Identify DTMF Events in a Packet Capture

Contents

Introduction

This document describes identifying Dual-Tone Multi-Frequency (DTMF) events within a packet capture.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Webex Control Hub
- Calling in Webex (Unified CM)
- DTMF

Components Used

The information in this document is based on these software and hardware versions:

- Wireshark version 4.0.7 (v4.0.7-0-g0ad1823cc090)
- Webex Control Hub

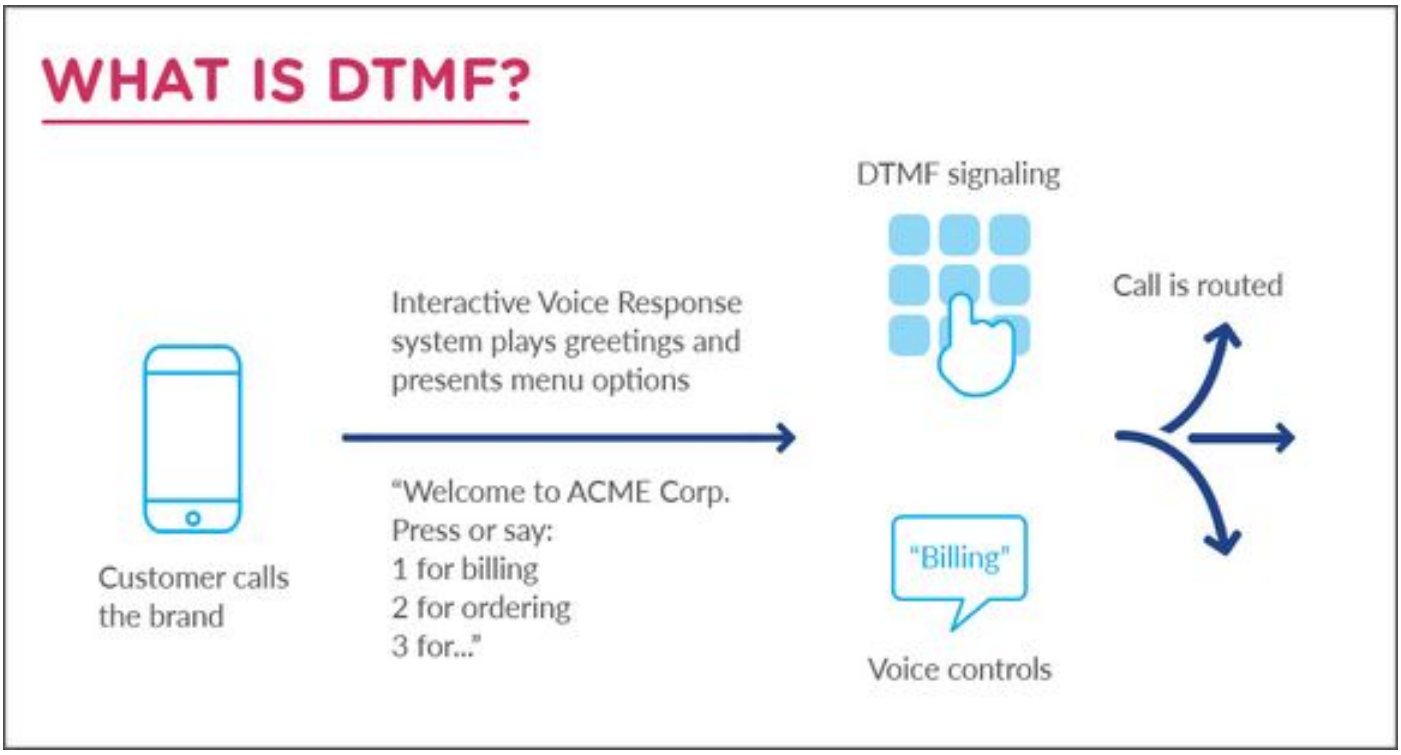
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This article outlines how to identify Dual-Tone Multi-Frequency (DTMF) events within a packet capture using Wireshark. DTMF events are being passed within a call while using Calling in Webex (Unified CM). The call does not show any abnormal behavior or error messages. During this test call, digits 6,7,8,9,1,2 and 3 are pressed in sequence as DTMF input.

