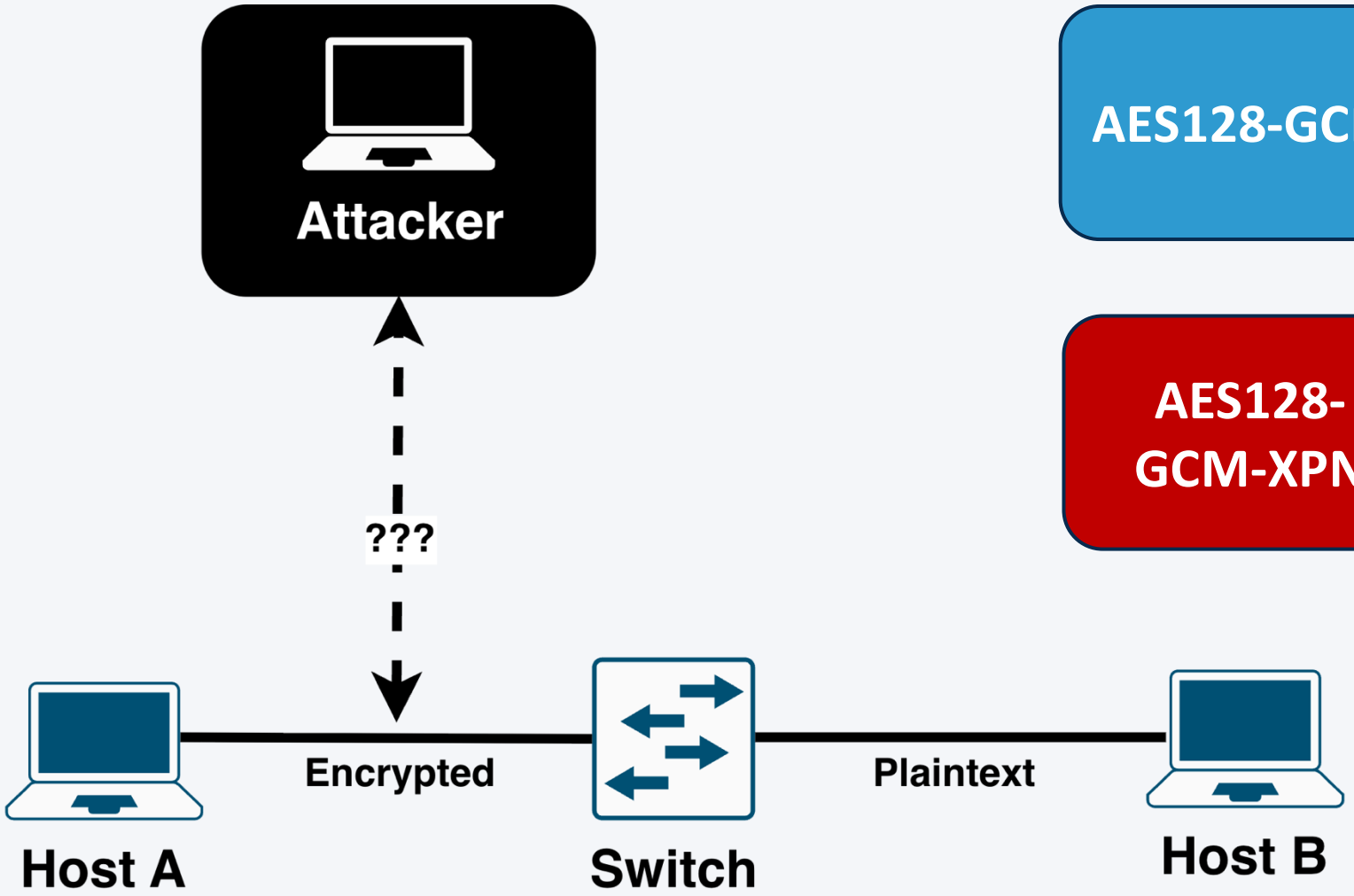
What is MACsec?

What is MACsec?

- Layer 2 Encryption
- Integrity Check
- Hop-by-Hop
- IEEE 802.1AE
- IEEE 802.1X-2010 & 2020



What is MACsec?



