

音声とビデオ コールにおける Wireshark のパケット損失分析のための RTP ストリームの解読

内容

[概要](#)

[問題](#)

概要

このドキュメントでは、Wireshark で音声コールとビデオ コールのパケット損失分析を行うためにリアルタイム ストリーミング (RTP) ストリームを解読する方法について説明します。コールの送信元と宛先でまたはその近くで収集された同時パケット キャプチャを分析するために Wireshark フィルタを使用できます。これは、ネットワーク損失が疑われる音声とビデオの品質問題をトラブルシューティングする必要がある場合に役に立ちます。


問題

この例では、次のコール フローを使用します。

IP フォン A (セントラル サイト A) > 2960 スイッチ > ルータ > WAN ルータ (セントラル サイト) > IPWAN > WAN ルータ (サイト B) > ルータ > 2960 > IP フォン B

このシナリオで発生する問題は、IP フォン A から IP フォン B へのビデオ コールが、セントラル サイト A からブランチ サイト B に向かってビデオ品質が低下し、セントラルでは良かった品質がブランチ側では悪くなることです。

ブランチ IP フォンのストリーミング統計での受信側損失パケットを参照してください。

		<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	

解決方法

品質の悪化はブランチ側においてのみ見られ、セントラル サイトでの画像は良好なので、セントラル サイトからブランチ サイトまでのネットワーク上でパケットの損失が発生しているものと考えられます。

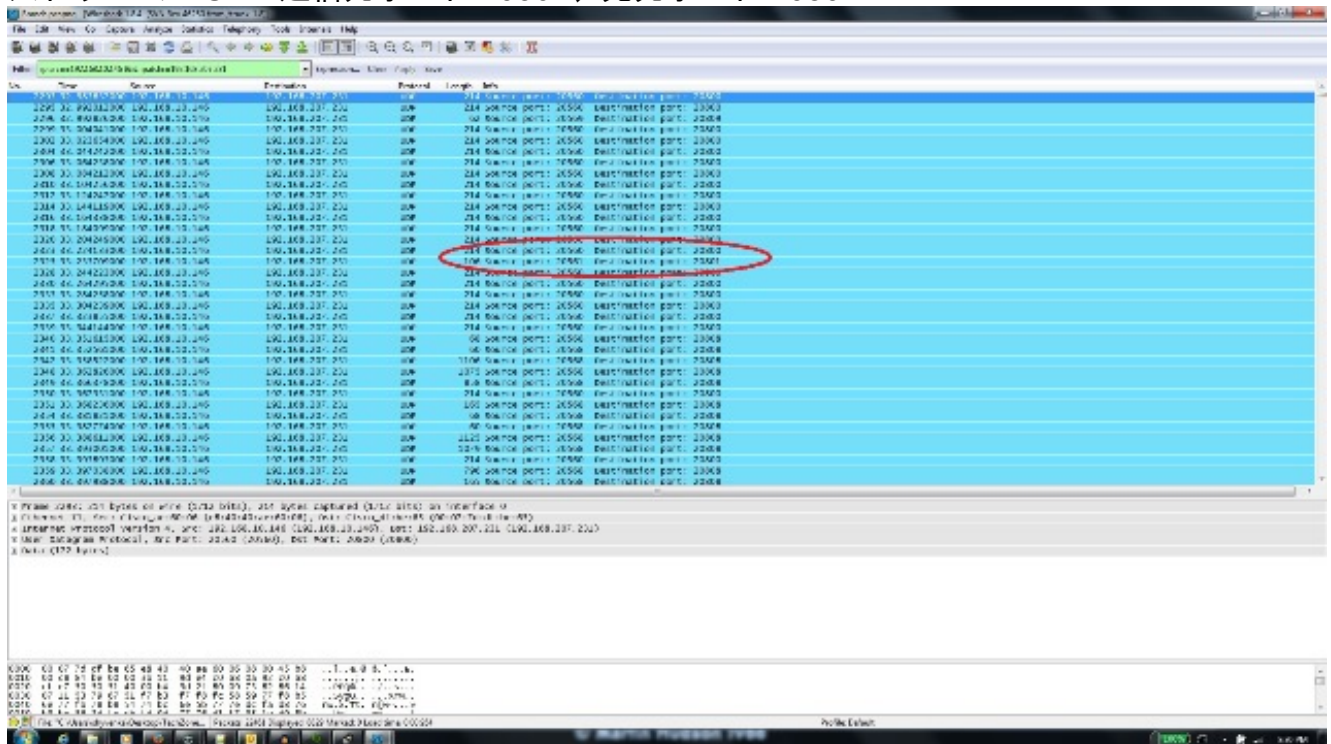
Central Gateway: 192.168.10.253
Central WAN router: 192.168.10.254
Branch WAN router: 192.168.206.210
Branch Gateway: 192.168.206.253
Branch IP phone: 192.168.207.231

