セキュアなファイアウォールのためのVoice over IP(VoIP)プロトコルの基本を理解する

内容

- はじめに
- 前提条件
  - 要件
  - 使用するコンポーネント
- VoIPの基本
  - シグナリング
  - メディア
    - メディアフロースルー
    - メディアフローアラウンド
- Session Initiation Protocol（SIP）
  - SIPコールメッセージ
  - SIPオプションメッセージ
  - SIP REGISTERメッセージ
  - セッション記述プロトコル（SDP）
  - 早期オファー
  - 遅延オファー
  - 初期メディア
- H.323
  - H.225
  - H.245
  - スロースタート
  - Fast Start
- SCCP
- MGCP
- ベスト プラクティス
- トラブルシュート
  - ファイアウォールのシグナリング問題のトラブルシューティング
  - ファイアウォールのメディア問題のトラブルシューティング
  - SIPコールのトラブルシューティング
- 関連情報

はじめに

このドキュメントでは、エンジニアがセキュアファイアウォールでVoIPプロトコルを効果的にトラブルシューティングする際に役立つさまざまなVoIPプロトコルの基礎について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントは、次のデバイスのトラブルシューティングシナリオでの使用を目的としています。

- セキュアファイアウォール脅威対策(FTD)
- セキュアファイアウォール適応型セキュリティアプライアンス(ASA)

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。

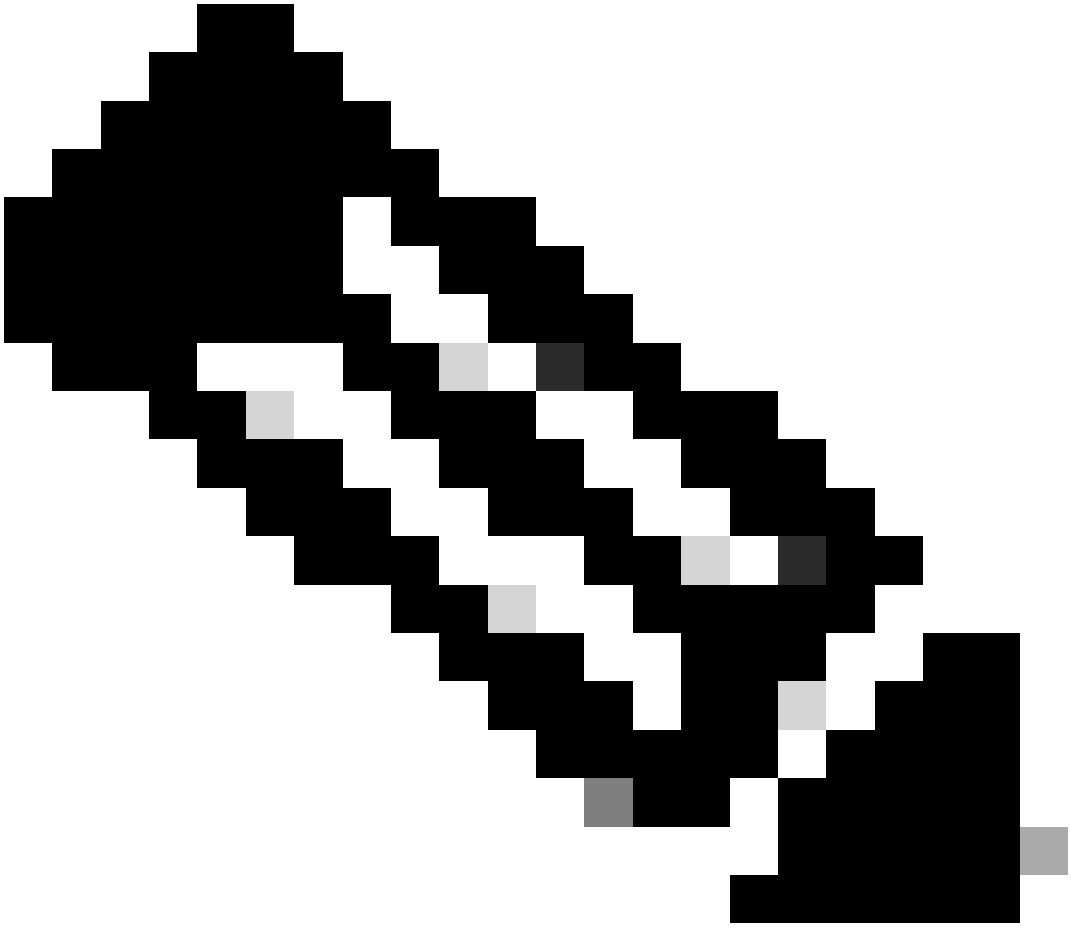
VoIPの基本

コミュニケーションは人と人とのインタラクションの基盤であり、Voice over IP(VoIP)プロトコルは人と人とのコミュニケーションに不可欠なものとなっています。そのため、ファイアウォール(FW)を含むシナリオをトラブルシューティングする際に、それぞれの役割を理解しておくことが重要です。

