WIRESHARK EDUCATION DAY – Olten CH 2026

Wireshark Use Cases
Real World Use Cases

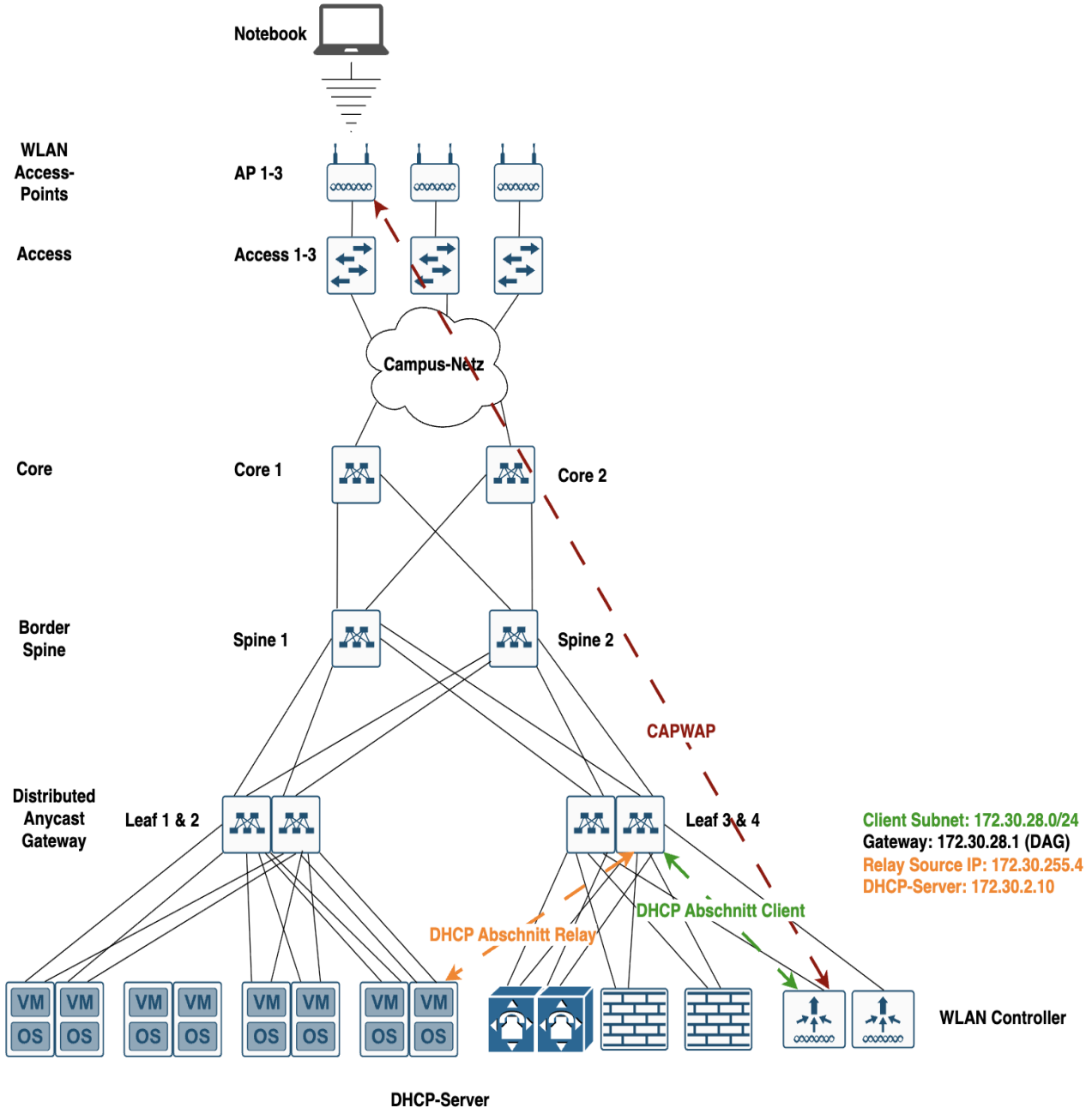
Benjamin Pfister

Inhalt

- DHCP-Fehler
- Abbrechende VoIP-Gespräche
- Verzögerter E-Mail Empfang

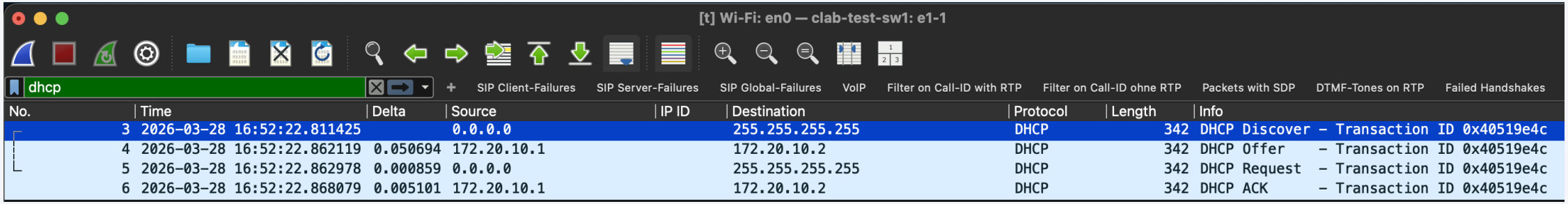
DHCP-Fehler

DHCP-Fehler

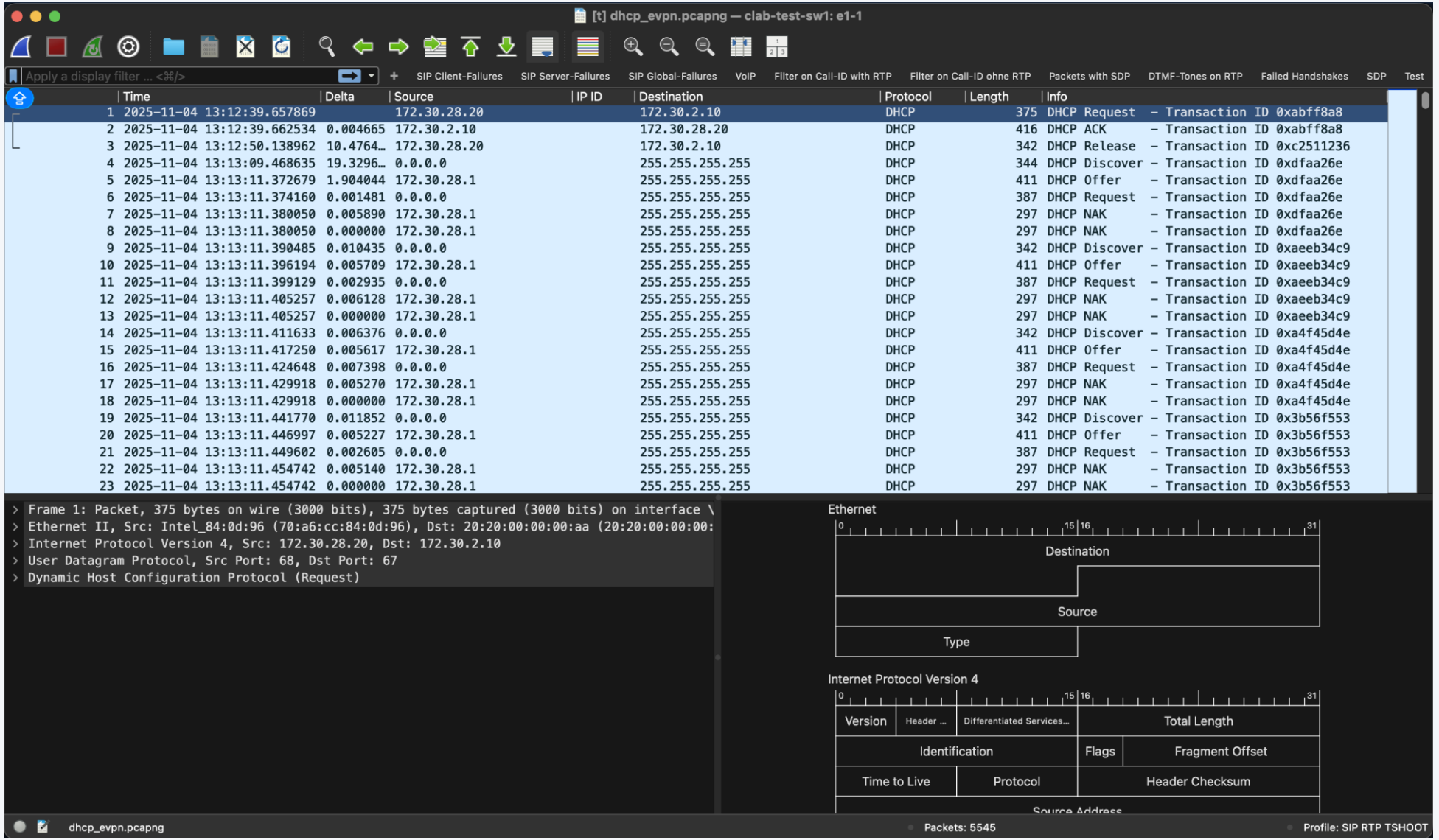

Notebook
WLAN Access-Points
AP 1-3
Access
Access 1-3
Campus-Netz
Core
Core 1
Core 2
Border Spine
Spine 1
Spine 2
CAPWAP
Distributed Anycast Gateway
Leaf 1 & 2
Leaf 3 & 4
Client Subnet: 172.30.28.0/24
Gateway: 172.30.28.1 (DAG)
Relay Source IP: 172.30.255.4
DHCP-Server: 172.30.2.10
DHCP Abschnitt Client
DHCP Abschnitt Relay
VM
OS
WLAN Controller
DHCP-Server

