

Déterminez le flux RTP pour l'analyse des pertes de paquets dans Wireshark pour les appels vocaux et vidéo

Contenu

[Introduction](#)

[Problème](#)

Introduction

Ce document décrit le processus de déchiffrement du flux RTP (Real-Time Streaming) pour l'analyse de perte de paquets dans Wireshark pour les appels vocaux et vidéo. Vous pouvez utiliser des filtres Wireshark afin d'analyser les captures de paquets simultanées prises à la source et à la destination d'un appel ou à proximité de celle-ci. Cela est utile lorsque vous devez résoudre des problèmes de qualité audio et vidéo lorsque vous soupçonnez des pertes de réseau.


Problème

Cet exemple utilise ce flux d'appels :

Téléphone IP A (site central A) > Commutateur 2960 > Routeur > Routeur WAN (site central) > IPWAN > Routeur WAN (site B) > Routeur > 2960 > Téléphone IP B

Dans ce scénario, le problème rencontré est que les appels vidéo du téléphone IP A au téléphone IP B entraînent une mauvaise qualité vidéo du site central A au site de filiale B, où le site central est de bonne qualité, mais où le côté succursale présente des problèmes.

Reportez-vous à la section Réception des paquets perdus dans les statistiques de diffusion du téléphone IP de la 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	

Solution

La mauvaise qualité n'est visible que du côté de la succursale et comme le site central voit une bonne image, il semble que le flux du site central vers le site de la succursale semble perdre des paquets sur le réseau.

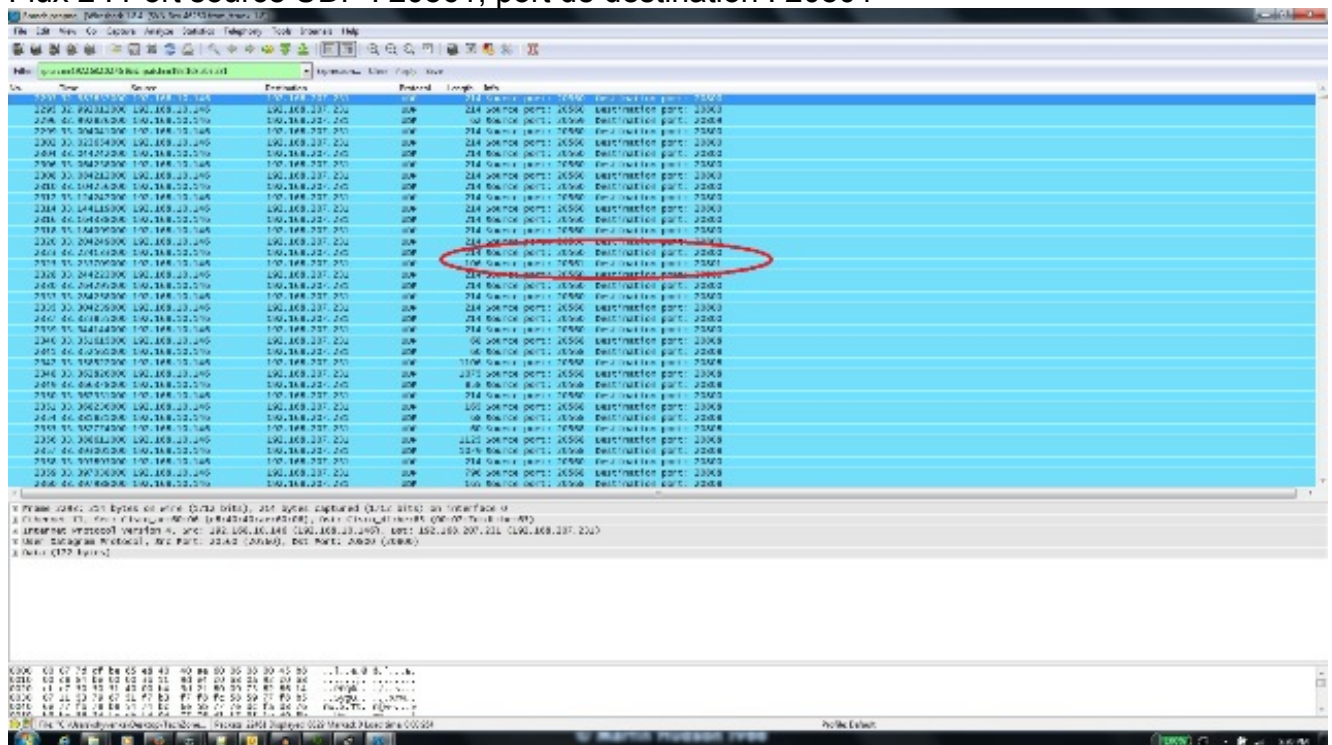
Central Gateway: 192.168.10.253
Central WAN router: 192.168.10.254
Branch WAN router: 192.168.206.210
Branch Gateway: 192.168.206.253
Branch IP phone: 192.168.207.231

