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 Problem

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 Device Information	Streaming Statistics Cisco IP Phone CP-8941(SEP00077ddfbe65)	
	Remote Address	192.168.10.146/20568
Network Setup	Local Address	192.168.207.231/20808
Fetwork Statistics	Start Time	00:00:00
Ethernet Information	Stream Status	Not Ready
Network	Host Name	SEP00077ddfbe65
evice 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 Cont.	11:19:34
streaming Statistics 🤇	Revr Lost Packets	199
Stream 1	Avg Jitter	40
Stream 2	Revr Codec	H264
	Revr Reports Sent	1
	Revr Report Time Sent	11:18:14
	Revr Packets	4675
	Revr Octers	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 Conreal Ratio	0.0000
	Conceal Sees	0
	Severely Conceal Secs	0
	Latency	389
	Max Jitter	50
	Sender Size	0 ms

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:

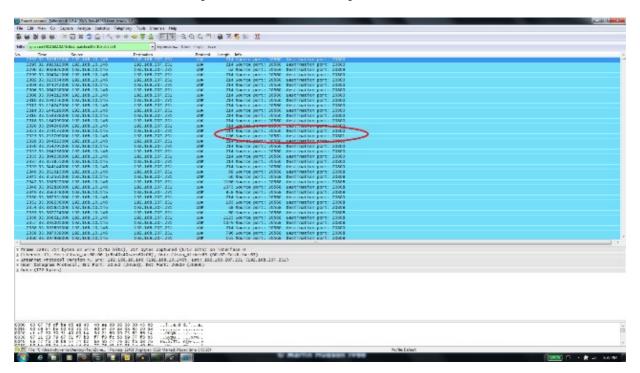
- 1. Open the capture in wireshark.
- 2. Use the filter ip.src==192.168.10.146 && ip.dst==192.168.207.231. This filters out all UDP streams

from central IP phone to branch IP phone.

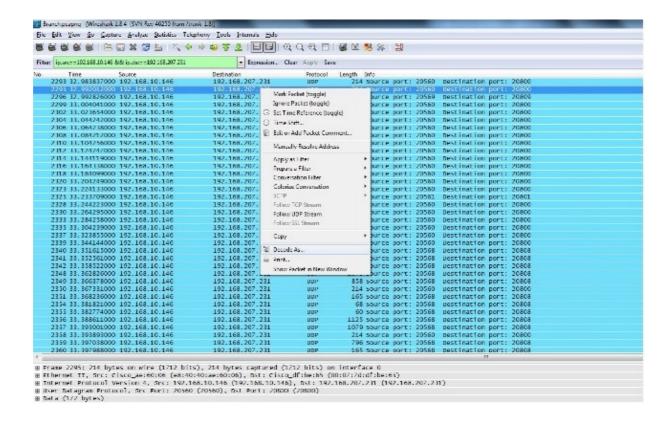
- 3. Perform the analysis on the branch side capture only but note you must perform these steps for the central capture as well.
- 4. In this screenshot, the UDP stream is filtered between the source and the destination IP addresses and contains two UDP streams (differentiated by the UDP port numbers). 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

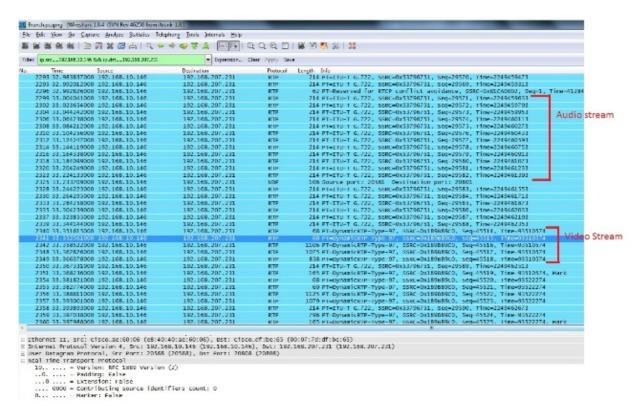
♦ Stream 2 : UDP source port : 20561, destination port : 20801



- 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.

