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

Contenu

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 :

Cisco Systems, Inc. http://192.168.207.231/StreamingStatistics?2

CISCO

Streaming Statistics

Cisco IP Phone CP-8941(SEP00077ddfbe65)

- Device Information
- Network Setup
- Network Statistics
  - Ethernet Information
  - Network
- Device Logs
  - Console Logs
  - Core Dumps
  - Status Messages
  - Debug Display
- Streaming Statistics
  - Stream 1
  - Stream 2

Remote Address	192.168.10.146/20568
Local Address	192.168.207.231/20808
Start Time	00:00:00
Stream Status	Not Ready
Host Name	SEP00077ddfbe65
Sender Packets	4745
Sender Octets	3144928
Sender Codec	H264
Sender Reports Sent	16
Sender Report Time Sent	11:19:34
Rcvr Lost Packets	199
Avg Jitter	40
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

de 2 30/10/2013 11:21

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.

```
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
```

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.

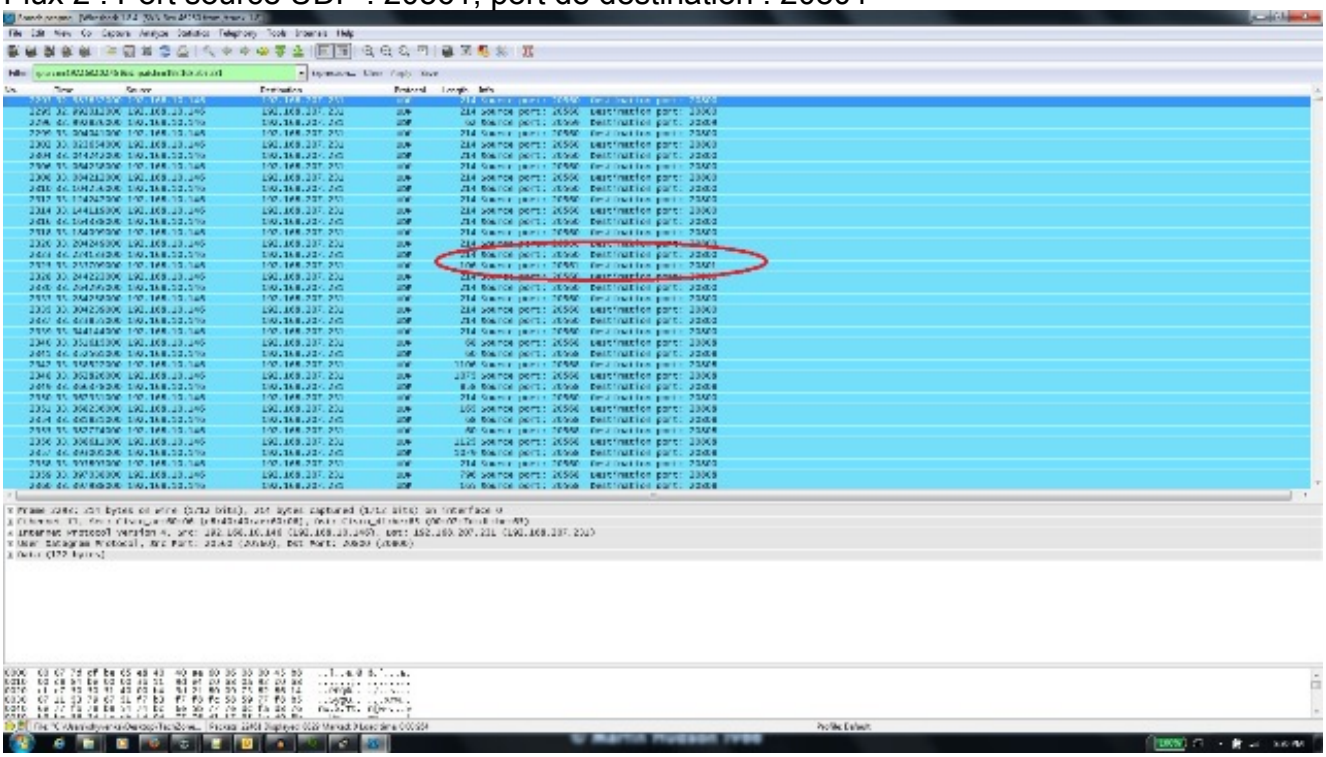
2. Utilisez le filtre ip.src==192.168.10.146 && ip.dst==192.168.207.231. Cela filtre tous les flux UDP du téléphone IP central au téléphone IP de filiale.

