

Setup

To perform the lab task, some setting up needed to be done.

After downloading all the necessary files, first we launched the debian VM to obtain the IP to connect to the VoIP server:

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:35:34:6d brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe35:346d/64 scope link
        valid_lft forever preferred_lft forever
```

We see the address IPv4 enp0s3 being 192.168.56.102

Then, knowing the IP address and other information, we set up 3cx profile:

Account settings

Account name:

Caller ID:

Credentials

Enter your SIP account credentials

Extension:

ID:

Password:

My location

Specify the IP of your PBX/SIP server

☒ I am in the office - local IP of PBX

☐ I am out of the office - external IP of PBX

☐ Use 3CX Tunnel

Eliminates firewall configuration. Requires 3CX Phone System for Windows

Local IP of remote PBX:

Tunnel password: Port:

☐ Use Outbound Proxy server

Required by some VoIP Providers. Specify IP or name.

☐ Perform provisioning from following URL:

Advanced settings OK Cancel

ID and pass was given in the instruction .pdf

Wireshark setup

Wireshark was set to sniff traffic on the VirtualBox Host-Only Network. No capture filter was used, but later on a display filter was used to only display SIP and RTP traffic. Some other traffic, unrelated to the lab, was captured.

The obtained .pcapng was saved and analyzed after two calls were made.

3cx calls setup

Going into advanced settings, we can see more detailed call settings. Since the task required to make two calls with different settings, we show the used settings. 1st call:

Account advanced settings

PBX voicemail:

STUN server:

Registration time: minutes

SIP transport: Certificates

RTP mode:

☒ Support RFC2833 DTMF
Payload number:

☐ Support INBAND DTMF

☐ Support SIPINFO DTMF

Audio codecs
PCMA
PCMU
GSM

Video codecs
H.263 (ffdsnow)

Video formats
176 x 144
352 x 288
128 x 96
704 x 576

OK Cancel

And for the 2nd call, GSM was the primary codec. Furthermore, RFC2833 DTMF support was turned off. Instead - SIPINFO DTMF support was turned on:

Account advanced settings

PBX voicemail:

STUN server:

Registration time: minutes

SIP transport: Certificates

RTP mode:

☐ Support RFC2833 DTMF
Payload number:

☐ Support INBAND DTMF

☒ Support SIPINFO DTMF

Audio codecs
GSM
PCMA
PCMU

Video codecs
H.263 (ffdsnow)

Video formats
176 x 144
352 x 288
128 x 96
704 x 576

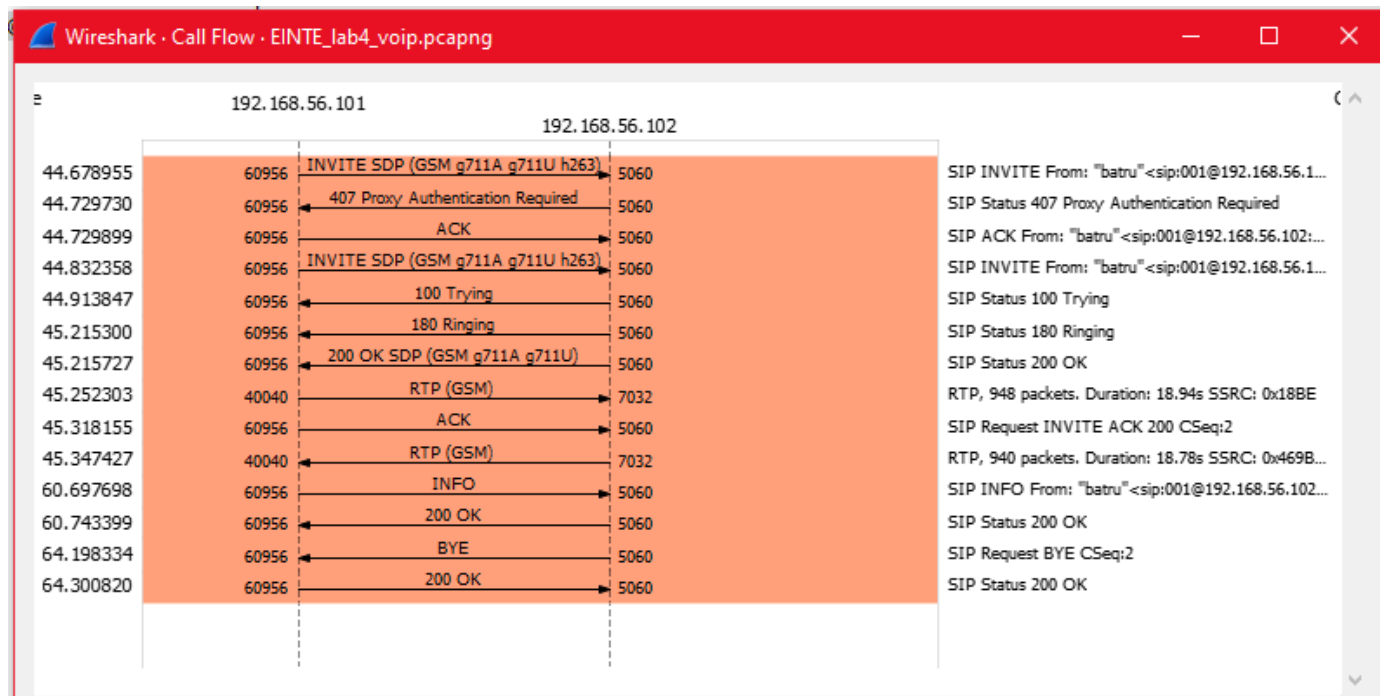
OK Cancel

VoIP session analysis - Call Flow

Below we present the sequence of messages regarding the VoIP calls, as seen in the wireshark's telephony tab, flow sequence. For the first call (PCMA):

Wireshark · Call Flow · EINTE_lab4_voip.pcapng			
Time	192.168.56.101	192.168.56.102	Comment
2.195304	51840	INVITE SDP (g711A g711U GSM teleph...	SIP INVITE From: "batru" <sip:001@192.168.56.1...
2.246501	51840	407 Proxy Authentication Required	SIP Status 407 Proxy Authentication Required
2.246660	51840	ACK	SIP ACK From: "batru" <sip:001@192.168.56.102:...
2.349534	51840	INVITE SDP (g711A g711U GSM teleph...	SIP INVITE From: "batru" <sip:001@192.168.56.1...
2.430505	51840	100 Trying	SIP Status 100 Trying
2.682159	51840	180 Ringing	SIP Status 180 Ringing
2.682436	51840	200 OK SDP (g711A g711U GSM teleph...	SIP Status 200 OK
