Catalyst 9000スイッチでのネットワーク関連の音声問題のトラブルシューティング

内容

概要

このドキュメントでは、Voice over IP(VoIP)環境でネットワーク関連の音声の問題をトラブルシューティングする方法について説明します。

要件

次の項目に関する知識があることが推奨されます。

- QoS
- VoIPネットワーク
- SPAN（スイッチポートアナライザ）
- Wireshark

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して

ください。

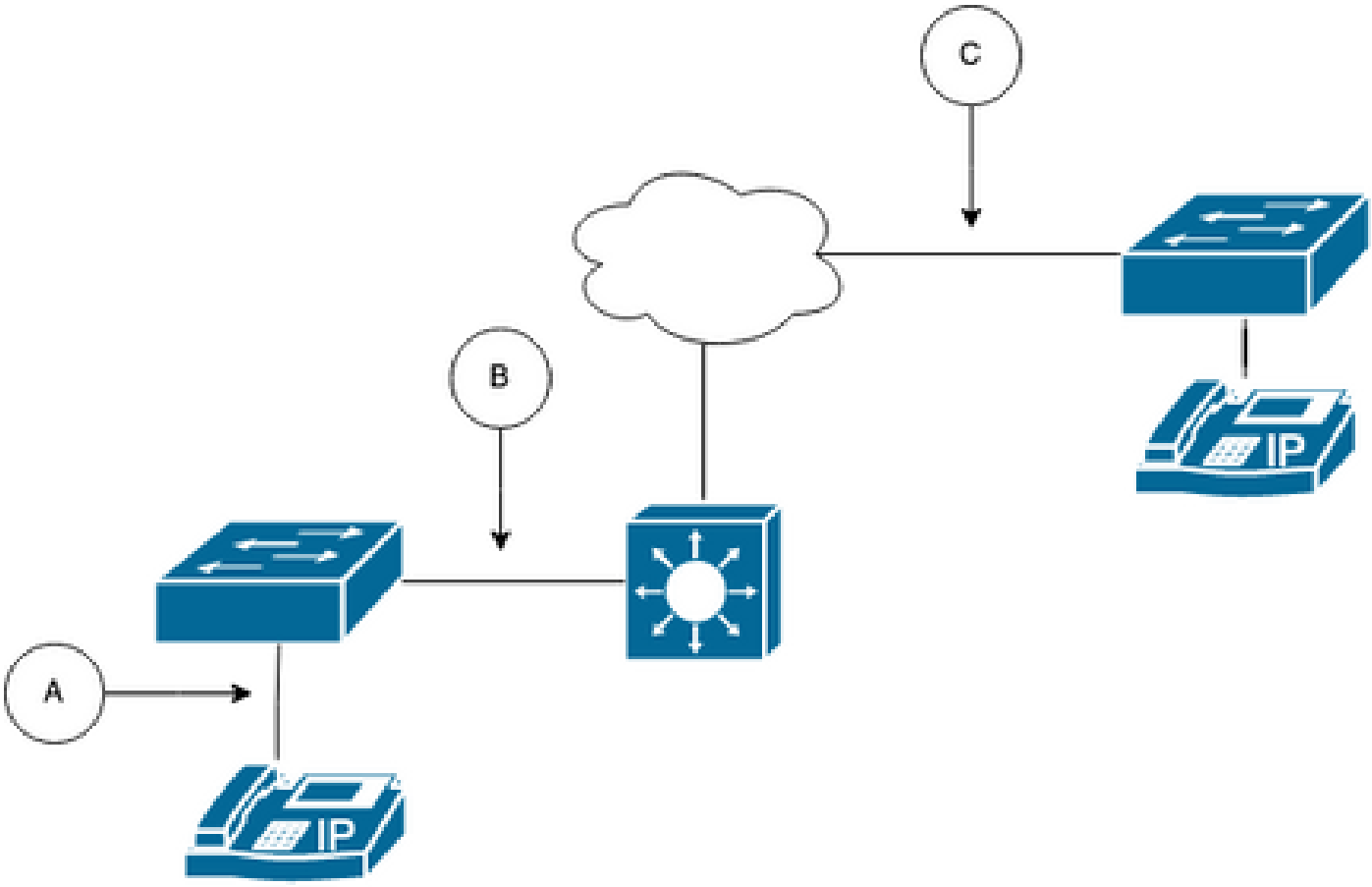
背景説明

VoIPインフラストラクチャでは、音声の品質がネットワーク関連の問題の影響を受ける可能性があります。その症状には次のものがあります。

- 断続的な音声の途切れや途切れる音声。
- 片通話.
- 単一のユーザではなく、同じVLANやアクセススイッチを共有するなど、共通の特性を持つユーザグループに分離される。

ネットワーク関連の問題をトラブルシューティングするには、音声パケットの送信元から宛先までの明確なトポロジを持つことが重要です。この問題の診断は、ネットワーク内で音声パケットがスイッチングまたはルーティングされる任意の時点から始まる可能性がありますが、トラブルシューティングはアクセス層から始めて、上位のルーティング層に移動することを推奨します。