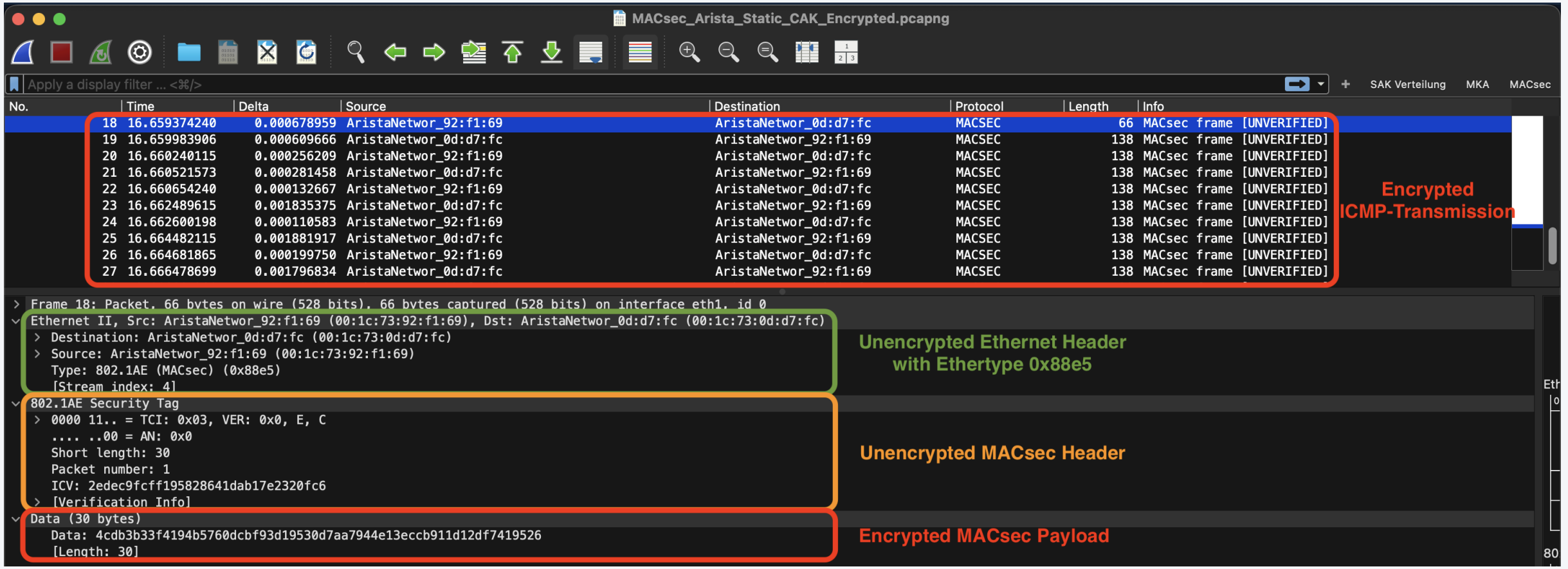
AES128-GCM

AES256-GCM

AES128-GCM-XPN

AES256-GCM-XPN

What is MACsec?

