



SharkFest '19 Europe



Analysing VoIP Protocols

Discover Wireshark's numerous features to troubleshoot VoIP

Rolf Leutert

Leutert NetServices
Switzerland
www.netsniffing.ch

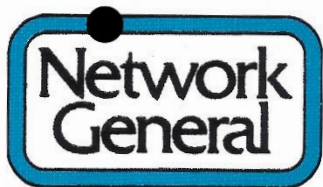


Rolf Leutert, El. Eng. HTL
Leutert NetServices
Zürich-Airport, Switzerland

- Network Analysis & Troubleshooting
- Protocol Trainings TCP/IP, WLAN, VoIP, IPv6
- Wireshark® Certified Network Analyst 2010
- Wireshark® Instructor since 2006
- Sniffer® certified Instructor since 1990

leutert@netsniffing.ch
www.netsniffing.ch





Sniffer[®] has been registered as trademark in 1989

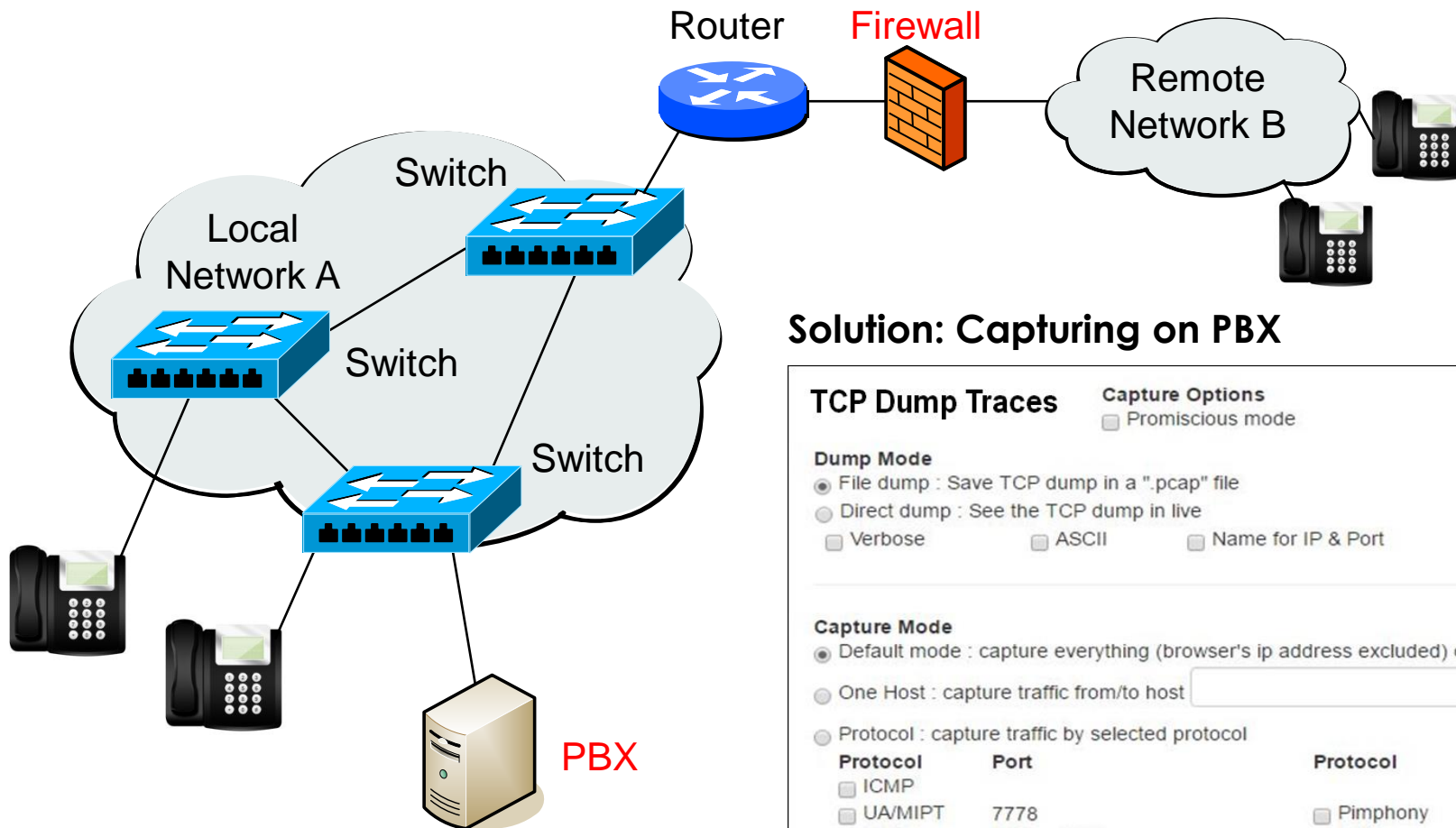


- First **Network General Sniffer** in Switzerland
- Bought 1988 by Swissair airline to analyse **Token-Ring**
- Compaq Portable, DOS Version 1.30 / 256 KByte Capture Buffer
- Price US \$ 30'000 (and more for each decoder)
- No trainings available (Sniffer University started in 1997)



- ▀ Where to capture VoIP traffic
- ▀ Analysing SIP signalling
- ▀ Use Case: Call interrupted after 32 seconds
- ▀ Analysing HFA and UA signalling
- ▀ Analysing SDP negotiation
- ▀ Use Case: Bad VoIP port negotiation
- ▀ Analysing RTP traffic
- ▀ RTP QOS, Delay, Jitter & Packet Loss
- ▀ RTP protocol forcing





Solution: Capturing on PBX



TCP Dump Traces Capture Options

Promiscuous mode

Dump Mode

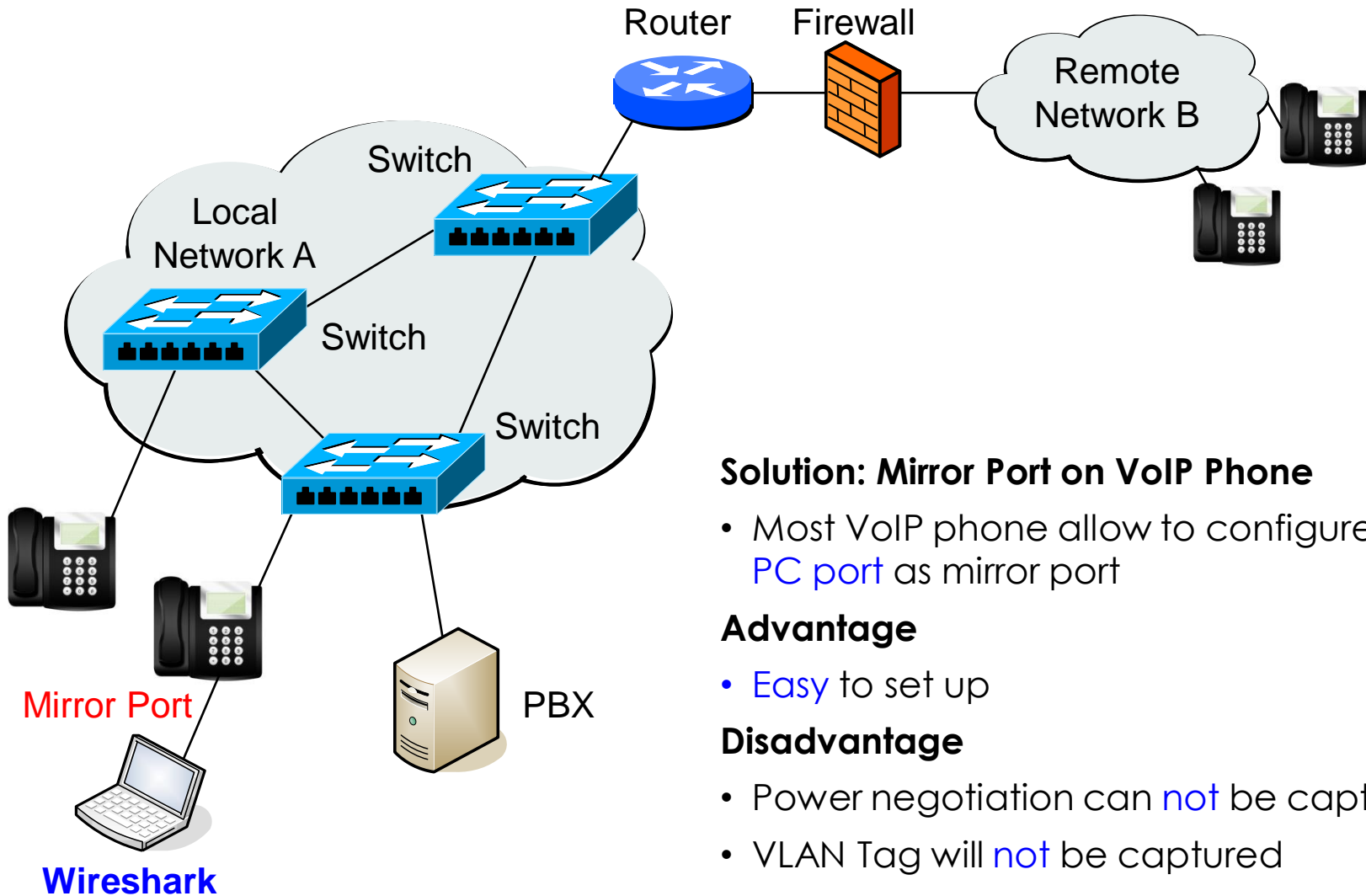
- File dump : Save TCP dump in a ".pcap" file
- Direct dump : See the TCP dump in live
- Verbose ASCII Name for IP & Port

Capture Mode

- Default mode : capture everything (browser's ip address excluded) on eth0
- One Host : capture traffic from/to host on eth0
- Protocol : capture traffic by selected protocol

Protocol	Port	Protocol	Port
<input type="checkbox"/> ICMP		<input type="checkbox"/> Pimphony	7779
<input type="checkbox"/> UA/MIPT	7778	<input type="checkbox"/> DNS	
<input type="checkbox"/> H323	1719 - 1720	<input type="checkbox"/> VoipDebug	7123
<input type="checkbox"/> SIP	5059 - 5060 - 5080		
<input type="checkbox"/> UDP-TCP	<input type="text"/>		

