

在语音和视频呼叫的Wireshark中破译RTP流以进行丢包分析

目录

[简介](#)

[问题](#)

简介

本文档介绍如何在Wireshark中解密用于语音和视频呼叫的丢包分析的实时流(RTP)流的过程。您可以使用Wireshark过滤器来分析在呼叫源和目标位置或靠近呼叫源和目标位置捕获的同步数据包。当怀疑网络丢失时，您必须排除音频和视频质量问题时，此功能非常有用。


问题

本示例使用以下呼叫流：

IP电话A (中心站点A) > 2960交换机>路由器>广域网路由器 (中心站点) > IPWAN >广域网路由器 (站点B) >路由器> 2960 > IP电话B

在此场景中，遇到的问题是，从IP电话A到IP电话B的视频呼叫会导致从中心站点A到分支站点B的视频质量不佳，其中中心站点质量良好，但分支站点有问题。

请参阅分支IP电话的流统计信息中的接收方丢失的数据包：

		<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	

解决方案

只有在分支机构端才会看到质量不佳，而且由于中心站点看到的图像良好，从中心到分支站点的数据流似乎正在网络中丢失数据包。

IP addressing scheme

Central IP phone: 192.168.10.146

Central Gateway: 192.168.10.253

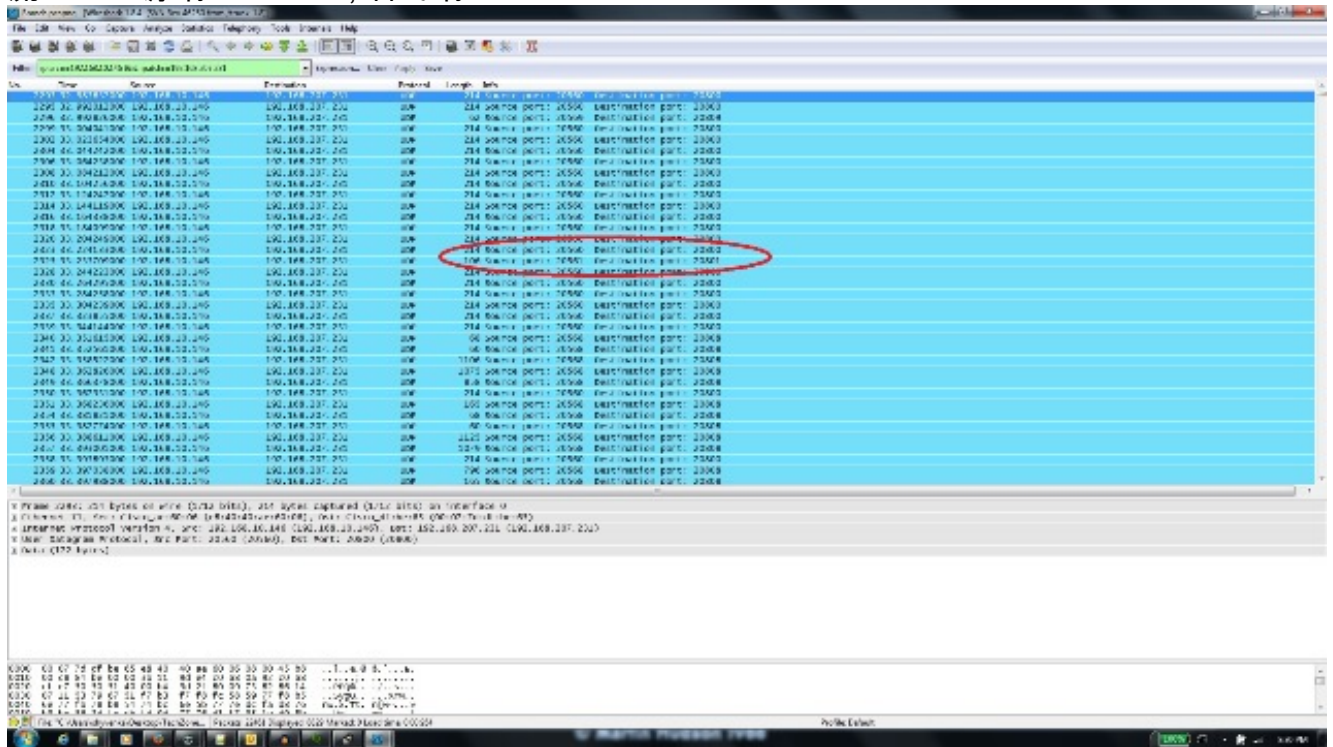
Central WAN router: 192.168.10.254
Branch WAN router: 192.168.206.210
Branch Gateway: 192.168.206.253
Branch IP phone: 192.168.207.231

