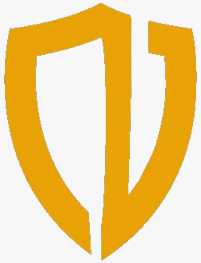
Fun & Pitfalls in VDSL



Troopers 2019
Brian Butterly

brian@security-bits.de ~~ www.security-bits.de ~~ @BadgeWizard

About Me

- Security Researcher / Hacker
  - Officially: Incident Response
- Hardware-, Embedded-, a bit of Telko-Security

- (Finally) Back in Heidelberg

Why DSL?

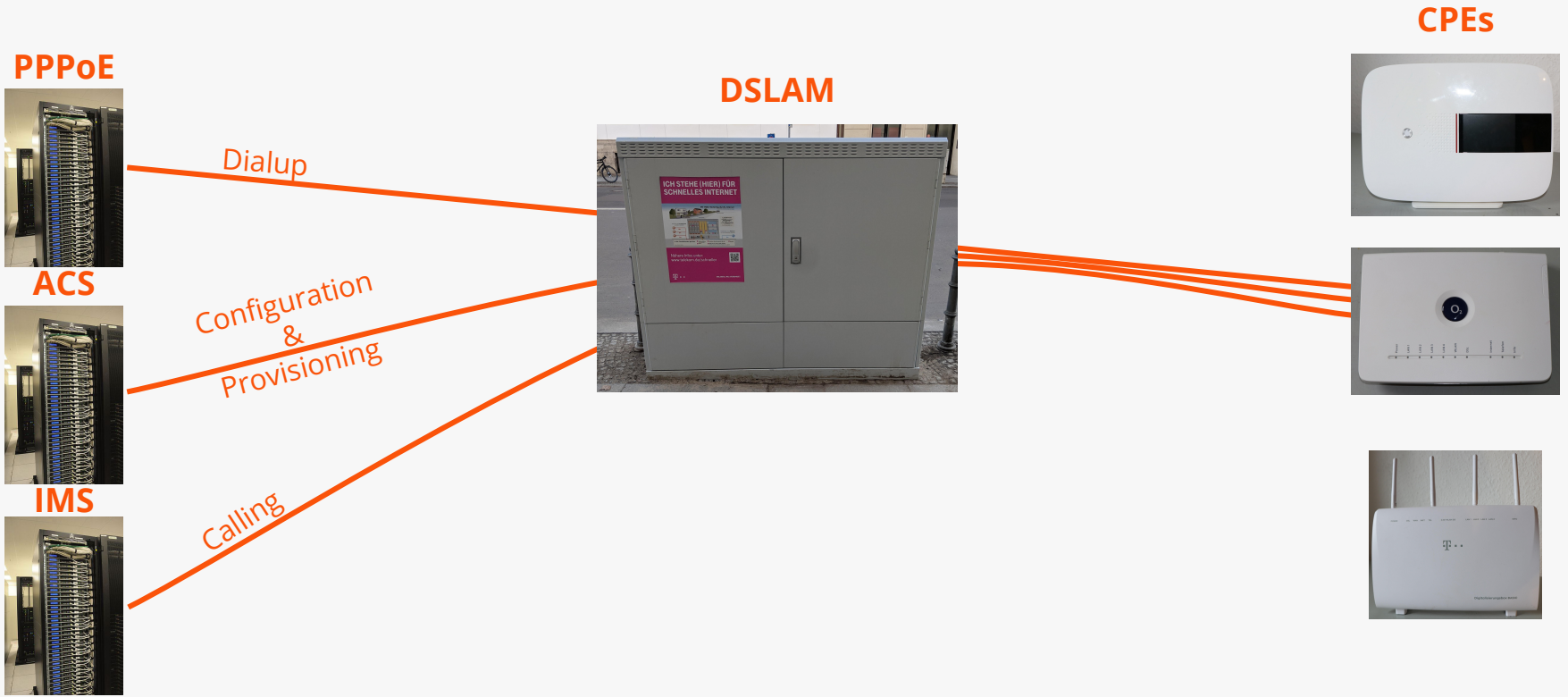
- Because it’s more critical than many realize
  - There still are people (parents, grandparents) who rely on landlines!
- Phones used to just work
  - Didn’t even need a power supply
- Nowadays many have to rely on both the access network and the operator’s router
  - Which both are a black box
- (...it was on my list...)

(Danke Anke & Chris!)

Who here knows ...

- ...how your home router authenticates to the provider's network?
- ...what the communication between your router and ISP looks like?
- ...how their calls via VoIP are protected?

Agenda I


PPPoE
ACS
IMS
Dialup
Configuration
&
Provisioning
Calling
DSLAM
ICH STEHE (HIER) FÜR
SCHNELLES INTERNET
CPEs

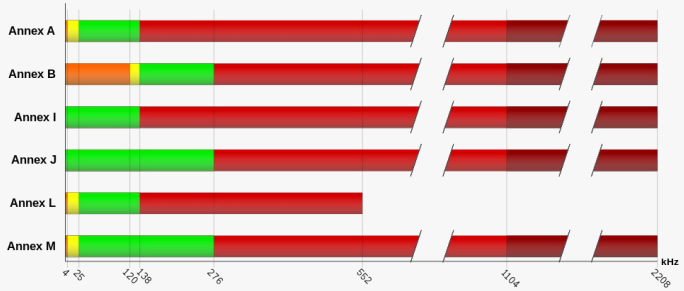
About VDSL

- Very-high-bit-rate Digital Subscriber Line
- Uses Quadrature Amplitude Modulation or Discrete Multi-Tone Modulation
- Initially as ITU G.993.1
  - With 55Mbit/s down and 3 Mbit/s up
- Since 2015 as VDSL2-Vplus / ITU G.993.2 Amendment 1 (11/15)
  - With 300Mbit/s down and 100Mbit/s up

		Empfangsrichtung	Senderichtung
DSLAM-Datenrate Max.	kbit/s	102400	102400
DSLAM-Datenrate Min.	kbit/s	64	64
Leitungskapazität	kbit/s	201465	95593
Aktuelle Datenrate	kbit/s	102399	95512
Nahtlose Ratenadaption		aus	aus
Latenz		fast	fast
Impulsstörungsschutz (INP)		0	0
G.INP		aus	aus
Störabstandsmarge	dB	20	5
Trägertausch (Bitswap)		an	aus
Leitungsdämpfung	dB	1	0
Profil	30a		
G.Vector		aus	aus
Trägersatz		B43	B43

Where did my Splitter go?

- With VDSL the analog usage of the lines was completely dropped
  - Thus no analog calling / ISDN only VoIP
- The splitter was a diplexer
  - The orange frequency range is wired to the TAE or ISDN socket
  - The green & red to the DSL Modem
- With Annex J the complete frequency range is used for DSL



DSLAM

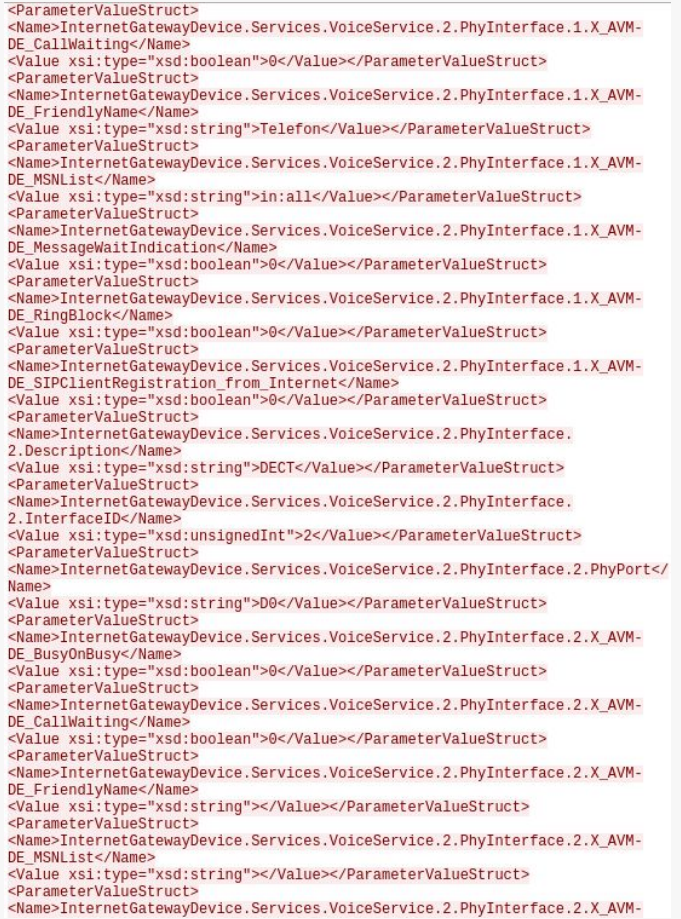
- Digital Subscriber Line/Loop Access Multiplexer
- Terminates the twisted pair copper line from the customer
- Forwards traffic to a transport network
  - Nowadays mostly fibre
- Has a separate line card for each customer
- Basically just converts the DSL signal to the protocol on the transport network
  - I.e Ethernet

VoIP

- With dropping analog calling VoIP has taken over
  - And is fusing together with LTE's IMS
- Using the VoIP client / forwarder in Home Routers, one relies on the internal settings
- Authentication streams, encryption etc. usually can't be set by hand

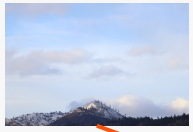
Configuration & Provisioning

- Operators “regularly” push updates
  - Both firmware and configuration
- Process to do so is automated
  - Often using TR-069
- Some routers / networks also support auto-configuration
  - Where credentials and configuration are pushed to a router

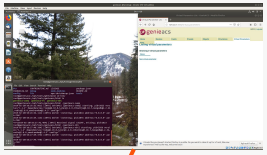


```
<ParameterValueStruct>
<Name>InternetGatewayDevice.Services.VoiceService.2.PhyInterface.1.X_AVM-
DE_CallWaiting</Name>
<Value xsi:type="xsd:boolean">0</Value></ParameterValueStruct>
<ParameterValueStruct>
<Name>InternetGatewayDevice.Services.VoiceService.2.PhyInterface.1.X_AVM-
DE_FriendlyName</Name>
<Value xsi:type="xsd:string">Telefon</Value></ParameterValueStruct>
<ParameterValueStruct>
<Name>InternetGatewayDevice.Services.VoiceService.2.PhyInterface.1.X_AVM-
DE_MSNList</Name>
<Value xsi:type="xsd:string">in:all</Value></ParameterValueStruct>
<ParameterValueStruct>
<Name>InternetGatewayDevice.Services.VoiceService.2.PhyInterface.1.X_AVM-
DE_MessageWaitIndication</Name>
<Value xsi:type="xsd:boolean">0</Value></ParameterValueStruct>
<ParameterValueStruct>
<Name>InternetGatewayDevice.Services.VoiceService.2.PhyInterface.1.X_AVM-
DE_RingBlock</Name>
<Value xsi:type="xsd:boolean">0</Value></ParameterValueStruct>
<ParameterValueStruct>
<Name>InternetGatewayDevice.Services.VoiceService.2.PhyInterface.1.X_AVM-
DE_SIPClientRegistration_from_Internet</Name>
<Value xsi:type="xsd:boolean">0</Value></ParameterValueStruct>
<ParameterValueStruct>
<Name>InternetGatewayDevice.Services.VoiceService.2.PhyInterface.
2.Description</Name>
<Value xsi:type="xsd:string">DECT</Value></ParameterValueStruct>
<ParameterValueStruct>
<Name>InternetGatewayDevice.Services.VoiceService.2.PhyInterface.
2.InterfaceID</Name>
<Value xsi:type="xsd:unsignedInt">2</Value></ParameterValueStruct>
<ParameterValueStruct>
<Name>InternetGatewayDevice.Services.VoiceService.2.PhyInterface.2.PhyPort</
Name>
<Value xsi:type="xsd:string">D0</Value></ParameterValueStruct>
<ParameterValueStruct>
<Name>InternetGatewayDevice.Services.VoiceService.2.PhyInterface.2.X_AVM-
DE_BusyOnBusy</Name>
<Value xsi:type="xsd:boolean">0</Value></ParameterValueStruct>
<ParameterValueStruct>
<Name>InternetGatewayDevice.Services.VoiceService.2.PhyInterface.2.X_AVM-
DE_CallWaiting</Name>
<Value xsi:type="xsd:boolean">0</Value></ParameterValueStruct>
<ParameterValueStruct>
<Name>InternetGatewayDevice.Services.VoiceService.2.PhyInterface.2.X_AVM-
DE_FriendlyName</Name>
<Value xsi:type="xsd:string"></Value></ParameterValueStruct>
<ParameterValueStruct>
<Name>InternetGatewayDevice.Services.VoiceService.2.PhyInterface.2.X_AVM-
DE_MSNList</Name>
<Value xsi:type="xsd:string"></Value></ParameterValueStruct>
<ParameterValueStruct>
<Name>InternetGatewayDevice.Services.VoiceService.2.PhyInterface.2.X_AVM-
```