パケット キャプチャはセントラルとブランチの WAN ルータで取得され、WAN でこれらのパケットがドロップしています。セントラル IP フォン (192.168.10.146) からブランチ IP フォン (192.168.207.231) への RTP ストリームに注目します。WANが中央WANルータからブランチWANルータへのストリームでパケットをドロップすると、このストリームはブランチWANルータでパケットを失います。問題を切り分けるには、wiresharkのフィルタオプションを使用します。

1. Wireshark でキャプチャを開きます。
2. フィルタip.src==192.168.10.146 && ip.dst==192.168.207.231を使用します。これにより、中央のIP電話からブランチのIP電話へのすべてのUDPストリームがフィルタリングされます。
3. ここではブランチ側のキャプチャについてのみ分析を実行しますが、セントラル キャプチャに対してもこれらの手順を実行する必要があることに注意してください。
4. このスクリーンショットでは、UDP ストリームは送信元と宛先の IP アドレスの間でフィルタリングされ、2 つの UDP ストリームが含まれます (UDP ポート番号を区別されます)。これはビデオ コールなので、2 つのストリームがあります。音声とビデオです。この例の 2 つのストリームは次のとおりです。

ストリーム 1:UDP 送信元ポート:20560、宛先ポート:20800

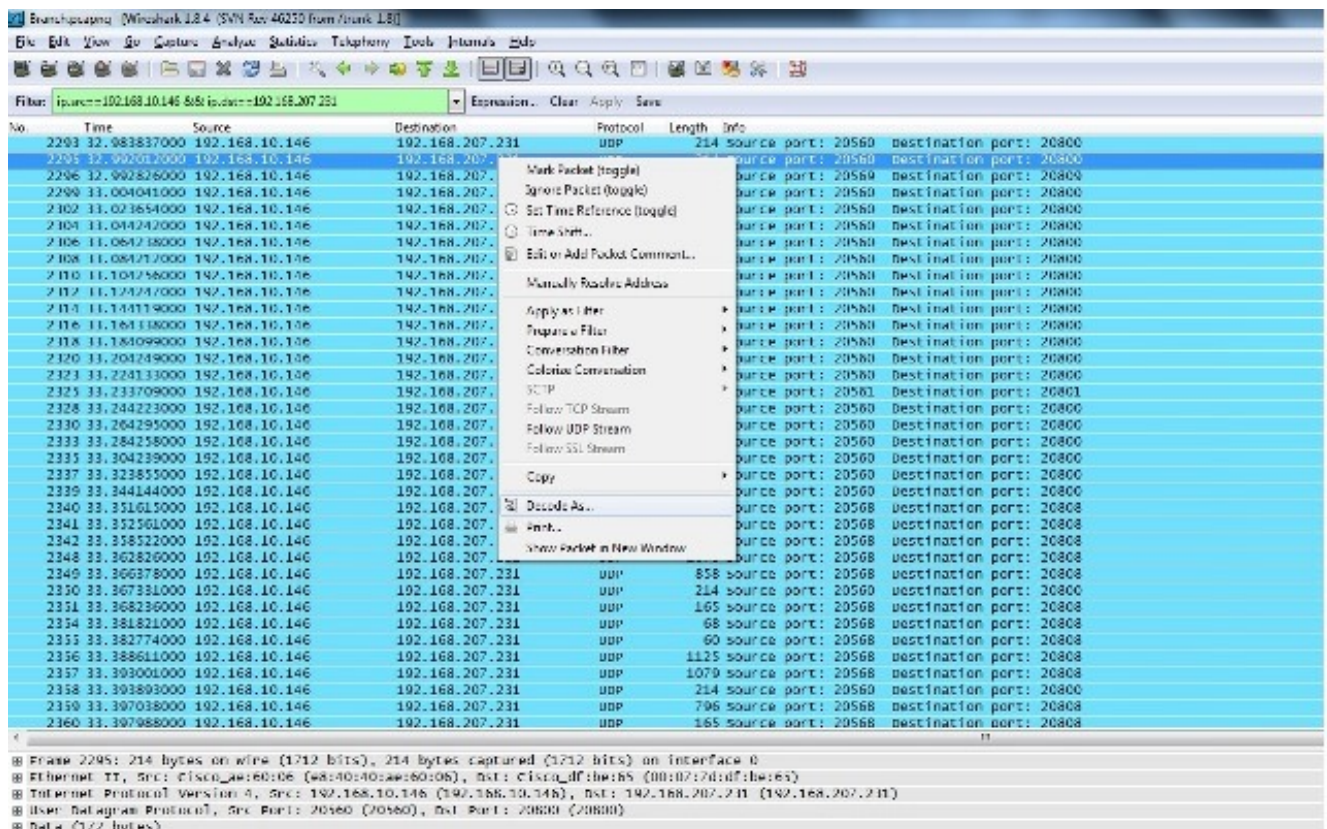
ストリーム 2:UDP 送信元ポート:20561、宛先ポート:20801



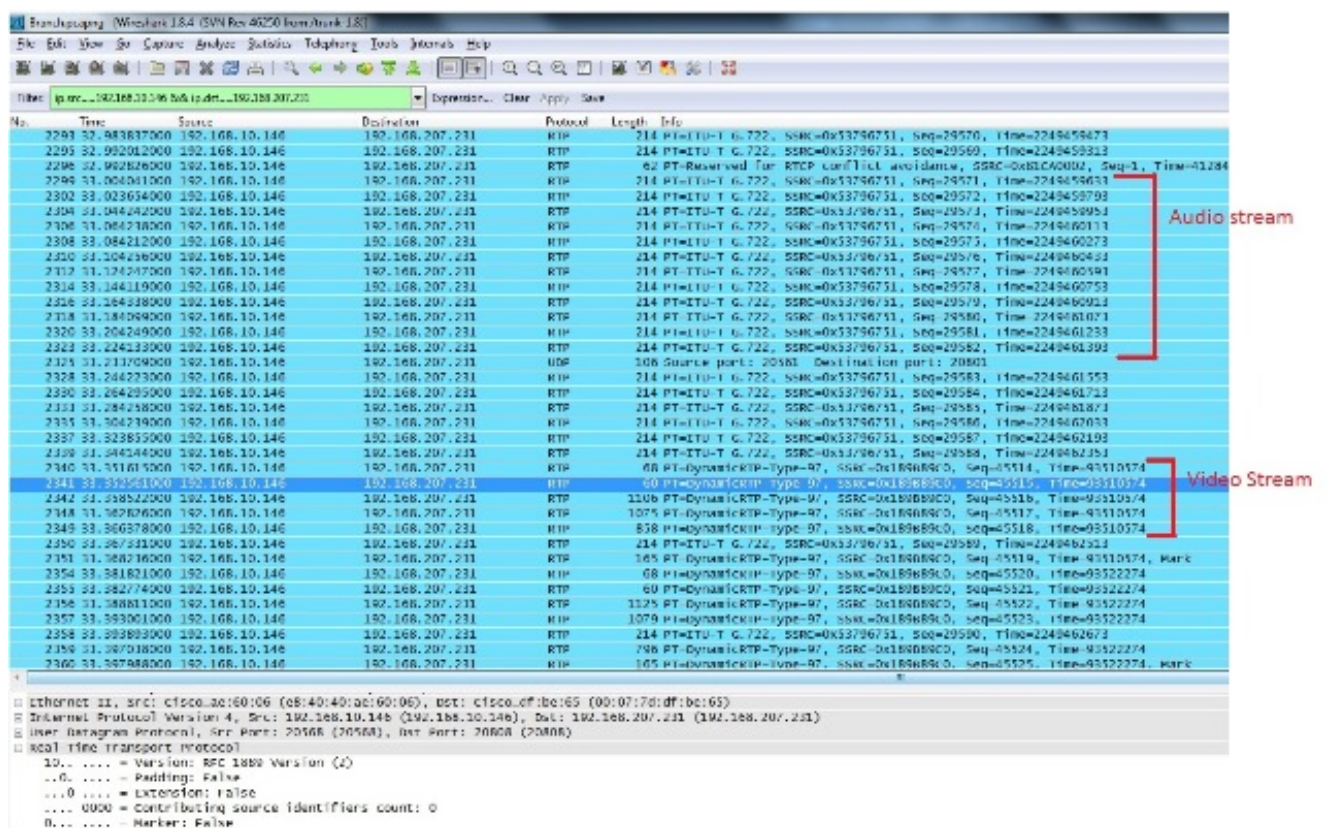
5. ストリームからパケットを 1 つ選択し、パケットを右クリックします。

6. [Decode As...] を選択して、「RTP」と入力します。

7. [Accept] をクリックして [OK] をクリックし、ストリームを RTP としてデコードします。

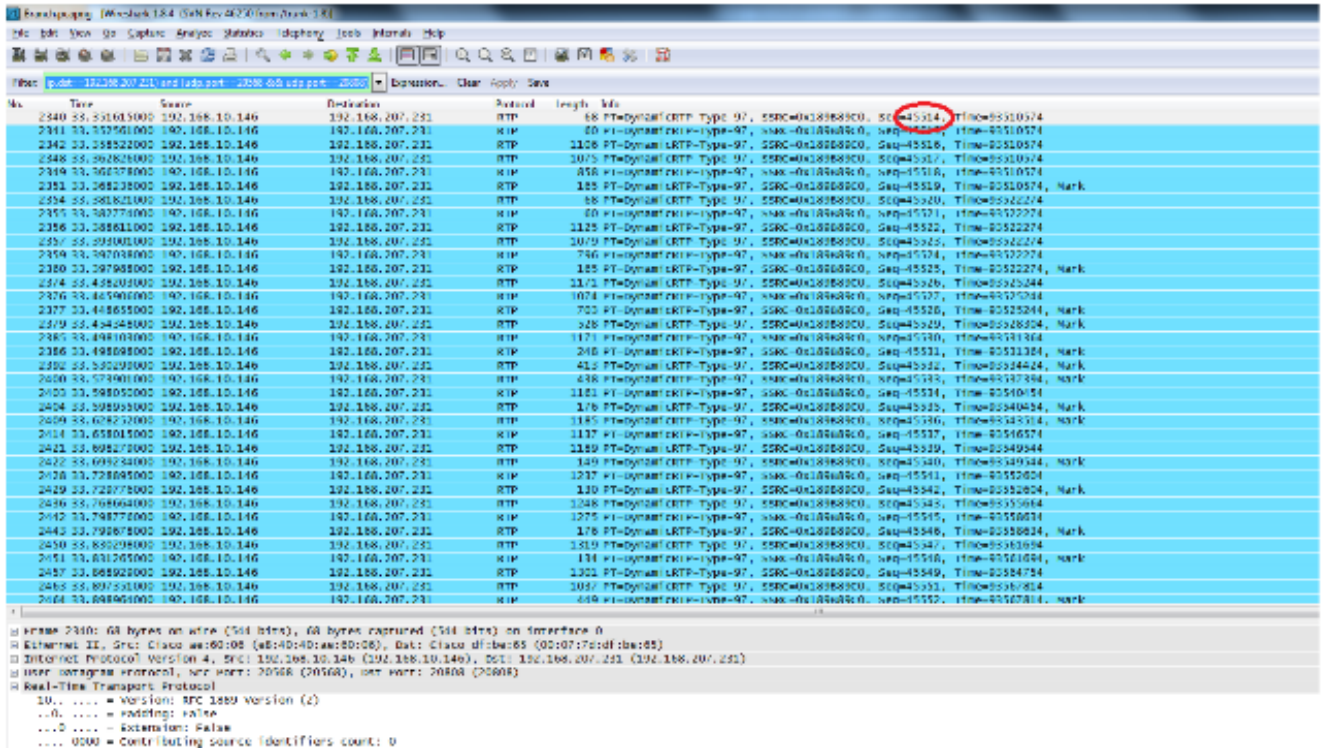


