Troubleshoot Network Related Audio Issues on Catalyst 9000 Switches

Contents

Introduction

This document describes how to troubleshoot network-related audio issues in a voice over IP (VoIP) environment.

Requirements

Cisco recommends that you have knowledge of these topics:

- QoS
- VoIP networks
- SPAN (Switchport Analyzer)
- Wireshark

Components Used

The information in this document is based on these software and hardware versions:

- Catalyst 9200
- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

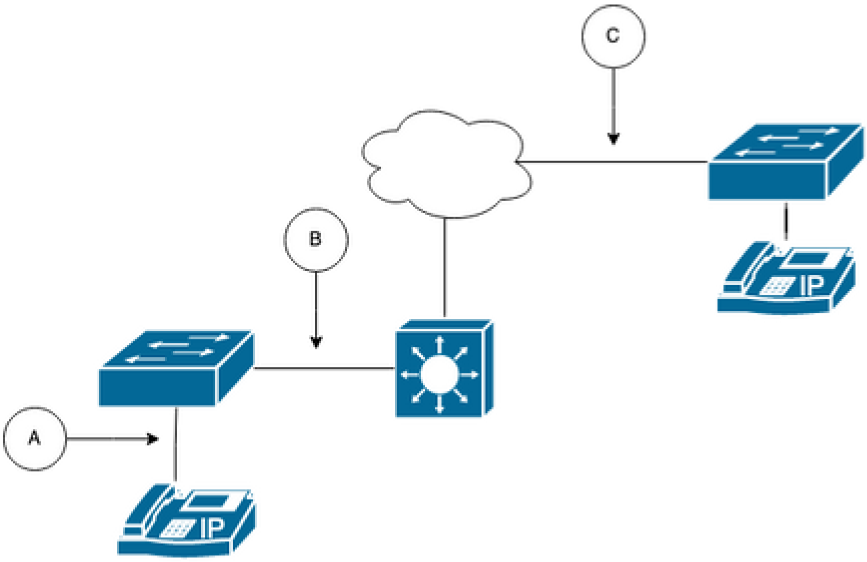
Background Information

In a VoIP infrastructure, the quality of the audio can be impacted by network-related issues, whose symptoms include:

- Intermittent gaps in the voice or choppy audio.
- One-way audio.
- Not isolated to a single user but to a group of users that have common characteristics, such as sharing the same VLAN or sharing the same access switch.

In order to troubleshoot network-related issues, it is important to have a clear topology from source to destination of the voice packets. The diagnosis of the problem can start at any point in the network where voice packets are switched or routed, however it is recommended to start the troubleshoot at the access layer and move up to the routing layer.

Network Diagram



Choose a capture point in the path. It can be either A (Closest to one IP Phone), B (Before routing), C (Closest to the destination).

The SPAN capture is normally taken in both directions (TX and RX) in order to identify both sides of the conversation and extract the respective audio, along with other variables such as jitter, or packet loss, from the capture for further analysis.

After having the capture point determined, setup the SPAN configuration on the switch.

<#root>

Switch(config)#

monitor session 1 source interface Gig1/0/1 both

```
Switch(config)#
```

monitor session 1 destination interface Gig1/0/6 encapsulation replicate

```
Switch#
```

show monitor session all

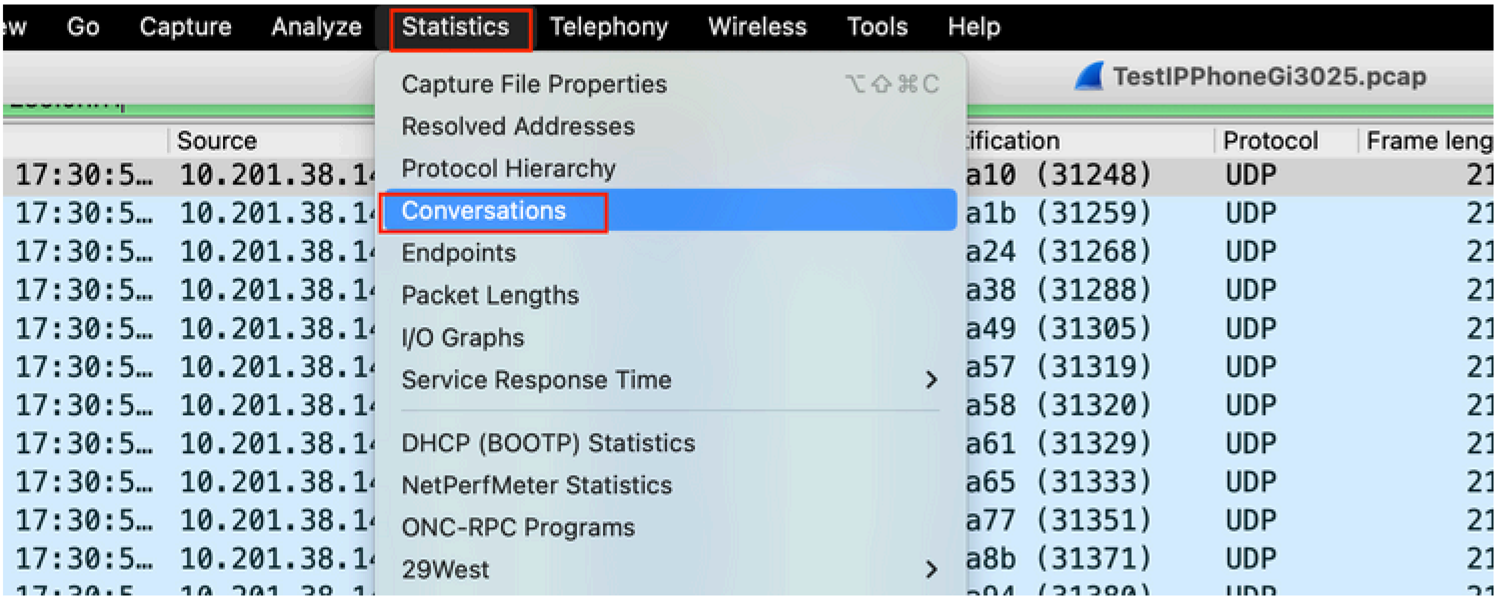
```
Session 1
---------
Type : Local Session
Source Ports :
Both : Gi1/0/1
Destination Ports : Gi1/0/6
```

```
Encapsulation : Replicate
Ingress : Disabled
```