Les captures de paquets sont prises sur le routeur WAN central et de filiale et le WAN abandonne ces paquets. Concentrez-vous sur le flux RTP du téléphone IP central (192.168.10.146) au téléphone IP de filiale (192.168.207.231). Ce flux manque des paquets sur le routeur WAN de la filiale si le WAN abandonne les paquets sur le flux du routeur WAN central au routeur WAN de la filiale. Utilisez les options de filtre de Wireshark pour isoler le problème :

1. Ouvrez la capture dans Wireshark.
2. Utilisez le filtre `ip.src==192.168.10.146 && ip.dst==192.168.207.231`. Cela filtre tous les flux UDP du téléphone IP central au téléphone IP de filiale.
3. Effectuez l'analyse sur la capture côté succursale uniquement, mais notez que vous devez également effectuer ces étapes pour la capture centrale.
4. Dans cette capture d'écran, le flux UDP est filtré entre les adresses IP source et de destination et contient deux flux UDP (différenciés par les numéros de port UDP). Il s'agit d'un appel vidéo, il y a donc deux flux : audio et vidéo. Dans cet exemple, les deux flux sont :

Flux 1 : Port source UDP : 20560, port de destination : 20800

Flux 2 : Port source UDP : 20561, port de destination : 20801



5. Sélectionnez un paquet dans l'un des flux et cliquez avec le bouton droit sur le paquet.
6. Sélectionnez **Décoder en tant que...** et tapez **RTP**.
7. Cliquez sur **Accept** et **Ok** afin de décoder le flux en tant que RTP.

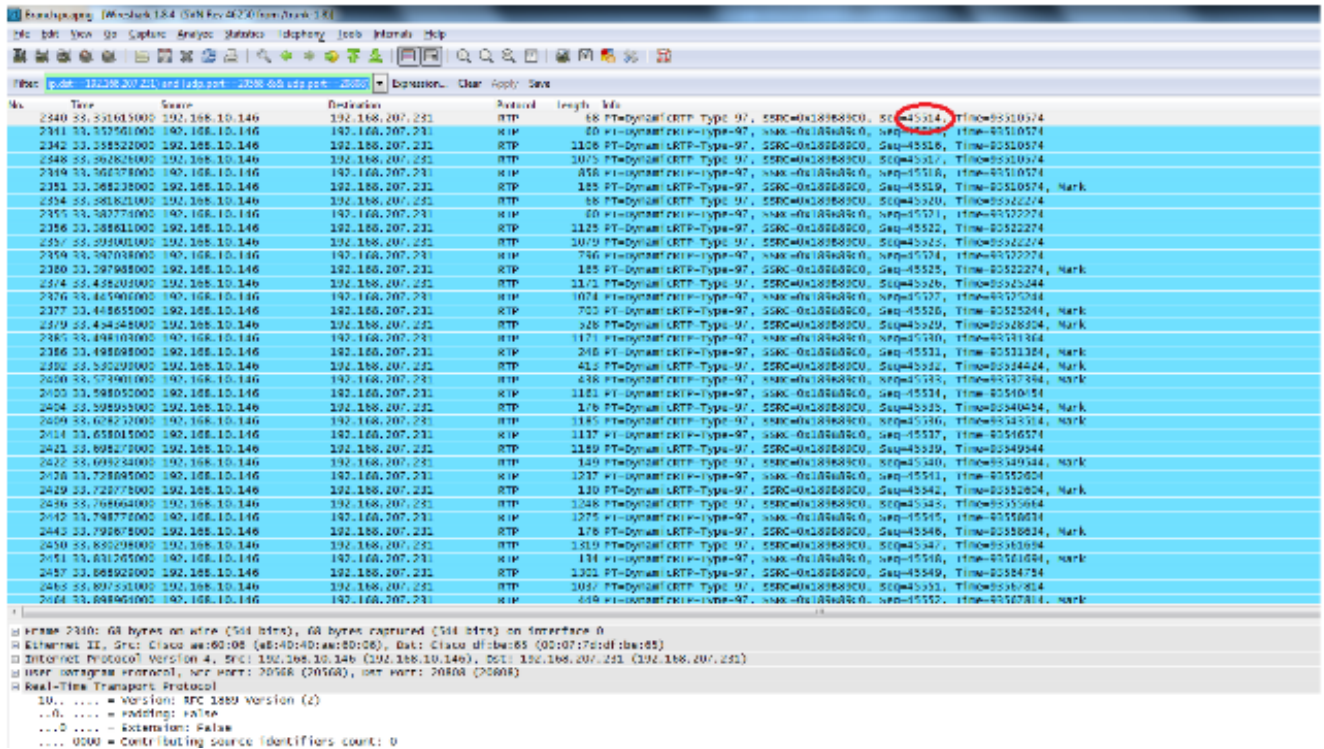
Vous restez avec un flux décodé en tant que RTP et l'autre en tant qu'UDP non décodé.

