

Descifrar el flujo RTP para el análisis de pérdida de paquetes en Wireshark para llamadas de voz y vídeo

Contenido

[Introducción](#)

[Problema](#)

Introducción

Este documento describe el proceso de descifrar el flujo de transmisión en tiempo real (RTP) para el análisis de pérdida de paquetes en Wireshark para llamadas de voz y vídeo. Puede utilizar los filtros de Wireshark para analizar las capturas de paquetes simultáneas realizadas en o cerca del origen y el destino de una llamada. Esto es útil cuando debe resolver problemas de calidad de audio y vídeo cuando se sospechan pérdidas de red.


Problema

Este ejemplo utiliza este flujo de llamada:

Teléfono IP A (sitio centralA) > Switch 2960 > Router > Router WAN (sitio central) > IPWAN > Router WAN (sitio B) > Router > 2960 > Teléfono IP B

En este escenario, el problema encontrado es que las videollamadas desde el teléfono IP A al teléfono IP B dan como resultado una mala calidad de vídeo desde el sitio central A a la sucursal B, donde central tiene buena calidad pero el lado de la sucursal tiene problemas.

Vea el receptor perdió paquetes en las estadísticas de transmisión del teléfono IP de la sucursal:

		<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	

Solución

La mala calidad se ve solamente en el lado de la sucursal y como el sitio central ve una buena imagen, parece que el flujo de la central a la sucursal parece estar perdiendo paquetes por la red.

IP addressing scheme

Central IP phone: 192.168.10.146

Central Gateway: 192.168.10.253

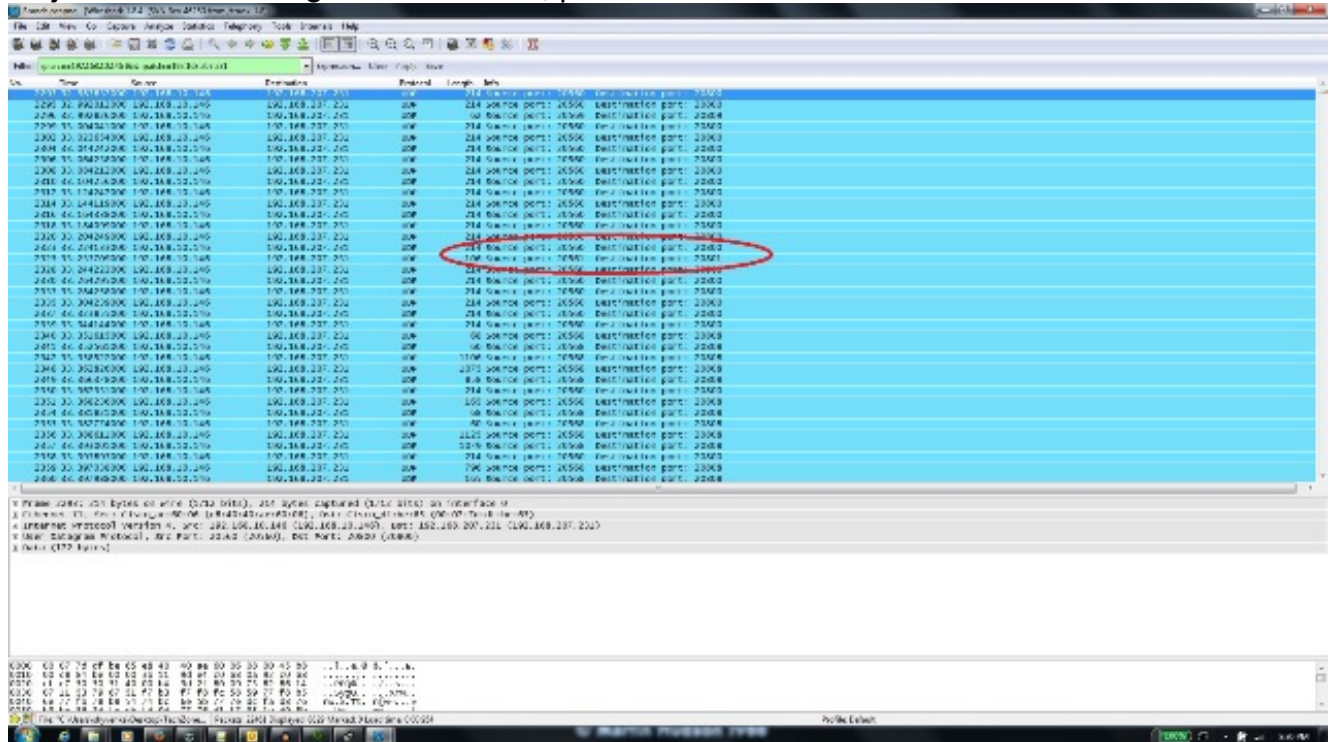
Central WAN router: 192.168.10.254
Branch WAN router: 192.168.206.210
Branch Gateway: 192.168.206.253
Branch IP phone: 192.168.207.231