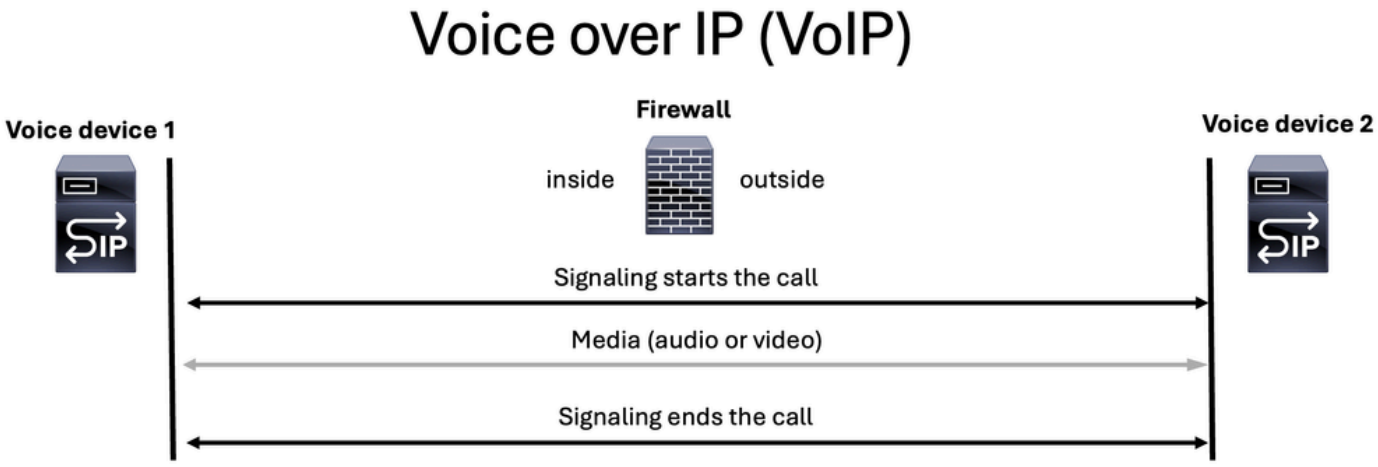
VoIPは、次の2つの部分で構成されています。

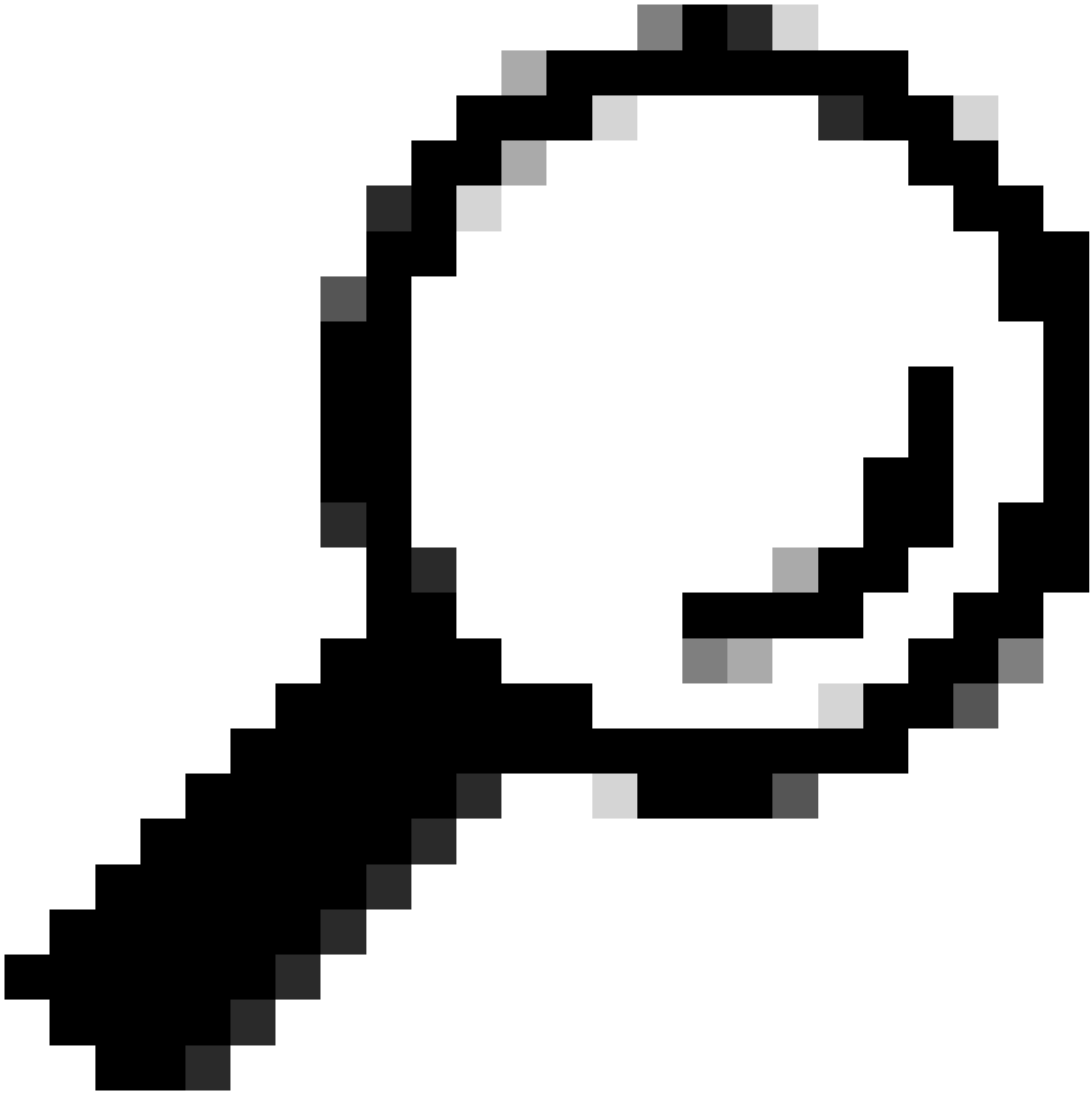
- シグナリング
- メディア（音声またはビデオ）

VoIP通信は常にコールを開始するためのシグナリング部分で始まり、メディア（音声またはビデオ）がストリーミングされ、最後にシグナリングがコールを終了します。

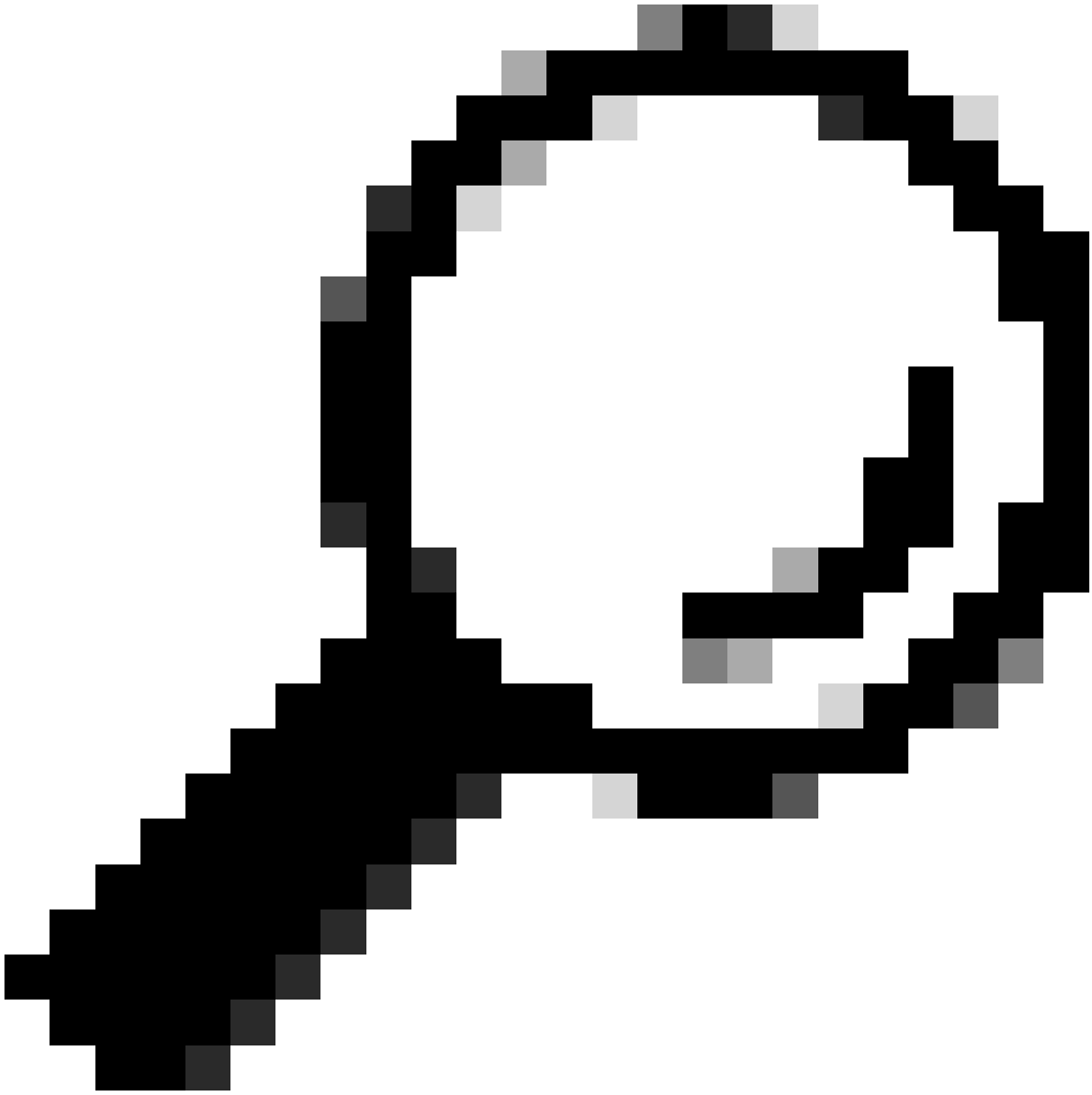


注:SIPは最も広く使用されているプロトコルであるため、多くの図では一貫してSIP音声サーバアイコンとして表されています。





ヒント:ASAまたはFTDの音声の問題をトラブルシューティングする場合は、ユーザの観点からシナリオを検討することが重要です。コールが確立されているかどうか、または音声が聞こえないか、片通話かを確認する必要があります。この情報は、問題がシグナリングプロトコルにあるのか、メディア（音声またはビデオ）プロトコルにあるのかについて、貴重な手がかりとなります。



ヒント：音声デバイスは、音声Real-time Transport Protocol(RTP)トラフィック、シグナリングトラフィック、またはその両方を同時に管理できます。音声の問題をトラブルシューティングする際には、次の主要な概念を覚えておくことが重要です。

++シグナリングサーバ：シグナリングトラフィックのみを処理します。

++メディアサーバ：音声RTPトラフィックのみを処理します。

++両方のタスクを処理できるデバイスもあります。

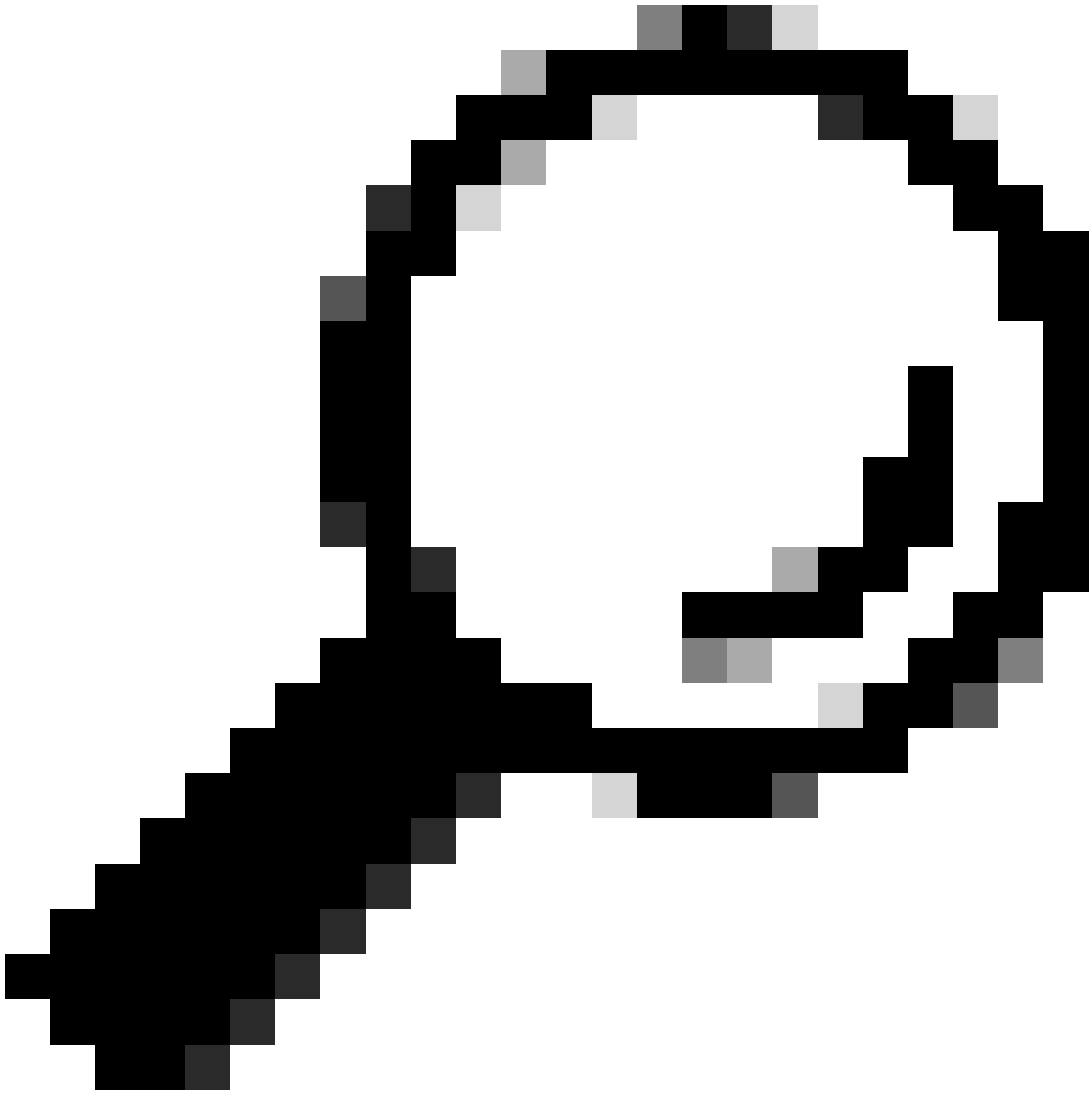
シグナリング

シグナリングプロトコルは、音声通信を開始するコールの一部であり、次の機能も実行します。

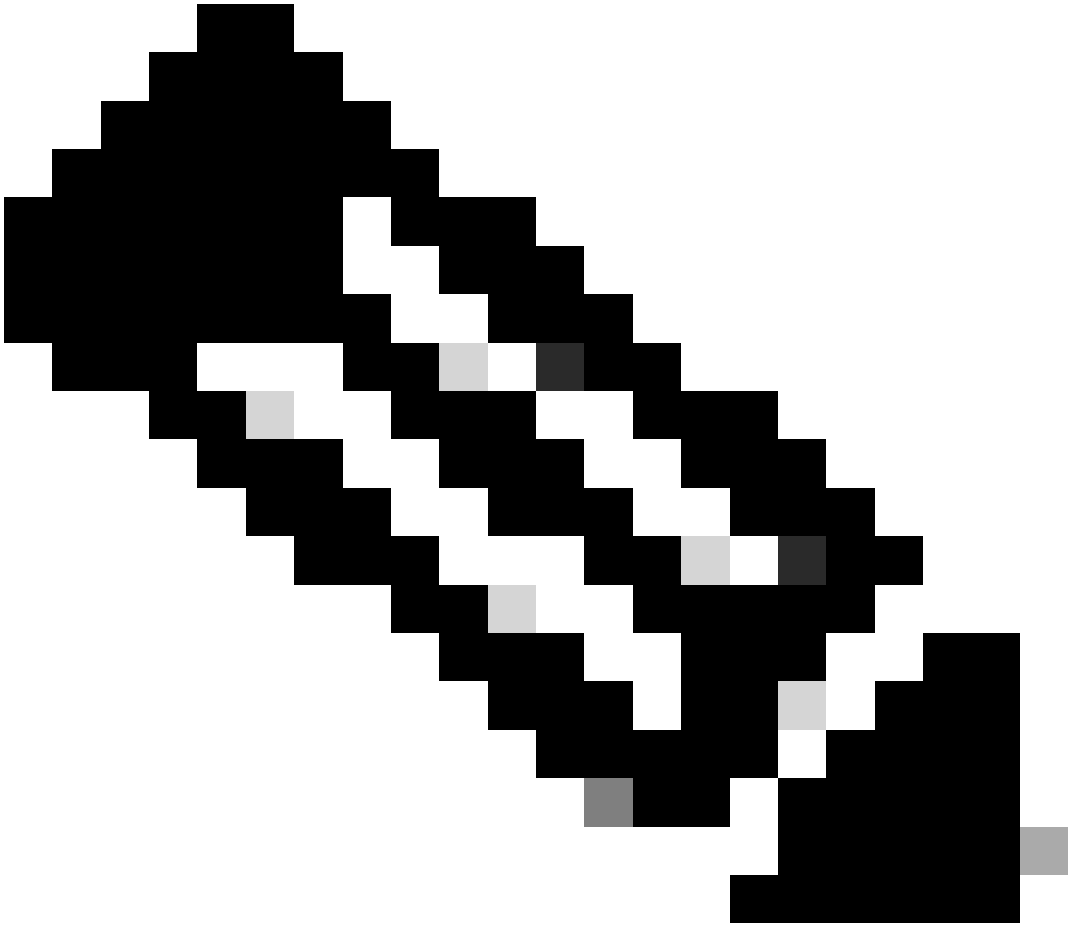
- 通信を維持する
- 通信を変更します。
- 通信を終了します。

コールの確立に役立つさまざまなタイプのシグナリングプロトコルのうち、最も一般的なものは次のとおりです。

- Session Initiation Protocol（SIP）
- H.323
- Media Gateway Control Protocol（MGCP）
- Skinny Call Control Protocol（SCCP）



ヒント：使用されているシグナリングプロトコルを特定して、ASAまたはFTDのパケットキャプチャに適したポートを判別することが重要です。また、コールフローとネットワークトポロジは、シグナリングパスを理解するのに役立ちます。