No Capture is running



Solution: Mirror Port on VoIP Phone

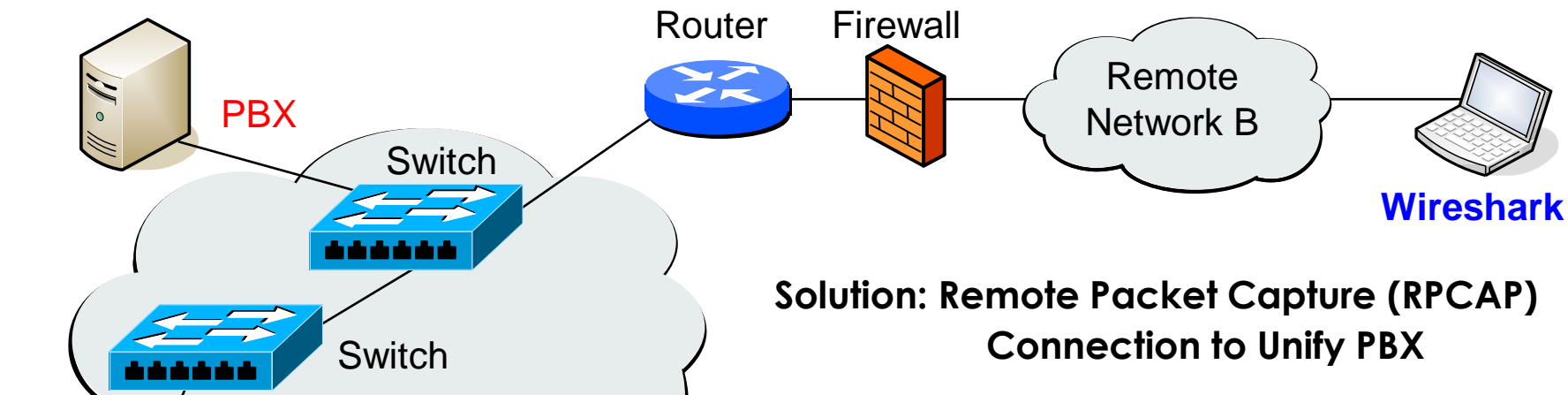
- Most VoIP phone allow to configure the **PC port** as mirror port

Advantage

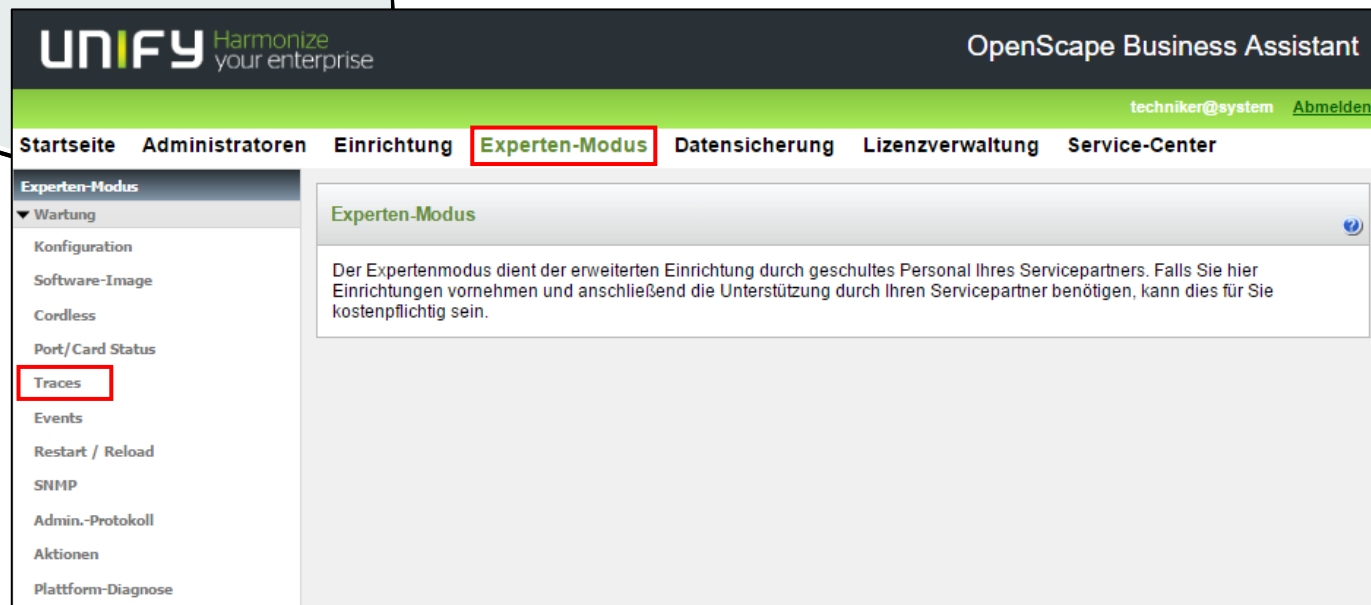
- **Easy** to set up

Disadvantage

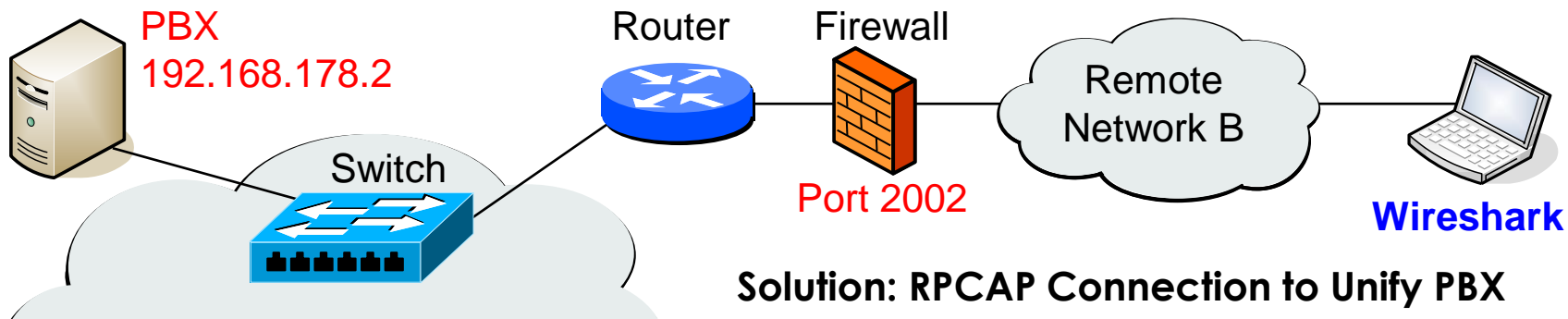
- Power negotiation can **not** be captured
- VLAN Tag will **not** be captured



**Solution: Remote Packet Capture (RPCAP)
Connection to Unify PBX**



Screenshot: Unify PBX



Solution: RPCAP Connection to Unify PBX

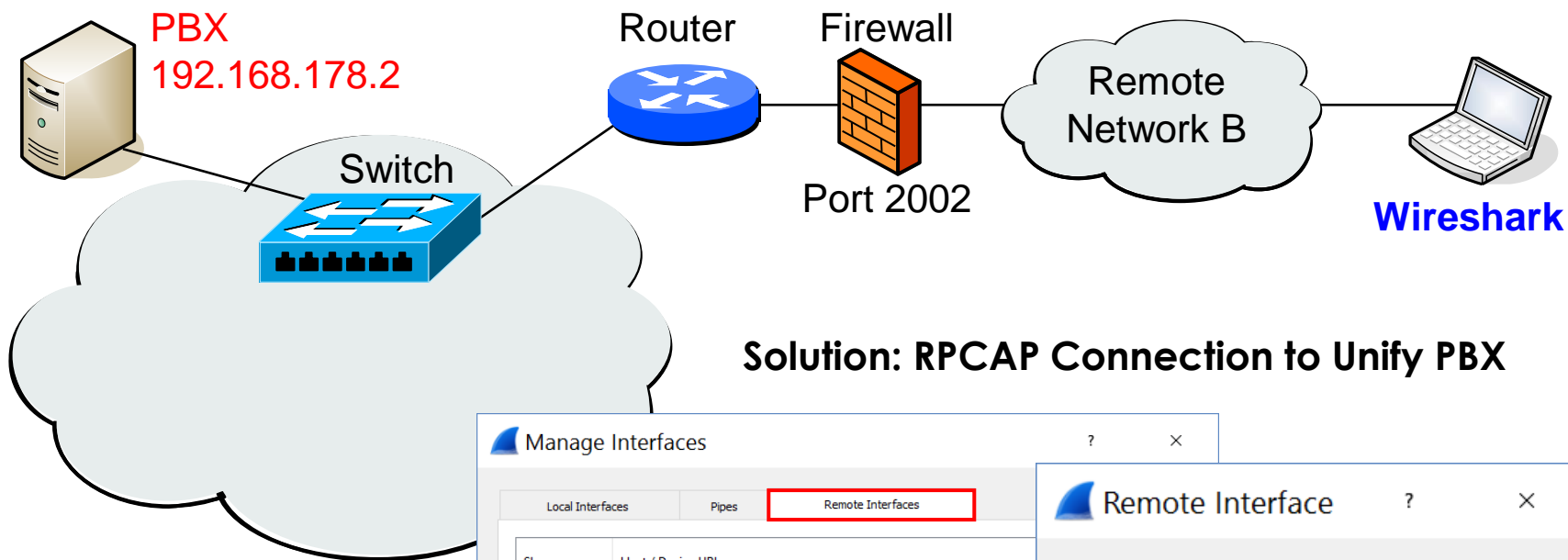
The screenshot shows the 'Experten-Modus - Wartung' (Expert Mode - Maintenance) interface. On the left is a navigation tree with 'rpcap Dämon' selected and highlighted in green. The main area displays the 'rpcap' configuration window. It includes the following fields and options:

- Adresse, an die gebunden werden soll** (Address to be bound to):
 - IP-Adresse (numerisch oder literal): 192.168.178.2 *
 - Port (bitte einen unbelegten Port auswählen): 2002
 - Internes LAN tracen:
- Client-Identifikation für Zugriffskontrolle** (Client identification for access control):
 - IP-Adresse (numerisch oder literal): 192.168.178.202 *

Below the configuration fields, there are two red notes:

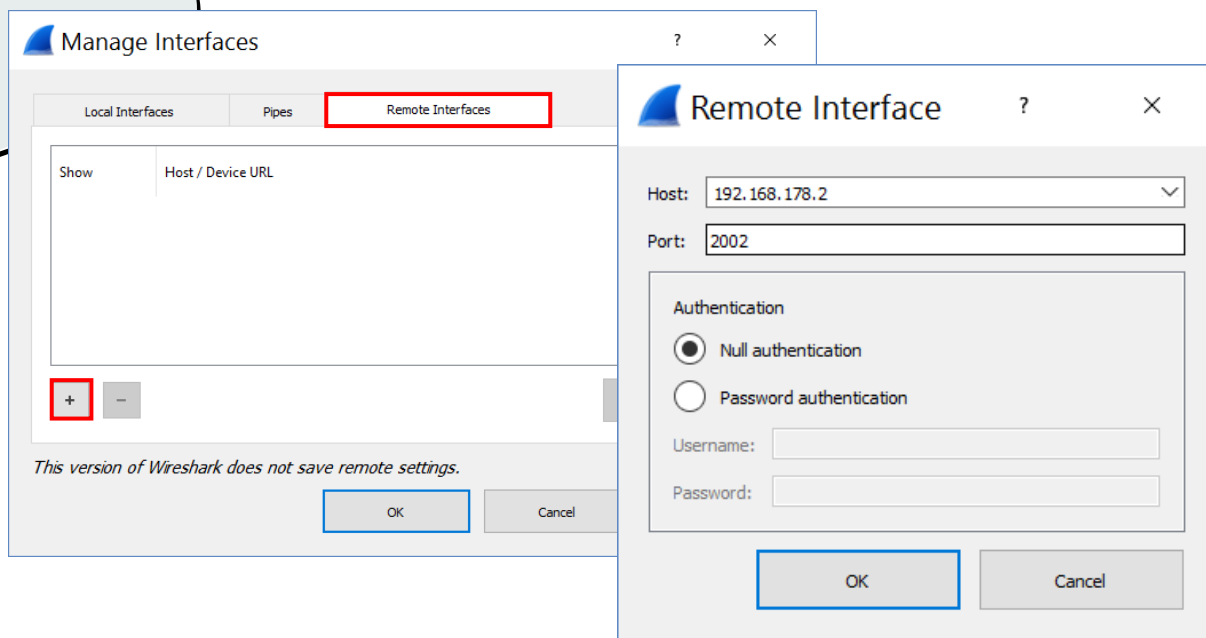
- *) 0.0.0.0 bindet an alle lokalen IPv4 Adressen (PBX)
- *) 0.0.0.0 erlaubt allen Clients Zugriff (Wireshark)

