

Decifrar o fluxo RTP para análise de perda de pacotes no Wireshark para chamadas de voz e vídeo

Contents

[Introduction](#)

[Problema](#)

Introduction

Este documento descreve o processo de como decifrar o fluxo RTP (Real-Time Streaming) para análise de perda de pacotes no Wireshark para chamadas de voz e vídeo. Você pode usar os filtros do Wireshark para analisar capturas simultâneas de pacotes feitas na origem e no destino de uma chamada ou perto dela. Isso é útil quando você precisa solucionar problemas de qualidade de áudio e vídeo quando houver suspeita de perda de rede.


Problema

Este exemplo usa este fluxo de chamada:

Telefone IP A (site centralA) > switch 2960 > Roteador > Roteador WAN (site central) > IPWAN > Roteador WAN (site B) > Roteador > 2960 > Telefone IP B

Neste cenário, o problema encontrado é que as chamadas de vídeo do telefone IP A para o telefone IP B resultam em má qualidade de vídeo do site central A para a filial B, onde a central tem boa qualidade, mas a filial tem problemas.

Veja o receptor perdeu pacotes nas estatísticas de transmissão do telefone IP da filial:

		<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	

Solução

A má qualidade é vista apenas na filial e como o site central vê uma boa imagem, parece que o fluxo da central para a filial parece estar perdendo pacotes pela rede.

IP addressing scheme

Central IP phone: 192.168.10.146

Central Gateway: 192.168.10.253

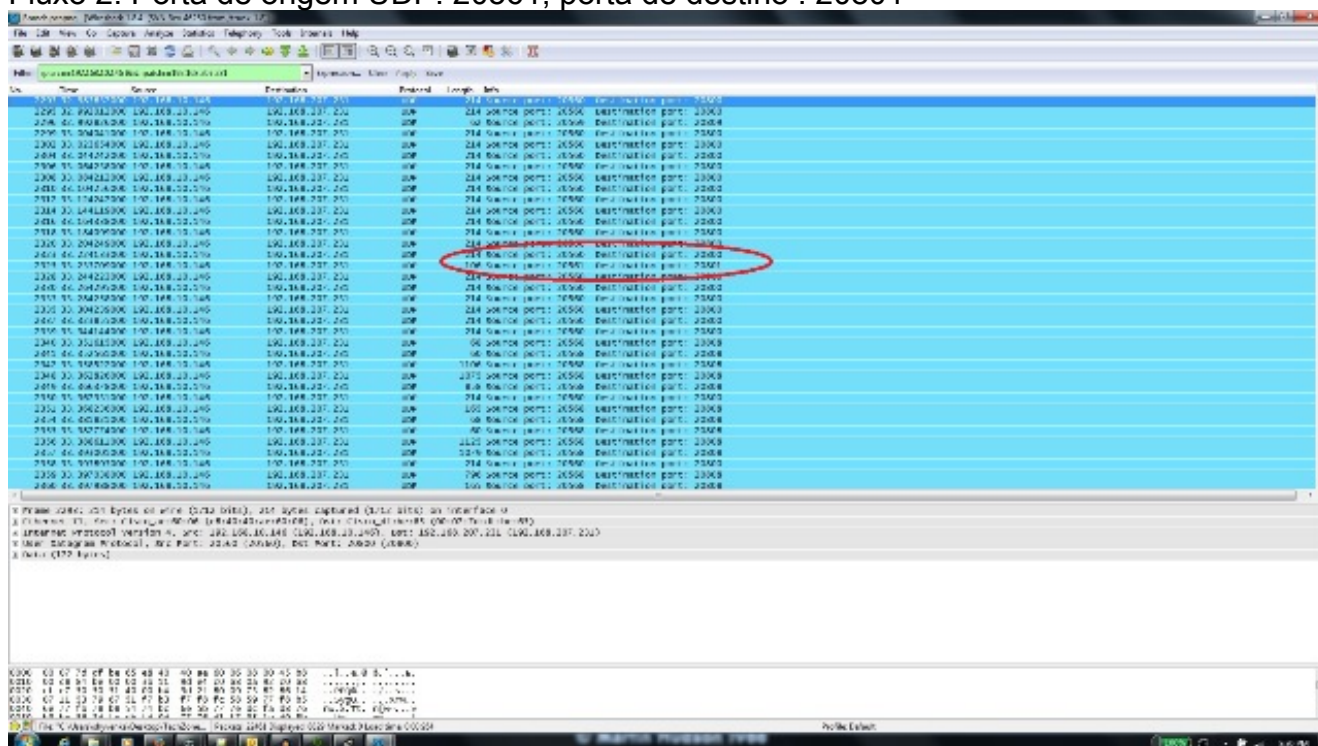
Central WAN router: 192.168.10.254
Branch WAN router: 192.168.206.210
Branch Gateway: 192.168.206.253
Branch IP phone: 192.168.207.231