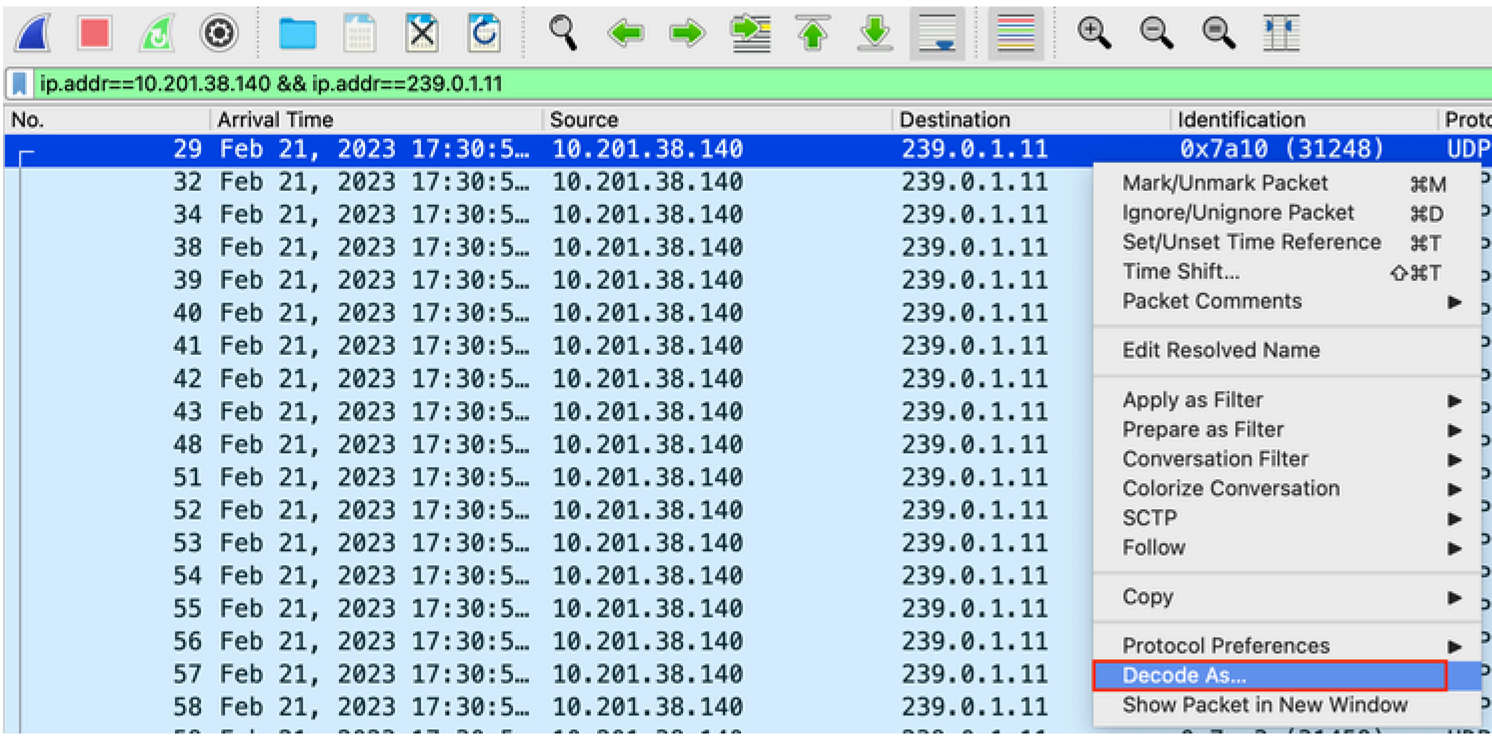
Initiate a test call to capture the audio flow from the chosen capture point in a PC/Laptop with Wireshark.