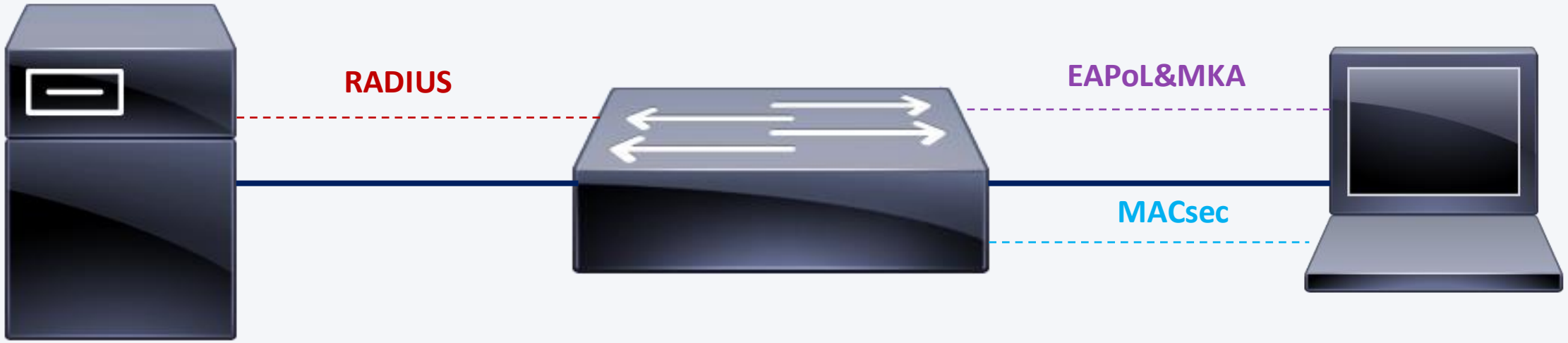


Scenarios



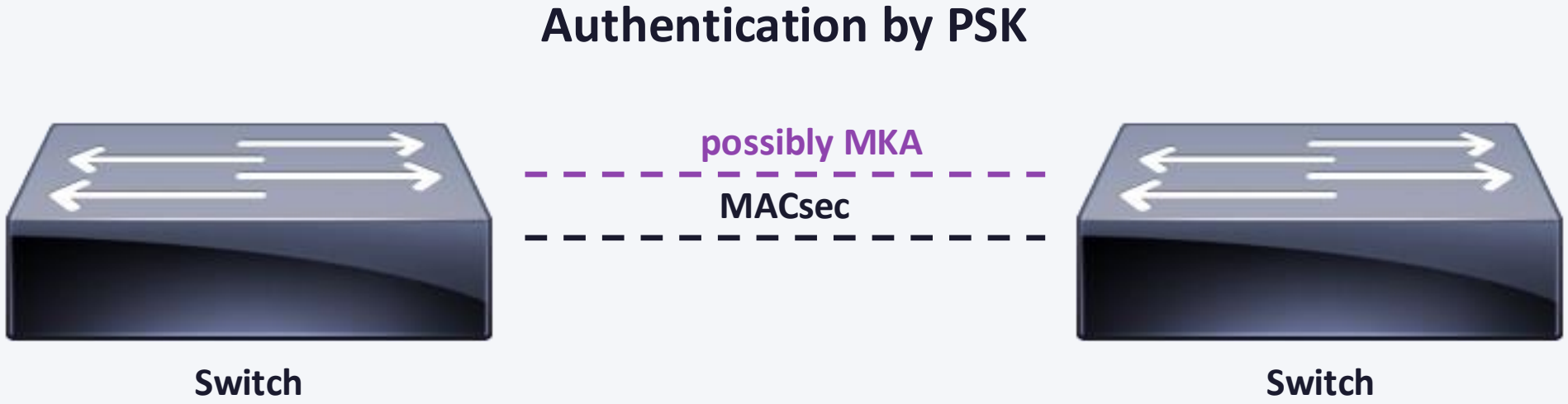
Scenarios

- Switch <-> Host



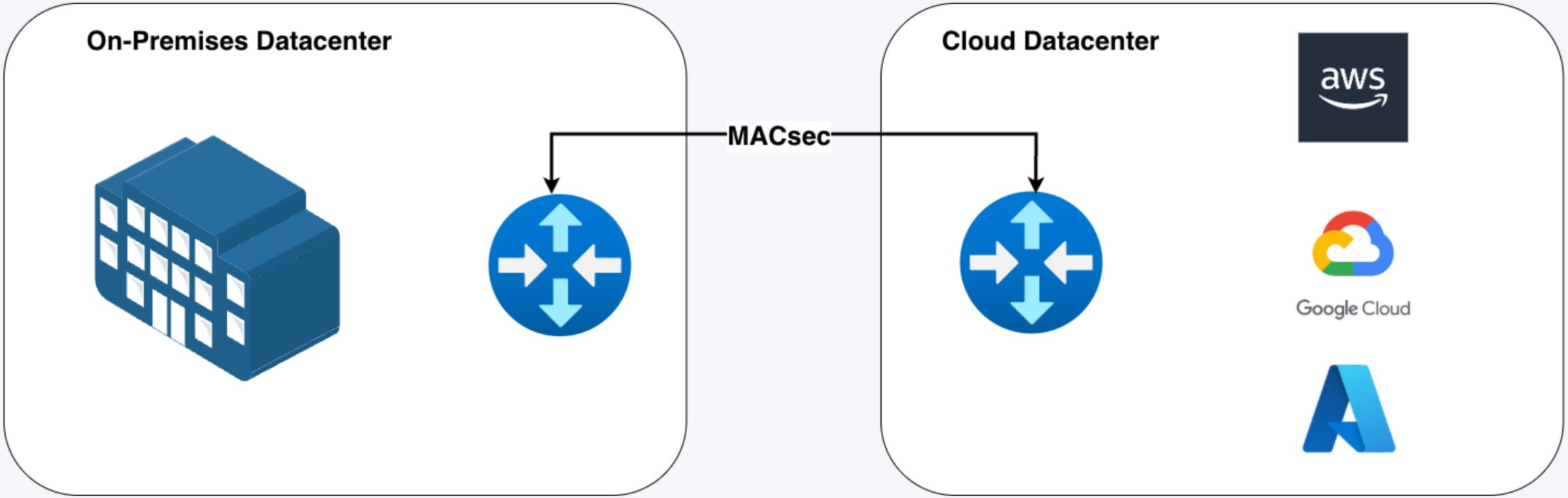
Scenarios

- Switch <-> Switch



Scenarios

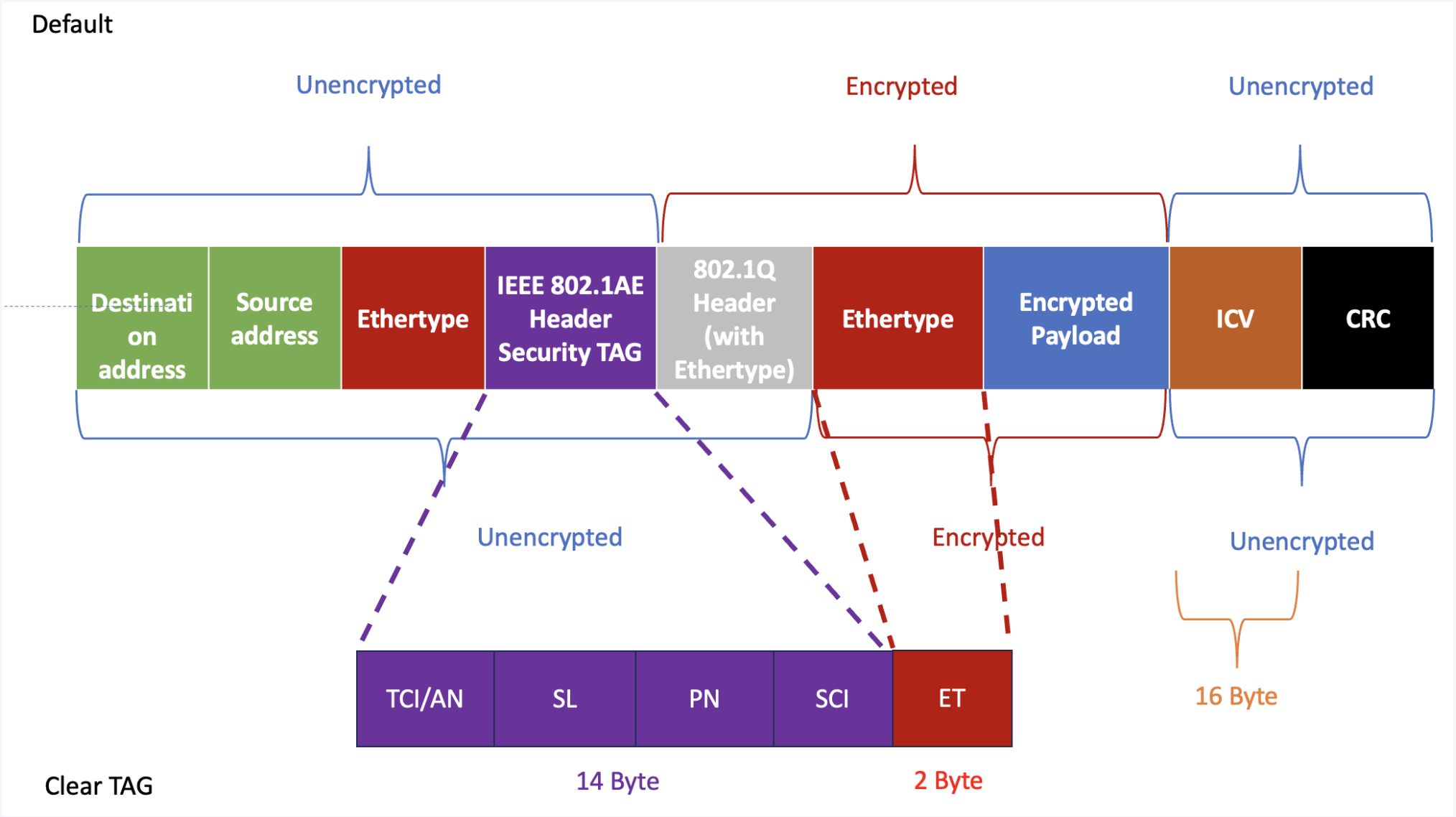
Cloud On-Ramp



Frame

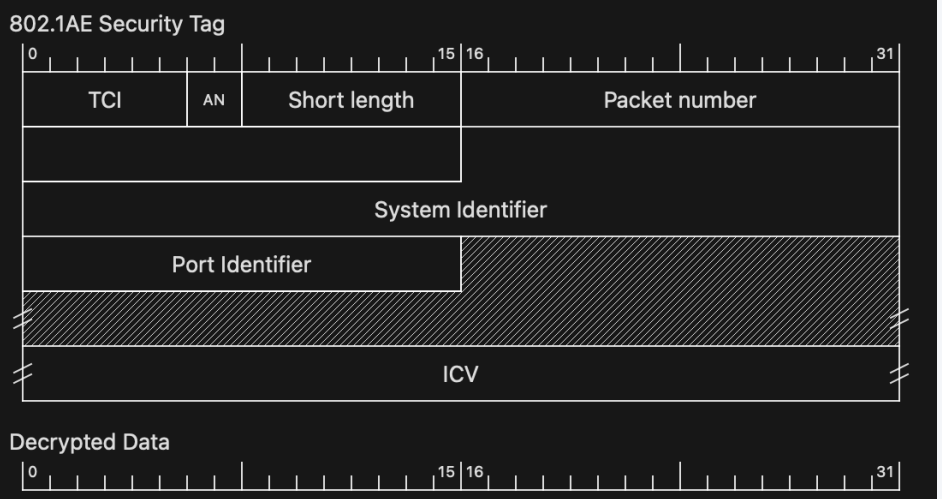


Frame


Default
Unencrypted
Encrypted
Unencrypted
Destinati on address
Source address
Ethertype
IEEE 802.1AE Header Security TAG
802.1Q Header (with Ethertype)
Ethertype
Encrypted Payload
ICV
CRC
Unencrypted
Encrypted
Unencrypted
TCI/AN
SL
PN
SCI
ET
16 Byte
Clear TAG
14 Byte
2 Byte

Frame

```
> 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
```



Key Terms

Term	Description
MKA	MACsec Key Agreement: Key agreement protocol for discovering MACsec peers, and for generating, renewing and exchanging keys.
CKN	Connectivity Association Key Name: Serves as a description for the control-plane in conjunction with the CAK. The peers transmit this amongst themselves in plain text for validation.
CAK	Connectivity Association Key: The control-plane key from which the session key is derived.
SAK	Security Association Key: A session key derived from the CAK and used for encryption between two MACsec peers.
MSK	Master Session Key: Generated during the EAP exchange. The supplicant and authenticator use MSK to generate the CAK.