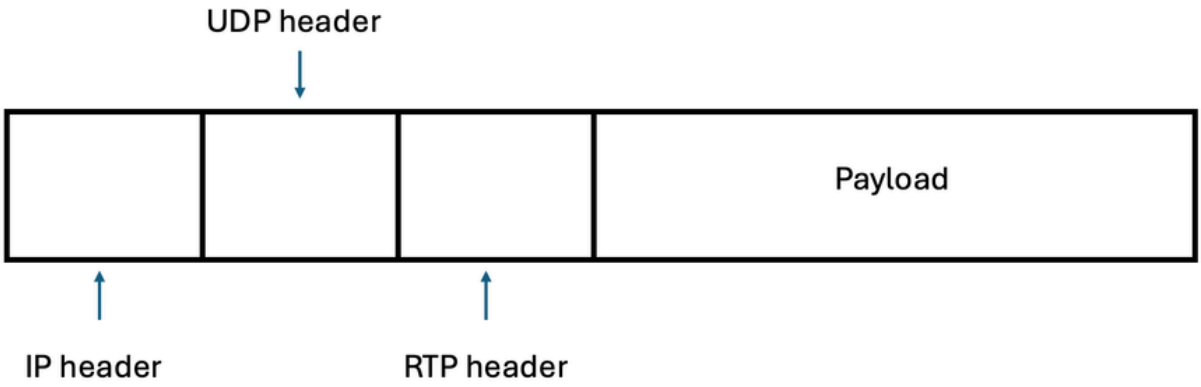


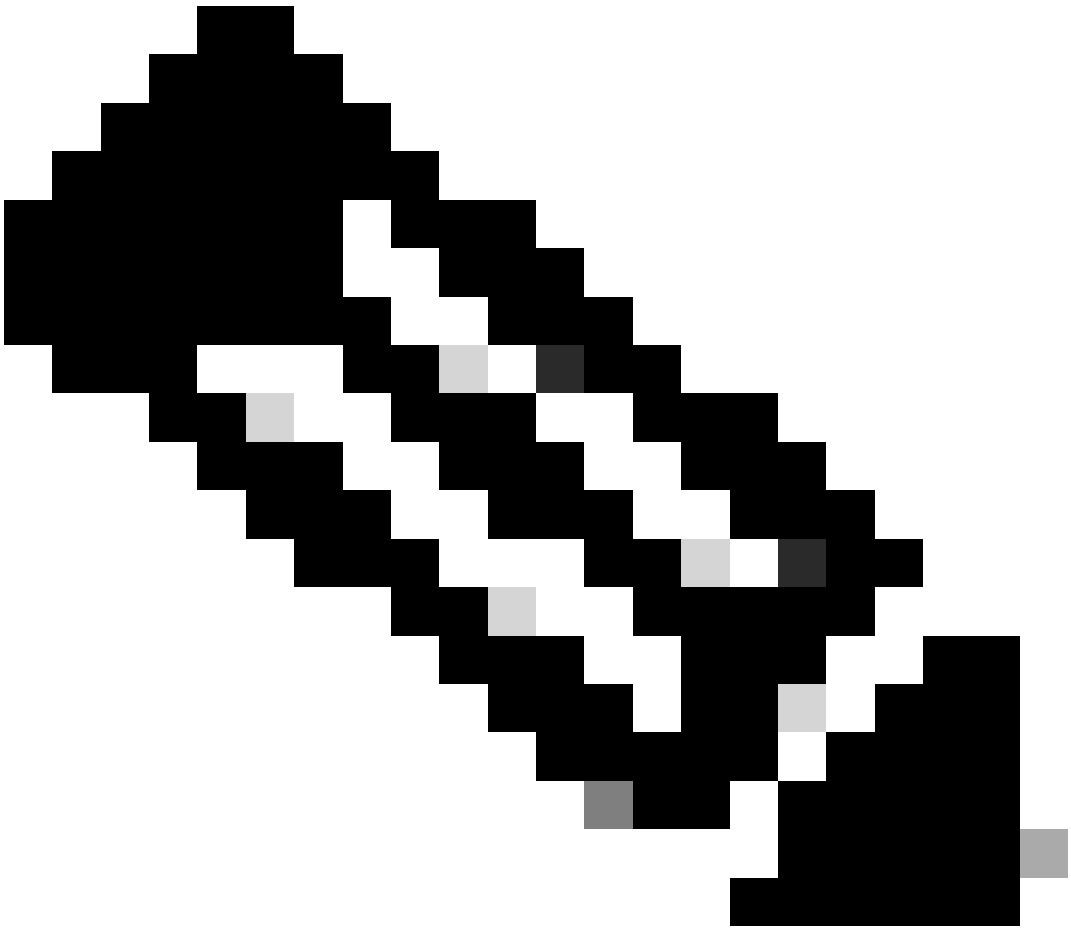
注：シグナリングパケットには送信元と宛先のIPアドレスが含まれ、RTPメディアストリームの送受信に関与する当事者の識別に役立ちます。

メディア

シグナリングが完了し、シグナリングコンポーネント（デバイスまたはサーバ）がメディアタイプについて合意すると、Real Time Protocol(RTP)が関与するすべての当事者にメディア（音声および/またはビデオ）の送信を開始します。

RTPは、ストリーミングメディアに使用されるインターネットプロトコルで、コールが確立された後にのみ送信され、ユーザデータグラムプロトコル(UDP)上で実行されます。

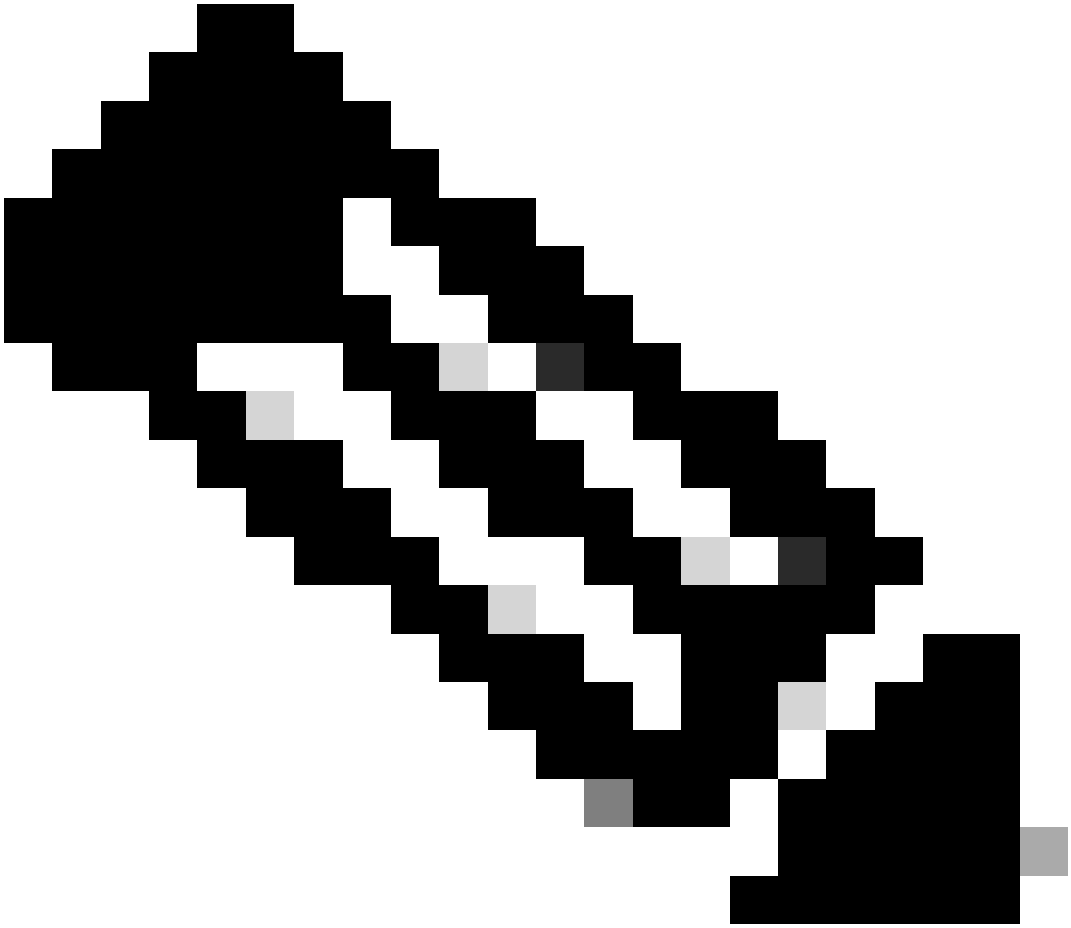




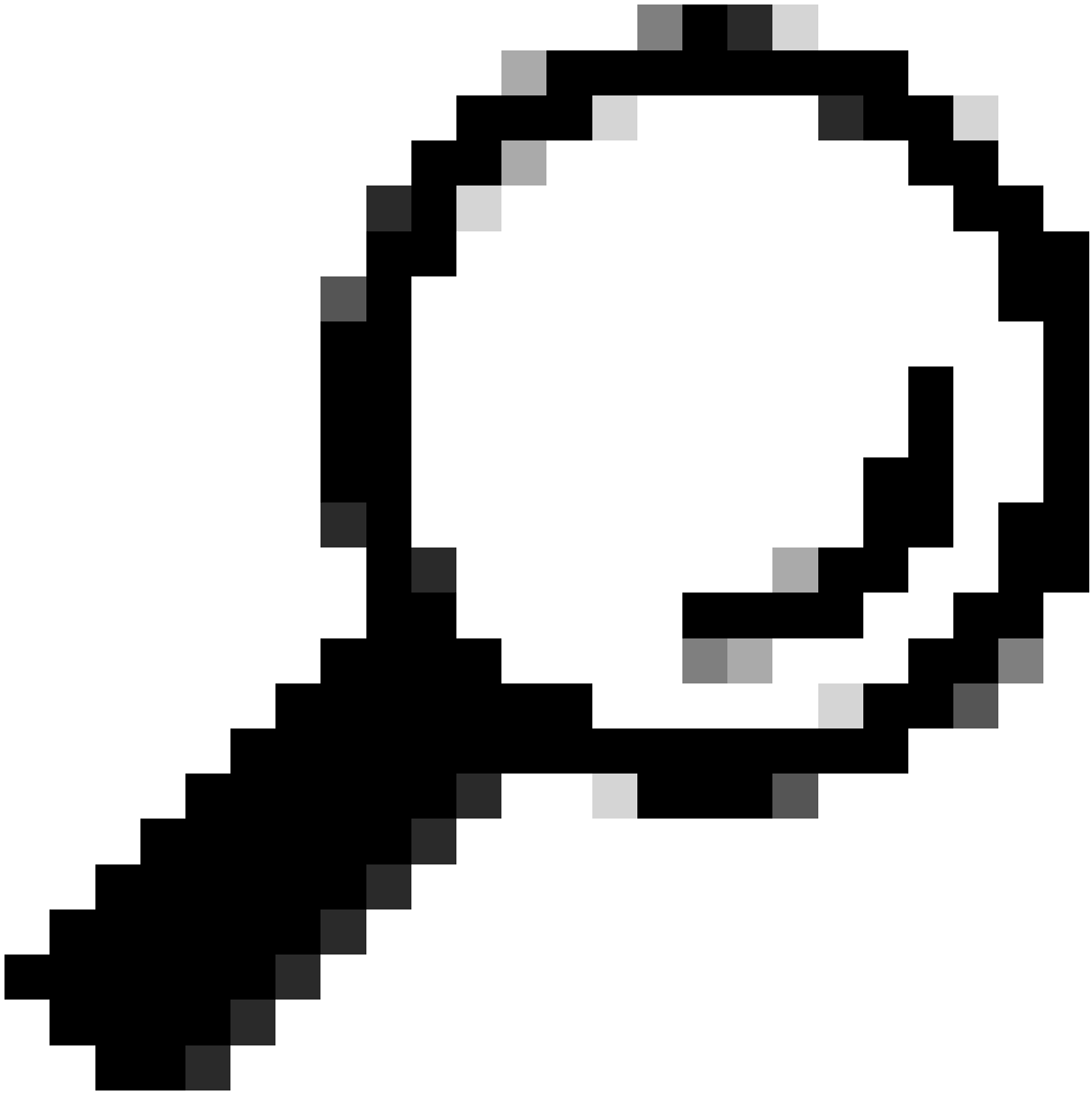
注：メディアは、音声またはビデオ、あるいはその両方で、RTPパケットを使用して伝送されます。

シグナリングコンポーネント（デバイスまたはサーバ）は、メディア（音声および/またはビデオ）の送受信に使用されるポートを決定します。 RTPの最も一般的なポート範囲は、ほとんどのデ