As capturas de pacotes são feitas no roteador da WAN Central e da Filial e a WAN descarta esses pacotes. Foco no fluxo de RTP do telefone IP central (192.168.10.146) para o telefone IP da filial (192.168.207.231). Esse fluxo perde pacotes no roteador da WAN da filial se a WAN descartar os pacotes no fluxo do roteador da WAN central para o roteador da WAN da filial. Use as opções de filtro no wireshark para isolar o problema:

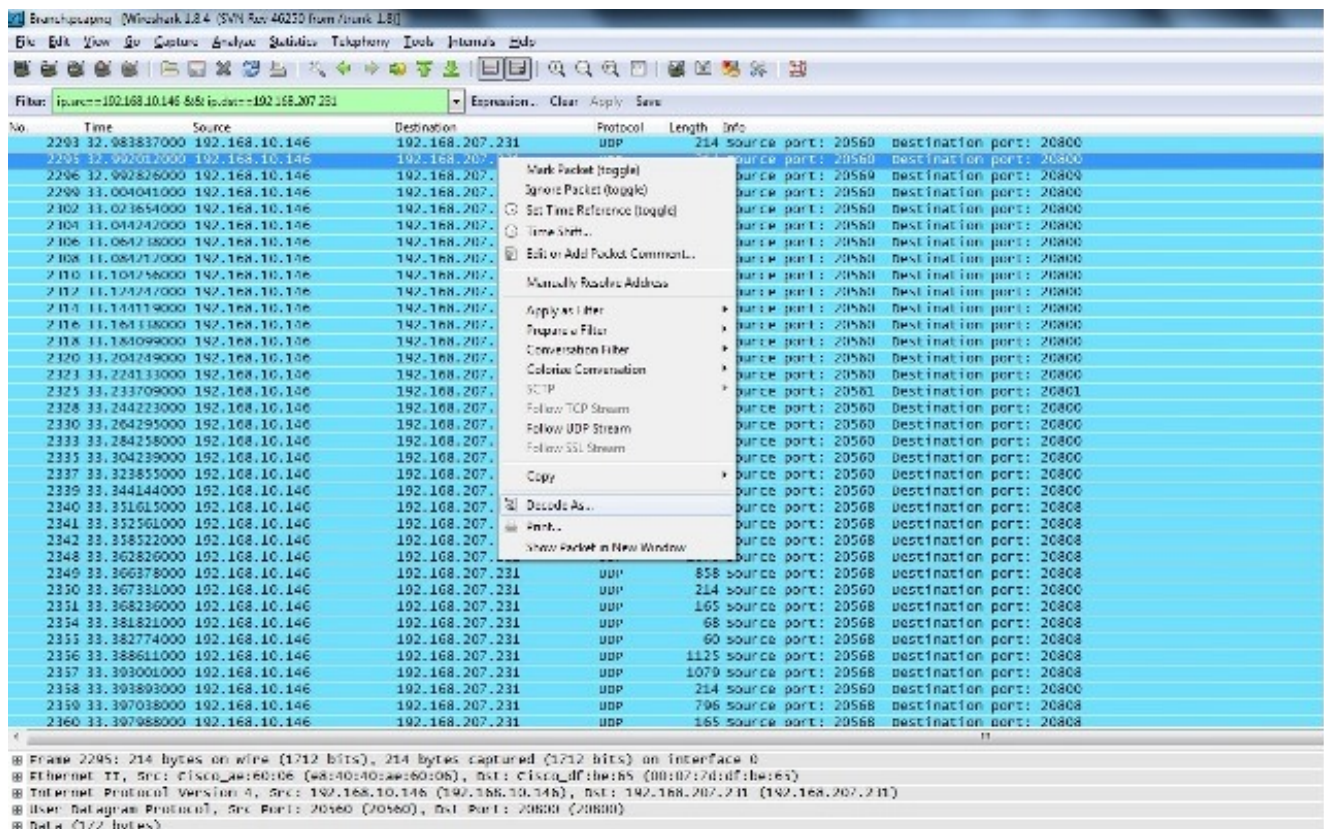
1. Abra a captura no wireshark.
2. Use o filtro `ip.src==192.168.10.146 && ip.dst==192.168.207.231`. Isso filtra todos os fluxos UDP do telefone IP central para o telefone IP da filial.
3. Execute a análise somente na captura do lado da filial, mas observe que você deve executar essas etapas para a captura central também.
4. Nesta captura de tela, o fluxo UDP é filtrado entre os endereços IP origem e destino e contém dois fluxos UDP (diferenciados pelos números de porta UDP). Esta é uma chamada de vídeo, portanto há dois fluxos: áudio e vídeo. Neste exemplo, os dois fluxos são:

Fluxo 1: Porta de origem UDP: 20560, porta de destino : 20800

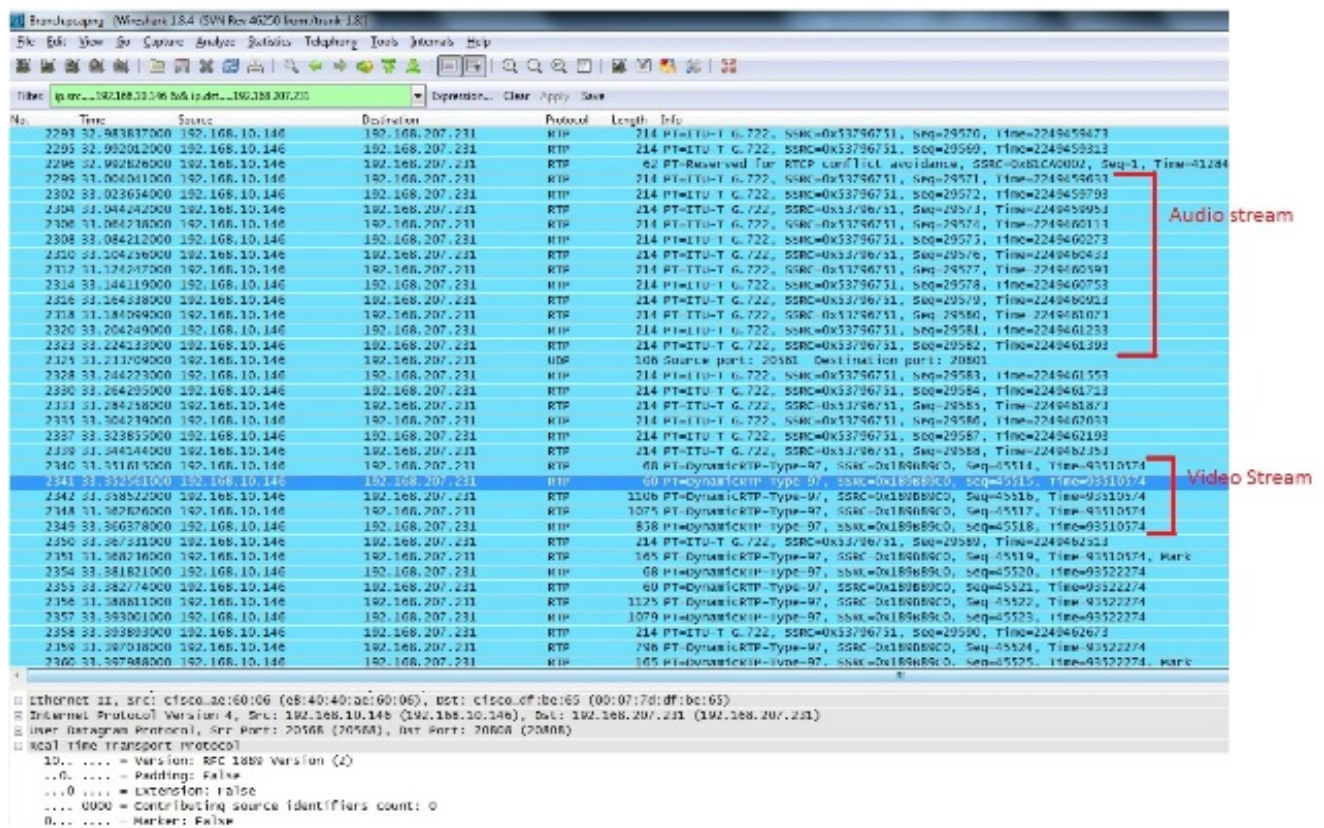
Fluxo 2: Porta de origem UDP: 20561, porta de destino : 20801



5. Selecione um pacote de um dos fluxos e clique com o botão direito do mouse no pacote.
6. Selecionar **Decodificar como...** e digite RTP.
7. Clique em **Aceitar** e **Ok** para decodificar o fluxo como RTP.