Capture Analysis

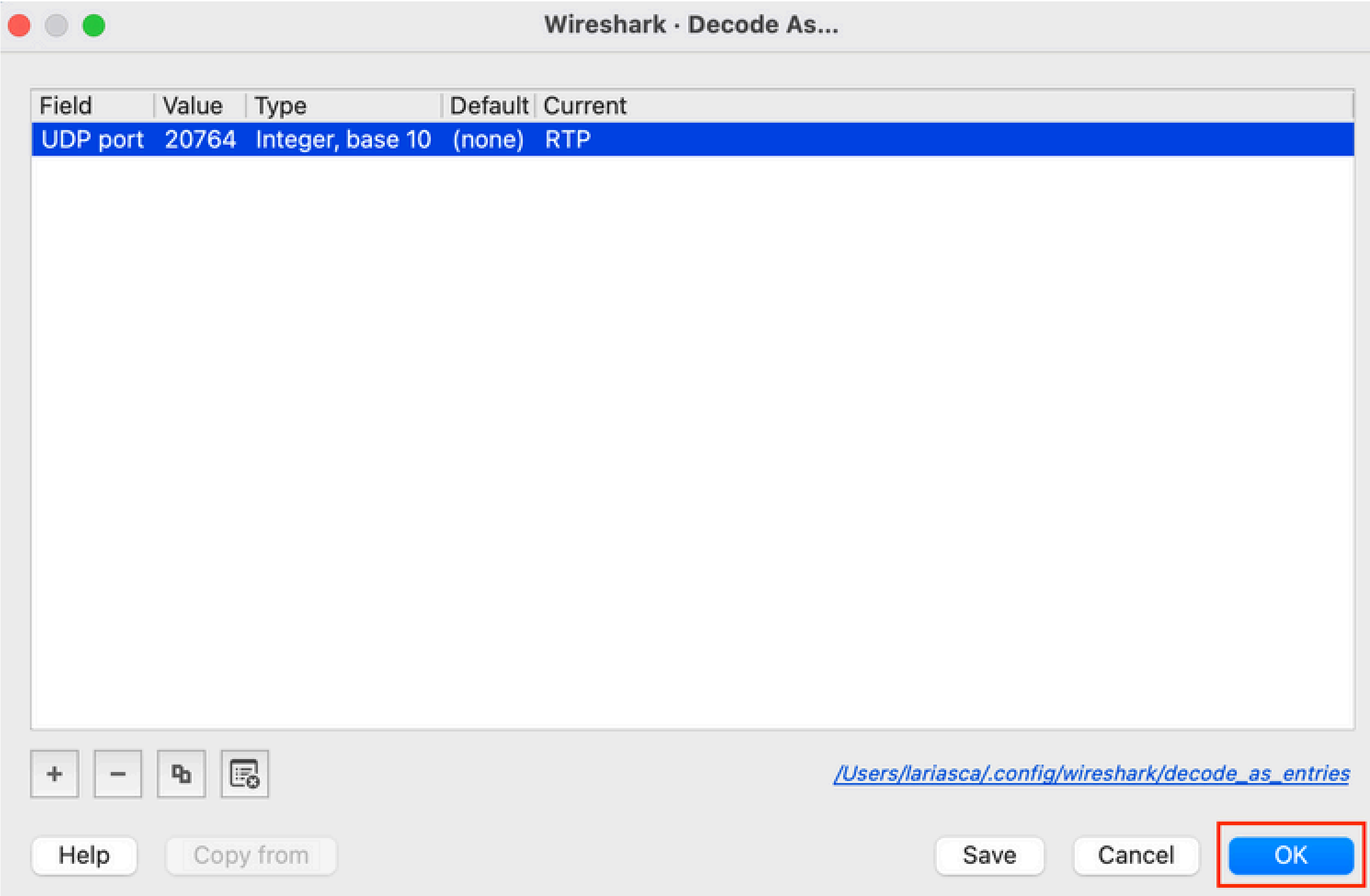
1. Open the packet capture taken using Wireshark and navigate to **Statistics** > **Conversations**. Find the audio conversation based on the IP address of the involved devices (IP Phone source and destination).



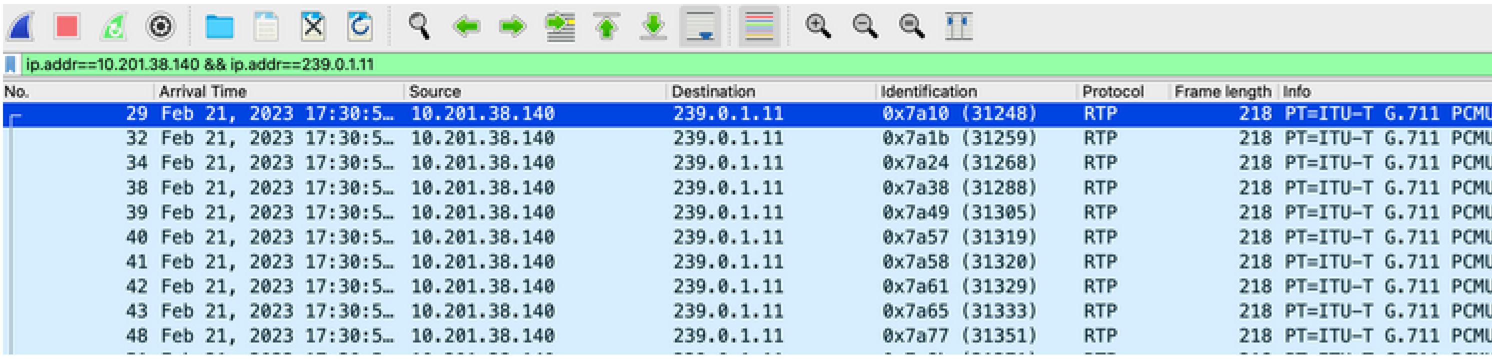
2. Normally, audio streams are carried by the UDP protocol, and most of the times they are not decoded in the proper format for Wireshark to extract the audio embedded into it. Then, the next step is to decode the UDP stream into audio format, by default RTP is used. Right click on any packet of the stream, then click on **Decode as**.