バイスで通常16384 ~ 32767です。



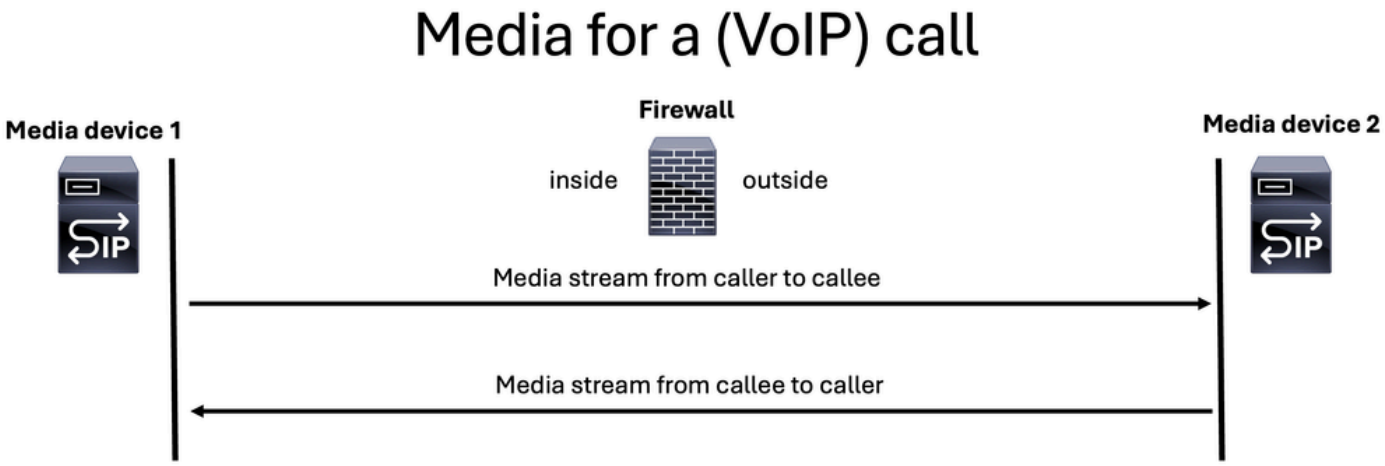
注:ASRやISR G3プラットフォーム（ISR4Kプラットフォームなど）などの特定のシスコデバイスでは、標準化されたRTPポート範囲である8000 ~ 48200が使用されています。デバイスに設定されている特定のRTPポート範囲は、これらの標準化された値と異なる場合があり、サードパーティ製デバイスによって異なる場合があるため、確認することが重要です。

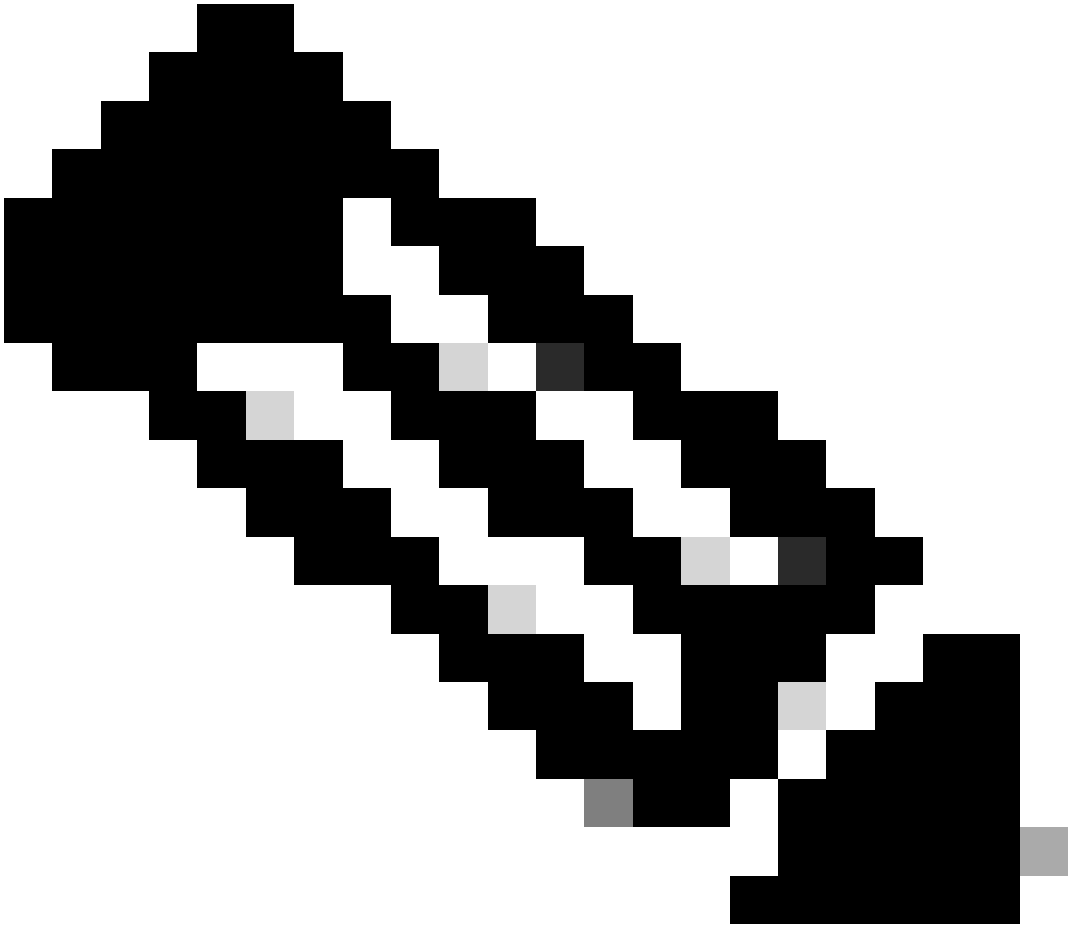


ヒント:RTPパスがシグナリングパスと異なる場合があるため、音声RTPパケットの送受信を担当するデバイスを特定することが重要です。これにより、ASAまたはFTDを通過するデバイス間のUDPトラフィックを確実にキャプチャできます。

通常の音声コールで生成される2つのメディアストリームまたはRTPストリームがあります。

1. 発信者から着信者への1つのメディアストリーム
2. 着信側から発信側への1つのメディアストリーム





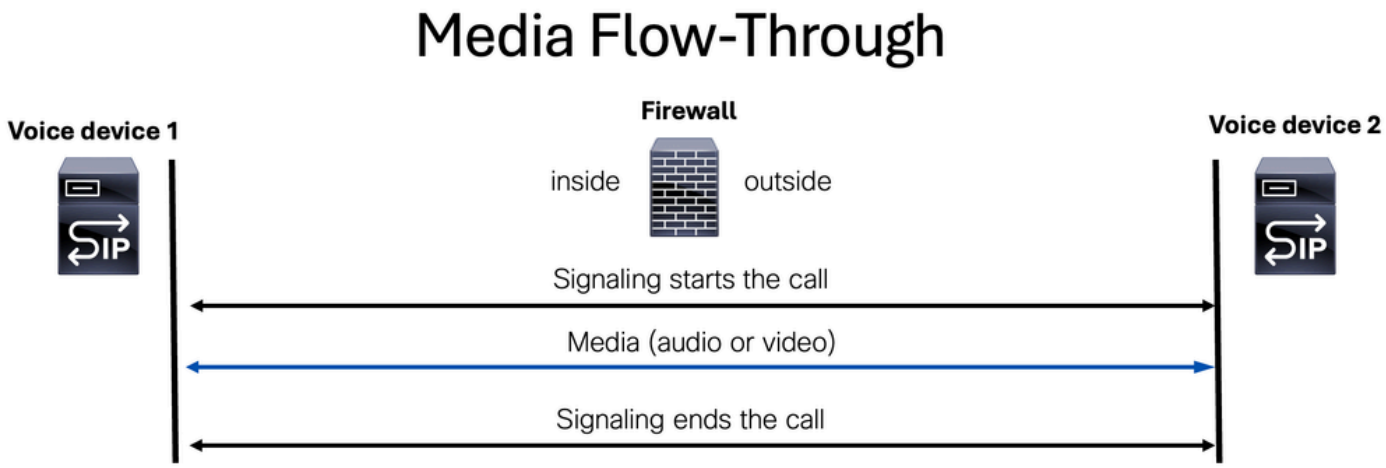
注：説明の便宜上、SIPサーバアイコンはすべてのイメージでシグナリングサーバまたはメディアサーバのいずれかを表すために使用されます。

