识别数据包捕获中的DTMF事件

目录

简介

本文档介绍如何识别数据包捕获中的双音多频(DTMF)事件。

先决条件

要求

Cisco 建议您了解以下主题：

- Webex Control Hub
- 在Webex中呼叫(Unified CM)
- DTMF

使用的组件

本文档中的信息基于以下软件和硬件版本：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

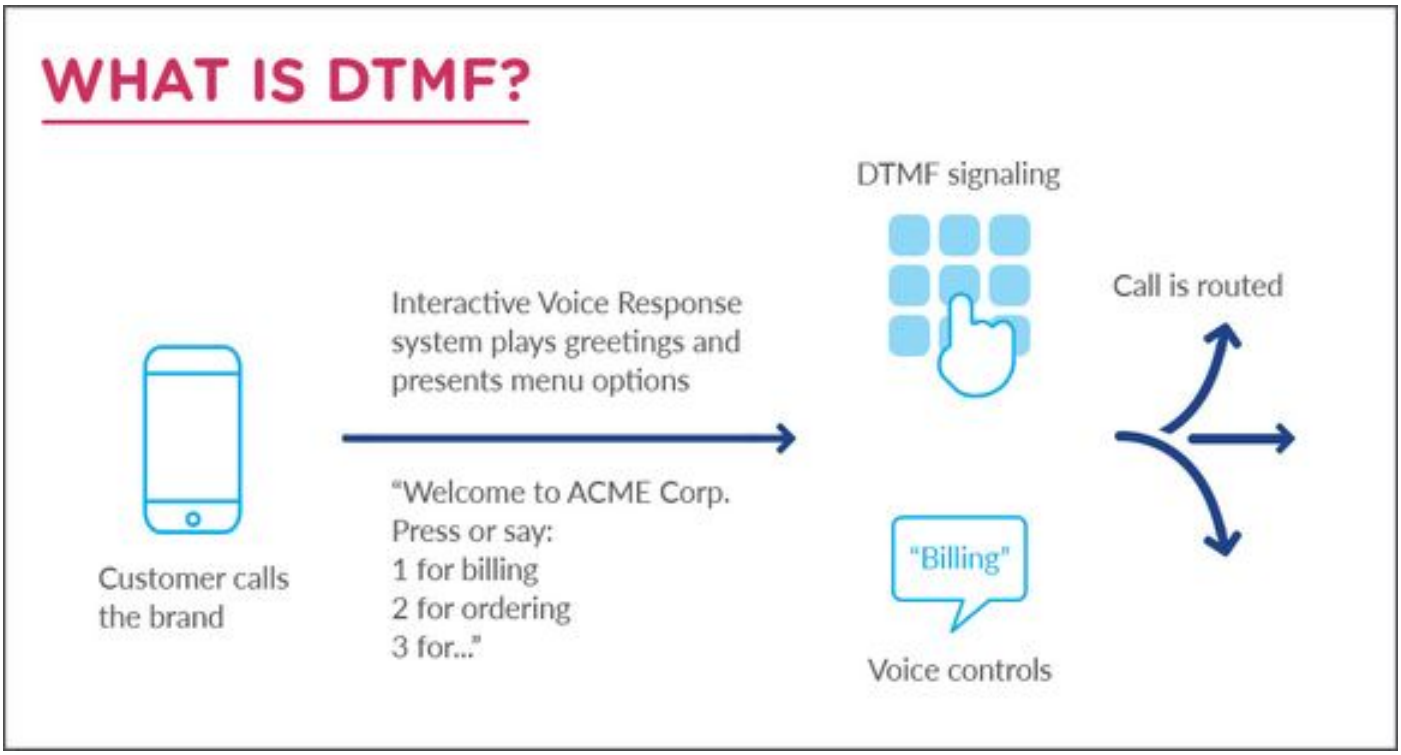
始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文概述了如何使用Wireshark识别数据包捕获中的双音多频(DTMF)事件。在Webex(Unified CM)中使用呼叫时，呼叫内正在传递DTMF事件。 该呼叫未显示任何异常行为或错误消息。在此测试呼叫期间，数字6、7、8、9、1、2和3按顺序作为DTMF输入。

什么是DTMF?