Las capturas de paquetes se realizan en el router WAN central y de la sucursal y la WAN descarta estos paquetes. Céntrese en el flujo RTP desde el teléfono IP central (192.168.10.146) hasta el teléfono IP de sucursal (192.168.207.231). Este flujo pierde paquetes en el router WAN de la sucursal si la WAN descarta los paquetes en el flujo desde el router WAN central al router WAN de la sucursal. Utilice las opciones de filtro de Wireshark para aislar el problema:

1. Abra la captura en wireshark.
2. Utilice el filtro `ip.src==192.168.10.146 && ip.dst==192.168.207.231`. Esto filtra todos los flujos UDP del teléfono IP central al teléfono IP de la sucursal.
3. Realice el análisis en la captura del lado de la bifurcación solamente pero tenga en cuenta que debe realizar estos pasos para la captura central también.
4. En esta captura de pantalla, el flujo UDP se filtra entre las direcciones IP de origen y de destino y contiene dos secuencias UDP (diferenciadas por los números de puerto UDP). Esta es una videollamada, por lo que hay dos transmisiones: audio y vídeo. En este ejemplo, las dos secuencias son:

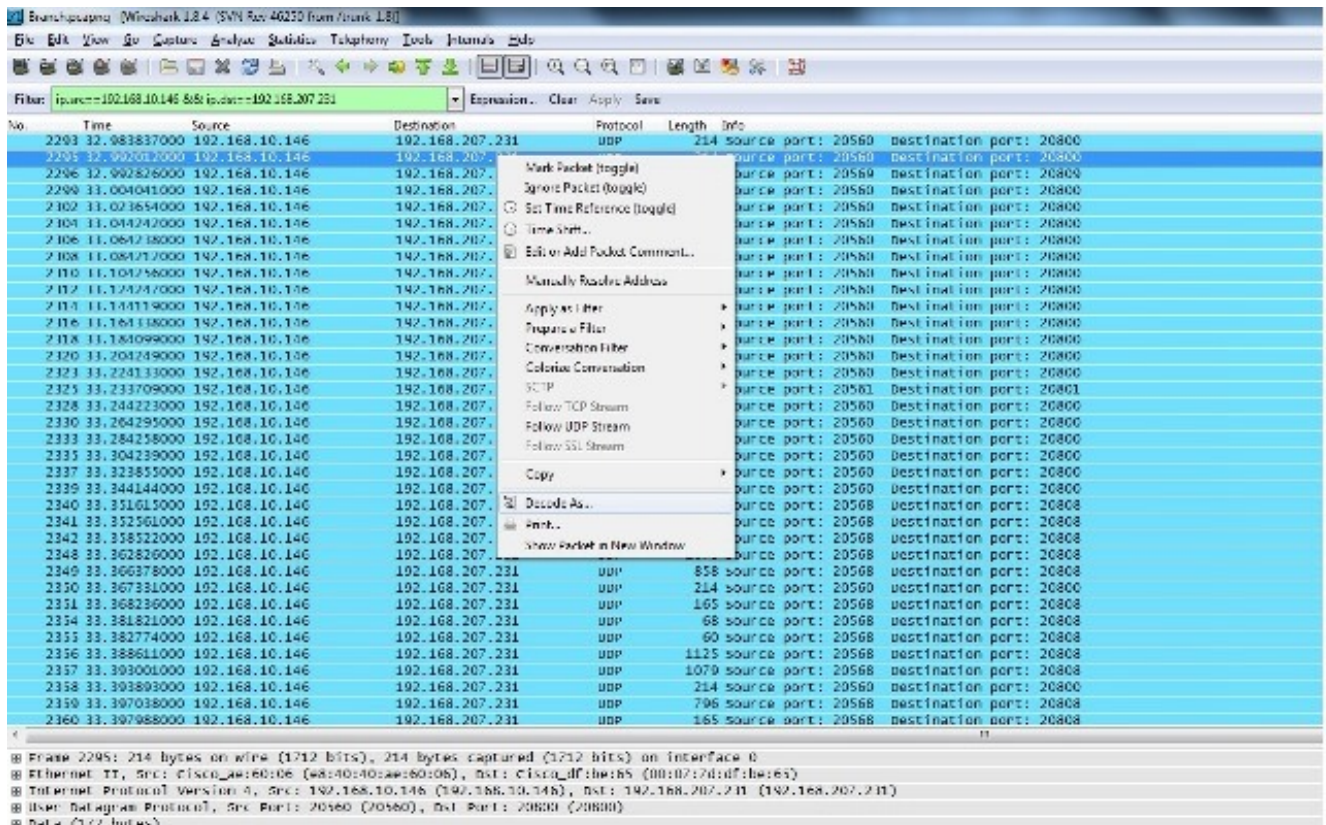
Flujo 1: Puerto de origen UDP: 20560, puerto de destino: 20800