音声通話のメディアストリーミングについて説明する際は、次の2つの主要なシナリオを強調することが重要です。

1. メディアフロースルー
2. メディアフローアラウンド

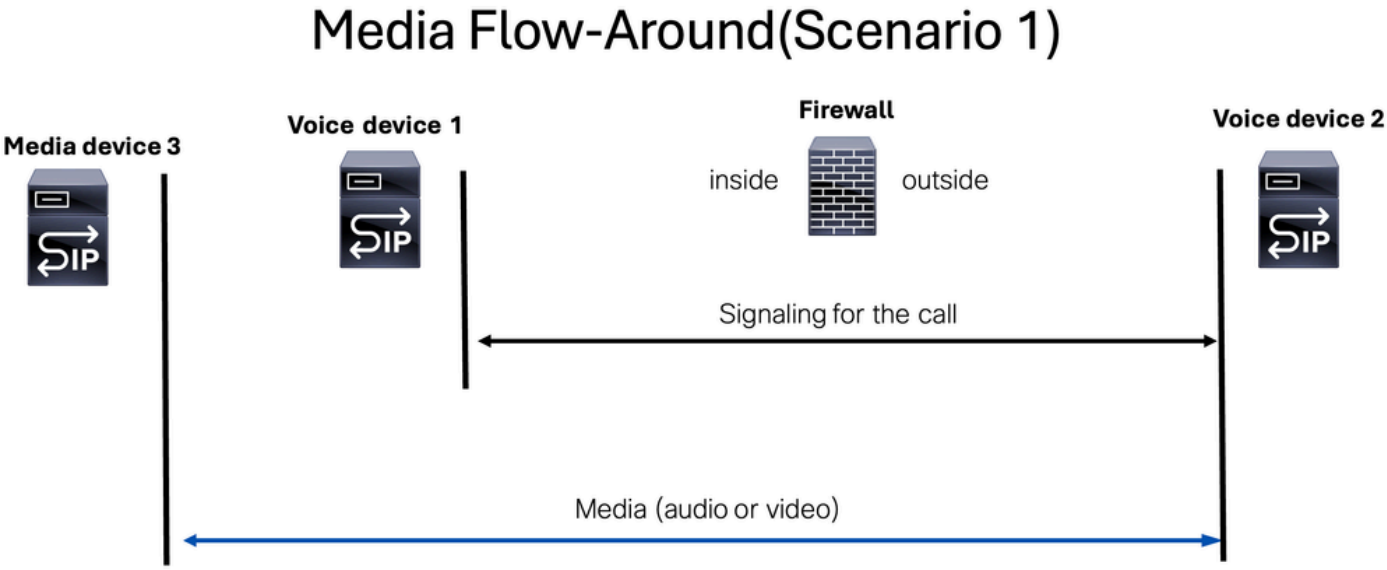
メディアフロースルー

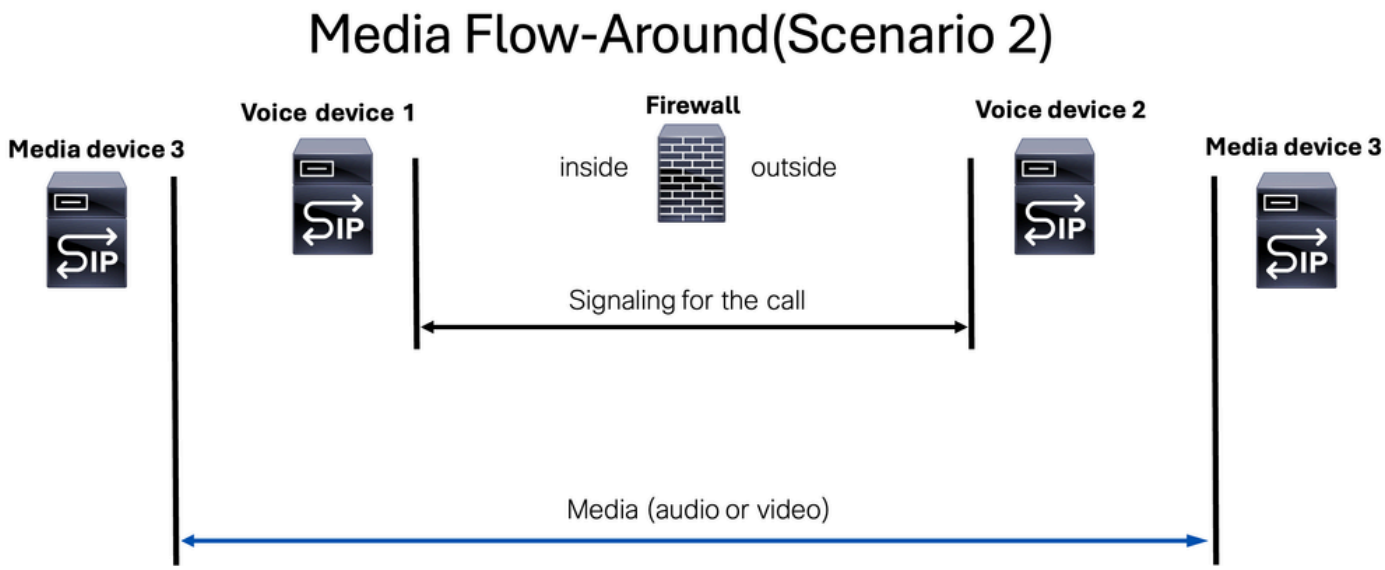
メディアフロースルーは、メディア（音声やビデオ）とシグナリングパケットの両方が同じデバイスで処理されるモードです。



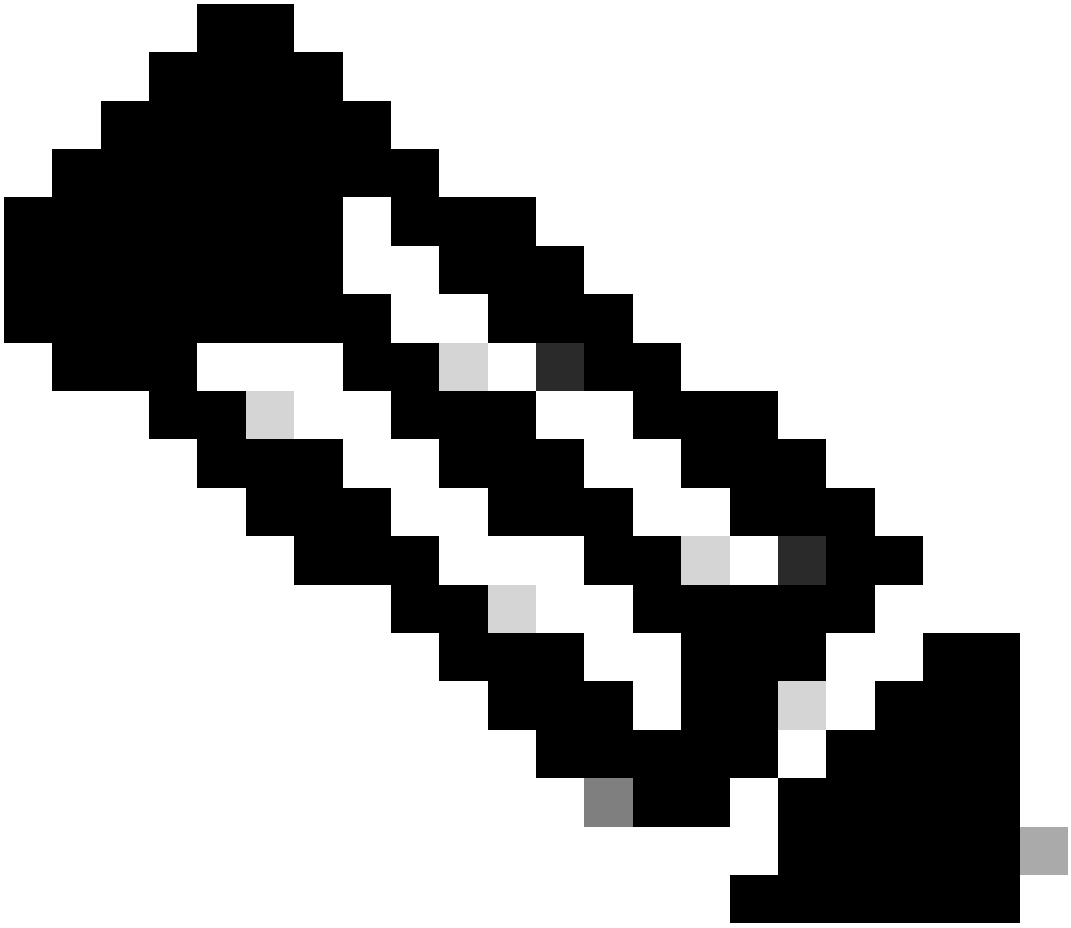
メディアフローアラウンド

メディアストリームのフローアラウンドとは、シグナリングパケットが2つの個別のシグナリングコンポーネント（デバイスまたはサーバ）で処理され、メディアストリーム（音声またはビデオ）がメディアデバイスと呼ばれる3番目のデバイスで管理されるモードです。





このモードでは、関係するデバイスの役割と、シグナリングとメディアストリームまたはデバイスの違いを明確にします。



注：これは、作成されたアクセスリストのトラブルシューティングを行う際に特に重要です。このアクセスリストによって、シグナリングコンポーネント（デバイスまたはサーバ）が許可される可能性がありますが、メディアストリームで別のメディアデバイスが使用されている場合は、FWデバイスのアクセスリストでこのアクセスリストを許可する必要があります。

Session Initiation Protocol（SIP）

SIPは、RFC 3261のInternet Engineering Task Force（IETF；インターネット技術特別調査委員会）によって定義されたアプリケーションレイヤ制御プロトコルです。

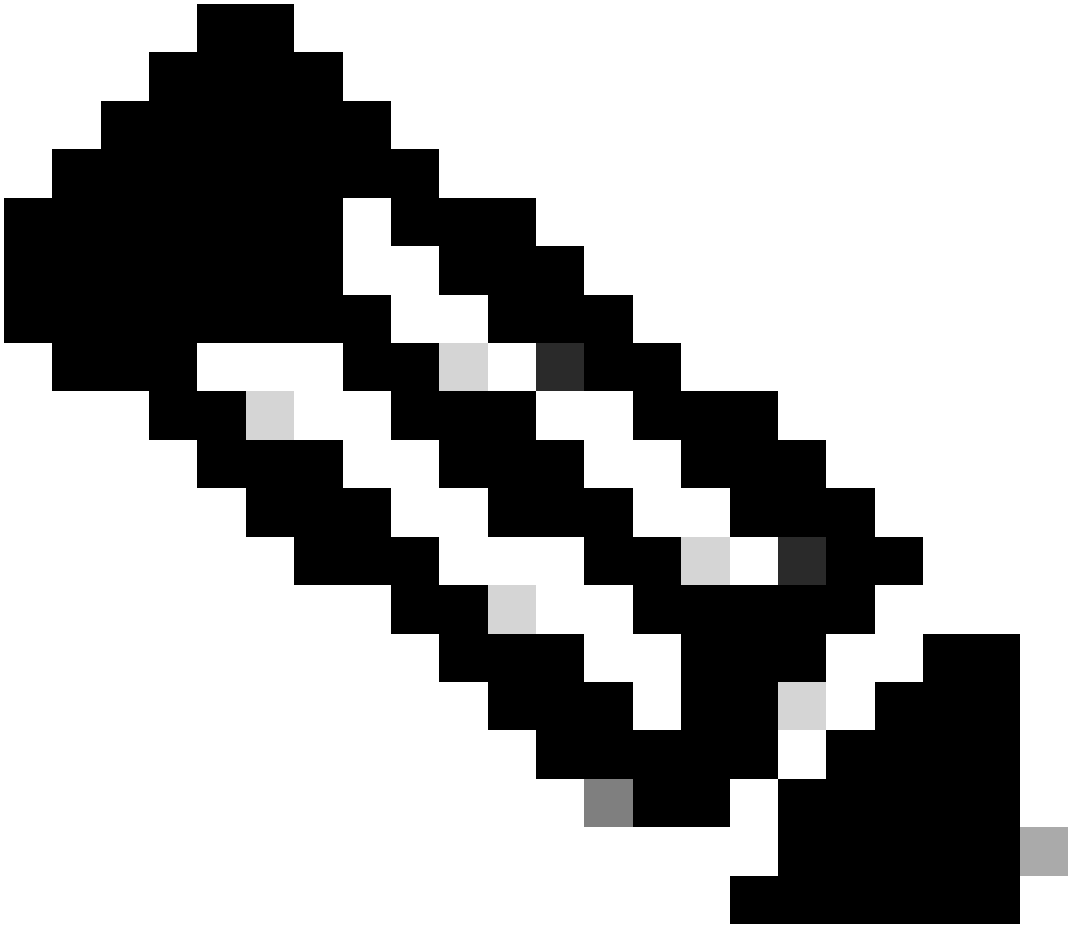
SIPはテキストベースのプロトコルです。つまり、SIPメッセージは、HTTPの動作と同様に、人間が判読できるテキストで構成されます。

