Decipher the RTP Stream for Packet Loss Analysis in Wireshark for Voice and Video Calls

Document ID: 117881

Contributed by Shyam Venkatesh, Cisco TAC Engineer.

Jul 28, 2014

Contents

Introduction

This document describes the process of how to decipher the Real−Time Streaming (RTP) stream for packet loss analysis in Wireshark for voice and video calls. You can use Wireshark filters in order to analyze simultaneous packet captures taken at or close−to the source and destination of a call. This is useful when you must troubleshoot audio and video quality issues when network losses are suspected.

Problem

This example uses this call flow:

IP phone A (central siteA) > 2960 switch > Router > WAN router (Central site) > IPWAN > WAN router(site B) > Router > 2960 > IP phone B

In this scenario, the problem encountered is that video calls from IP phone A to IP phone B result in bad video quality from central site A to branch site B where central has good quality but the branch side has issues.

See the receiver lost packets in the streaming statistics of the branch IP phone:

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

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

Bad quality is seen only on the branch side and because the central site sees a good image, it looks like the stream from the central to the branch site seems to be losing packets over the network.

```
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
```

The packet captures are taken on the Central and Branch WAN router and the WAN drops these packets. Focus on the RTP stream from central IP phone (192.168.10.146) to branch IP phone (192.168.207.231). This stream misses packets on the branch WAN router if the WAN drops the packets on the stream from central WAN router to branch WAN router. Use the filter options in wireshark to isolate the problem:

1. Open the capture in wireshark.

2. Use the filter ip.src==192.168.10.146 && ip.dst==192.168.207.231. This filters out all UDP streams

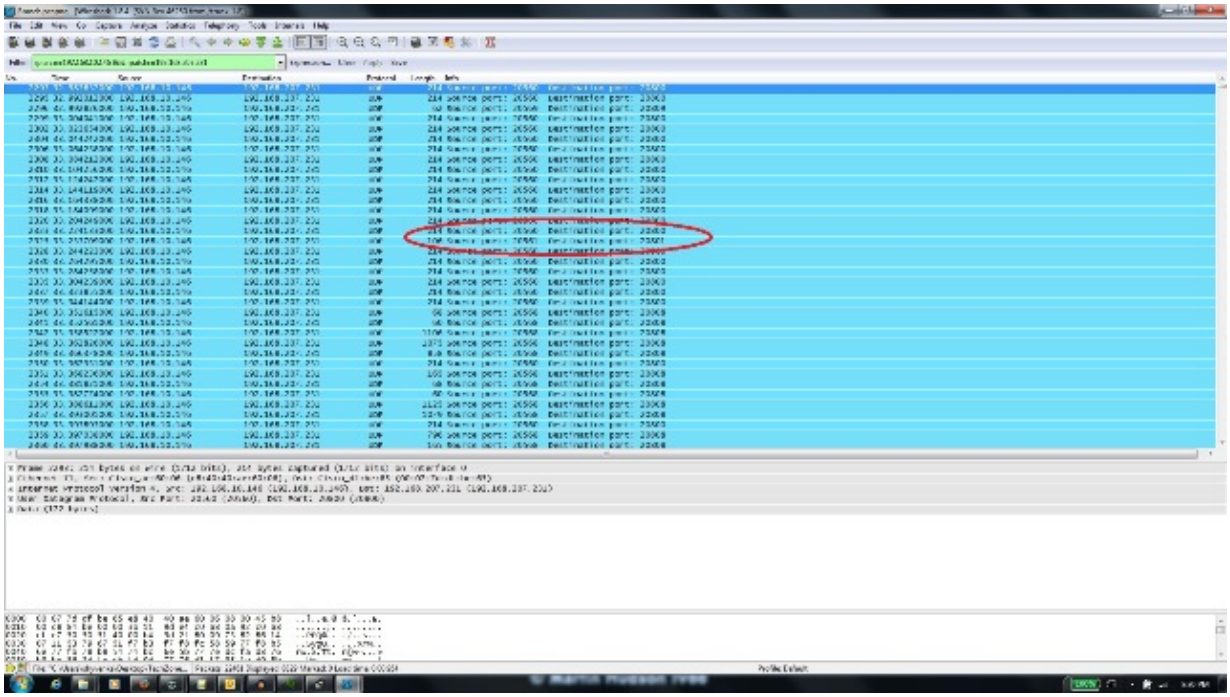
from central IP phone to branch IP phone.