ネットワーク図



パス内のキャプチャポイントを選択します。A（1台のIP Phoneに最も近いポート）、B（ルーティング前）、C（宛先に最も近いポート）のいずれかです。

SPANキャプチャは通常、会話の両側を識別し、ジッタやパケット損失などのその他の変数とともに各音声をキャプチャから抽出して詳細な分析を行うために、両方向（TXとRX）で取得され

ます。

キャプチャポイントを決定した後、スイッチのSPAN設定をセットアップします。

<#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#

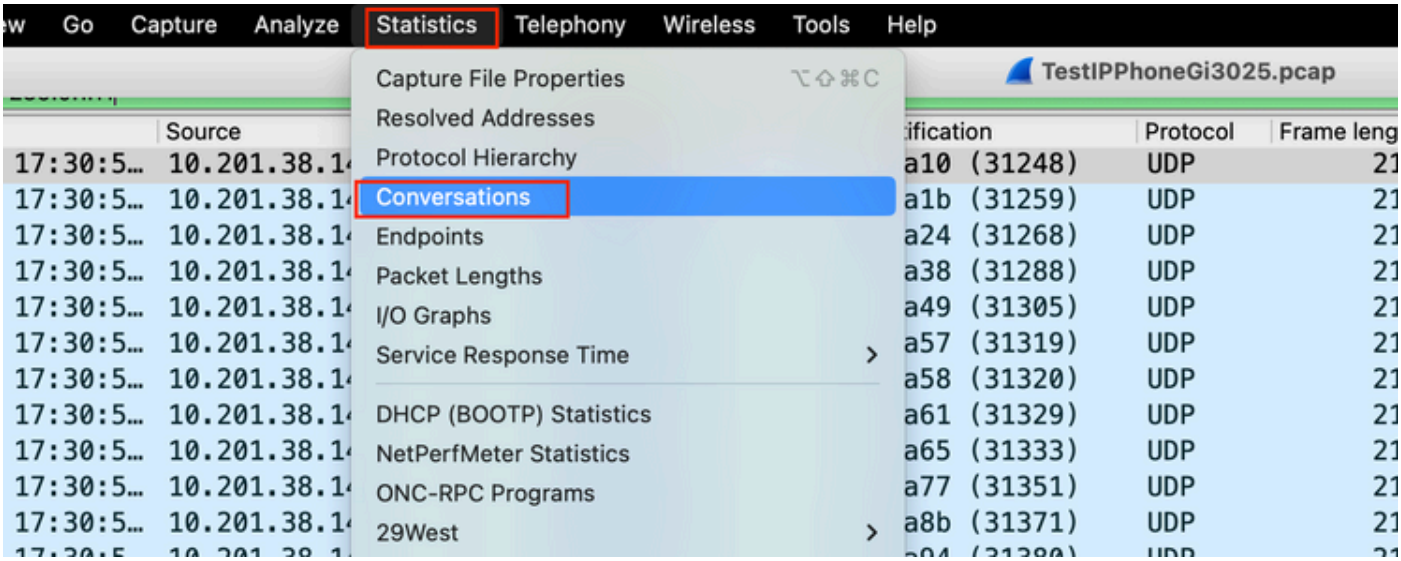
show monitor session all

```
Session 1
---------
Type : Local Session
Source Ports :
Both : Gi1/0/1
Destination Ports : Gi1/0/6
Encapsulation : Replicate
Ingress : Disabled
```