3. Look for the **Current** column and choose RTP. Click **Ok**.



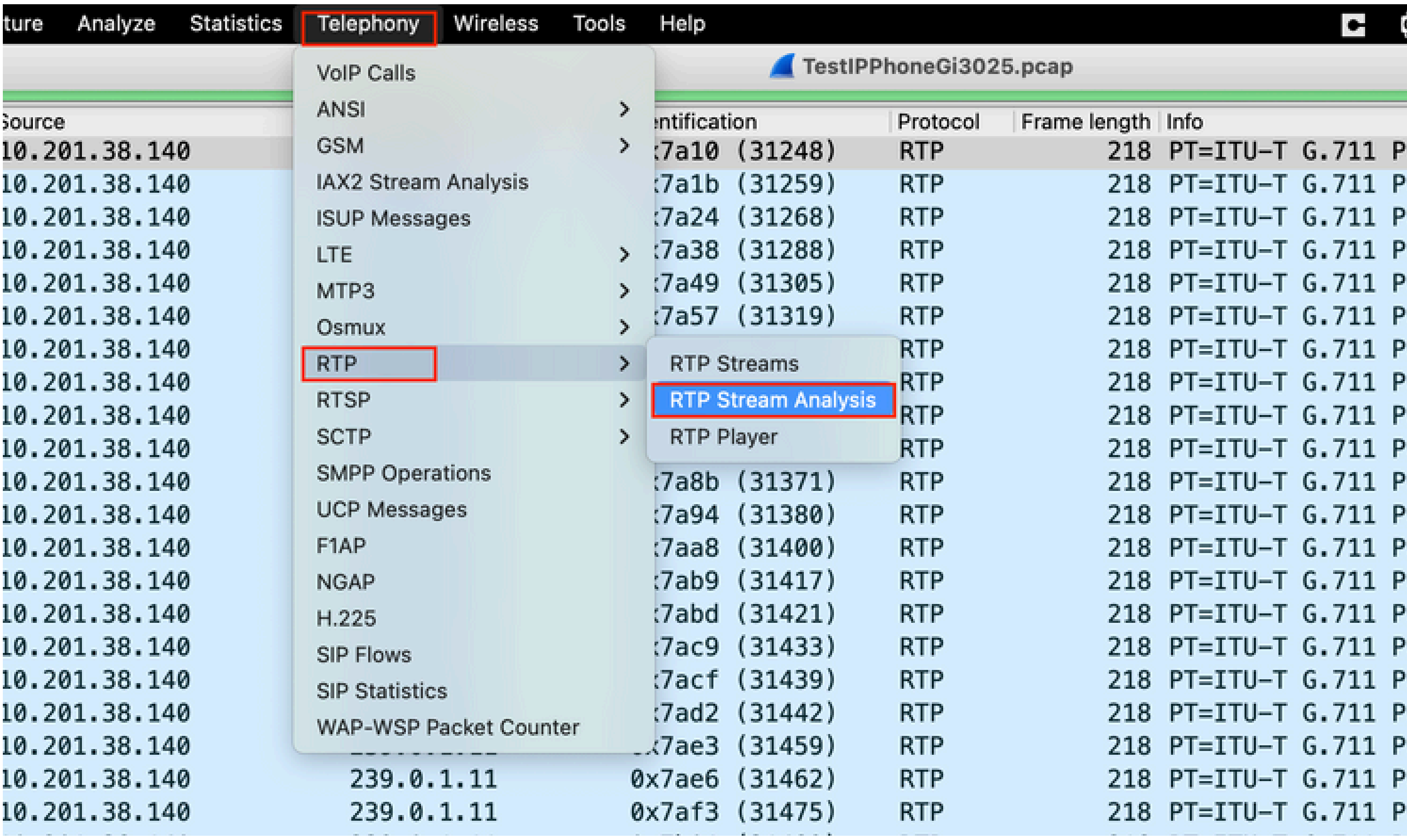
Wireshark decodes the entire UDP stream into RTP and we can now analyze the contents.