3. Perform the analysis on the branch side capture only but note you must perform these steps for the central capture as well.

4. In this screenshot, the UDP stream is filtered between the source and the destination IP addresses and contains two UDP streams (differentiated by the UDP port numbers). This is a video call so there are two streams: audio and video. In this example, the two streams are:

    - Stream 1 : UDP source port : 20560, destination port : 20800

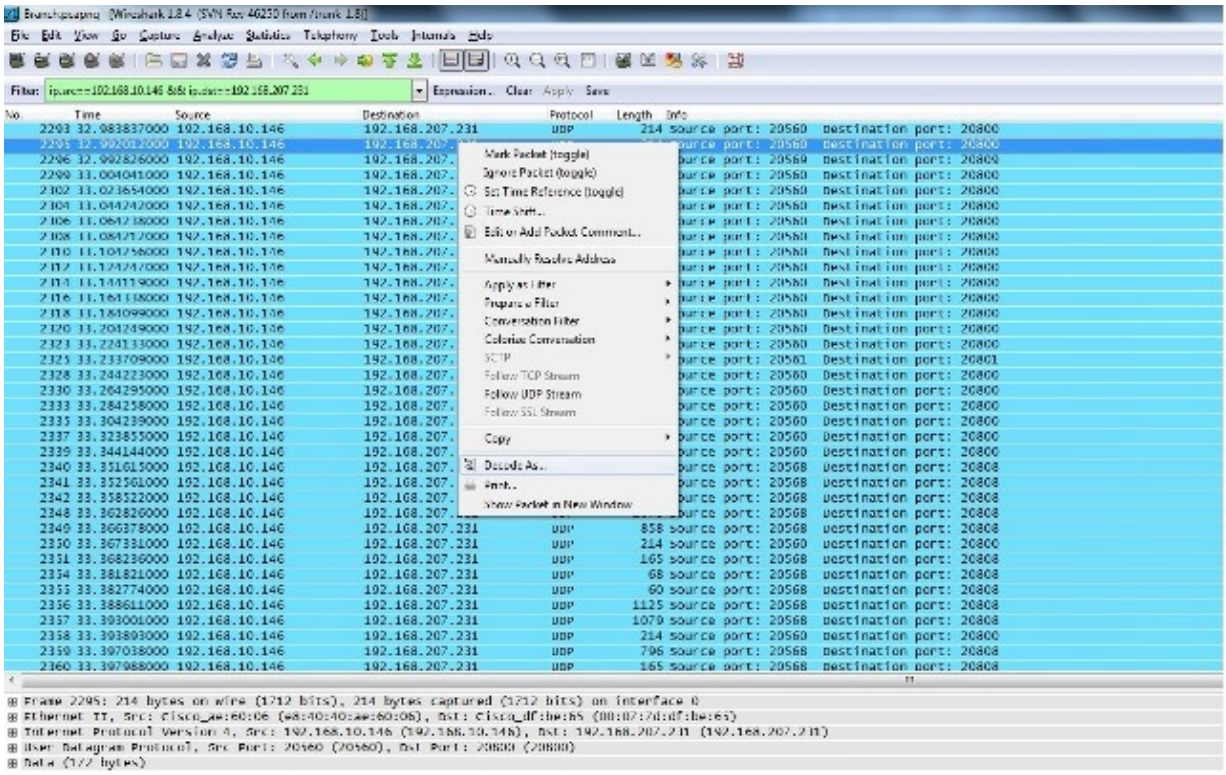
    - Stream 2 : UDP source port : 20561, destination port : 20801



