

在語音和影片呼叫的Wireshark中解密RTP流以進行丟包分析

目錄

[簡介](#)

[問題](#)

簡介

本文說明如何破解即時流(RTP)流，以便在語音和影片呼叫的Wireshark中進行資料包丟失分析。您可以使用Wireshark過濾器來分析在呼叫的源和目標處或靠近源處捕獲的同步資料包。當懷疑網路丟失時，您必須排除音訊和影片品質問題，這一點很有用。


問題

此示例使用此呼叫流：

IP電話A (中央站點A) > 2960 switch > Router > WAN router (中央站點) > IPWAN > WAN router (站點B) > Router > 2960 > IP電話B

在此方案中，遇到的問題是從IP電話A到IP電話B的影片呼叫會導致從中心站點A到分支站點B的影片品質變差，其中中心站點品質較好，但分支站點出現問題。

檢視分支IP電話的流統計資料中的接收方丟失的資料包：

		<h2>Streaming Statistics</h2> <p>Cisco IP Phone CP-8941(SEP00077ddfbe65)</p>	
Device Information	Remote Address	192.168.10.146/20568	
Network Setup	Local Address	192.168.207.231/20808	
Network Statistics	Start Time	00:00:00	
Ethernet Information	Stream Status	Not Ready	
Network	Host Name	SEP00077ddfbe65	
Device Logs	Sender Packets	4745	
Console Logs	Sender Octets	3144928	
Core Dumps	Sender Codec	H264	
Status Messages	Sender Reports Sent	16	
Debug Display	Sender Report Time Sent	11:19:34	
Streaming Statistics	Rcvr Lost Packets	199	
Stream 1	Avg Jitter	40	
Stream 2	Rcvr Codec	H264	
	Rcvr Reports Sent	1	
	Rcvr Report Time Sent	11:18:14	
	Rcvr Packets	4675	
	Rcvr Octets	3113320	
	MOS LQK	0.0000	
	Avg MOS LQK	0.0000	
	Min MOS LQK	0.0000	
	Max MOS LQK	0.0000	
	MOS LQK Version	0.9500	
	Cumulative Conceal Ratio	0.0000	
	Interval Conceal Ratio	0.0000	
	Max Conceal Ratio	0.0000	
	Conceal Secs	0	
	Severely Conceal Secs	0	
	Latency	389	
	Max Jitter	50	
	Sender Size	0 ms	

解決方案

品質僅在分支站點上可見，並且由於中心站點看到的是一個好的影象，因此從中心站點到分支站點的流似乎正在通過網路丟失資料包。

IP addressing scheme

Central IP phone: 192.168.10.146

Central Gateway: 192.168.10.253

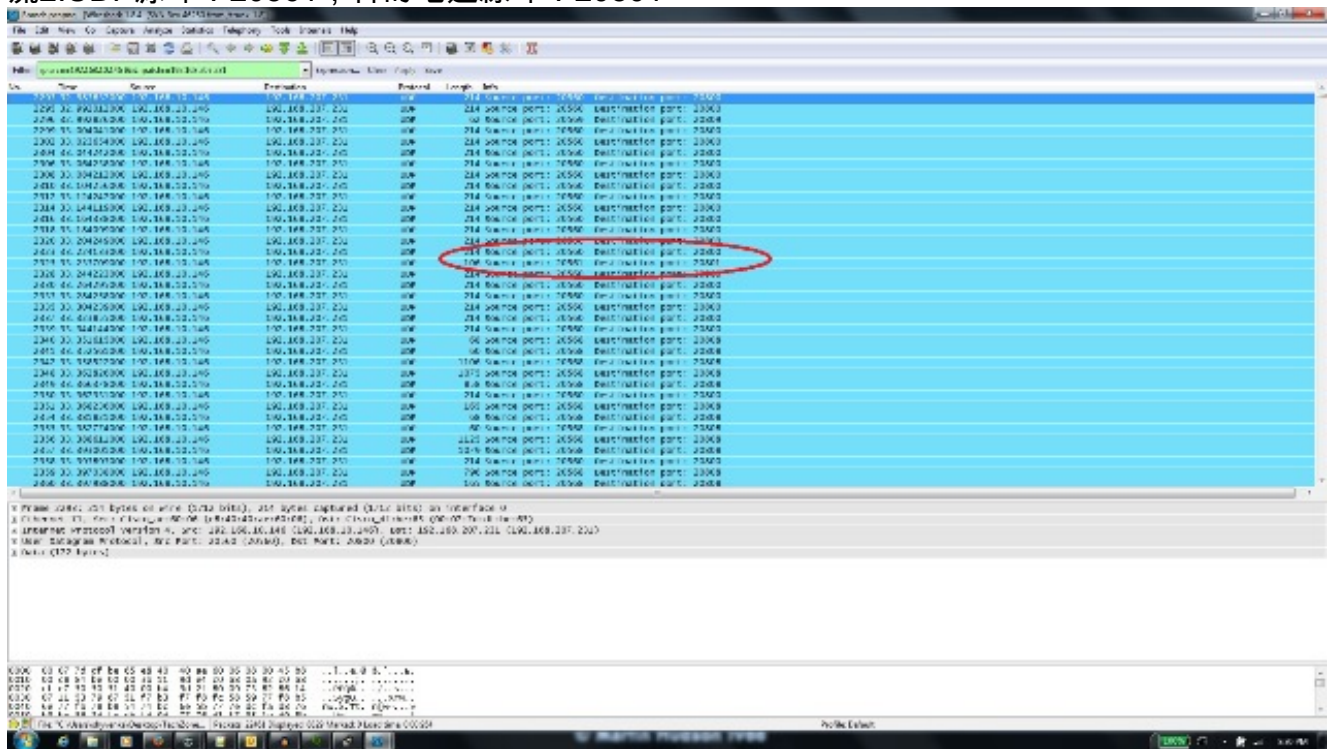
Central WAN router: 192.168.10.254
Branch WAN router: 192.168.206.210
Branch Gateway: 192.168.206.253
Branch IP phone: 192.168.207.231

