識別資料包捕獲中的DTMF事件

目錄

簡介

必要條件

- 需求
- 採用元件

背景資訊

- 什麼是DTMF?
- 為什麼有些品牌仍然使用DTMF技術？
- DTMF如何工作？
- 帶內和帶外信令
- 帶外DTMF
  - 帶外DTMF的關鍵技術

疑難排解步驟

- 封包擷取分析
- 正常RTP資料包
- DTMF資料包

相關資訊

簡介

本文檔介紹在資料包捕獲中識別雙音多頻(DTMF)事件。

必要條件

需求

思科建議您瞭解以下主題：

- Webex Control Hub
- 在Webex中通話(Unified CM)
- DTMF

採用元件

本文中的資訊係根據以下軟體和硬體版本：

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

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

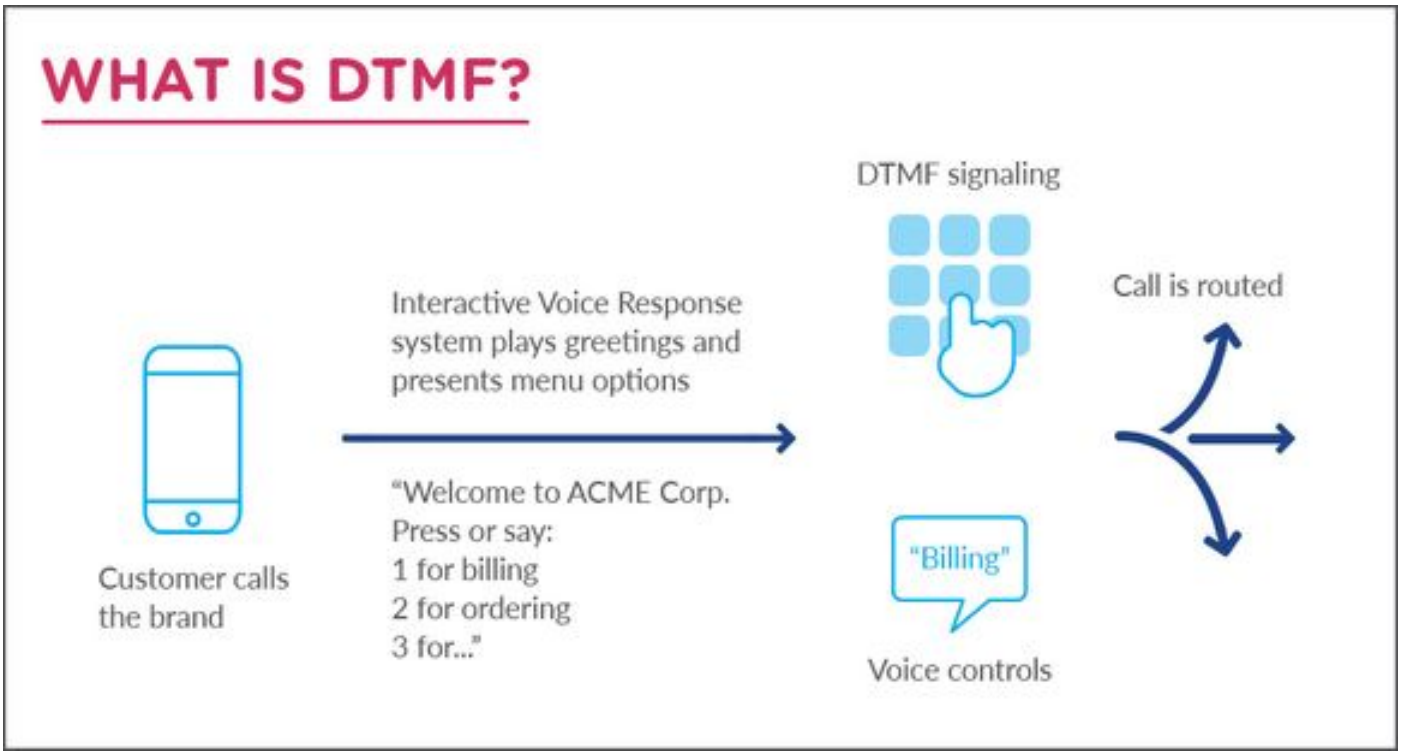
）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本文介紹如何在使用Wireshark的資料包捕獲中識別雙音多頻(DTMF)事件。在Webex(Unified CM)中使用呼叫時，在呼叫內傳遞DTMF事件。 該呼叫未顯示任何異常行為或錯誤消息。在此測試呼叫期間，數字6、7、8、9、1、2和3按順序作為DTMF輸入。

什麼是DTMF?