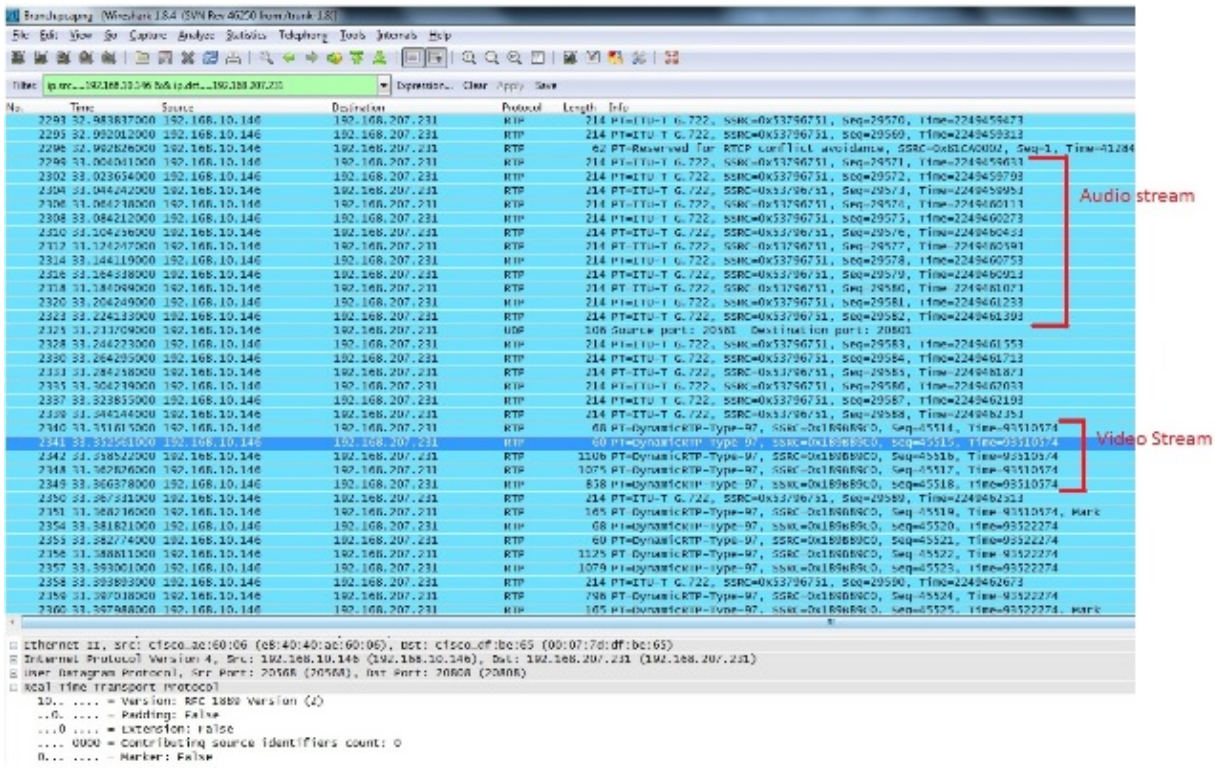
5. Select a packet from one of the streams and right−click the packet.