数据包捕获在中央和分支WAN路由器上进行，WAN会丢弃这些数据包。重点介绍从中央IP电话(192.168.10.146)到分支IP电话(192.168.207.231)的RTP流。如果WAN丢弃从中央WAN路由器到分支WAN路由器的数据流上的数据包，则此数据流会丢失分支WAN路由器上的数据包。使用wireshark中的过滤器选项来隔离问题：

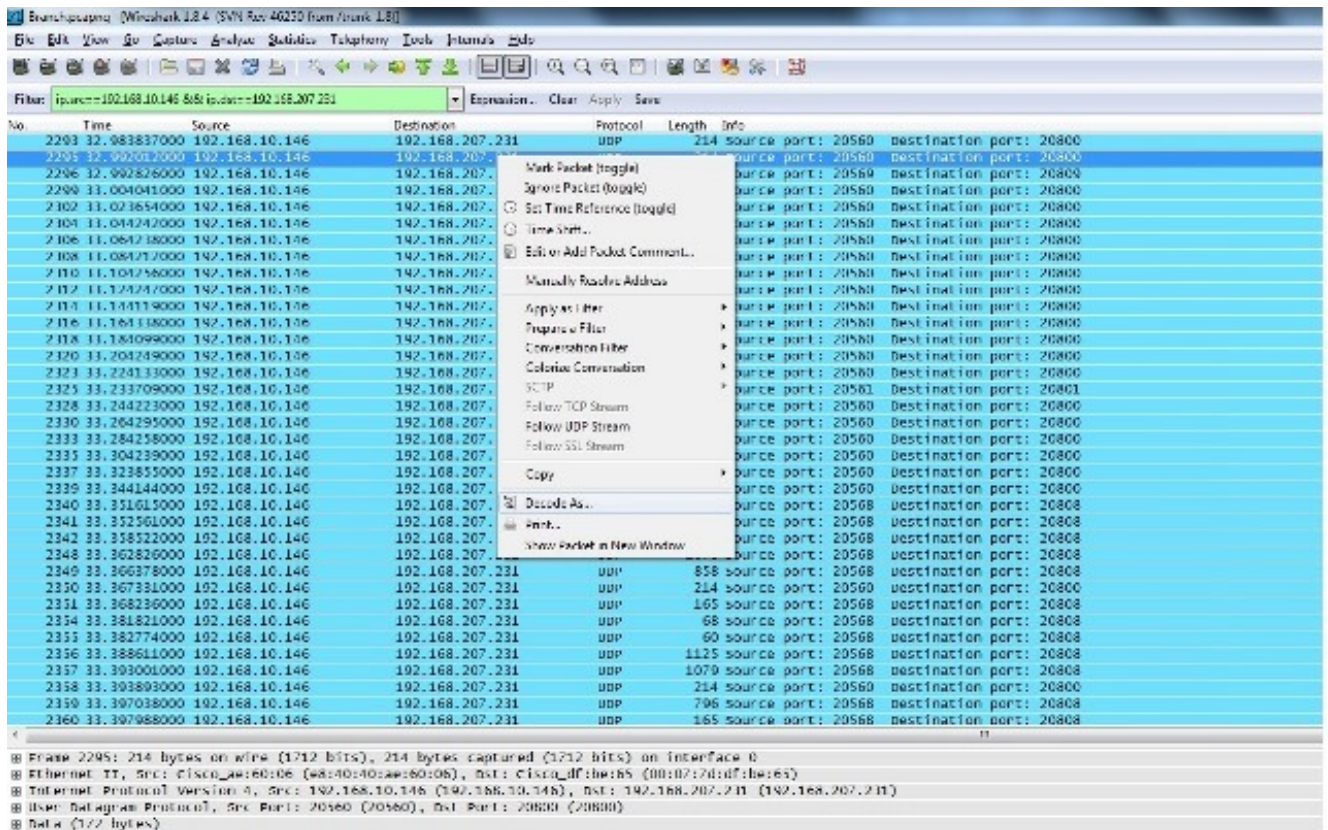
1. 在wireshark中打开捕获。
2. 使用过滤器ip.src==192.168.10.146 && ip.dst==192.168.207.231。这会过滤掉从中央IP电话到分支IP电话的所有UDP流。
3. 仅对分支机构端捕获执行分析，但请注意，对于中央捕获，您也必须执行这些步骤。
4. 在此屏幕截图中，UDP流在源IP地址和目的IP地址之间过滤，并包含两个UDP流（由UDP端口号区分）。这是视频呼叫，因此有两个流：音频和视频。在本例中，两个流是：