雙音多頻(DTMF)是按下號碼時電話產生的聲音/音調。DTMF用於控制自動化裝置並指示使用者意圖，如要撥打的號碼。每個按鍵在特定頻率上有兩個音調。



DTMF流程圖

從1970年代末到1980年代初，DTMF技術成為聯絡中心的正規化轉變。這是呼叫者首次通過選擇正確的選單選項完成自助服務，從而減少了平均處理時間和誤路由。

20世紀90年代末，引入了語音導向對話。現在，呼叫者可以說「計費」或「一個」，而不是按數字。對於自助服務來說，這絕對是一個更好的擴音選擇。

但在過去幾十年裡，情況發生了很大變化。

企業發展了。對於現代企業而言，電話是用來與您溝通的眾多管道之一。他們致力於通過所有通訊管道（網路、移動、社群媒體和電話）提供最先進的技術和您的體驗。

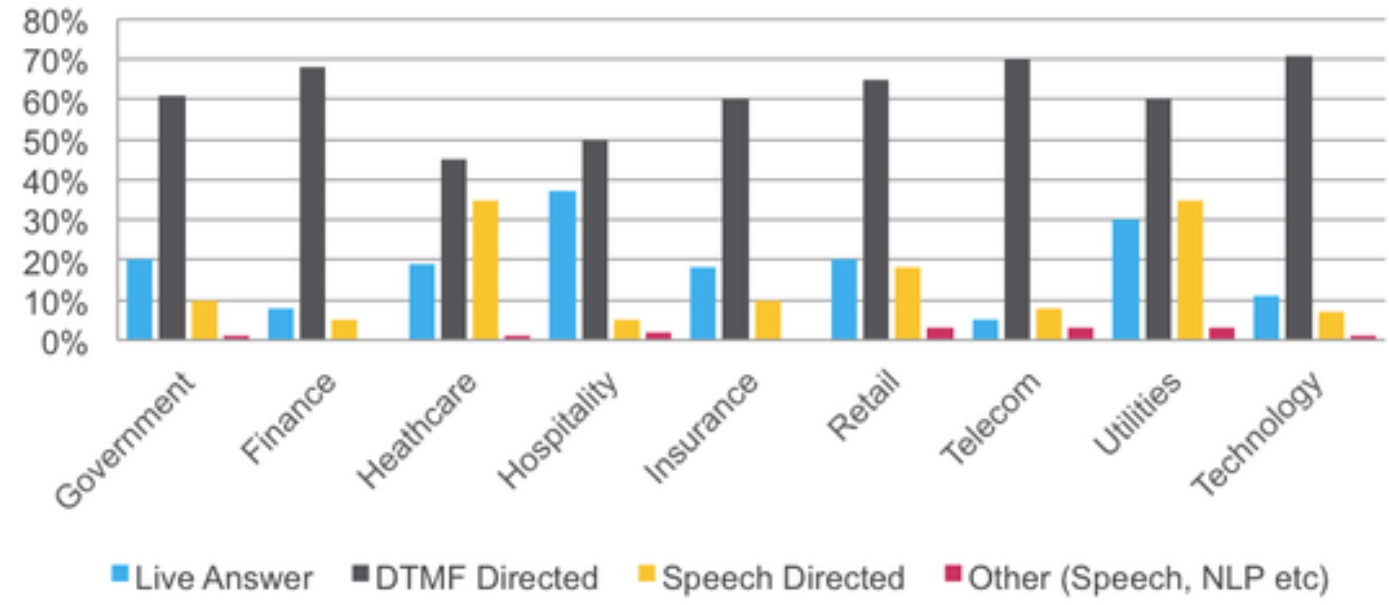
當今的技術精通環境要求所有管道都能提供無縫體驗。現代消費者遠比他們的前輩更直言不諱，他

