

Decifratura del flusso RTP per l'analisi della perdita di pacchetti in Wireshark per chiamate voce e video

Sommario

[Introduzione](#)

[Problema](#)

Introduzione

Questo documento descrive il processo di decifrazione del flusso RTP (Real-Time Streaming) per l'analisi della perdita di pacchetti in Wireshark per chiamate vocali e video. I filtri Wireshark possono essere usati per analizzare acquisizioni simultanee di pacchetti all'origine o vicino alla destinazione di una chiamata. Questa funzione è utile quando è necessario risolvere problemi di qualità audio e video quando si sospetta la presenza di perdite nella rete.


Problema

In questo esempio viene utilizzato il flusso di chiamata seguente:

IP Phone A (sito centrale A) > switch 2960 > Router > router WAN (sito centrale) > IPWAN > router WAN (sito B) > Router > 2960 > IP Phone B

In questo scenario, il problema riscontrato è che le videochiamate dal telefono IP A al telefono IP B determinano una cattiva qualità video dal sito centrale A al sito di succursale B, dove il sito centrale è di buona qualità ma il lato della succursale presenta dei problemi.

Vedere i pacchetti persi dal ricevitore nelle statistiche di streaming del telefono IP della filiale:

		<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	

Soluzione

La cattiva qualità è visibile solo sul lato della filiale e, poiché il sito centrale vede una buona immagine, sembra che il flusso dal sito centrale al sito della filiale stia perdendo pacchetti sulla rete.

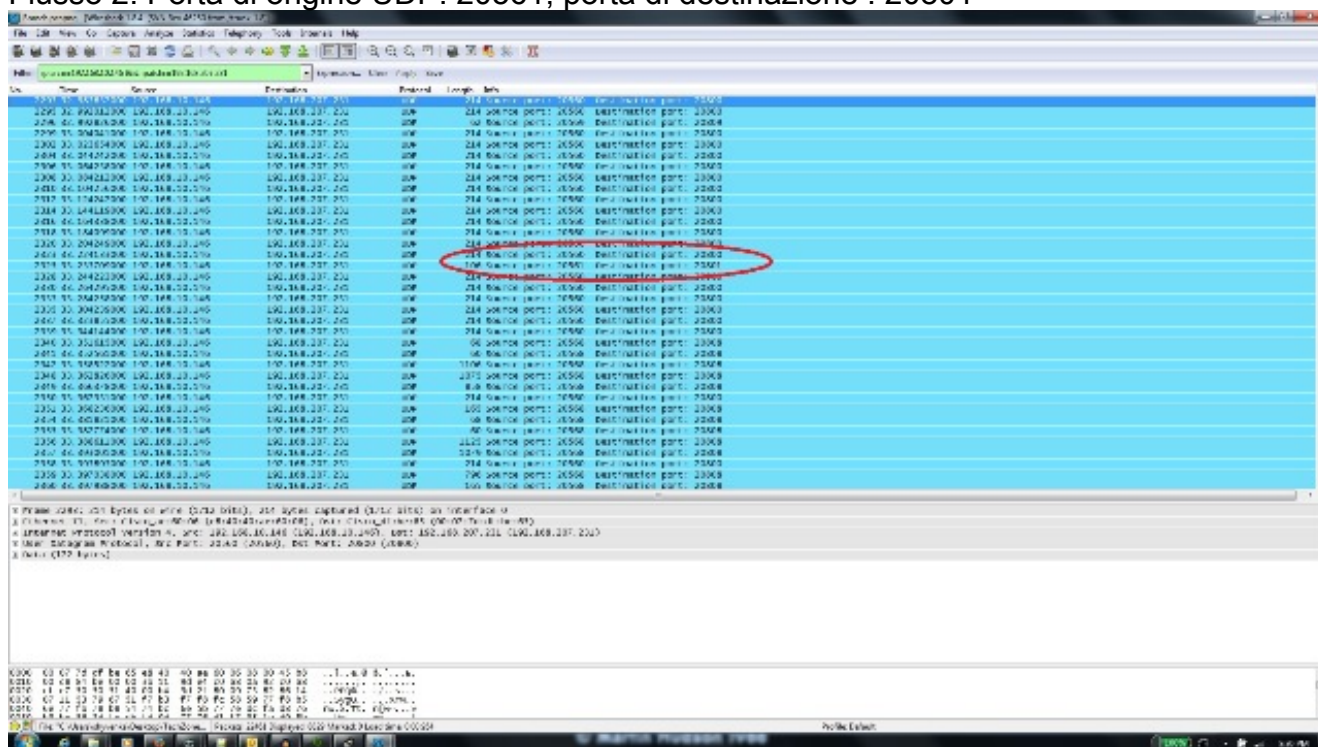
Central Gateway: 192.168.10.253
Central WAN router: 192.168.10.254
Branch WAN router: 192.168.206.210
Branch Gateway: 192.168.206.253
Branch IP phone: 192.168.207.231