DHCP-Fehler

Normalablauf



DHCP-Fehler


[t] dhcp_evpn.pcapng — clab-test-sw1: e1-1
Apply a display filter ... <⌘/>
SIP Client-Failures
SIP Server-Failures
SIP Global-Failures
VoIP
Filter on Call-ID with RTP
Filter on Call-ID ohne RTP
Packets with SDP
DTMF-Tones on RTP
Failed Handshakes
SDP
Test
No. Time Delta Source IP ID Destination Protocol Length Info
1 2025-11-04 13:12:39.657869 172.30.28.20 172.30.2.10 DHCP 375 DHCP Request - Transaction ID 0xabff8a8
2 2025-11-04 13:12:39.662534 0.004665 172.30.2.10 172.30.28.20 DHCP 416 DHCP ACK - Transaction ID 0xabff8a8
3 2025-11-04 13:12:50.138962 10.4764… 172.30.28.20 172.30.2.10 DHCP 342 DHCP Release - Transaction ID 0xc2511236
4 2025-11-04 13:13:09.468635 19.3296… 0.0.0.0 255.255.255.255 DHCP 344 DHCP Discover - Transaction ID 0xdfaa26e
5 2025-11-04 13:13:11.372679 1.904044 172.30.28.1 255.255.255.255 DHCP 411 DHCP Offer - Transaction ID 0xdfaa26e
6 2025-11-04 13:13:11.374160 0.001481 0.0.0.0 255.255.255.255 DHCP 387 DHCP Request - Transaction ID 0xdfaa26e
7 2025-11-04 13:13:11.380050 0.005890 172.30.28.1 255.255.255.255 DHCP 297 DHCP NAK - Transaction ID 0xdfaa26e
8 2025-11-04 13:13:11.380050 0.000000 172.30.28.1 255.255.255.255 DHCP 297 DHCP NAK - Transaction ID 0xdfaa26e
9 2025-11-04 13:13:11.390485 0.010435 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0xaeeb34c9
10 2025-11-04 13:13:11.396194 0.005709 172.30.28.1 255.255.255.255 DHCP 411 DHCP Offer - Transaction ID 0xaeeb34c9
11 2025-11-04 13:13:11.399129 0.002935 0.0.0.0 255.255.255.255 DHCP 387 DHCP Request - Transaction ID 0xaeeb34c9
12 2025-11-04 13:13:11.405257 0.006128 172.30.28.1 255.255.255.255 DHCP 297 DHCP NAK - Transaction ID 0xaeeb34c9
13 2025-11-04 13:13:11.405257 0.000000 172.30.28.1 255.255.255.255 DHCP 297 DHCP NAK - Transaction ID 0xaeeb34c9
14 2025-11-04 13:13:11.411633 0.006376 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0xa4f45d4e
15 2025-11-04 13:13:11.417250 0.005617 172.30.28.1 255.255.255.255 DHCP 411 DHCP Offer - Transaction ID 0xa4f45d4e
16 2025-11-04 13:13:11.424648 0.007398 0.0.0.0 255.255.255.255 DHCP 387 DHCP Request - Transaction ID 0xa4f45d4e
17 2025-11-04 13:13:11.429918 0.005270 172.30.28.1 255.255.255.255 DHCP 297 DHCP NAK - Transaction ID 0xa4f45d4e
18 2025-11-04 13:13:11.429918 0.000000 172.30.28.1 255.255.255.255 DHCP 297 DHCP NAK - Transaction ID 0xa4f45d4e
19 2025-11-04 13:13:11.441770 0.011852 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x3b56f553
20 2025-11-04 13:13:11.446997 0.005227 172.30.28.1 255.255.255.255 DHCP 411 DHCP Offer - Transaction ID 0x3b56f553
21 2025-11-04 13:13:11.449602 0.002605 0.0.0.0 255.255.255.255 DHCP 387 DHCP Request - Transaction ID 0x3b56f553
22 2025-11-04 13:13:11.454742 0.005140 172.30.28.1 255.255.255.255 DHCP 297 DHCP NAK - Transaction ID 0x3b56f553
23 2025-11-04 13:13:11.454742 0.000000 172.30.28.1 255.255.255.255 DHCP 297 DHCP NAK - Transaction ID 0x3b56f553
Frame 1: Packet, 375 bytes on wire (3000 bits), 375 bytes captured (3000 bits) on interface \
Ethernet II, Src: Intel_84:0d:96 (70:a6:cc:84:0d:96), Dst: 20:20:00:00:00:aa (20:20:00:00:00:
Internet Protocol Version 4, Src: 172.30.28.20, Dst: 172.30.2.10
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)
Ethernet
Destination
Source
Type
Internet Protocol Version 4
Version
Header ...
Differentiated Services...
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
dhcp_evpn.pcapng
Packets: 5545
Profile: SIP RTP TSHOOT