What is DTMF?

Dual Tone Multi-Frequency (DTMF) is the sound/tone generated by a telephone when the numbers are pressed. DTMF is used to control automated equipment and signal user intent, such as the number they wish to dial. Each key has two tones at specific frequencies.



DTMF Flow Diagram

At its start, in the late 1970s to early 1980s, DTMF technology was a paradigm shift for contact centers. For the first time, callers could complete self-service by selecting the right menu option, reducing average handle times and misroutes.

In the late 1990s, speech directed dialogue was introduced. Now, callers could say "billing" or "one" instead of pressing a number. It was definitely a better, hands-free option for self-service.

But a lot has changed in the past few decades.

Businesses have evolved. For modern businesses, telephony is one of the many channels used to engage with you. They strive to deliver state of the art technology and your experience across all channels of communication – web, mobile, social media and telephony.

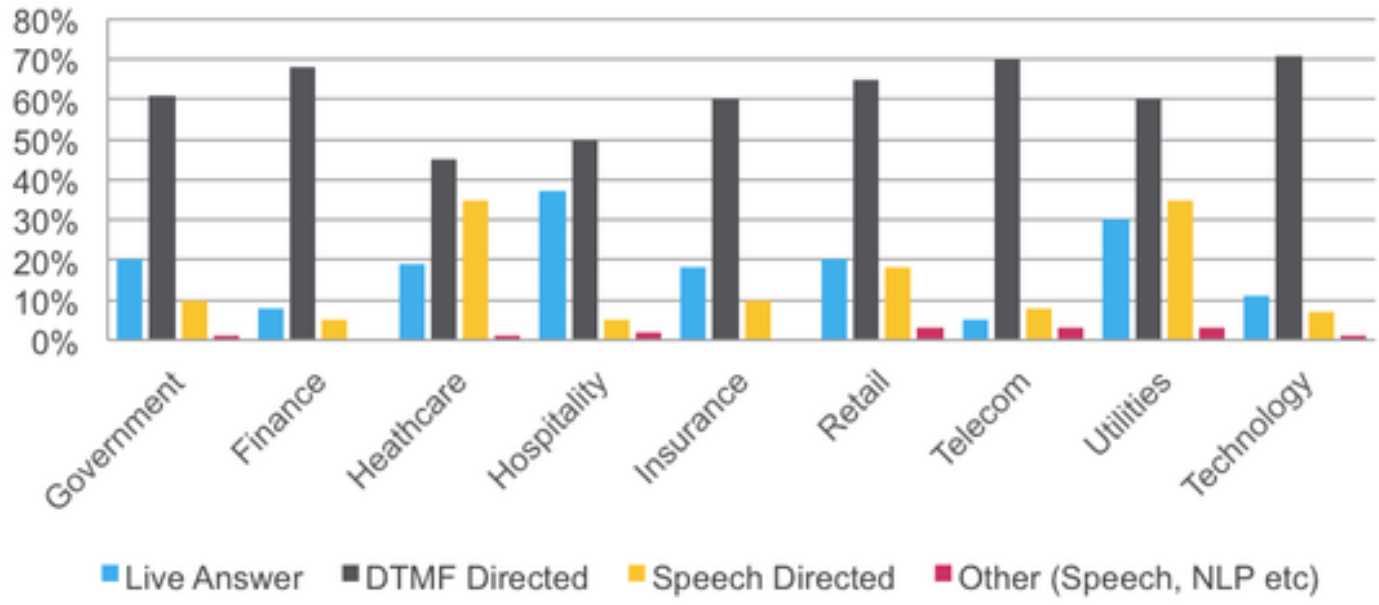
Today’s tech-savvy environment demands seamless experiences across all channels. Modern customers are far more vocal than their predecessors and take a lot of pride in the brands they associate themselves with.

So a dated or bad customer experience has an immediate impact on brand loyalty.