I pacchetti vengono acquisiti sul router WAN centrale e di branch e la WAN scarta questi pacchetti. Mettere a fuoco il flusso RTP dal telefono IP centrale (192.168.10.146) al telefono IP della filiale (192.168.207.231). Il flusso non riceve i pacchetti sul router WAN della succursale se la WAN scarta i pacchetti sul flusso dal router WAN centrale al router WAN della succursale. Usare le opzioni di filtro in wireshark per isolare il problema:

1. Aprire la cattura in wireshark.
2. Usare il filtro ip.src==192.168.10.146 && ip.dst==192.168.207.231. In questo modo vengono esclusi tutti i flussi UDP dal telefono IP centrale al telefono IP della filiale.
3. Eseguite l'analisi solo sull'acquisizione lato diramazione, ma dovete eseguire questi passi anche per l'acquisizione centrale.
4. In questa schermata, il flusso UDP viene filtrato tra gli indirizzi IP di origine e di destinazione e contiene due flussi UDP (differenziati dai numeri di porta UDP). Questa è una videochiamata, quindi ci sono due flussi: audio e video. In questo esempio, i due flussi sono:

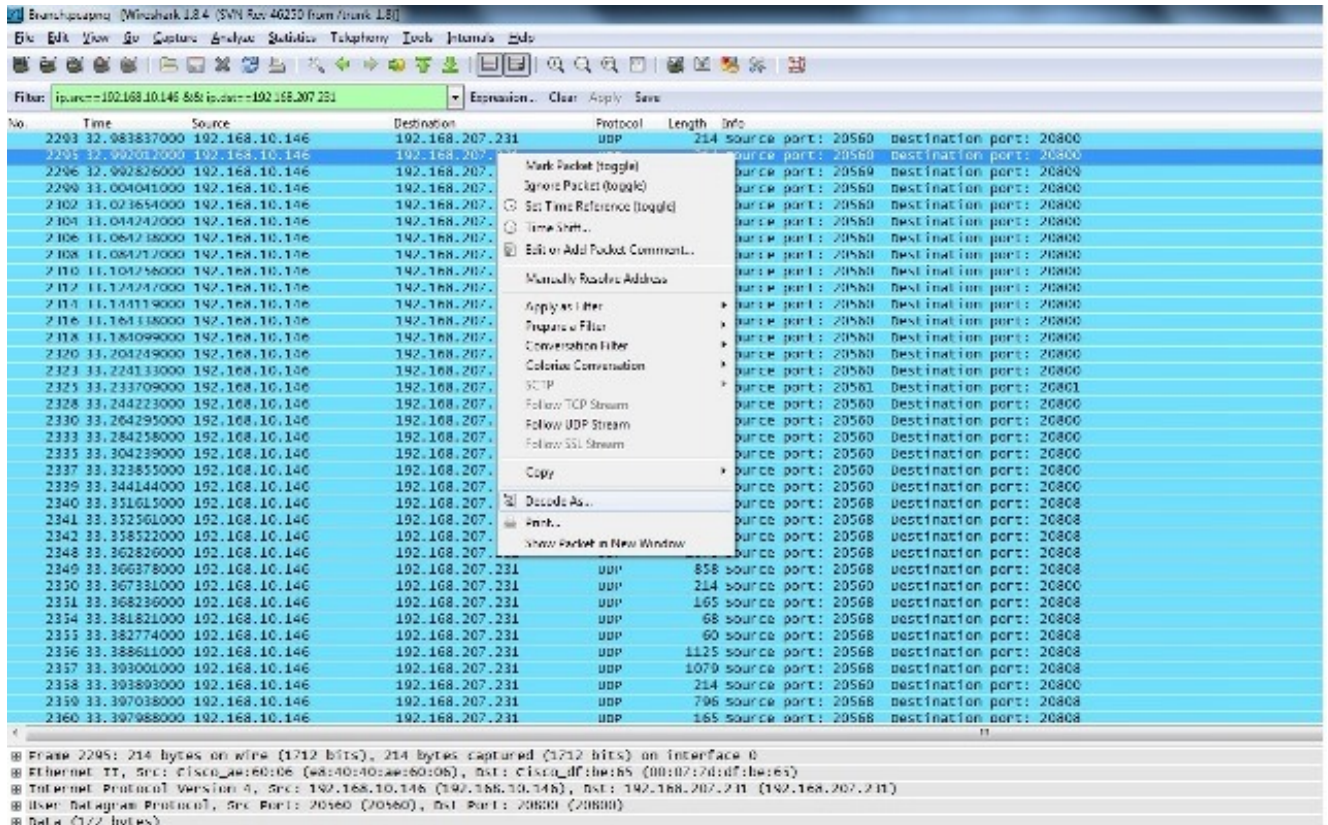
Flusso 1: Porta di origine UDP: 20560, porta di destinazione : 20800