テストコールを開始して、Wiresharkを使用するPC/ラップトップで、選択したキャプチャポイントからのオーディオフローをキャプチャします。

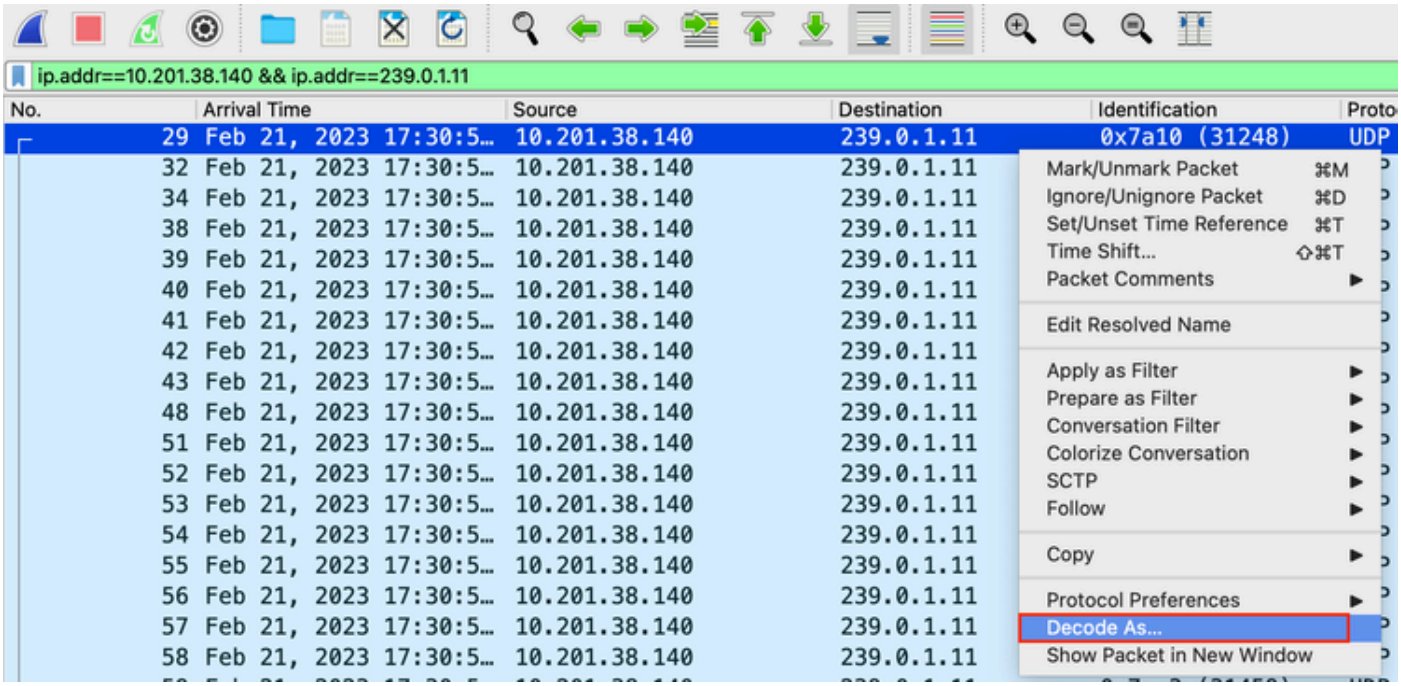
キャプチャ分析

1. Wiresharkで取得したパケットキャプチャを開き、Statistics > Conversationsの順に移動します。関係するデバイスのIPアドレス（IP Phoneの送信元と宛先）に基づいて音声会話を検索します。