Customer service has evolved. As a joint effect of these two shifts, customer service has transformed over the past decade. It is no longer an afterthought but ingrained in all aspects of the business. Customer obsession, a key differentiator for many leading businesses, is the new marketing.

Why Do Some Brands Still Use DTMF Technology?

DTMF directed dialogue and speech directed dialogue are still the primary choice of technology for call handling across industry verticals.



Call Handling Technology Across Industries

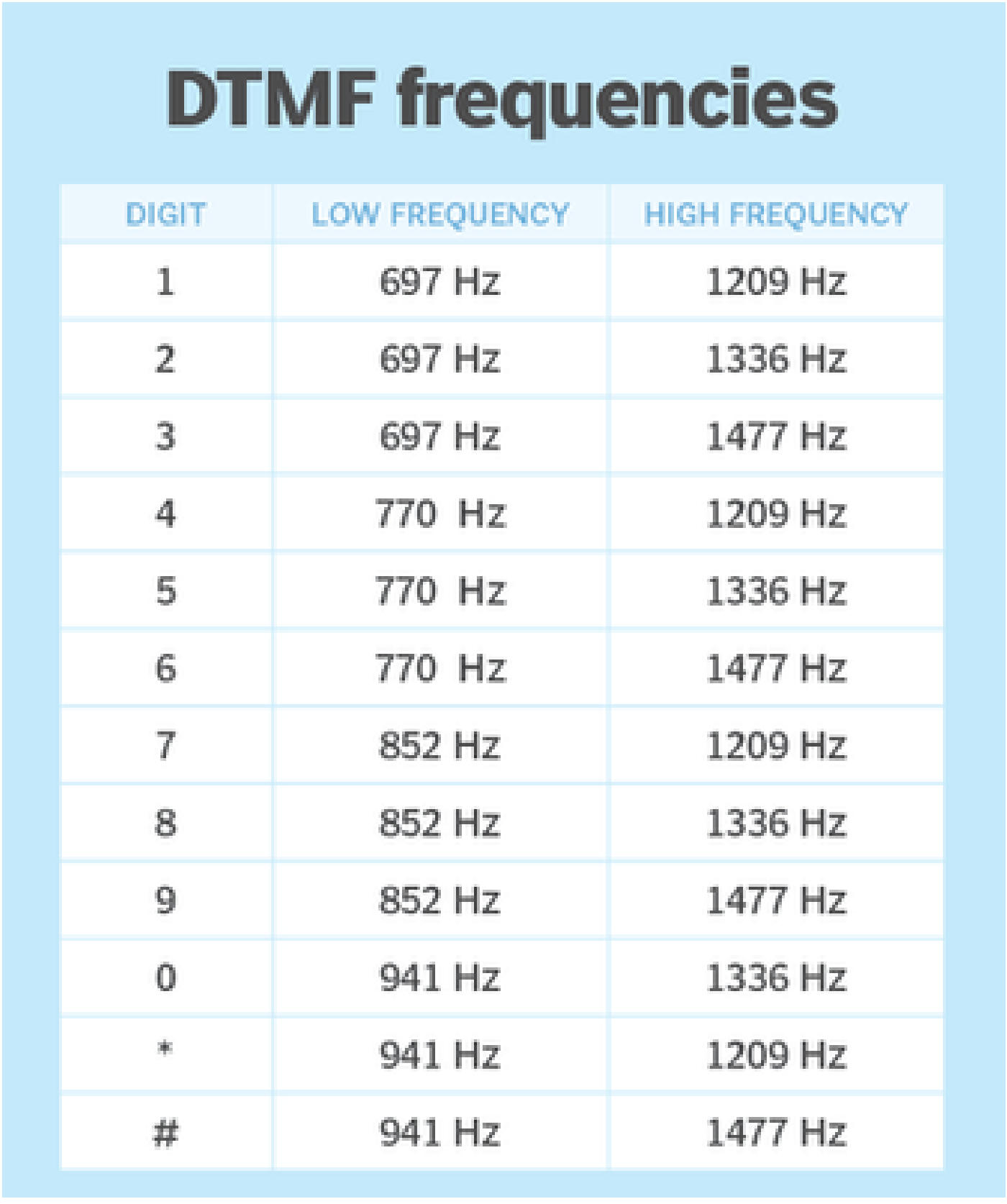
How Does DTMF Work?