双音多频(DTMF)是按下号码时电话生成的声音/音调。DTMF用于控制自动化设备并传达用户意图，例如他们希望拨打的号码。每个按键在特定频率上有两个音调。



DTMF流程图

从1970年代末到1980年代初，DTMF技术成为联系中心的范式转变。首次通过选择正确的菜单选项，主叫方可以完成自助服务，从而减少平均处理时间和错误路由。

在1990年代后期，引入了语音指导对话。现在，主叫方可以说“帐单”或“一个”，而不是按数字。对于自助服务来说，这绝对是更好的免提选择。

但在过去几十年里，情况发生了很大变化。

企业不断发展。对于现代企业而言，电话是众多与您沟通的渠道之一。他们致力于通过所有通信渠道（网络、移动、社交媒体和电话）提供最先进的技术和您的体验。

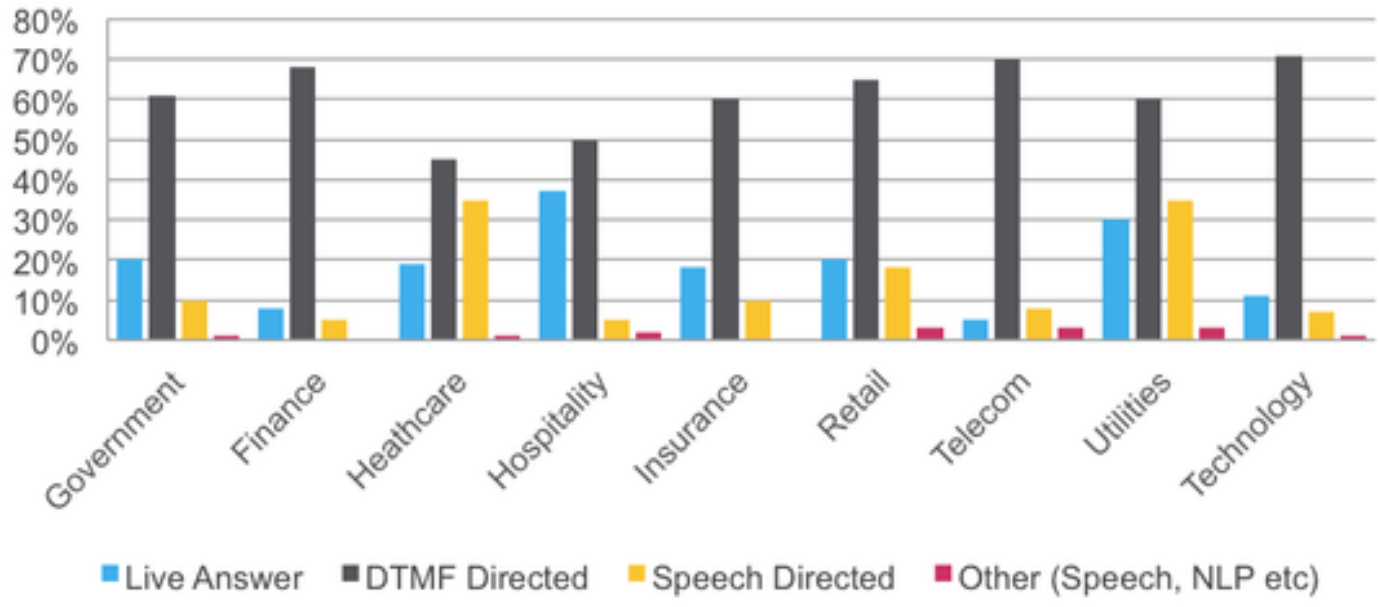
当今的技术精通环境需要跨所有渠道提供无缝体验。现代消费者比他们的前辈更敢于直言不讳，对