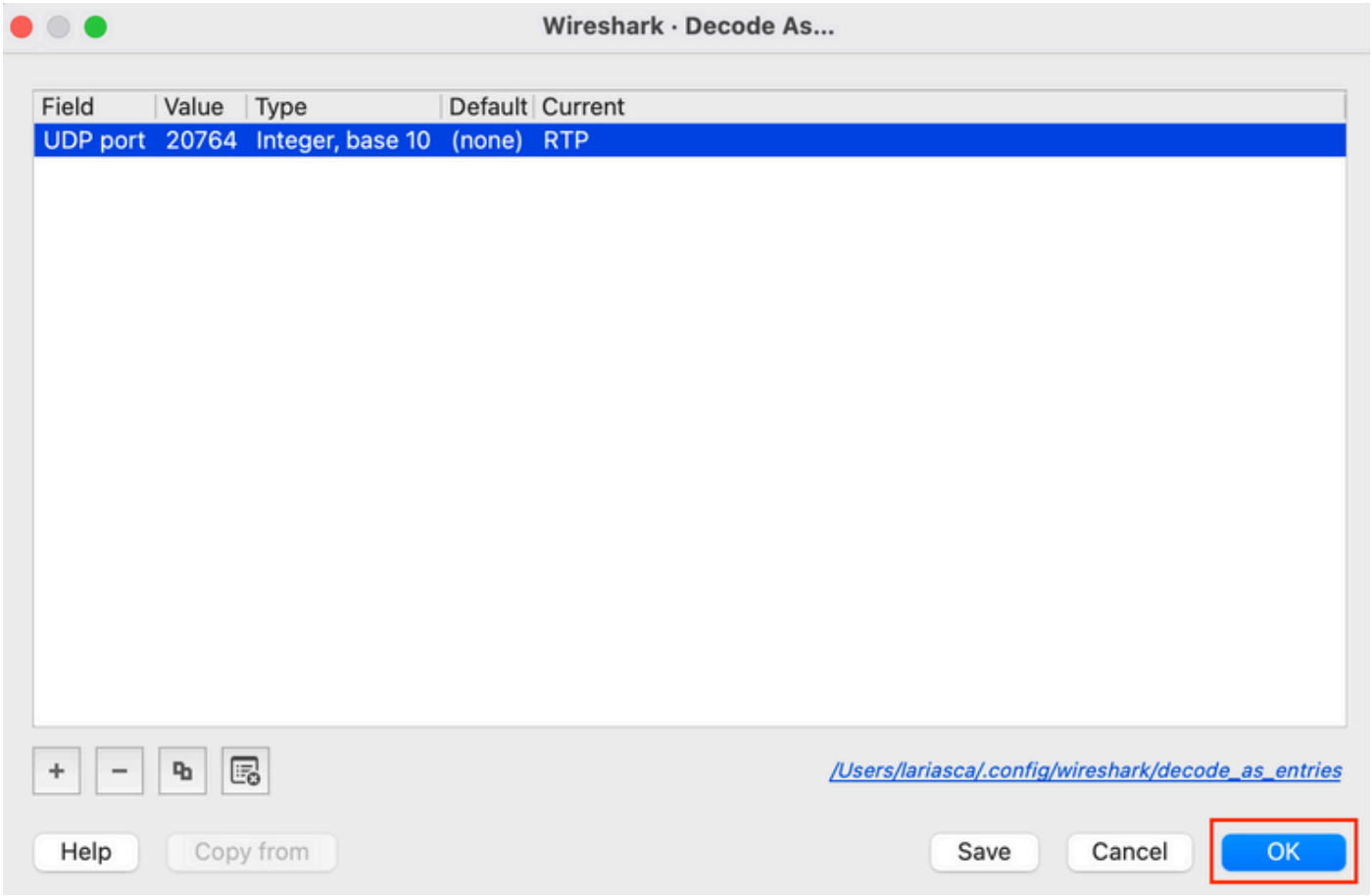


2.通常、オーディオストリームはUDPプロトコルによって伝送され、ほとんどの場合、

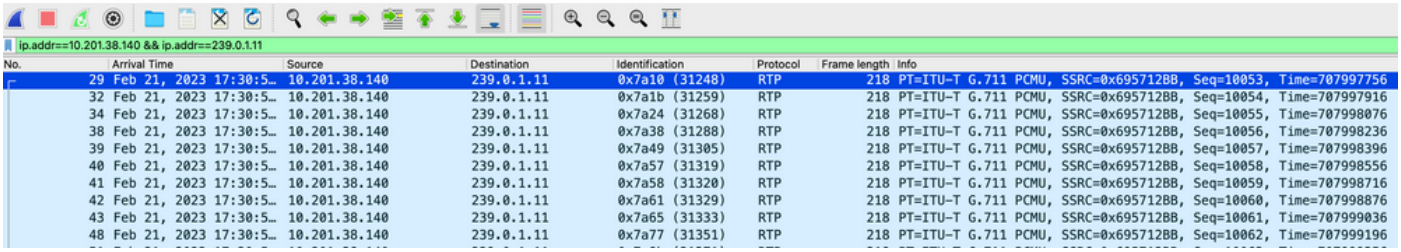
Wiresharkが埋め込まれたオーディオを抽出するための適切な形式でデコードされません。次に、UDPストリームをオーディオ形式にデコードします。デフォルトでは、RTPが使用されます。ストリームの任意のパケットを右クリックし、Decode asをクリックします。