2.709628	40038	RTP (g711A)	RTP, 941 packets. Duration: 18.80s SSRC: 0xBAE...
2.722242	40038	RTP (g711A)	RTP, 762 packets. Duration: 15.22s SSRC: 0x18BE
2.785511	51840	ACK	SIP Request INVITE ACK 200 CSeq:2
17.961763	40038	RTP (telephone-event) DTMF Five 5	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
17.961870	40038	RTP (g711A)	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
17.981296	40038	RTP (telephone-event) DTMF Five 5	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
17.981433	40038	RTP (g711A)	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.001784	40038	RTP (telephone-event) DTMF Five 5	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.001889	40038	RTP (g711A)	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.021316	40038	RTP (telephone-event) DTMF Five 5	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.021429	40038	RTP (g711A)	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.041818	40038	RTP (telephone-event) DTMF Five 5	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.041915	40038	RTP (g711A)	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.061351	40038	RTP (telephone-event) DTMF Five 5	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.061448	40038	RTP (g711A)	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.081861	40038	RTP (telephone-event) DTMF Five 5	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.081976	40038	RTP (g711A)	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.101386	40038	RTP (telephone-event) DTMF Five 5	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.101503	40038	RTP (g711A)	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.121897	40038	RTP (telephone-event) DTMF Five 5	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.122020	40038	RTP (g711A)	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.141438	40038	RTP (telephone-event) DTMF Five 5	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.141581	40038	RTP (g711A)	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.161934	40038	RTP (telephone-event) DTMF Five 5	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.162057	40038	RTP (g711A)	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.182159	40038	RTP (telephone-event) DTMF Five 5	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.182278	40038	RTP (g711A)	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.201692	40038	RTP (telephone-event) DTMF Five 5	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.201820	40038	RTP (g711A)	RTP, 1 packets. Duration: 0.00s SSRC: 0x18BE
18.221334	40038	RTP (g711A)	RTP, 169 packets. Duration: 3.36s SSRC: 0x18BE
21.584430	51840	BYE	SIP Request BYE CSeq:2
21.687580	51840	200 OK	SIP Status 200 OK

And below - 2nd call (GSM):



VoIP questions - first session (PCMA)

What is the meaning of 407 Proxy Authentication Required response received after the first INVITE?

The first INVITE packet does not contain any authentication information. After the 3cx client acknowledges that, it sends an INVITE message, but this time with credentials that are used for authentication.

That is why after the 2nd INVITE message, the SIP is 'trying' and then 'ringing'. In general - after the 2nd INVITE message, the session is properly established.

To see this actually being the case, we look into the following packet info:

```

▼ Message Header
  > Via: SIP/2.0/UDP 192.168.56.101:51840;branch=z9hG4bK-d8754z-b20d8068893a9c77-1---d8754z-;rport
    Max-Forwards: 70
  > Contact: <sip:001@192.168.56.101:51840;rinstance=272907d0edf2b8d9>
  > To: <sip:801@192.168.56.102:5060>
  > From: "batru"<sip:001@192.168.56.102:5060>;tag=3724367c
    Call-ID: YjVkyZUzOWRkNThhZDdjOTkzYzZkZMDZiNDg5NzRmOWI.
    [Generated Call-ID: YjVkyZUzOWRkNThhZDdjOTkzYzZkZMDZiNDg5NzRmOWI.]
  > CSeq: 1 INVITE
    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REGISTER, SUBSCRIBE, NOTIFY, REFER, INFO, MESSAGE
    Content-Type: application/sdp
    Supported: replaces
    User-Agent: 3CXPhone 6.0.26523.0
    Content-Length: 410

```

Is the header of the first INVITE.

EINTE_lab4_voip.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::a00:27ff:fe35...	ff02::2	ICMPv6	70	Router Solicitation from 08:00:27:35:34:6d
2	2.195304	192.168.56.101	192.168.56.102	SIP/SDP	1043	Request: INVITE sip:801@192.168.56.102:5060
3	2.246501	192.168.56.102	192.168.56.101	SIP	509	Status: 407 Proxy Authentication Required
4	2.246660	192.168.56.101	192.168.56.102	SIP	391	Request: ACK sip:801@192.168.56.102:5060
5	2.349534	192.168.56.101	192.168.56.102	SIP/SDP	1269	Request: INVITE sip:801@192.168.56.102:5060
6	2.430505	192.168.56.102	192.168.56.101	SIP	348	Status: 100 Trying
7	2.682159	192.168.56.102	192.168.56.101	SIP	447	Status: 180 Ringing
8	2.682436	192.168.56.102	192.168.56.101	SIP/SDP	993	Status: 200 OK (INVITE)
9	2.709628	192.168.56.102	192.168.56.101	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0xBAEBC87, Seq=10946, Time=1212094366, Mark
10	2.722242	192.168.56.101	192.168.56.102	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x18BE, Seq=18467, Time=4273, Mark
11	2.730205	192.168.56.102	192.168.56.101	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0xBAEBC87, Seq=10947, Time=1212094526
12	2.741774	192.168.56.101	192.168.56.102	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x18BE, Seq=18468, Time=4433
13	2.750980	192.168.56.102	192.168.56.101	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0xBAEBC87, Seq=10948, Time=1212094686
14	2.762217	192.168.56.101	192.168.56.102	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x18BE, Seq=18469, Time=4593
15	2.772226	192.168.56.102	192.168.56.101	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0xBAEBC87, Seq=10949, Time=1212094846
16	2.781745	192.168.56.101	192.168.56.102	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x18BE, Seq=18470, Time=4753
17	2.785511	192.168.56.101	192.168.56.102	SIP	719	Request: ACK sip:801@192.168.56.102:5060
18	2.788620	192.168.56.102	192.168.56.101	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0xBAEBC87, Seq=10950, Time=1212095006
19	2.802262	192.168.56.101	192.168.56.102	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x18BE, Seq=18471, Time=4913
20	2.810291	192.168.56.102	192.168.56.101	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0xBAEBC87, Seq=10951, Time=1212095166
21	2.821804	192.168.56.101	192.168.56.102	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x18BE, Seq=18472, Time=5073
22	2.831612	192.168.56.102	192.168.56.101	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0xBAEBC87, Seq=10952, Time=1212095326
23	2.841309	192.168.56.101	192.168.56.102	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x18BE, Seq=18473, Time=5233

Method: INVITE
 > Request-URI: sip:801@192.168.56.102:5060
 [Resent Packet: False]

Message Header
 > Via: SIP/2.0/UDP 192.168.56.101:51840;branch=z9hG4bK-d8754z-a2523008cb740a35-1--d8754z-rport
 Max-Forwards: 70
 > Contact: <sip:001@192.168.56.101:51840;rinstance=272907d0edf2b8d9>
 > To: <sip:801@192.168.56.102:5060>