Vous restez avec un flux décodé en tant que RTP et l'autre en tant qu'UDP non décodé.

8. Sélectionnez un paquet dans le flux non décodé et décodez-le en tant que RTP. Cela décode le flux audio et vidéo dans RTP.

Remarque : le flux audio est au format de codec G.722 et le type de charge utile Dynamic-

RTP-97 indique le flux RTP vidéo.



Le problème est maintenant uniquement lié à la qualité vidéo. Concentrez-vous sur le flux vidéo RTP et utilisez les numéros de port UDP de ce flux pour filtrer d'autres flux.

- Affichez le numéro de port en sélectionnant l'un des paquets qui affiche les informations de port UDP dans le volet inférieur de l'utilitaire Wireshark. Dans la capture d'écran précédente, l'un des paquets du flux vidéo est sélectionné et vous pouvez voir les informations du port Src (20568) et du port Dst (20808) dans le volet inférieur.

Astuce : Utilisez ce filtre : (ip.src==192.168.10.146 && ip.dst==192.168.207.231) && (udp.port équip 20568 et udp.port équip 2080). Vous ne verrez que le flux vidéo RTP présenté dans cette capture d'écran.

Note: Notez les premiers et derniers numéros de séquence RTP pour ce flux.

11. Affinez le filtre pour qu'il corresponde uniquement aux paquets entre le premier et le dernier flux RTP.

Les numéros de séquence sont utilisés pour affiner le flux au cas où les captures n'étaient pas prises simultanément, mais avec un léger retard entre elles.

Note: Il est possible que le site de la branche commence certains numéros d'ordre après 45514.

12. Sélectionnez un numéro de séquence de début et de fin. Ces paquets sont présents dans les captures et affinent le filtre pour afficher uniquement les paquets entre les numéros de séquence RTP de début et de fin. Le filtre pour ceci est :

```
(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 )
```

Lorsque des captures sont prises simultanément, aucun paquet n'est manqué au début ou à la fin des deux captures. Si vous voyez que l'une des captures n'inclut pas quelques paquets au début/à la fin, utilisez le premier numéro de séquence ou le dernier numéro de séquence de la capture manquée dans les deux paquets pour affiner le filtre des deux captures. Observez les paquets capturés aux deux points entre les mêmes numéros de séquence (plage de numéros de séquence RTP).

Lorsque vous appliquez le filtre, vous voyez ceci sur le site central et le site de la succursale :

Site central :