Flusso 2: Porta di origine UDP: 20561, porta di destinazione : 20801

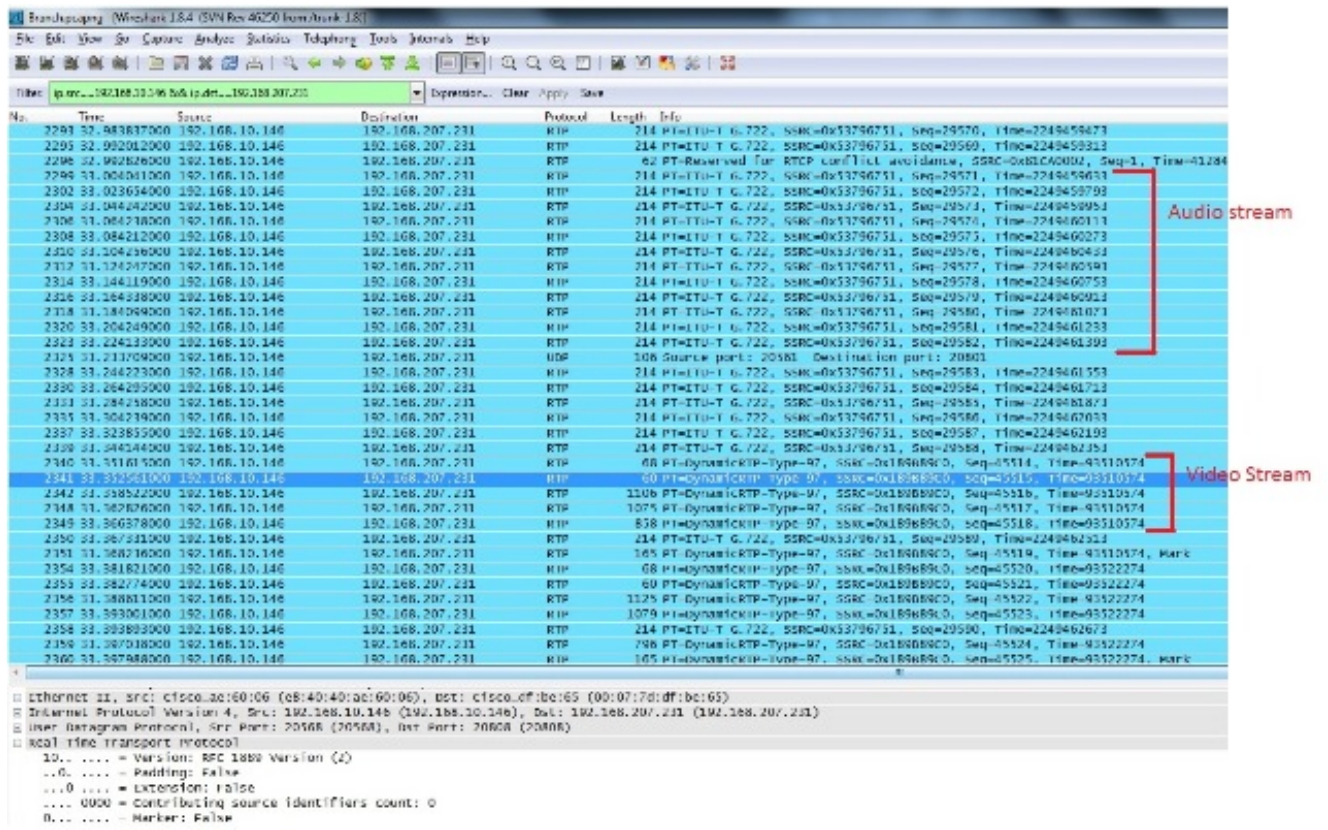


5. Selezionare un pacchetto da uno dei flussi e fare clic con il pulsante destro del mouse sul pacchetto.
6. Selezionare Decodifica con nome... e digitare RTP.

7. Per decodificare il flusso come RTP, fare clic su **Accept** (Accetto) e **Ok**.