資料包捕獲在中央和分支WAN路由器上進行，WAN丟棄這些資料包。關注從中央IP電話(192.168.10.146)到分支IP電話(192.168.207.231)的RTP流。如果WAN丟棄從中央WAN路由器到分支WAN路由器的資料流上的資料包，此資料流會丟失分支WAN路由器上的資料包。請使用wireshark中的過濾器選項來隔離問題：

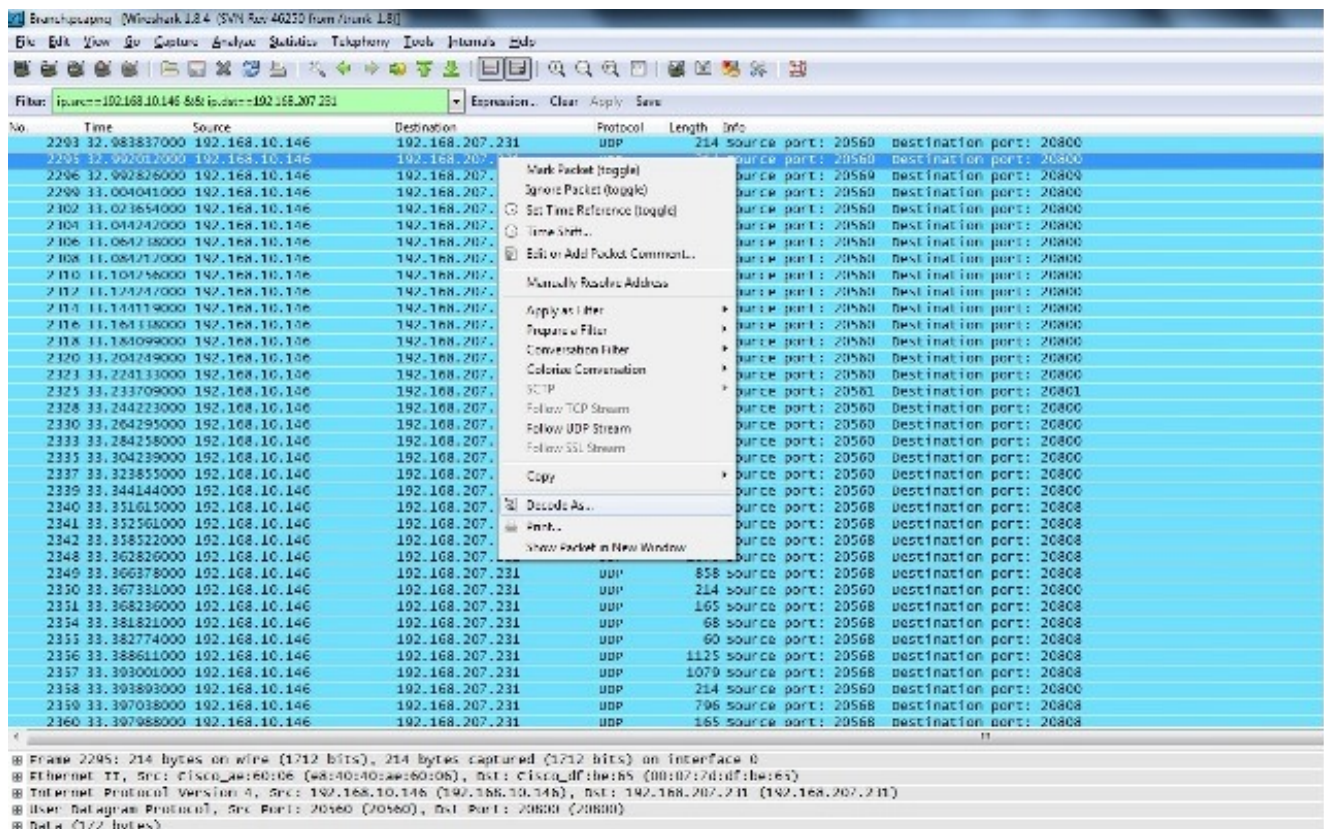
1. 在wireshark中開啟捕獲。
2. 使用過濾器ip.src==192.168.10.146 && ip.dst==192.168.207.231。這將過濾掉從中央IP電話到分支IP電話的所有UDP資料流。
3. 僅對分支側捕獲執行分析，但請注意，還必須對集中捕獲執行這些步驟。
4. 在此螢幕截圖中，UDP流在源IP地址和目標IP地址之間過濾，並包含兩個UDP流（由UDP埠號區分）。這是一個影片呼叫，因此有兩個流：音訊和影片。在本示例中，兩個流是：