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

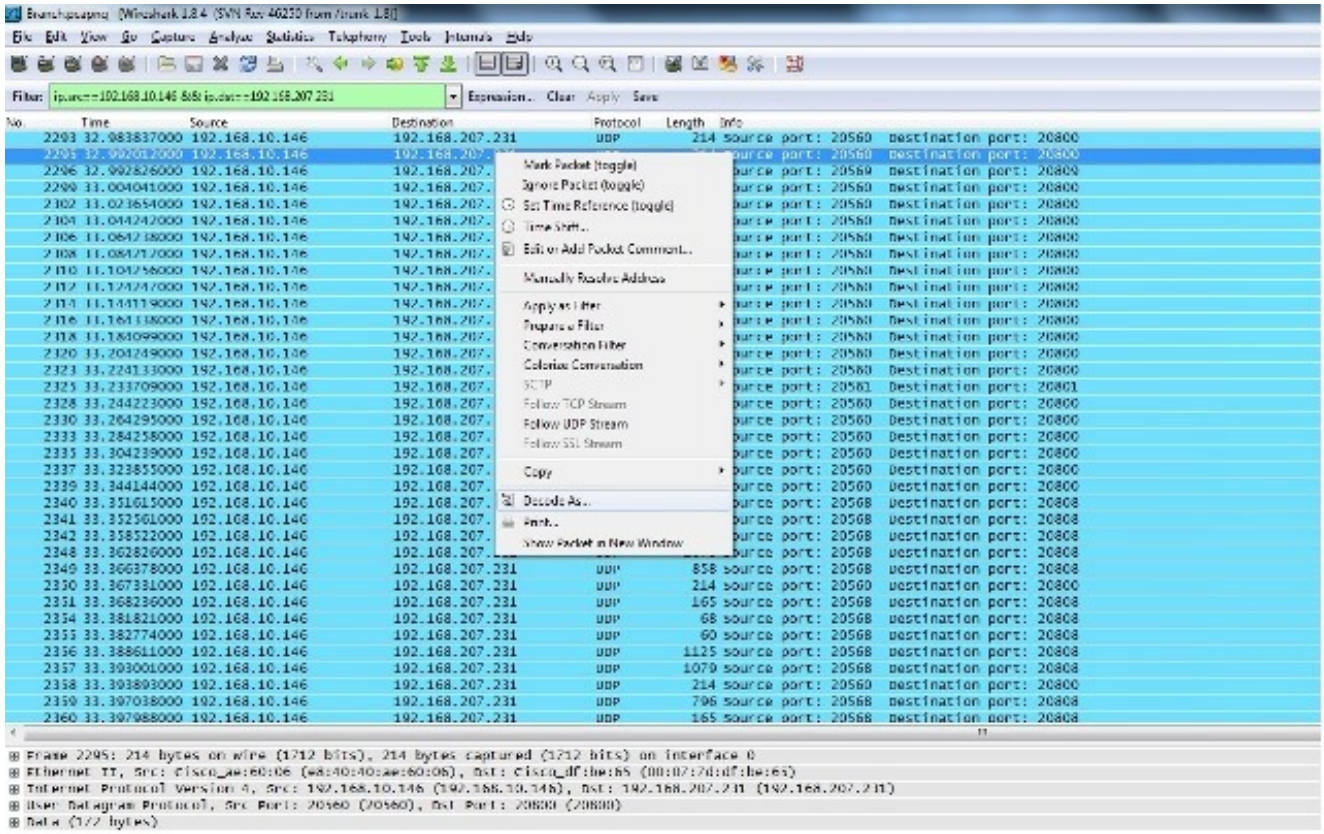
   Flux 2 : Port source UDP : 20561, port de destination : 20801