1つのストリームは RTP としてデコードされ、もう1つはデコードされていない UDP のままです。



8. デコードされていないストリームからパケットを選択し、RTPとしてデコードします。これにより、オーディオストリームとビデオストリームの両方がRTPにデコードされます。

注：オーディオストリームはG.722コーデック形式で、Dynamic-RTP-97ペイロードタイプはビデオRTPストリームを示します。



問題はビデオ品質のみになりました。ビデオRTPストリームに注目し、このストリームのUDPポート番号を使用して他のストリームを除外します。

9. パケットの1つを選択してポート番号を表示します。Wiresharkユーティリティの下部ペインに、UDPポートの情報が表示されます。前のスクリーンショットでは、ビデオストリームのパケットの1つが選択されており、送信元ポート(20568)と宛先ポート(20808)の情報を下部ペインで見ることができます。

ヒント：(ip.src==192.168.10.146 && ip.dst==192.168.207.231) && (udp.port eq 20568およびudp.port eq 20808)のフィルタを使用します。このスクリーンショットではビデオRTPストリームのみが示されています。

注：このストリームの最初と最後のRTPシーケンス番号を記録しておきます。

Wireshark packet capture showing RTP stream details. The 'Sequence' field in the 'RTP' section is circled in red, showing the value 45514. The packet list shows a sequence of RTP packets starting from sequence number 45514 and ending at 50449.