DTMF technology works by having the handset generate tones at specific frequencies and playing them over the phone line when a button is pressed on the keypad. Equipment at the other end of the phone line listens to the specific sounds and decodes them into commands.

DTMF uses audio frequencies, so key presses can be used to play recognizable melodies. Since each button makes two tones and they do not directly line up to standard musical notes, it is not an exact correlation.

DTMF specifies eight different tones divided into a high group and a low group. Each key press corresponds to two tones -- hence the name dual tone -- one from the high group and one from the low group. This allows for 16 total keys.

These keys are specified as the numbers 0 through 9, * (asterisk or star), # (pound, hash or octothorpe) and the letters A through D. The letter keys are not generally used and are omitted from the majority of consumer telephones. The telecommunications industry chose two simultaneous tones for each key to eliminate the possibility of the human voice triggering the system.



DTMF Frequencies

In-Band and Out-of-Band Signaling

Traditional DTMF is an in-band signaling system, meaning the signals are transmitted using the same channel as the voice traffic. But in voice over IP, DTMF signals can be transmittedin-band (RFC2833) orout-of-band. Out-of-band VoIP DTMF signaling can be implemented using protocols like SIP and MGCP,

whereby special message types are defined for the transmission of digits.

The standardin-bandmethod is to simply transmit the tones along with the audio, but this can result in unreliable signals due to codec compression, packet loss or audio interference. In-band DTMF transmission is usually only reliable when the uncompressed G.711 codec is used. If G.729 or G.723 are used, signaling normally fails as a result of the compression.

The in-band DTMF relay mechanism is defined by RFC2833. The DTMF tones/sounds are sent using the RTP stream after establishing media. You could differentiate DTMF with audio by the payload type.

Most often than not, we see the payload type as 101 for in-band DTMF. The number must be within the range 96-127.

Out-of-Band DTMF

Out-of-band DTMF transmission involves sending DTMF tones separately from the main voice stream, typically using a separate signaling channel. This method offers reliability and can be more secure than in-band DTMF, as it separates the DTMF data from the voice stream.

Key Aspects of Out-of-Band DTMF

Separate Channel:
DTMF information is not mixed into the audio stream but transmitted via a separate signaling channel.

Signaling Protocols:
Out-of-band DTMF often relies on established signaling protocols like Session Initiation Protocol (SIP), H.323, etc to transmit DTMF events.

Reliable Transmission:
Out-of-band DTMF can provide more reliable transmission of DTMF tones, especially over compressed codecs or in network conditions that can affect audio quality.

Reduced Complexity:
It simplifies the processing of DTMF events, as the receiving end does not need to filter the DTMF tones from the audio stream.

There are situations where it is crucial to confirm whether the in-band DTMF digits are being transmitted within the RTP stream. Wireshark is an excellent tool for verifying this. Additionally, it allows you to check the payload type of specific packets.

Troubleshooting Steps

These are the steps to troubleshooting your issue:

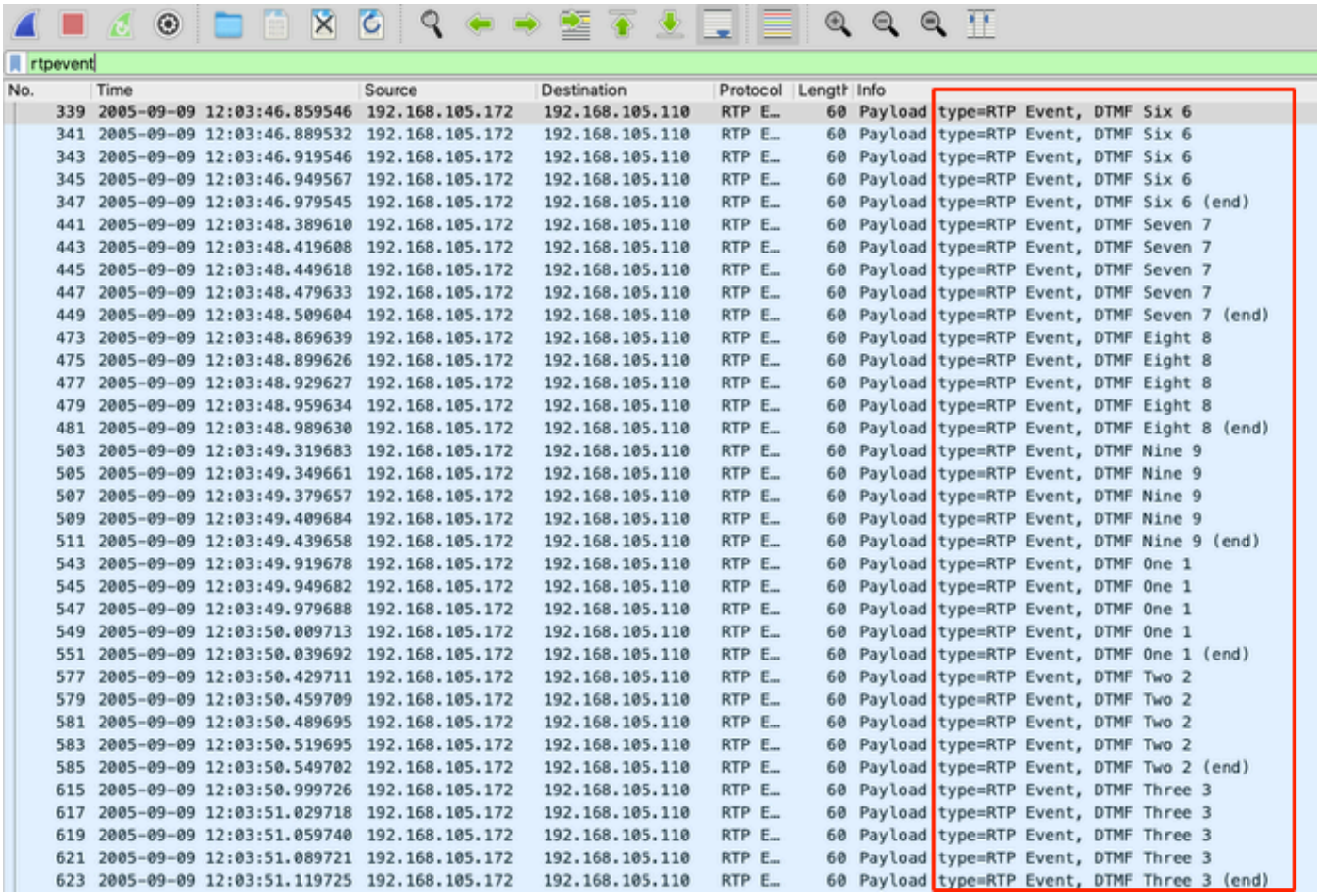
1. Enable capturing the traffic with the help of Wireshark on the client PC.
2. Proceed to make a call to a destination number which you know has IVR configured so that DTMF can be used.
3. Once you have entered the DTMF digits corresponding to the prompts heard in the IVR, stop the packet capture and save the file.

During this test call, digits 6,7,8,9,1,2 and 3 are pressed in sequence as DTMF input.