DHCP-Fehler

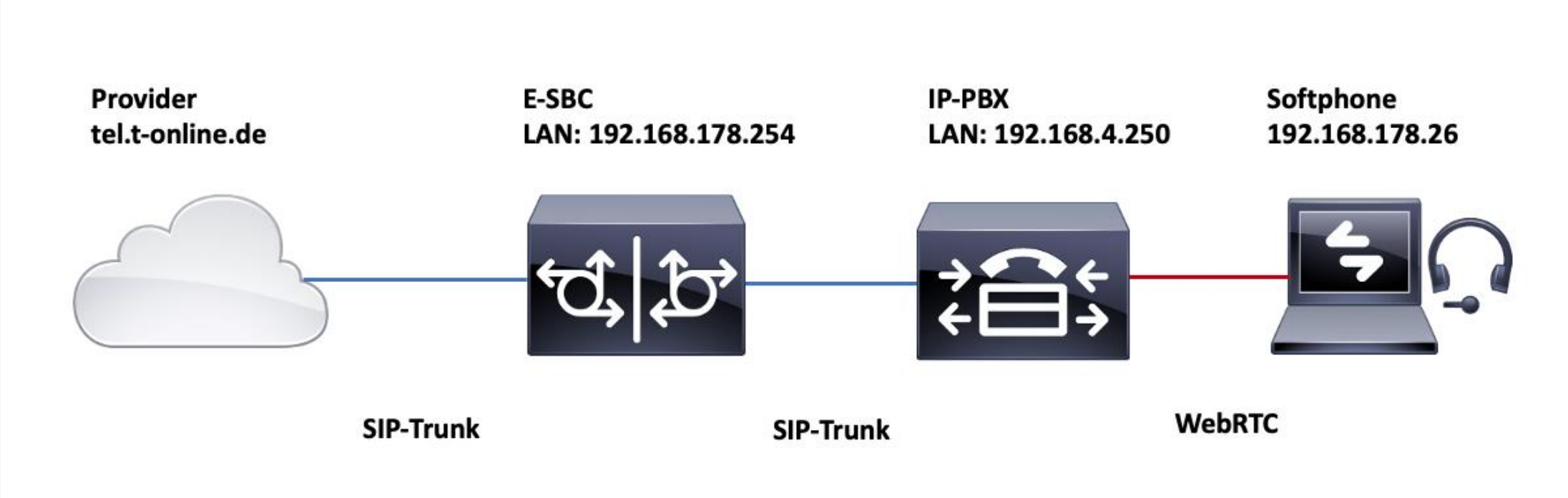
```
Bootstrap Protocol
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 1
  Transaction ID: 0x0860cd13
  Seconds elapsed: 0
  Bootp flags: 0x0000 (unicast)
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 0.0.0.0 (0.0.0.0)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 172.30.255.4 (172.30.255.4)
  Client MAC address: 70:a6:cc:84:0d:96 (70:a6:cc:84:0d:96)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (53) DHCP Message Type
    Length: 1
    DHCP: Discover (1)
  Option: (55) Parameter Request List
  Option: (61) Client Identifier
  Option: (82) Agent Information Option
    Length: 47
  Option 82 suboption: (1) Agent Circuit ID
  Option 82 suboption: (151) Agent Remote ID
  Option 82 suboption: (11) Server ID Override
    Length: 4
    Server ID override: 172.30.28.1 (172.30.28.1)
  Option 82 suboption: (5) Link selection
    Length: 4
    Link selection: 172.30.28.0 (172.30.28.0)
```

> **Note**
>
> All relay agent IP addresses (GIADDR) must be part of an active DHCP scope IP address range. Any GIADDR outside of the DHCP scope IP address ranges is considered a rogue relay and Windows DHCP Server will not acknowledge DHCP client requests from those relay agents.
>
> A special scope can be created to "authorize" relay agents. Create a scope with the GIADDR (or multiple if the GIADDR's are sequential IP addresses), exclude the GIADDR address(es) from distribution, and then activate the scope. This will authorize the relay agents while preventing the GIADDR addresses from being assigned.