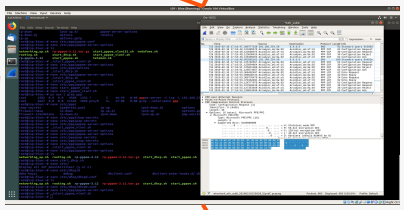
Agenda II



Internet

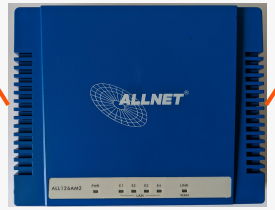


ACS VM



Provider VM

Ether

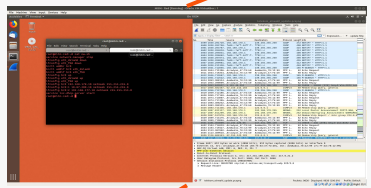


DSLAM Provider

DSL

Modem

Ether



MitM VM

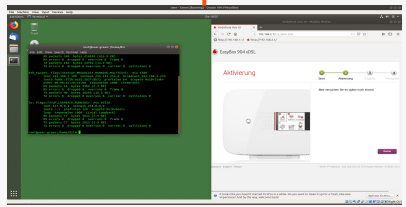
Ether

DSLAM MitM

DSL

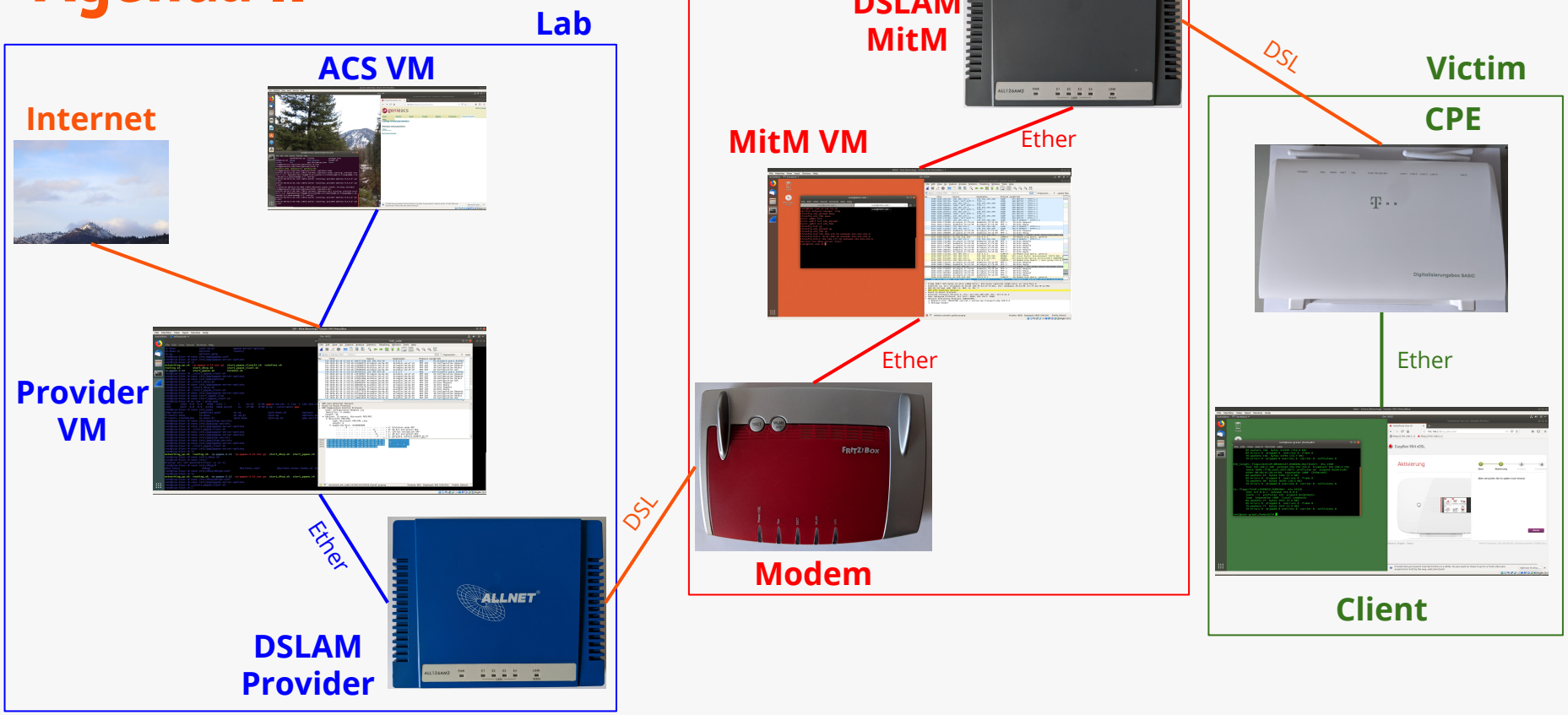
CPE

Ether

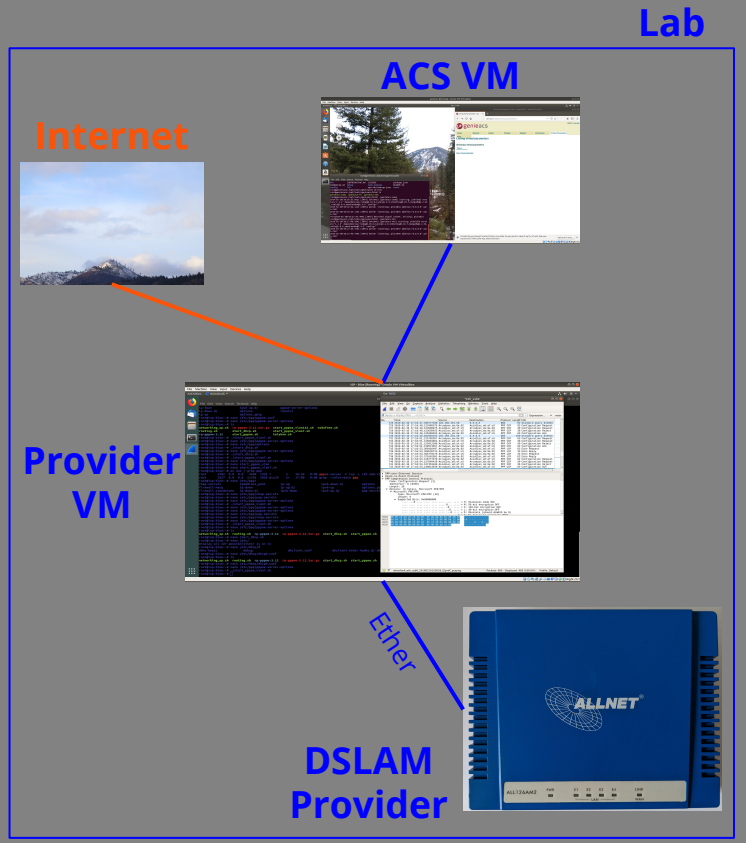


Client

Agenda II


Lab
ACS VM
Internet
Provider VM
Ether
DSLAM Provider
DSL
Attacker
DSLAM MitM
DSL
Victim
CPE
MitM VM
Ether
Ether
Ether
Modem
Client

Lab

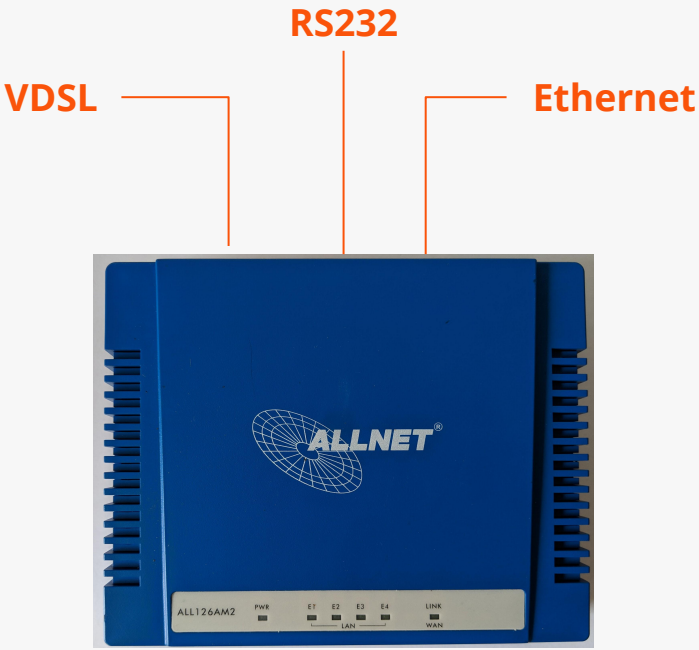

Lab
ACS VM
Internet
Provider
VM
Ether
DSLAM
Provider
ALLNET

Lab

- One DSLAM is enough to perform MitM
  - And play with both the upstream network and the router
- I wanted a complete setup
  - Test MitM functionality
  - Not have to develop on a live network
    - Touch a live network will be illegal!

DSLAM

- ALLNET ALL126AM
  - VDSL DSLAM, 1 Port, upto 100Mbit/100Mbit
  - 4 Ethernet Ports
  - Serial Console / Telnet
- Runs a basic Linux
  - Most settings are done via Shell scripts
  - Thus the device is great for fiddling
- For basic start one just has to select:
  - Profile: Vdsl2 Profile17a, 30a
  - Band Plan: Annex A, Annex B
  - Filter
  - ToneMode: B43



Thx to Christian Kagerhuber for pointing out this DSLAM back then

Provider VM

- PPPoE Server
  - Roaring Penguin PPPoe
  - Supports
    - PAP, CHAP and no login
- VLANs
  - Various routers use different VLANs
  - It’s easy to see requests and replies and wonder why nothing works, due to being in different VLANs

```
root@isp-blue:/etc/ppp# cat pppoe-server-opt
ions
#require-chap
#require-pap
#login
lcp-echo-interval 10
lcp-echo-failure 2
ms-dns 192.168.58.3
netmask 255.255.255.0
defaultroute
noipdefault
usepeerdns
root@isp-blue:/etc/ppp# cat chap-secrets
# Secrets for authentication using CHAP
# client                                        s
erver   secret          IP addresses
"a"                                             *
"b"             *
"arcor.komplett/acsaka-AR904X-R4422027049" *
"acsaka"        *
#"4083045163-001A2A@s93.bbi-o2.de"          *
"2285622000"    *
"4083045163-001A2A@s93.bbi-o2.de"
    *       "0000000000"    *
root@isp-blue:/etc/ppp#
```

ACS - Auto Configuration Server

- The service using the infamous TR-069 protocol
- GenieACS is well known OpenSource solution
- Exchange in XML/SOAP format
- CPE regularly connects to the ACS and fetches new settings
    - Or the Server asks for a callback

```
POST / HTTP/1.1
Host: 192.168.58.4:7547
Content-Length: 2567
Content-Type: text/xml; charset="utf-8"
SOAPAction: "cwmp:Inform"


<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:soap-
enc="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:cwmp="urn:dslforum-org:cwmp-1-0">
<soap:Header>
<cwmp:ID soap:mustUnderstand="1">106</cwmp:ID></soap:Header>
<soap:Body>
<cwmp:Inform>
<DeviceId>
<Manufacturer>AVM</Manufacturer>
<OUI>00040E</OUI>
<ProductClass>FRITZ!Box</ProductClass>
<SerialNumber>7C        99</SerialNumber></DeviceId>
<Event soap-enc:arrayType="cwmp:EventStruct[2]">
<EventStruct>
<EventCode>1 BOOT</EventCode>
<CommandKey></CommandKey></EventStruct>
<EventStruct>
<EventCode>0 BOOTSTRAP</EventCode>
<CommandKey></CommandKey></EventStruct></Event>
<MaxEnvelopes>1</MaxEnvelopes>
<CurrentTime>0001-01-02T14:02:40</CurrentTime>
<RetryCount>0</RetryCount>
<ParameterList soap-enc:arrayType="cwmp:ParameterValueStruct[8]">
<ParameterValueStruct>
<Name>InternetGatewayDevice.DeviceSummary</Name>
<Value xsi:type="xsd:string">InternetGatewayDevice:1.4[](Baseline:2, EthernetLAN:1,
ADSLWAN:1,ADSL2WAN:1, Time:2, IPPing:1, WiFiLAN:2, DeviceAssociation:1), VoiceService:
1.0[2](SIPEndpoint:1, Endpoint:1, TAEndpoint:1), StorageService:1.0[1](Baseline:1,
FTPServer:1, NetServer:1, HTTPServer:1, UserAccess:1, VolumeConfig:1)</Value></
ParameterValueStruct>
<ParameterValueStruct>
<Name>InternetGatewayDevice.DeviceInfo.HardwareVersion</Name>
```