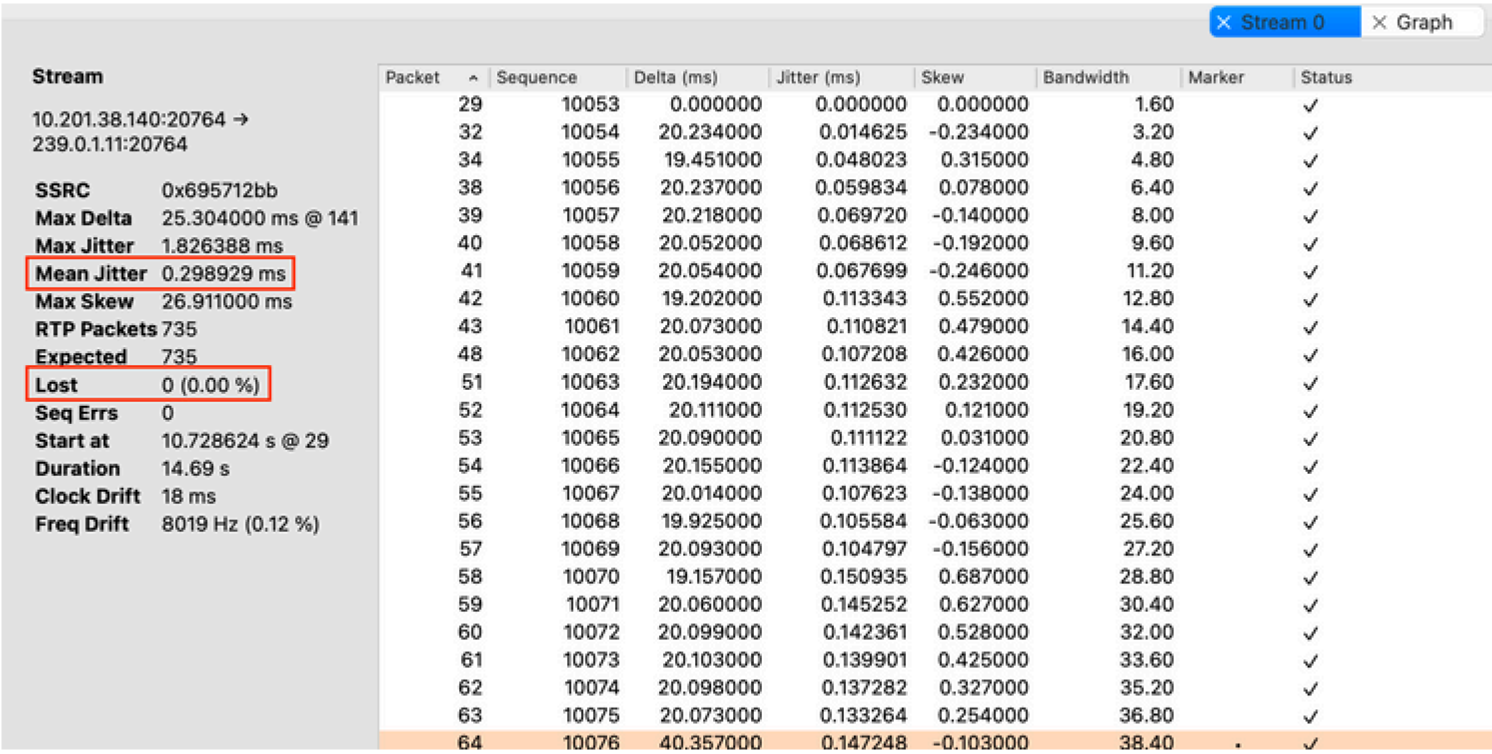


Caution: RTP Player is able to play any codec supported by an installed plugin. The codecs supported by RTP Player depend on the version of Wireshark youâ€™re using. The official builds contain all of the plugins maintained by the Wireshark developers, but custom/distribution builds are not include some of those codecs. To check your Wireshark installed codec plugins, do the following: **Open Help > About Wireshark**. Select the **Plugins** tab. In the **Filter by** type menu, select **Codec**.

---

4. Check the RTP statistics to see if there is any jitter or loss in the audio stream. To see the analyzis navigate to **Telephony > RTP > RTP Stream Analysis**.