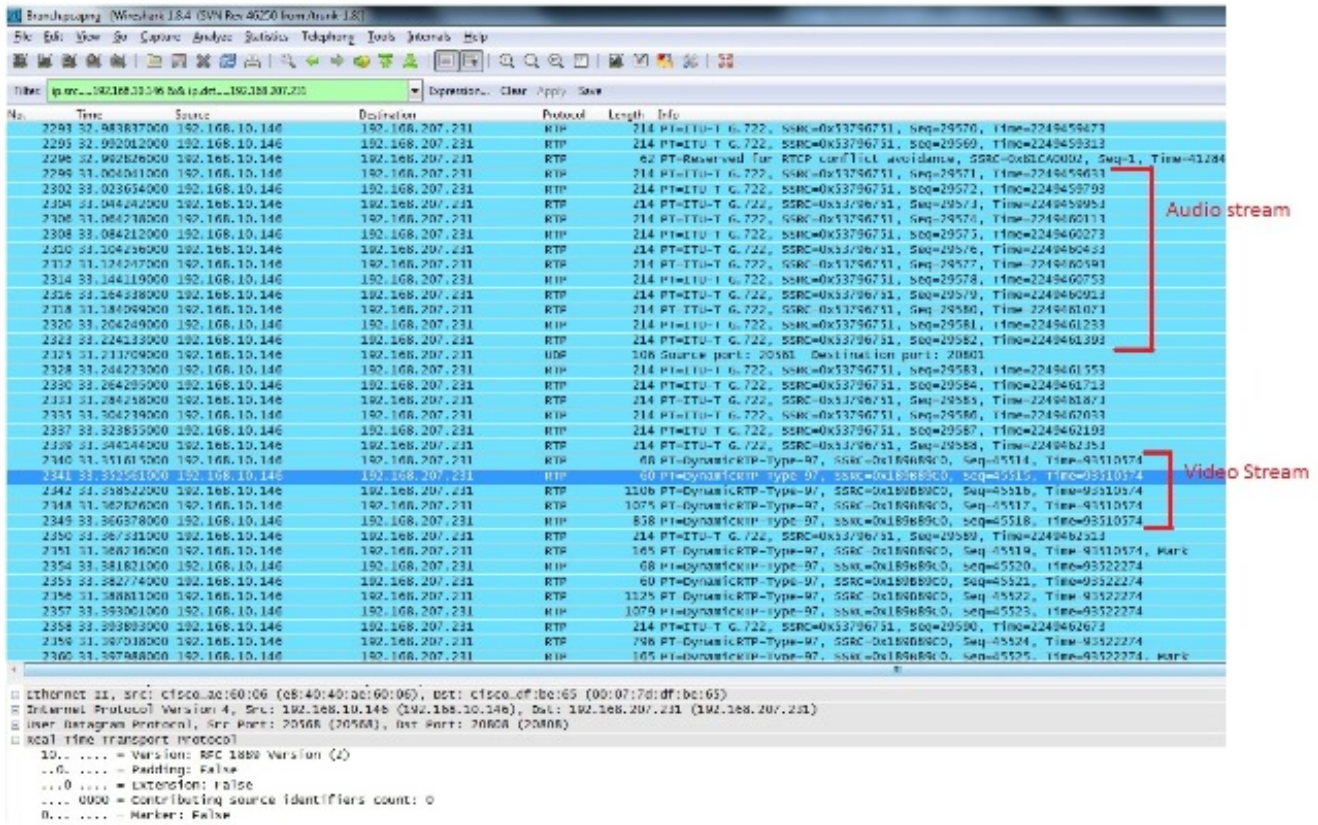
5. Sélectionnez un paquet dans l'un des flux et cliquez avec le bouton droit sur le paquet.