Time	Source IP	Destination IP	Protocol	Length	Info
14572	192.168.10.146	192.168.207.231	RTP	248	PT=dynamic RTP-Type=97, SSRC=0x189e89c0, Seq=45531, Time=93531364, Mark
14591	192.168.10.146	192.168.207.231	RTP	413	PT=dynamic RTP-Type=97, SSRC=0x189e89c0, Seq=45532, Time=93534420, Mark
14609	192.168.10.146	192.168.207.231	RTP	418	PT=dynamic RTP-Type=97, SSRC=0x189e89c0, Seq=45533, Time=93537180, Mark
14619	192.168.10.146	192.168.207.231	RTP	1161	PT=dynamic RTP-Type=97, SSRC=0x189e89c0, Seq=45534, Time=93540434, Mark
14620	192.168.10.146	192.168.207.231	RTP	176	PT=dynamic RTP-Type=97, SSRC=0x189e89c0, Seq=45535, Time=93540434, Mark
14634	192.168.10.146	192.168.207.231	RTP	1185	PT=dynamic RTP-Type=97, SSRC=0x189e89c0, Seq=45536, Time=93543514, Mark
14646	192.168.10.146	192.168.207.231	RTP	1117	PT=dynamic RTP-Type=97, SSRC=0x189e89c0, Seq=45537, Time=93546570, Mark
14647	192.168.10.146	192.168.207.231	RTP	111	PT=dynamic RTP-Type=97, SSRC=0x189e89c0, Seq=45538, Time=93546570, Mark
14666	192.168.10.146	192.168.207.231	RTP	1180	PT=dynamic RTP-Type=97, SSRC=0x189e89c0, Seq=45539, Time=93549544, Mark
14667	192.168.10.146	192.168.207.231	RTP	149	PT=dynamic RTP-Type=97, SSRC=0x189e89c0, Seq=45540, Time=93549544, Mark
14679	192.168.10.146	192.168.207.231	RTP	1237	PT=dynamic RTP-Type=97, SSRC=0x189e89c0, Seq=45541, Time=93552600, Mark
14680	192.168.10.146	192.168.207.231	RTP	110	PT=dynamic RTP-Type=97, SSRC=0x189e89c0, Seq=45542, Time=93552600, Mark
14699	192.168.10.146	192.168.207.231	RTP	1248	PT=dynamic RTP-Type=97, SSRC=0x189e89c0, Seq=45543, Time=93555664, Mark
14700	192.168.10.146	192.168.207.231	RTP	135	PT=dynamic RTP-Type=97, SSRC=0x189e89c0, Seq=45544, Time=93555664, Mark
14711	192.168.10.146	192.168.207.231	RTP	1275	PT=dynamic RTP-Type=97, SSRC=0x189e89c0, Seq=45545, Time=93558634, Mark
14712	192.168.10.146	192.168.207.231	RTP	176	PT=dynamic RTP-Type=97, SSRC=0x189e89c0, Seq=45546, Time=93558634, Mark
14724	192.168.10.146	192.168.207.231	RTP	1114	PT=dynamic RTP-Type=97, SSRC=0x189e89c0, Seq=45547, Time=93561694, Mark
14725	192.168.10.146	192.168.207.231	RTP	134	PT=dynamic RTP-Type=97, SSRC=0x189e89c0, Seq=45548, Time=93561694, Mark
14744	192.168.10.146	192.168.207.231	RTP	1301	PT=dynamic RTP-Type=97, SSRC=0x189e89c0, Seq=45549, Time=93564754, Mark

```

# Frame 14495: 88 bytes on wire (544 bits), 88 bytes captured (544 bits)
# Ethernet II, Src: Cisco_E7:13:F0 (30:e4:db: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 88  -b....0.-g....R.
0010  00 36 b4 d3 00 00 3f 11 9e 91 c0 a8 0a 92 c0 a8  -6....7.....
0020  cf c7 50 58 31 48 00 22 9b c4 80 61 b1 c3 05 92  -...X...D...
0030  db ae 18 9b 89 c9 27 42 89 14 95 a9 58 25 b9 10  -.....*...X...
0040  1e 24 4d 40                                     .e.4d0
  
```

Site de la succursale :