4. Proceed to filter the DTMF packets within the packet capture.
5. Use the filter **rtpevent** to see the DTMF packets.

Packet Capture Analysis

1. You can see the digits 6,7,8,9,1,2 and 3 being pressed in sequence.



rtpevent

No.	Time	Source	Destination	Protocol	Length	Info
339	2005-09-09 12:03:46.859546	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Six 6
341	2005-09-09 12:03:46.889532	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Six 6
343	2005-09-09 12:03:46.919546	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Six 6
345	2005-09-09 12:03:46.949567	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Six 6
347	2005-09-09 12:03:46.979545	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Six 6 (end)
441	2005-09-09 12:03:48.389610	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Seven 7
443	2005-09-09 12:03:48.419608	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Seven 7
445	2005-09-09 12:03:48.449618	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Seven 7
447	2005-09-09 12:03:48.479633	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Seven 7
449	2005-09-09 12:03:48.509604	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Seven 7 (end)
473	2005-09-09 12:03:48.869639	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Eight 8
475	2005-09-09 12:03:48.899626	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Eight 8
477	2005-09-09 12:03:48.929627	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Eight 8
479	2005-09-09 12:03:48.959634	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Eight 8
481	2005-09-09 12:03:48.989630	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Eight 8 (end)
503	2005-09-09 12:03:49.319683	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Nine 9
505	2005-09-09 12:03:49.349661	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Nine 9
507	2005-09-09 12:03:49.379657	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Nine 9
509	2005-09-09 12:03:49.409684	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Nine 9
511	2005-09-09 12:03:49.439658	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Nine 9 (end)
543	2005-09-09 12:03:49.919678	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF One 1
545	2005-09-09 12:03:49.949682	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF One 1
547	2005-09-09 12:03:49.979688	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF One 1
549	2005-09-09 12:03:50.009713	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF One 1
551	2005-09-09 12:03:50.039692	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF One 1 (end)
577	2005-09-09 12:03:50.429711	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Two 2
579	2005-09-09 12:03:50.459709	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Two 2
581	2005-09-09 12:03:50.489695	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Two 2
583	2005-09-09 12:03:50.519695	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Two 2
585	2005-09-09 12:03:50.549702	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Two 2 (end)
615	2005-09-09 12:03:50.999726	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Three 3
617	2005-09-09 12:03:51.029718	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Three 3
619	2005-09-09 12:03:51.059740	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Three 3
621	2005-09-09 12:03:51.089721	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Three 3
623	2005-09-09 12:03:51.119725	192.168.105.172	192.168.105.110	RTP E…	60	Payload type=RTP Event, DTMF Three 3 (end)

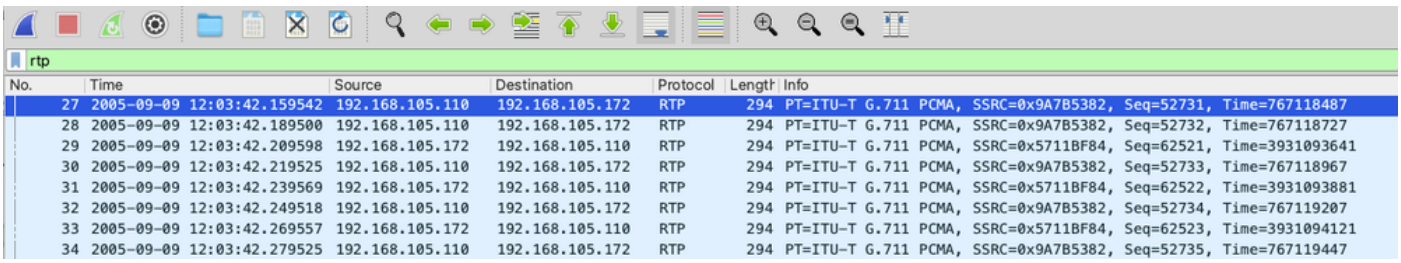
DTMF Events Seen in the Packet Capture

Since this is in-band DTMF, the events are sent inside the RTP stream, at which point you can see Protocol **RTP EVENT**. The payload type shows as RTP Event.