 > From: "batru"<sip:001@192.168.56.102:5060>;tag=3724367c
 Call-ID: YjVkyZuZOWRkNThhZDdjOTkzYzZkMDZiNDg5NzRmOWI.
 [Generated Call-ID: YjVkyZuZOWRkNThhZDdjOTkzYzZkMDZiNDg5NzRmOWI.]
 > CSeq: 2 INVITE
 Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REGISTER, SUBSCRIBE, NOTIFY, REFER, INFO, MESSAGE
 Content-Type: application/sdp
 > Proxy-Authorization: Digest username="QV8JpkcM0W",realm="3CXPoneSystem",nonce="414d535961c3694216:3ea4e160675ad1c5e1cb60d8c3030456",uri="sip:801@192.168.56.102:5060",response="49141160503e8c29f890022de8f39b37",algorithm=MD5
 Supported: replaces
 User-Agent: 3CXPone 6.0.26523.0
 Content-Length: 410

Message Body
 Session Description Protocol
 Session Description Protocol Version (v): 0

0220 61 74 69 6f 6e 2f 73 64 70 0d 0a 50 72 6f 78 79 ation/sd p Proxy
 0230 2d 41 75 74 68 6f 72 69 7a 61 74 69 6f 6e 3a 20 -Authri zation:
 0240 44 69 67 65 73 74 20 75 73 65 72 6e 61 6d 65 3d Digest u sername=
 0250 22 51 56 38 4a 70 6b 63 4d 30 57 22 2c 72 65 61 "QV8Jpkc M0W",rea
 0260 6c 6d 3d 22 33 43 58 50 68 6f 6e 65 53 79 73 74 lm="3CXP oneSyst
 0270 65 6d 22 2c 6e 6f 6e 63 65 3d 22 34 31 34 64 35 em",nonc e="414d5
 0280 33 35 39 36 31 63 33 36 39 34 32 31 36 3a 33 65 35961c36 94216:3e

RFC 3261: Proxy-Authorization Header (sip.Proxy-Authorization), 226 bytes

Packets: 3873 · Displayed: 3873 (100.0%) · Dropped: 0 (0.0%) Profile: Default

Is the header of the 2nd invite message. We see the proxy-authorization message.
 We can't see the exact password and username due to md5 encryption.

What is the content of the Media Description line in SDP descriptions sent within the SIP INVITE and 200 OK messages? Attach the relevant screenshots and explain the meaning of the most important fields

The following sources were used to understand the body of SDP:
Page 32 and 33 from: <https://datatracker.ietf.org/doc/html/rfc3551>
Codes for the formats

Table 1, page 10 from: <https://datatracker.ietf.org/doc/html/rfc2833>
DTMF (Dual-tone multi-frequency signaling) range explained

The explanations are on the screenshot. Text in green borders are our comments on the information to the left:

Message Body

Session Description Protocol

Session Description Protocol Version (v): 0

> Owner/Creator, Session Id (o): 3cxVCE 370090755 367251405 IN IP4 192.168.56.101 session ID info: username, ID, session version, owner address

Session Name (s): 3cxVCE Audio Call

> Connection Information (c): IN IP4 192.168.56.101

> Time Description, active time (t): 0 0

> Media Description, name and address (m): audio 40038 RTP/AVP 8 0 3 101 Media type (audio), port on which media is transmitted, protocol used (RTP), codes for the formats. 8 - PCMA; 0 - PCMU; 3 - GSM. RFC3551 page 32 and 33

> Media Attribute (a): rtptime:8 PCMA/8000

> Media Attribute (a): rtptime:0 PCMU/8000

> Media Attribute (a): rtptime:3 GSM/8000

> Media Attribute (a): rtptime:101 telephone-event/8000 Information that telephone-event is supported. telephone-event is e.g. click on the telephone pad

> Media Attribute (a): fmtp:101 0-15 DTMF range 0-15

> Media Attribute (a):ptime:20 Packet time

> Media Attribute (a): sendrecv Defines the connection as 2-way Refer to RFC2833

> Media Description, name and address (m): video 40004 RTP/AVP 34 Video information. Unused in our exercise

> Connection Information (c): IN IP4 192.168.56.101

> Media Attribute (a): rtptime:34 H263/90000

> Media Attribute (a): fmtp:34 QCIF=1;CIF=1;SQCIF=1;CIF4=1

Media Attribute (a): sendrecv

[Generated Call-ID: YjVkyZuZOWRkNThhZDdjOTkzYzkzMDZiNDg5NzRmOWI.]

What is the voice codec used in the session?

Looking at arbitrary payload that was sent during the first call:

[illegible]