SIP はシグナリングとセッション管理の機能をパケット テレフォニー ネットワークの内部で処理するように設計されています。

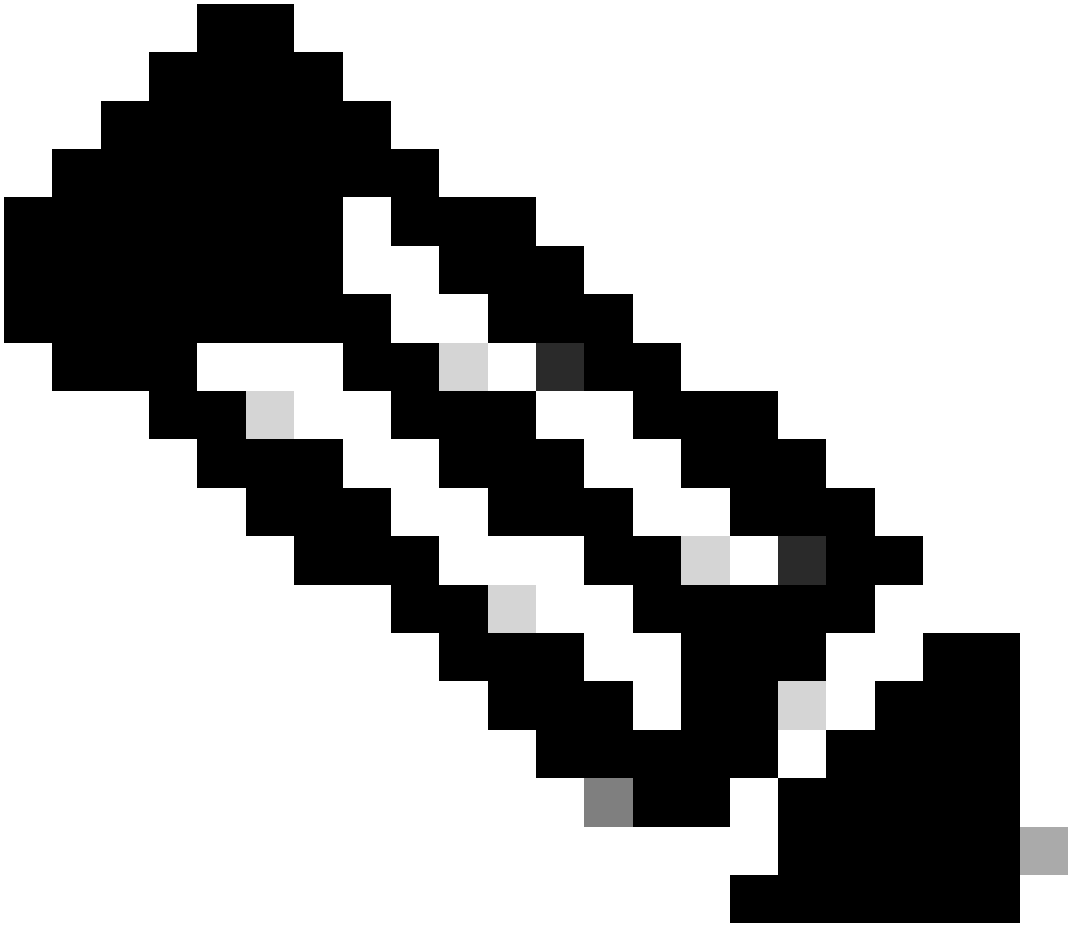
SIPで可能なこと：

- コールを作成する
- コールの変更
- コールを終了する

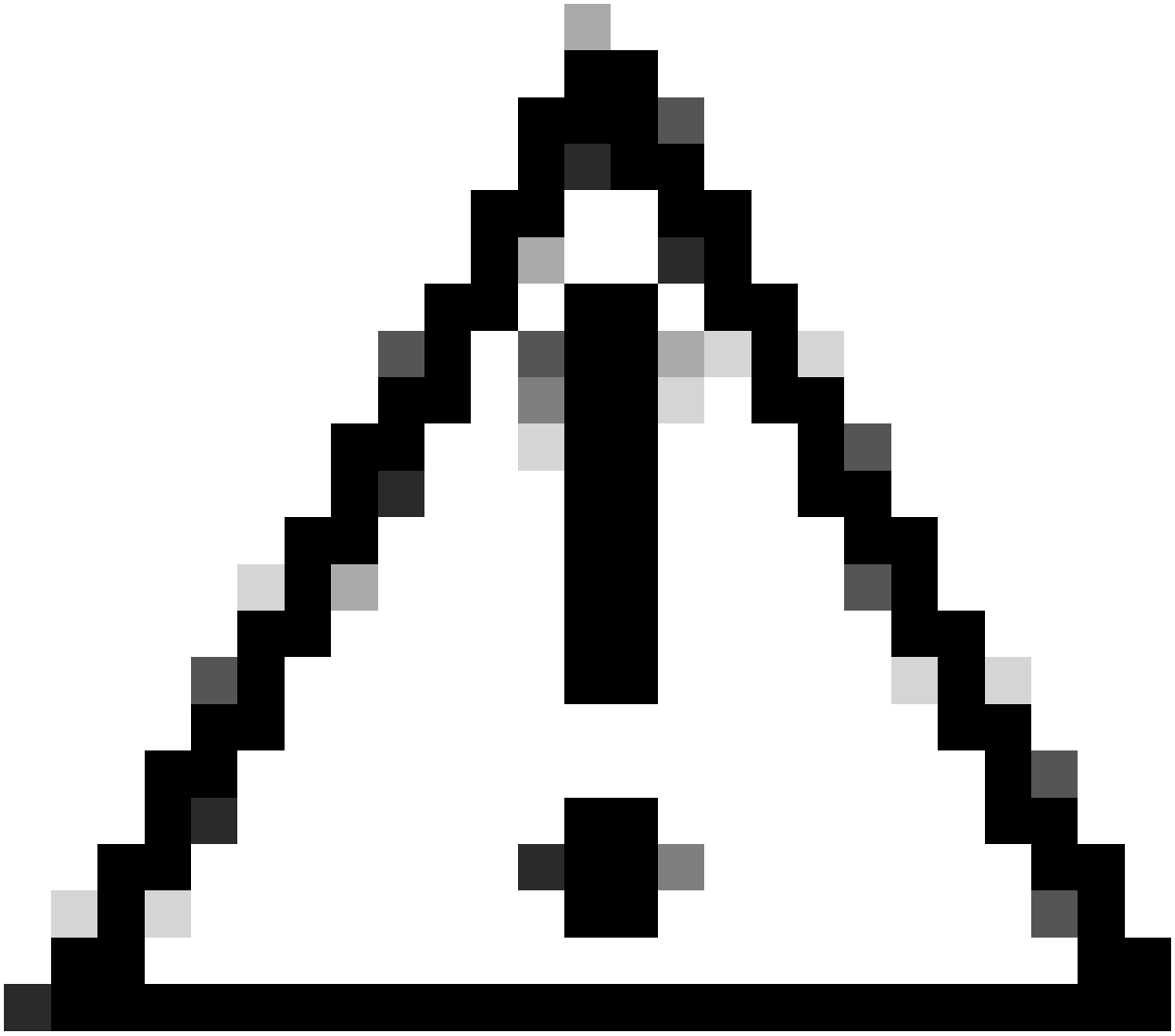
SIPは、標準化されたポート5060でUDPまたはTCPのいずれかを使用できます。また、SIPがTransport Layer Security(TLS)を使用して暗号化されている場合、標準化されたポート5061を使用できます。



注:SIPシグナリングが暗号化されている場合、実際のSIPパケットはASAまたはFTDデバイスのパケットキャプチャに表示されません。ただし、SIPクライアントとSIPサーバデバイスの間で、TCPハンドシェイクとそれに続くTLSハンドシェイクは引き続き監視できます。



注:SIPインスペクションは、Cisco Secure Firewall Threat Defense(FTD)およびSecure Firewall Adaptive Security Appliance(ASA)ではデフォルトで有効になっています。



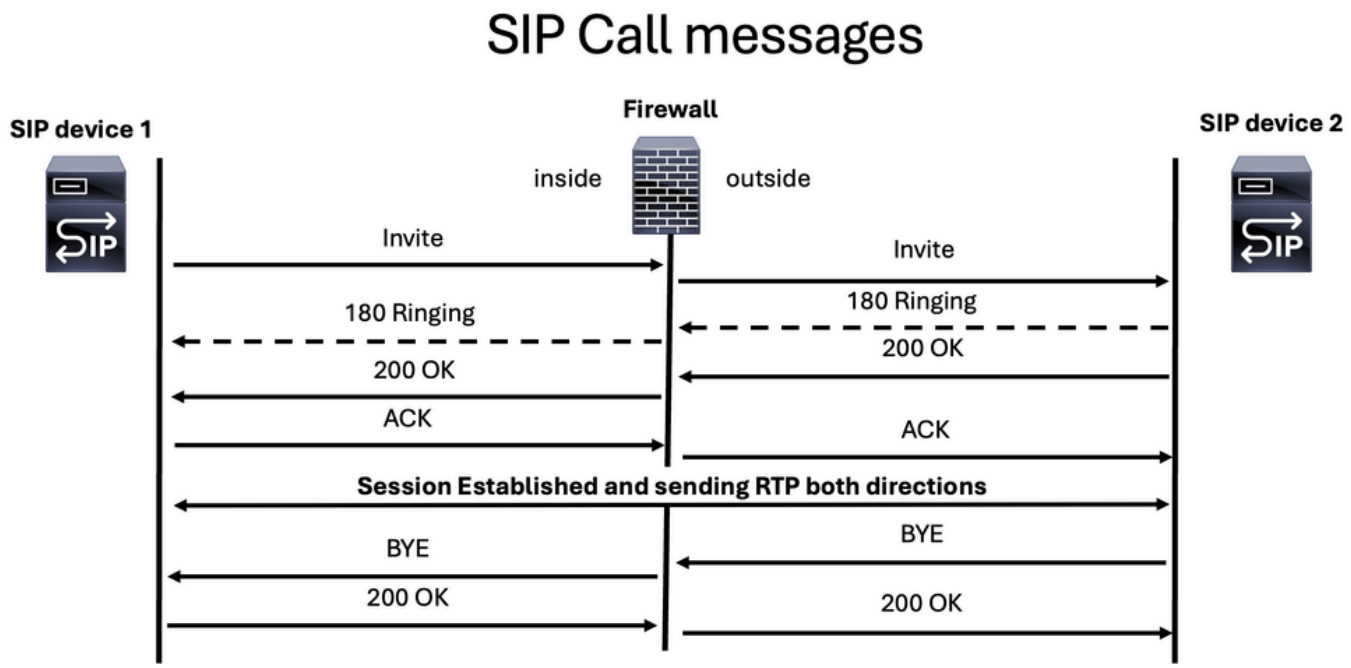
注意：シグナリングに使用されるポートを必ず確認してください。SIPプロトコルは一般にポート5060または5061を使用しますが、一部の導入はこれらの標準から逸脱し、SIPプロトコルに異なるポートを使用する可能性があることに注意してください。

SIPシグナリングの問題のトラブルシューティングには、次の3つのシナリオがあります。

- SIPコールシグナリングメッセージ
- SIPオプションメッセージ
- SIP REGISTERメッセージ

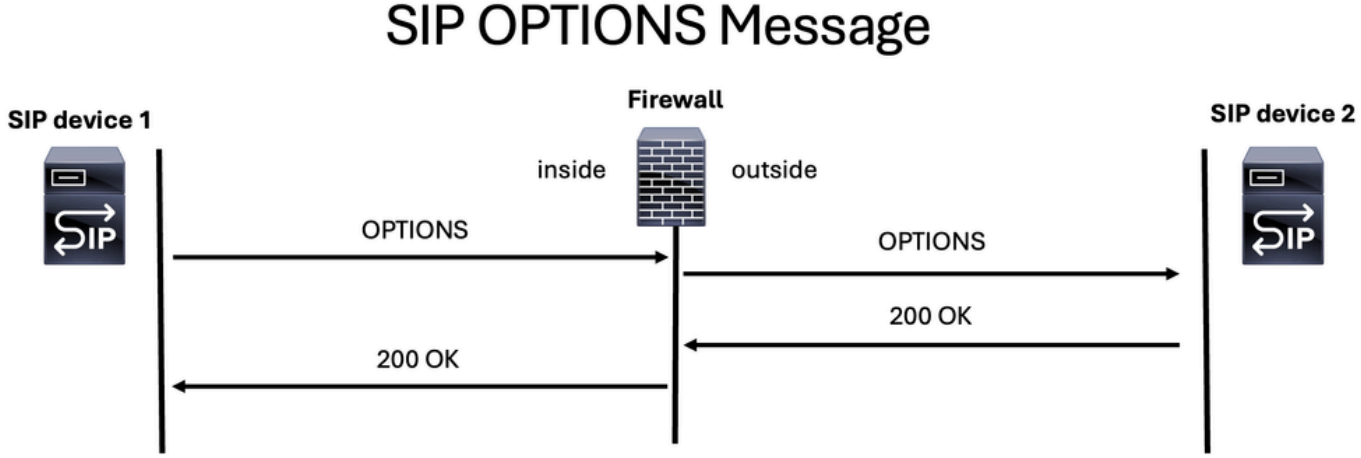
SIPコールメッセージ

音声コールを確立および終了するための主なSIPメッセージは次のとおりです。



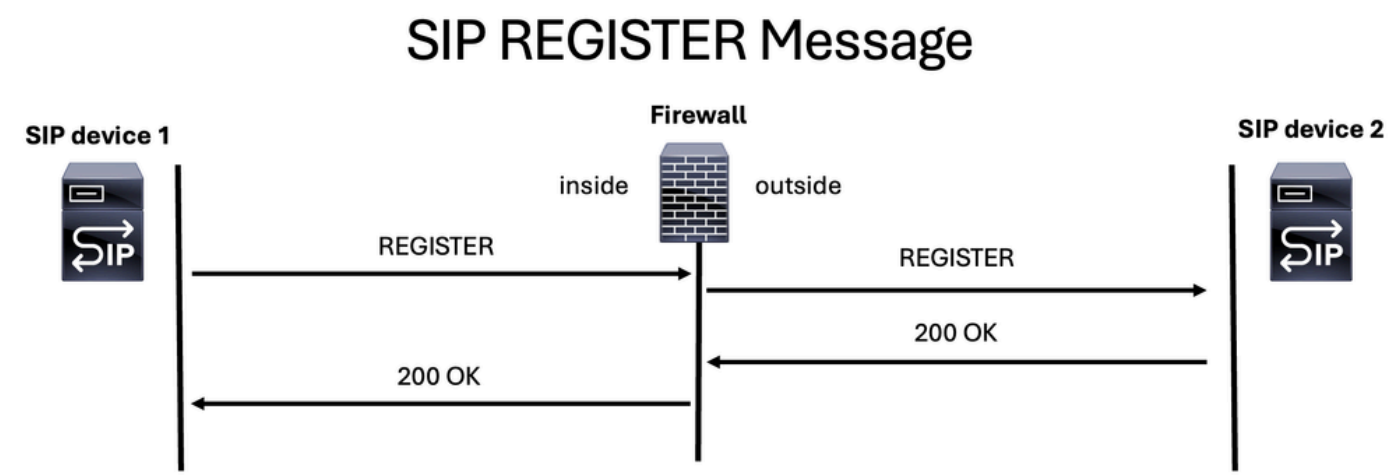
SIPオプションメッセージ

SIP OPTIONSメッセージは、SIPデバイスがオンラインであり、応答できるかどうかを判断するために重要です。これはping ICMPメッセージに似ていますが、SIPでは異なります。