ACS - Getting started

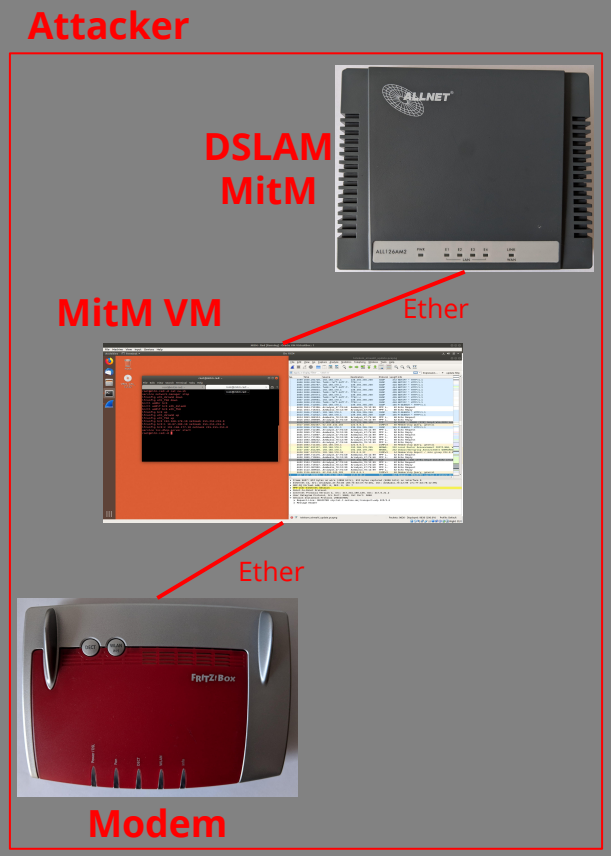
- Use an AVM FritzBox!
  - Can be configured via TR-064 to use TR-069
- GenieACS offers basic functionality
  - Show status, firmware info, configuration
  - Trigger reset etc.
- Being typical HTTP, all traffic can be redirected through a proxy
  - I.e. burp

FritzBox - TR-064

- uPnP based protocol for configuration of CPE
  - Standard specified by broadband forum
- SOAP interface
- Nicely documented by AVM
  - Multiple documents for specific functions
  - Usually authenticated (disabled in my lab setup)

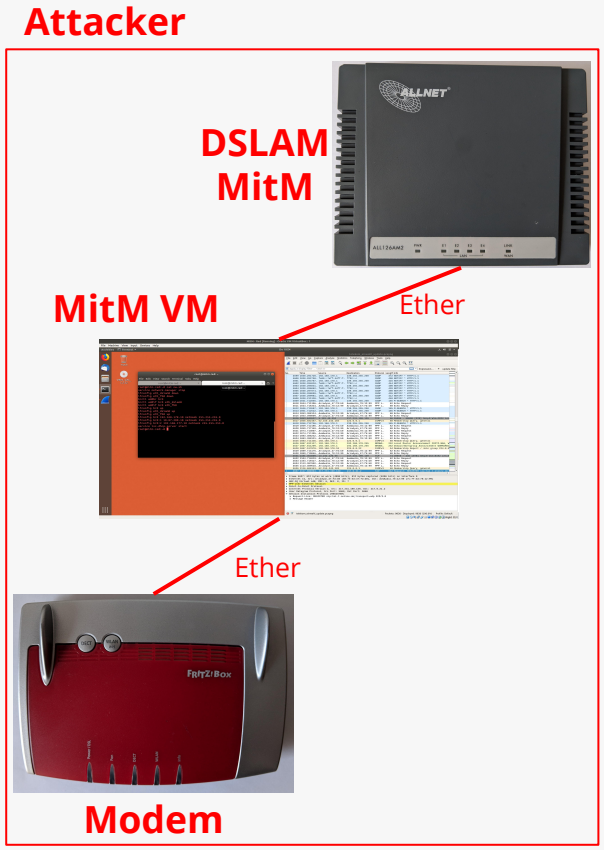
```
import requests

url = 'http://192.168.178.1:49000'
path = '/upnp/control/mgmsrv'


service = 'ManagementServer:1'
action = 'SetManagementServerURL'
#parameters = '<NewURL>http://192.168.58.5/tr069</NewURL>'
parameters = '<NewURL>http://192.168.58.4:7547</NewURL>'

payload= '<?xml version="1.0"?>'\
                '<s:Envelope
xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"s:encodingStyle="http://schemas.
xmlsoap.org/soap/encoding/">'\
                '<s:Body>'\
                '<u:' + action + ' xmlns:u="urn:dslforum-org:service:' + service + '">'\
                        '' + parameters + ''\
                '</u:' + action + '>'\
                '</s:Body>'\
                '</s:Envelope>'

headers = {
'SOAPACTION' : 'urn:dslforum-org:service:' + service + '#' + action,
'USER-AGENT' : 'Evil Hacker',
'CONTENT-TYPE' : 'text/xml; charset="utf-8"',
}

resp = requests.post(url+path,headers=headers,data=payload)

print resp.text
```

Attacker


Attacker
DSLAM
MitM
ALLNET
MitM VM
Ether
Ether
FRITZ!Box
Modem

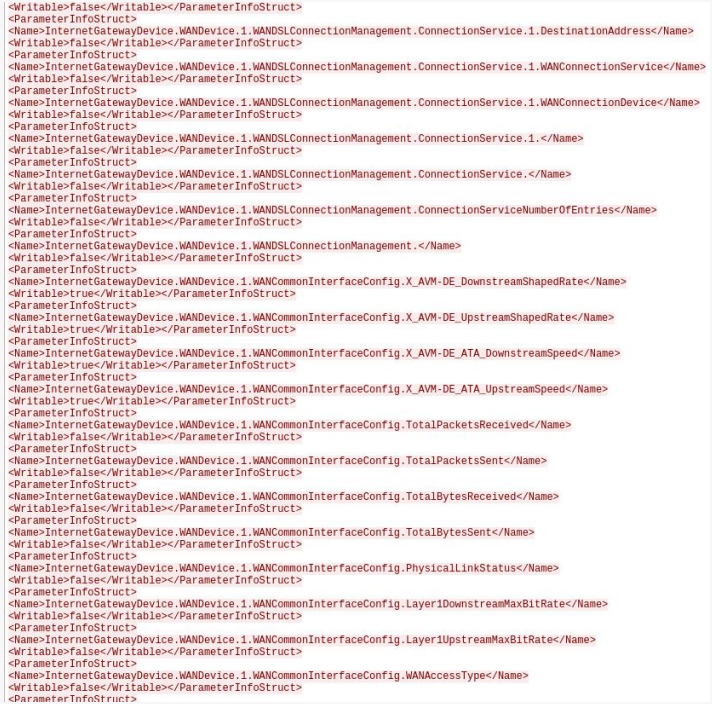
MitM

- The DSLAM terminates victim’s physical DSL connection
  - Layer2
- VM allows full access to traffic
- Modem forwards traffic to operator’s network
- Traffic is encapsulated in PPPoE
  - Needs to be opened or terminated



Playing with TR-069

- CPE has a callback address
  - I.e. 192.168.254.50:8089/1630d01718605b7
- When URL is called, the CPE will call home
  - And fetch data
- A vast amount of settings can be configured via TR-069
  - Thus fuzzing is a “quick” approach for testing
- Obviously, payloads can be sent into both directions



Port Scanning

- Not necessarily very trivial
  - Some services might be bound to certain source IPs
  - Others to specific VLANs
- Passive recon is key
  - Prior running active detection
- Afterwards NMAP does the job!

```
Not shown: 65533 filtered ports
PORT     STATE SERVICE VERSION
5070/tcp open  vtsas?
7547/tcp open  soap    gSOAP 2.7
|_http-server-header: gSOAP/2.7
|_http-title: Site doesn't have a title (text/
xml; charset=utf-8).
Warning: OSScan results may be unreliable because
we could not find at least 1 open and 1 closed
port
Device type: specialized|storage-misc
Running (JUST GUESSING): Crestron 2-Series (87%),
HP embedded (85%)
OS CPE: cpe:/o:crestron:2_series cpe:/
h:hp:p2000_g3
Aggressive OS guesses: Crestron XPanel control
system (87%), HP P2000 G3 NAS device (85%)
No exact OS matches for host (test conditions non-
ideal).
Uptime guess: 0.073 days (since     Mar
         2019)
TCP Sequence Prediction: Difficulty=263 (Good
luck!)
IP ID Sequence Generation: All zeros
```

SIP

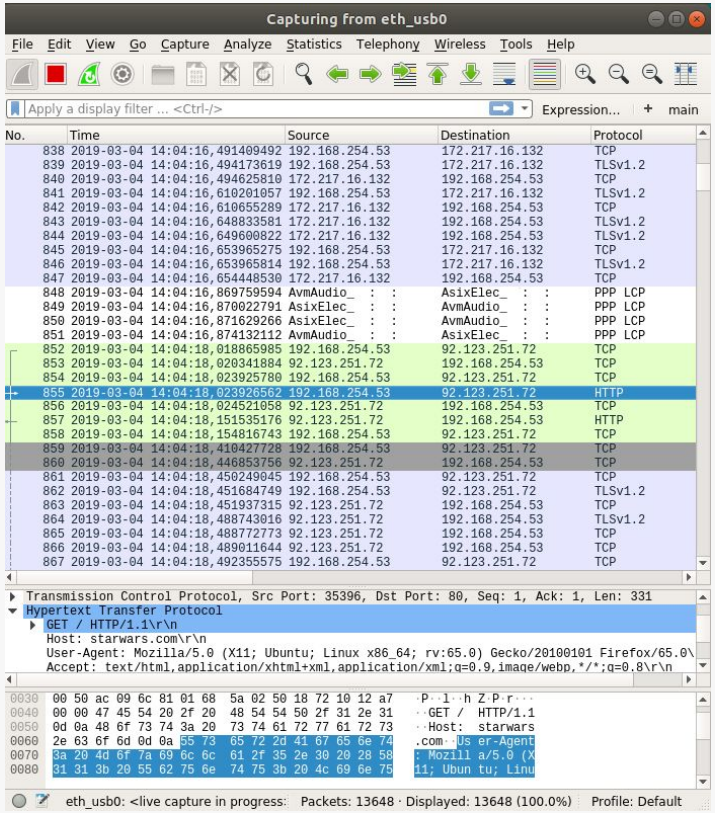
- Talking SIP is possible into both directions
  - Towards CPE and the backend / IMS
- The past has already shown various issues with VoIP implementations
- I’d recommend having a look at Fatih Ozavci’s work
  - Viproy
- Otherwise Wireshark will do the job if you just want to listen

Backend Access

- Obviously a very dark grey & black topic!
- Many services might have public IPs
  - But access is limited to within the operator's network
- Thus working anonymously will be very tough

This was a short chapter

- It’s all IP!