Wireshark packet capture showing RTP stream details. The 'Sequence' field in the 'RTP' section is circled in red, showing the value 50449. The packet list shows a sequence of RTP packets starting from sequence number 45514 and ending at 50449.

抽出されたビデオ RTP ストリームの最初の RTP シーケンス番号は 45514、最後のシーケンス番号は 50449 です。

- 最初と最後の RTP シーケンス番号のバケットが、両方のキャプチャ (たとえば、セントラル キャプチャとブランチ キャプチャ) に存在することを確認し、ストリームの SSRC が両方のキャプチャで一致することに注意します。

11. 最初と最後の RTP ストリームの間のパケットだけに一致するようにフィルタを調整します。

。

キャプチャが同時に取得されず、両者の間にわずかな遅延がある場合は、シーケンス番号を使用してストリームを調整します。

注：ブランチ サイトが 45514 の後にいくつかのシーケンス番号を開始している可能性があります。

12. 開始と終了のシーケンス番号を選択します。これらのパケットは両方のキャプチャに存在し、開始と終了の RTP シーケンス番号の間のパケットのみを表示するようにフィルタを調整します。このフィルタは次のようになります。

```
(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 )
```

キャプチャが同時に取得された場合は、両方のキャプチャの開始または終了時に失われたパケットはありません。キャプチャの 1 つの開始または終了時にいくつかのパケットが含まれない場合は、両方のパケットで失われたキャプチャの最初のシーケンス番号または最後のシーケンス番号を使用して、両方のキャプチャのフィルタを調整します。同じシーケンス番号の間に (RTP シーケンス番号範囲) 両方のポイントでキャプチャされたパケットを観察します。

フィルタを適用すると、セントラル サイトとブランチ サイトの表示は次のようになります。

セントラル サイト:

14572	37.720005	192.168.10.146	192.168.207.231	RTP	248	PT=DynamicRTP-Type-97, SSRC=0x180e89c0, Seq=45531, Time=93531364, Mark
14591	37.749752	192.168.10.146	192.168.207.231	RTP	413	PT=DynamicRTP-Type-97, SSRC=0x180e89c0, Seq=45532, Time=93534476, Mark
14609	37.799790	192.168.10.146	192.168.207.231	RTP	418	PT=DynamicRTP-Type-97, SSRC=0x180e89c0, Seq=45533, Time=93537180, Mark
14619	37.819902	192.168.10.146	192.168.207.231	RTP	1161	PT=DynamicRTP-Type-97, SSRC=0x180e89c0, Seq=45534, Time=93540434, Mark
14620	37.819927	192.168.10.146	192.168.207.231	RTP	176	PT=DynamicRTP-Type-97, SSRC=0x180e89c0, Seq=45535, Time=93540434, Mark
14634	37.849993	192.168.10.146	192.168.207.231	RTP	1185	PT=DynamicRTP-Type-97, SSRC=0x180e89c0, Seq=45536, Time=93543514, Mark
14646	37.860019	192.168.10.146	192.168.207.231	RTP	1117	PT=DynamicRTP-Type-97, SSRC=0x180e89c0, Seq=45537, Time=93546576, Mark
14647	37.860061	192.168.10.146	192.168.207.231	RTP	111	PT=DynamicRTP-Type-97, SSRC=0x180e89c0, Seq=45538, Time=93546576, Mark
14666	37.919887	192.168.10.146	192.168.207.231	RTP	1189	PT=DynamicRTP-Type-97, SSRC=0x180e89c0, Seq=45539, Time=93549544, Mark
14667	37.919930	192.168.10.146	192.168.207.231	RTP	149	PT=DynamicRTP-Type-97, SSRC=0x180e89c0, Seq=45540, Time=93549544, Mark