Key Distribution & Analysis

Analysis with Wireshark

- What can we analyse in general?
  - Validate whether encrypted
  - Errors in the MKA
    - Errors in the transmission of EAPoL frames
    - Key server selection
    - CAK names
    - Confidentiality Offset
    - SAK distribution
  - ICV errors due to manipulation or transmission errors
  - Packet loss based on packet number
  - Latency based on packet number
  - Decrypted Payload with Static SAK and Static CAK Mode



Analysis with Wireshark

- Capture Filter
  - EAPoL/MKA
    - ether proto 0x888e
    - ether dst 01:80:c2:00:00:03
  - MACsec
    - ether proto 0x88e5
  - EAPoL/MKA or MACsec
    - ether proto 0x888e or ether proto 0x88e5

- Display Filter
  - Key server selection
    - mka.key_server == True && mka.ks_prio > 0
    - mka.key_server == True && mka.distributed_sak_set
  - CAK names
    - mka.cak_name == 01:23:45:67:89:01:23:45:67:89:01:23:45:67:89:12
  - Confidentiality Offset
    - mka.confidentiality_offset > 1
  - SAK distribution
    - mka.distributed_sak_set



Key Distribution

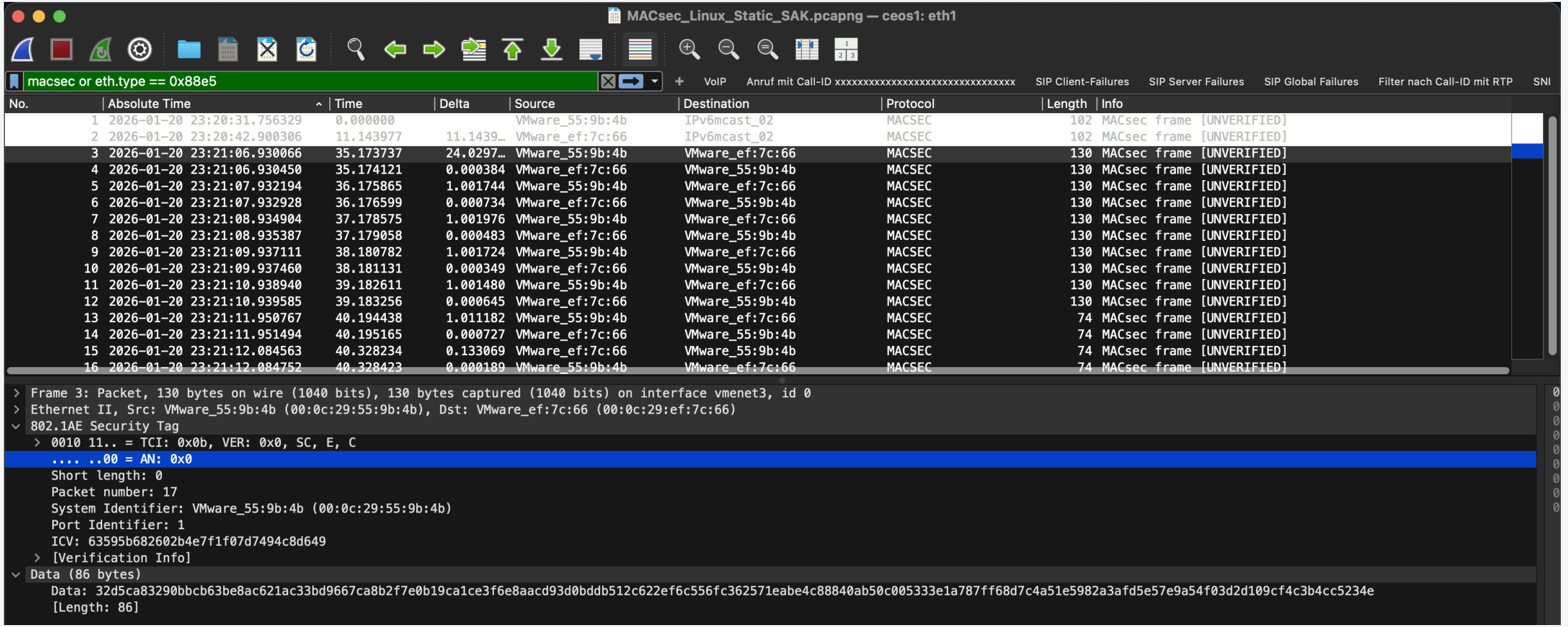
Key Distribution	Description	Scenario
Static SAK	Manual configuration of the symmetric session key	Switch-to-Switch Linux-to-Linux
Static CAK	Manual configuration of the CAK and CKN and use of MKA for SAK exchange	Switch-to-Switch
Dynamic CAK | MSK-Distribution via RADIUS and EAP-TLS	Distributes MSK as part of EAP-TLS to derive the CAK. Uses MKA afterwards.	Client-to-Switch