6. Select ***Decode As...*** and type ***RTP***.

7. Click ***Accept*** and ***Ok*** in order to decode the stream as RTP.

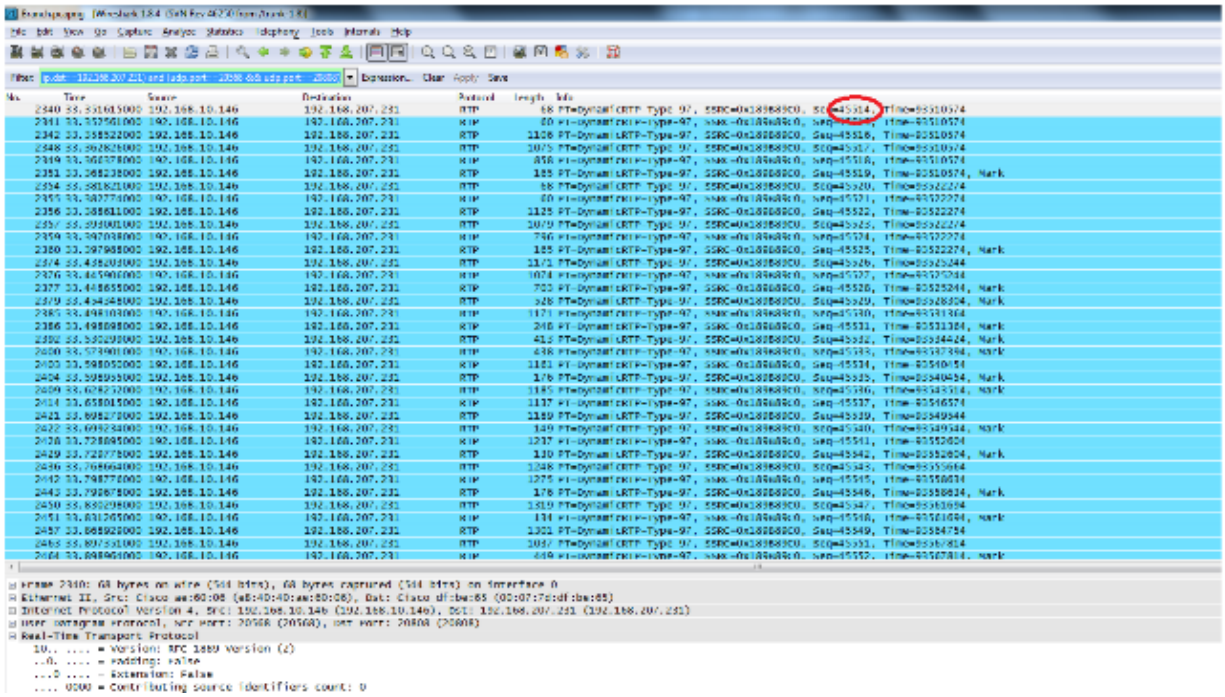


You are left with one stream decoded as RTP and the other as undecoded UDP.



8. Select a packet from the undecoded stream and decode it as RTP. This decodes both the audio and the video streams into RTP.

Note: The Audio stream is in G.722 codec format and the Dynamic−RTP−97 payload type indicates the video RTP stream.