Victim


Victim
CPE
Digitalisierungsbox BASIC
Ether
Aktivierung
Client

Vodafone EasyBox 904 xDSL

- Manufactured by Astoria Networks
- Should be from 2015
- Latest Firmware: 04.13 / 20.03.2018
- Serial: R4422027049
- Communication runs on VLAN 132
- Creates PPP context with “default” credentials
  - Happy to speak both CHAP & PAP
  - User: arcor.komplett/acsaka-AR904X-R4422027049
  - Pass: acsaka

Vodafone EasyBox 904 xDSL

- Not a lot of fun to start working with
  - Requires a Modem Initialization Code (MIC) for initial setup - which I didn't have and couldn't find
  - So…radare2/Cutter and/or Burp
  - 99117 87247 21403 44796
- Tries to connect to acsaka.arcor-ip.de:22154/TCP after boot
  - Boot does take a few minutes :-(

O2 Box 6431

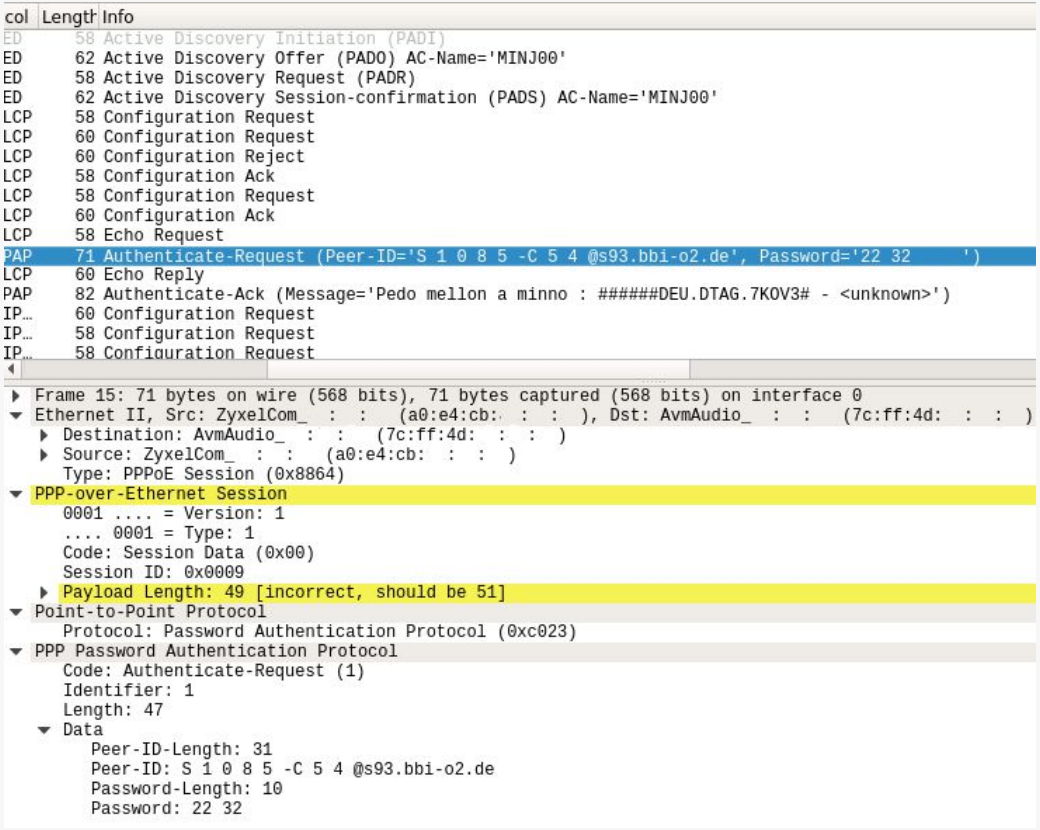
- Manufactured by Astoria Networks
- From 2013?2012?
- Serial: 4083045163
- Communication runs on VLAN7
- Creates PPP Context with a real password?
  - Starts of using PAP
  - User: 4083045163-001A2A@s93.bbi-o2.de
  - Pass: 2285622000 (oops)
  - After Reset it uses the Pass: 0000000000

O2 HomeBox 6641

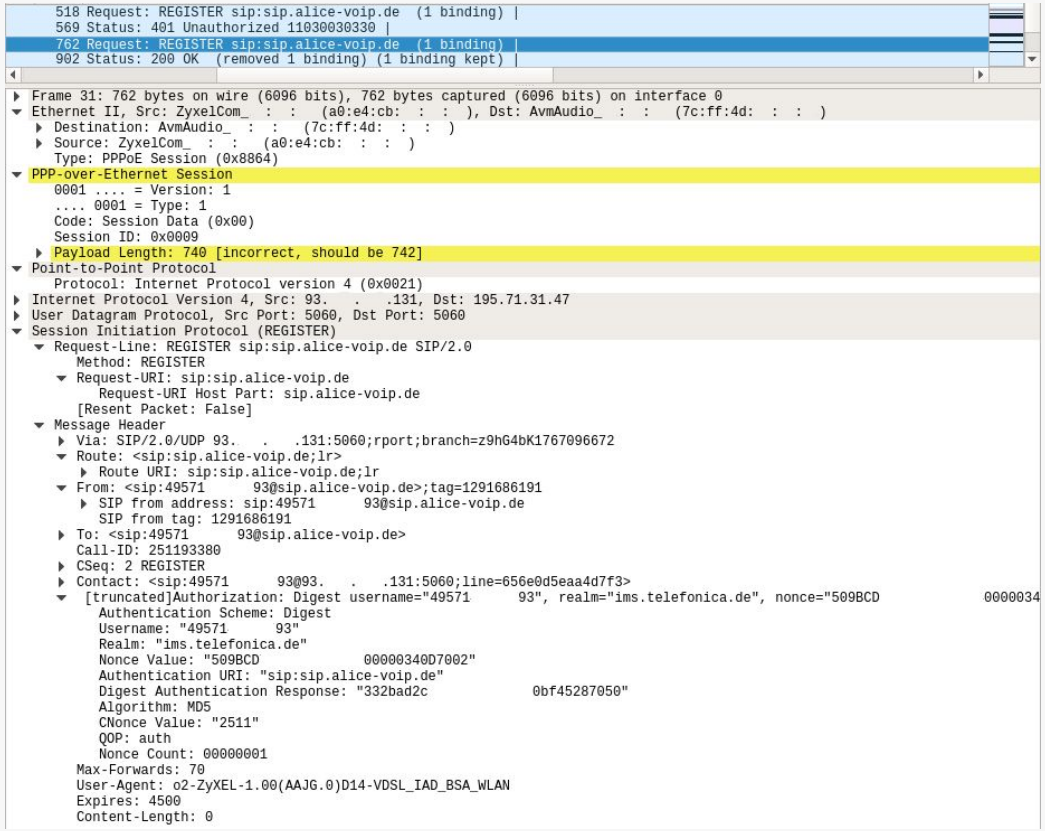
- Manufactured by Zyxel

- A good friend has one in use and allowed me to do a quick sniff

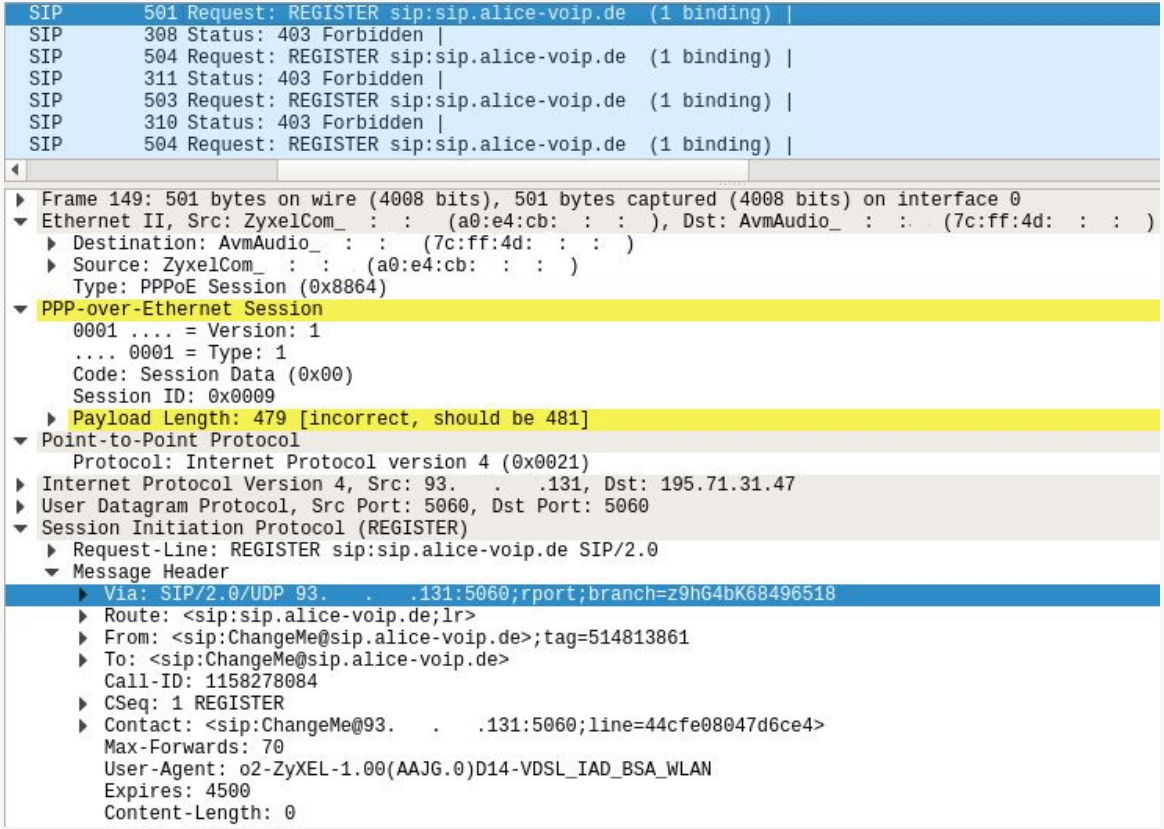
And I forgot to take a picture :(


col Length Info
ED 58 Active Discovery Initiation (PADI)
ED 62 Active Discovery Offer (PADO) AC-Name='MINJ00'
ED 58 Active Discovery Request (PADR)
ED 62 Active Discovery Session-confirmation (PADS) AC-Name='MINJ00'
LCP 58 Configuration Request
LCP 60 Configuration Request
LCP 60 Configuration Reject
LCP 58 Configuration Ack
LCP 58 Configuration Request
LCP 60 Configuration Ack
LCP 58 Echo Request
PAP 71 Authenticate-Request (Peer-ID='S 1 0 8 5 -C 5 4 @s93.bbi-o2.de', Password='22 32 ')
LCP 60 Echo Reply
PAP 82 Authenticate-Ack (Message='Pedo mellon a minno : ######DEU.DTAG.7KOV3# - <unknown>')
IP… 60 Configuration Request
IP… 58 Configuration Request
IP… 58 Configuration Request
Frame 15: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
Ethernet II, Src: ZyxelCom_ : : (a0:e4:cb: : :), Dst: AvmAudio_ : : (7c:ff:4d: : :)
Destination: AvmAudio_ : : (7c:ff:4d: : :)
Source: ZyxelCom_ : : (a0:e4:cb: : :)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 .... = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x0009
Payload Length: 49 [incorrect, should be 51]
Point-to-Point Protocol
Protocol: Password Authentication Protocol (0xc023)
PPP Password Authentication Protocol
Code: Authenticate-Request (1)
Identifier: 1
Length: 47
Data
Peer-ID-Length: 31
Peer-ID: S 1 0 8 5 -C 5 4 @s93.bbi-o2.de
Password-Length: 10
Password: 22 32

O2 Dial In



SIP Register

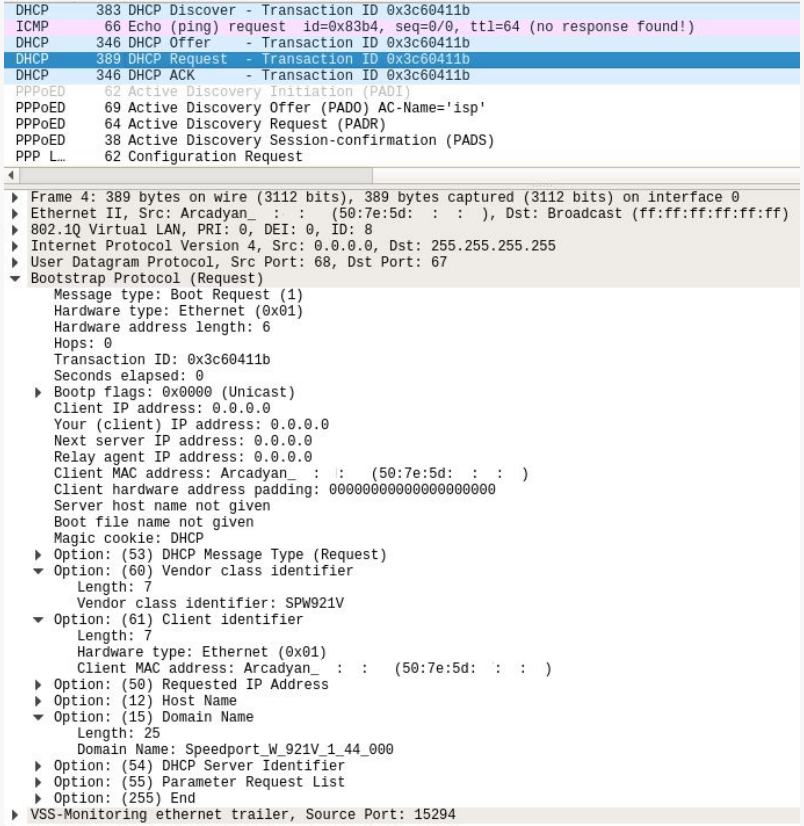


SIP Register - Unconfigured? :)