們對自己所認同的品牌非常自豪。因此，過時的或糟糕的顧客體驗會直接影響品牌忠誠度。

客戶服務已有所發展。作為這兩種轉變的共同結果，客戶服務在過去十年發生了轉變。它不再是事後的想法，而是深深植根於企業的方方面面。對客戶著迷是許多領先企業的關鍵競爭優勢，是新的行銷策略。

為什麼有些品牌仍然使用DTMF技術？

DTMF定向對話和語音定向對話仍然是行業垂直行業呼叫處理的主要技術選擇。



跨行業的呼叫處理技術

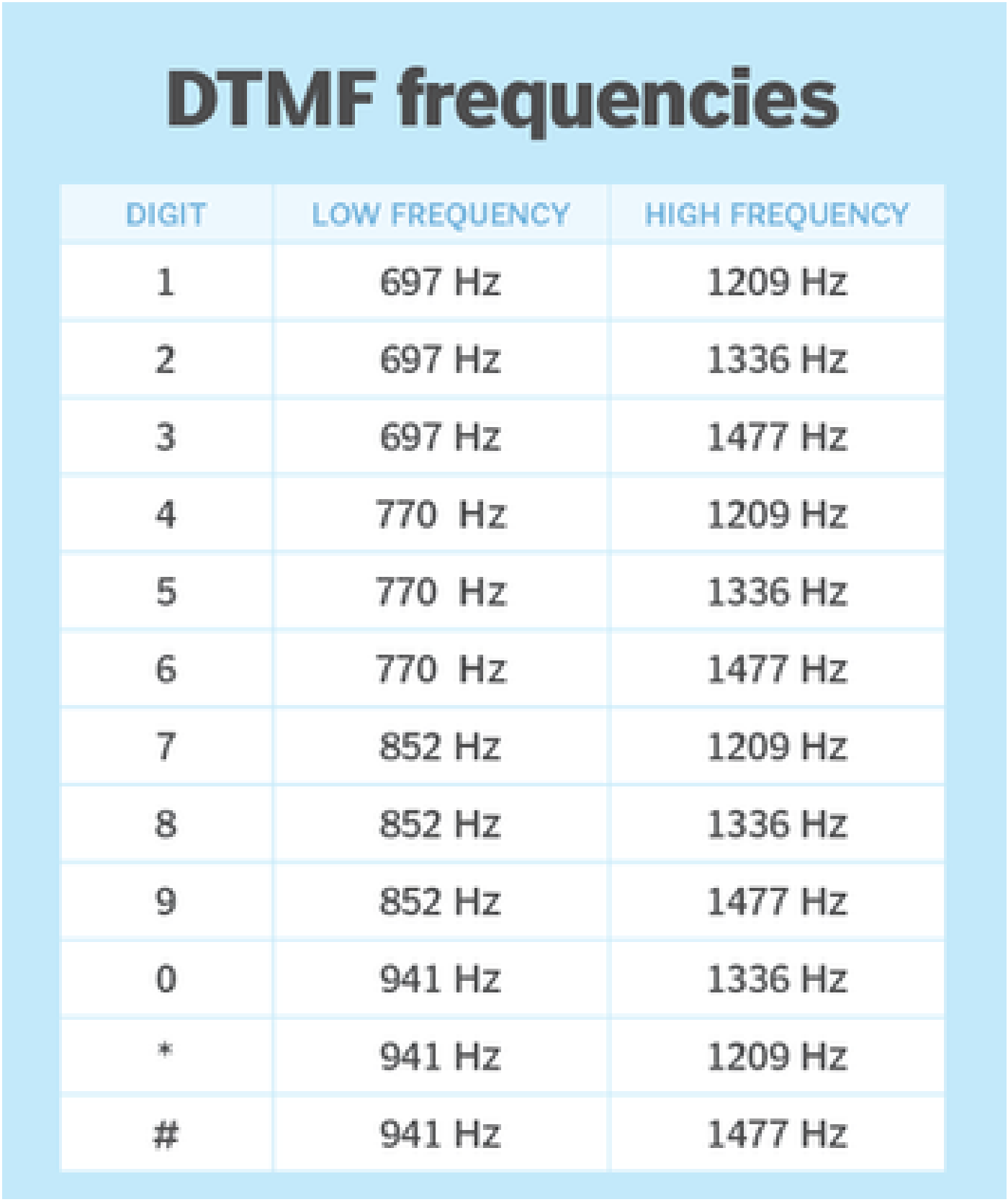
DTMF如何工作？

DTMF技術的工作原理是讓聽筒在特定頻率生成聲音，然後在小鍵盤上按下一個按鈕時在電話線上播放這些聲音。電話線路另一端的裝置會偵聽特定聲音，並將它們解碼為命令。

DTMF使用音訊頻率，因此可以使用按鍵來播放可識別的旋律。由於每個按鈕都會產生兩個音調，而且它們不會直接與標準音符對齊，因此它並不是一個確切的關聯。

DTMF指定八個不同的音調，分為高組和低組。每個按鍵對應兩個音調（因此稱為雙音調），一個來自高音組，一個來自低音組。這樣可提供16個金鑰。