6. Sélectionnez **Décoder en tant que...** et tapez **RTP**.

7. Cliquez sur **Accept** et **Ok** afin de décoder le flux en tant que RTP.



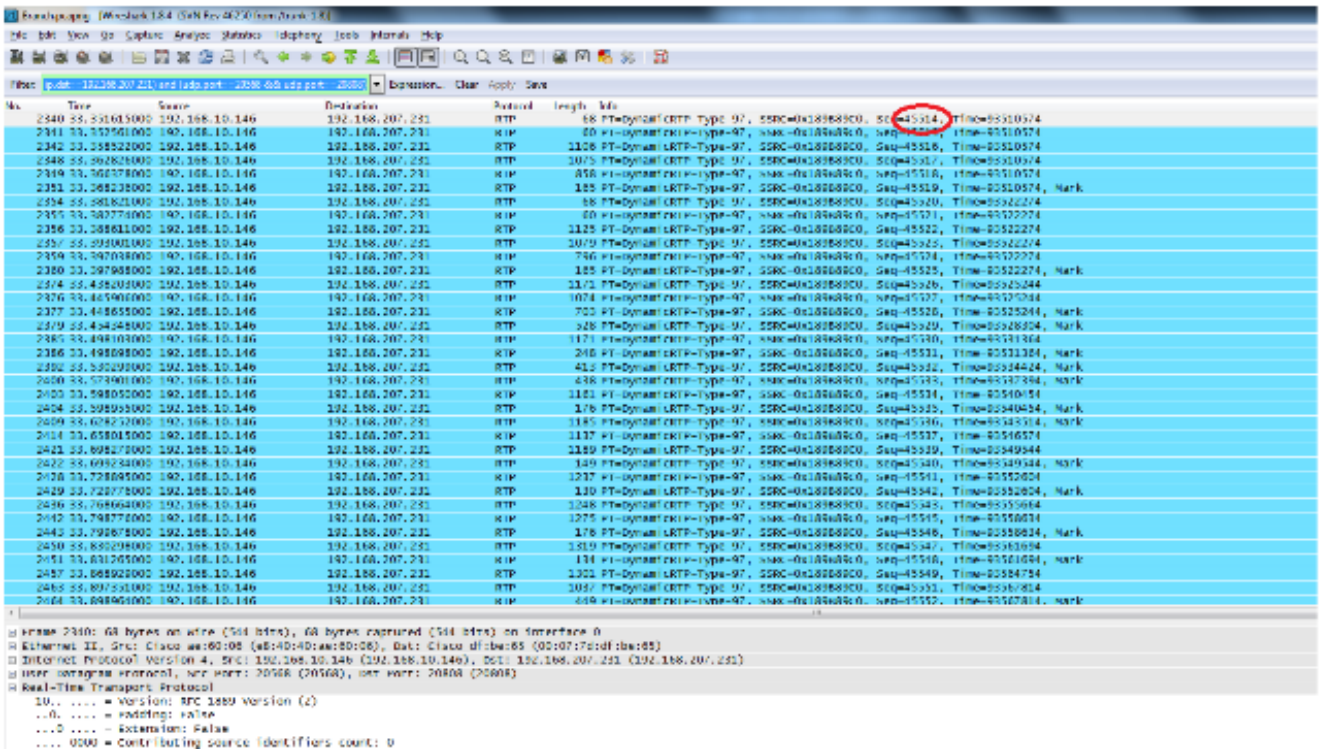
Vous restez avec un flux décodé en tant que RTP et l'autre en tant qu'UDP non décodé.