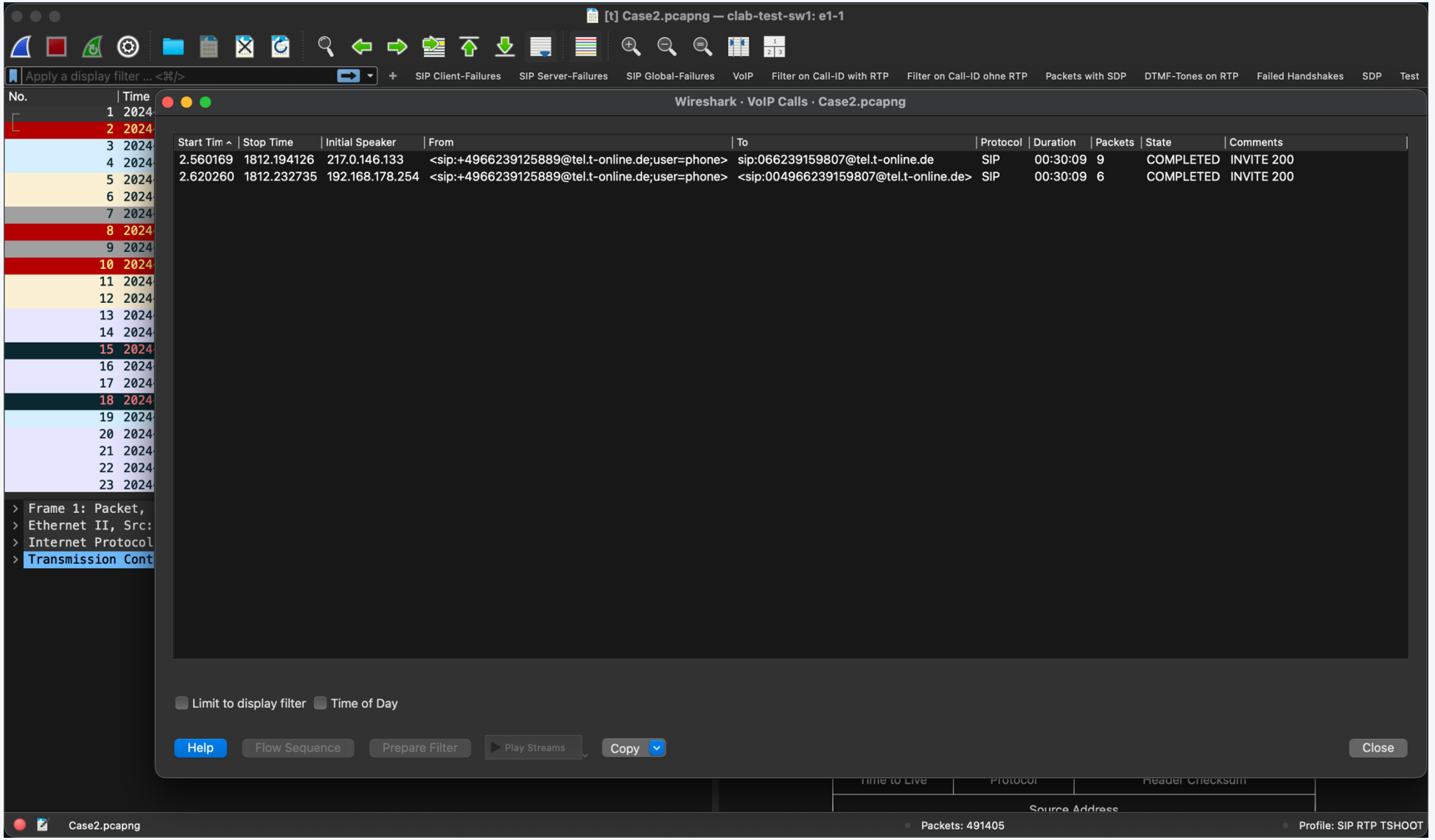
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DhcpServer\Parameters
DhcpFlagSubnetChangeDHCPRequest = 1