Key Distribution

- Static SAK
  - Static configuration of key ID and key
  - Example Ubuntu with iproute2

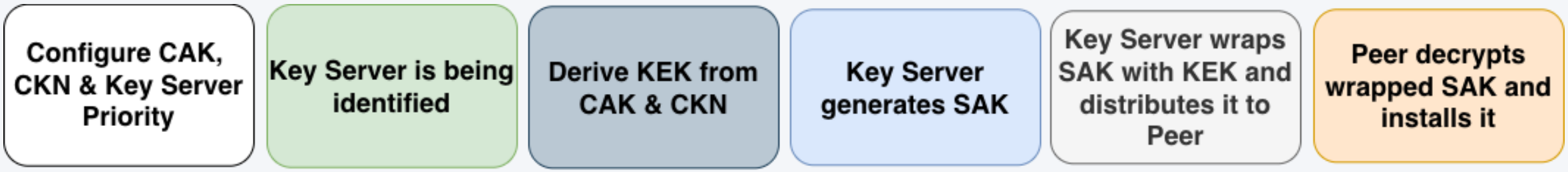
```
231  ip link set ens160 down
232  ip link add link ens160 macsec0 type macsec encrypt on
233  ip macsec add macsec0 tx sa 0 pn 1 on key AAAA 01234567012345670123456701234567
234  ip macsec add macsec0 rx address 00:0c:29:ef:7c:66 port 1
235  ip macsec add macsec0 rx address 00:0c:29:ef:7c:66 port 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]

Key Distribution

Static CAK



Key Distribution Static CAK

- Static CAK
  - Configure CKN and CAK
  - Key-Server