3. 「現行」列を検索し、「RTP」を選択します。[OK] をクリックします。

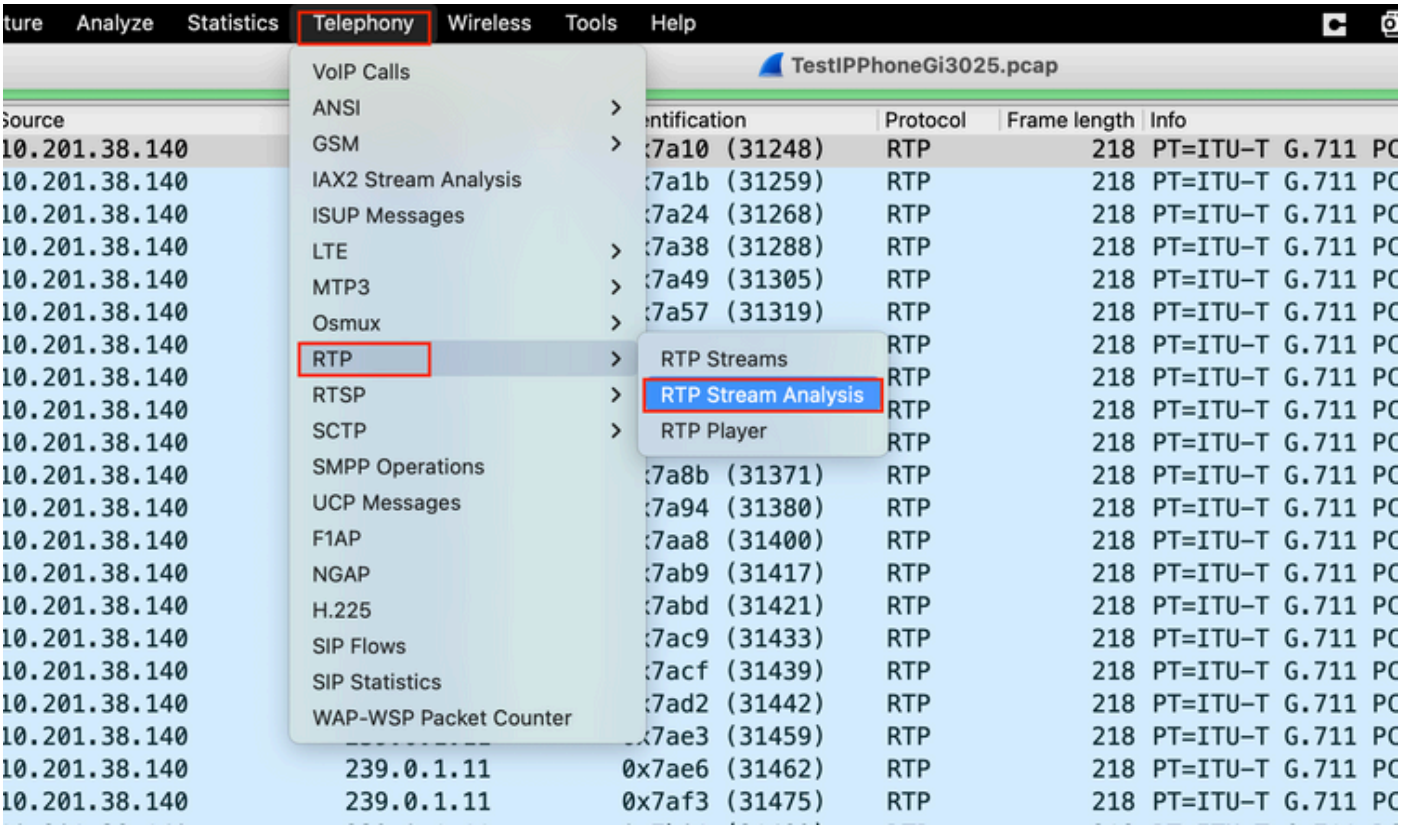


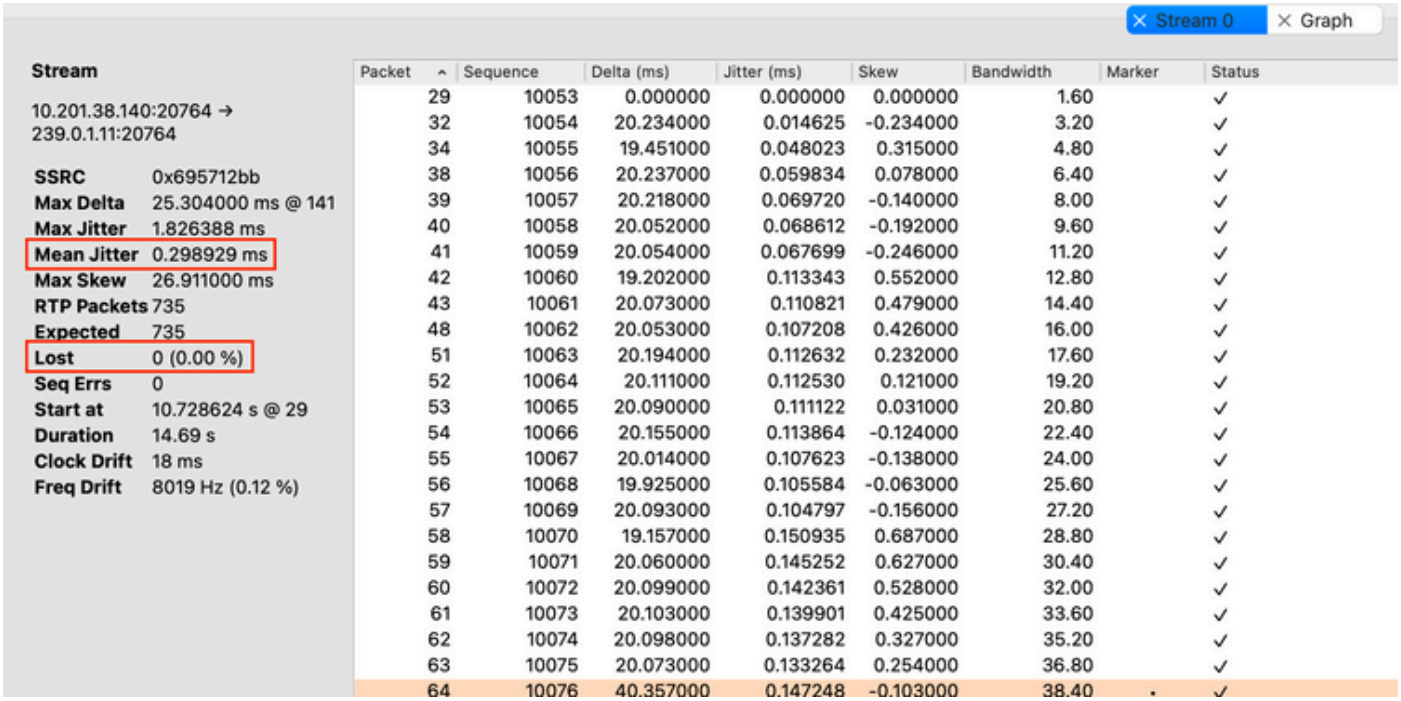
WiresharkはUDPストリーム全体をRTPにデコードし、コンテンツを分析できます。



注意:RTPプレーヤーは、インストールされているプラグインでサポートされている任意のコーデックを再生できます。RTP Playerでサポートされるコーデックは、使用しているWiresharkのバージョンによって異なります。公式のビルドには、Wireshark開発者が管理するすべてのプラグインが含まれていますが、カスタム/配布ビルドにはこれらのコーデックの一部は含まれていません。Wiresharkにインストールされているコーデックプラグインを確認するには、次の手順を実行します。Help > About Wiresharkを開きます。Pluginsタブを選択します。Filter by typeメニューで、Codecを選択します。