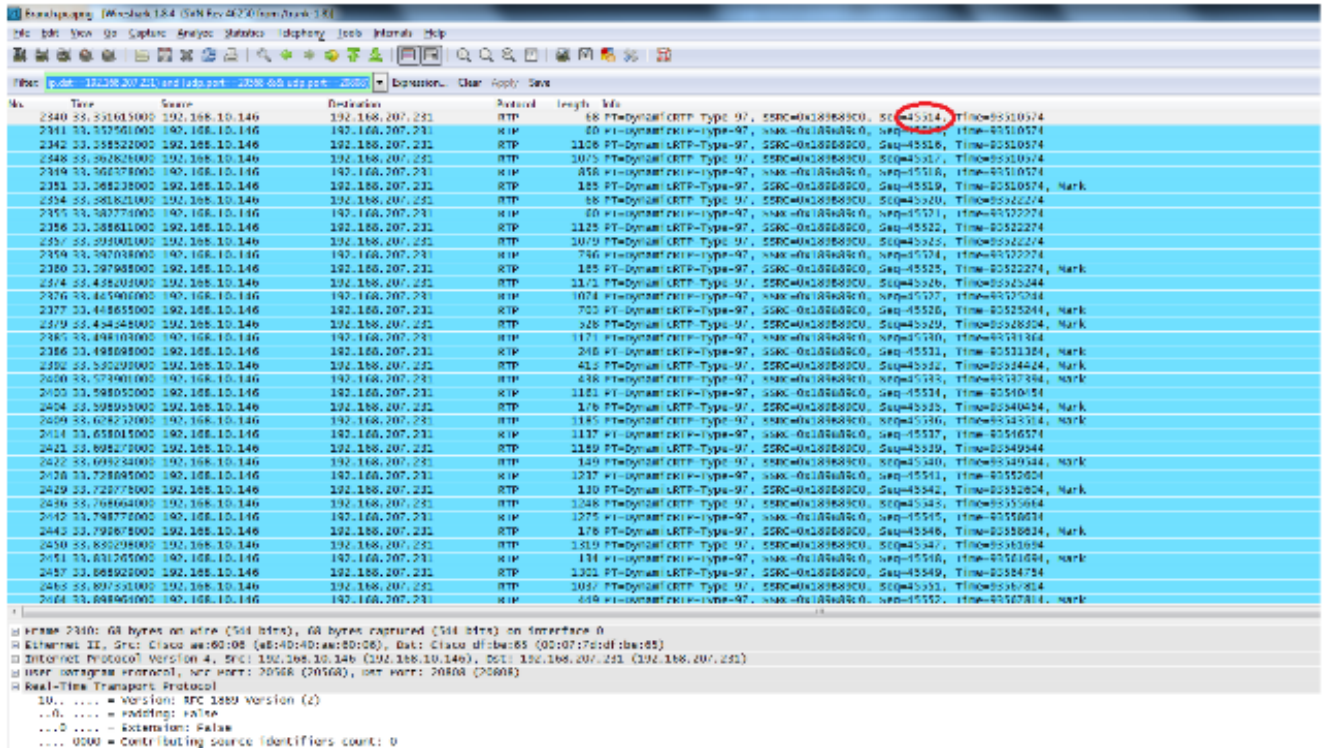


Vi resta un flusso decodificato come RTP e l'altro come UDP non decodificato.



8. Selezionare un pacchetto dal flusso non decodificato e decodificarlo come RTP. In questo modo, vengono decodificati sia i flussi audio che video in RTP.