14679	37.950212	192.168.10.146	192.168.207.231	RTP	1237	PT=DynamicRTP-Type-97, SSRC=0x180e89c0, Seq=45541, Time=93552604, Mark
14680	37.950246	192.168.10.146	192.168.207.231	RTP	110	PT=DynamicRTP-Type-97, SSRC=0x180e89c0, Seq=45542, Time=93552604, Mark
14699	37.989939	192.168.10.146	192.168.207.231	RTP	1248	PT=DynamicRTP-Type-97, SSRC=0x180e89c0, Seq=45543, Time=93555664, Mark
14700	37.989966	192.168.10.146	192.168.207.231	RTP	135	PT=DynamicRTP-Type-97, SSRC=0x180e89c0, Seq=45544, Time=93555664, Mark
14711	38.020065	192.168.10.146	192.168.207.231	RTP	1275	PT=DynamicRTP-Type-97, SSRC=0x180e89c0, Seq=45545, Time=93558634, Mark
14712	38.020092	192.168.10.146	192.168.207.231	RTP	176	PT=DynamicRTP-Type-97, SSRC=0x180e89c0, Seq=45546, Time=93558634, Mark
14724	38.050192	192.168.10.146	192.168.207.231	RTP	1114	PT=DynamicRTP-Type-97, SSRC=0x180e89c0, Seq=45547, Time=93561694, Mark
14725	38.050419	192.168.10.146	192.168.207.231	RTP	134	PT=DynamicRTP-Type-97, SSRC=0x180e89c0, Seq=45548, Time=93561694, Mark
14744	38.089989	192.168.10.146	192.168.207.231	RTP	1301	PT=DynamicRTP-Type-97, SSRC=0x180e89c0, 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 (08:00:27: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

```

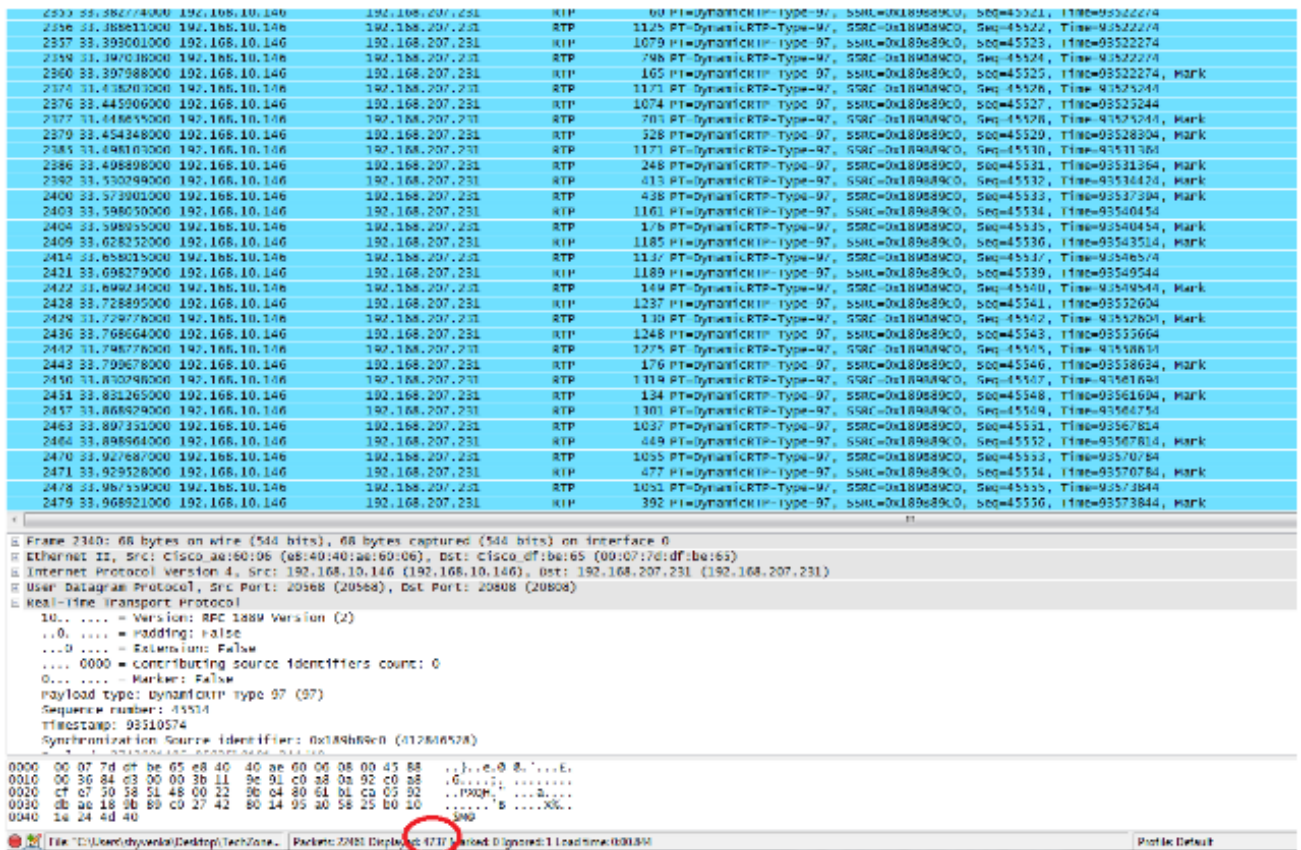
```

