

Bestimmen Sie den RTP-Stream für die Analyse von Paketverlusten in Wireshark für Sprach- und Videoanrufe.

Inhalt

[Einführung](#)

[Problem](#)

Einführung

In diesem Dokument wird beschrieben, wie der Real-Time Streaming (RTP)-Stream für die Analyse von Paketverlusten in Wireshark bei Sprach- und Videoanrufen entschlüsselt wird. Sie können Wireshark-Filter verwenden, um die gleichzeitige Paketerfassung zu analysieren, die an oder nahe der Quelle und dem Ziel eines Anrufs durchgeführt wird. Dies ist nützlich, wenn Sie Probleme mit der Audio- und Videoqualität beheben müssen, wenn Netzwerkverluste vermutet werden.


Problem

In diesem Beispiel wird dieser Anruffluss verwendet:

IP-Telefon A (zentraler Standort A) > 2960-Switch > Router > WAN-Router (zentraler Standort) > IPWAN > WAN-Router (Standort B) > Router > 2960 > IP-Telefon B

In diesem Szenario besteht das Problem darin, dass Videoanrufe von IP-Telefon A zu IP-Telefon B zu einer schlechten Videoqualität von dem zentralen Standort A zu der Zweigstelle B führen, wo die Zentrale eine gute Qualität hat, die Zweigstelle jedoch Probleme hat.

In der Streaming-Statistik des IP-Telefons der Außenstelle werden verlorene Pakete angezeigt:

		<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	

Lösung

Schlechte Qualität zeigt sich nur auf der Zweigstelle, und da der zentrale Standort ein gutes Bild sieht, sieht es so aus, als würde der Stream von der Zentrale zur Zweigstelle Pakete über das Netzwerk verlieren.

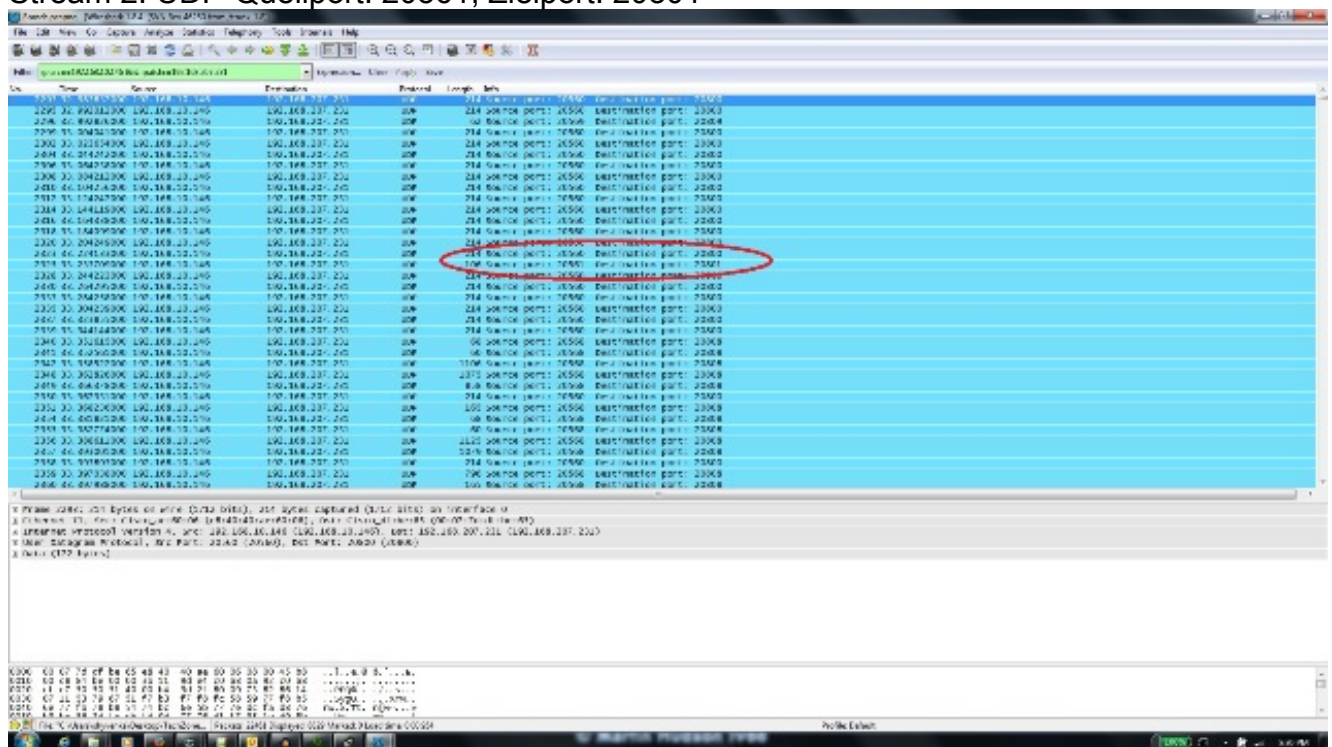
Central Gateway: 192.168.10.253
Central WAN router: 192.168.10.254
Branch WAN router: 192.168.206.210
Branch Gateway: 192.168.206.253
Branch IP phone: 192.168.207.231