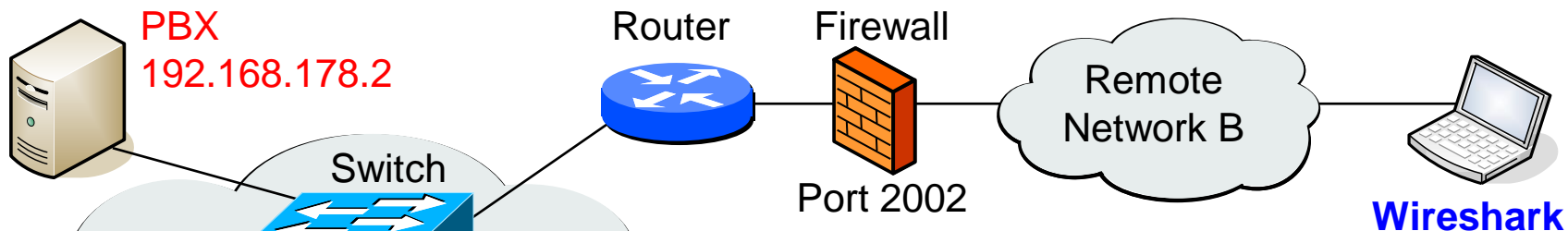
At the bottom, a red text block states: 'Diese Aktion startet den rpcap Dämonen und öffnet einen Server-Port, was einen direkten Remote-Zugriff auf TCP-, ICMP- und UDP-Pakete der LAN-Interfaces von Applikationen wie z.B. Wireshark aus'. At the very bottom are three buttons: 'Übernehmen', 'Rückgängig', and 'Hilfe'.



Solution: RPCAP Connection to Unify PBX

- Wireshark:
- Capture Options
 - Manage Interfaces
 - Remote Interfaces
 - Add Interface with +





Solution: RPCAP Connection to Unify PBX

Experten-Modus - Wartung

Traces

- Trace-Format-Konfiguration
- Trace-Ausgabe-Interfaces
- Trace-Protokoll
- Digitale Prüfschleife
- Kunden-Trace-Protokoll
- MST-Trace-Komponenten
- Secure Trace
- Call Monitoring
- Lizenzkomponente
- Trace-Profil
- Trace-Komponenten
- TCP-Dump
- rpcap Dämon

rpcap

```

eth1  Link encap:Ethernet  Hwaddr 00:1a:e8:74:52:6c
      UP BROADCAST MULTICAST  MTU:1500  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
      Base address:0x2000

eth2  Link encap:Ethernet  Hwaddr 00:1a:e8:74:52:6b
      inet addr:192.168.178.2  Bcast:192.168.178.255  Mask:255.255.255.0
      inet6 addr: fe80::21a:e8ff:fe74:526b/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:41887 errors:0 dropped:1415 overruns:0 frame:0
      TX packets:53322 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:7923386 (7.5 MiB)  TX bytes:8972975 (8.5 MiB)
      Base address:0xc000

eth3  Link encap:Ethernet  Hwaddr 00:1a:e8:01:25:07
      inet addr:192.168.3.1  Bcast:192.168.3.255  Mask:255.255.255.0
      inet6 addr: fe80::21a:e8ff:fe01:2507/64 Scope:Link
  
```

Manage Interfaces

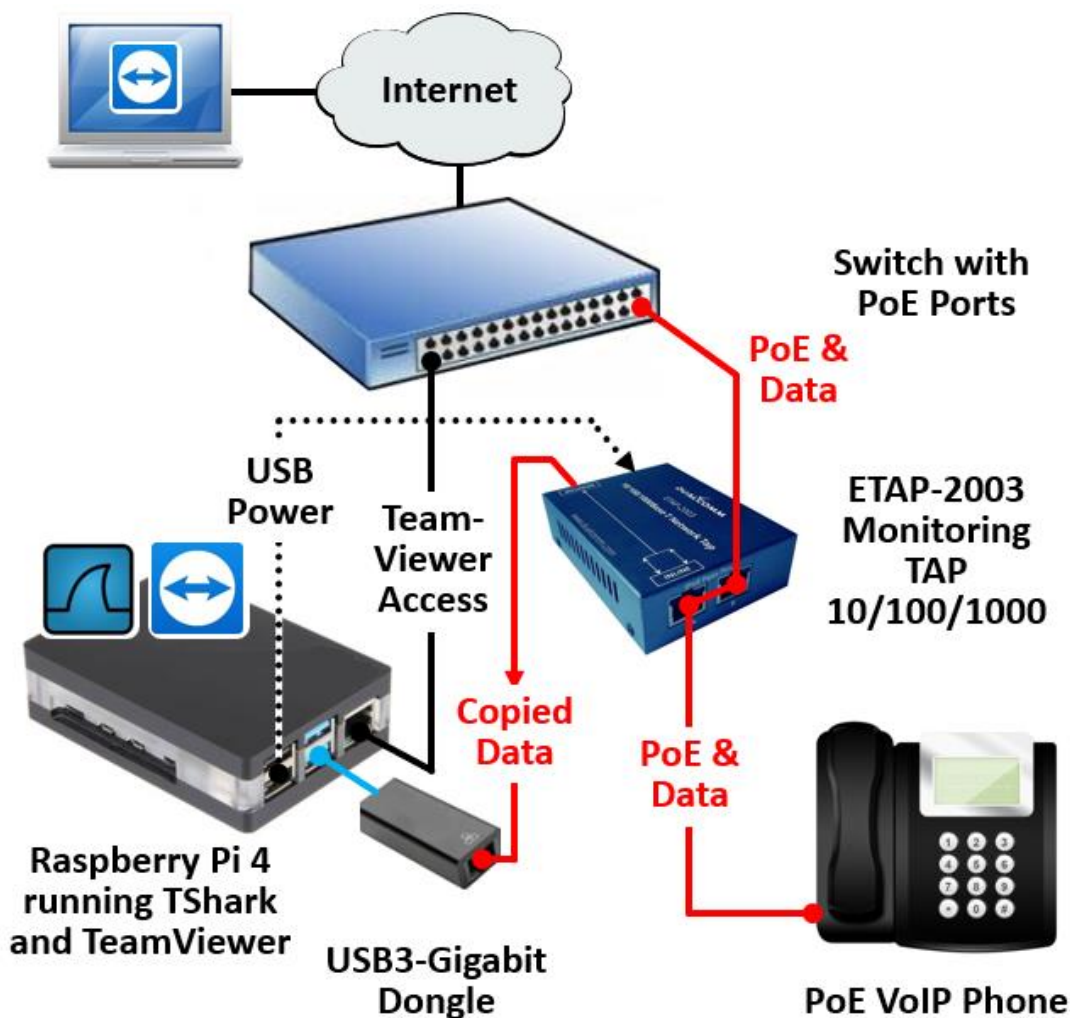
Local Interfaces | Pipes | Remote Interfaces

Show	Host / Device URL
✓	192.168.178.2
<input checked="" type="checkbox"/>	rpcap://[192.168.178.2]:2002/eth1
<input checked="" type="checkbox"/>	rpcap://[192.168.178.2]:2002/eth2
<input checked="" type="checkbox"/>	rpcap://[192.168.178.2]:2002/eth3
<input checked="" type="checkbox"/>	rpcap://[192.168.178.2]:2002/lo

+ - Remote Settings

This version of Wireshark does not save remote settings.

OK Cancel Help



Inexpensive solution for remote capturing with Raspberry Pi 4

- Raspberry with **two** Ethernet interfaces: one for capturing, one for TeamViewer access

Advantage

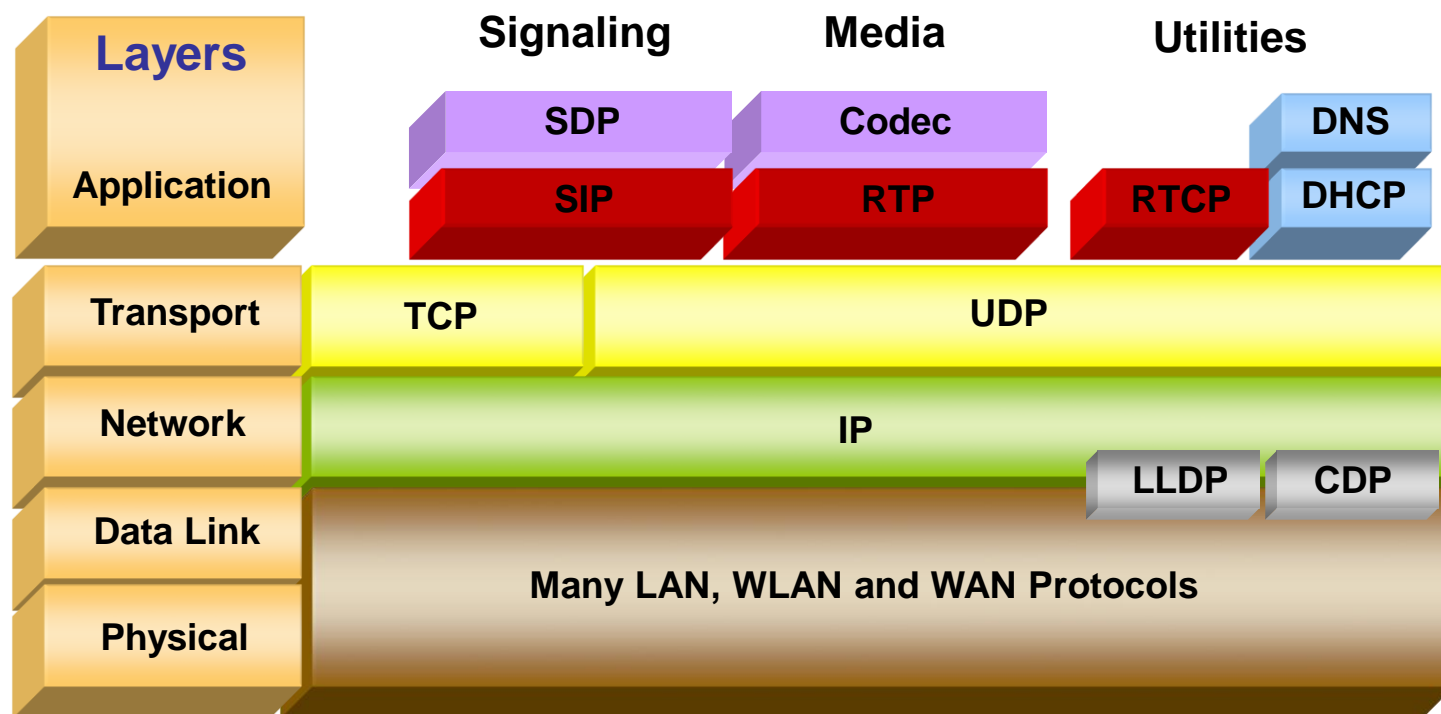
- Allows **remote configuration**
- Allows **long term capturing**
- Can be installed at multiple customer sites
- Using **TShark** to preserve CPU

Disadvantage

- Raspberry performance is limited, solution is **not suitable** to capture server traffic
- Requires **internet connection** for TeamViewer access.