他们眼中的品牌非常自豪。因此，过时的客户体验或不良的客户体验会直接影响品牌忠诚度。

客户服务不断发展。作为这两种转变的共同结果，客户服务在过去十年发生了转变。它不再是事后的想法，而是深深植根于企业的方方面面。对客户着迷是许多领先企业的关键竞争优势，它是新的营销方式。

为什么一些品牌仍在使用DTMF技术？

DTMF定向对话和语音定向对话仍然是行业垂直市场中呼叫处理的主要技术选择。



跨行业的呼叫处理技术

DTMF如何工作？

DTMF技术的工作原理是让听筒按特定频率生成声音，然后在键盘上按下按钮时在电话线路上播放这些声音。电话线路另一端的设备会侦听特定声音并将其解码为命令。

DTMF使用音频频率，因此按键可用于播放可识别的旋律。由于每个按钮会生成两个音调，而且它们不会直接与标准音符对齐，因此它并不是一个确切的关联。

DTMF指定八个不同的音调，分为高音组和低音组。每个按键对应于两个音调（因此称为双音），一个来自高音组，一个来自低音组。这允许总共16个密钥。

这些键被指定为0到9、*（星号或星号）、#（井号、散列或章鱼）和字母A到D。大多数消费者电话一般不使用字母键，且省略字母键。电信业为每把钥匙选择了两个同时发出的声音，以避免人声触发系统的可能性。

DTMF frequencies

DIGIT	LOW FREQUENCY	HIGH FREQUENCY
1	697 Hz	1209 Hz
2	697 Hz	1336 Hz
3	697 Hz	1477 Hz
4	770 Hz	1209 Hz
5	770 Hz	1336 Hz
6	770 Hz	1477 Hz
7	852 Hz	1209 Hz
8	852 Hz	1336 Hz
9	852 Hz	1477 Hz
0	941 Hz	1336 Hz
*	941 Hz	1209 Hz
#	941 Hz	1477 Hz

DTMF频率

带内和带外信令

传统DTMF是一种带内信令系统，这意味着信号使用与语音流量相同的信道进行传输。但是，在IP语音中，DTMF信号可以在带内(RFC2833)或带外传输。可以使用SIP和MGCP等协议实现带外VoIP DTMF信令，从而定义用于数字传输的特殊消息类型。

标准带内方法只是简单地随音频一起传输音频，但是由于编解码器压缩、丢包或音频干扰等原因，这会导致信号不可靠。带内DTMF传输通常仅在使用未压缩的G.711编解码器时才可靠。 如果使用G.729或G.723，信令通常由于压缩而失败。