流1 :UDP源埠：20560，目的地連線埠：20800

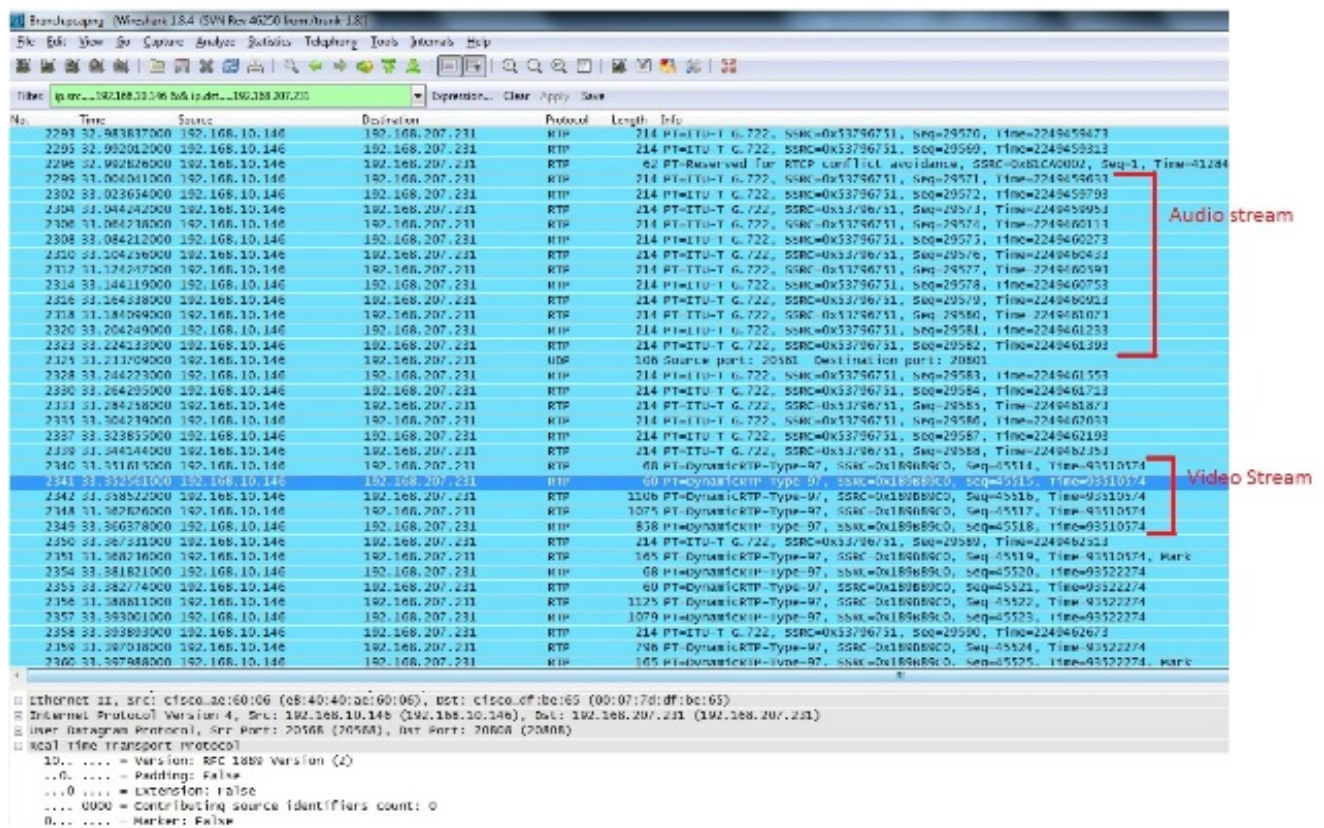
流2:UDP源埠：20561，目的地連線埠：20801



5. 從其中一個流中選擇資料包，然後按一下右鍵該資料包。
6. 選擇Decode As...並鍵入RTP。
7. 按一下「Accept」和「Ok」，將串流解碼為RTP。