Telekom Speedport W921V

- Produced by Arcadyan
- From ?2010?2011?
- Last firmware 1.45.000, 01.2019

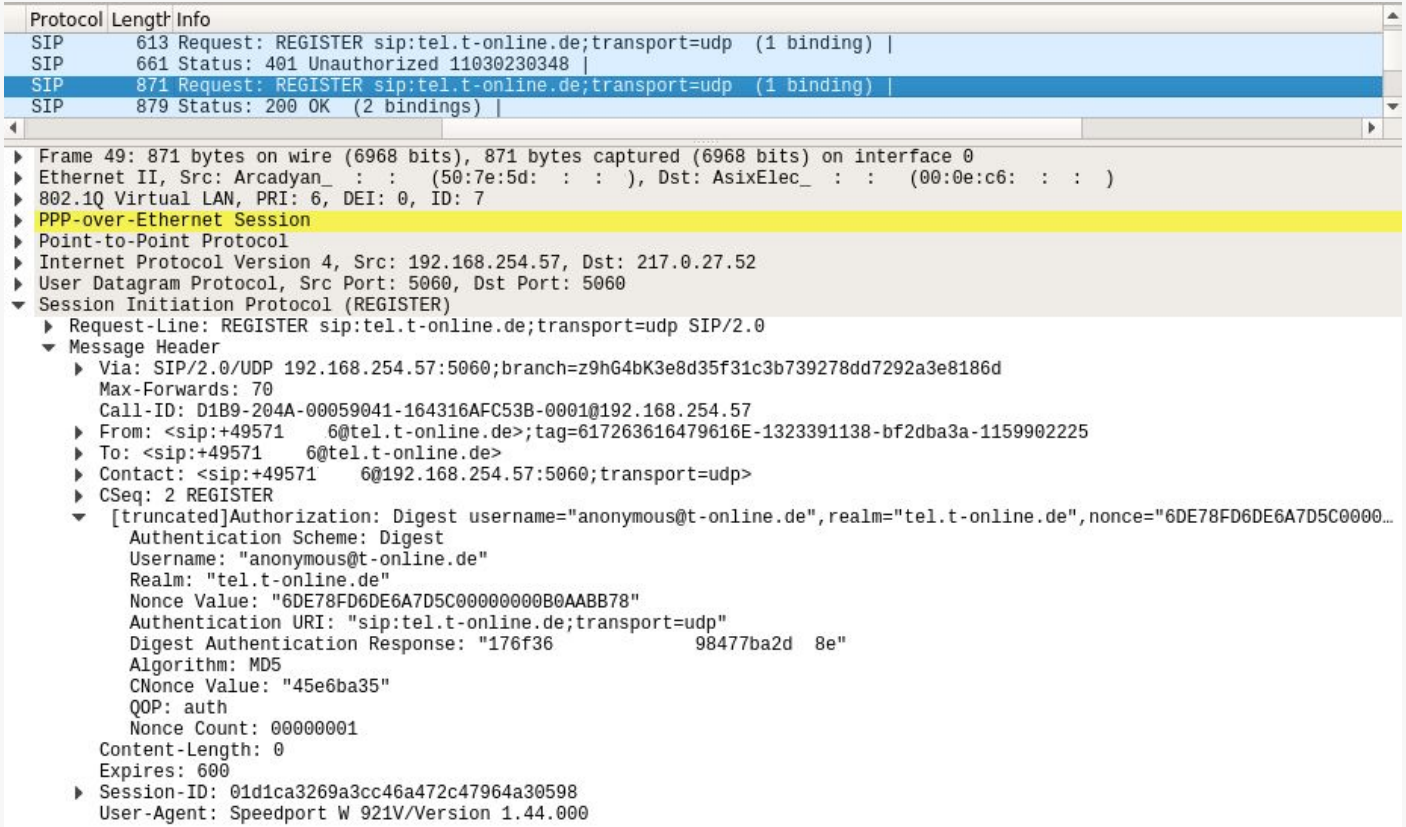
- Starts off by requesting DHCP on VLAN 8
  - Which should be used for Entertain



Telekom Dial In (Lab)

```
DNS        90 Standard query 0xfe38 A nTp1.t-OnLiNe.de
DNS       104 Standard query response 0xfe38 A nTp1.t-OnLiNe.de A 194.25.134.196
DNS        90 Standard query 0x214f AAAA NTp1.T-oNlInE.de
DNS       116 Standard query response 0x214f AAAA NTp1.T-oNlInE.de AAAA 2003:2:2:140:194:25:134:196
NTP       104 NTP Version 1, client
NTP       102 NTP Version 1, server
DNS        99 Standard query 0xc447 SRV _SIP._UdP.tEl.T-onlinE.DE
DNS       189 Standard query response 0xc447 SRV _SIP._UdP.tEl.T-onlinE.DE SRV 10 0 5060 do-epp-801.
DNS       100 Standard query 0x82c2 A DO-epP-801.eDns.t-IPnet.dE
DNS       114 Standard query response 0x82c2 A DO-epP-801.eDns.t-IPnet.dE A 217.0.27.52
DNS       100 Standard query 0xee18 AAAA do-ePP-801.EDnS.t-ipnET.De
DNS       160 Standard query response 0xee18 AAAA do-ePP-801.EDnS.t-ipnET.De SOA ns1.EDnS.t-ipnET.De
DNS       100 Standard query 0x1e75 A h2-ePP-801.eDNs.t-ipNeT.dE
DNS       114 Standard query response 0x1e75 A h2-ePP-801.eDNs.t-ipNeT.dE A 217.0.128.132
DNS       100 Standard query 0x89ca AAAA H2-epp-801.EDnS.T-iPnet.DE
DNS       160 Standard query response 0x89ca AAAA H2-epp-801.EDnS.T-iPnet.DE SOA ns1.EDnS.T-iPnet.DE
```

SPecIal DNs ReQUesTs?



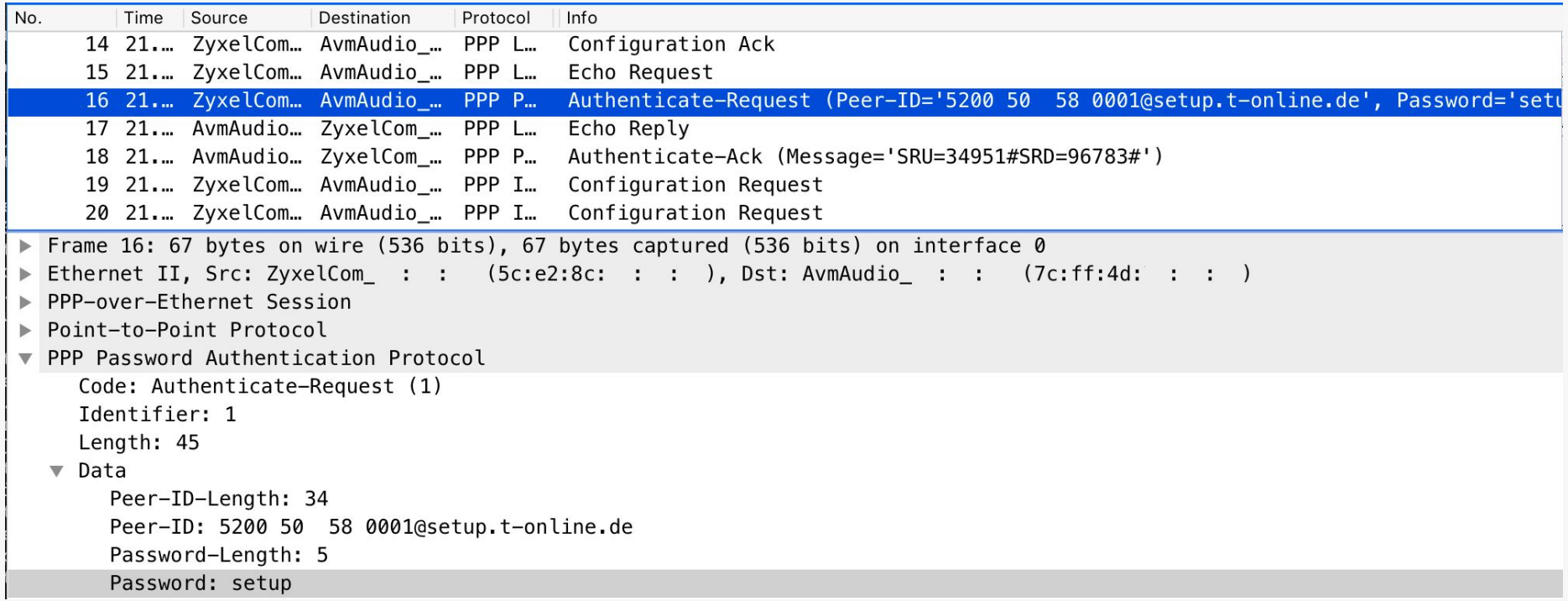
SIP Register

```
GET /tftpboot/cpe/DTAG-CPE-Information.xml HTTP/1.1
Accept: */*
Host: firmware.acs.t-online.de
Connection: close

HTTP/1.1 200 OK
Date: Wed, 17 Oct 2018 08:31:27 GMT
Server: Apache
Last-Modified: Wed, 10 Oct 2018 11:59:46 GMT
ETag: "1ca6-577de97285080"
Accept-Ranges: bytes
Content-Length: 7334
Connection: close
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<ns:DTAG-CPE-Information xmlns:ns="http://sdb.telekom.com/Files/CPEInfo/v1">
<ns:CPE>
  <ns:productClass>DTW724VA</ns:productClass>
  <ns:modelName>Speedport W 724V Typ B</ns:modelName>
  <ns:firmwareVersion>01011603.06.002</ns:firmwareVersion>
  <ns:level>mandatory</ns:level>
  <ns:imageURL>http://fw-acs.t-online.de:8880/tftpboot/DTW724VA/01011603.06.002.bin</ns:imageURL>
  <ns:digest>edaee134cb843e5efb9bec1a4bf4cf3b</ns:digest>
</ns:CPE>
<ns:CPE>
  <ns:productClass>DTW724VR</ns:productClass>
  <ns:modelName>Speedport W 724V Typ C</ns:modelName>
  <ns:firmwareVersion>09011603.05.017</ns:firmwareVersion>
  <ns:level>mandatory</ns:level>
  <ns:imageURL>http://fw-acs.t-online.de:8880/tftpboot/DTW724VR/09011603.05.017.img</ns:imageURL>
  <ns:digest>a1128fe2a47837de591f08b165480929</ns:digest>
</ns:CPE>
<ns:CPE>
  <ns:productClass>DTW724VH</ns:productClass>
  <ns:modelName>Speedport W 724V Typ A</ns:modelName>
  <ns:firmwareVersion>05011603.06.001</ns:firmwareVersion>
  <ns:level>mandatory</ns:level>
  <ns:imageURL>http://fw-acs.t-online.de:8880/tftpboot/DTW724VH/05011603.06.001.bin</ns:imageURL>
  <ns:digest>91c1e4cc7e60df89fa627241fa25f628</ns:digest>
</ns:CPE>
<ns:CPE>
  <ns:productClass>DTP700DT</ns:productClass>
  <ns:modelName>Speedphone 700</ns:modelName>
  <ns:firmwareVersion>Rel2_RC11</ns:firmwareVersion>
  <ns:level>mandatory</ns:level>
  <ns:imageURL>http://80.156.86.10:8880/tftpboot/DTP700DT/update.bin</ns:imageURL>
  <ns:digest>383b0b9bce8957f650d90d331ef28376</ns:digest>
</ns:CPE>
<ns:CPE>
  <ns:productClass>DTP701DT</ns:productClass>
  <ns:modelName>Speedphone 701</ns:modelName>
  <ns:firmwareVersion>SP701_REL2_RC19</ns:firmwareVersion>
  <ns:level>mandatory</ns:level>
  <ns:imageURL>http://fw-acs.t-online.de:8880/tftpboot/DTP701DT/update.bin</ns:imageURL>
  <ns:digest>d07bcd83678f1584e10ce2520c4bd21b</ns:digest>
  </ns:CPE>
<ns:CPE>
```