- **SIP** Session Initiation Protocol, create, modify, terminate sessions
- **SDP** Session Description Protocol, describing multimedia sessions
- **RTP** Real-Time Transport Protocol, audio and video packet format
- **RTCP** Real-Time Control Protocol, quality of reception data feedback
- **Codec** Analog/digital encodings; G.711, G.729, μ -Law, A-Law, AMR etc.





SIP basic Requests (called methods):

- **REGISTER** - Registers the address listed in the To header field with a SIP server
- **INVITE** - Indicates a client is being invited to participate in a call session
- **ACK** - Confirms that the client has received a final response to an INVITE request
- **BYE** - Terminates a call and can be sent by either the caller or the called
- **CANCEL** - Cancels any pending request but does not terminate a call
- **OPTIONS** - Queries the capabilities of servers
- **PRACK** - Provisional acknowledgement
- **SUBSCRIBE** - User wishes to receive information about the status of a service session
- **NOTIFY** - Status of the service session for which the Requestor has subscribed
- **PUBLISH** - Publishes an event to the Server
- **INFO** - Sends mid-session information that does not modify the session state
- **REFER** - Asks recipient to issue SIP request (call transfer)
- **MESSAGE** - Transports instant messages using SIP
- **UPDATE** - Modifies the state of a session without changing the state of the dialog

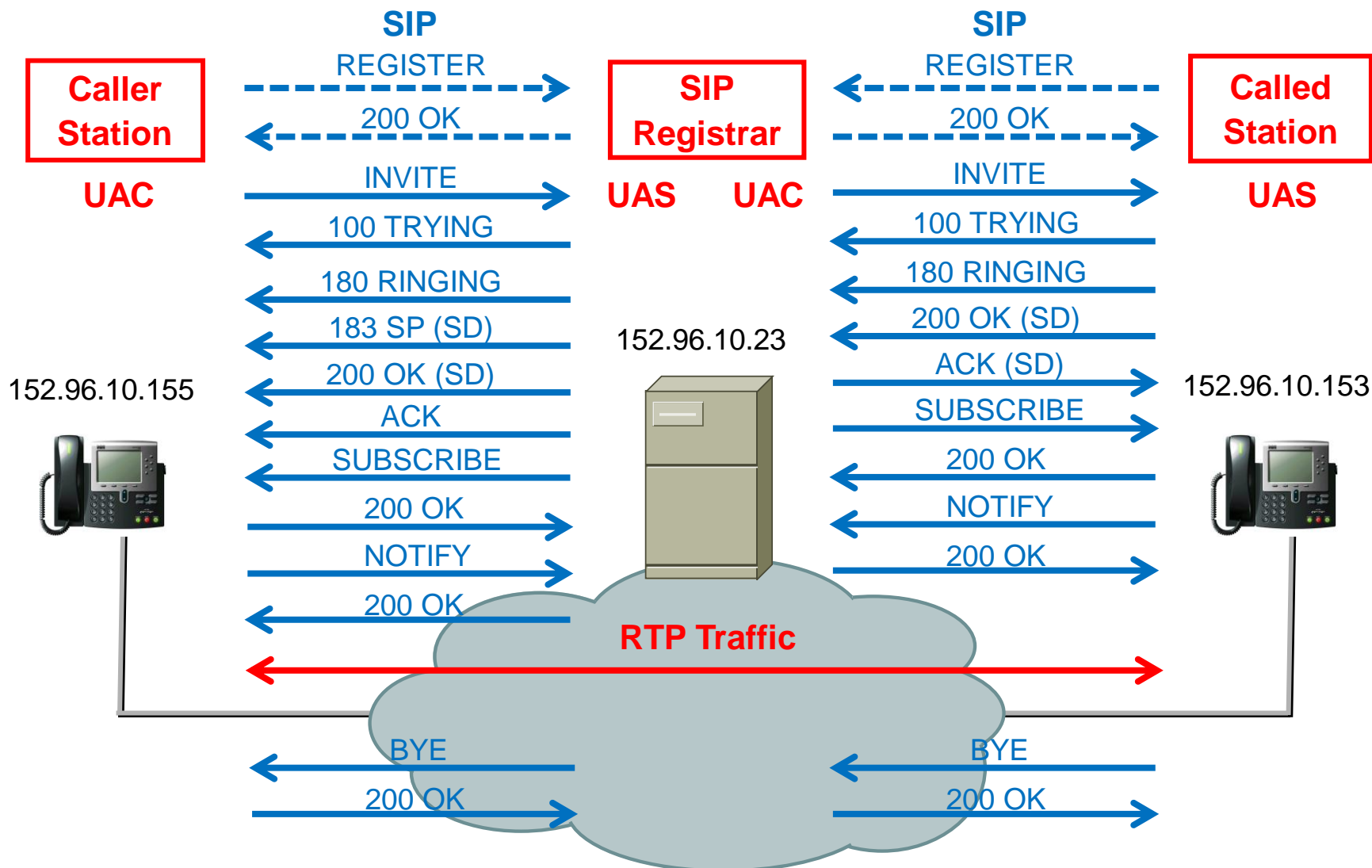


SIP basic **Response** codes:

	Description	Examples
1xx	Informational – Request received, continuing to process request.	100 Trying 180 Ringing 181 Call is Being Forwarded
2xx	Success – Action was successfully received, understood and accepted.	200 OK
3xx	Redirection – Further action needs to be taken in order to complete the request.	300 Multiple Choices 301 Moved Permanently 302 Moved Temporarily
4xx	Client Error – Request contains bad syntax or cannot be fulfilled at this server.	401 Unauthorized 406 Not Acceptable 407 Proxy Authentication Required 408 Request Timeout 415 Unsupported Media type
5xx	Server Error – Server failed to fulfill an apparently valid request.	502 Bad Gateway 503 Service Unavailable 505 Version Not Supported
6xx	Global Failure – Request is invalid at any server.	600 Busy Everywhere 603 Decline



Basic SIP Call Flows:





Graphical presentation of SIP calls:

The screenshot shows the Wireshark interface for analyzing SIP call data. The main window displays a list of packets with the following columns: No., Time, Source, Protocol, Length, Method, DSCP, and Info. The 'Telephony' menu is open, showing options like ANSI, GSM, IAX2 Stream Analysis, ISUP Messages, LTE, MTP3, RTP, RTSP, SCTP, SMPP Operations, UCP Messages, and H.225. A secondary window titled 'Wireshark · VoIP Calls · SIP Call 01' displays a table with the following data:

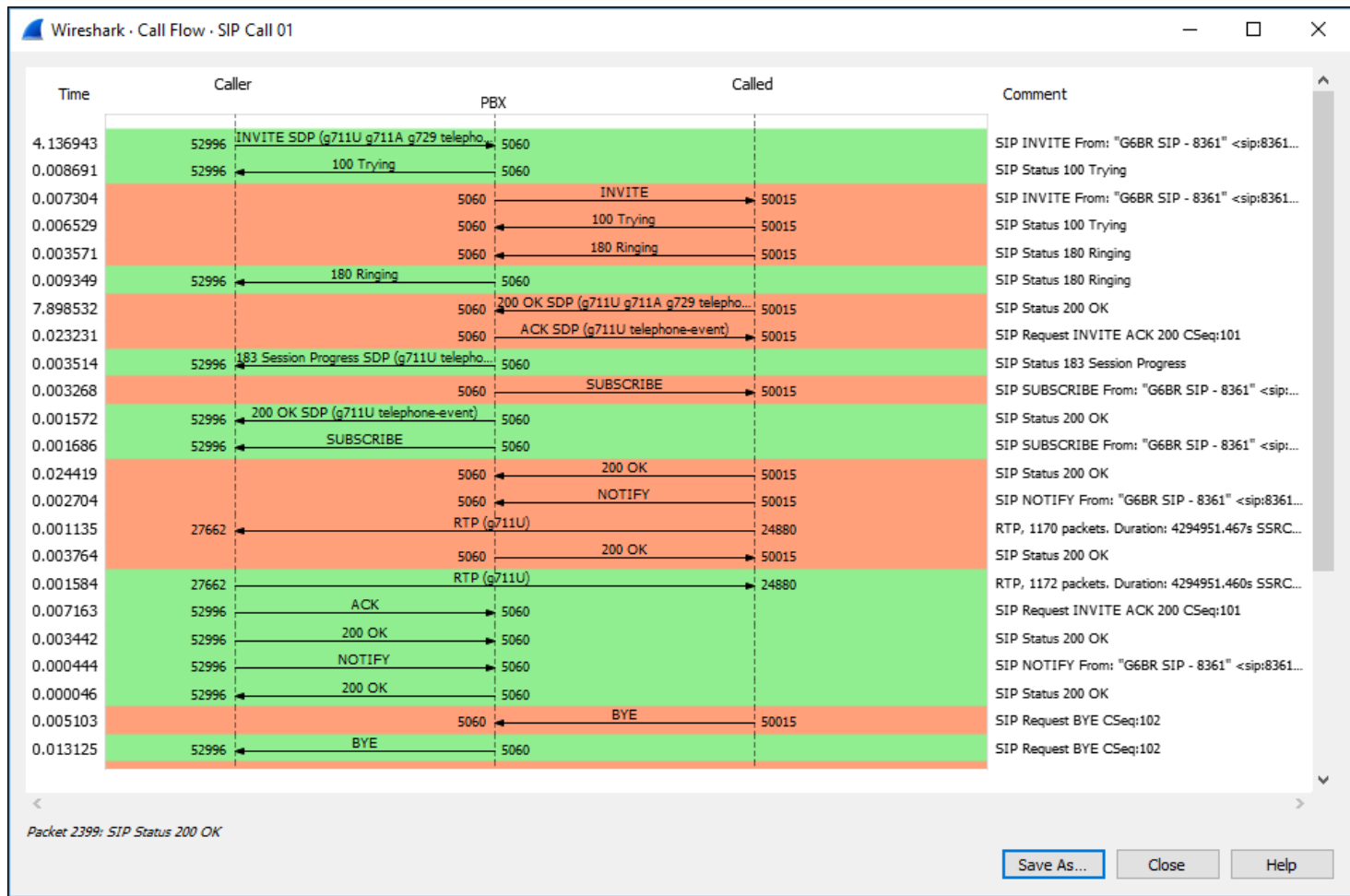
Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State	Comments
5.825598	39.307252	Caller	"G6BR SIP - 8361" <sip:8361@152.96.10.23>	<sip:8@152.96.10.23;user=phone	SIP	16	COMPLETED	INVITE 200
7.758808	39.297150	PBX	"G6BR SIP - 8361" <sip:8361@152.96.10.23>	<sip:20d21236-c361-8382-a931-08ff24061eef@152.96.10.153	SIP	15	COMPLETED	INVITE 200