```
ceos1#sh run | sec mac security
mac security
   profile mka
      cipher aes256-gcm
      key 020202020202020202020202020202020202020202020202020202020202020202 7 075F731C1C594B55454259
5C567A79747A6367724157445353060B0801045C534A460B080503005065B0956550805544156560B59565D711E1E5B495
747405B5E
      mka key-server priority 15
      mka session rekey-period 600
      traffic unprotected drop
interface Ethernet1
   mac security profile mka
```

Static CAK

EAPoL MKA

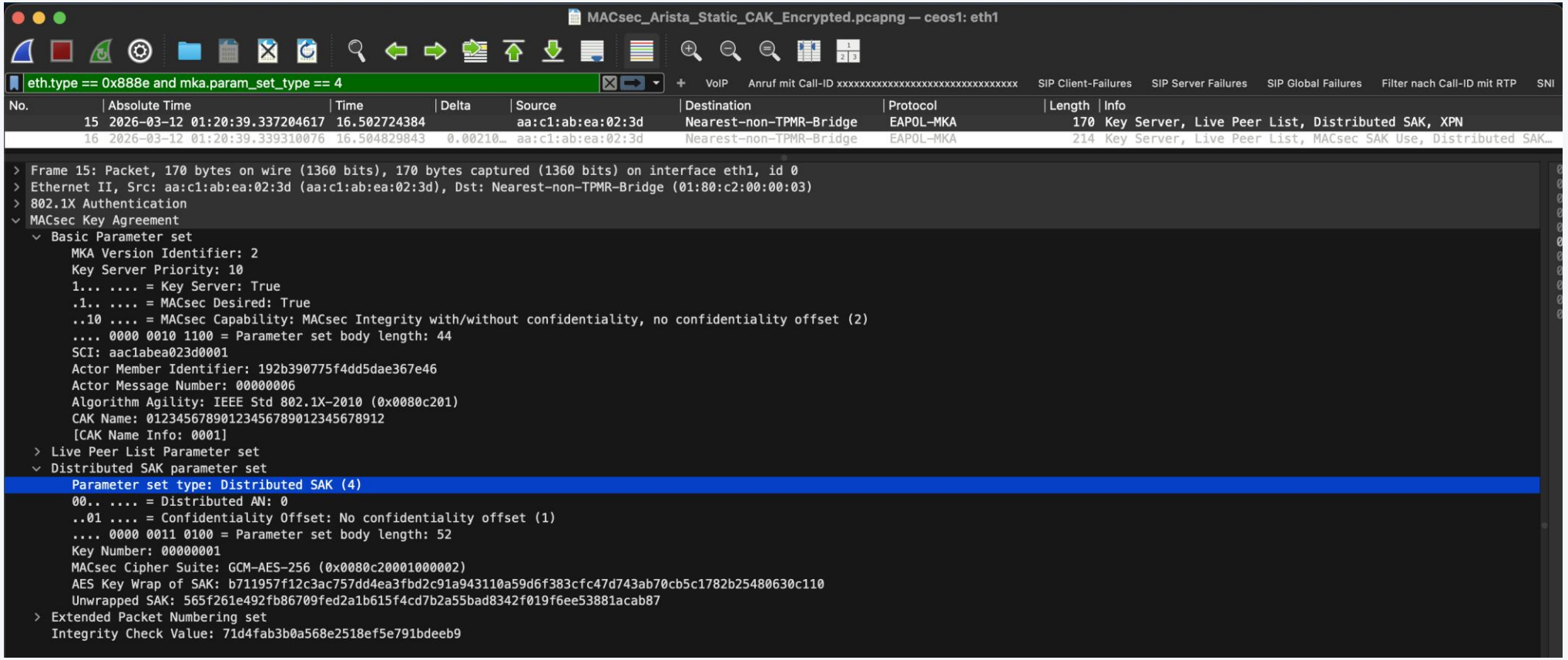
No.	Time	Delta	Source	Destination	Protocol	Length	Info
8	9.686986667		aa:c1:ab:ea:02:3d	Nearest-non-TPMR-Bridge	EAPOL-MKA	94	Key Server, XPN
9	10.501125324	0.814138657	aa:c1:ab:03:d3:81	Nearest-non-TPMR-Bridge	EAPOL-MKA	114	Key Server, Potential Peer List, XPN
10	11.793064591	1.291939267	aa:c1:ab:ea:02:3d	Nearest-non-TPMR-Bridge	EAPOL-MKA	114	Key Server, Live Peer List, XPN
11	12.599381955	0.806317364	aa:c1:ab:03:d3:81	Nearest-non-TPMR-Bridge	EAPOL-MKA	114	Live Peer List, XPN