4. RTP統計情報をチェックして、音声ストリームにジッタや損失がないか確認します。分析を表示するには、Telephony > RTP > RTP Stream Analysisの順に選択します。

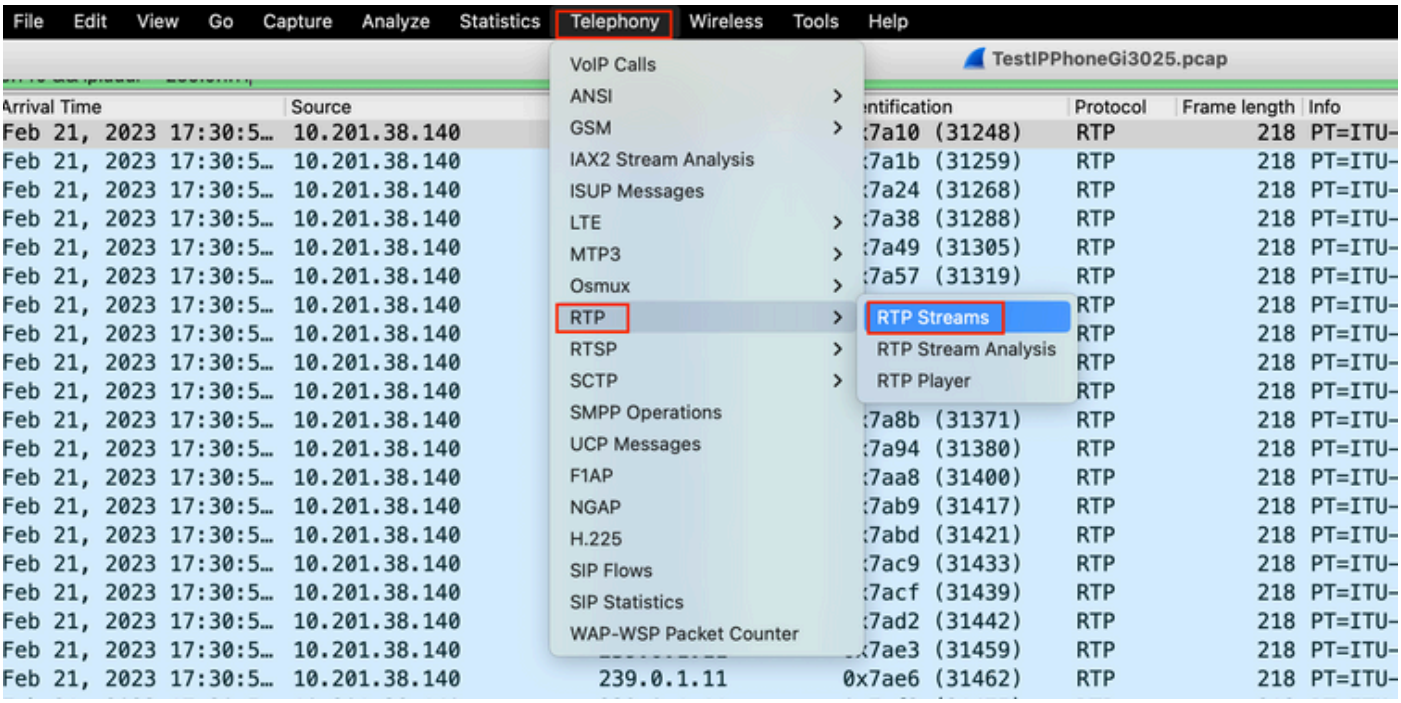




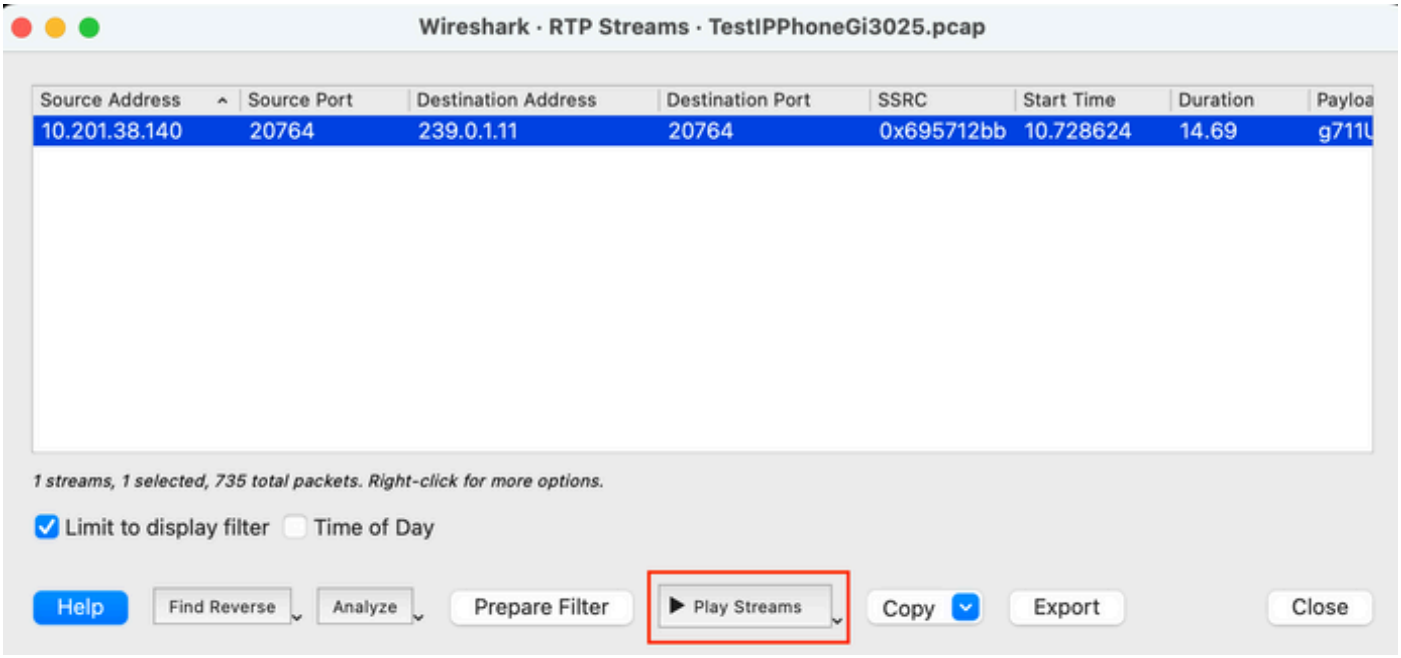
ジッタ：ネットワーク上で音声パケットを送信するときの遅延時間です。これは、多くの場合、ネットワークの輻輳またはルートの変更が原因で発生します。この測定値は30ミリ秒未満である必要があります。