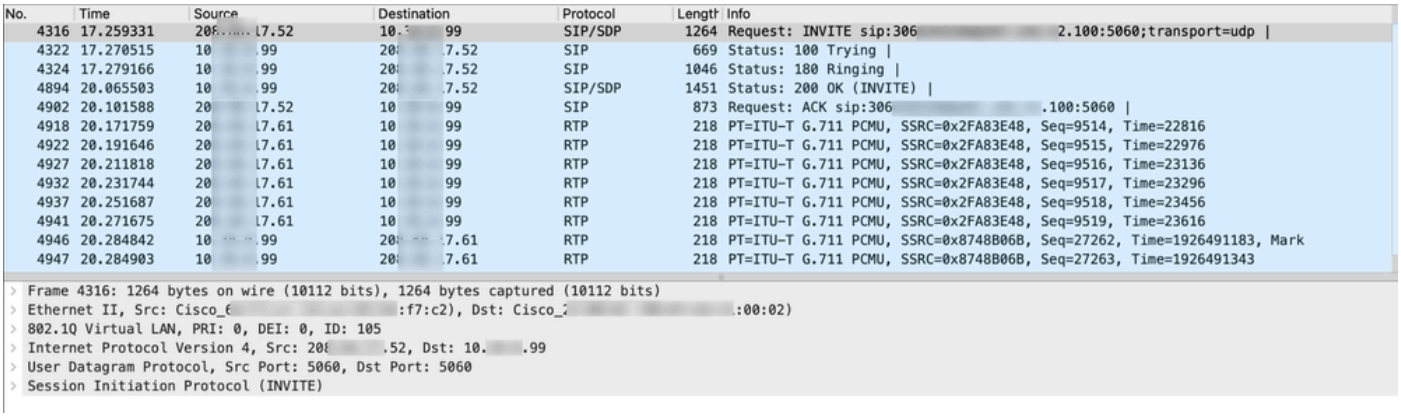


SIP REGISTERメッセージ

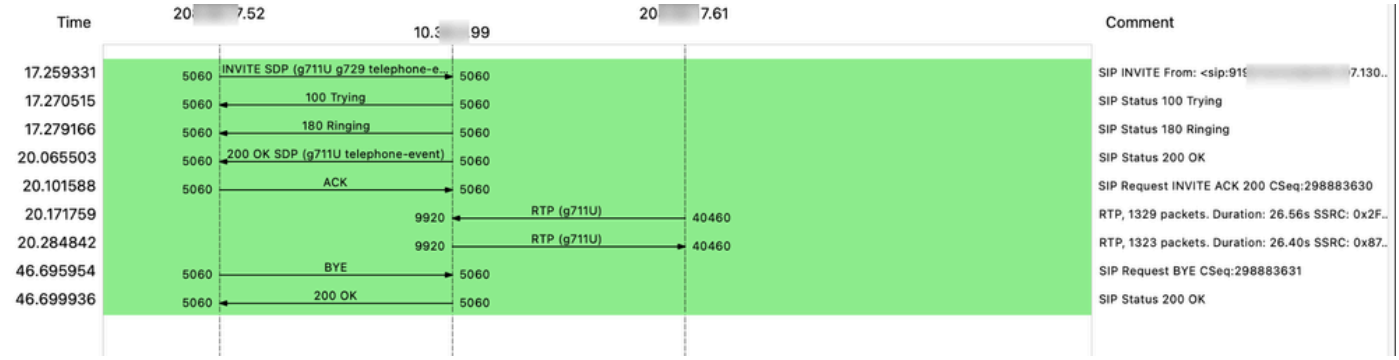
ファイアウォールのトラブルシューティングセッションで検出できるもう1つのSIPメッセージは、SIP REGISTERメッセージです。このメッセージを使用すると、デバイスをSIPサーバに登録できます。



次のパケットキャプチャは、2台のSIPデバイスからの要求と応答、およびメディア（音声）トラフィックを示しています。

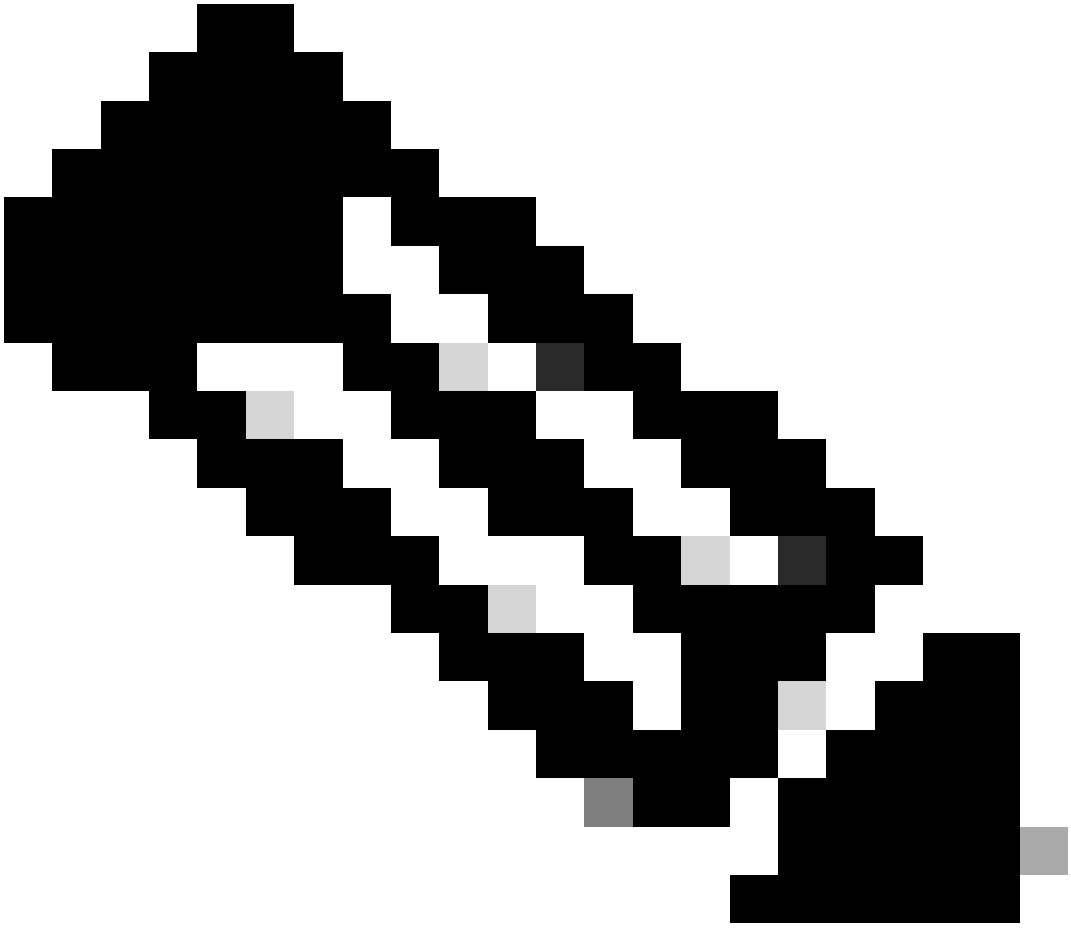


SIPシグナリング（シグナリング）とRTPメディア（音声）の両方のフローの例を次に示します。



セッション記述プロトコル（SDP）

セッション記述プロトコル(SDP)は、マルチメディアセッションのメディアストリームを記述するために使用される標準的な表現です。メディア自体は伝送されませんが、エンドポイント間でメディアのタイプと形式をネゴシエートするために使用されます。SDPは、セッションのメディア特性を管理およびネゴシエートするために、セッション開始プロトコル(SIP)とともに使用されます。

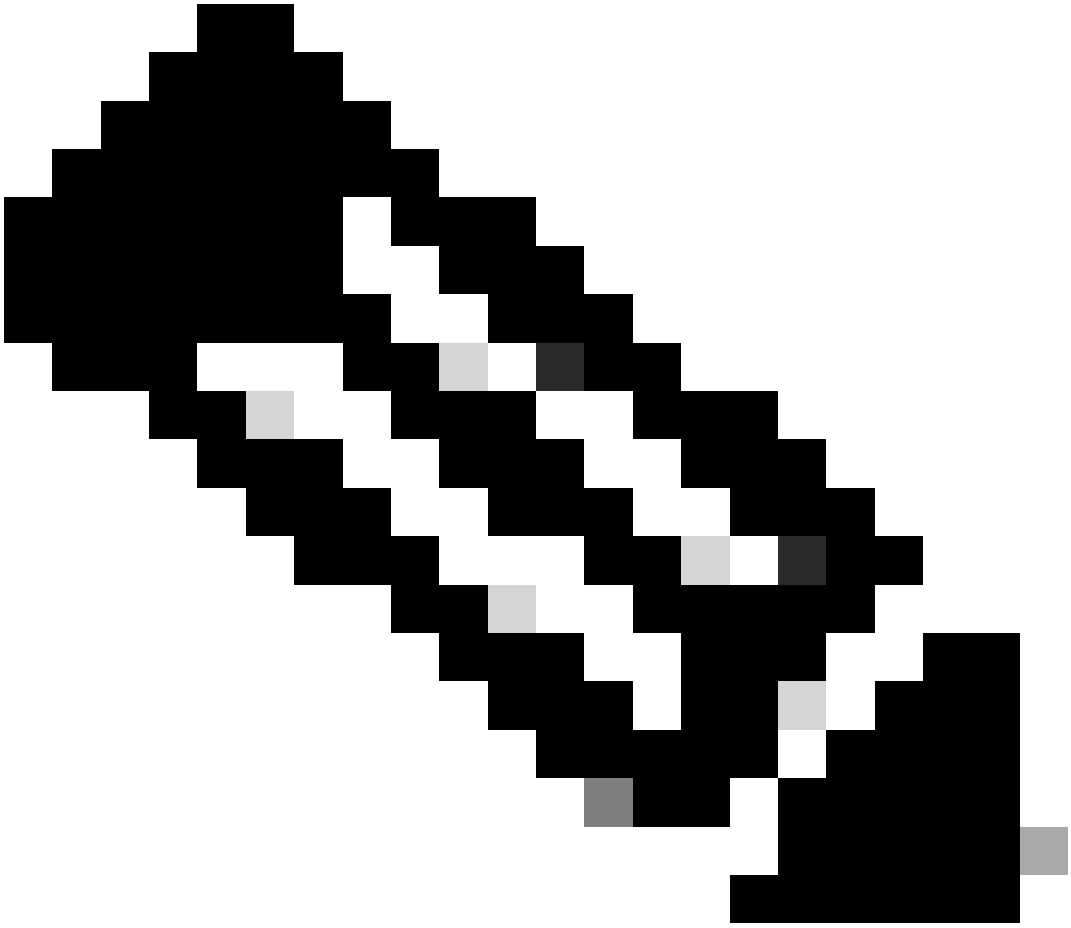


注:MGCPには、同じ目的で使用されるSDPの概念が組み込まれています。

SIPプロトコル内のSDPメッセージの例を次に示します。

```
INVITE sip:2003@192.168.245.9:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.245.6:5060;branch=z9hGXXX5763
Remote-Party-ID:



       ;party=calling;screen=no;privacy=off
From:



        ;tag=4E3XXXC-A9F
To:
```

```
Date: Thu, 17 Aug 2025 13:48:52 GMT
Call-ID: 2A7BE22B-XXXXXXXXX-XXXXXXXXX-F940DC75@192.168.245.6
Supported: 100rel,timer,resource-priority,replaces,sdp-anat
Min-SE:  1800
Cisco-Guid: 0350227076-XXXXXXXXX-XXXXXXXXX-1670485135
User-Agent: Cisco-SIPGateway/IOS-15.5.3.S4b
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
CSeq: 101 INVITE
Timestamp: 150299CC32
Contact:



Expires: 180
Allow-Events: telephone-event
Max-Forwards: 69
Content-Type: application/sdp    <========Session Description Protocol message start
Content-Disposition: session;handling=required
Content-Length: 266

v=0
o=CiscoSystemsSIP-GW-UserAgent 7317 4642 IN IP4 192.168.245.6
s=SIP Call
c=IN IP4 192.168.245.6
t=0 0
m=audio 8266 RTP/AVP 18 127
c=IN IP4 192.168.245.6
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:127 telephone-event/8000
a=fmtp:127 0-16
a=ptime:20
```