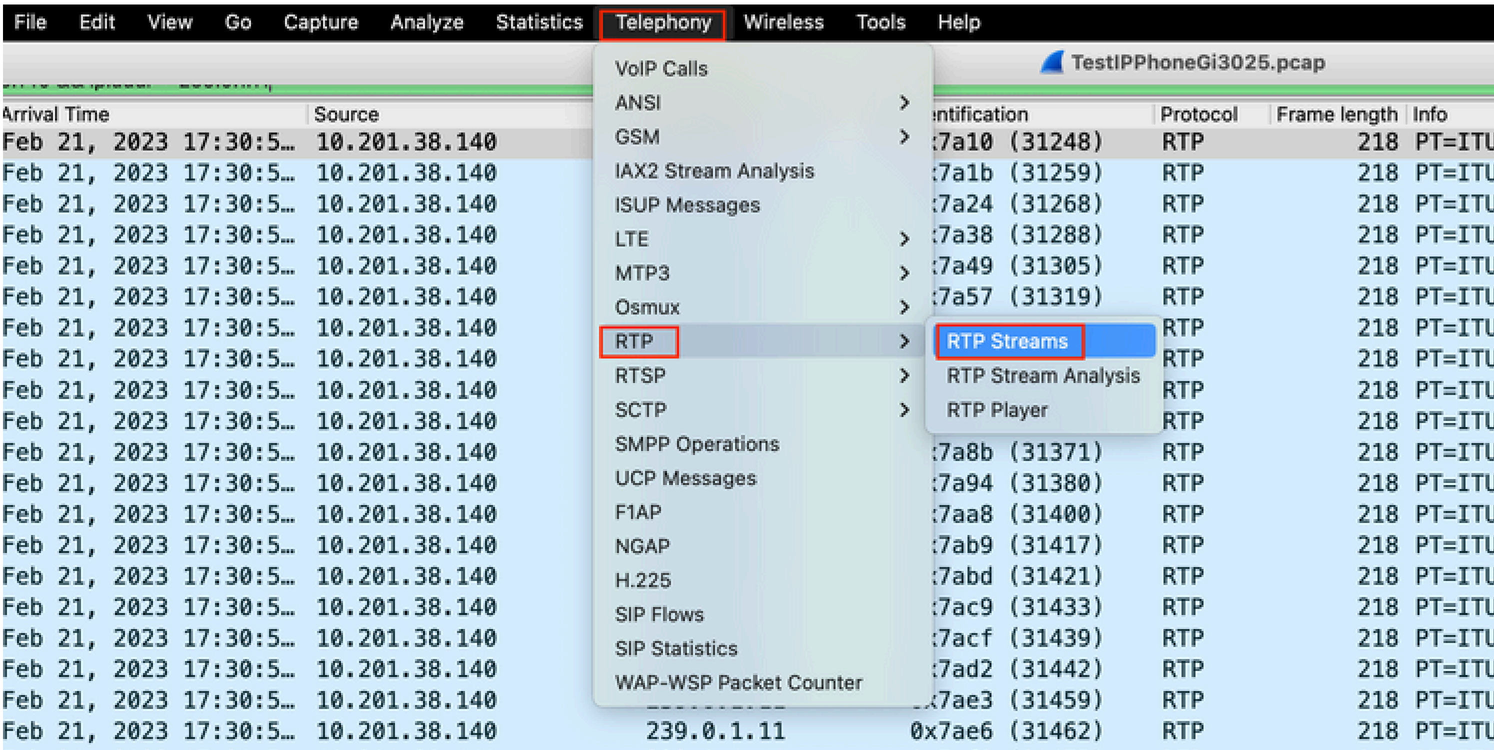




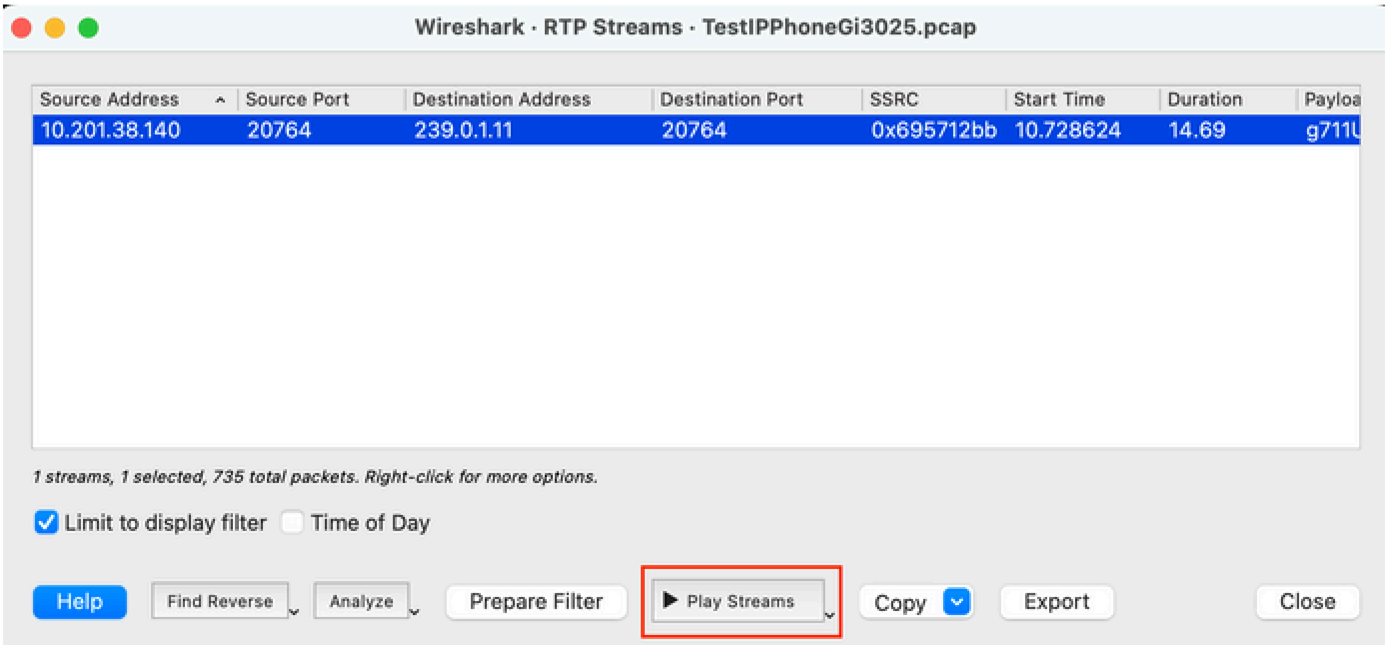
Jitter: Is the time delay in sending the voice packets over the network. This is often caused by network congestion or route changes. This measurement must be < 30ms.

Lost: Packets that were not received as part of the audio stream. Packet loss must not be more than 1%.