流1:UDP 源端口:20560，目的端口：20800

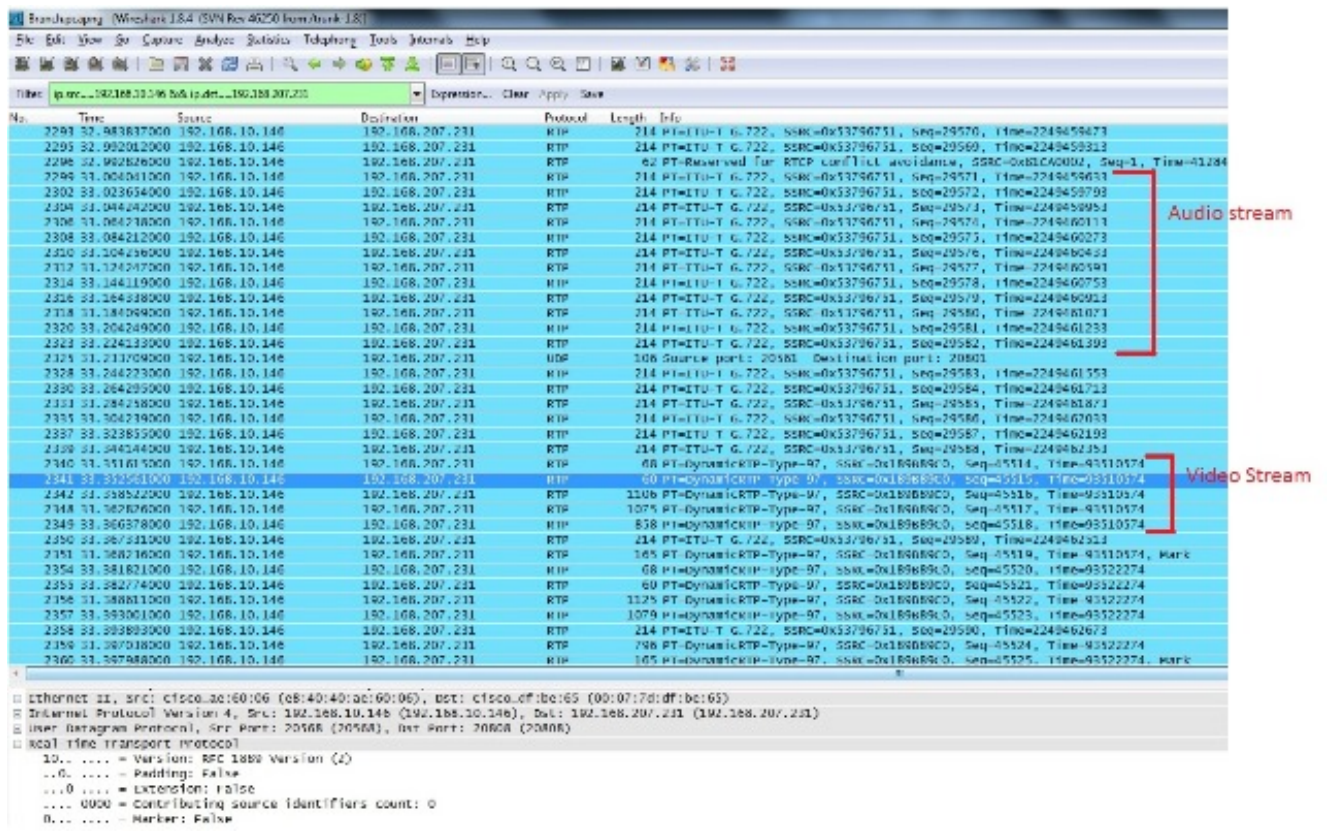
流2:UDP 源端口:20561，目的端口：20801



5. 从其中一个流中选择一个数据包，然后右键单击该数据包。
6. 选择Decode As...并键入RTP。
7. 单击Accept和Ok以将流解码为RTP。

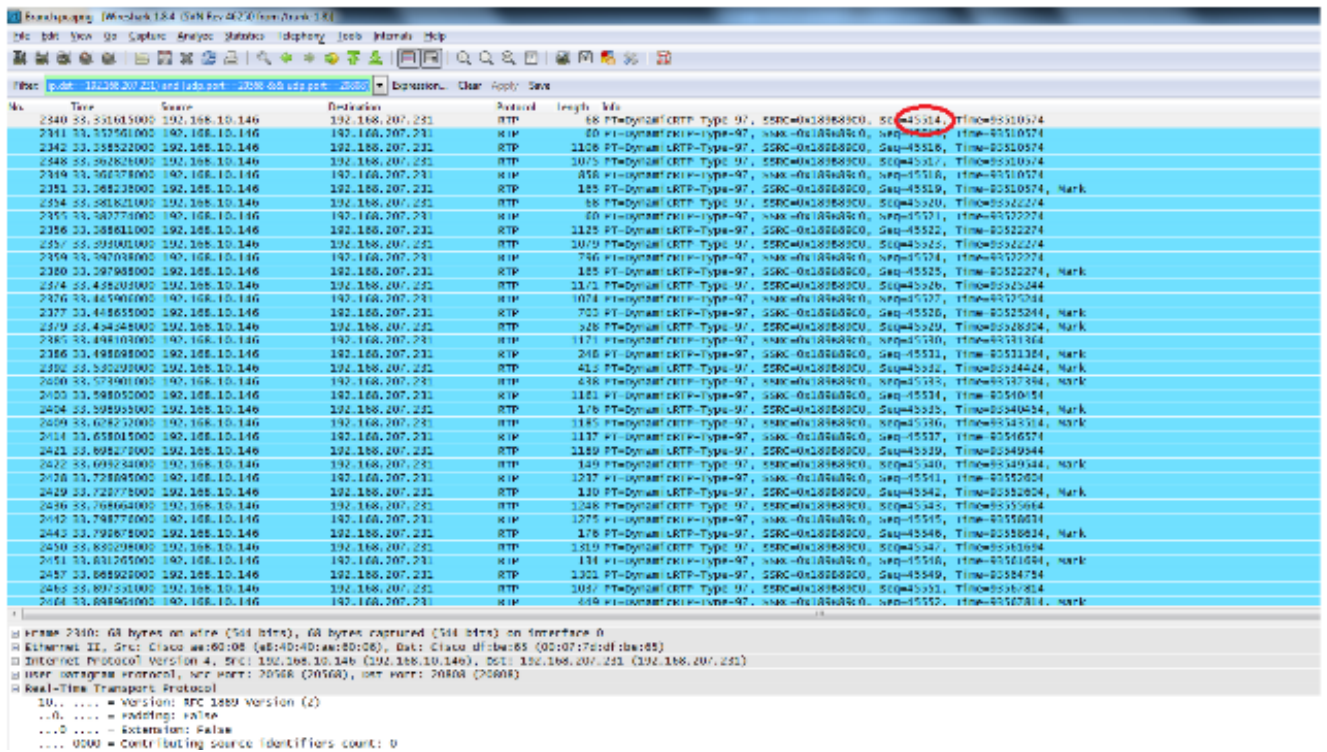


您的一个数据流被解码为 RTP，另一个被解码为未解码的 UDP。