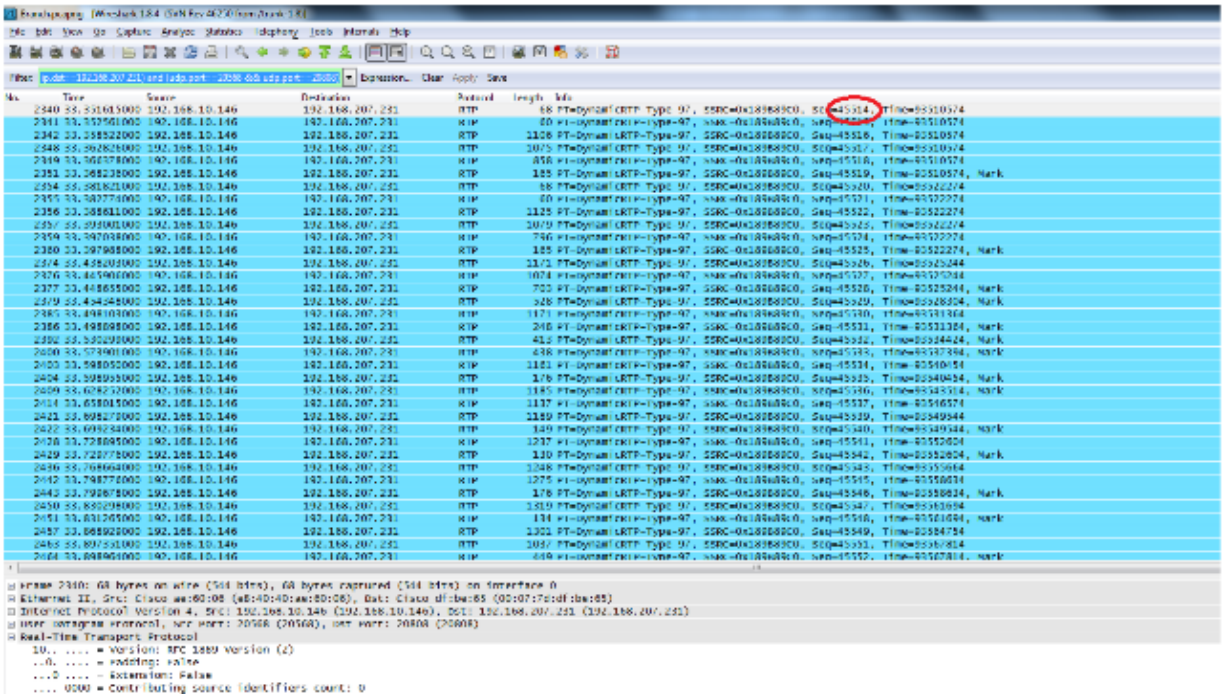


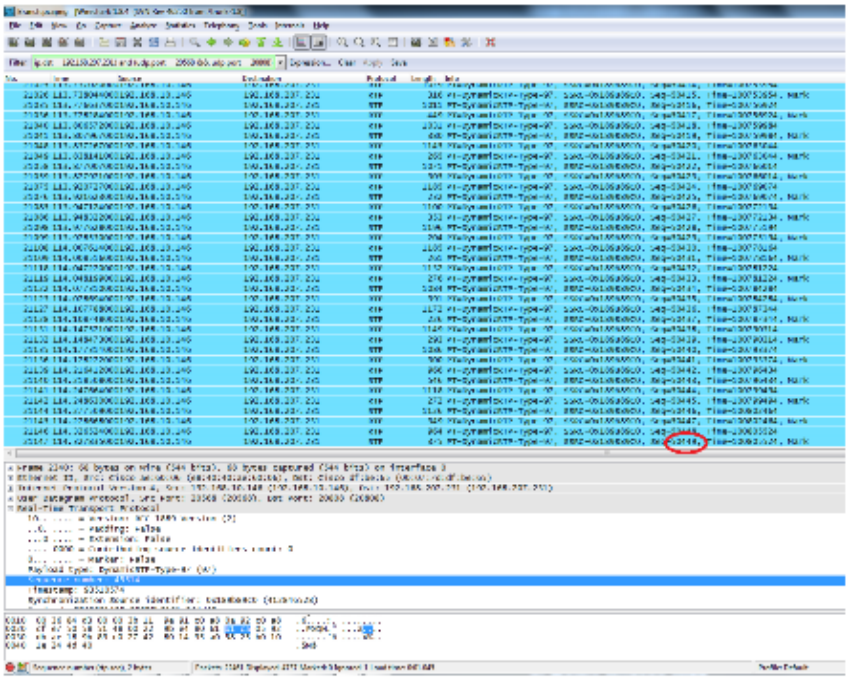
The problem is now only with video quality. Focus on the video RTP stream and use the UDP port numbers for this stream to filter out other streams.

9. View the port number by selecting one of the packets which displays the UDP port information on the bottom pane in the Wireshark utility. In the previous screenshot, one of the packets from the video stream is selected and you can see the Src Port (20568) and the Dst port (20808) information on the bottom pane.