Die Paketerfassungen werden auf dem WAN-Router der Zentrale und Zweigstelle durchgeführt, und das WAN verwirft diese Pakete. Konzentrieren Sie sich auf den RTP-Stream vom zentralen IP-Telefon (192.168.10.146) zum IP-Telefon der Außenstelle (192.168.207.231). Dieser Stream übersieht Pakete auf dem WAN-Router der Außenstelle, wenn das WAN die Pakete im Stream vom zentralen WAN-Router zum WAN-Router der Außenstelle verwirft. Verwenden Sie die Filteroptionen in Wireshark, um das Problem zu isolieren:

1. Öffnen Sie die Erfassung in Wireshark.
2. Verwenden Sie den Filter `ip.src==192.168.10.146 && ip.dst==192.168.207.231`. Dadurch werden alle UDP-Streams vom zentralen IP-Telefon an das IP-Telefon der Außenstelle gefiltert.
3. Führen Sie die Analyse nur für die Zweigstellenerfassung durch. Beachten Sie jedoch, dass Sie diese Schritte auch für die zentrale Erfassung ausführen müssen.
4. In diesem Screenshot wird der UDP-Stream zwischen der Quell- und der Ziel-IP-Adresse gefiltert und enthält zwei UDP-Streams (differenziert durch die UDP-Portnummern). Dies ist ein Videoanruf, sodass zwei Streams vorhanden sind: Audio und Video. In diesem Beispiel sind die beiden Streams:

Stream 1: UDP-Quellport: 20560, Zielport: 20800

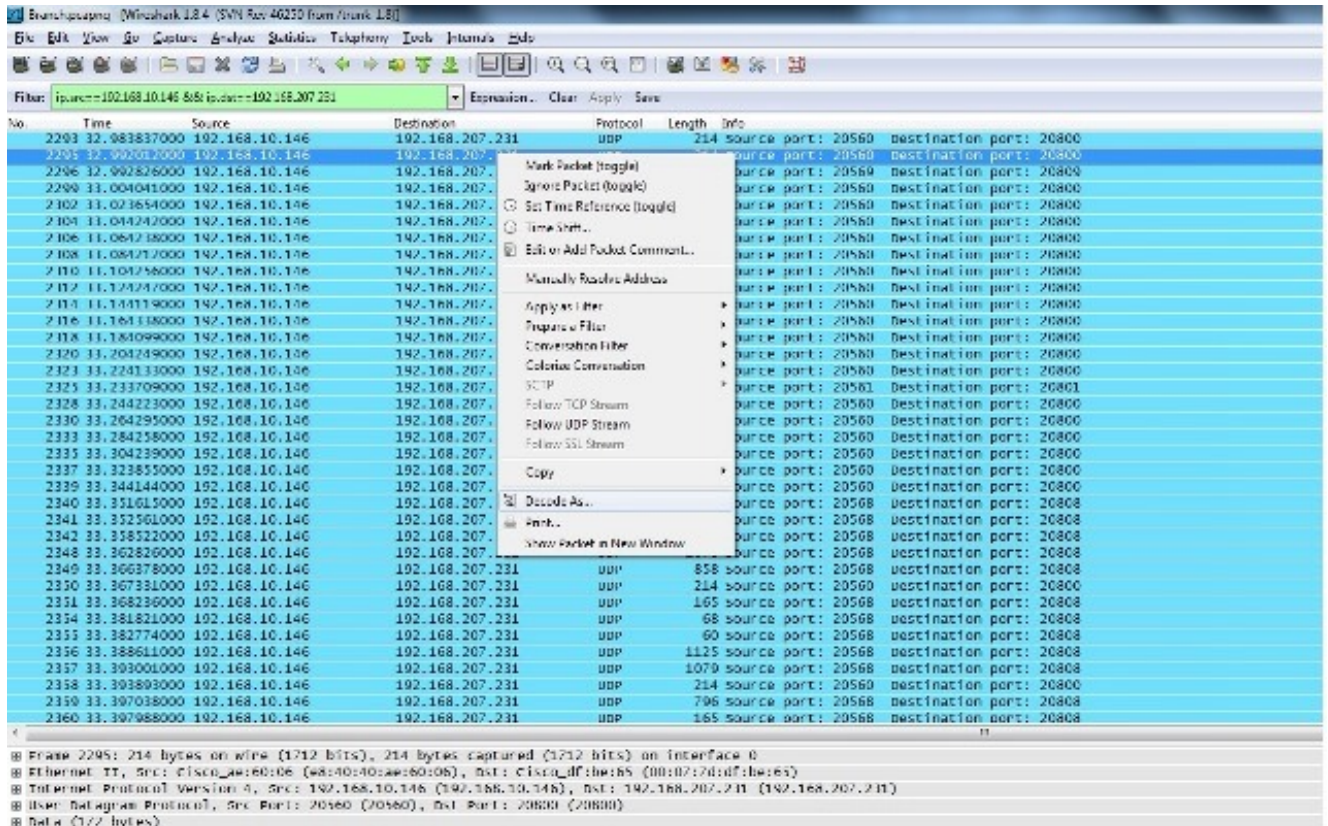
Stream 2: UDP-Quellport: 20561, Zielport: 20801