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

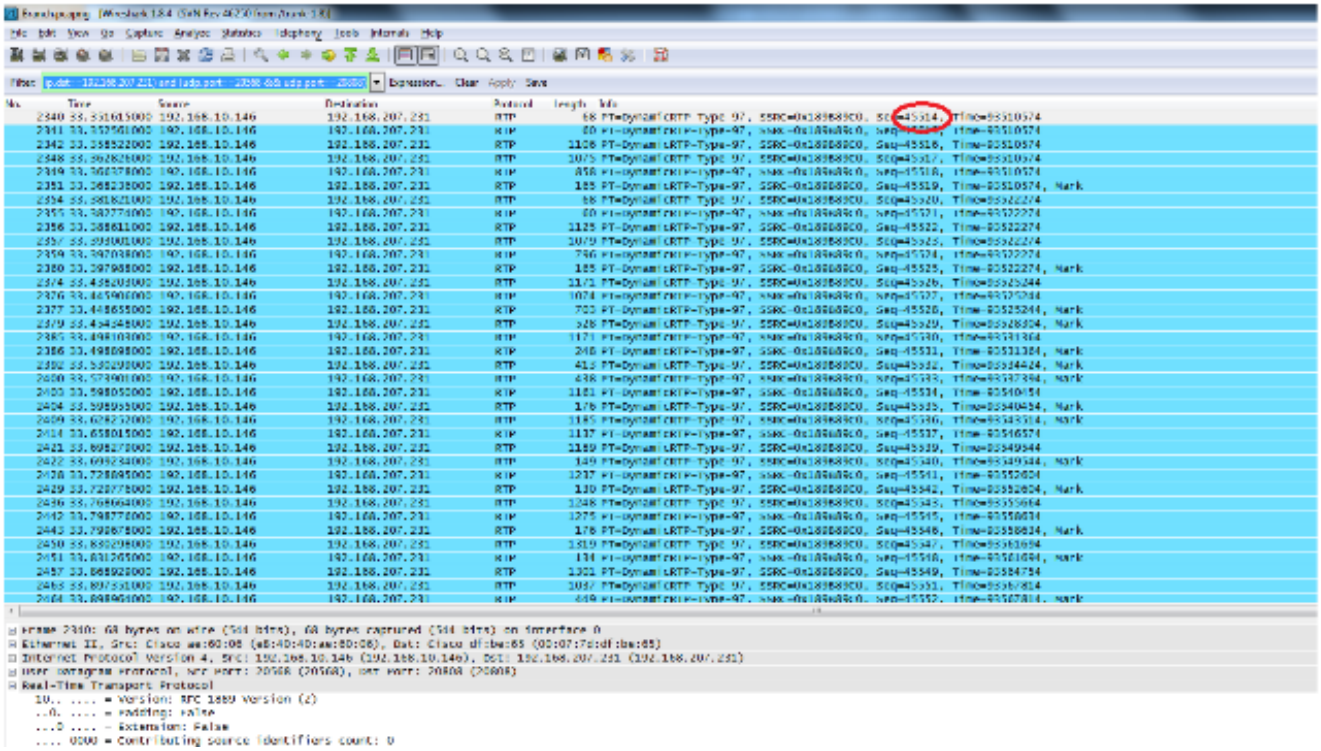


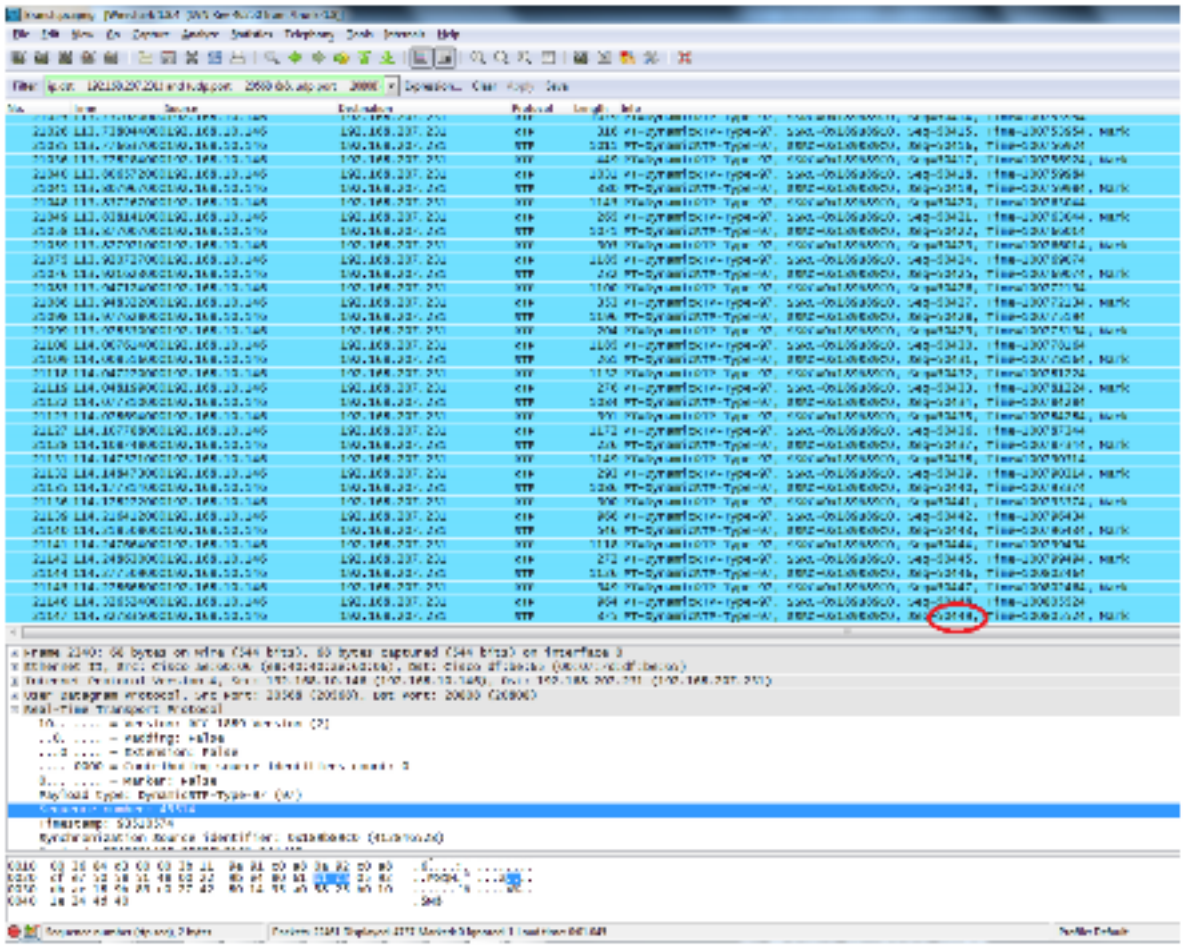
Le problème est maintenant uniquement lié à la qualité vidéo. Concentrez-vous sur le flux vidéo RTP et utilisez les numéros de port UDP de ce flux pour filtrer d'autres flux.