15	16.502724384	3.903342429	aa:c1:ab:ea:02:3d	Nearest-non-TPMR-Bridge	EAPOL-MKA	170	Key Server, Live Peer List, Distributed SAK, XPN
16	16.504829843	0.002105459	aa:c1:ab:ea:02:3d	Nearest-non-TPMR-Bridge	EAPOL-MKA	214	Key Server, Live Peer List, MACsec SAK Use, Distributed SAK, XPN

Key Server Negotiation & Peer Discovery

Negotiation of encryption parameters & distribution of session key

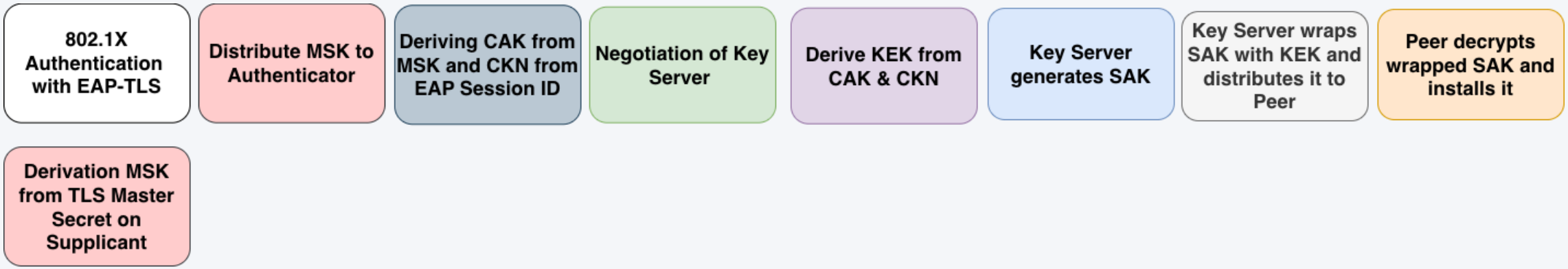
Static CAK

EAPoL MKA

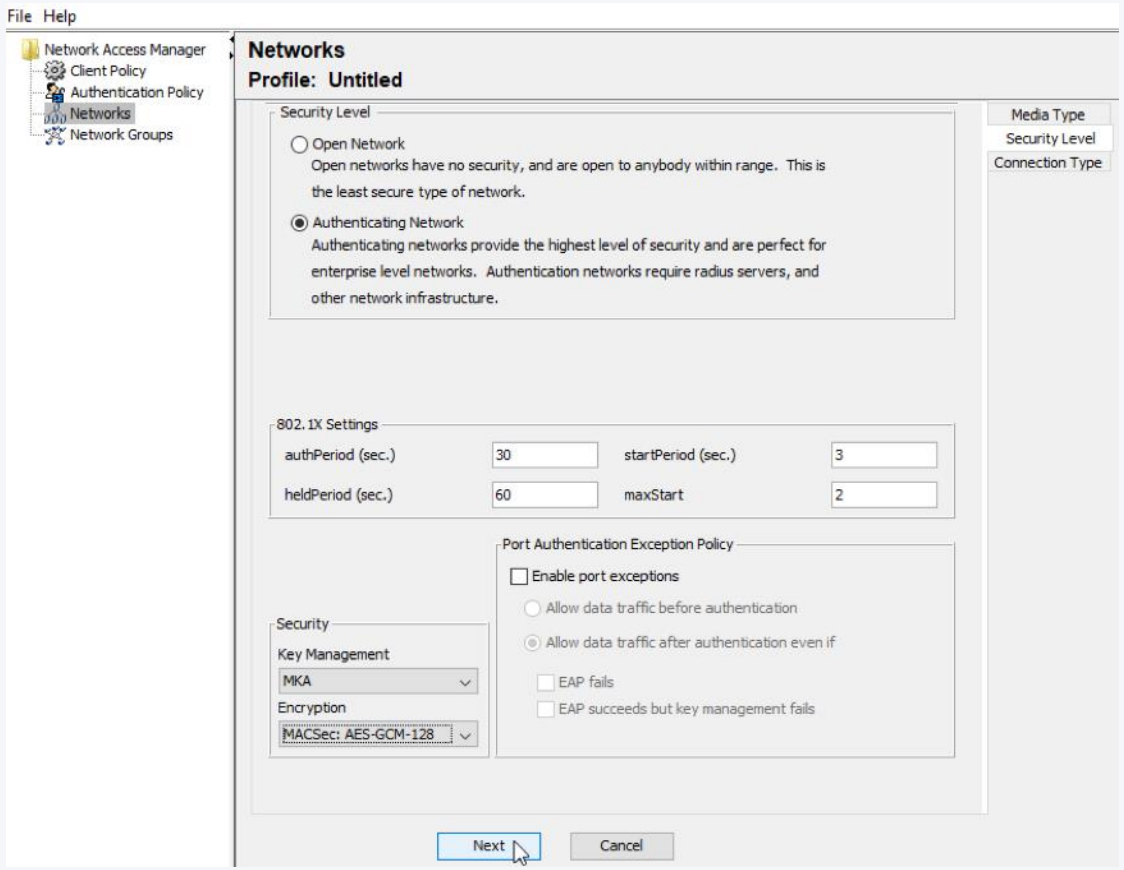


Key Distribution Dynamic CAK

Dynamic CAK



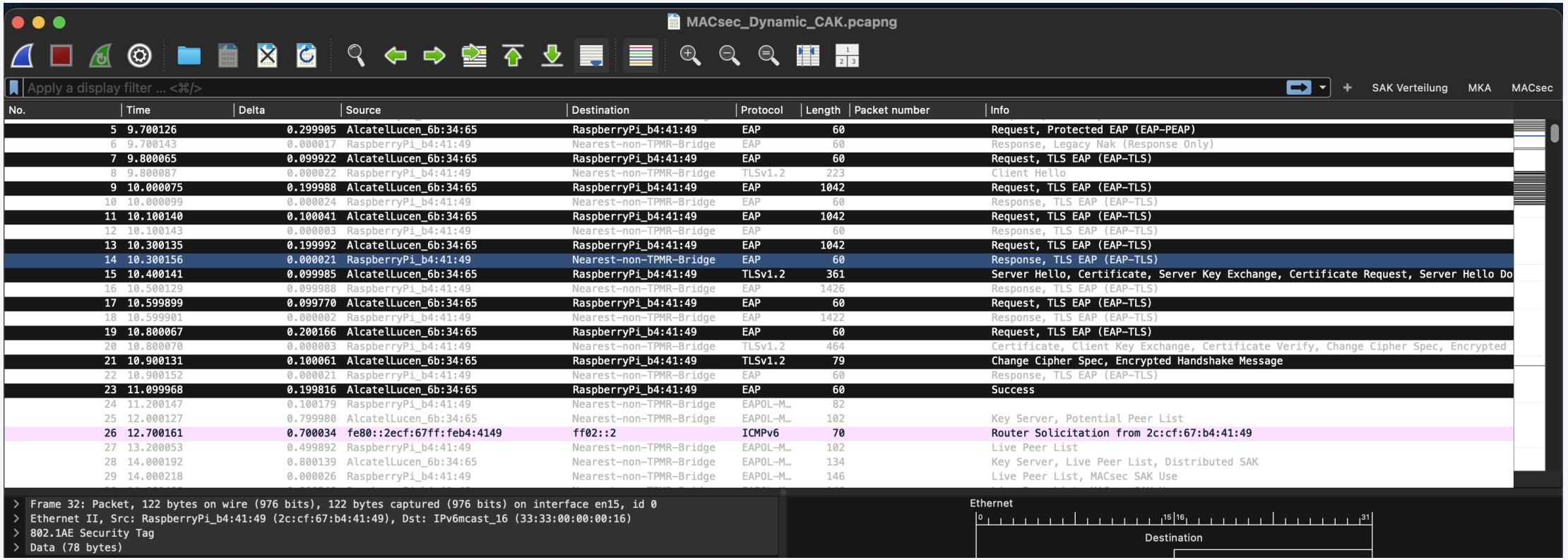
Key Distribution Dynamic CAK




```
eapol_version=3
ap_scan=0
network={
 key_mgmt=IEEE8021X
 eap=TLS
 identity="pc1234"
 ca_cert="/etc/ssl/certs/radius_ca_chain.pem"
 client_cert="/etc/ssl/client_certs/client.crt"
 private_key="/etc/ssl/client_certs/client.key"
 eapol_flags=0
 macsec_policy=1
}
```

Key Distribution

Dynamic CAK



Picture Sources

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

Thank You!

WIRESHARK

Benjamin Pfister

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