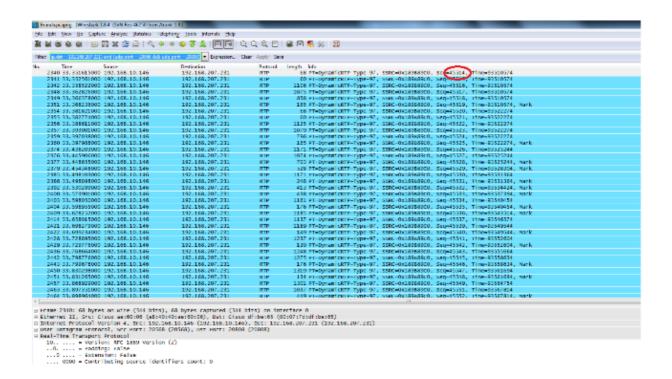


You are left with one stream decoded as RTP and the other as undecoded UDP.



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.



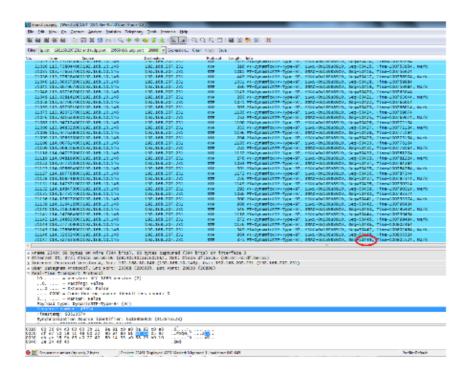
The problem is now only with video quality. Focus on the video RTP stream and use the UDP port numbers for this stream to filter out other streams.

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 continue of the continue
```



The first RTP sequence number is 45514 and 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 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:

```
14591 7.749732 192.168.10.146 192.168.207.231 HTP 248 H-SynamicKTP-Type-97, SMR. Calculations (SMR-SynamicKTP-Type-97, SMR-SALE) 1.118 H-SynamicKTP-Type-97, SMR-SALE SMR-SAL
```

Branch site:

```
100 PT-DynamicRTP-Type-97, SSRL-Dx189588CU, SEQ-45021, Time-95022274
1079 PT-DynamicRTP-Type-97, SSRL-Dx189588CU, Seq-45022, Time-95022274
1079 PT-DynamicRTP-Type-97, SSRL-Dx189588CU, Seq-45022, Time-95022274
1059 PT-DynamicRTP-Type-97, SSRL-Dx189588CU, Seq-45022, Time-95022274, Mark
1171 PT DynamicRTP-Type-97, SSRL-Dx189588CU, Seq-45022, Time-95022274, Mark
1171 PT DynamicRTP-Type-97, SSRL-Dx189588CU, Seq-45022, Time-9502244, Mark
1171 PT-DynamicRTP-Type-97, SSRL-Dx189588CU, Seq-45022, Time-9502244, Mark
1171 PT-DynamicRTP-Type-97, SSRL-Dx189588CU, Seq-45020, Time-9502344
1171 PT-DynamicRTP-Type-97, SSRL-Dx189588CU, Seq-45021, Time-95032364, Mark
1171 PT-DynamicRTP-Type-97, SSRL-Dx189588CU, Seq-45021, Time-95031364, Mark
1171 PT-DynamicRTP-Type-97, SSRL-Dx189588CU, Seq-45021, Time-95031364, Mark
1175 PT-DynamicRTP-Type-97, SSRL-Dx189588CU, Seq-45021, Time-95031364, Mark
1176 PT-DynamicRTP-Type-97, SSRL-Dx189588CU, Seq-45021, Time-95031364, Mark
1176 PT-DynamicRTP-Type-97, SSRL-Dx189588CU, Seq-45021, Time-95031364, Mark
1177 PT-DynamicRTP-Type-97, SSRL-Dx189588CU, Seq-45021, Time-95031364, Mark
1176 PT-DynamicRTP-Type-97, SSRL-Dx189588CU, Seq-45021, Time-95031364, Mark
1177 PT-DynamicRTP-Type-97, SSRL-Dx189588CU, Seq-45021, Time-95031664, Mark
1177 PT-DynamicRTP-Type-97, SSRL-Dx189588CU, Seq-45021, Time-95031664, Mark
1178 PT-DynamicRTP-Type-97, SSRL-Dx189588CU, Seq-45021, Time-95031664, Mark
1179 PT-DynamicRTP-Typ
                       2356 33,388611000 192,168,10,146
2357 33,393001000 192,168,10,146
                      2359 33.397038000 192.168.10.146
2360 33.397988000 192.168.10.146
                                                                                                                                                                                                                                             192,188,207,231
192,168,207,231
                     2174 31.418201000 192.188.10.148
2376 33.445906000 192.168.10.146
2177 31.448855000 192.168.10.146
                                                                                                                                                                                                                                             192.168.207.231
                   2377 31.448655000 192.168.10.16.279 33.451248000 192.168.10.146
2379 33.451248000 192.168.10.146
2386 33.49818000 192.168.10.166
2382 33.59239000 192.168.10.166
240 33.572901000 192.168.10.166
240 33.59255000 192.168.10.166
240 33.59255000 192.168.10.166
241 33.59255000 192.168.10.166
241 33.698275000 192.168.10.166
241 33.698275000 192.168.10.146
242 33.698275000 192.168.10.146
242 33.728895000 192.168.10.146
242 33.728895000 192.168.10.146
242 33.728895000 192.168.10.146
                                                                                                                                                                                                                                             192.168.207.231
                                                                                                                                                                                                                                             192.168.207.231
192.168.207.231
                                                                                                                                                                                                                                             192,168,207,231
192,168,207,231
                                                                                                                                                                                                                                              192.168.207.231
192.168.207.231
                      2429 31,729778000 192,185,10,146
2436 33,768664000 192,168,10,146
                                                                                                                                                                                                                                           192.168.207.231
                      2442 31.798778000 192.168.10.146
2443 33.799678000 192.168.10.146
                                                                                                                                                                                                                                          192.168.207.231
192.168.207.231
                     2450 33.830298000 197.168.10.146
2451 33.831265000 192.168.10.146
2457 33.868929000 192.168.10.146
                                                                                                                                                                                                                                          192,168,207,231
                       2463 33.897351000 192.168.10.146
2464 33.898964000 192.168.10.146
                      2470 33.927687000 192.168.10.146
2471 33.929528000 192.168.10.146
                                                                                                                                                                                                                                           192.168.207.231
192.168.207.231
                     2478 33.967559000 192.168.10.146
2479 33.968921000 192.168.10.146
                                                                                                                                                                                                                                           192,168,207,231
192,168,207,231
         Frame 2340: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0 thermat II, Sec. cisco aciso:06 (@8:40:40:aciso:06), sst: cisco ef:be:08 (@9:07:76:df:be:05)
Internet Protocol Version 4, Sec. 192:168.10.146 (192.168.10.146), bst: 192.168.207.231 (192.168.207.231)
User batagram Protocol, Sec Port: 20008 (20004), bst Port: 20008 (20004)
Real-ince imansport Protocol
10. ... - Version: REC 1889 Version (2)
... ... - Version: REC 1889 Version (2)
... ... - Eather ince: Ealbe
... ... 0000 - Contributing source identifiers count: 0
0. ... - Marker: False
Payload type: bynamicum type 97 (97)
Sequence masher: 45354
                                                                                                            45514
                      Timestamp: 98510574
Synchronization Source identifier: 0x189b89c0 (412846528)
                          00 07 7d dt be 65 e8 40 40 ae 60 00 08 00 45 88 00 38 84 d3 00 00 3b 11 9e 91 c0 a8 0a 92 c0 a8 cf cf 75 95 85 148 00 22 96 04 80 bi bi co 95 92 db ae 18 9b 80 c0 27 42 80 14 95 a0 58 25 b0 10 12 24 d4 40 5
                                                                                                                                                                                                                                                                                                 ● M | Disc 10: University (versity) Decktop (Tech Zone. | Packeto 2745) Display 4737 | Archet Displayed: 1 Load time (1998)
```

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.

Updated: Jul 28, 2014 Document ID: 117881