9. 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.





Le premier numéro de séquence RTP est 45514 et le dernier est 50449 pour le flux RTP vidéo filtré.

10. Assurez-vous que les premiers et les derniers paquets de numéros de séquence RTP sont présents dans les deux captures (par exemple, les captures centrales et de filiale) et notez que le SSRC pour le flux serait le même sur les deux captures.

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.

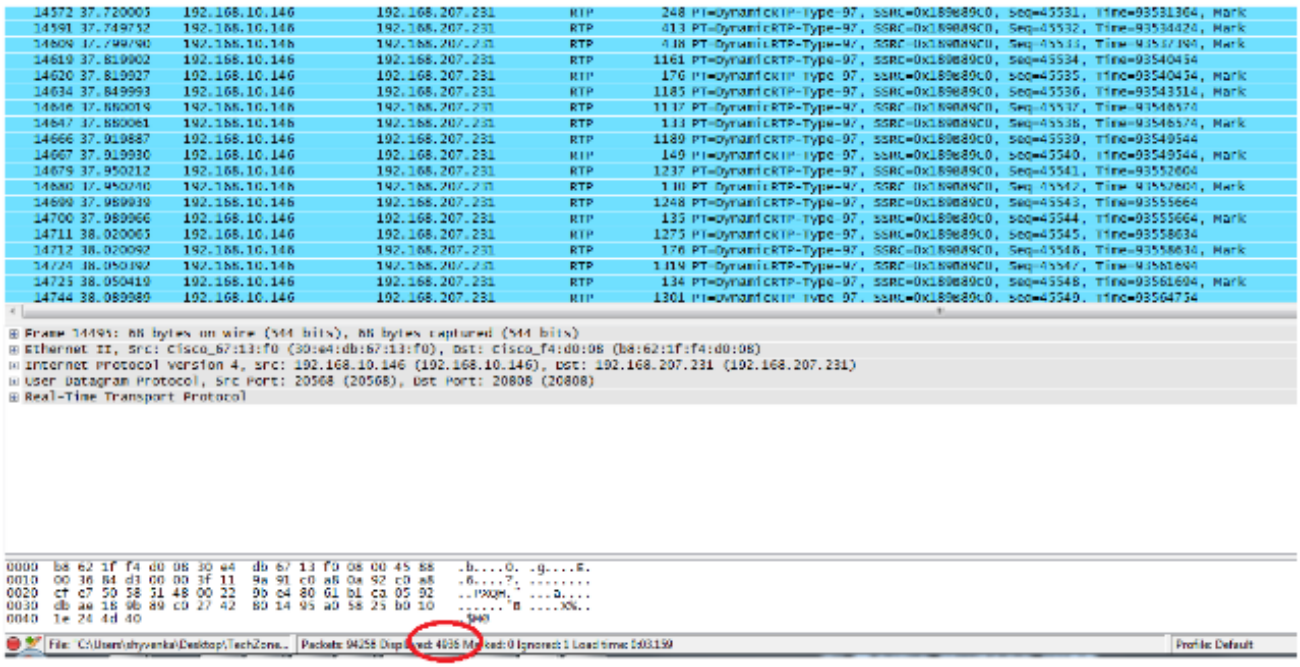
12. Sélectionnez un numéro de séquence de début et de fin. Ces paquets sont présents dans les captures et affinent le filtre pour afficher uniquement les paquets entre les numéros de séquence RTP de début et de fin. Le filtre pour ceci est :

```
(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 )
```