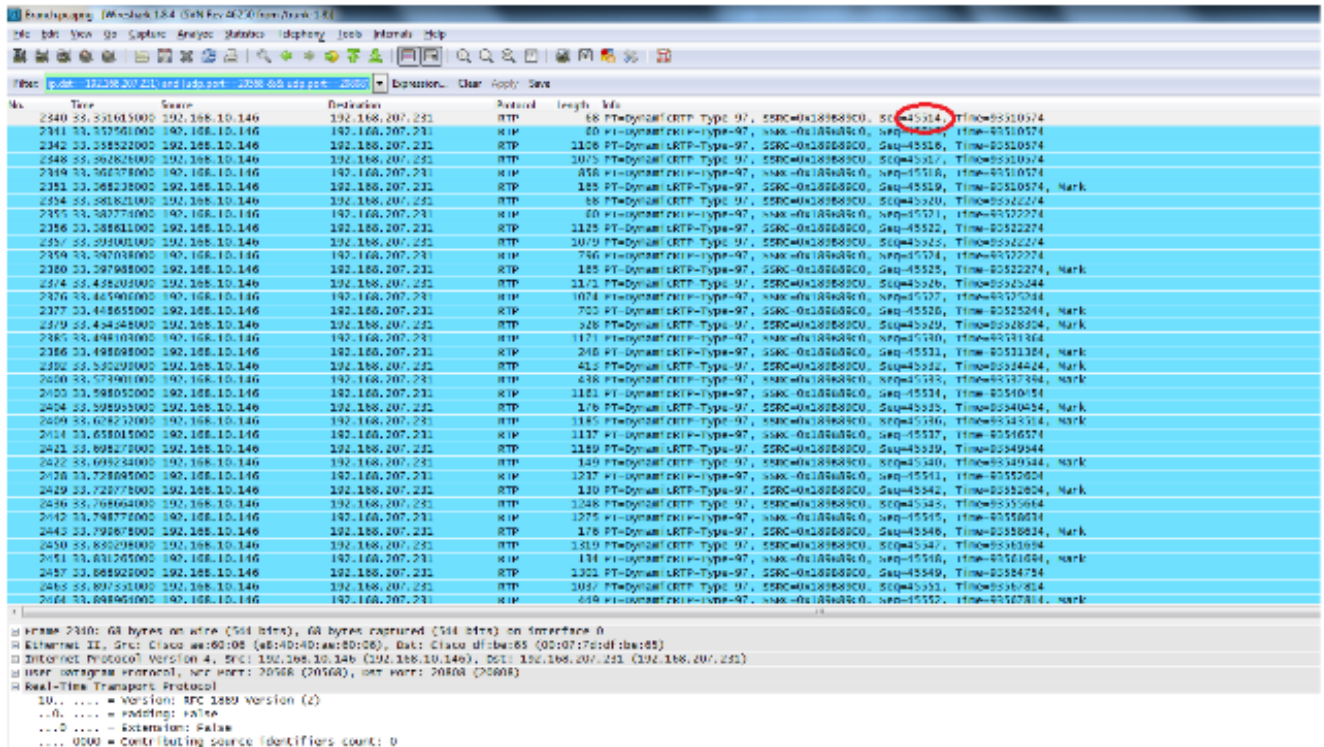
Você é deixado com um fluxo decodificado como RTP e o outro como UDP não decodificado.



8. Selecione um pacote do fluxo não decodificado e decodifique-o como RTP. Isso decodifica os fluxos de áudio e vídeo no RTP.

Observação: o fluxo de áudio está no formato de codec G.722 e o tipo de payload Dynamic-

RTP-97 indica o fluxo de vídeo RTP.



O problema agora está apenas na qualidade do vídeo. Concentre-se no fluxo de RTP de vídeo e use os números de porta UDP para esse fluxo para filtrar outros fluxos.