這些鍵被指定為0到9、*（星號或星號）、#（井號、雜湊或章形符號）和字母A到D。大多數消費者電話不使用字母鍵並省略。電信業為每個按鍵選擇兩個同時音調，以消除人類語音觸發系統的可能性。



DTMF頻率

帶內和帶外信令

傳統的DTMF是一種帶內信令系統，這意味著訊號使用與語音流量相同的通道進行傳輸。但在IP語音中，DTMF訊號可以在頻內(RFC2833)或頻外傳輸。可以使用SIP和MGCP等協定實現帶外VoIP DTMF信令，其中為數位傳輸定義了特殊消息型別。

標準帶內方法只是將音調與音訊一起傳輸，但是這會導致由於編解碼器壓縮、丟包或音訊干擾而導致的訊號不可靠。通常只有在使用未壓縮的G.711編解碼器時，帶內DTMF傳輸才是可靠的。 如果使用G.729或G.723，信令通常由於壓縮而失敗。

帶內DTMF中繼機制由RFC2833定義。建立媒體後，使用RTP流傳送DTMF音訊/聲音。您可以按負載型別區分DTMF與音訊。

通常，我們看到帶內DTMF的有效負載型別是101。數字必須在96-127範圍內。

帶外DTMF

帶外DTMF傳輸涉及獨立於主語音流傳送DTMF音，通常使用單獨的信令通道。由於將DTMF資料從語音流中分離出來，因此這種方法提供了可靠性，並且比帶內DTMF更安全。