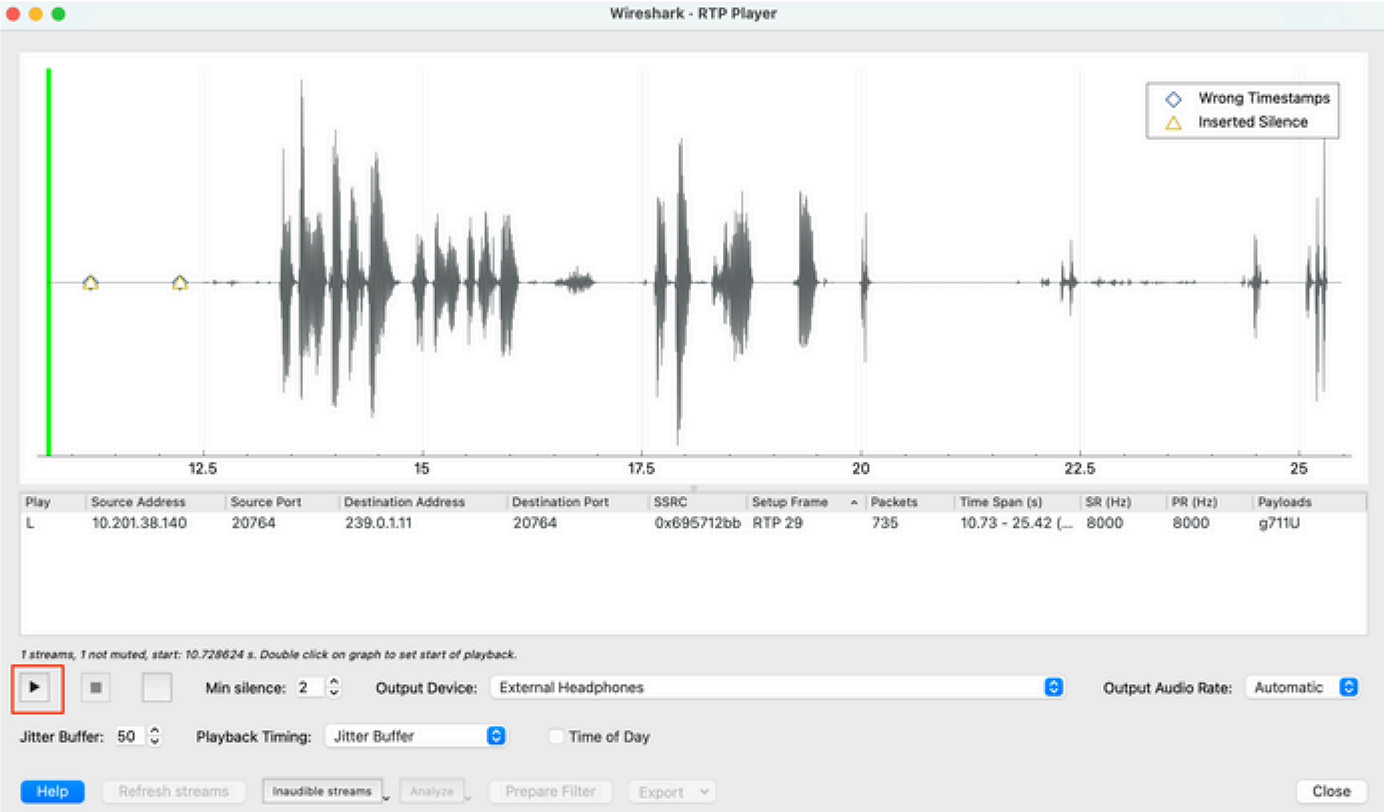
5. Convert the audio wave from this stream in **Telephony > RTP > RTP Streams**



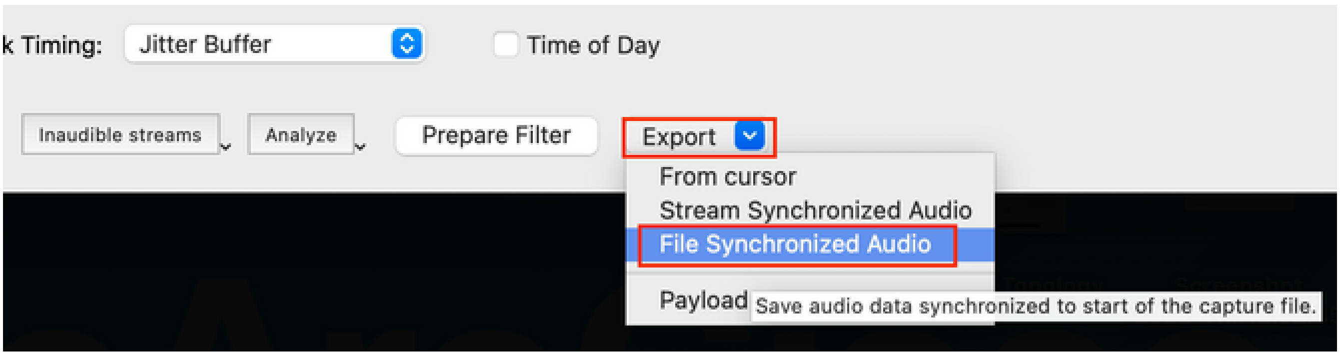
6. Select the stream to convert it to audio and click on **Play Streams.**



An audio wave must show up and the play button is available to listen in to the audio data. Hearing the audio helps to identify if there is choppy voice or one-way audio issues with the streams.