1. Mark both Calls with Shift + Right Mouse

2. Select Flow Sequence



Graphical presentation of SIP calls:



- Clicking on an arrow line jumps to the appropriate packet in the Packet List



Adding several columns for SIP analysis:

The screenshot shows the Wireshark interface for a capture file named 'SIP Call 01.pcap'. The packet list pane is filtered to show SIP packets. The columns 'Method', 'Sequence Number', 'DSCP', and 'Call-ID' are highlighted with red boxes, indicating they have been added for analysis. The packet details pane shows the structure of an INVITE message, with the 'Request-Line' and 'Message Header' fields also highlighted with red boxes.

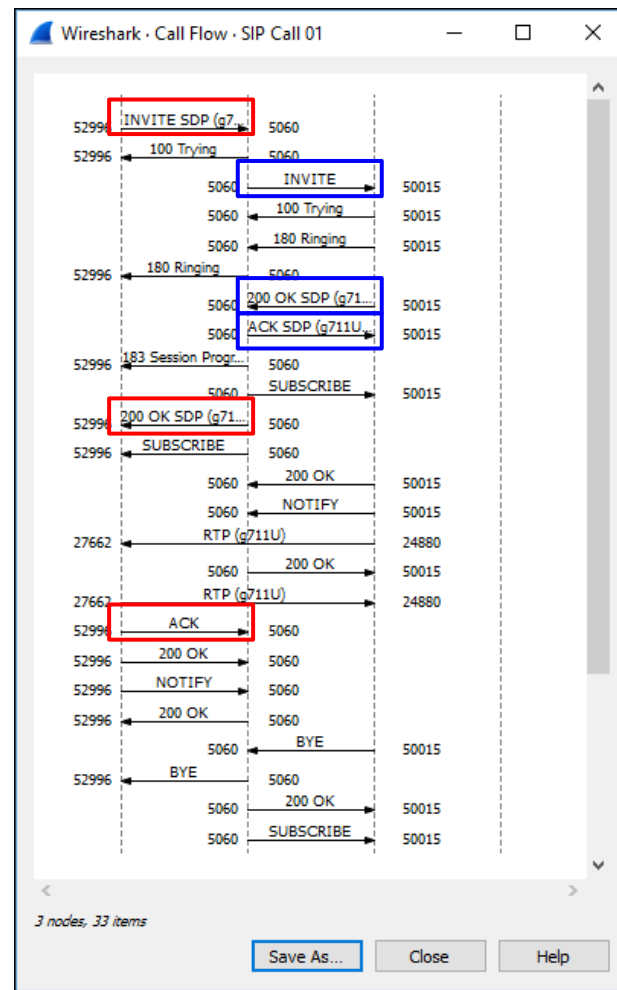
Source	Destination	Protocol	Length	Method	Sequence Number	DSCP	Info	Call-ID
Caller	PBX	SIP	1113	NOTIFY	1006	24	Request: NOTIFY sip:...	d62d700-5f11878f-
PBX	Caller	SIP	406		1006	24	Status: 200 OK	d62d700-5f11878f-
Caller	PBX	SIP/SDP	1163	INVITE	101	24	Request: INVITE sip:...	0015fae9-84940008
PBX	Caller	SIP	419		101	24	Status: 100 Trying	0015fae9-84940008
PBX	Caller	SIP	937	SUBSCRIBE	101	24	Request: SUBSCRIBE s...	2ad3f80-5f119844-
Caller	PBX	SIP	487		101	24	Status: 200 OK	2ad3f80-5f119844-
Caller	PBX	SIP	624	NOTIFY	1006	24	Request: NOTIFY sip:...	2ad3f80-5f119844-

Frame 5: 1163 bytes on wire (9304 bits), 1163 bytes captured (9304 bits)
Ethernet II, Src: Caller (00:15:fa:e9:84:94), Dst: CiscoInc_ef:af:93 (00:0d:bc:ef:af:93)
Internet Protocol Version 4, Src: Caller (152.96.10.155), Dst: PBX (152.96.10.23)
Transmission Control Protocol, Src Port: 52996 (52996), Dst Port: 5060 (5060), Seq: 1060, ...
Session Initiation Protocol (INVITE)
Request-Line: INVITE sip:8@152.96.10.23;user=phone SIP/2.0
Message Header
Message Body



SIP special message ACK:

- **SIP ACK** (Acknowledge) is an exception to the SIP Request and Response rules
- **SIP ACK** is a **Request without a Response**
- **SIP ACK** is sent as a **Confirmation** to a successfully established **Invite** transaction.
- **SIP ACK** Message is carrying the same sequence number and call-id as the invite transaction.
- **SIP ACK** is not confirmed with a response





Use Case: Call interrupted after 32 seconds

Call_interrupted_after_32sec.pcapng

File Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe

Anzeigefilter anwenden ... <Ctrl-/> Ausdrucken... + SIP RTP SIP or RTP

No.	Time	Delta Time	Source	Destination	Time to live	Protocol	Length	Sequence Number	Method	Info
1	0.000000	0.000000	Provider	PBX	55	SIP/SDP	980	1	INVITE	Request: INVITE sip:+4936824520@176.94.60.34:5060
2	0.000148	0.000148	PBX	Provider	64	TCP	66			5060 → 48380 [ACK] Seq=1 Ack=915 Win=1272 Len=0
3	0.180673	0.180525	PBX	Provider	64	SIP	669	1		Status: 180 Ringing
4	0.290555	0.109882	Provider	PBX	55	TCP	66			5060 → 33195 [ACK] Seq=1 Ack=604 Win=32768 Len=0
5	4.064327	3.773772	PBX	Provider	64	SIP/SDP	996	1		Status: 200 OK
6	4.130327	0.066000	Provider	PBX	240	RTP	214			PT=ITU-T G.711 PCMA, SSRC=0x21C0148D, Seq=0, Len=188
7	4.133857	0.003530	PBX	Provider	64	RTP	214			PT=ITU-T G.711 PCMA, SSRC=0xBF576815, Seq=0, Len=188
8	4.150407	0.016550	Provider	PBX	240	RTP	214			PT=ITU-T G.711 PCMA, SSRC=0x21C0148D, Seq=1, Len=188
9	4.153869	0.003462	PBX	Provider	64	RTP	214			PT=ITU-T G.711 PCMA, SSRC=0xBF576815, Seq=1, Len=188
10	4.170393	0.016524	Provider	PBX	240	RTP	214			PT=ITU-T G.711 PCMA, SSRC=0x21C0148D, Seq=2, Len=188
11	4.173851	0.003458	PBX	Provider	64	RTP	214			PT=ITU-T G.711 PCMA, SSRC=0xBF576815, Seq=2, Len=188
12	4.174582	0.000731	Provider	PBX	55	TCP	66			5060 → 33195 [ACK] Seq=1 Ack=1534 Win=32768 Len=0
13	4.190680	0.016098	Provider	PBX	240	RTP	214			PT=ITU-T G.711 PCMA, SSRC=0x21C0148D, Seq=3, Len=188
14	4.193893	0.003213	PBX	Provider	64	RTP	214			PT=ITU-T G.711 PCMA, SSRC=0xBF576815, Seq=3, Len=188
15	4.210558	0.016665	Provider	PBX	240	RTP	214			PT=ITU-T G.711 PCMA, SSRC=0x21C0148D, Seq=4, Len=188
16	4.213882	0.003324	PBX	Provider	64	RTP	214			PT=ITU-T G.711 PCMA, SSRC=0xBF576815, Seq=4, Len=188
17	4.230293	0.016411	Provider	PBX	240	RTP	214			PT=ITU-T G.711 PCMA, SSRC=0x21C0148D, Seq=5, Len=188
18	4.233838	0.003545	PBX	Provider	64	RTP	214			PT=ITU-T G.711 PCMA, SSRC=0xBF576815, Seq=5, Len=188

> Frame 1: 980 bytes on wire (7840 bits), 980 bytes captured (7840 bits) on interface 0

> Ethernet II, Src: Sophos_4c:50:f0 (7c:5a:1c:4c:50:f0), Dst: UnifySof_89:b8:0b (00:1a:e8:89:b8:0b)

> Internet Protocol Version 4, Src: Provider (176.95.49.1), Dst: PBX (192.168.70.100)

> Transmission Control Protocol, Src Port: 48380, Dst Port: 5060, Seq: 1, Ack: 1, Len: 914

> Session Initiation Protocol (INVITE)

Call_interrupted_after_32sec.pcapng | Pakete: 3234 · Angezeigt: 3234 (100.0%) | Profil: LNS SIP



- HFA (CorNet-IP) is TCP based and used for signaling in pure **HiPath** environment
- HFA can be decoded only by installing an additional **Plug-In** for Wireshark

Unify Startup static and call.pcapng

No.	Time	Source	Destination	Protocol	Length	Info
1940	57.985789	Phone	PBX	TCP	209	1415 → 4060 [PSH, ACK] Seq=33333333
1941	57.986133	PBX	Phone	TCP	66	4060 → 1415 [ACK] Seq=33333333
1942	57.988294	PBX	Phone	TCP	91	4060 → 1415 [PSH, ACK] Seq=33333333
1943	57.988319	Phone	PBX	TCP	66	1415 → 4060 [ACK] Seq=18000000

Frame 1940: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on interface 0
 Ethernet II, Src: Phone (00:1a:e8:9d:4b:d0), Dst: PBX (00:1a:e8:5f:0c:e1)
 Internet Protocol Version 4, Src: Phone (172.22.3.63), Dst: PBX (172.22.3.120)
 Transmission Control Protocol, Src Port: 1415, Dst Port: 4060, Seq: 43, Ack: 33, Len: 143
 Data (143 bytes)

0040 14 77 00 8f 00 0a 00 ff ff 00 00 ff 04 72 00 07 ..w.....r...
 0050 91 2a 2a 38 31 32 35 09 00 01 06 0e 00 50 00 00 ...**8125...P..