8. 从未解码的流中选择数据包并将其解码为 RTP。这会将音频和视频流解码为 RTP。

注意：音频流采用 G.722 编解码器格式，Dynamic-RTP-97 负载类型指示视频 RTP 流。

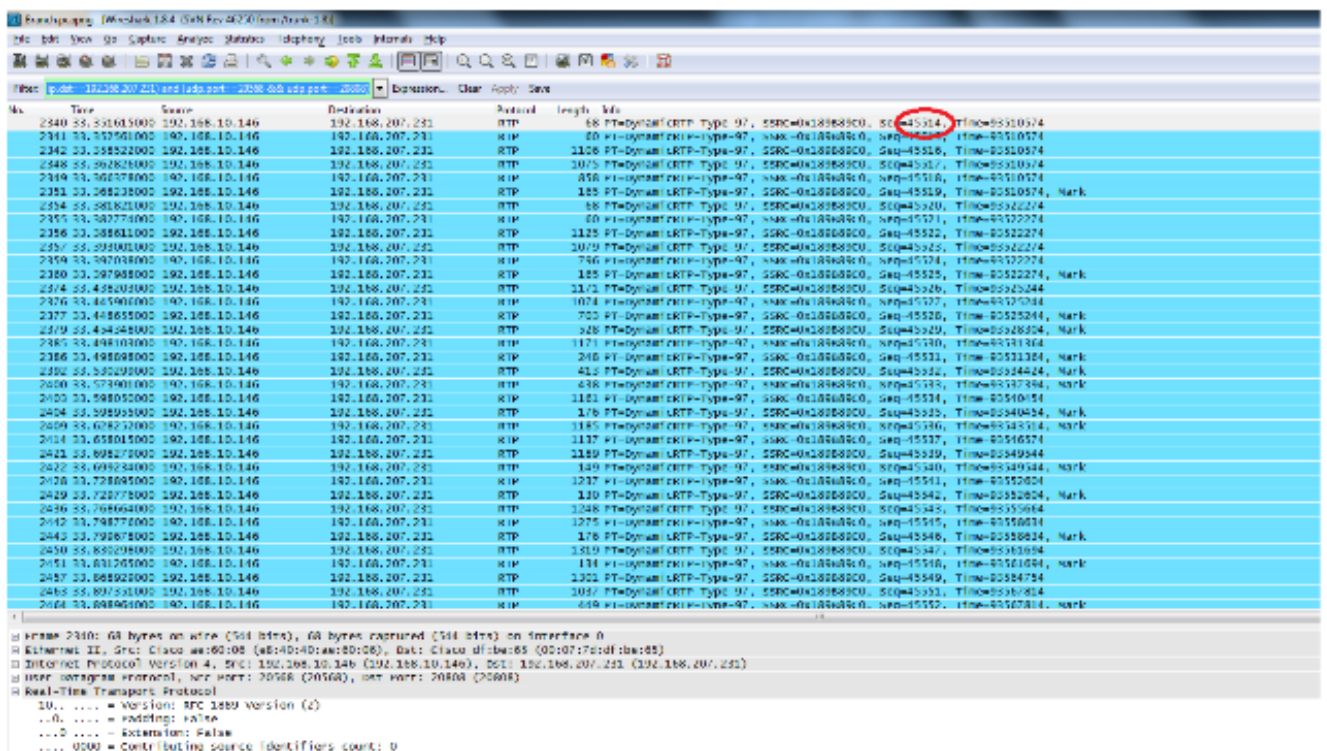


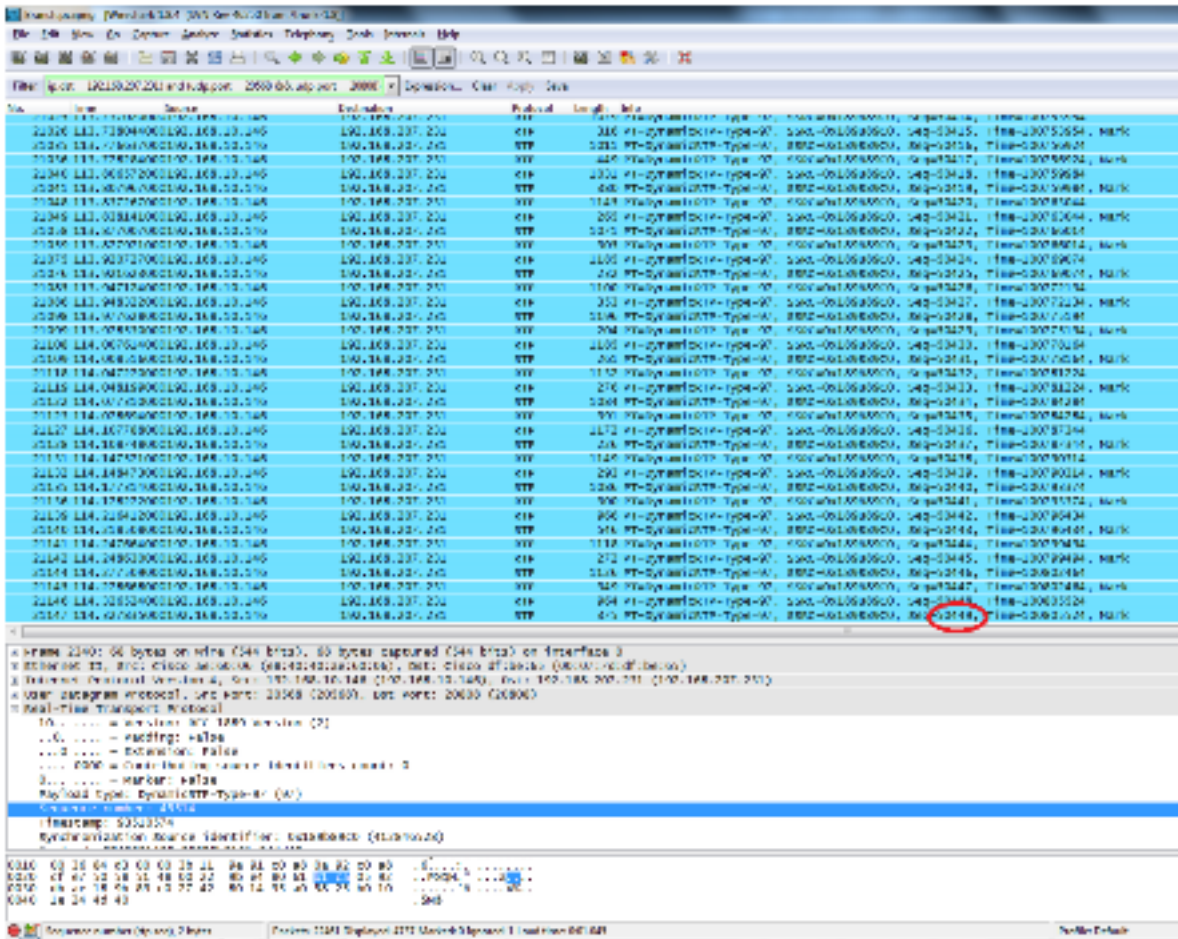
现在问题只出在视频质量上。关注视频RTP流，并使用此流的UDP端口号过滤掉其他流。

9. 在Wireshark实用程序的底部窗格中选择显示UDP端口信息的数据包之一，查看端口号。在上一屏幕截图中，从视频流中选择了其中一个数据包，您可以在底部窗格中看到源端口(20568)和目的端口(20808)信息。

提示：使用此过滤器：`(ip.src==192.168.10.146 && ip.dst==192.168.207.231)&(udp.port eq 20568&udp.port eq 20808)`。您只会看到此屏幕截图中显示的视频RTP流。

注意：写下此流的第一个和最后一个RTP序列号。





第一个RTP序列号45514，最后一个是50449，用于已过滤的视频RTP流。

10. 确保第一个和最后一个RTP序列号数据包同时存在于两个捕获中。例如，中心和分支捕获)，并注意流的SSRC在两个捕获上将相同。
11. 优化过滤器以仅匹配第一个和最后一个RTP流之间的数据包。

序列号用于细化数据流，以防捕获不同时进行，但两者之间有轻微延迟。

注意：分支站点可能会在45514后启动一些序列号。

12. 选择开始和结束序列号。这些数据包在捕获和优化过滤器中都存在，以仅显示开始和结束RTP序列号之间的数据包。此项的过滤器为：

```
(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 )
```