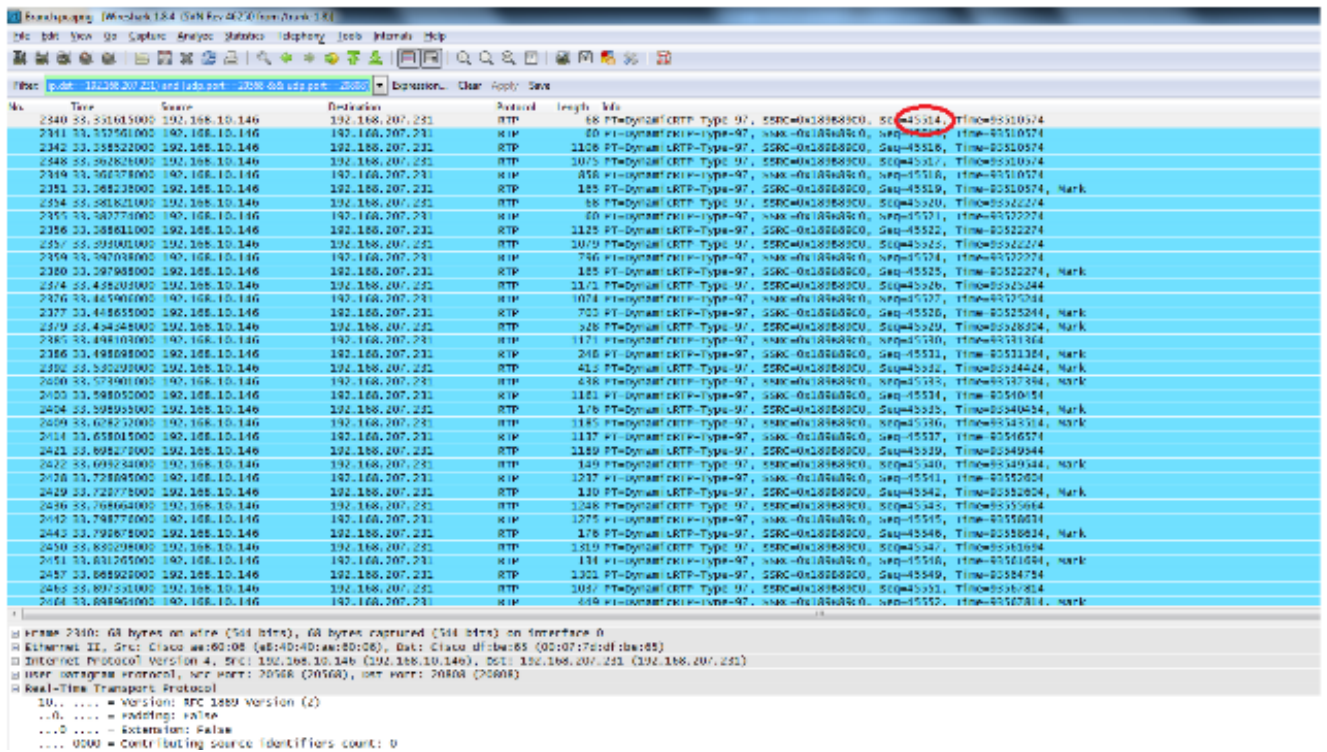


剩下的一個流被解碼為RTP，另一個流被解碼為未編碼的UDP。



8. 從未編碼流中選擇一個資料包，並將其解碼為RTP。這會將音訊和影片流解碼為RTP。

註：音訊流採用G.722編解碼器格式，Dynamic-RTP-97負載型別表示影片RTP流。

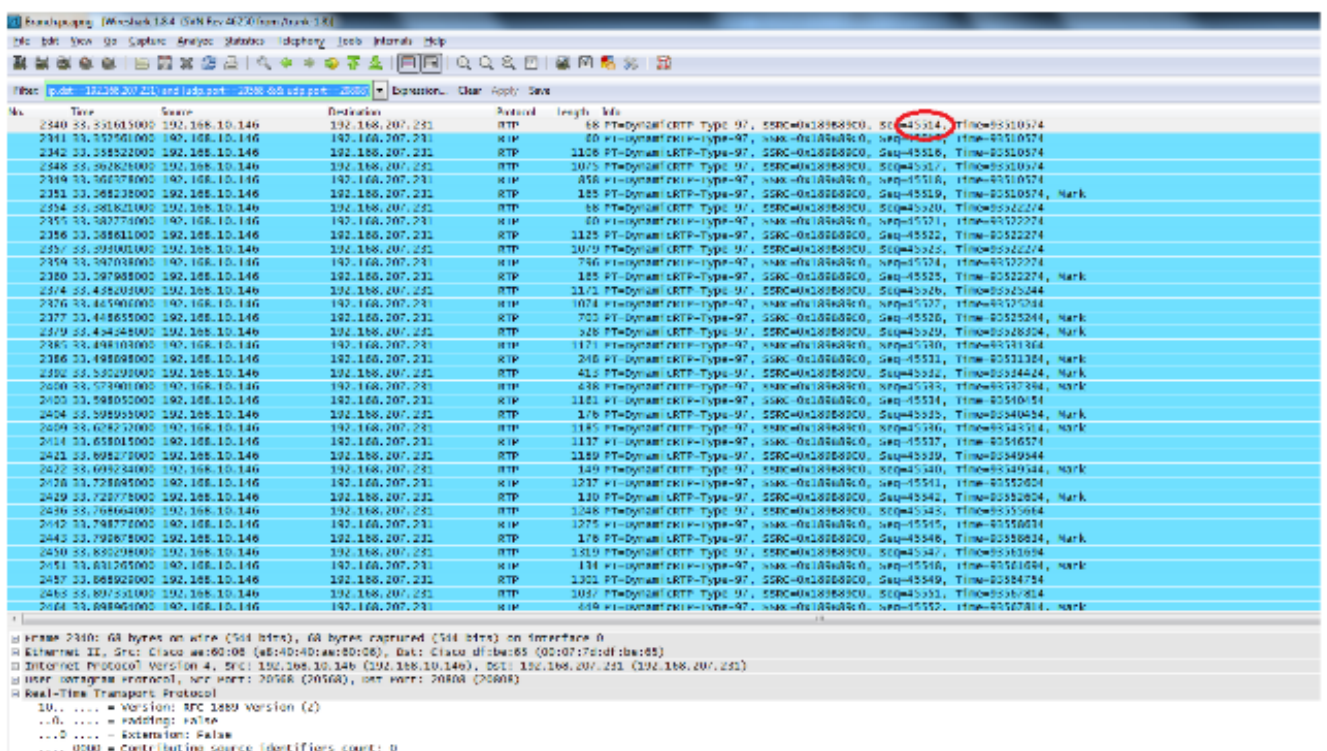


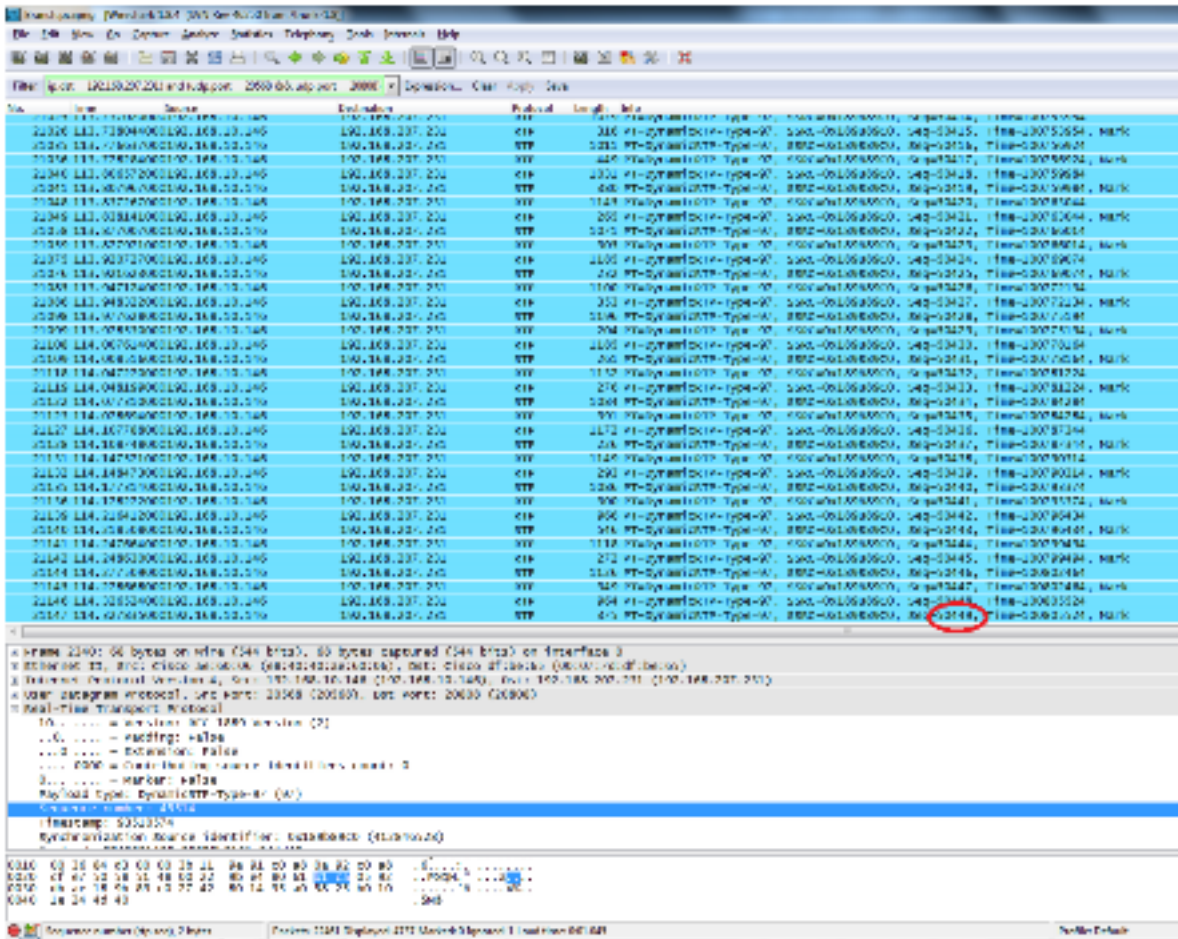
現在問題只在於影片品質。關注影片RTP流，並使用此流的UDP埠號過濾掉其他流。

9. 在Wireshark實用模式的底部窗格中選擇一個顯示UDP埠資訊的資料包，以檢視埠號。在上一個螢幕截圖中，選擇了來自影片流的一個資料包，您可以在底部窗格中看到Src Port(20568)和Dst port(20808)資訊。