帶外DTMF的關鍵技術

獨立通道：
DTMF資訊不混合到音訊流中，而是通過單獨的信令通道傳輸。

訊號通訊協定：
帶外DTMF通常依靠已建立的信令協定(如會話初始協定(SIP)、H.323等)來傳輸DTMF事件。

可靠傳輸：
帶外DTMF可以提供更可靠的DTMF音調傳輸，特別是在壓縮編解碼器上或可能影響音訊品質的網路條件下。

降低複雜性：
由於接收端不需要從音訊流中過濾DTMF音，因此簡化了DTMF事件的處理。

有些情況下，確認帶內DTMF數字是否在RTP流內傳輸至關重要。Wireshark是驗證這一情況的絕佳工具。此外，還允許您檢查特定資料包的負載型別。

疑難排解步驟

以下是疑難排解問題的步驟：

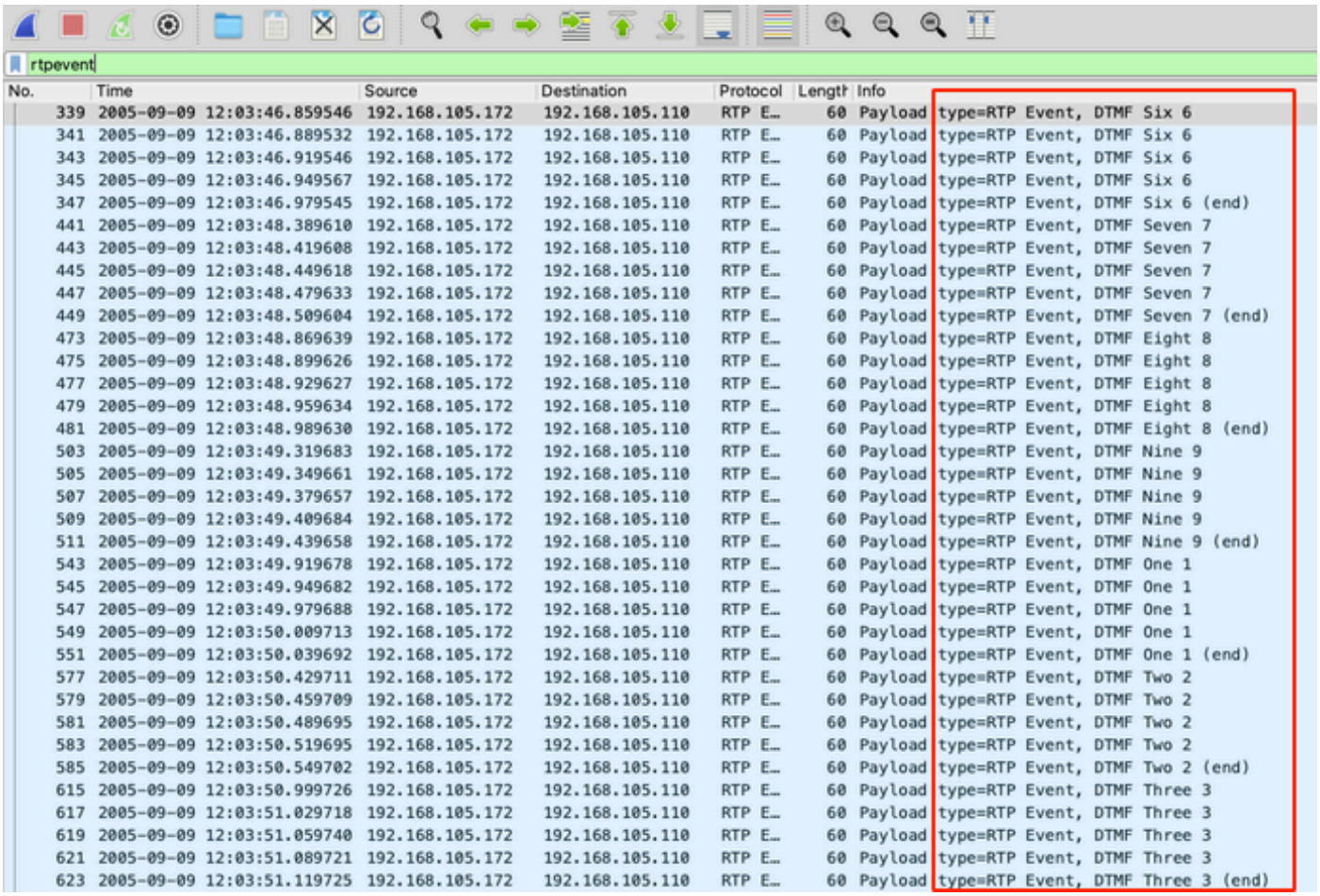
1. 在客戶端PC上啟用Wireshark幫助捕獲流量。
2. 繼續撥打您知道已配置IVR的目標號碼，以便使用DTMF。
3. 輸入與IVR中聽到的提示相對應的DTMF數字後，停止資料包捕獲並儲存檔案。