- 9. Visualize o número da porta selecionando um dos pacotes que exibe as informações da porta UDP no painel inferior do utilitário Wireshark. Na captura de tela anterior, um dos pacotes do fluxo de vídeo é selecionado e você pode ver as informações da porta Src (20568) e da porta Dst (20808) no painel inferior.

Tip: Use este filtro: (ip.src==192.168.10.146 && ip.dst==192.168.207.231) && (udp.port eq 20568 e udp.port eq 20808). Você verá apenas o fluxo de RTP de vídeo mostrado nesta captura de tela.

Note: Anote o primeiro e o último número de sequência RTP para este fluxo.

11. Refine o filtro para corresponder somente os pacotes entre o primeiro e o último fluxo de RTP.

Os números de sequência são usados para refinar o fluxo caso as capturas não tenham sido feitas simultaneamente, mas com um pequeno atraso entre elas.

Note: É possível que a filial inicie alguns números de sequência após 45514.

12. Selecione um número de sequência inicial e final. Esses pacotes estão presentes em ambas as capturas e refinam o filtro para exibir somente esses pacotes entre os números de sequência de RTP inicial e final. O filtro para isso é:

```
(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 as capturas são feitas simultaneamente, nenhum pacote é perdido no início ou no fim das duas capturas. Se você vir que uma das capturas não inclui alguns pacotes no início/fim, use o primeiro número de sequência ou o último número de sequência na captura perdida em ambos os pacotes para refinar o filtro para ambas as capturas. Observe os pacotes capturados em ambos os pontos entre os mesmos números de sequência (intervalo de número de sequência RTP).

Ao aplicar o filtro, você vê isso no site central e na filial:

Site central:

The screenshot shows the Wireshark interface with a packet capture list and details pane. The packet list shows a series of RTP packets between 192.168.10.146 and 192.168.207.231. The details pane shows the following information:

- Ethernet II, Src: cisco_67:13: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

The packet list shows the following information:

No.	Time	Source	Destination	Protocol	Length	Info
14572	37.720003	192.168.10.146	192.168.207.231	RTP	248	PT=Dynami... Type=97, SSRC=0x189e89c0, Seq=45531, Time=93551364, Mark
14591	37.749752	192.168.10.146	192.168.207.231	RTP	613	PT=Dynami... Type=97, SSRC=0x189e89c0, Seq=45532, Time=93554426, Mark
14608	37.779490	192.168.10.146	192.168.207.231	RTP	518	PT=Dynami... Type=97, SSRC=0x189e89c0, Seq=45533, Time=93557490, Mark
14619	37.810902	192.168.10.146	192.168.207.231	RTP	1161	PT=Dynami... Type=97, SSRC=0x189e89c0, Seq=45534, Time=93560434
14620	37.843927	192.168.10.146	192.168.207.231	RTP	176	PT=Dynami... Type=97, SSRC=0x189e89c0, Seq=45535, Time=93564034, Mark
14634	37.849993	192.168.10.146	192.168.207.231	RTP	1185	PT=Dynami... Type=97, SSRC=0x189e89c0, Seq=45536, Time=93567314, Mark
14656	37.880094	192.168.10.146	192.168.207.231	RTP	1117	PT=Dynami... Type=97, SSRC=0x189e89c0, Seq=45537, Time=93570376
14667	37.910687	192.168.10.146	192.168.207.231	RTP	1189	PT=Dynami... Type=97, SSRC=0x189e89c0, Seq=45538, Time=93573756, Mark
14667	37.910690	192.168.10.146	192.168.207.231	RTP	149	PT=Dynami... Type=97, SSRC=0x189e89c0, Seq=45540, Time=93574544, Mark
14679	37.950212	192.168.10.146	192.168.207.231	RTP	1237	PT=Dynami... Type=97, SSRC=0x189e89c0, Seq=45541, Time=93577604
14680	37.980090	192.168.10.146	192.168.207.231	RTP	1101	PT=Dynami... Type=97, SSRC=0x189e89c0, Seq=45542, Time=93580604, Mark
14699	37.989939	192.168.10.146	192.168.207.231	RTP	1248	PT=Dynami... Type=97, SSRC=0x189e89c0, Seq=45543, Time=93583604
14700	37.989966	192.168.10.146	192.168.207.231	RTP	135	PT=Dynami... Type=97, SSRC=0x189e89c0, Seq=45544, Time=93586604, Mark
14711	38.020063	192.168.10.146	192.168.207.231	RTP	1275	PT=Dynami... Type=97, SSRC=0x189e89c0, Seq=45545, Time=93589634