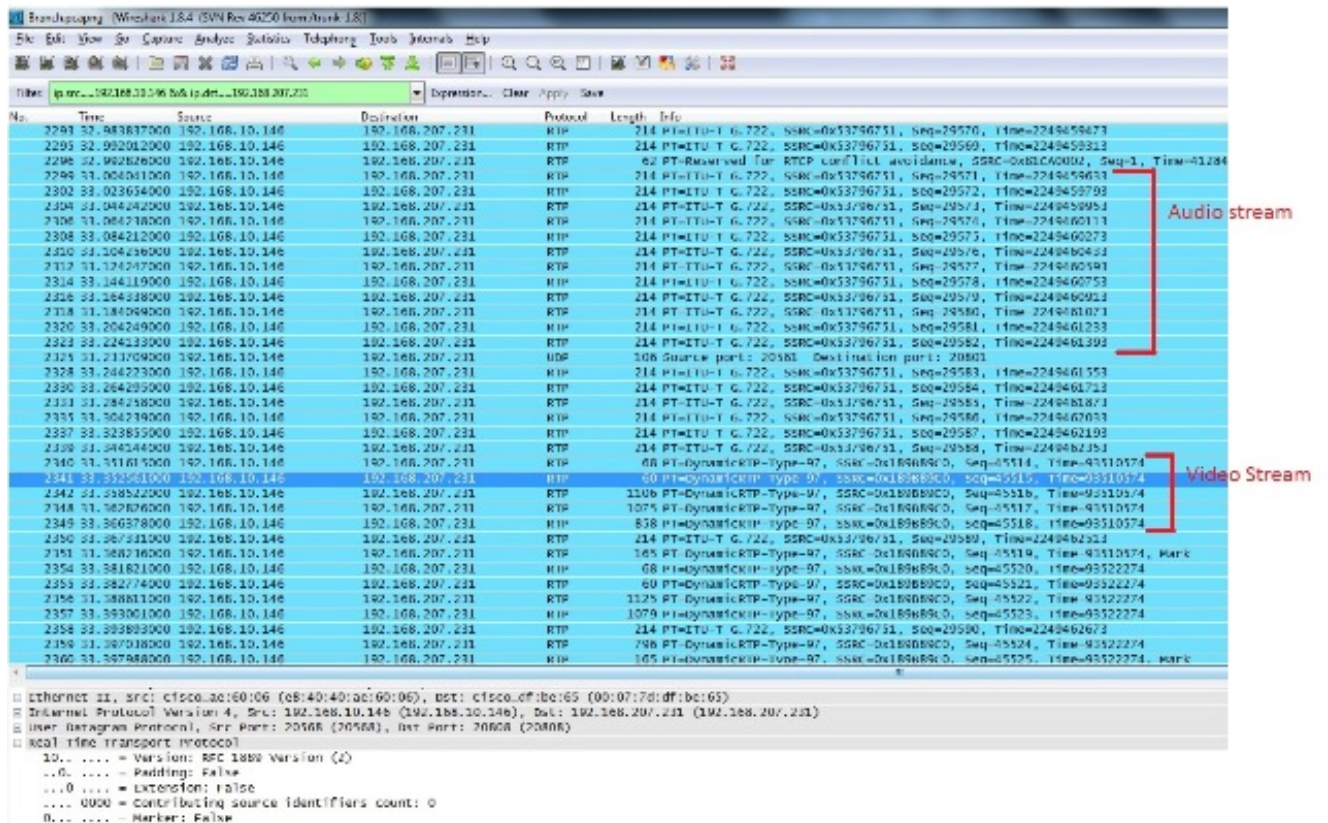
5. Wählen Sie ein Paket aus einem der Streams aus, und klicken Sie mit der rechten Maustaste auf das Paket.