Lost:オーディオストリームの一部として受信されなかったパケット。パケット損失は1 %以下である必要があります。

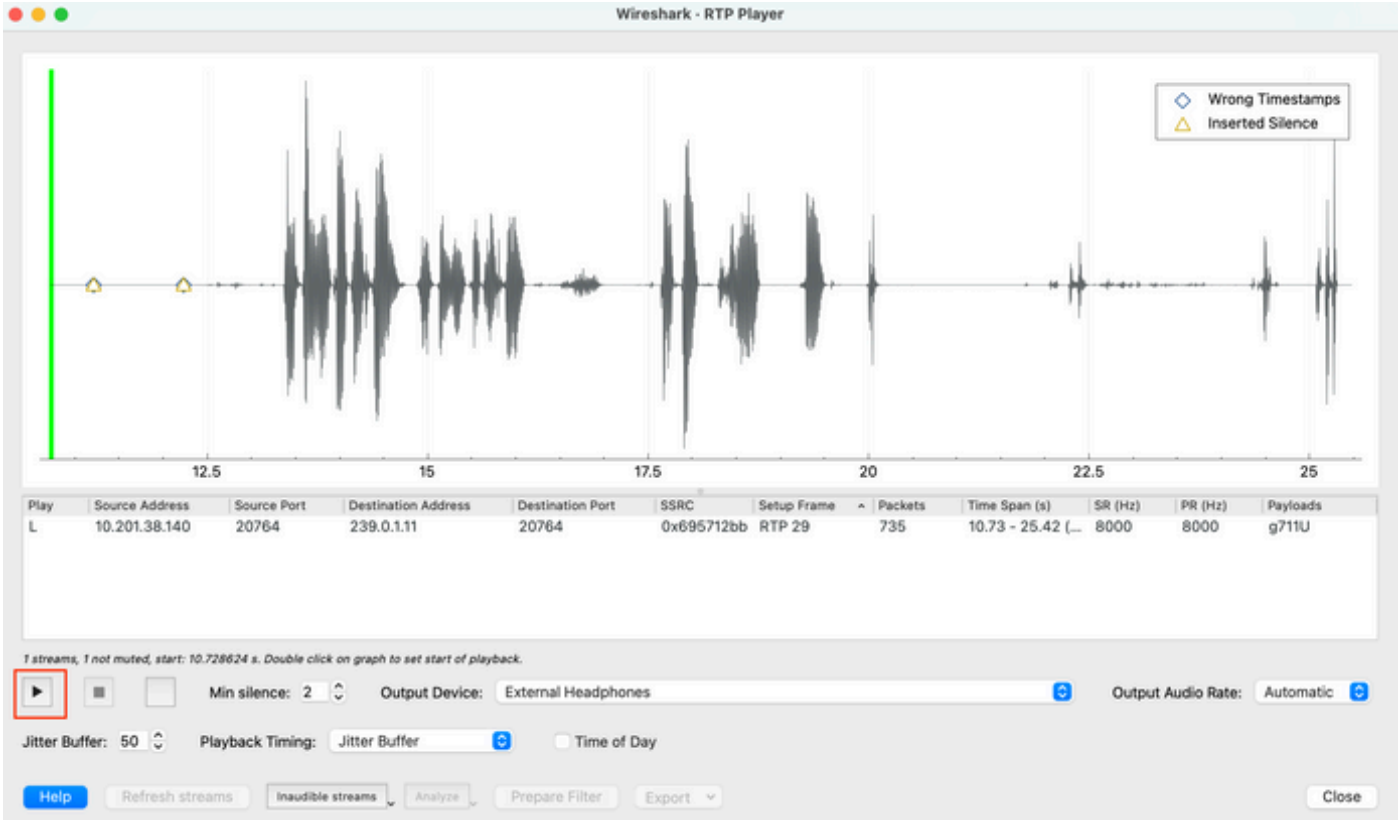
5. Telephony > RTP > RTP Streamsで、このストリームからの音声ウェーブを変換します。