在此測試呼叫期間，數字6、7、8、9、1、2和3按順序作為DTMF輸入。

4. 繼續過濾資料包捕獲中的DTMF資料包。
5. 使用過濾器rtpevent檢視DTMF資料包。

封包擷取分析

1.您可以看到數字6、7、8、9、1、2和3按順序。



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)

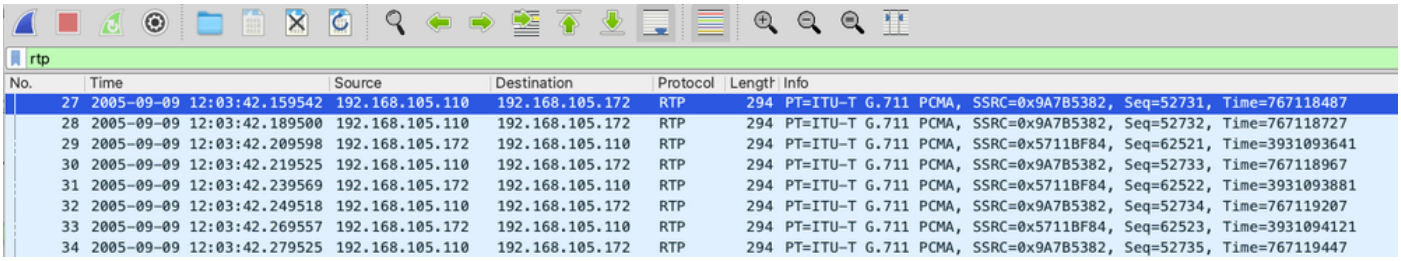
在資料包捕獲中看到的DTMF事件

由於這是帶內DTMF，因此事件在RTP流中傳送，此時您可以看到協定RTP EVENT。負載型別顯示為RTP事件。

2.您可以比較普通RTP資料包和aDTMF資料包之間的負載值。

正常RTP資料包

片段描繪的是以藍色突出顯示的正常RTP資料包。



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資料包

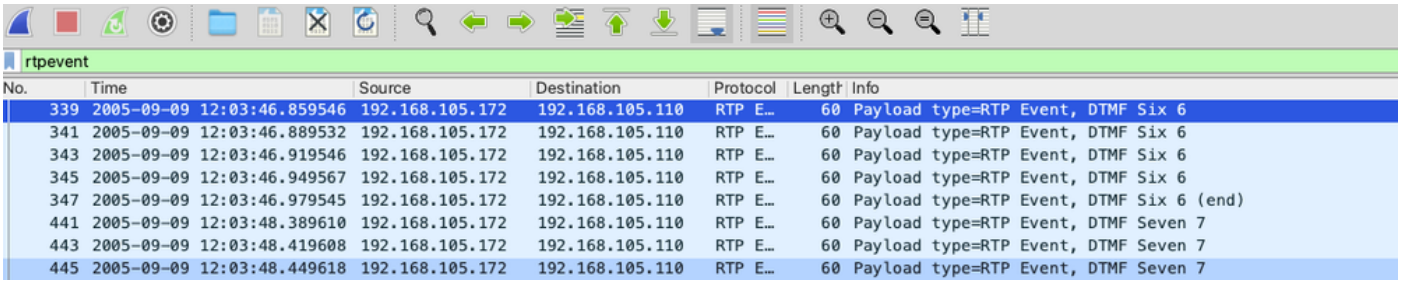
如果您觀察到此封包的額外詳細資訊，會看到Payload type:即時傳輸協定下的ITU-T G.711 PCMA(8)。

```
> 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
```

資料包的RTP詳細資訊

DTMF資料包

該片段描繪了一個DTMF資料包，以藍色突出顯示。您可以看到數字6已作為DTMF輸入按下。



已按下DTMF事件6

如果您觀察到此封包的更多詳細資訊，可以看到Payload type:即時傳輸協定下的電話事件(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)
```

相同封包的負載型別

96是帶內DTMF的有效負載。範圍：96-127 .

相關資訊

- 通過SIP信令的DTMF事件
- 用於支援影片裝置的Webex會議的DTMF命令
- 在CUBE上配置DTMF中繼

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。