Update Check

Telekom Digitalisierungsbox Basic

- Produced by Zyxel
  - All-IP-Router VMG8825-D70B
  - Sadly Telekom removed SSH
- From 2018
- Latest Firmware: 12.39.2.04.00, 03.2019
- Supports Auto-Configuration
  - Has to be enabled in the Telekom Customer interface
  - Thought this might be a good chance to give it a try



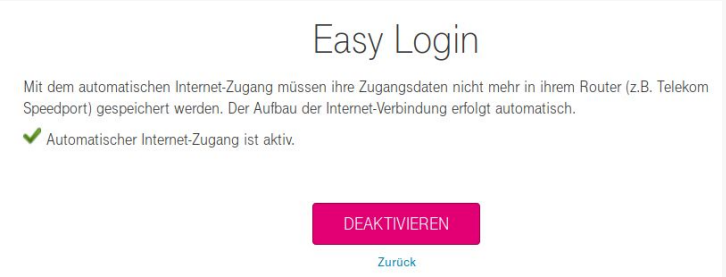
Initial Login

No.	Time	Source	Destination	Protocol	Info
158	177…	2003:db:…	2003:180:…	DNS	Standard query 0xbe2b A acs.t-online.de
159	177…	2003:180…	2003:db:3…	DNS	Standard query response 0xbe2b A acs.t-online.de A 80.156.86.10
160	177…	79.218.2…	80.156.86…	TCP	56414 → 443 [SYN, ECN, CWR] Seq=0 Win=14520 Len=0 MSS=1452 SACK_PERM=1 TSval=4294884043
161	177…	80.156.8…	79.218.29…	TCP	443 → 56414 [SYN, ACK] Seq=0 Ack=1 Win=4356 Len=0 MSS=1452 TSval=1983717461 TSecr=429488
162	177…	79.218.2…	80.156.86…	TCP	56414 → 443 [ACK] Seq=1 Ack=1 Win=14520 Len=0 TSval=4294884056 TSecr=1983717461
163	177…	79.218.2…	80.156.86…	TLSv1…	Client Hello
164	177…	80.156.8…	79.218.29…	TCP	443 → 56414 [ACK] Seq=1 Ack=518 Win=4873 Len=0 TSval=1983717475 TSecr=4294884057
165	177…	80.156.8…	79.218.29…	TLSv1…	Server Hello
166	177…	80.156.8…	79.218.29…	TCP	443 → 56414 [ACK] Seq=1441 Ack=518 Win=4873 Len=1440 TSval=1983717477 TSecr=4294884057 [
167	177…	80.156.8…	79.218.29…	TLSv1…	Certificate [TCP segment of a reassembled PDU]
168	177…	79.218.2…	80.156.86…	TCP	56414 → 443 [ACK] Seq=518 Ack=1441 Win=17280 Len=0 TSval=4294884074 TSecr=1983717477
169	177…	79.218.2…	80.156.86…	TCP	56414 → 443 [ACK] Seq=518 Ack=2881 Win=20160 Len=0 TSval=4294884074 TSecr=1983717477
170	177…	79.218.2…	80.156.86…	TCP	56414 → 443 [ACK] Seq=518 Ack=4321 Win=23040 Len=0 TSval=4294884075 TSecr=1983717477
171	177…	80.156.8…	79.218.29…	TLSv1…	Server Key Exchange, Certificate Request, Server Hello Done
172	177…	79.218.2…	80.156.86…	TCP	56414 → 443 [ACK] Seq=518 Ack=4527 Win=25920 Len=0 TSval=4294884086 TSecr=1983717491
173	178…	79.218.2…	80.156.86…	TLSv1…	Certificate, Client Key Exchange
174	178…	79.218.2…	80.156.86…	TLSv1…	Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
175	178…	80.156.8…	79.218.29…	TCP	443 → 56414 [ACK] Seq=4527 Ack=2176 Win=6531 Len=0 TSval=1983718459 TSecr=4294885040
176	178…	80.156.8…	79.218.29…	TLSv1…	Change Cipher Spec
177	178…	80.156.8…	79.218.29…	TLSv1…	Encrypted Handshake Message
178	178…	79.218.2…	80.156.86…	TCP	56414 → 443 [ACK] Seq=2176 Ack=4533 Win=25920 Len=0 TSval=4294885057 TSecr=1983718461
179	178…	79.218.2…	80.156.86…	TCP	56414 → 443 [ACK] Seq=2176 Ack=4578 Win=25920 Len=0 TSval=4294885057 TSecr=1983718461
180	178…	79.218.2…	80.156.86…	TLSv1…	Application Data

Time for the ACS, actually twice

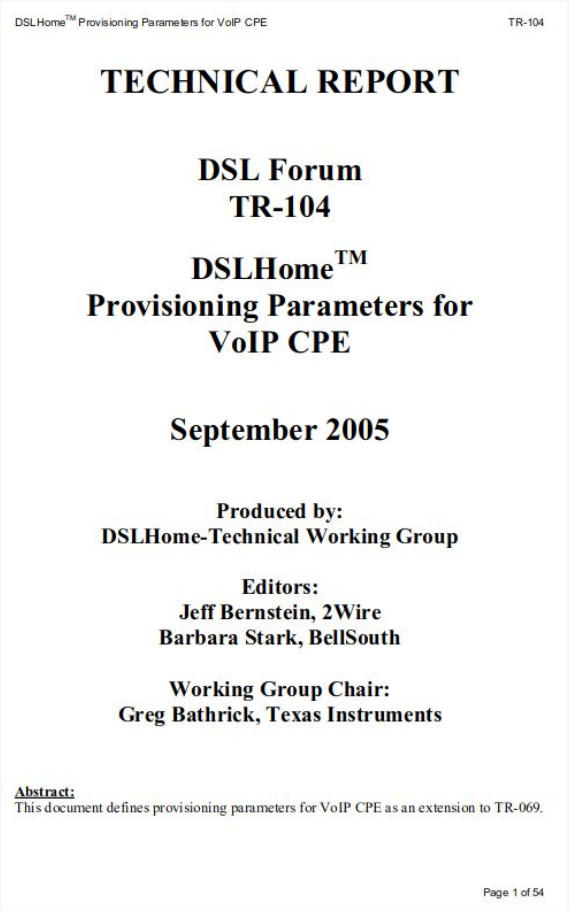
Automatic Configuration

- Automatic configuration will be performed during the ACS connections
- All connections are authenticated using a client certificate
    - Due to only having the one router, I have not had the chance to check whether they're unique



SIP Configuration

- (Contract has three numbers included)
- I have three connections to the ACS
- And then a SIP Register each
  - The same as with the previous Telekom Router
- Cold be a pattern, could be random



DSLHome™ Provisioning Parameters for VoIP CPE TR-104

TECHNICAL REPORT

DSL Forum
TR-104

DSLHome™
Provisioning Parameters for VoIP CPE

September 2005

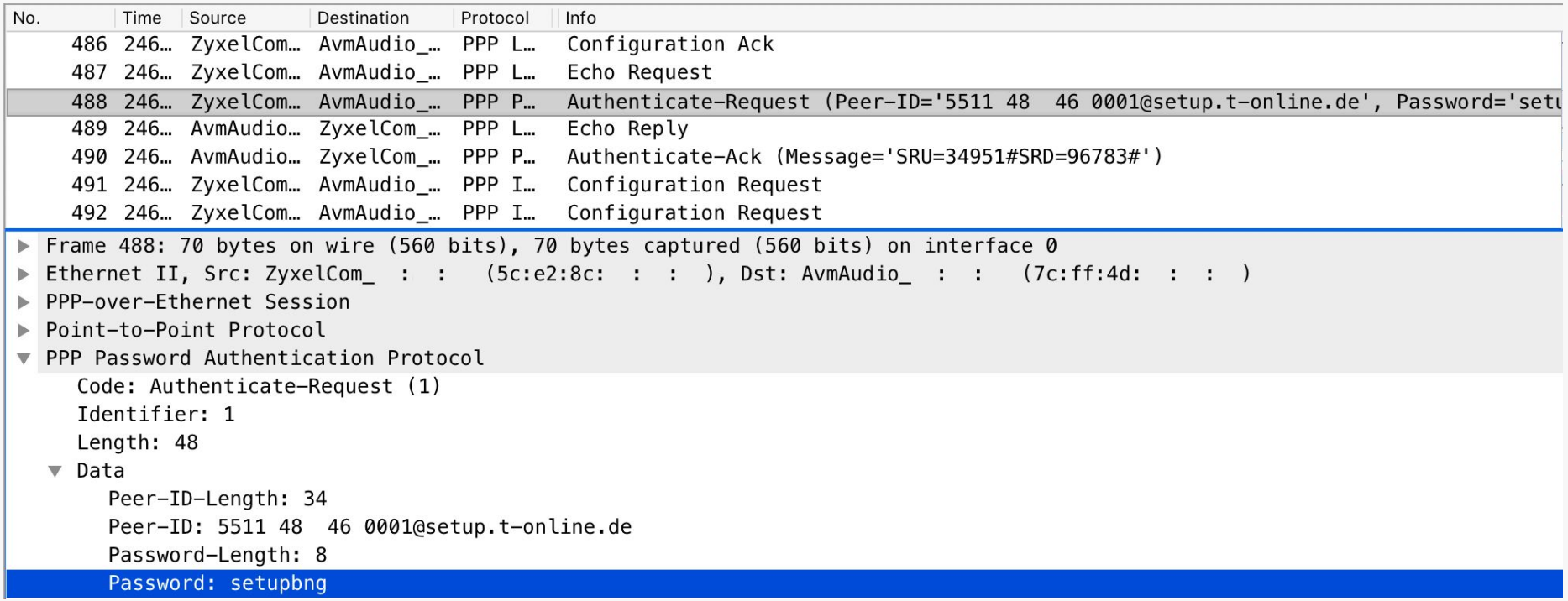
Produced by:
DSLHome-Technical Working Group

Editors:
Jeff Bernstein, 2Wire
Barbara Stark, BellSouth

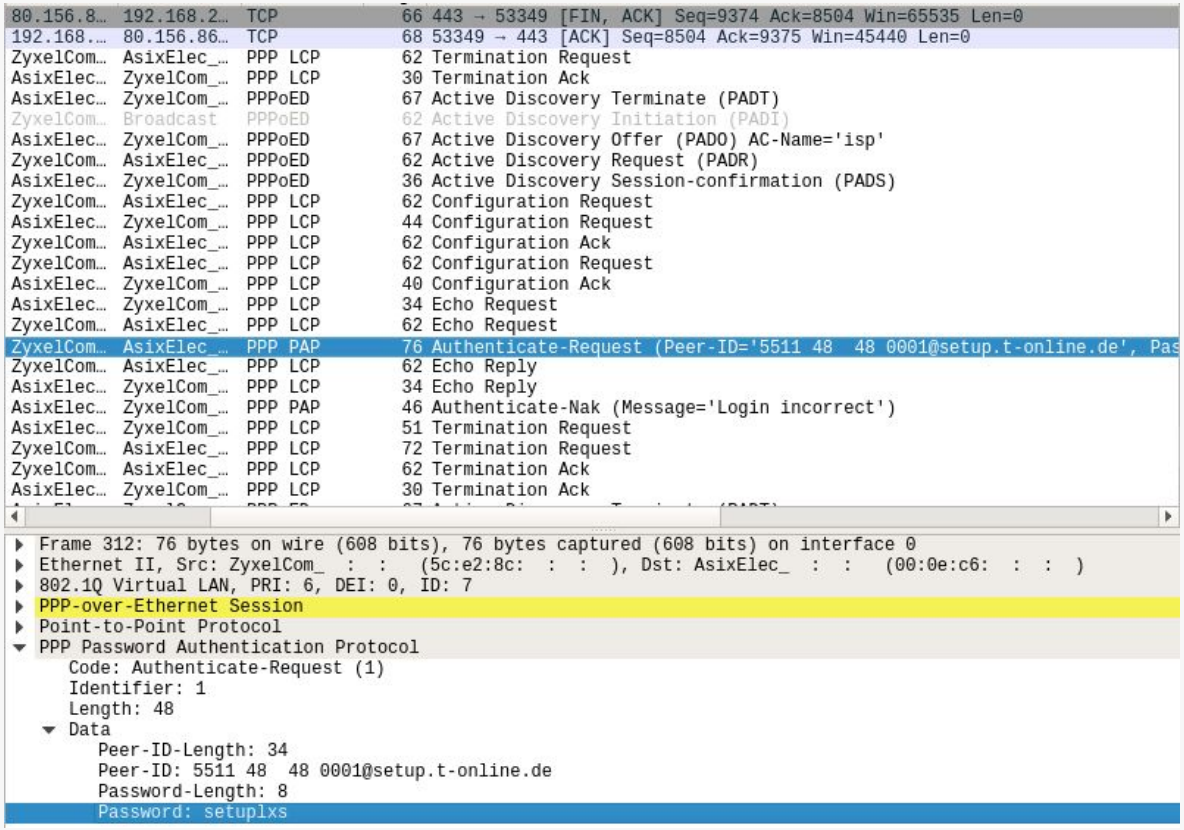
Working Group Chair:
Greg Bathrick, Texas Instruments

Abstract:
This document defines provisioning parameters for VoIP CPE as an extension to TR-069.