Flujo 2: Puerto de origen UDP: 20561, puerto de destino: 20801

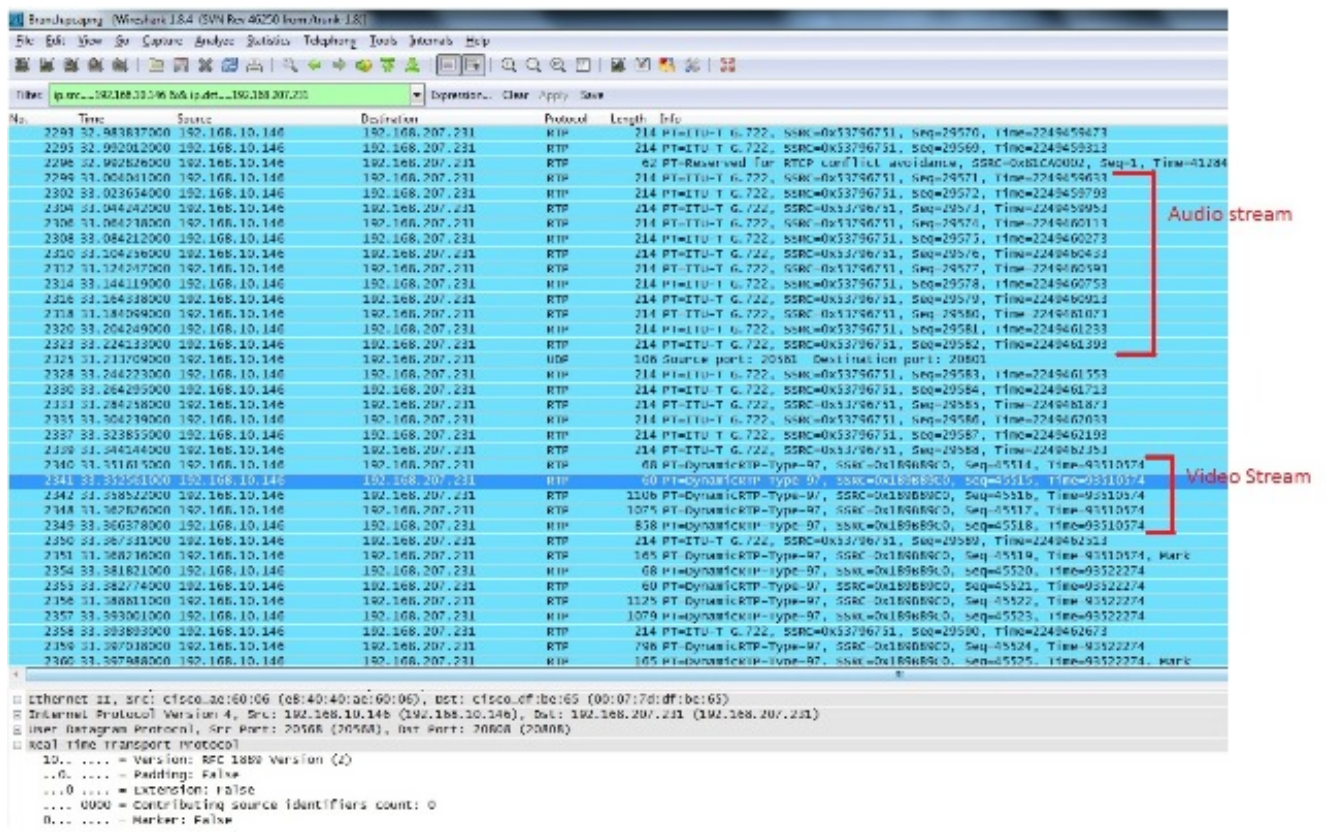


5. Seleccione un paquete de una de las secuencias y haga clic con el botón derecho del ratón en el paquete.