提示：使用以下過濾器：(ip.src==192.168.10.146和& ip.dst==192.168.207.231)&(udp.port eq 20568和udp.port eq 20808)。您只能看到此螢幕截圖中所示的影片RTP流。

附註：記下此流的第一個和最後一個RTP序列號。





第一個RTP序列號是45514而最後一個RTP50449號是過濾出的影片RTP流。

- 10. 確保兩個捕獲中都有第一個和最後一個RTP序列號資料包（例如，中央捕獲和分支捕獲），並注意兩個捕獲上流的SSRC相同。
- 11. 最佳化過濾器以僅匹配第一個和最後一個RTP流之間的資料包。

序列號用於最佳化資料流，以防捕獲不是同時捕獲，而是稍微延遲。

附註：分支站點可能在IP後啟動一些序45514。

- 12. 選擇開始和結束序列號。這些封包同時存在於擷取和縮小篩選條件中，以僅顯示開始RTP序列號和結束RTP序列號之間的那些封包。此方法的篩選器為：

```
(ip.src==192.168.10.146 && ip.dst==192.168.207.231) && (udp.port eq 20568 and udp.port eq 20808) && ( rtp.seq>=44514 && rtp.seq<=50449 )
```

同時進行擷取時，兩個擷取的時刻開始或結束時不會遺漏封包。如果您看到其中一個擷取在開始/結束時不包含幾個封包，請使用兩個封包中遺失的擷取中的第一個序號或最後一個序號，來精簡兩個擷取的篩選條件。觀察在相同序列號（RTP序列號範圍）之間的兩個點捕獲的資料包。