Abbrechende VoIP-Gespräche

Abbrechende VoIP-Gespräche

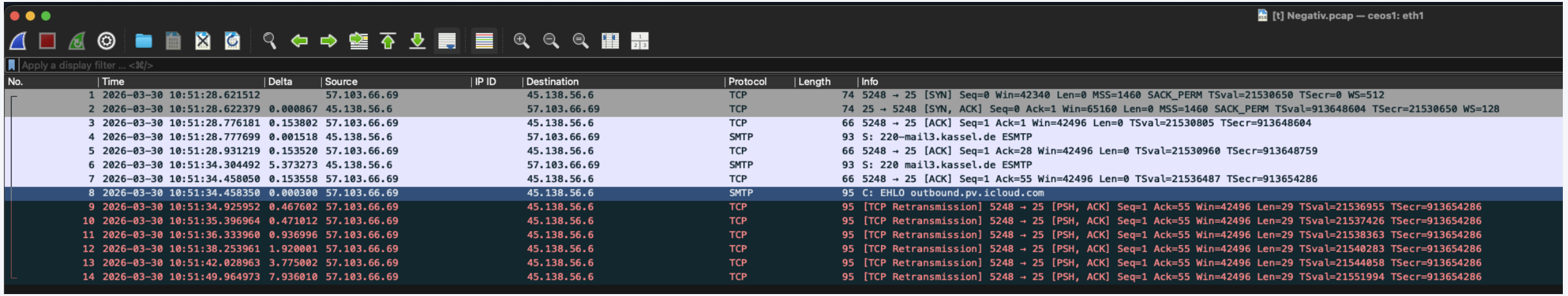


Abbrechende VoIP-Gespräche



Verzögerter E-Mail Empfang

Verzögerter E-Mail Empfang



No.	Time	Delta	Source	IP ID	Destination	Protocol	Length	Info
1	2026-03-30 10:51:28.621512		57.103.66.69		45.138.56.6	TCP	74	5248 → 25 [SYN] Seq=0 Win=42340 Len=0 MSS=1460 SACK_PERM TSval=21530650 TSecr=0 WS=512
2	2026-03-30 10:51:28.622379	0.000867	45.138.56.6		57.103.66.69	TCP	74	25 → 5248 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=913648604 TSecr=21530650 WS=128
3	2026-03-30 10:51:28.776181	0.153802	57.103.66.69		45.138.56.6	TCP	66	5248 → 25 [ACK] Seq=1 Ack=1 Win=42496 Len=0 TSval=21530805 TSecr=913648604
4	2026-03-30 10:51:28.777699	0.001518	45.138.56.6		57.103.66.69	SMTP	93	S: 220-mail3.kassel.de ESMTP
5	2026-03-30 10:51:28.931219	0.153520	57.103.66.69		45.138.56.6	TCP	66	5248 → 25 [ACK] Seq=1 Ack=28 Win=42496 Len=0 TSval=21530960 TSecr=913648759
6	2026-03-30 10:51:34.304492	5.373273	45.138.56.6		57.103.66.69	SMTP	93	S: 220 mail3.kassel.de ESMTP
7	2026-03-30 10:51:34.458050	0.153558	57.103.66.69		45.138.56.6	TCP	66	5248 → 25 [ACK] Seq=1 Ack=55 Win=42496 Len=0 TSval=21536487 TSecr=913654286
8	2026-03-30 10:51:34.458350	0.000300	57.103.66.69		45.138.56.6	SMTP	95	C: EHLO outbound.pv.icloud.com
9	2026-03-30 10:51:34.925952	0.467602	57.103.66.69		45.138.56.6	TCP	95	[TCP Retransmission] 5248 → 25 [PSH, ACK] Seq=1 Ack=55 Win=42496 Len=29 TSval=21536955 TSecr=913654286