带内DTMF中继机制由RFC2833定义。DTMF音频/声音在创建媒体后使用RTP流发送。您可以按负载类型区分DTMF与音频。

通常，我们看到带内DTMF的有效负载类型是101。数字必须在96-127范围内。

带外DTMF

带外DTMF传输涉及与主语音流分开发送DTMF音，通常使用单独的信令信道。此方法提供了可靠性，并且比带内DTMF更安全，因为它将DTMF数据从语音流中分离出来。

带外DTMF的主要方面

独立通道：
DTMF信息不混入音频流，而是通过单独的信令信道传输。

信令协议：
带外DTMF通常依靠已建立的信令协议（如会话初始协议[SIP]、H.323等）来传输DTMF事件。

可靠的传输:
带外DTMF可以提供更可靠的DTMF音调传输，特别是在压缩编解码器上或可能影响音频质量的网络条件下。

降低复杂性:
它简化了DTMF事件的处理，因为接收端不需要从音频流中过滤DTMF音。

有些情况下，确认带内DTMF数字是否在RTP流内传输至关重要。Wireshark是验证此情况的极佳工具。此外，它还允许您检查特定数据包的负载类型。

故障排除步骤

以下是故障排除问题的步骤：

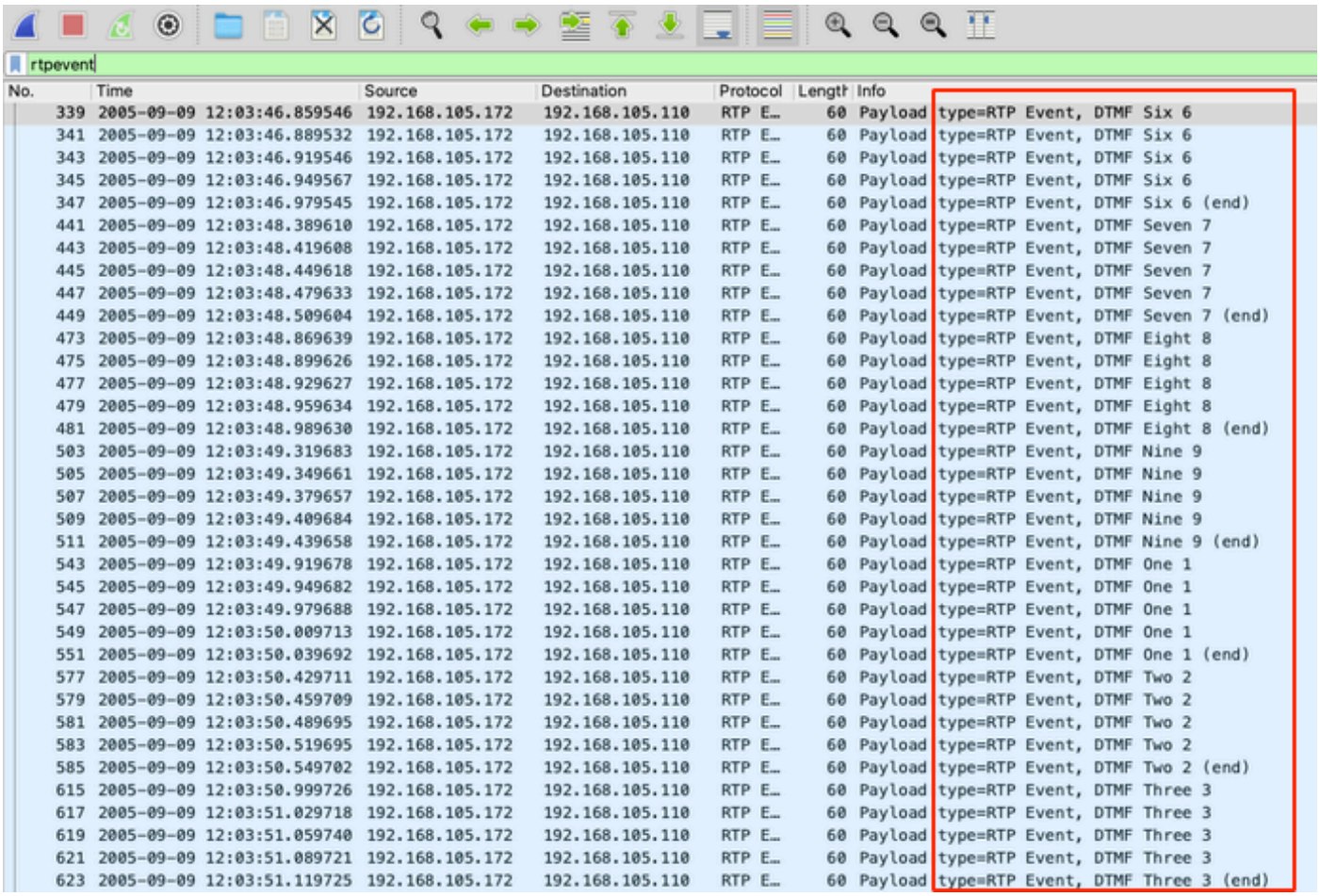
1. 在客户端PC上启用Wireshark帮助捕获流量。
2. 继续呼叫您知道已配置IVR的目的号码，以便使用DTMF。
3. 输入与IVR中听到的提示相对应的DTMF数字后，停止数据包捕获并保存文件。

在此测试呼叫期间，数字6、7、8、9、1、2和3按顺序作为DTMF输入。

4. 继续过滤数据包捕获中的DTMF数据包。
5. 使用过滤器rtpevent查看DTMF数据包。

数据包捕获分析

1.您可以看到按顺序按下数字6、7、8、9、1、2和3。



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)