7. Export the stream into an audio file with .wav extension by clicking in **Export > File Synchronized Audio**.



Troubleshoot

After using the SPAN feature to collect and analyze the capture with Wireshark, we would have an understanding if the issue can be related to jitter, packet loss or one-way audio. If any issues found in the packet captures, next step is to check the device where capture was taken for any common problems that can impact a RTP audio stream.

Choppy Audio

Insufficient bandwidth, jitter and/or packet loss can be common causes to hearing broken voice or distortion in the audio capture.

1. Check if the jitter on the capture is > 30ms. If so, this indicates there is a time delay on the reception of the packets that can be caused by QoS policies or routing issues.

2. Verify if the packet lost on the capture is > 1%. In case this value is high, need to look for packet drops

along the path of the audio stream flow.

3. Check for drops on the ingress and egress interfaces involved in the path.

<#root>

Switch#

show interface Gi1/0/1 | inc drops

```
Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
0 unknown protocol drops
```

<#root>

Switch#

show interfaces Gi1/0/1 counters errors

```
Port           Align-Err     FCS-Err    Xmit-Err     Rcv-Err  UnderSize  OutDiscards
Gi1/0/1                0           0           0           0          0            0

Port         Single-Col  Multi-Col   Late-Col  Excess-Col  Carri-Sen      Runts
Gi1/0/1               0          0          0           0          0          0
```

Verify that there are no incrementing input/output drops or other incrementing errors on the interfaces.

4. Check the QoS egress policy on the interfaces involved in the path. Ensure that your traffic is mapped/classified in the Priority queue and that there are no drops in this queue.

<#root>

Switch#

show platform hardware fed switch 1 qos queue stats interface Gi1/0/1

```
----------------------------------------------------------------------------------------------
AQM Global counters
GlobalHardLimit:  3976   |   GlobalHardBufCount: 0
GlobalSoftLimit: 15872   |   GlobalSoftBufCount: 0

----------------------------------------------------------------------------------------------
High Watermark Soft Buffers:  Port Monitor Disabled
----------------------------------------------------------------------------------------------
Asic:0 Core:1 DATA Port:0 Hardware Enqueue Counters
----------------------------------------------------------------------------------------------
 Q Buffers          Enqueue-TH0          Enqueue-TH1          Enqueue-TH2             Qpolicer
   (Count)              (Bytes)              (Bytes)              (Bytes)              (Bytes)
-- ------- -------------------- -------------------- -------------------- --------------------
 0       0                    0               707354              2529238                    0
```

<<< Priority Q

```
 1       0                    0                    0              1858516                    0
 2       0                    0                    0                    0                    0
 3       0                    0                    0                    0                    0
```

```
 4       0                   0                   0                   0                   0
 5       0                   0                   0                   0                   0
 6       0                   0                   0                   0                   0
 7       0                   0                   0                   0                   0
Asic:0 Core:1 DATA Port:0 Hardware Drop Counters
--------------------------------------------------------------------------------------------------------------
 Q             Drop-TH0            Drop-TH1            Drop-TH2            SBufDrop              QebD
                (Bytes)             (Bytes)             (Bytes)             (Bytes)               (Byt
-- ------------------- ------------------- ------------------- ------------------- ------------------
 0                   0                   0                   0                   0
```

<<< Priority Q Drops

```
 1                   0                   0                   0                   0
 2                   0                   0                   0                   0
 3                   0                   0                   0                   0
 4                   0                   0                   0                   0
 5                   0                   0                   0                   0
 6                   0                   0                   0                   0
 7                   0                   0                   0                   0
```

> **Note**: If there are drops, make sure to profile the Voice traffic properly with DSCP Expedite Forwarding (EF) markings, and confirm that there are no other rogue flows erroneously been marked with the EF bit, thus congesting the Priority queue.

One-Way Audio

When a phone call is established, only one of the parties receive the audio. Common causes for this issue are related to reachability issues, routing problems or NAT/Firewall issues.

1. Do a ping to the destination subnet or destination gateway to confirm there is bi-directional reachability.

<#root>

Switch#

ping 192.168.1.150

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.150, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

2. Do a traceroute from source to destination subnet and viceversa. This can help check how many hops are in the path and if it is symmetric.

<#root>

Switch#

traceroute 192.168.1.150

```
Type escape sequence to abort.
Tracing the route to 192.168.1.150
```

```
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.2.12 2 msec * 1 msec
2 192.168.1.12 2 msec * 1 msec
3 192.168.1.150 2 msec 2 msec 1 msec
```

3. Check that the Gateway device for each subnet has optimal routing in place and that there is no assymetric paths potentially affecting the communication.

> **Tip**: Common one-way audio issues are related to misconfigured ACLs on Firewall rules or NAT issues. It is suggested to verify if these things could be affecting the audio stream flow.

---

4. Take a packet capture on the last device where the audio traffic was seen in for the failing direction. This can help isolate in which device of the path is the audio flow been lost. This is important because ping traffic can be allowed via NAT or firewall device, but specific audio traffic can be blocked or not translated properly.

Related Information

- **Cisco Technical Support & Downloads**