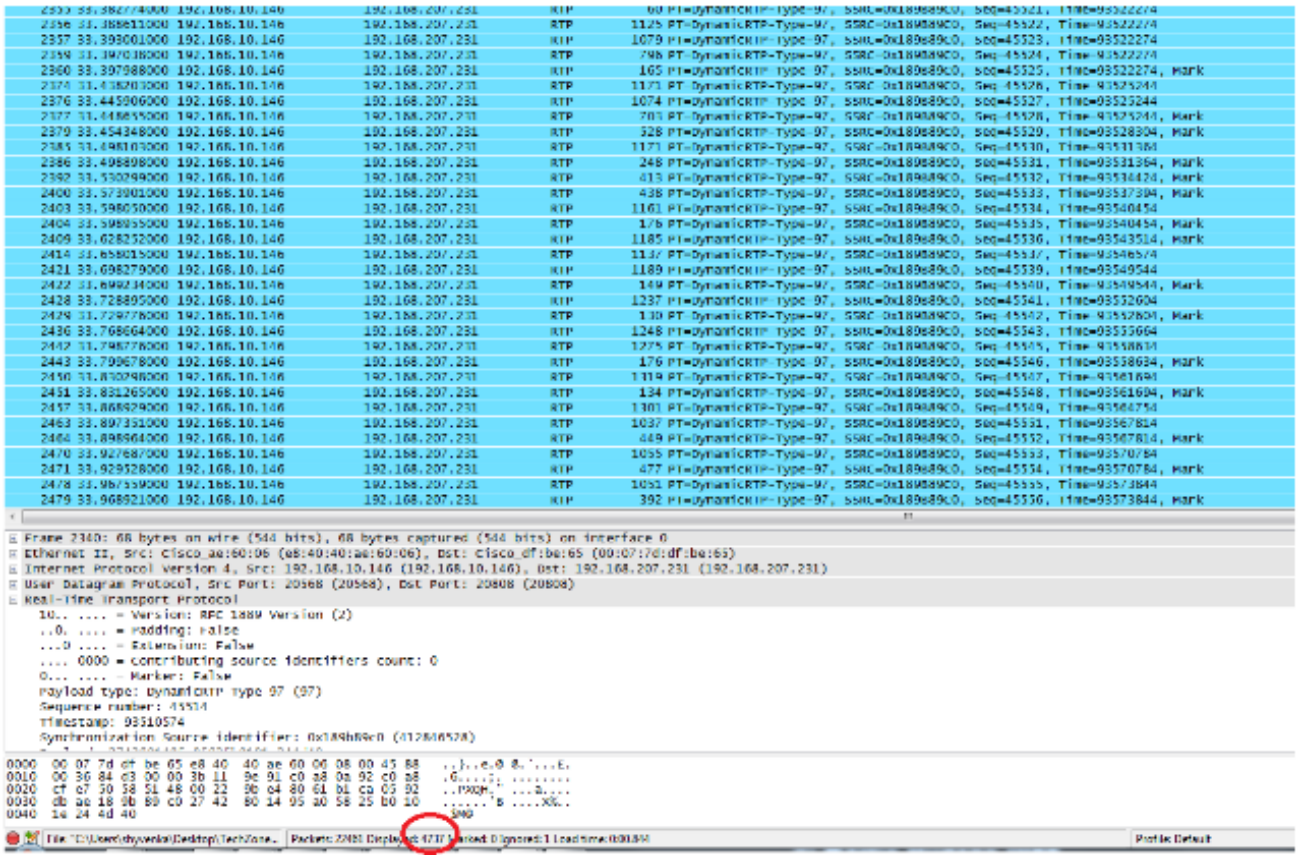
    Lorsque des captures sont prises simultanément, aucun paquet n'est manqué au début ou à la fin des deux captures. Si vous voyez que l'une des captures n'inclut pas quelques paquets au début/à la fin, utilisez le premier numéro de séquence ou le dernier numéro de séquence de la capture manquée dans les 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 :



    Site de la succursale :



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.