10	2026-03-30 10:51:35.396964	0.471012	57.103.66.69		45.138.56.6	TCP	95	[TCP Retransmission] 5248 → 25 [PSH, ACK] Seq=1 Ack=55 Win=42496 Len=29 TSval=21537426 TSecr=913654286
11	2026-03-30 10:51:36.333960	0.936996	57.103.66.69		45.138.56.6	TCP	95	[TCP Retransmission] 5248 → 25 [PSH, ACK] Seq=1 Ack=55 Win=42496 Len=29 TSval=21538363 TSecr=913654286
12	2026-03-30 10:51:38.253961	1.920001	57.103.66.69		45.138.56.6	TCP	95	[TCP Retransmission] 5248 → 25 [PSH, ACK] Seq=1 Ack=55 Win=42496 Len=29 TSval=21540283 TSecr=913654286
13	2026-03-30 10:51:42.028963	3.775002	57.103.66.69		45.138.56.6	TCP	95	[TCP Retransmission] 5248 → 25 [PSH, ACK] Seq=1 Ack=55 Win=42496 Len=29 TSval=21544058 TSecr=913654286
14	2026-03-30 10:51:49.964973	7.936010	57.103.66.69		45.138.56.6	TCP	95	[TCP Retransmission] 5248 → 25 [PSH, ACK] Seq=1 Ack=55 Win=42496 Len=29 TSval=21551994 TSecr=913654286

Verzögerter E-Mail Empfang


```
The format for multiline replies requires that every line, except the
last, begin with the reply code, followed immediately by a hyphen,
"-" (also known as minus), followed by text.  The last line will
begin with the reply code, followed immediately by <SP>, optionally
some text, and <CRLF>.  As noted above, servers SHOULD send the <SP>
if subsequent text is not sent, but clients MUST be prepared for it
to be omitted.

For example:

   250-First line
   250-Second line
   250-234 Text beginning with numbers
   250 The last line
```

Bildquellen

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

Vielen Dank!

WIRESHARK

Benjamin Pfister

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