```
0020 38 65 1b 70 9c 66 00 b4 ad a0 80 08 2a c4 48 3f 8e p f . . . . . * . H ?
```

We see the payload type being ITU-T G.711 PCMA (G.711 with A-law algorithm)

In some RTP packets the Mark field in the packet header has the value of 1 – why?

From RFC3550, <https://datatracker.ietf.org/doc/html/rfc3550> page 13:

marker (M): 1 bit

The interpretation of the marker is defined by a profile. It is intended to allow significant events such as frame boundaries to be marked in the packet stream.

So the point of the marker bit is to separate bitstreams, frame boundaries.

For the first call, there are two marker bits set to 1 at the beginning.

How the information about the pressed key is sent by the SIP client to the VoIP server?

With the use of RTP EVENT packet type. Example snippet showing these packets:

1569	17.961763	192.168.56.101	192.168.56.102	RTP EVENT	58 Payload type=RTP Event, DTMF Five 5
1570	17.961870	192.168.56.101	192.168.56.102	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x18BE, Seq=19230, Time=126193
1571	17.970735	192.168.56.102	192.168.56.101	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0xBAEBC87, Seq=11709, Time=1212216446
1572	17.981296	192.168.56.101	192.168.56.102	RTP EVENT	58 Payload type=RTP Event, DTMF Five 5
1573	17.981433	192.168.56.101	192.168.56.102	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x18BE, Seq=19232, Time=126353
1574	17.992355	192.168.56.102	192.168.56.101	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0xBAEBC87, Seq=11710, Time=1212216606
1575	18.001784	192.168.56.101	192.168.56.102	RTP EVENT	58 Payload type=RTP Event, DTMF Five 5
1576	18.001889	192.168.56.101	192.168.56.102	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x18BE, Seq=19234, Time=126513
1577	18.012905	192.168.56.102	192.168.56.101	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0xBAEBC87, Seq=11711, Time=1212216766
1578	18.021316	192.168.56.101	192.168.56.102	RTP EVENT	58 Payload type=RTP Event, DTMF Five 5
1579	18.021429	192.168.56.101	192.168.56.102	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x18BE, Seq=19236, Time=126673
1580	18.028733	192.168.56.102	192.168.56.101	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0xBAEBC87, Seq=11712, Time=1212216926
1581	18.041818	192.168.56.101	192.168.56.102	RTP EVENT	58 Payload type=RTP Event, DTMF Five 5
1582	18.041915	192.168.56.101	192.168.56.102	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x18BE, Seq=19238, Time=126833
1583	18.049204	192.168.56.102	192.168.56.101	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0xBAEBC87, Seq=11713, Time=1212217086
1584	18.061351	192.168.56.101	192.168.56.102	RTP EVENT	58 Payload type=RTP Event, DTMF Five 5

We see that the event is a 'DTMF Five 5'