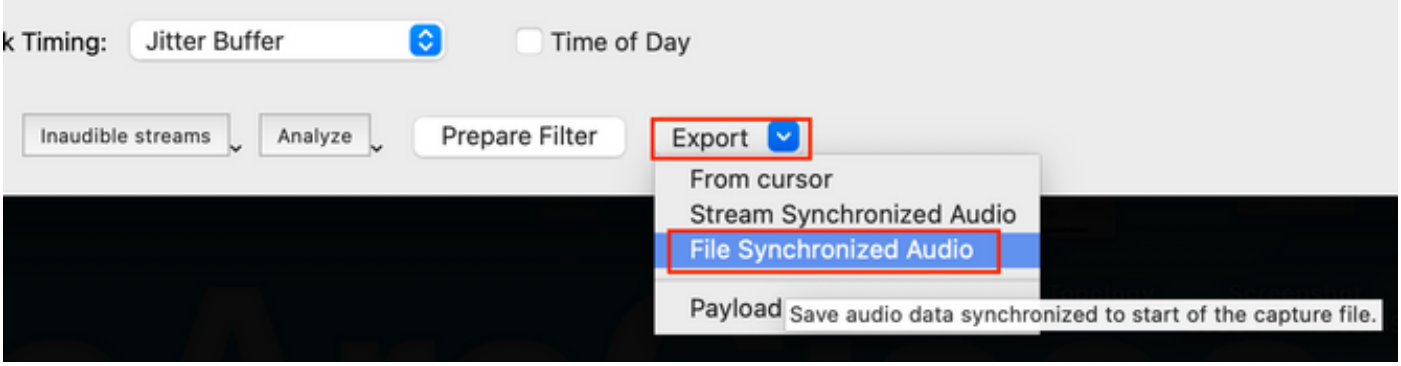
6.ストリームを選択してオーディオに変換し、 [ストリームの再生]をクリックします。



オーディオ波が表示され、再生ボタンを使用してオーディオデータを聞くことができます。音声を聞くと、音声が途切れていたり、ストリームに片通話の問題があったりするかどうかを特定するのに役立ちます。



7. Export > File Synchronized Audioの順にクリックして、.wav拡張子を持つオーディオファイルにストリームをエクスポートします。



トラブルシュート

SPAN機能を使用してWiresharkでキャプチャを収集して分析した後、ジッタ、パケット損失、または片通話に関連する問題が発生する可能性があるかどうかを理解できます。パケットキャプチャで問題が見つかった場合は、次にキャプチャが行われたデバイスで、RTPオーディオストリームに影響を与える可能性がある一般的な問題を確認します。

音声の途切れ

不十分な帯域幅、ジッタ、および/またはパケット損失は、音声キャプチャの音声の切断や歪みを聞く一般的な原因となる可能性があります。

1.キャプチャのジッタが30ミリ秒を超えているかどうかを確認します。その場合、QoSポリシーまたはルーティングの問題によって発生する可能性があるパケットの受信に時間遅延があることを示します。

2.キャプチャで失われたパケットが1 %を超えているかどうかを確認します。この値が高い場合は、オーディオストリームフローのパスに沿ってパケットドロップを探す必要があります。

3.パスに関係する入力インターフェイスと出力インターフェイスでのドロップを確認します。

<#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 Mult
```

インターフェイスで入出力の廃棄が増加していないこと、またはエラーが増加していないことを確認します。

4.パスに関係するインターフェイスのQoS出力ポリシーを確認します。トラフィックがプライオリティキューでマッピング/分類され、このキューでドロップが発生していないことを確認します。

<#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             Qeb
                (Bytes)              (Bytes)              (Bytes)              (Bytes)             (By
-- -------------------- -------------------- -------------------- -------------------- ----------
 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
```

注：ドロップが発生する場合は、DSCP緊急フォワーディング(EF)マーキングを使用して音声トラフィックを適切にプロファイリングし、EFビットで誤ってマーキングされた他の不

正フローがないことを確認します。これにより、プライオリティキューが輻輳します。

片通話

通話が確立されると、通話者の1人だけが音声を受信します。この問題の一般的な原因は、到達可能性の問題、ルーティングの問題、またはNAT/ファイアウォールの問題に関連しています。

1.宛先サブネットまたは宛先ゲートウェイにpingを実行して、双方向の到達可能性があることを確認します。

<#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.送信元サブネットから宛先サブネット、およびviceversaにtracerouteを実行します。これは、パス内にホップがいくつあるかを確認し、ホップが対称であるかどうかを確認する際に役立ちます。

<#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.各サブネットのゲートウェイデバイスに最適なルーティングが設定されていること、および通信に影響を与える可能性のある非対称パスが存在しないことを確認します。

ヒント：一般的な片通話の問題は、ファイアウォールルールのACLの誤設定やNATの問題に関連しています。これらの要因がオーディオストリームフローに影響を与えているかどうかを確認することを推奨します。

4.最後に音声トラフィックが見られたデバイスで、障害が発生している方向のパケットキャプチャを取得します。これは、音声フローが失われたパスのどのデバイスを特定するのに役立ちます

。pingトラフィックはNATまたはファイアウォールデバイスを介して許可できますが、特定の音声トラフィックはブロックされたり、正しく変換されなかったりする可能性があるため、これは重要です。

関連情報

- シスコテクニカルサポートおよびダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。