6. Seleccione **Decodificar como...** y escriba **RTP**.

7. Haga clic en **Aceptar** y **Aceptar** para decodificar la secuencia como RTP.

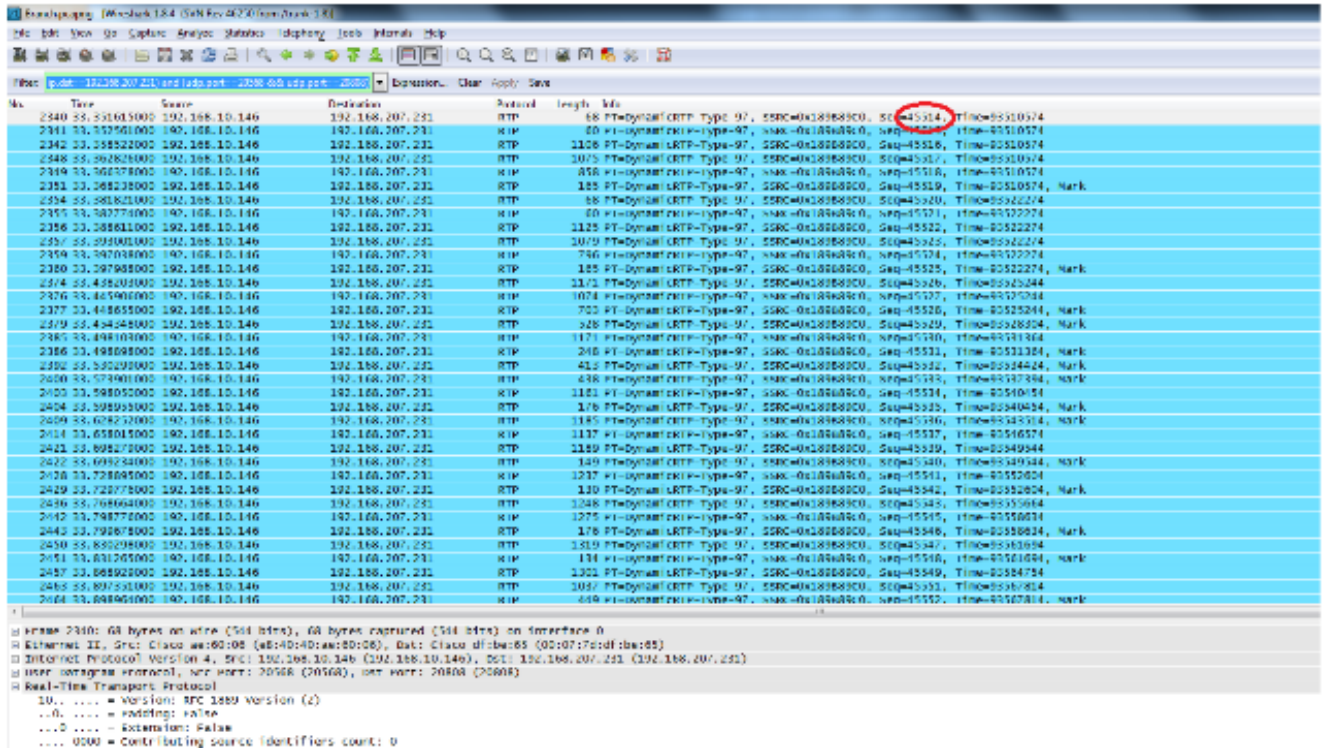


Se queda con una secuencia decodificada como RTP y la otra como UDP no decodificado.