2537	33.399001000	192.168.10.146	192.168.207.231	RTP	60	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45521, Time=9532274
2538	33.399001000	192.168.10.146	192.168.207.231	RTP	1125	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45522, Time=9532274
2539	33.399001000	192.168.10.146	192.168.207.231	RTP	1079	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45523, Time=9532274
2540	33.397988000	192.168.10.146	192.168.207.231	RTP	796	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45524, Time=9532274
2541	33.397988000	192.168.10.146	192.168.207.231	RTP	165	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45525, Time=9532274, Mark
2542	33.445906000	192.168.10.146	192.168.207.231	RTP	1173	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45526, Time=9532274
2543	33.445906000	192.168.10.146	192.168.207.231	RTP	1074	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45527, Time=9532274
2544	33.452480000	192.168.10.146	192.168.207.231	RTP	783	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45528, Time=9532274, Mark
2545	33.452480000	192.168.10.146	192.168.207.231	RTP	528	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45529, Time=9532274, Mark
2546	33.498100000	192.168.10.146	192.168.207.231	RTP	1171	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45530, Time=9532274
2547	33.498100000	192.168.10.146	192.168.207.231	RTP	248	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45531, Time=9532274, Mark
2548	33.530299000	192.168.10.146	192.168.207.231	RTP	413	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45532, Time=9532274, Mark
2549	33.573901000	192.168.10.146	192.168.207.231	RTP	438	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45533, Time=9532274, Mark
2550	33.598950000	192.168.10.146	192.168.207.231	RTP	1161	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45534, Time=9532274, Mark
2551	33.598950000	192.168.10.146	192.168.207.231	RTP	176	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45535, Time=9532274, Mark
2552	33.628320000	192.168.10.146	192.168.207.231	RTP	1189	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45536, Time=9532274, Mark
2553	33.658015000	192.168.10.146	192.168.207.231	RTP	1137	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45537, Time=9532274, Mark
2554	33.698279000	192.168.10.146	192.168.207.231	RTP	1189	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45538, Time=9532274, Mark
2555	33.698279000	192.168.10.146	192.168.207.231	RTP	149	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45539, Time=9532274, Mark
2556	33.728895000	192.168.10.146	192.168.207.231	RTP	1237	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45540, Time=9532274, Mark
2557	33.728895000	192.168.10.146	192.168.207.231	RTP	130	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45541, Time=9532274, Mark
2558	33.768604000	192.168.10.146	192.168.207.231	RTP	1248	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45542, Time=9532274, Mark
2559	33.768604000	192.168.10.146	192.168.207.231	RTP	1275	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45543, Time=9532274, Mark
2560	33.799678000	192.168.10.146	192.168.207.231	RTP	176	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45544, Time=9532274, Mark
2561	33.830299000	192.168.10.146	192.168.207.231	RTP	1119	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45545, Time=9532274, Mark
2562	33.830299000	192.168.10.146	192.168.207.231	RTP	134	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45546, Time=9532274, Mark
2563	33.868829000	192.168.10.146	192.168.207.231	RTP	1301	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45547, Time=9532274, Mark
2564	33.897351000	192.168.10.146	192.168.207.231	RTP	1037	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45548, Time=9532274, Mark
2565	33.898604000	192.168.10.146	192.168.207.231	RTP	649	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45549, Time=9532274, Mark
2566	33.927680000	192.168.10.146	192.168.207.231	RTP	1055	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45550, Time=9532274, Mark
2567	33.929280000	192.168.10.146	192.168.207.231	RTP	477	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45551, Time=9532274, Mark
2568	33.967399000	192.168.10.146	192.168.207.231	RTP	1051	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45552, Time=9532274, Mark
2569	33.968921000	192.168.10.146	192.168.207.231	RTP	392	PT=DYNAMICRTP-Type-97, SSRC=0x189889C0, Seq=45553, Time=9532274, Mark

```

Frame 2340: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
Ethernet II, Src: Cisco_ae:60:06 (e8:40:40:ae:60:06), 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: 20408 (20408)
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: DYNAMICRTP type 97 (97)
Sequence number: 45514
Timestamp: 95310574
Synchronization Source identifier: 0x189889C0 (412866528)
  0... .. = SSRC: 0x189889C0 (412866528)
  0000 00 07 7d df be 65 e8 40 40 ae 60 06 08 00 45 88 ..e.0 8...E.
  0010 00 36 84 e3 00 00 3b 11 9e 91 c0 38 0a 92 c0 38 ..G...?;....
  0020 cf 07 30 51 48 00 22 9e 04 80 61 01 c0 05 02 ..e....
  0030 0b 0e 18 90 80 c0 27 42 80 14 95 30 58 25 00 10 .....8....X...
  0040 1a 24 ad 40                                     ....

```

Notez le nombre de paquets filtrés dans le volet inférieur de l'utilitaire Wireshark sur les deux captures. Le nombre **affiché** indique le nombre de paquets correspondant aux critères de filtre souhaités.

Le site central contient 4 936 paquets qui correspondent aux critères de filtre souhaités entre les numéros de séquence RTP de début (45514) et de fin (50449), tandis qu'au site de la filiale il n'y a que 4 737 paquets. Cela indique une perte de 199 paquets. Notez que ces 199 paquets correspondent au nombre de « Rcvr Lost Pkts » de 199 qui a été vu dans les statistiques de diffusion du téléphone IP côté succursale affichées au début de ce document.

Ceci confirme que tous les paquets perdus Rcvr étaient en fait des pertes de réseau abandonnées sur le WAN. C'est ainsi que le point de perte de paquets dans le réseau est isolé tandis que les problèmes de qualité audio/vidéo sont traités avec des suppositions de perte de réseau.