應用過濾器時，您會在中心站點和分支站點看到以下內容：

中心站點：

No.	Time	Source	Destination	Protocol	Length	Info
14572	37.720005	192.168.10.146	192.168.207.231	RTP	248	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45531, Time=93531364, Mark
14591	37.749752	192.168.10.146	192.168.207.231	RTP	313	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45532, Time=93534426, Mark
14609	37.779990	192.168.10.146	192.168.207.231	RTP	418	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45533, Time=93537490, Mark
14619	37.819992	192.168.10.146	192.168.207.231	RTP	1161	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45534, Time=93540454, Mark
14620	37.819993	192.168.10.146	192.168.207.231	RTP	176	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45535, Time=93540454, Mark
14634	37.849993	192.168.10.146	192.168.207.231	RTP	1185	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45536, Time=93543514, Mark
14646	37.880004	192.168.10.146	192.168.207.231	RTP	1137	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45537, Time=93546574, Mark
14647	37.880004	192.168.10.146	192.168.207.231	RTP	131	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45538, Time=93546574, Mark
14666	37.919987	192.168.10.146	192.168.207.231	RTP	1189	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45539, Time=93549544, Mark
14667	37.919990	192.168.10.146	192.168.207.231	RTP	149	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45540, Time=93549544, Mark
14679	37.950012	192.168.10.146	192.168.207.231	RTP	1237	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45541, Time=93552604, Mark
14680	37.950016	192.168.10.146	192.168.207.231	RTP	130	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45542, Time=93552604, Mark
14699	37.989936	192.168.10.146	192.168.207.231	RTP	1248	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45543, Time=93555664, Mark
14700	37.989966	192.168.10.146	192.168.207.231	RTP	176	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45544, Time=93555664, Mark
14711	38.020065	192.168.10.146	192.168.207.231	RTP	1275	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45545, Time=93558634, Mark
14712	38.020067	192.168.10.146	192.168.207.231	RTP	176	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45546, Time=93558634, Mark
14724	38.050192	192.168.10.146	192.168.207.231	RTP	1314	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45547, Time=93561694, Mark
14725	38.050419	192.168.10.146	192.168.207.231	RTP	134	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45548, Time=93561694, Mark
14744	38.089989	192.168.10.146	192.168.207.231	RTP	1301	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45549, Time=93564754, Mark

Frame 14495: 88 bytes on wire (544 bits), 88 bytes captured (544 bits) on interface 0
Ethernet II, Src: Cisco_eb:13:f0 (30:e4:db:67:13:f0), Dst: Cisco_f4:d0:08 (b8:62:1f:f4:d0:08)
Internet Protocol version 4, Src: 192.168.10.146 (192.168.10.146), Dst: 192.168.207.231 (192.168.207.231)
User Datagram Protocol, Src Port: 20568 (20568), Dst Port: 20808 (20808)
Real-Time Transport Protocol

0000 b8 62 1f f4 d0 08 30 e4 db 67 13 f0 08 00 45 e8 .b....0..g....E.
0010 00 36 84 e3 00 00 3f 11 9e 91 c0 a8 0a 92 c0 a8 .6....?.....
0020 cf c7 50 58 51 48 00 22 9b 04 80 61 d1 ca 05 92 ..PROM.....
0030 db ae 18 9b 89 c0 27 42 89 14 95 a0 58 25 b9 10b.....
0040 1e 24 4d 40

File: C:\Users\shyvenka\Desktop\TechZone... Packets: 9458 Displayed 4635 Merged Ignored: 1 Load time: 1603.150 Profile: Default