```
▼ Real-Time Transport Protocol
  ▼ [Stream setup by SDP (frame 5)]
    [Setup frame: 5]
    [Setup Method: SDP]
    [Generated Call-ID: YjVkyZuZOWRkNThhZDdjOTkzYzgzMDZiNDg5NzRmOWI.]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    1... .... = Marker: True
    Payload type: telephone-event (101)
    Sequence number: 19229
    [Extended sequence number: 84765]
    Timestamp: 126193
    Synchronization Source identifier: 0x000018be (6334)
  ▼ RFC 2833 RTP Event
    Event ID: DTMF Five 5 (5)
    0... .... = End of Event: False
    .0.. .... = Reserved: False
    ..00 1010 = Volume: 10
    Event Duration: 160
```

This is a telephone-event that was mentioned before.

Then at the end of the button press, RTP EVENTS showing the press has ended are sent. Note the 'end of event: true':

1608	18.221217	192.168.56.101	192.168.56.102	RTP EVENT	58 Payload type=RTP Event, DTMF Five 5 (end)
1609	18.221231	192.168.56.101	192.168.56.102	RTP EVENT	58 Payload type=RTP Event, DTMF Five 5 (end)
1610	18.221237	192.168.56.101	192.168.56.102	RTP EVENT	58 Payload type=RTP Event, DTMF Five 5 (end)
1611	18.221334	192.168.56.101	192.168.56.102	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x18BE, Seq=192
1612	18.231136	192.168.56.102	192.168.56.101	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0xBAEBC87, Seq=
1613	18.241820	192.168.56.101	192.168.56.102	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x18BE, Seq=192
1614	18.251843	192.168.56.102	192.168.56.101	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0xBAEBC87, Seq=


```

> Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.102
> User Datagram Protocol, Src Port: 40038, Dst Port: 7024
✓ Real-Time Transport Protocol
  ✓ [Stream setup by SDP (frame 5)]
    [Setup frame: 5]
    [Setup Method: SDP]
    [Generated Call-ID: YjVkyZUzOWRkNThhZDdjOTkzYzkzMDZiNDg5NzRmOWI.]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    0... .... = Marker: False
    Payload type: telephone-event (101)
    Sequence number: 19255
    [Extended sequence number: 84791]
    Timestamp: 126193
    Synchronization Source identifier: 0x000018be (6334)
  ✓ RFC 2833 RTP Event
    Event ID: DTMF Five 5 (5)
    1... .... = End of Event: True
    .0.. .... = Reserved: False
    ..00 1010 = Volume: 10
    Event Duration: 2000
  
```



```

0000  08 00 27 35 34 6d 0a 00 27 00 00 05 08 00 45 00  ..'54m.. '.....E..
0010  00 2c b6 ae 00 00 80 11 91 f6 c0 a8 38 65 c0 a8  ,.....8e..
0020  38 66 9c 66 1b 70 00 18 76 d3 80 65 4b 37 00 01  8f·f·p· v·ek7..
0030  ec f1 00 00 18 be 05 8a 08 20  ....5.
  
```

What is the sequence number and timestamp of the first RTP packet sent by the server to the client, and why are they not 0 or 1?

If the sequence number would be 0 or 1 in every case, then simultaneous streams would interfere with each other. Or it wouldn't even be possible to have many different streams at the same time.

Randomisation of that prevents the issue of collision with other streams.

For the first RTP packet received FROM SIP server in the 1st call:

- Sequence number is 10946
- Time is 1212094366

2nd RTP packet, which is 1st sent TO SIP server is:

- Sequence number 18467
- Time 4273

VoIP questions - second session (GSM)

Which voice codec was used [in the second session]?

Looking at an arbitrary RTP packet:

```
▼ Real-Time Transport Protocol
  > [Stream setup by SDP (frame 1975)]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    0... .... = Marker: False
    Payload type: GSM 06.10 (3)
    Sequence number: 18472
    [Extended sequence number: 84008]
    Timestamp: 5801
    Synchronization Source identifier: 0x000018be (6334)
    Payload: d820a2e15a50004924924924500049249249245000492492492450004924924924
```

We see the payload type being GSM 06.10. This codec is also known as Full Rate. It is a rather old codec, with low bitrate for modern standards.

The difference in the sound quality was heard (comparing to 1st call)

How is the information about the pressed key sent to the VoIP server?

With the use of SIP INFO:

3521	60.697698	192.168.56.101	192.168.56.102	SIP	784 Request: INFO sip:801@192.168.56.102:5060
3522	60.709770	192.168.56.102	192.168.56.101	RTP	87 PT=GSM 06.10, SSRC=0x469B7262, Seq=62139, T
3523	60.712552	192.168.56.101	192.168.56.102	RTP	87 PT=GSM 06.10, SSRC=0x18BE, Seq=19240, Time=
3524	60.726346	192.168.56.102	192.168.56.101	RTP	87 PT=GSM 06.10, SSRC=0x469B7262, Seq=62140, T
3525	60.733094	192.168.56.101	192.168.56.102	RTP	87 PT=GSM 06.10, SSRC=0x18BE, Seq=19241, Time=
3526	60.743399	192.168.56.102	192.168.56.101	SIP	440 Status: 200 OK (INFO)
3527	60.747951	192.168.56.102	192.168.56.101	RTP	87 PT=GSM 06.10, SSRC=0x469B7262, Seq=62141, T
3528	60.750501	192.168.56.101	192.168.56.102	RTP	87 PT=GSM 06.10, SSRC=0x18BE, Seq=19242, Time=

>	Frame 3521: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{23EA1C08-ECE5-4CC3-A34}
>	Ethernet II, Src: 0a:00:27:00:00:05 (0a:00:27:00:00:05), Dst: PcsCompu_35:34:6d (08:00:27:35:34:6d)
>	Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.102
>	User Datagram Protocol, Src Port: 60956, Dst Port: 5060
▼	Session Initiation Protocol (INFO)
▼	Request-Line: INFO sip:801@192.168.56.102:5060 SIP/2.0
	Method: INFO
>	Request-URI: sip:801@192.168.56.102:5060
	[Resent Packet: False]
>	Message Header
▼	Message Body
	Signal=5\r\n
	Duration=250\r\n

Then an OK response is received, which means the signal '5' was sent properly.

3521	60.697698	192.168.56.101	192.168.56.102	SIP	784 Request: INFO sip:801@192.168.56.102:5060
3522	60.709770	192.168.56.102	192.168.56.101	RTP	87 PT=GSM 06.10, SSRC=0x469B7262, Seq=62139,
3523	60.712552	192.168.56.101	192.168.56.102	RTP	87 PT=GSM 06.10, SSRC=0x18BE, Seq=19240, Time
3524	60.726346	192.168.56.102	192.168.56.101	RTP	87 PT=GSM 06.10, SSRC=0x469B7262, Seq=62140,
3525	60.733094	192.168.56.101	192.168.56.102	RTP	87 PT=GSM 06.10, SSRC=0x18BE, Seq=19241, Time
3526	60.743399	192.168.56.102	192.168.56.101	SIP	440 Status: 200 OK (INFO)
3527	60.747951	192.168.56.102	192.168.56.101	RTP	87 PT=GSM 06.10, SSRC=0x469B7262, Seq=62141,
3528	60.750501	192.168.56.101	192.168.56.102	RTP	87 PT=GSM 06.10, SSRC=0x18BE, Seq=19242, Time

> Frame 3526: 440 bytes on wire (3520 bits), 440 bytes captured (3520 bits) on interface \Device\NPF_{23EA1C08-ECE5-4CC3-A3}

> Ethernet II, Src: PcsCompu_35:34:6d (08:00:27:35:34:6d), Dst: 0a:00:27:00:00:05 (0a:00:27:00:00:05)

> Internet Protocol Version 4, Src: 192.168.56.102, Dst: 192.168.56.101

> User Datagram Protocol, Src Port: 5060, Dst Port: 60956

▼ Session Initiation Protocol (200)

▼ Status-Line: SIP/2.0 200 OK

Status-Code: 200

[Resent Packet: False]

[Request Frame: 3521]

[Response Time (ms): 45]

Closing remarks

Below we provide a list of sources and what info was taken from them:

- <https://datatracker.ietf.org/doc/html/rfc3551> - rtpmap format codes
- <https://datatracker.ietf.org/doc/html/rfc2833> - DTMF code ranges
- <https://datatracker.ietf.org/doc/html/rfc3550> - marker information

Naturally, the display filter in wireshark should be sip || rtp. That way, packets unrelated to the lab are not seen.

.pdf files of sequence flow are also attached, exported from Wireshark.

End