0000  08 02 1f f4 d0 08 30 e4 db 07 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  --RXXM...D...
0030  db ae 18 9b 89 c9 27 42 89 14 95 a9 58 25 b9 10  -.....*...X...
0040  1e 24 4d 40                                     .p

```

File: C:\Users\shyrenka\Desktop\Tech2con... Packets: 94/28 Dropped: 4525 Marked: 0 Ignored: 1 Load time: 503.19s Profile: Default

ブランチ サイト:



Wireshark ユーティリティの下部ペインで、両方のキャプチャのフィルタ処理されたパケット数に注意してください。[Displayed] の数は、指定したフィルタ条件に一致するパケットの数を示します。

開始 (45514) と終了 (50449) の RTP シーケンス番号の間で指定したフィルタ条件に一致するパケットの数は、セントラル サイトでは 4,936 個であるのに対し、ブランチ サイトでは 4,737 個だけです。これは、199個のパケットの損失を示します。これらの199個のパケットは、このドキュメントの最初に示すブランチ側のIP電話のストリーミング統計情報で見られる「Rcvr Lost Pkts」の数199個に一致9個です。

これにより、Rcvr Lost Packets のすべてが WAN 上のネットワーク損失で実際に失われたことがわかります。以上が、ネットワークドロップが疑われる音声とビデオの品質の問題に対処するとき、ネットワークのパケット損失ポイントを分離する方法です。