6. Wählen Sie **Decode As.. (Decodieren als)** aus. und geben Sie **RTP** ein.

7. Klicken Sie auf **Akzeptieren** und **OK**, um den Stream als RTP zu decodieren.

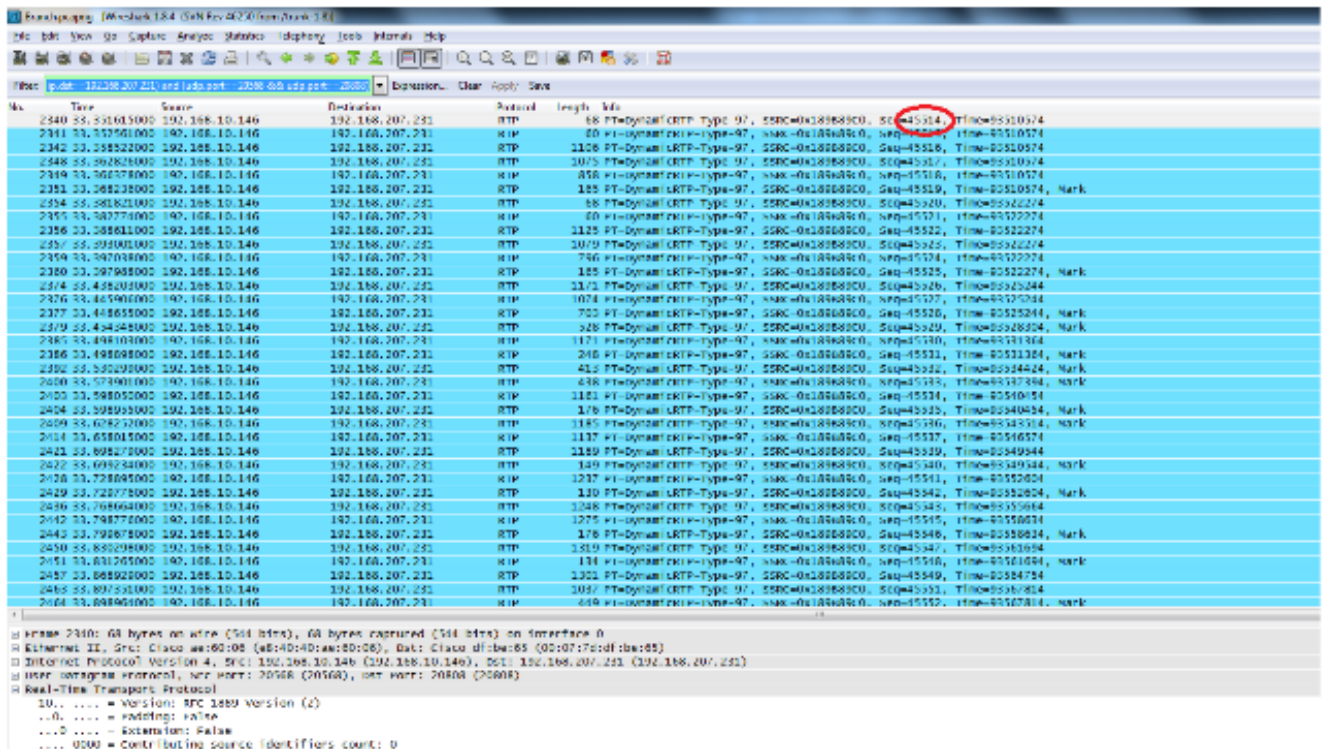


Ein Stream wird als RTP decodiert, der andere als nicht codiertes UDP.