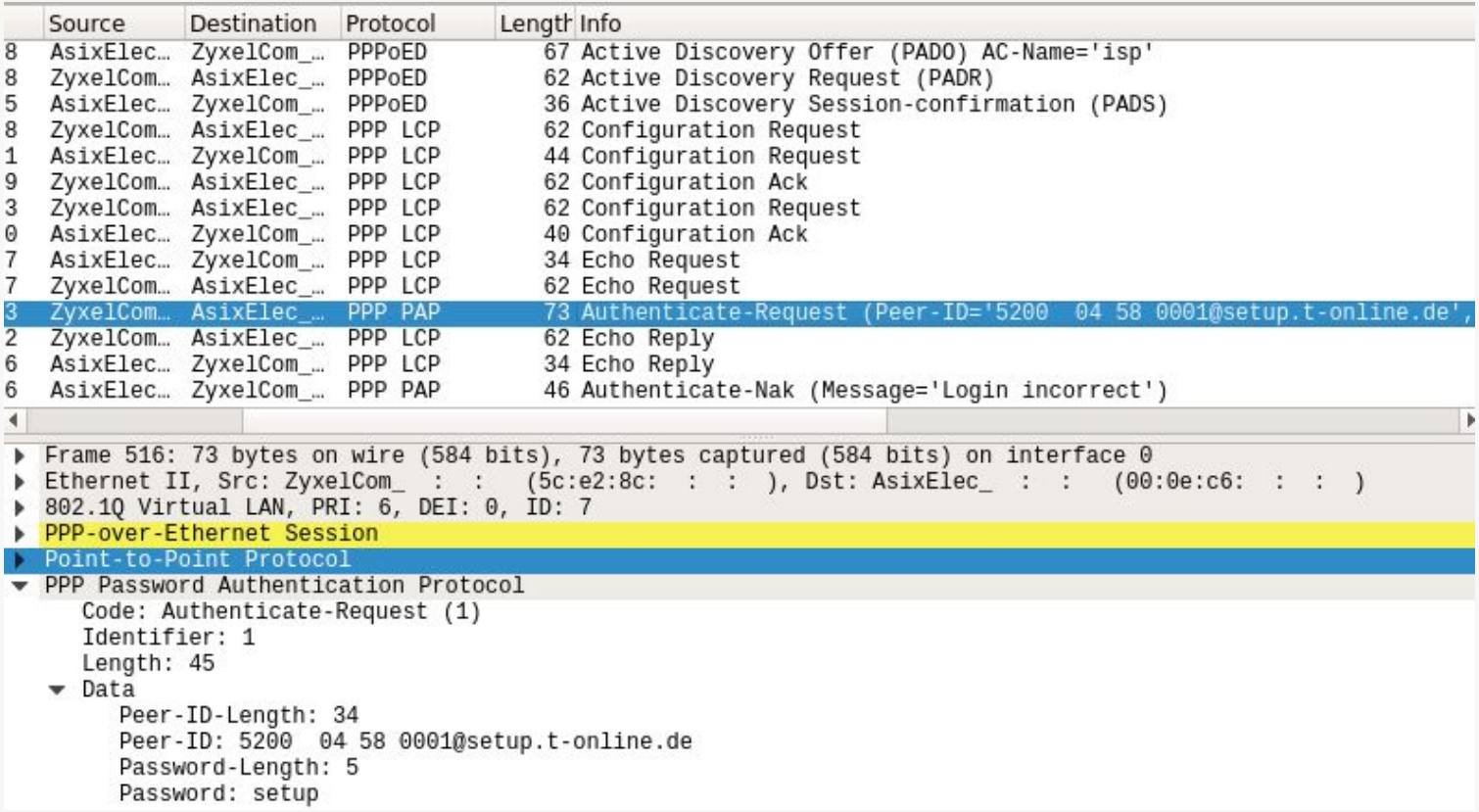
Page 1 of 54



Meanwhile…a Reconnect



Later, in the lab


Source Destination Protocol Length Info
8 AsixElec… ZyxelCom_… PPPoED 67 Active Discovery Offer (PADO) AC-Name='isp'
8 ZyxelCom… AsixElec_… PPPoED 62 Active Discovery Request (PADR)
5 AsixElec… ZyxelCom_… PPPoED 36 Active Discovery Session-confirmation (PADS)
8 ZyxelCom… AsixElec_… PPP LCP 62 Configuration Request
1 AsixElec… ZyxelCom_… PPP LCP 44 Configuration Request
9 ZyxelCom… AsixElec_… PPP LCP 62 Configuration Ack
3 ZyxelCom… AsixElec_… PPP LCP 62 Configuration Request
0 AsixElec… ZyxelCom_… PPP LCP 40 Configuration Ack
7 AsixElec… ZyxelCom_… PPP LCP 34 Echo Request
7 ZyxelCom… AsixElec_… PPP LCP 62 Echo Request
3 ZyxelCom… AsixElec_… PPP PAP 73 Authenticate-Request (Peer-ID='5200 04 58 0001@setup.t-online.de',
2 ZyxelCom… AsixElec_… PPP LCP 62 Echo Reply
6 AsixElec… ZyxelCom_… PPP LCP 34 Echo Reply
6 AsixElec… ZyxelCom_… PPP PAP 46 Authenticate-Nak (Message='Login incorrect')
Frame 516: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
Ethernet II, Src: ZyxelCom_ : : (5c:e2:8c: : :), Dst: AsixElec_ : : (00:0e:c6: : :)
802.1Q Virtual LAN, PRI: 6, DEI: 0, ID: 7
PPP-over-Ethernet Session
Point-to-Point Protocol
PPP Password Authentication Protocol
Code: Authenticate-Request (1)
Identifier: 1
Length: 45
Data
Peer-ID-Length: 34
Peer-ID: 5200 04 58 0001@setup.t-online.de
Password-Length: 5
Password: setup

And then….

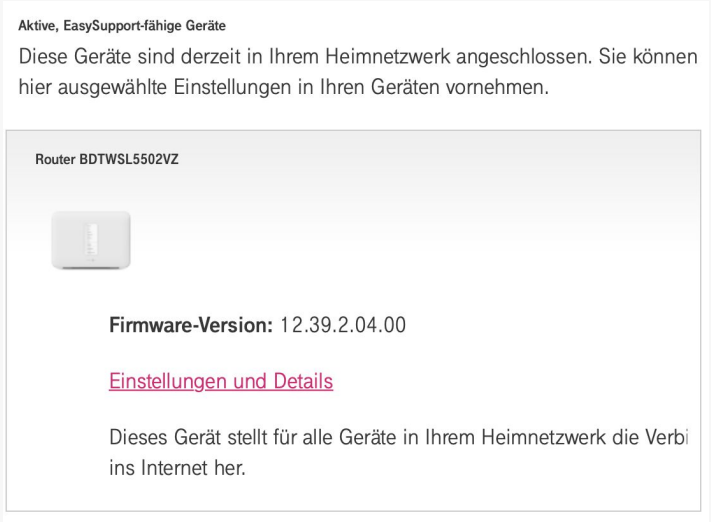
Updates

- Same as before
- Unencrypted update
  - Via HTTP
- Update file is signed

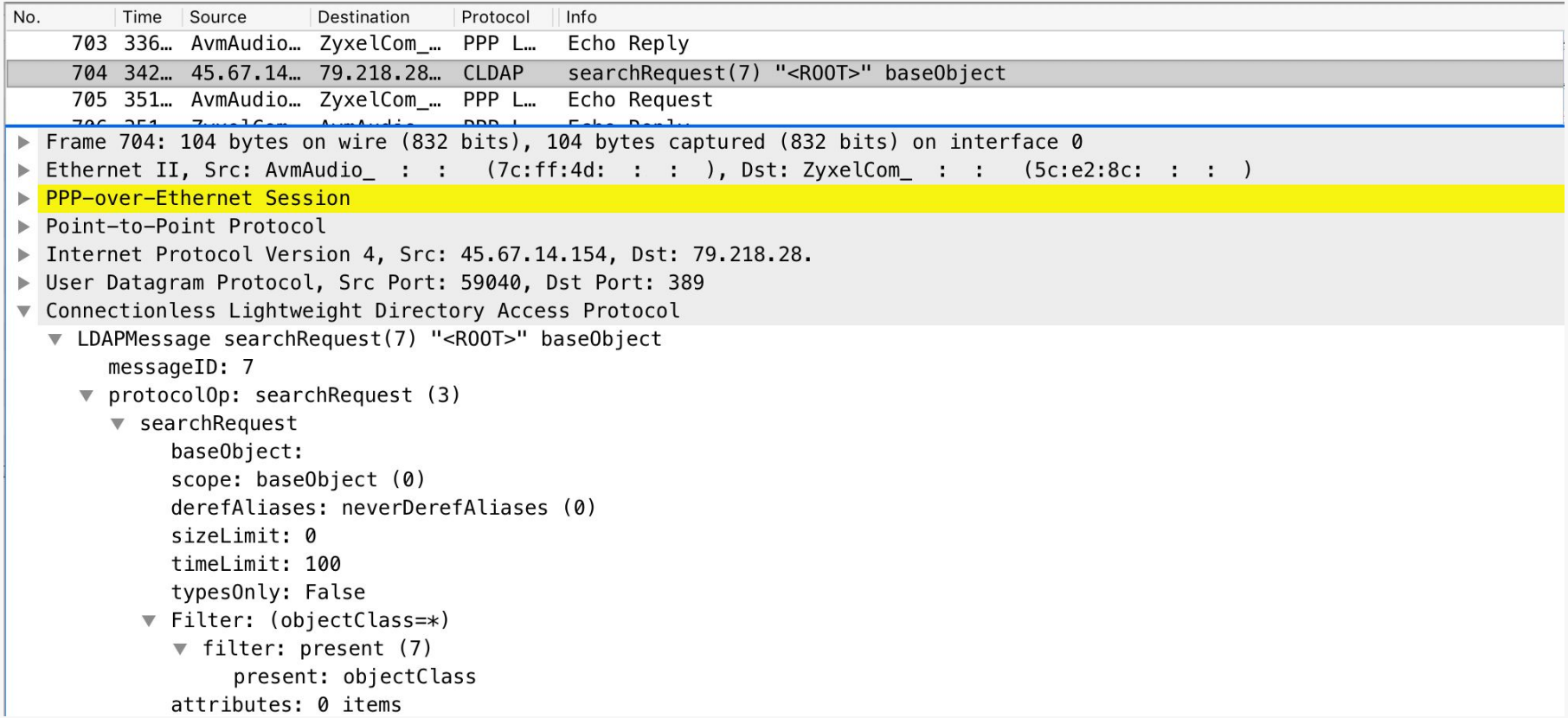
```
GET /tftpboot/BDTWSL5502VZ/12.39.2.03.01.img HTTP/1.1
Range: bytes=0-1023
User-Agent: Sphairon IAD Firmware Downloader/2.0
Host: fw-acs.t-online.de:8880
Accept: */*

HTTP/1.1 206 Partial Content
Date: Wed, 13 Mar 2019 10:03:12 GMT
Server: Apache
Last-Modified: Mon, 01 Oct 2018 08:57:08 GMT
ETag: "1686f92-57726fd702100"
Accept-Ranges: bytes
Content-Length: 1024
Cache-Control: max-age=7200
Expires: Wed, 13 Mar 2019 12:03:12 GMT
Content-Range: bytes 0-1023/23621522
Keep-Alive: timeout=150, max=100
Connection: Keep-Alive
Content-Type: text/plain

Sphairon Software Image Version=1
uimage_size=02260564
uimage_start=00000318
uimage_md5=3cd8d30404f2ef12942a1f77913156d7
platformfs_size=21360640
platformfs_start=02260882
platformfs_md5=72641342b93bd9721c16ce69dc272d73
sign=302c02141cc32a95a77847f2cbd6405cf1c911cba70a1c1002147a9da534764fd09958d77fc68aab91252aa8cea9
.
..."~T...8."}....(..............l."|.....................................\
[..........$....kernel#Linux-3.10.104-zyxel12-
devel.....................images......kernel@0.................3.10.104-
zyxel12-devel........y.....]..............o.......L4...X.
..a..D.....&.$.Xg......;.Eeo.h.L<.j....o...)K0...o..k..22...s.2.:AaN.&.X\Q
+....$..`.C&Z1...h...{4_....41).......$.........     ].
```