Nota: il flusso audio è in formato codec G.722 e il tipo di payload Dynamic-RTP-97 indica il flusso RTP video.



Il problema ora riguarda solo la qualità video. Attivare il flusso RTP video e utilizzare i numeri di porta UDP per questo flusso per filtrare altri flussi.

9. Visualizzare il numero di porta selezionando uno dei pacchetti per la visualizzazione delle informazioni sulla porta UDP nel riquadro inferiore dell'utility Wireshark. Nella schermata precedente, viene selezionato uno dei pacchetti dal flusso video e nel riquadro inferiore vengono visualizzate le informazioni sulla porta Src (20568) e sulla porta Dst (20808).

Suggerimento: Utilizzare questo filtro: (ip.src==192.168.10.146 && ip.dst==192.168.207.231) && (udp.port eq 20568 and udp.port eq 20808). In questa schermata verrà visualizzato solo il flusso RTP video.

Nota: Annotare il primo e l'ultimo numero di sequenza RTP per il flusso.

RTP.

I numeri di sequenza vengono utilizzati per perfezionare il flusso nel caso in cui le clip non siano state acquisite contemporaneamente, ma con un lieve ritardo tra di esse.

Nota: È possibile che il sito di succursale inizi alcuni numeri di sequenza dopo 45514.

12. Selezionare un numero di sequenza iniziale e finale. Questi pacchetti sono presenti sia nella clip che nel filtro per visualizzare solo i pacchetti tra il numero di sequenza RTP iniziale e finale. Filtro:

```
(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 )
```

Quando si acquisiscono due clip contemporaneamente, non si perde alcun pacchetto all'inizio o alla fine di entrambe le acquisizioni. Se una delle acquisizioni non include alcuni pacchetti all'inizio o alla fine, usare il primo numero di sequenza o l'ultimo numero di sequenza nella cattura non effettuata in entrambi i pacchetti per rifinire il filtro per entrambe le acquisizioni. Osservare i pacchetti acquisiti in entrambi i punti tra gli stessi numeri di sequenza (intervallo di numeri di sequenza RTP).

Quando si applica il filtro, questo viene visualizzato nel sito centrale e nel sito di succursale:

Sito centrale:

The screenshot displays a list of network packets captured on a central site. The list includes columns for time, source IP, destination IP, protocol, and packet details. The packets are identified as RTP (Real-time Transport Protocol) and are filtered by sequence number (seq) between 44514 and 50449. The source IP is 192.168.10.146 and the destination IP is 192.168.207.231. The UDP ports are 20568 and 20808. Below the list, the packet details for the first packet (seq 44514) are shown, including the Ethernet II header, Internet Protocol version 4 header, and User Datagram Protocol header. The packet is identified as Real-Time Transport Protocol. The bottom of the screenshot shows the file path, packet count (94/58), and the selected packet (seq 44514).

Sito di succursale:

2357	33.399001000	192.168.10.146	192.168.207.231	RTP	60	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45521, Time=9352274
2358	33.399010000	192.168.10.146	192.168.207.231	RTP	1125	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45522, Time=9352274
2359	33.399020000	192.168.10.146	192.168.207.231	RTP	1079	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45523, Time=9352274
2360	33.397988000	192.168.10.146	192.168.207.231	RTP	796	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45524, Time=9352274
2376	33.445000000	192.168.10.146	192.168.207.231	RTP	165	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45525, Time=9352274
2376	33.445000000	192.168.10.146	192.168.207.231	RTP	1173	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45526, Time=9352274
2376	33.445000000	192.168.10.146	192.168.207.231	RTP	1074	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45527, Time=9352274
2377	33.445000000	192.168.10.146	192.168.207.231	RTP	703	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45528, Time=9352274
2379	33.454248000	192.168.10.146	192.168.207.231	RTP	528	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45529, Time=9352274
2385	33.498100000	192.168.10.146	192.168.207.231	RTP	1171	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45530, Time=9352274
2386	33.498198000	192.168.10.146	192.168.207.231	RTP	248	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45531, Time=9352274
2392	33.530298000	192.168.10.146	192.168.207.231	RTP	413	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45532, Time=9352274
2400	33.573901000	192.168.10.146	192.168.207.231	RTP	438	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45533, Time=9352274
2403	33.598050000	192.168.10.146	192.168.207.231	RTP	1161	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45534, Time=9352274
2404	33.598950000	192.168.10.146	192.168.207.231	RTP	176	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45535, Time=9352274
2406	33.628232000	192.168.10.146	192.168.207.231	RTP	1185	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45536, Time=9352274
2414	33.658035000	192.168.10.146	192.168.207.231	RTP	1137	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45537, Time=9352274
2421	33.698279000	192.168.10.146	192.168.207.231	RTP	1189	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45538, Time=9352274
2422	33.699240000	192.168.10.146	192.168.207.231	RTP	149	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45539, Time=9352274
2428	33.728895000	192.168.10.146	192.168.207.231	RTP	1237	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45540, Time=9352274
2429	33.729778000	192.168.10.146	192.168.207.231	RTP	130	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45541, Time=9352274
2436	33.768664000	192.168.10.146	192.168.207.231	RTP	1248	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45542, Time=9352274
2442	33.798778000	192.168.10.146	192.168.207.231	RTP	1275	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45543, Time=9352274
2443	33.799678000	192.168.10.146	192.168.207.231	RTP	176	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45544, Time=9352274
2450	33.830298000	192.168.10.146	192.168.207.231	RTP	1119	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45545, Time=9352274
2451	33.831265000	192.168.10.146	192.168.207.231	RTP	134	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45546, Time=9352274
2457	33.868529000	192.168.10.146	192.168.207.231	RTP	1301	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45547, Time=9352274
2463	33.897354000	192.168.10.146	192.168.207.231	RTP	1027	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45548, Time=9352274
2466	33.898564000	192.168.10.146	192.168.207.231	RTP	449	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45549, Time=9352274
2470	33.927687000	192.168.10.146	192.168.207.231	RTP	1055	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45550, Time=9352274
2471	33.928572000	192.168.10.146	192.168.207.231	RTP	477	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45551, Time=9352274
2478	33.967539000	192.168.10.146	192.168.207.231	RTP	1052	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45552, Time=9352274
2479	33.968521000	192.168.10.146	192.168.207.231	RTP	392	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45553, Time=9352274

```

Frame 2340: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
Ethernet II, Src: Cisco_ae:60:96 (e8:40:14:ae:60:06), Dst: Cisco_df:ba:65 (00:07:17:df:ba: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
  0... .. = Version: RFC 1889 version (2)
  ..0... .. = Padding: false
  ...0... .. = Extension: false
  ....0000 = contributing source identifiers count: 0
  0... .. = Marker: false
  payload type: dynamicRTP type 97 (97)
  Sequence number: 45514
  Timestamp: 93510574
  Synchronization Source identifier: 0x189b89c0 (412866528)
  0... .. = CSRC: 0x189b89c0 (412866528)
0000 00 07 f4 0f be 65 e8 40 40 ae 00 06 08 00 45 88  ....e.0 8.....
0010 00 36 84 03 00 3b 11 9e 91 c0 38 0a 92 c0 85  ....6.....
0020 0f 07 50 58 51 48 00 22 96 04 80 61 01 c0 65 92  ....fP.....
0030 0b 00 18 9b 83 c0 27 42 80 14 95 30 58 25 00 10  .......5....X...
0040 1a 24 ad 40                                     ....a.....

```

Notare il numero di pacchetti filtrati nel riquadro inferiore dell'utilità Wireshark in entrambe le clip. Il conteggio **Visualizzato** indica il numero di pacchetti che soddisfano i criteri di filtro desiderati.

Il sito centrale ha 4.936 pacchetti che soddisfano i criteri del filtro desiderati tra i numeri di sequenza RTP iniziale (45514) e finale (50449), mentre il sito della filiale ha solo 4.737 pacchetti. Ciò indica una perdita di 199 pacchetti. Notare che questi 199 pacchetti corrispondono al conteggio "Rcvr Lost Pkts" di 199, che è stato visualizzato nelle statistiche di streaming del telefono IP lato filiale mostrato all'inizio di questo documento.

Ciò conferma che tutti i pacchetti perduti RCV erano in realtà perdite di rete a livello di WAN. In questo modo, viene isolato il punto di perdita dei pacchetti nella rete, mentre i problemi di qualità audio/video vengono gestiti usando cadute sospette nella rete.