Tip: Use this filter: (ip.src==192.168.10.146 && ip.dst==192.168.207.231) && (udp.port eq 20568 and udp.port eq 20808). You will only see the video RTP stream shown in this screenshot.

Note: Write down the first and the last RTP sequence numbers for this stream.





The first RTP sequence number is 45514 an the last is 50449 for the filtered out video RTP stream.

10. Make sure that the first and the last RTP sequence number packets are present in both captures.for example, central and branch captures) and note that the SSRC for the the stream would be the same on both the captures.
11. Refine the filter to match only the packets between the first and the last RTP streams.

    The sequence numbers are used to refine the stream in case the captures were not taken simultaneously, but with slight delay between them.

Note: It is possible that the branch site might start some sequence numbers after 45514.

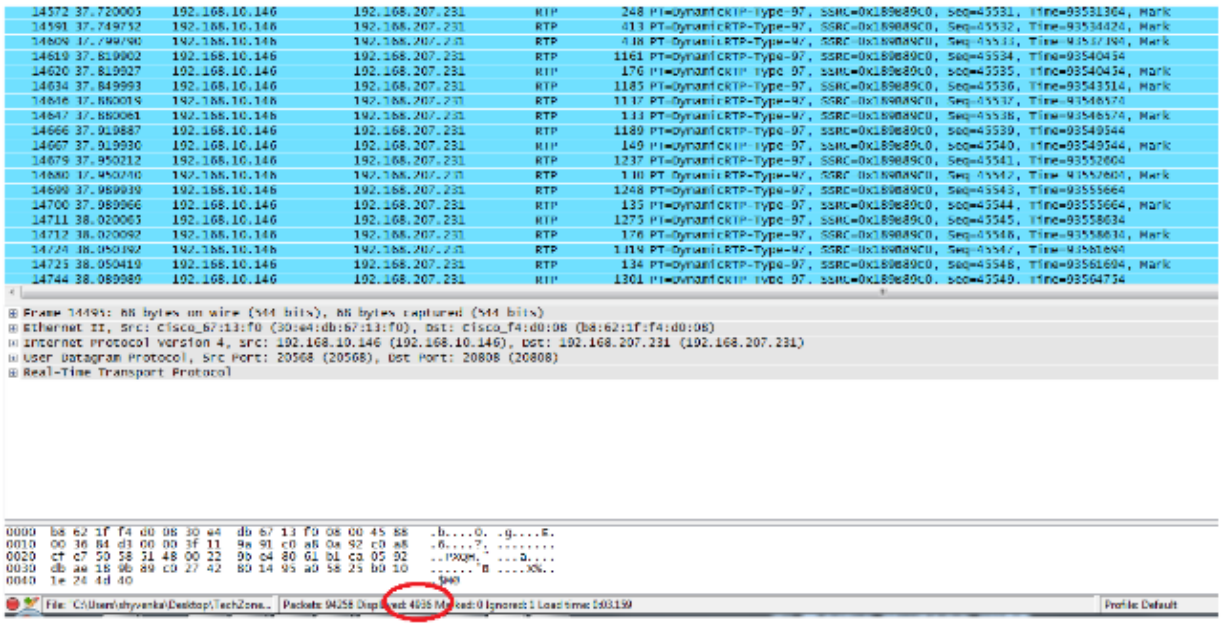
12. Select a start and end sequence number. These packets are present in both the captures and refine the filter to display only those packets between the start and the end RTP sequence numbers. The filter for this is:

```
(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 )
```