14712	38.020092	192.168.10.146	192.168.207.231	RTP	176	PT=Dynami... Type=97, SSRC=0x189e89c0, Seq=45546, Time=93592634, Mark
14724	38.050182	192.168.10.146	192.168.207.231	RTP	1114	PT=Dynami... Type=97, SSRC=0x189e89c0, Seq=45547, Time=93595634
14725	38.050419	192.168.10.146	192.168.207.231	RTP	134	PT=Dynami... Type=97, SSRC=0x189e89c0, Seq=45548, Time=93598634, Mark
14744	38.089989	192.168.10.146	192.168.207.231	RTP	1301	PT=Dynami... Type=97, SSRC=0x189e89c0, Seq=45549, Time=93601634

Local da filial:

2337	33.39801000	192.168.10.146	192.168.207.231	RTP	60	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45521, Time=9352274
2338	33.39801000	192.168.10.146	192.168.207.231	RTP	1125	PT-DynamicRTP-Type-W/	SSRC=0x189b89c0, Seq=45522, Time=9352274
2337	33.39801000	192.168.10.146	192.168.207.231	RTP	1079	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45523, Time=9352274
2338	33.39801000	192.168.10.146	192.168.207.231	RTP	796	PT-DynamicRTP-Type-W/	SSRC=0x189b89c0, Seq=45524, Time=9352274
2360	33.397988000	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-W/	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-W/	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	33.498098000	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	33.598050000	192.168.10.146	192.168.207.231	RTP	176	PT-DynamicRTP-Type-W/	SSRC=0x189b89c0, Seq=45535, Time=9352274
2405	33.628252000	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-W/	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	33.698279000	192.168.10.146	192.168.207.231	RTP	149	PT-DynamicRTP-Type-W/	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	33.728895000	192.168.10.146	192.168.207.231	RTP	149	PT-DynamicRTP-Type-W/	SSRC=0x189b89c0, Seq=45541, Time=9352274
2436	33.768640000	192.168.10.146	192.168.207.231	RTP	1248	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45542, Time=9352274
2442	33.798678000	192.168.10.146	192.168.207.231	RTP	1275	PT-DynamicRTP-Type-97	SSRC=0x189b89c0, Seq=45543, Time=9352274
2443	33.798678000	192.168.10.146	192.168.207.231	RTP	176	PT-DynamicRTP-Type-W/	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	33.928528000	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-W/	SSRC=0x189b89c0, Seq=45552, Time=9352274
2479	33.968921000	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:60:9b (08:00:40:ae:60:06), Dst: Cisco_df:ba:65 (00:07:70: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)
  01 ..... = Padding: false
  02 ..... = Extension: false
  03 ..... = Contributing source identifiers count: 0
  04 ..... = Marker: false
  payload type: dynamicRTP type 97 (97)
  Sequence number: 45514
  Timestamp: 93510574
  Synchronization Source identifier: 0x189b89c0 (412866528)
  0000 00 07 7d 0f be 65 e8 40 40 ae 00 06 08 00 45 88  ....e.0 8.....
  0010 00 36 84 c3 00 0b 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 06 18 9b 8b c0 27 42 80 14 95 30 58 25 00 10  .......5.....
  0040 1a 24 ad 40 390
  
```

Observe a contagem de pacotes filtrados no painel inferior do utilitário Wireshark em ambas as capturas. A contagem **exibida** indica o número de pacotes que correspondem aos critérios de filtro desejados.

O local central tem 4.936 pacotes que correspondem aos critérios de filtragem desejados entre os números de sequência RTP de início (45514) e fim (50449), enquanto no local da filial há apenas 4.737 pacotes. Isso indica uma perda de 199 pacotes. Observe que esses 199 pacotes correspondem à contagem de "Rcvr Lost Pkts", vista nas estatísticas de transmissão do telefone IP da filial mostrada no início deste documento.

Isso confirma que todos os pacotes perdidos de Rcvr foram na verdade perdas de rede descartadas na WAN. É assim que o ponto de perda de pacotes na rede é isolado, enquanto os problemas de qualidade de áudio/vídeo são tratados com a suspeita de quedas de rede.