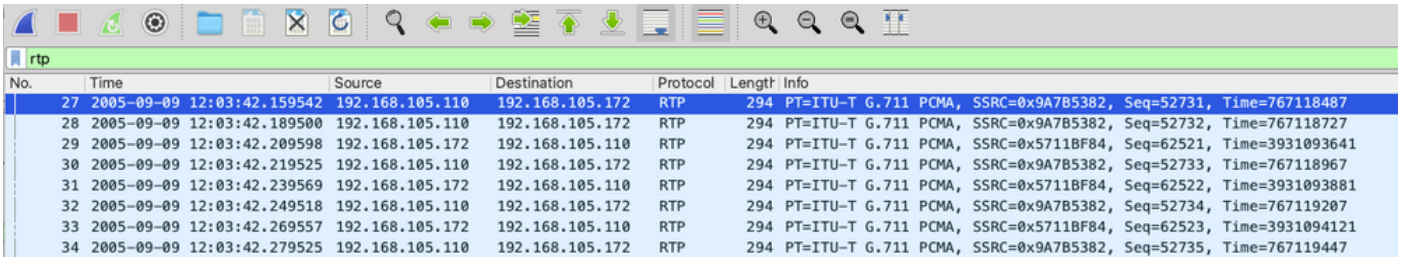
在数据包捕获中看到的DTMF事件

由于这是带内DTMF，因此事件在RTP流内发送，此时您可以看到协议RTP EVENT。负载类型显示为RTP事件。

2.您可以比较普通RTP数据包和DTMF数据包之间的负载值。

正常RTP数据包

该代码片断描绘的是正常的RTP数据包，以蓝色突出显示。



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

正常RTP数据包

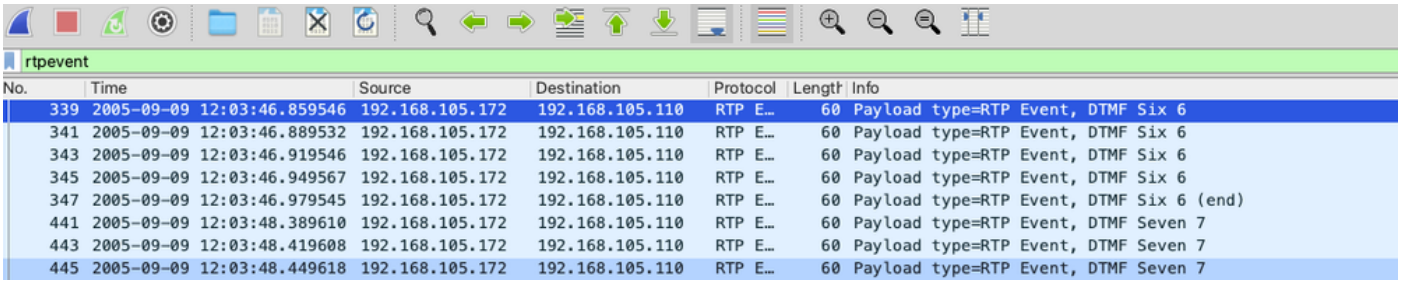
如果观察此数据包的其他详细信息，您会看到Payload type:ITU-T G.711 PCMA(8)在实时传输协议下。

```
> 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
```

数据包的RTP详细信息

DTMF数据包

该代码片断描绘了一个DTMF数据包，以蓝色突出显示。您可以看到数字6已作为DTMF输入按下。



已按下DTMF事件6

如果观察此数据包的其他详细信息，可以看到负载类型：实时传输协议下的电话事件(96)。

```
> 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)
```

相同数据包的负载类型

96是带内DTMF的负载。范围：96-127 的多播地址发送一次邻居消息。

相关信息

- 通过SIP信令的DTMF事件
- 支持视频设备的Webex会议的DTMF命令
- 在CUBE上配置DTMF中继

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。