Remote Configuration

- Telekom offers “EasySupport” feature
  - Remote configuration of network devices
- Triggers a callback request to the ACS
  - Authenticated, but callback is also triggered without authentication
- Then performs encrypted communications
  - As with the initial setup via ACS



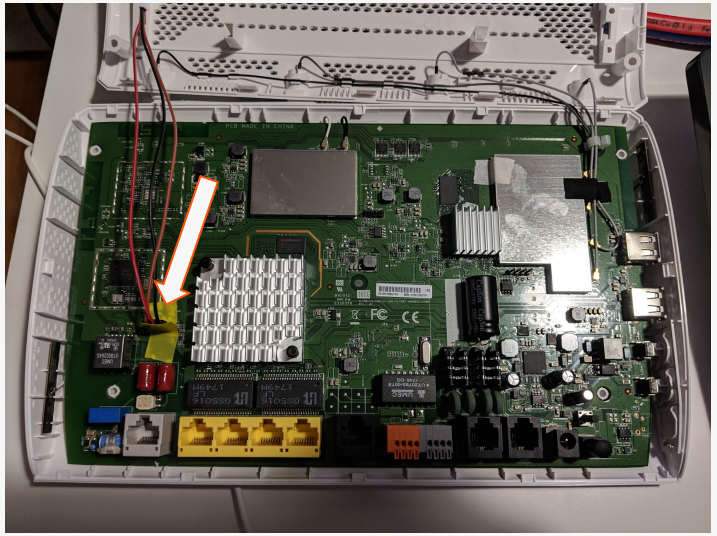

```
GET /e4604e01d294496aa5f3e5d132f34bd3 HTTP/1.1
User-Agent: Jakarta Commons-HttpClient/3.0.1
Authorization: Digest username="acs.t-online.de", realm="SphaironIAD",
nonce="5c8ccbc2ca55906711c8", uri="/e4604e01d294496aa5f3e5d132f34bd3",
response="b0aeb38bdf73aaee0a5210ff7c6f69b1", qop=auth, nc=00000001,
cnonce="eea6d87cda3c6d5e5890e987ad0f7d5d", opaque="265e724b"
Host: 79.218.16.247:7547

HTTP/1.1 200 OK
Server: gSOAP/2.7
Content-Type: text/xml; charset=utf-8
Content-Length: 0
Connection: close
```



Something for the Todo List

Hardware...

- Device has an open UART interface
  - Bootloader: U-Boot
  - Root Shell: BusyBox v1.22.1-sphairon14
- Boot output contains the following lines
  - * ACS authentication STEqv4RZ9Nm6NsBP *
  - * GUI authentication 2296954290 *
- The first should be the password used by the router when connecting to the acs
- The second one is the password for the admin iface



Configuration

- Settings are stored as sqlite tables
  - Directly accessible
- The client key is stored in /config/keys/
  - Binary blob
  - Encrypted? Encoded?

8hr73D+Ytz7EArl9llYJeir5q7z08OiU1MzRwwtZ3JzJU
3uV3ZcEO1ILGS/IKgKogdYrWSC2a88I
Ym0kJ5uc07lFBmD2RieMPZbGZufKMGQiC26ro/FN
gwrLrecIjOKFyaGmNJFJilWRP6lmov3ylmB8
/vxccyHOuO4lhDIjykbSz/6mL6nUm4tB44HuDSipY
Tw1bz6HlKbNcUOVhw5DrcLKBEaAjAgdO5rM
hFBpc4zJnT7bHwwahdZ7PS+0vY+eIoEON5WorrW
UQajA/T0JsPAABghTMObLLUK8bVRbvA1kfS4n
JKD/iuLMlqGq+tc2U/+cv98Tga2mbSa7hxwz3ad+2
hLq7TNvyb2vYd8YI3LM2CNiwY0RODulsz3P
paqsyOT0gytNOKzDdjFQzQEHkAr8aA3CDA4QKW9
DIOrxw4bYzs8/JVe0gRzbu9+FtcS07yv+sqbO
6msKMhvspYvuTaOFggpefeiVcwq6xFhJn3Lv5n5CY
c1EzHdlXgQnauUD237fJfOZIZJavcEjOcqX
DzMxbRb3vSDi26KMHs/GMSWh5cvxq7me5x0nD9
GSnKz3dVzweffjKFzm4kOMlwy0wy47pLvGcXJN
WId+oob5MejpFDmVWq+HqwamydryKd++BkM5iL
q5iUOhq/Kc0TS0CYN7edCnRnsZwCTgGXzq/lkL

This is the actual beginning encoded in B64

```
CREATE TABLE TR069Config
(
	Id INTEGER PRIMARY KEY AUTOINCREMENT,
	Enable INTEGER NOT NULL,
	CNRPort INTEGER NOT NULL,
	CNRPath TEXT NOT NULL,
	ProvisioningCode TEXT NOT NULL,
	CommStateEnable INTEGER NOT NULL,
	BootstrapEventSent INTEGER NOT NULL,
	DynamicCNRPort INTEGER NOT NULL,
	CNRPortWhitelist TEXT NOT NULL,
	CNRPortBlacklist TEXT NOT NULL,
	RootDataModel TEXT NOT NULL,
	ServiceDataModels TEXT NOT NULL,
	ComponentDefinitions TEXT NOT NULL
);
INSERT INTO "TR069Config"
VALUES(1,1,7547,'e4604e01d294496aa5f3e5d132f34bd3','000.001.001.000',0,1,0,'1024-65535','1-7000','Device:2','VoiceSer
vice:2Rev5','');
```

Callback URL

```
CREATE TABLE TR069ACS
(
	Id INTEGER PRIMARY KEY AUTOINCREMENT, ACSName TEXT NOT NULL,
	ACSURL TEXT NOT NULL,  ACSUser TEXT NOT NULL,
	ACSPassword TEXT NOT NULL, ACSDiscovery INTEGER NOT NULL,
	CNRAuthEnable INTEGER NOT NULL, CNRUser TEXT NOT NULL,
	CNRPassword TEXT NOT NULL,  ParameterKey TEXT NOT NULL,
	PeriodicInformEnable INTEGER NOT NULL, PeriodicInformInterval INTEGER NOT NULL,
	PeriodicInformTime TEXT NOT NULL, UpgradesManaged INTEGER NOT NULL,
	SSLCertCheckEnable INTEGER NOT NULL, SSLCertCNCheckEnable INTEGER NOT NULL,
	SSLCertExpirationCheckMode INTEGER NOT NULL, RetryDelayMaxIncrement INTEGER NOT NULL,
	RetryDelayFactor INTEGER NOT NULL, RetryDelayBase INTEGER NOT NULL,
	VcCnrTimeout INTEGER NOT NULL, ClientCertificateEnable INTEGER NOT NULL,
	IpProtocolVersionPriority INTEGER NOT NULL
);
INSERT INTO "TR069ACS"
VALUES(1,'Default','https://acs.t-online.de/acs-v2/','90EF68-BDTWSL5502VZ-S182V13000142','STEqv4RZ9Nm6NsBP',0,1,'acs
.t-online.de','0f5bc0a4bb5a85990872214f29e15bb1','',1,432000,'1980-09-2$
DELETE FROM sqlite_sequence;
```

ACS Connection parameters

Configure my ACS, disable crypto

```
# cfgclient "updatekey TR069ACS ID 1 SSLCertCheckEnable integer:0;"
Operation succeeded
# cfgclient "selectkey TR069ACS ID 1 SSLCertCheckEnable;"
0
# cfgclient "updatekey TR069ACS ID 1 SSLCertCNCheckEnable integer:0;"
Operation succeeded
# cfgclient "updatekey TR069ACS ID 1 ClientCertificateEnable integer:0;"
Operation succeeded
#cfgclient "updatekey TR069ACS ID 1 ACSURL text:http://192.168.58.4:7547;"
Operation succeeded
#cfgclient "updatekey TR069ACS ID 1 CNRAuthEnable integer:0;"
Operation succeeded
```

Data delivered to GenieACS

Device
Device.DeviceInfo
Device.DeviceInfo.HardwareVersion VMG8825-D70B-DE02V1F.1/00
Device.DeviceInfo.ProvisioningCode **000.001.001.000**
Device.DeviceInfo.SoftwareVersion 12.39.2.04.00
Device.DeviceInfo.Description VDSL Annex B IAD with switch with WLAN wit…
Device.DeviceInfo.FirstUseDate 2019-03-15T14:52:31Z+00:00
Device.DeviceInfo.Manufacturer SPHAIRON
Device.DeviceInfo.ManufacturerOUI 90EF68
Device.DeviceInfo.ModelName Digitalisierungsbox BASIC
Device.DeviceInfo.ProductClass BDTWSL5502VZ
Device.DeviceInfo.SerialNumber S182V13000142

Just had to patch GenieACS to support empty tags

<Value>http://192.168.254.53:7547/e4604e01d294496aa5f3e5d132f34bd3</Value></ParameterValueStruct><ParameterValueStruct><Name>Device.ManagementServer.ParameterKey</Name><Value></Value></ParameterValueStruct></ParameterList></cwmp:Inform></SOAP-ENV:Body></SOAP-ENV:Envelope>

Just for completeness

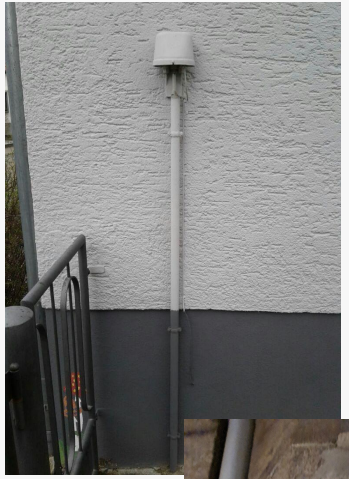
The real end...

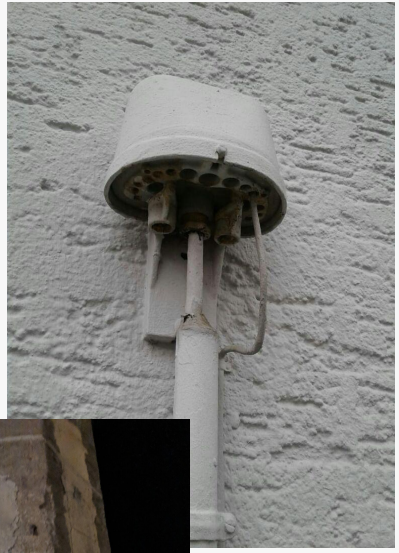
- DSL environments still offer various research potential
  - Carry on testing routers
  - Optimize tools
  - See how far one can go while staying passive / non-disruptive / legal
- Explore all the possibilities the DSLAM offers
  - Document the control / setup scripts
  - Play with the actual DSL handshake
- The attack vector is key for most issues

Finally, some physical security!

- Attacks are improbable
  - Attackers won’t dig up the cables
  - Attacker won’t break into houses
- They might still have to be considered!
  - Office buildings with bad routing?
  - Blocks of flats?

- Well....and... →





Thanks for your time!

Questions?

P.S.
Full lab documentation / instructions / scripts will be published after Troopers

brian@security-bits.de ~~ www.security-bits.de ~~ @BadgeWizard

Sources

- Serverrack: https://commons.wikimedia.org/wiki/File:Rear_of_rack_at_NERSC_data_center.jpg
- Annex overview: https://en.wikipedia.org/wiki/Asymmetric_digital_subscriber_line#/media/File:ADSL_annex_overview.svg
- Stop sign: https://de.wikipedia.org/wiki/Stoppschild#/media/File:Vienna_Convention_road_sign_B2a.svg
- TR-104 Cover: https://www.broadband-forum.org/technical/download/TR-104.pdf