Decode **without**
HFA Plug-In

Unify Startup static and call.pcapng

No.	Time	Source	Destination	Protocol	Length	Info
1940	57.985789	Phone	PBX	HFA	209	Register **8125
1942	57.988294	PBX	Phone	HFA	91	Register Response
1968	58.531109	Phone	PBX	HFA	170	Codec Capabilities
1983	59.097182	Phone	PBX	HFA	92	Phone Initialization Request

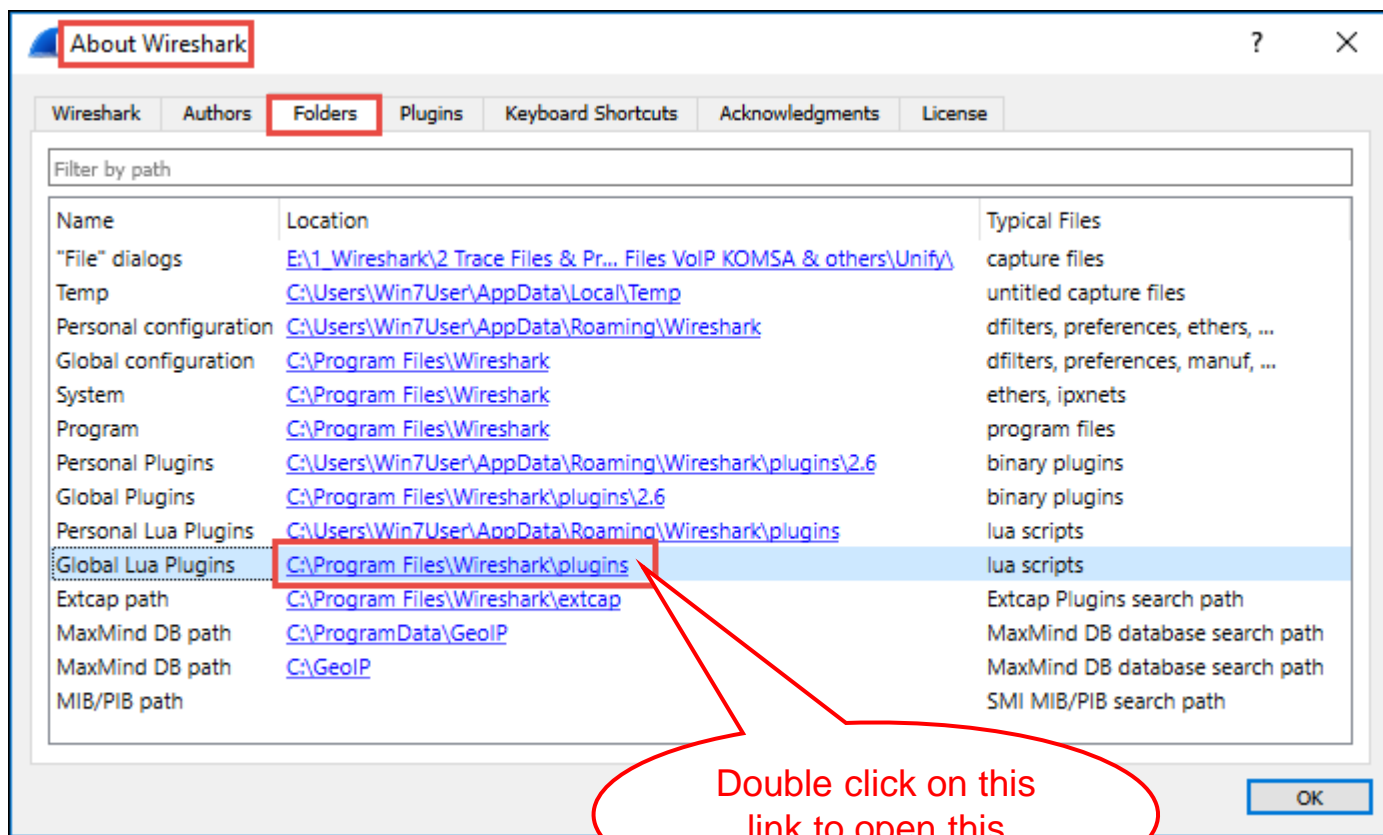
Frame 1940: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on interface 0
 Ethernet II, Src: Phone (00:1a:e8:9d:4b:d0), Dst: PBX (00:1a:e8:5f:0c:e1)
 Internet Protocol Version 4, Src: Phone (172.22.3.63), Dst: PBX (172.22.3.120)
 Transmission Control Protocol, Src Port: 1415, Dst Port: 4060, Seq: 43, Ack: 33, Len: 143
 HFA
 Message Length: 143
 Message Type: 0x04 (Register)
 Information Element: 0x72 (Subscriber Number)
 Length: 7
 Type of Number: E.164 International, ISDN/telephony numbering plan (0x91)
 Subscriber Number: **8125
 Information Element: 0x09
 Length: 1
 [Expert Info (Warning/Undecoded): Unknown Item Type]
 [Unknown Item Type]
 [Severity level: Warning]
 [Group: Undecoded]
 Information Element: 0x0e (Registration Data)
 Length: 80
 Timestamp: Mar 1, 2018 09:09:33.000000000 Mitteleuropäische Zeit
 Password Hash: 861849835e43d75e805dff2a5806dc349ebee705
 Client Version: HLB_V2.01 3 14 3 2 26
 Information Element: 0x01 (Device IP-Address)
 Length: 12
 IP-Address: 172.22.3.63
 Information Element: 0x7a

0040 14 77 00 8f 00 0a 00 ff ff 00 00 ff 04 72 00 07 ..w.....r...
 0050 91 2a 2a 38 31 32 35 09 00 01 06 0e 00 50 00 00 ...**8125...P..

Decode **with**
HFA Plug-In



- The **HiPath Feature Access (HFA)** is proprietary and not included in Wireshark
- Download **hfa.lua** Plug-In from <https://github.com/jonas-koeritz/hfa-dissector>
- Copy the **hfa.lua** to the Wireshark Plugins folder, close and restart Wireshark





Wireshark decodes the following UA protocols:

- **UAUDP** Universal Alcatel over UDP, **NOE** New Office Environment, **UA3G** and **UASIP**

UA Call432 & Incoming Call.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

uauudp

No.	Time	Source	Destination	Length	Protocol	Sequence No (sent)	Sequence No (expected)	Info
1	1509551125.523	Phone	PBX	56	UAUDP	121	303	Data - NOE Protocol (CS): Notify EVT_KEY_PRES
2	1509551125.523	PBX	Phone	60	UAUDP	303	122	Data ACK
3	1509551125.525	PBX	Phone	325	UAUDP	303	122	Data - UA3G Message: Main Voice Mode: Handsfr
5	1509551125.527	Phone	PBX	56	UAUDP	121	304	Data ACK
8	1509551125.824	Phone	PBX	56	UAUDP	122	304	Data - NOE Protocol (CS): Notify EVT_KEY_PRES
9	1509551125.824	PBX	Phone	60	UAUDP	304	123	Data ACK
10	1509551125.824	PBX	Phone	60	UAUDP	304	123	Data - NOE Protocol (CS): SetProperty TextBox
11	1509551125.825	Phone	PBX	56	UAUDP	122	305	Data ACK
13	1509551126.033	Phone	PBX	56	UAUDP	123	305	Data - NOE Protocol (CS): Notify EVT_KEY_PRES
14	1509551126.034	PBX	Phone	60	UAUDP	305	124	Data ACK
16	1509551126.043	PBX	Phone	60	UAUDP	305	124	Data - NOE Protocol (CS): SetProperty TextBox
17	1509551126.043	Phone	PBX	56	UAUDP	123	306	Data ACK

<

> Frame 1: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0

> Ethernet II, Src: Phone (00:80:9f:b1:44:63), Dst: AlcatelB_bf:ea:ae (00:80:9f:bf:ea:ae)

> Internet Protocol Version 4, Src: Phone (172.28.51.1), Dst: PBX (172.28.10.12)

> User Datagram Protocol, Src Port: 32512, Dst Port: 32640

> Universal Alcatel/UDP Encapsulation Protocol, Data

> Universal Alcatel Protocol, Terminal -> System



Session Description Protocol (SDP) features:

- **SDP** is intended for describing multimedia sessions for the purposes of session announcement, session invitation, and other forms of multimedia session initiation
- **SDP** is used by many protocols to describe media sessions such as SIP, MGCP, RTSP, BICC, H.248/MEGACO
- **SDP** does not deliver media itself but is used for negotiation between end points
- **SDP** contains three main sections, detailing the session, timing, and media descriptions.
- **SDP** is simple and flexible because it is Text-based
- **SDP** describes the session by a series of fields, one per line.



Introduction

SIP Call 01.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

sip.Call-ID == "0015fae9-84940008-4ff1580c-85340a0d@152.96.10.155"

Source	Destination	Protocol	Length	Sequence Number	Info
Caller	PBX	SIP/SDP	1163	101	Request: INVITE sip:8@152.96.10.23;user=ph
PBX	Caller	SIP	419	101	Status: 100 Trying
PBX	Caller	SIP	813	101	Status: 180 Ringing
PBX	Caller	SIP/SDP	1068	101	Status: 183 Session Progress
PBX	Caller	SIP/SDP	1053	101	Status: 200 OK
PBX	Caller	SIP	934	101	Request: SUBSCRIBE sip:b56daa0c-e25d-7a68
Caller	PBX	SIP	630	101	Request: ACK sip:8@152.96.10.23:5060;trans
Caller	PBX	SIP	558	101	Status: 200 OK
Caller	PBX	SIP	692	102	Request: NOTIFY sip:152.96.10.23:5060
PBX	Caller	SIP	441	102	Status: 200 OK
PBX	Caller	SIP	547	102	Request: BYE sip:b56daa0c-e25d-7a68-f5b6-2
Caller	PBX	SIP	450	102	Status: 200 OK
PBX	Caller	SIP	632	103	Request: SUBSCRIBE sip:b56daa0c-e25d-7a68
Caller	PBX	SIP	555	103	Status: 200 OK
Caller	PBX	SIP	1003	103	Request: NOTIFY sip:152.96.10.23:5060
PBX	Caller	SIP	441	103	Status: 200 OK



SDP Variables:

The screenshot shows a Wireshark capture of an SIP INVITE packet. The packet details pane is expanded to show the Session Description Protocol (SDP) body. Two red callouts are present: one pointing to the 'Request-Line' and another pointing to the 'Media Profile Numbers' in the 'Media Description' field. The 'Media Description' field is highlighted with a red box and contains the text 'audio 27662 RTP/AVP 0 8 18 101'. The values 0, 8, 18, and 101 are each enclosed in a colored box (blue, pink, green, and orange respectively). Arrows of the same colors point from these boxes to the corresponding values in the 'Media Attribute' list below. The 'Media Attribute' list includes: 'rtptime:0 PCMU/8000', 'rtptime:8 PCMA/8000', 'rtptime:18 G729/0', 'fmtp:18 annexb=no', 'rtptime:101 telephone-event/8000', and 'fmtp:101 0-15'. The 'Connection Information' field is also highlighted with a red box and contains 'IN IP4 152.96.10.155'.

```
Session Description Protocol (INVITE)
  Request-Line: INVITE sip:8@152.96.10.155
  Message Header
  Message Body
    Session Description Protocol
      Session Description Protocol Version (v): 0
      Owner/Creator, Session Id (o): Cisco-SIPUA 5732 IN IP4 152.96.10.155
      Session Name (s): SIP Call
      Time Description, active time (t): 0 0
      Media Description, name and address (m): audio 27662 RTP/AVP 0 8 18 101
      Connection Information (c): IN IP4 152.96.10.155
      Media Attribute (a): rtptime:0 PCMU/8000
      Media Attribute (a): rtptime:8 PCMA/8000
      Media Attribute (a): rtptime:18 G729/0
      Media Attribute (a): fmtp:18 annexb=no
      Media Attribute (a): rtptime:101 telephone-event/8000
      Media Attribute (a): fmtp:101 0-15
      Media Attribute (a): sendrecv
```



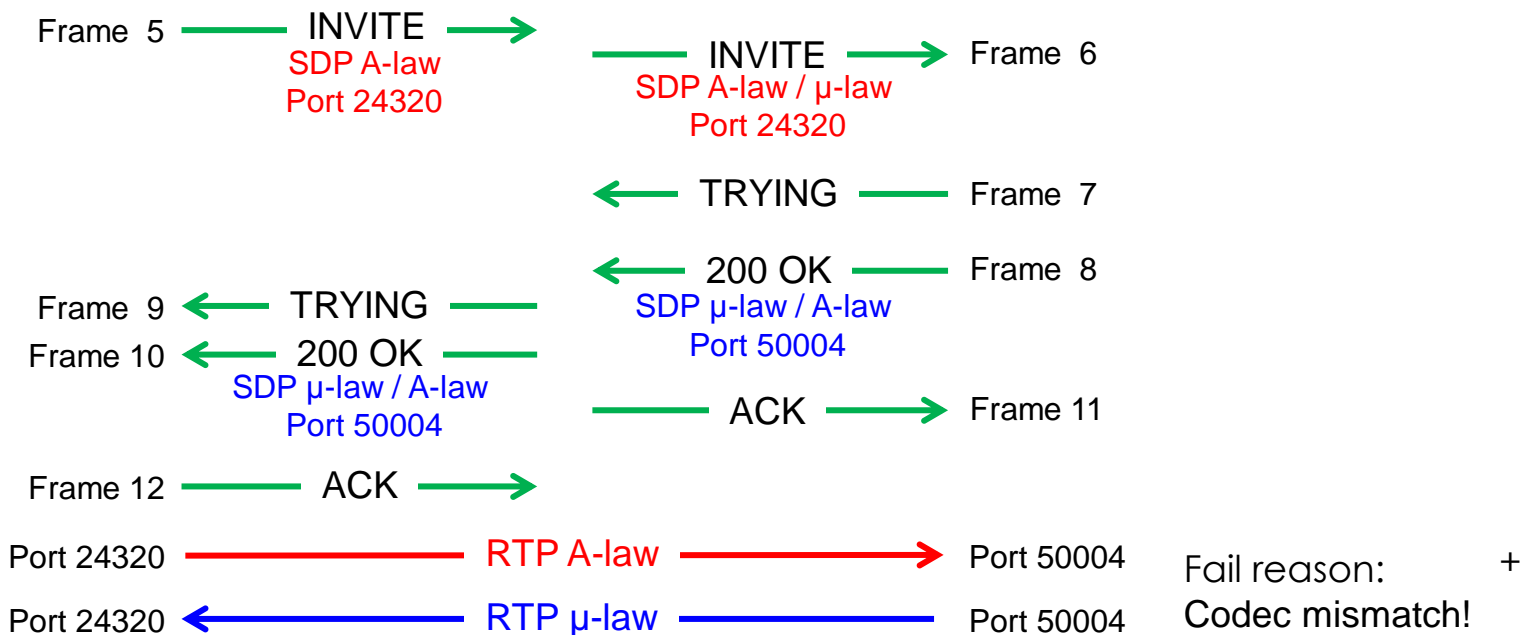
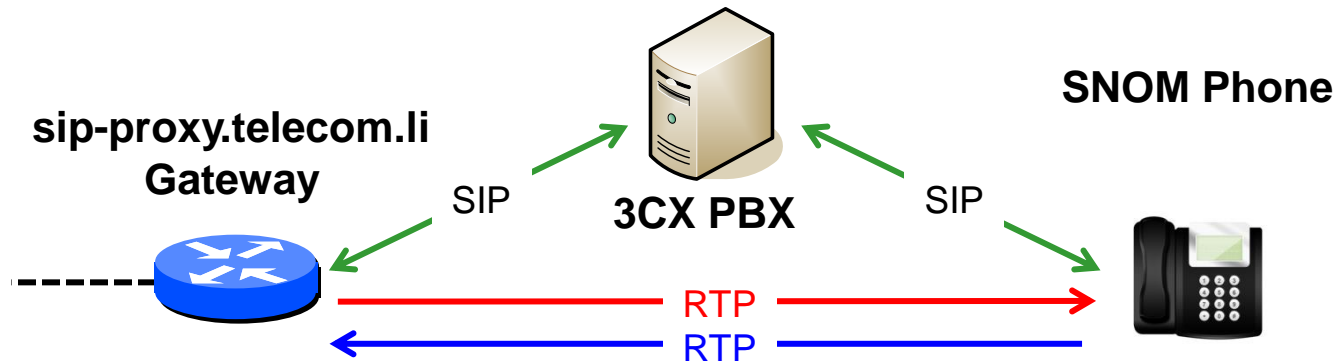
Use Case: Voice channel call be established

No.	Time	Source	Destination	Protocol	Sequence Number	Method	Info
1	0.000000	SNOM Phone	3CX PBX	SIP	99762	REGISTER	Request: REGISTER sip:3cxpbx.com
2	0.100748	3CX PBX	SNOM Phone	SIP	99762		Status: 407 Proxy Authentication Required
3	0.122080	SNOM Phone	3CX PBX	SIP	99763	REGISTER	Request: REGISTER sip:3cxpbx.com
4	0.222033	3CX PBX	SNOM Phone	SIP	99763		Status: 200 OK (2 bytes)
5	5.688349	sip-proxy.telecom.li	3CX PBX	SIP/SDP	2	INVITE	Request: INVITE sip:3cxpbx.com
6	5.692957	3CX PBX	SNOM Phone	SIP/SDP	2	INVITE	Request: INVITE sip:3cxpbx.com
7	5.715344	SNOM Phone	3CX PBX	SIP	2		Status: 100 Trying
8	5.746859	SNOM Phone	3CX PBX	SIP/SDP	2		Status: 200 OK
9	5.767967	3CX PBX	sip-proxy.telecom.li	SIP	2		Status: 100 Trying
10	5.767973	3CX PBX	sip-proxy.telecom.li	SIP/SDP	2		Status: 200 OK
11	5.768013	3CX PBX	SNOM Phone	SIP	2	ACK	Request: ACK sip:523
12	5.790120	sip-proxy.telecom.li	3CX PBX	SIP	2	ACK	Request: ACK sip:004
13	5.802239	sip-proxy.telecom.li	SNOM Phone	RTP			PT=ITU-T G.711 PCMA
14	5.804689	SNOM Phone	sip-proxy.telecom.li	RTP			PT=ITU-T G.711 PCMU
15	5.821539	sip-proxv.telecom.li	SNOM Phone	RTP			PT=ITU-T G.711 PCMA

> Frame 1: 609 bytes on wire (4872 bits), 609 bytes captured (4872 bits) on interface 0
> Ethernet II, Src: SnomTech_61:4b:6f (00:04:13:61:4b:6f), Dst: Elitegro_14:c5:89 (94:c6:91:14:c5:89)
> Internet Protocol Version 4, Src: SNOM Phone (192.168.1.58), Dst: 3CX PBX (192.168.1.110)
> User Datagram Protocol, Src Port: 5060, Dst Port: 5060
> Session Initiation Protocol (REGISTER)

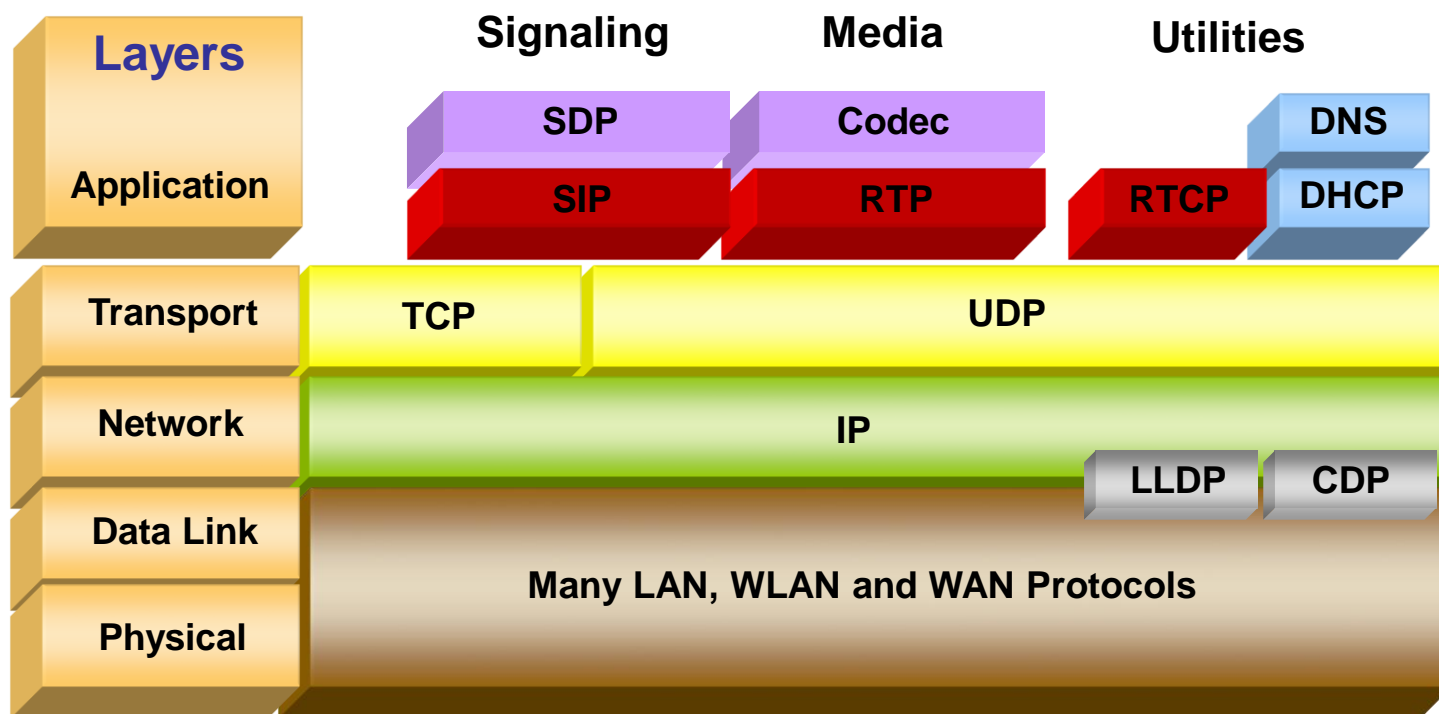


Use Case: Voice channel call be established





- **SIP** Session Initiation Protocol, create, modify, terminate sessions
- **SDP** Session Description Protocol, describing multimedia sessions
- **RTP** Real-Time Transport Protocol, audio and video packet format
- **RTCP** Real-Time Control Protocol, quality of reception data feedback
- **Codec** Analog/digital encodings; G.711, G.729, μ -Law, A-Law, AMR etc.