8. Wählen Sie ein Paket aus dem nicht codierten Stream aus, und decodieren Sie es als RTP. Dadurch werden Audio- und Videostreams in RTP dekodiert.

Hinweis: Der Audio-Stream hat das Codec-Format G.722, und der Payload-Typ Dynamic-RTP-97 gibt den Video-RTP-Stream an.



Das Problem besteht nun nur noch in der Videoqualität. Konzentrieren Sie sich auf den Video-Stream, und verwenden Sie die UDP-Portnummern für diesen Stream, um andere Streams herauszufiltern.

9. Zeigen Sie die Portnummer an, indem Sie eines der Pakete auswählen, das im Wireshark-Dienstprogramm im unteren Bereich die UDP-Portinformationen anzeigt. Im vorherigen Screenshot wird eines der Pakete aus dem Video-Stream ausgewählt. Im unteren Bereich finden Sie die Informationen zu Src Port (20568) und Dst Port (20808).

Tipp: Verwenden Sie diesen Filter: (ip.src==192.168.10.146 && ip.dst==192.168.207.231) & (udp.port eq 20568 und udp.port eq 20808). In diesem Screenshot wird nur der Video-RTP-Stream angezeigt.

Hinweis: Notieren Sie die ersten und letzten RTP-Sequenznummern für diesen Stream.

11. Der Filter kann so angepasst werden, dass nur die Pakete zwischen dem ersten und dem letzten RTP-Stream übereinstimmen.

Die Sequenznummern werden zur Optimierung des Streams verwendet, falls die Aufnahmen nicht gleichzeitig, sondern mit geringer Verzögerung zwischen den Aufnahmen durchgeführt werden.

Hinweis: Es ist möglich, dass der Zweigstellen-Standort einige Sequenznummern nach 4514 startet.

12. Wählen Sie eine Start- und eine Endsequenznummer aus. Diese Pakete befinden sich sowohl in den Erfassungen als auch in der Optimierung des Filters, sodass nur die Pakete zwischen der Start- und der End-RTP-Sequenznummer angezeigt werden. Der Filter hierfür ist:

```
(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 )
```

Wenn gleichzeitig Erfassungen durchgeführt werden, werden bei beiden Erfassungen keine Pakete am Anfang oder Ende verpasst. Wenn Sie sehen, dass eine der Erfassungen nicht wenige Pakete am Anfang/Ende enthält, verwenden Sie die erste Sequenznummer oder die letzte Sequenznummer in der Erfassung, die in beiden Paketen verpasst wurde, um den Filter für beide Erfassungen zu verfeinern. Beobachten Sie die Pakete, die an beiden Punkten zwischen denselben Sequenznummern erfasst wurden (RTP-Sequenznummernbereich).

Wenn Sie den Filter anwenden, sehen Sie dies an der Zentrale und in der Zweigstelle:

Zentrale Website:

The screenshot shows a network traffic capture tool interface. At the top, a list of captured packets is displayed with columns for time, source IP, destination IP, protocol, and sequence number. The packets are RTP packets of type 97, with source IP 192.168.10.146 and destination IP 192.168.207.231. The sequence numbers range from 248 to 1301. Below the list, the details of a selected packet (Frame 1449) are shown. The details include Ethernet II, Internet Protocol version 4, User Datagram Protocol (UDP), and Real-Time Transport Protocol (RTP) information. The RTP section shows sequence number 44514, timestamp 93531364, and other RTP-specific fields. At the bottom, a hex dump of the packet data is visible, with a red circle highlighting the RTP sequence number field (0x00000000).