2. You can compare the payload value between a normal**RTP packet**and a**DTMF packet**.

Normal RTP Packet

The snippet depicts a normal RTP packet, highlighted in blue.



rtp

No.	Time	Source	Destination	Protocol	Length	Info
27	2005-09-09 12:03:42.159542	192.168.105.110	192.168.105.172	RTP	294	PT=ITU-T G.711 PCMA, SSRC=0x9A7B5382, Seq=52731, Time=767118487
28	2005-09-09 12:03:42.189500	192.168.105.110	192.168.105.172	RTP	294	PT=ITU-T G.711 PCMA, SSRC=0x9A7B5382, Seq=52732, Time=767118727
29	2005-09-09 12:03:42.209598	192.168.105.172	192.168.105.110	RTP	294	PT=ITU-T G.711 PCMA, SSRC=0x5711BF84, Seq=62521, Time=3931093641
30	2005-09-09 12:03:42.219525	192.168.105.110	192.168.105.172	RTP	294	PT=ITU-T G.711 PCMA, SSRC=0x9A7B5382, Seq=52733, Time=767118967
31	2005-09-09 12:03:42.239569	192.168.105.172	192.168.105.110	RTP	294	PT=ITU-T G.711 PCMA, SSRC=0x5711BF84, Seq=62522, Time=3931093881
32	2005-09-09 12:03:42.249518	192.168.105.110	192.168.105.172	RTP	294	PT=ITU-T G.711 PCMA, SSRC=0x9A7B5382, Seq=52734, Time=767119207
33	2005-09-09 12:03:42.269557	192.168.105.172	192.168.105.110	RTP	294	PT=ITU-T G.711 PCMA, SSRC=0x5711BF84, Seq=62523, Time=3931094121
34	2005-09-09 12:03:42.279525	192.168.105.110	192.168.105.172	RTP	294	PT=ITU-T G.711 PCMA, SSRC=0x9A7B5382, Seq=52735, Time=767119447

Normal RTP Packet

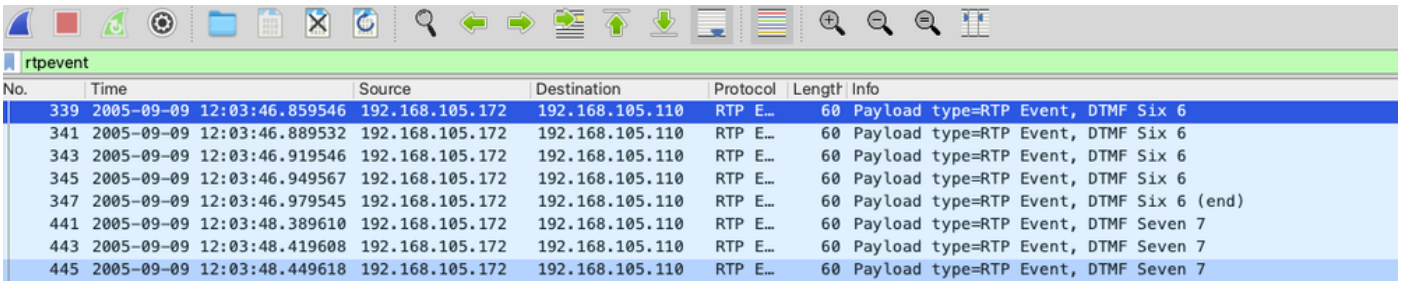
If you observe the additional details of this packet, you see**Payload type: ITU-T G.711 PCMA (8)**under Real-Time Transport Protocol.

```
> User Datagram Protocol, Src Port: 4374, Dst Port: 4376
v Real-Time Transport Protocol
  > [Stream setup by SDP (frame 23)]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    0... .... = Marker: False
    Payload type: ITU-T G.711 PCMA (8)
    Sequence number: 52731
```

RTP Details of the Packet

DTMF Packet

The snippet depicts a DTMF packet, highlighted in blue. You can see digit 6 was pressed as a DTMF input.



DTMF Event 6 Pressed

If you observe the additional details of this packet, you can see**Payload type: telephone-event (96)**under Real-Time Transport Protocol.

```
> User Datagram Protocol, Src Port: 4376, Dst Port: 4376
v Real-Time Transport Protocol
  > [Stream setup by SDP (frame 21)]
    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 (96)
```

Payload Type of the Same Packet

96 is the payload for in-band DTMF. Range: 96-127.

Related Information

- DTMF Events Through SIP Signaling
- DTMF Commands For Video Device Enabled Webex Meetings
- Configure DTMF Relay on CUBE