当同时捕获时，两个捕获的开始或结束时不会丢失任何数据包。如果您看到其中一个捕获在开始/结束时不包含几个数据包，请使用两个数据包中丢失的捕获的第一个序列号或捕获中的最后一个序列号来细化两个捕获的过滤器。观察在同一序列号（RTP序列号范围）之间两点捕获的数据包。

应用过滤器时，您会在中心站点和分支站点看到以下内容：

中心站点:

Time	Source IP	Destination IP	Protocol	Length	Info
14572	37.720005	192.168.10.146	RTP	248	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45531, Time=93531364, Mark
14591	37.749752	192.168.10.146	RTP	413	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45532, Time=93534420, Mark
14609	17.799790	192.168.10.146	RTP	418	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45533, Time=93537180, Mark
14619	37.819092	192.168.10.146	RTP	1161	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45534, Time=93540454, Mark
14620	37.819092	192.168.10.146	RTP	176	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45535, Time=93540454, Mark
14634	37.849993	192.168.10.146	RTP	1185	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45536, Time=93543514, Mark
14646	17.860019	192.168.10.146	RTP	1137	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45537, Time=93546574, Mark
14647	17.860019	192.168.10.146	RTP	1111	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45538, Time=93546574, Mark
14666	37.919887	192.168.10.146	RTP	1189	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45539, Time=93549544, Mark
14667	37.919887	192.168.10.146	RTP	149	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45540, Time=93549544, Mark
14679	37.950212	192.168.10.146	RTP	1237	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45541, Time=93552604, Mark
14680	17.950210	192.168.10.146	RTP	1181	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45542, Time=93555664, Mark
14699	37.989939	192.168.10.146	RTP	1248	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45543, Time=93558664, Mark
14700	37.989939	192.168.10.146	RTP	176	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45544, Time=93558664, Mark
14711	38.020065	192.168.10.146	RTP	1275	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45545, Time=93561664, Mark
14712	38.020065	192.168.10.146	RTP	176	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45546, Time=93561664, Mark
14724	38.050192	192.168.10.146	RTP	1119	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45547, Time=93564664, Mark
14725	38.050419	192.168.10.146	RTP	134	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45548, Time=93564664, Mark
14744	38.089989	192.168.10.146	RTP	1301	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45549, Time=93567724, Mark

Frame 14495: 88 bytes on wire (544 bits), 88 bytes captured (544 bits) on interface 0
Ethernet II, Src: Cisco_e7:13:f0 (30:e4:db:67:13:f0), Dst: Cisco_f4:d0:08 (08:00:27:14: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 00 36 84 e3 00 00 3f 11 9e 91 c0 a8 0a 92 c0 a8 ...6...?.....E.
0010 00 36 84 e3 00 00 3f 11 9e 91 c0 a8 0a 92 c0 a8 ...6...?.....E.
0020 cf c7 50 58 51 48 00 22 9b 04 80 61 d1 ca 05 92 ...PROM.....D...
0030 db ae 18 9b 89 c0 27 42 89 14 95 a0 58 25 b9 10B.....X...
0040 1e 24 4d 40@

File: C:\Users\shyvenal\Desktop\TechZone... Packets: 9458 Dropped: 4635 Marked: 0 Ignored: 1 Load time: 1603150 Profile: Default

分支站点:

Time	Source IP	Destination IP	Protocol	Length	Info
2330	33.386274000	192.168.10.146	RTP	60	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45514, Time=93522274, Mark
2356	33.386274000	192.168.10.146	RTP	1125	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45522, Time=93522274, Mark
2357	33.399001000	192.168.10.146	RTP	1079	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45523, Time=93522274, Mark
2359	33.397000000	192.168.10.146	RTP	798	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45524, Time=93522274, Mark
2360	33.397988000	192.168.10.146	RTP	165	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45525, Time=93522274, Mark
2374	33.443501000	192.168.10.146	RTP	1173	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45526, Time=93525244, Mark
2376	33.443501000	192.168.10.146	RTP	1074	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45527, Time=93525244, Mark
2377	33.443501000	192.168.10.146	RTP	705	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45528, Time=93525244, Mark
2379	33.454348000	192.168.10.146	RTP	528	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45529, Time=93528304, Mark
2385	33.498193000	192.168.10.146	RTP	1173	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45530, Time=93531364, Mark
2386	33.498193000	192.168.10.146	RTP	248	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45531, Time=93531364, Mark
2392	33.530299000	192.168.10.146	RTP	413	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45532, Time=93534424, Mark
2400	33.573901000	192.168.10.146	RTP	428	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45533, Time=93537384, Mark
2403	33.596550000	192.168.10.146	RTP	1161	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45534, Time=93540454, Mark
2404	33.598550000	192.168.10.146	RTP	176	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45535, Time=93540454, Mark
2406	33.628252000	192.168.10.146	RTP	1185	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45536, Time=93543514, Mark
2414	33.658015000	192.168.10.146	RTP	1119	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45537, Time=93546574, Mark
2421	33.698279000	192.168.10.146	RTP	1189	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45539, Time=93549544, Mark
2422	33.698279000	192.168.10.146	RTP	149	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45540, Time=93549544, Mark
2428	33.728950000	192.168.10.146	RTP	1237	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45541, Time=93552604, Mark
2429	33.729778000	192.168.10.146	RTP	130	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45542, Time=93552604, Mark
2436	33.768604000	192.168.10.146	RTP	1248	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45543, Time=93555664, Mark
2442	33.798778000	192.168.10.146	RTP	1275	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45545, Time=93558664, Mark
2443	33.799678000	192.168.10.146	RTP	176	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45546, Time=93558664, Mark
2450	33.830298000	192.168.10.146	RTP	1119	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45547, Time=93561664, Mark
2451	33.831265000	192.168.10.146	RTP	134	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45548, Time=93561664, Mark
2457	33.868829000	192.168.10.146	RTP	1301	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45549, Time=93564664, Mark
2463	33.897310000	192.168.10.146	RTP	1037	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45551, Time=93567724, Mark
2464	33.898829000	192.168.10.146	RTP	449	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45552, Time=93567724, Mark
2470	33.927687000	192.168.10.146	RTP	1035	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45553, Time=93570784, Mark
2471	33.929528000	192.168.10.146	RTP	477	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45554, Time=93570784, Mark
2478	33.967339000	192.168.10.146	RTP	1051	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45555, Time=93573844, Mark
2479	33.968921000	192.168.10.146	RTP	392	PT=DynanmicRTP-Type-97, SSRC=0x189689c0, Seq=45556, Time=93573844, Mark

Frame 2340: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
Ethernet II, Src: Cisco_ae10:09 (08:40:40:1a:e6:09), Dst: Cisco_df:be:65 (00:07:1d:df:be: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

10..... = Version: RFC 1889 Version (2)
..0..... = Padding: false
...0..... = Extension: false
....0000 = contributing source identifiers count: 0
0..... = Marker: false
Payload type: dynanmicrtp type 97 (97)
Sequence number: 45514
Timestamp: 93510574
Synchronization Source identifier: 0x189689c0 (417866578)

0000 00 07 7d cf be 65 e8 40 40 ae 00 00 08 00 45 88 ...E...@...E...
0010 00 36 84 e3 00 00 3f 11 9e 91 c0 a8 0a 92 c0 a8 ...6...?.....E.
0020 cf c7 50 58 51 48 00 22 9b 04 80 61 d1 ca 05 92 ...PROM.....D...
0030 db ae 18 9b 89 c0 27 42 89 14 95 a0 58 25 b9 10B.....X...
0040 1e 24 4d 40@

File: C:\Users\shyvenal\Desktop\TechZone... Packets: 2981 Dropped: 4737 Marked: 0 Ignored: 1 Load time: 603150 Profile: Default

注意Wireshark实用程序底部窗格中两个捕获的过滤数据包计数。Displayed 计数指示符合所需过滤条件的数据包数。

中心站点有4,936个数据包，这些数据包在开始(45514)和结束(50449)RTP序列号之间符合所需的过滤条件，而在分支站点只有4,737个数据包。这表示丢失了199个数据包。请注意，这199个数据包与“Rcvr Lost Pkts”计数199匹配，该计数在本文档开头显示的分支机构端IP电话

的流统计信息中可见。

这确认了所有接收器丢失数据包实际上是广域网上丢弃的网络丢失。这就是处理涉及可疑网络丢弃的音频/视频质量问题时隔离网络中丢包点的方式。