Zweigstelle:

The screenshot displays a Wireshark capture of RTP packets. The top pane shows a list of packets with columns for No., Time, and Length. The middle pane shows the details of the selected packet (No. 2340), including Ethernet II, Internet Protocol version 4, User Datagram Protocol, and Real-time Transport Protocol. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Length	Protocol	Source	Destination
2330	35.38274000	192	RTP	192.168.10.146	192.168.207.231
2336	31.388611000	192	RTP	192.168.207.231	192.168.10.146
2337	33.399001000	192	RTP	192.168.207.231	192.168.10.146
2354	31.397038000	192	RTP	192.168.207.231	192.168.10.146
2360	33.397988000	192	RTP	192.168.207.231	192.168.10.146
2370	31.418201000	192	RTP	192.168.207.231	192.168.10.146
2376	33.445906000	192	RTP	192.168.207.231	192.168.10.146
2377	31.448655000	192	RTP	192.168.207.231	192.168.10.146
2379	33.454348000	192	RTP	192.168.207.231	192.168.10.146
2385	31.498103000	192	RTP	192.168.207.231	192.168.10.146
2386	33.498498000	192	RTP	192.168.207.231	192.168.10.146
2392	33.530298000	192	RTP	192.168.207.231	192.168.10.146
2400	33.573001000	192	RTP	192.168.207.231	192.168.10.146
2403	33.598650000	192	RTP	192.168.207.231	192.168.10.146
2408	33.598935000	192	RTP	192.168.207.231	192.168.10.146
2409	33.628232000	192	RTP	192.168.207.231	192.168.10.146
2416	33.658035000	192	RTP	192.168.207.231	192.168.10.146
2421	33.698279000	192	RTP	192.168.207.231	192.168.10.146
2422	31.699034000	192	RTP	192.168.207.231	192.168.10.146
2428	33.728895000	192	RTP	192.168.207.231	192.168.10.146
2429	31.729778000	192	RTP	192.168.207.231	192.168.10.146
2436	33.768664000	192	RTP	192.168.207.231	192.168.10.146
2442	31.798778000	192	RTP	192.168.207.231	192.168.10.146
2443	33.799678000	192	RTP	192.168.207.231	192.168.10.146
2450	31.830798000	192	RTP	192.168.207.231	192.168.10.146
2451	33.831265000	192	RTP	192.168.207.231	192.168.10.146
2457	31.868529000	192	RTP	192.168.207.231	192.168.10.146
2463	33.897331000	192	RTP	192.168.207.231	192.168.10.146
2466	33.898664000	192	RTP	192.168.207.231	192.168.10.146
2470	33.927687000	192	RTP	192.168.207.231	192.168.10.146
2471	33.929528000	192	RTP	192.168.207.231	192.168.10.146
2478	31.967359000	192	RTP	192.168.207.231	192.168.10.146
2479	33.968921000	192	RTP	192.168.207.231	192.168.10.146

Packet details for packet 2340:

- Ethernet II, Src: Cisco_ae:60:96 (e8:40:1aa:60:96), Dst: Cisco_df:be:65 (00:07:7d: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
 - Version: RFC 1889 Version (2)
 - Padding: false
 - Extension: False
 - Contributing source identifiers count: 0
 - Marker: False
 - Payload type: dynamic type 97 (97)
 - Sequence number: 45534
 - Timestamp: 93310574
 - Synchronizer source identifier: 0x189b89c0 (412866578)

Beachten Sie die Anzahl gefilterter Pakete im unteren Bereich des Wireshark-Dienstprogramms für beide Erfassungen. Die **angezeigte** Anzahl gibt die Anzahl der Pakete an, die den gewünschten Filterkriterien entsprechen.

Der zentrale Standort verfügt über 4.936 Pakete, die zwischen dem Start (4514) und dem Ende (50449) der RTP-Sequenznummern den gewünschten Filterkriterien entsprechen, während es in der Außenstelle nur 4.737 Pakete gibt. Dies weist auf einen Verlust von 199 Paketen hin. Beachten Sie, dass diese 199 Pakete mit der Anzahl der "Rcvr Lost Pkts" von 199 übereinstimmen, die in der Streaming-Statistik des IP-Telefons der Außenstelle zu sehen war, die am Anfang dieses Dokuments gezeigt wurde.

Dies bestätigt, dass alle verlorenen Rcvr-Pakete tatsächlich Netzwerkverluste im WAN verursacht haben. Auf diese Weise wird der Punkt des Paketverlusts im Netzwerk isoliert, während Probleme mit der Audio-/Videoqualität bei mutmaßlichen Netzwerkverlusten auftreten.