Real-Time Transport Protocol (RTP) features:

- **RTP** is the carrier protocol for **real-time** applications (Voice, Video etc.)
- **RTP** is using **two streams**, one in each direction and is based on UDP
- **RTP** does **not** address resource reservation and does **not** guarantee quality-of-service
- **RTP** does **not** provide any features to ensure **timely delivery** or mechanism to **avoid jitter**
- **RTP** contains the **codec** used (Payload Type), the **sequence number** (for sequential reassembly), the **timestamp** and the **SSRC**
- **RTP** carries the **Synchronization source identifier SSRC** which uniquely identifies the source of a stream.



Adding QOS column

The screenshot shows the Wireshark interface for a file named 'SIP Call 01.pcap'. The main display area shows a list of RTP packets. A red box highlights the 'DSCP' column, which contains the value '46' for all visible packets. The 'Info' column shows details for each packet, including 'PT=ITU-T G.711 PCMU, SSRC=0'.

No.	Delta Time	Source	Destination	Protocol	Length	DSCP	Info
48	0.001135	152.96.10.153	152.96.10.155	RTP	214	46	PT=ITU-T G.711 PCMU, SSRC=0
51	0.001584	152.96.10.155	152.96.10.153	RTP	214	46	PT=ITU-T G.711 PCMU, SSRC=0
55	0.000559	152.96.10.153	152.96.10.155	RTP	214	46	PT=ITU-T G.711 PCMU, SSRC=0
58	0.003856	152.96.10.155	152.96.10.153	RTP	214	46	PT=ITU-T G.711 PCMU, SSRC=0
61	0.008647	152.96.10.153	152.96.10.155	RTP	214	46	PT=ITU-T G.711 PCMU, SSRC=0
62	0.006640	152.96.10.155	152.96.10.153	RTP	214	46	PT=ITU-T G.711 PCMU, SSRC=0

Below the packet list, the details pane for the selected packet (Frame 48) is shown. A red box highlights the 'Differentiated Services Field' section, which is expanded to show the following details:

- Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
 - 1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
 -00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

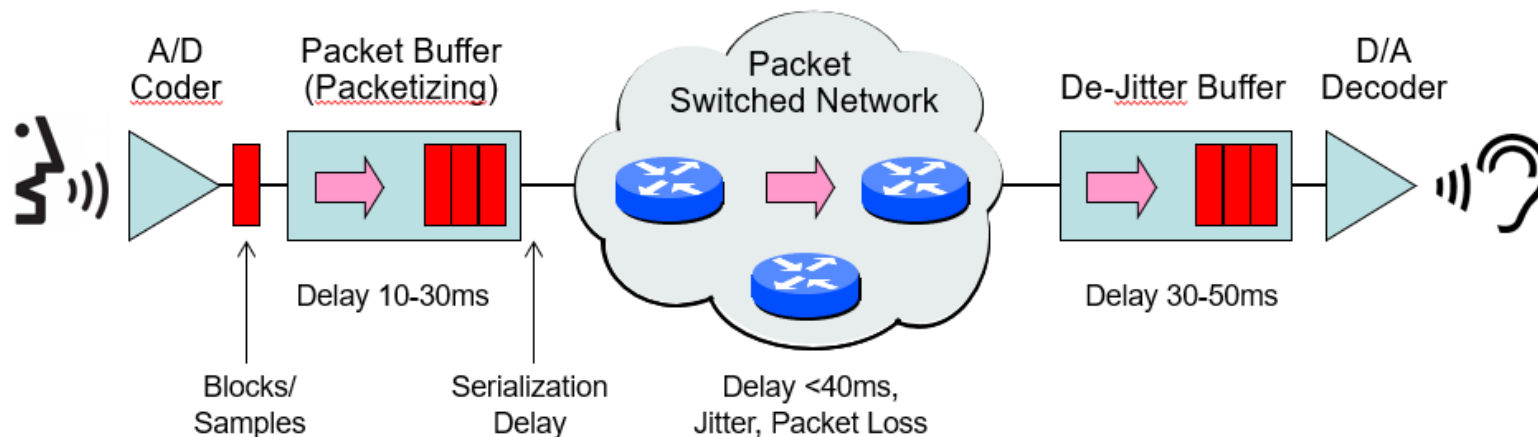
Total Length: 200

DiffServ (Differentiated Services Code Point) Header
 Bits 0-5: DSCP (Differentiated Services Code Point)
 Bits 6-7: ECN (Explicit Congestion Notification - IP Flow Control)



Delay, Jitter & Packet Loss

- **Coder Delay** Caused by the digital signal processor (DSP) to compress a block of digitized voice samples.
- **Packetization Delay** Time taken to fill a packet payload with speech blocks. Also called accumulation delay, dependant of number of blocks loaded in one packet.
- **Serialization Delay** Time required to clock a voice or data frame onto the network interface. It is directly related to the clock rate on the trunk (Bandwidth).
- **Network Delay** Caused by buffers of router and switches, ideally <40ms. **QOS** must be used to prioritize forwarding of voice packets.
- **De-Jitter Delay** Receive buffer to transform variable delay into a fixed delay.





Wireshark can analyze Jitter, Packet Loss etc.

bytes on wire (1712 bits), 214 bytes
 Src: 152.96.10.153 (00:18:19:71:5e:ef)
 Protocol Version 4, Src: 152.96.10.153 (152.96.10.153)
 Protocol, Src Port: 24880 (24880), Dst Port: 24880 (24880)
 Transport Protocol

Wireshark calculates Mean Jitter according to RFC3550

Packet	Sequence	Delta (ms)	Jitter (ms)	Skew	Bandwidth	Marker	Status
1	2199	0.00	0.00	0.00	1.60	•	✓
3	2200	19.98	0.00	0.02	3.20		✓
5	2201	20.02	0.00	0.00	4.80		✓
6	2202	19.89	0.01	0.11	6.40		✓
7	2203	20.03	0.01	0.08	8.00		✓
9	2204	19.97	0.01	0.11	9.60		✓
11	2205	20.05	0.01	0.07	11.20		✓
13	2206	19.96	0.02	0.11	12.80		✓
16	2208	39.99	0.02	0.12	14.40		Wrong sequence number
18	2209	20.00	0.01	0.12	16.00		✓
20	2210	20.05	0.02	0.07	17.60		✓
22	2211	19.96	0.02	0.11	19.20		✓
24	2212	20.04	0.02	0.07	20.80		✓
26	2213	20.00	0.02	0.08	22.40		✓
28	2214	20.04	0.02	0.04	24.00		✓
30	2215	19.96	0.02	0.08	25.60		✓
32	2216	19.96	0.02	0.12	27.20		✓
34	2217	20.05	0.02	0.06	28.80		✓
36	2218	20.01	0.02	0.05	30.40		✓
38	2219	20.04	0.02	0.01	32.00		✓
40	2220	19.98	0.02	0.03	33.60		✓
42	2221	20.04	0.02	-0.01	35.20		✓
44	2222	19.98	0.02	0.01	36.80		✓
46	2223	19.96	0.03	0.05	38.40		✓
48	2224	20.03	0.03	0.02	40.00		✓
50	2225	19.98	0.02	0.04	41.60		✓
52	2226	20.01	0.02	0.04	43.20		✓
53	2227	20.01	0.02	0.03	44.80		✓



Forcing Wireshark to decode RTP

1. Right click on UDP header

2. Select Decode As..

3. Select RTP

No.	Time	Delta	Source	Destination	QoS	Length	Protocol	Info
1	0.000000	0.000000	152.96.10.153	152.96.10.155	46	214	UDP	24880 → 27662 Len=172
2	0.006669	0.006669	152.96.10.155	152.96.10.153	46	214	UDP	27662 → 24880 Len=172
3	0.019978	0.013309	152.96.10.153	152.96.10.155	46	214	UDP	24880 → 27662 Len=172
4	0.026628	0.006650	152.96.10.155	152.96.10.153	46	214	UDP	27662 → 24880 Len=172
5	0.040000	0.013372	152.96.10.153	152.96.10.155	46	214	UDP	24880 → 27662 Len=172
6	0.046669	0.006640	152.96.10.155	152.96.10.153	46	214	UDP	27662 → 24880 Len=172
7	0.060000	0.013331	152.96.10.153	152.96.10.155	46	214	UDP	24880 → 27662 Len=172
8	0.066669	0.006669	152.96.10.155	152.96.10.153	46	214	UDP	27662 → 24880 Len=172
9	0.080000	0.013331	152.96.10.153	152.96.10.155	46	214	UDP	24880 → 27662 Len=172
10	0.086669	0.006759	152.96.10.155	152.96.10.153	46	214	UDP	27662 → 24880 Len=172
11	0.100000	0.013206	152.96.10.153	152.96.10.155	46	214	UDP	24880 → 27662 Len=172
12	0.106669	0.006792	152.96.10.155	152.96.10.153	46	214	UDP	27662 → 24880 Len=172
13	0.119978	0.013255	152.96.10.153	152.96.10.155	46	214	UDP	24880 → 27662 Len=172
14	0.126669	0.006740	152.96.10.155	152.96.10.153	46	214	UDP	27662 → 24880 Len=172

> Frame 1: 214 bytes on wire (1712 bits) captured (0 bytes captured on interface) on interface 0
> Ethernet II, Src: Cisco_71:5e:ef:c4:00:09, Dst: Cisco_71:5e:ef:c4:00:09, Length: 144
> Internet Protocol Version 4, Src: 152.96.10.153, Dst: 152.96.10.155, Len: 60, TOS: 0
> User Datagram Protocol, Src Port: 24880, Dst Port: 27662
> Data (172 bytes)

Feld	Wert	Typ	Standard	Aktuell
UDP port	24880	Integer, base10	(none)	RTP

OK Speichern Abbrechen Hilfe



SharkFest '19 Europe



Hope you learned something useful!



© Rolf Leutert, Leutert NetServices, www.netsniffing.ch

VoIP Trainings with Wireshark available all over Europe