8. Seleccione un paquete de la secuencia sin decodificar y decodificarlo como RTP. Esto decodifica tanto el audio como los flujos de vídeo en RTP.

Nota: La secuencia de audio está en formato de códec G.722 y el tipo de carga útil Dynamic-RTP-97 indica la secuencia RTP de vídeo.



El problema ahora es sólo con la calidad del vídeo. Céntrese en el flujo RTP de vídeo y utilice los números de puerto UDP para este flujo para filtrar otras secuencias.

9. Vea el número de puerto seleccionando uno de los paquetes que muestra la información del puerto UDP en el panel inferior de la utilidad Wireshark. En la captura de pantalla anterior, se selecciona uno de los paquetes de la secuencia de vídeo y puede ver la información del puerto Src (20568) y del puerto Dst (20808) en el panel inferior.

Consejo: Utilice este filtro: `(ip.src==192.168.10.146 && ip.dst==192.168.207.231) && (udp.port eq 20568 & udp.port eq 20808)`. Solo verá la secuencia RTP de vídeo que se muestra en esta captura de pantalla.

Nota: Anote los primeros y últimos números de secuencia RTP para esta secuencia.

11. Refinar el filtro para que coincida sólo con los paquetes entre los flujos RTP primero y último.

Los números de secuencia se utilizan para refinar la secuencia en caso de que las capturas no se hayan tomado simultáneamente, pero con un ligero retraso entre ellas.

Nota: Es posible que la sucursal inicie algunos números de secuencia después de 45514.

12. Seleccione un número de secuencia inicial y final. Estos paquetes están presentes tanto en las capturas como en la refinación del filtro para mostrar solamente esos paquetes entre los números de secuencia RTP inicial y final. El filtro para esto es:

```
(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 )
```

Cuando se toman capturas simultáneamente, no se pierden paquetes al principio o al final en ambas capturas. Si ve que una de las capturas no incluye algunos paquetes en el inicio/fin, utilice el primer número de secuencia o el último número de secuencia en la captura perdida en ambos paquetes para refinar el filtro para ambas capturas. Observe los paquetes que capturaron en ambos puntos entre los mismos números de secuencia (rango de números de secuencia RTP).

Cuando aplica el filtro, lo ve en el sitio central y en el sitio de la sucursal:

Sitio central:

The screenshot displays the Wireshark interface for a central site. The top pane shows a list of captured packets, all of which are RTP packets. The columns include No., Time, Source, Destination, Protocol, Length, and Info. The Info column for each packet shows details like 'RTP [Dynamic] RTP-Type=97, SSRC=0x189e89c0, Seq=45531, Time=93551364, Mark...'. The middle pane shows the details of the selected packet (No. 14493), including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Real-time Transport Protocol. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Sucursal:

2337	33.386774000	192.168.10.146	192.168.207.231	RTP	60	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45521, Time=9352274
2338	33.386811000	192.168.10.146	192.168.207.231	RTP	1125	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45522, Time=9352274
2337	33.399001000	192.168.10.146	192.168.207.231	RTP	1079	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45523, Time=9352274
2338	33.399038000	192.168.10.146	192.168.207.231	RTP	796	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45524, Time=9352274
2360	33.397988000	192.168.10.146	192.168.207.231	RTP	165	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45525, Time=9352274, Mark
2375	33.418202000	192.168.10.146	192.168.207.231	RTP	1173	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45526, Time=9352274
2376	33.445906000	192.168.10.146	192.168.207.231	RTP	1074	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45527, Time=9352274
2377	33.446559000	192.168.10.146	192.168.207.231	RTP	785	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45528, Time=9352274, Mark
2379	33.454248000	192.168.10.146	192.168.207.231	RTP	528	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45529, Time=9352274, Mark
2385	33.498102000	192.168.10.146	192.168.207.231	RTP	1171	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45530, Time=93511365
2386	33.498298000	192.168.10.146	192.168.207.231	RTP	248	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45531, Time=93511364, Mark
2392	33.530299000	192.168.10.146	192.168.207.231	RTP	413	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45532, Time=93511364, Mark
2400	33.573901000	192.168.10.146	192.168.207.231	RTP	438	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45533, Time=93511364, Mark
2403	33.598050000	192.168.10.146	192.168.207.231	RTP	1161	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45534, Time=9350454
2404	33.598955000	192.168.10.146	192.168.207.231	RTP	176	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45535, Time=9350454, Mark
2405	33.628252000	192.168.10.146	192.168.207.231	RTP	1185	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45536, Time=9350454, Mark
2414	33.658035000	192.168.10.146	192.168.207.231	RTP	1137	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45537, Time=9350454
2421	33.698279000	192.168.10.146	192.168.207.231	RTP	1189	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45539, Time=9350454
2422	33.699240000	192.168.10.146	192.168.207.231	RTP	149	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45540, Time=9350454, Mark
2428	33.728895000	192.168.10.146	192.168.207.231	RTP	1237	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45541, Time=93522604
2429	33.729778000	192.168.10.146	192.168.207.231	RTP	130	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45542, Time=93522604, Mark
2436	33.768640000	192.168.10.146	192.168.207.231	RTP	1248	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45543, Time=93522604
2442	33.798778000	192.168.10.146	192.168.207.231	RTP	1275	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45545, Time=93508614
2443	33.799678000	192.168.10.146	192.168.207.231	RTP	176	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45546, Time=93508624, Mark
2450	33.830298000	192.168.10.146	192.168.207.231	RTP	1119	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45547, Time=93508624
2451	33.831265000	192.168.10.146	192.168.207.231	RTP	134	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45548, Time=93508624, Mark
2457	33.868529000	192.168.10.146	192.168.207.231	RTP	1301	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45549, Time=93508624
2463	33.897352000	192.168.10.146	192.168.207.231	RTP	1027	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45551, Time=93508624
2466	33.898564000	192.168.10.146	192.168.207.231	RTP	449	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45552, Time=93508624, Mark
2470	33.927887000	192.168.10.146	192.168.207.231	RTP	1055	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45553, Time=93508624
2471	33.928528000	192.168.10.146	192.168.207.231	RTP	477	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45554, Time=93508624, Mark
2478	33.967539000	192.168.10.146	192.168.207.231	RTP	1052	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45555, Time=93508624
2479	33.968921000	192.168.10.146	192.168.207.231	RTP	392	PT=DYNAMIC RTP-Type=97, SSRC=0x189889c0, Seq=45556, Time=93508624, Mark

```

Frame 2340: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
Ethernet II, Src: Cisco_ae:60:9b (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
  00 ..... = 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: 0x189889c0 (412866528)
  0000 00 07 f4 0f be 65 e8 40 40 ae 00 06 08 00 45 88 .....e.0 8.....E.
  0010 00 36 84 c3 00 00 3b 11 9e 91 c0 38 0a 92 c0 85 .....0.....?;.....
  0020 ff 07 50 58 51 48 00 21 96 04 80 61 01 c0 05 92 .....P.....5.....
  0030 0b 00 18 9b 8b c0 27 42 80 14 95 30 58 25 00 10 .....5.....X...
  0040 1a 24 ad 40 .....
  
```

Observe el recuento de paquetes filtrados en el panel inferior de la utilidad Wireshark en ambas capturas. El conteo **Mostrado** indica el número de paquetes que coinciden con los criterios de filtro deseados.

El sitio central tiene 4,936 paquetes que coinciden con los criterios de filtro deseados entre los números de secuencia RTP inicial (45514) y final (50449) mientras que en el sitio de la sucursal hay sólo 4,737 paquetes. Esto indica una pérdida de 199 paquetes. Tenga en cuenta que estos 199 paquetes coinciden con el recuento "Rcvr Lost Pkts" de 199 que se vio en las estadísticas de streaming del teléfono IP del lado de la sucursal que se muestran al inicio de este documento.

Esto confirma que todos los paquetes perdidos de Rcvr fueron pérdidas de red descartadas a través de la WAN. Así es como se aísla el punto de pérdida de paquetes en la red mientras se gestionan los problemas de calidad de audio/vídeo que implican caídas sospechosas de la red.