分支站點：

No.	Time	Source	Destination	Protocol	Length	Info
2530	35.38674000	192.168.10.146	192.168.207.231	RTP	60	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45514, Time=93522274
2556	35.38811000	192.168.10.146	192.168.207.231	RTP	1125	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45521, Time=93522274
2557	35.39901000	192.168.10.146	192.168.207.231	RTP	1079	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45523, Time=93522274
2559	35.39703000	192.168.10.146	192.168.207.231	RTP	798	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45524, Time=93522274
2560	35.39798000	192.168.10.146	192.168.207.231	RTP	165	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45525, Time=93522274, Mark
2574	35.41820000	192.168.10.146	192.168.207.231	RTP	1173	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45528, Time=93525244
2576	35.44506000	192.168.10.146	192.168.207.231	RTP	1074	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45527, Time=93525244
2577	35.44565000	192.168.10.146	192.168.207.231	RTP	705	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45528, Time=93525244, Mark
2579	35.45434000	192.168.10.146	192.168.207.231	RTP	528	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45529, Time=93528304, Mark
2585	35.49819000	192.168.10.146	192.168.207.231	RTP	1173	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45530, Time=93531364
2586	35.49889000	192.168.10.146	192.168.207.231	RTP	248	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45531, Time=93531364, Mark
2592	35.53099000	192.168.10.146	192.168.207.231	RTP	615	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45532, Time=93534424, Mark
2400	35.57390000	192.168.10.146	192.168.207.231	RTP	438	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45533, Time=93537494, Mark
2403	35.59650000	192.168.10.146	192.168.207.231	RTP	1161	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45534, Time=93540454, Mark
2404	35.59855000	192.168.10.146	192.168.207.231	RTP	176	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45535, Time=93540454, Mark
2406	35.62832000	192.168.10.146	192.168.207.231	RTP	1185	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45536, Time=93543514, Mark
2414	35.65803000	192.168.10.146	192.168.207.231	RTP	1137	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45537, Time=93546574, Mark
2421	35.69827900	192.168.10.146	192.168.207.231	RTP	1189	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45539, Time=93549544, Mark
2422	35.69924000	192.168.10.146	192.168.207.231	RTP	149	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45540, Time=93549544, Mark
2428	35.72895000	192.168.10.146	192.168.207.231	RTP	1237	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45541, Time=93552604, Mark
2429	35.72978000	192.168.10.146	192.168.207.231	RTP	130	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45542, Time=93552604, Mark
2436	35.76864000	192.168.10.146	192.168.207.231	RTP	1248	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45543, Time=93555664, Mark
2442	35.79878000	192.168.10.146	192.168.207.231	RTP	1275	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45545, Time=93558634, Mark
2443	35.79967000	192.168.10.146	192.168.207.231	RTP	176	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45546, Time=93558634, Mark
2450	35.83079000	192.168.10.146	192.168.207.231	RTP	1314	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45547, Time=93561694, Mark
2451	35.83126500	192.168.10.146	192.168.207.231	RTP	134	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45548, Time=93561694, Mark
2457	35.86892900	192.168.10.146	192.168.207.231	RTP	1301	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45549, Time=93564754, Mark
2463	35.89731000	192.168.10.146	192.168.207.231	RTP	1037	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45551, Time=93567814, Mark
2464	35.89869000	192.168.10.146	192.168.207.231	RTP	649	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45552, Time=93567814, Mark
2470	35.92768000	192.168.10.146	192.168.207.231	RTP	1055	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45553, Time=93570784, Mark
2471	35.92952800	192.168.10.146	192.168.207.231	RTP	677	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45554, Time=93570784, Mark
2478	35.96735000	192.168.10.146	192.168.207.231	RTP	1051	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45555, Time=93573844, Mark
2479	35.96892100	192.168.10.146	192.168.207.231	RTP	392	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45556, Time=93573844, Mark

Frame 2340: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
Ethernet II, Src: Cisco_ae:10:06 (e8:40:40:1a:e:06), Dst: Cisco_df:be:65 (00:07:7d:df:be:65)
Internet Protocol version 4, Src: 192.168.10.146 (192.168.10.146), Dst: 192.168.207.231 (192.168.207.231)
User Datagram Protocol, Src Port: 20568 (20568), Dst Port: 20808 (20808)
Real-time Transport Protocol
10. = Version: RFC 1889 Version (2)
.0. = Padding: false
...0. = Extension: false
.... 0000 = contributing source identifiers count: 0
0... = Marker: false
Payload type: dynanmicRTP type 97 (97)
Sequence number: 45514
Timestamp: 93510574
Synchronization Source identifier: 0x189689c0 (417866578)
.....0x189689c0:45514:93510574:0x189689c0

0000 00 07 7d cf be 65 e8 40 40 ae 00 00 06 00 45 e8 .b....0..g....E.
0010 00 36 84 e3 00 00 3f 11 9e 91 c0 a8 0a 92 c0 a8 .6....?.....
0020 cf c7 50 58 51 48 00 22 9b 04 80 61 d1 ca 05 92 ..PROM.....
0030 db ae 18 9b 89 c0 27 42 89 14 95 a0 58 25 b9 10b.....
0040 1e 24 4d 40

File: C:\Users\shyvenka\Desktop\TechZone... Packets: 2981 Displayed 4737 Merged Ignored: 1 Load time: 0.01150 Profile: Default

請注意Wireshark實用程式底部窗格中兩個捕獲上的過濾資料包計數。Displayed計數表示與所需過濾條件匹配的資料包數。

中心站點有4,936個資料包符合開始(45514)和結束(50449)RTP序列號之間的期望過濾標準，而分支站點只有4,737個資料包。這表示丟失199個資料包。請注意，這199個資料包與本文檔開頭所示的分支端IP電話的流統計資訊中的「Rcvr Lost Pkts」計數匹配199。

這確認所有Rcvr丟失的資料包實際上是通過WAN丟棄的網路丟失。這就是在處理涉及可疑網路丟棄的音訊/影片品質問題時隔離網路中丟包點的方式。