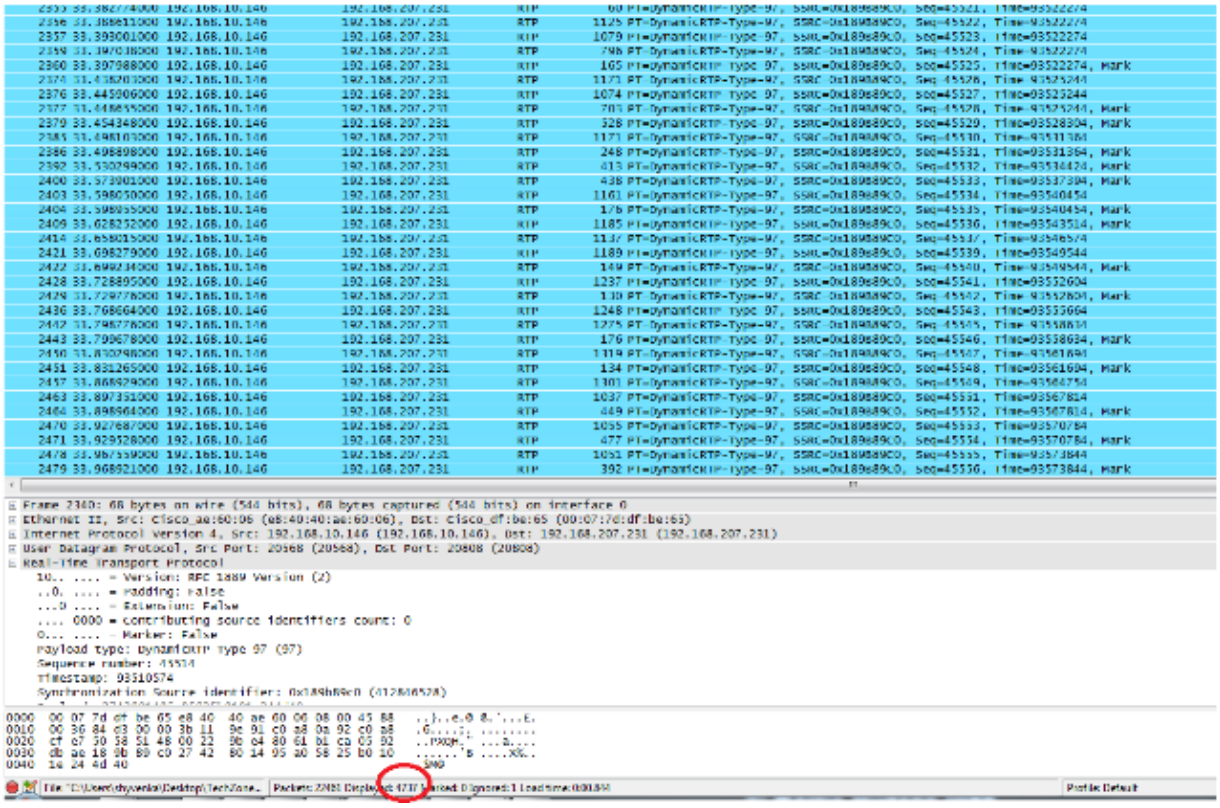
When captures are simultaneously taken, no packets are missed at the start or end on both captures. If you see that one of the captures does not include a few packets at the start/end, use the first sequence number or the last sequence number in the capture missed in both packets to refine the filter for both the captures. Observe the packets that captured at both points between the same sequence numbers (RTP sequence number range).

When you apply the filter, you see this at the central site and the branch site:

Central Site :



Branch site :



Note the filtered packet count at the bottom pane on the Wireshark utility on both captures. The ***Displayed*** count indicates the number of packets matching the desired filter criteria.

The central site has 4,936 packets that match the desired filter criteria between the start (45514) and end (50449) RTP sequence numbers while at the branch site there are only 4,737 packets. This indicates a loss of 199 packets. Note that these 199 packets match the "Rcvr Lost Pkts" count of 199 which was seen in the streaming statistics of the branch side IP phone shown at the start of this document.

This confirms that all the Rcvr Lost Packets were actually network losses dropped across the WAN. This is how the point of packet loss in the network is isolated while audio/video quality issues are handled involving suspected network drops.