注：一部のSDPメッセージの例には、次のパラメータが含まれています。

++c-IN IP4：メディアサーバのIPアドレス

++m=audio：メディアタイプがオーディオであることを示します。

++8266：これは、オーディオストリームが送信されるポート番号です。

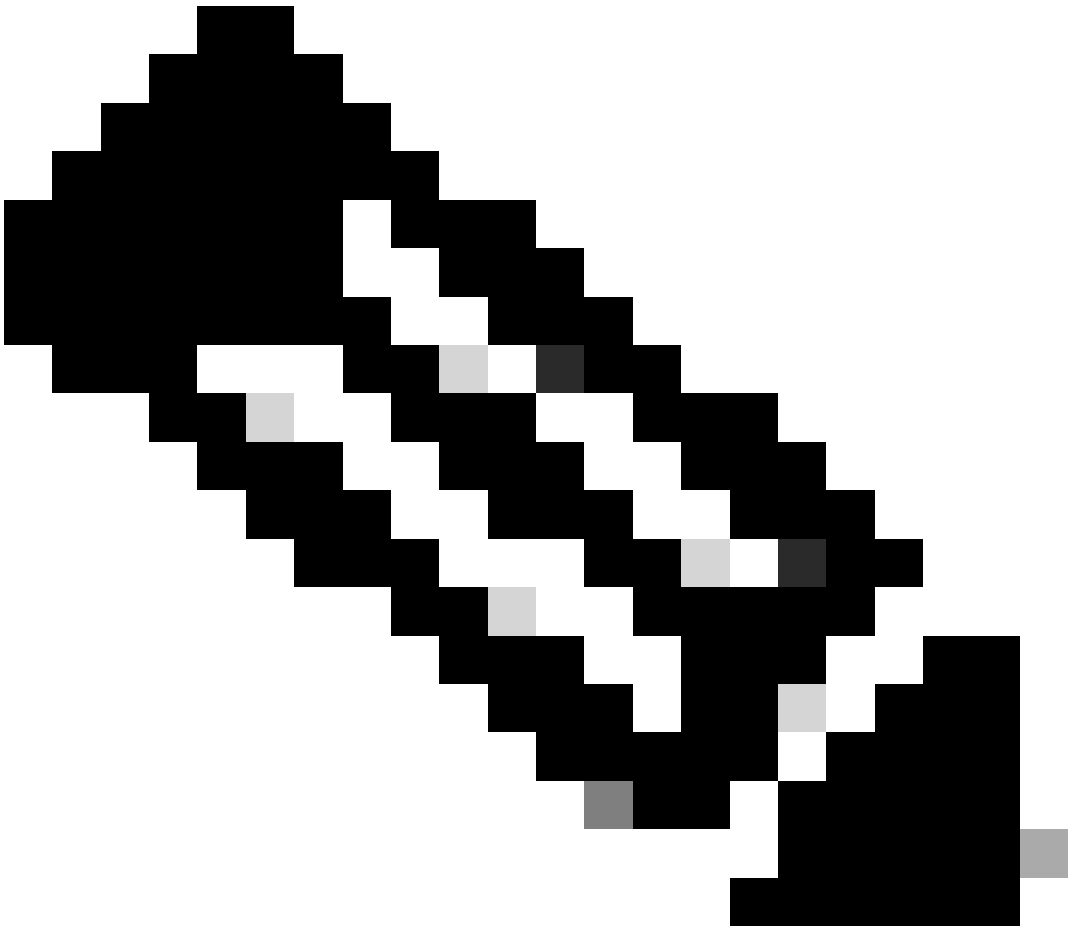
++RTP/AVP：トランスポートプロトコルを指定します。これは、音声/ビデオプロファイル(AVP)を使用するRTPです。

++18 127：これらは、オーディオコーデックのペイロードタイプです。ペイロードタイプ18は通常G.729コーデックに対応し、127はエンドポイント間のネゴシエーションに従ってコーデックに割り当てることができる動的ペイロードタイプです。

Session Description Protocol(SDP)は、INVITE、183 Session in Progress、200 OK、ACKなどの複数のSIPメッセージ内にあります。 SDPは、通話者間で音声やビデオの機能を交換するための応答方式として機能します。コールの問題をトラブルシューティングする際には、次の3つの主要

な概念を理解することが重要です。

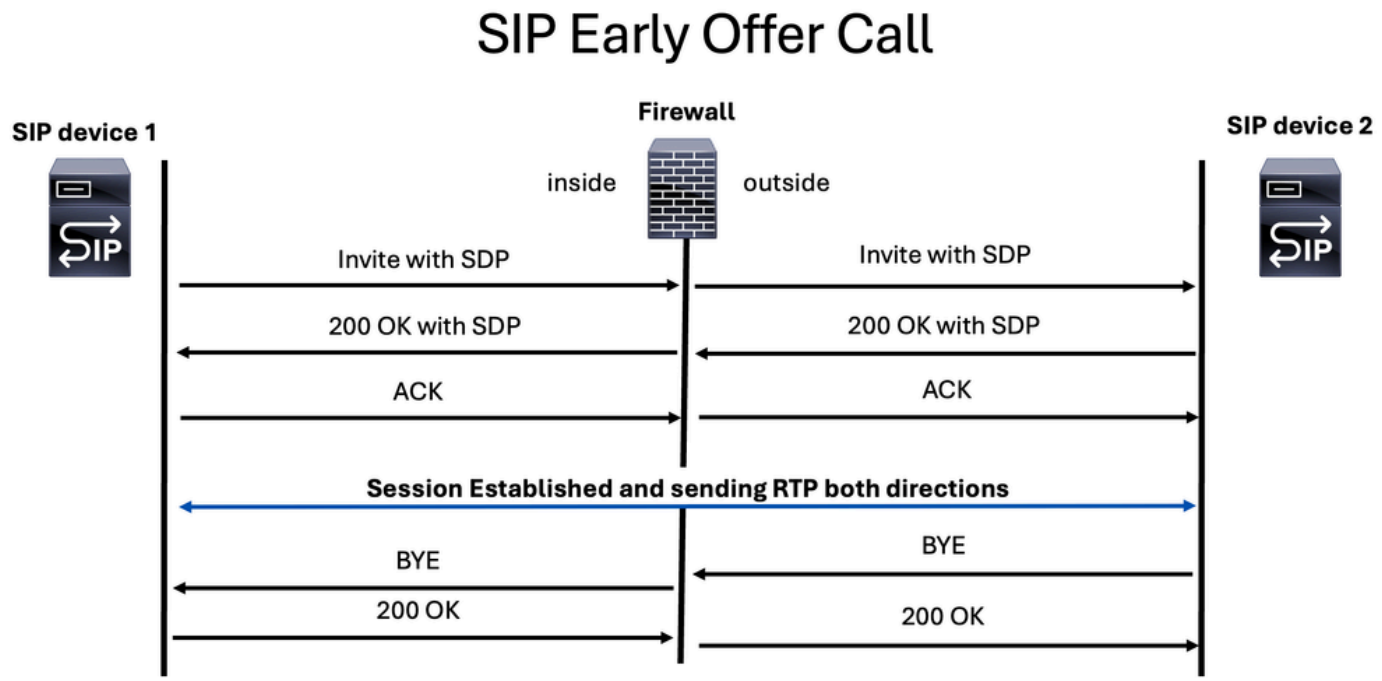
1. 早期オファー
2. 遅延オファー
3. 初期メディア



注：ファイアウォールのインスペクション機能はSIPヘッダー内だけでなくSDPセクション内のIPアドレスを変更できるため、SDPメッセージの宛先を理解することが重要です。

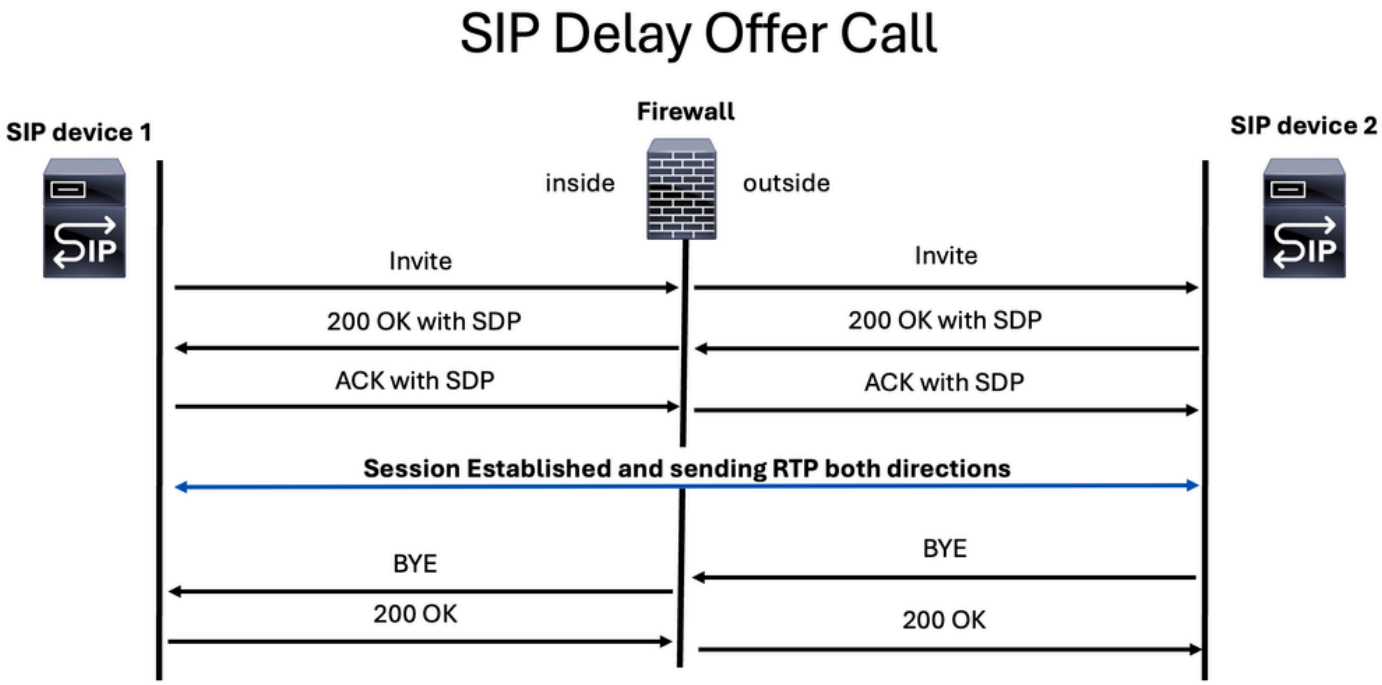
早期オファー

ここでは、SDPのメディアパラメータはINVITEメッセージおよび200 OK SIPメッセージ内にあります。



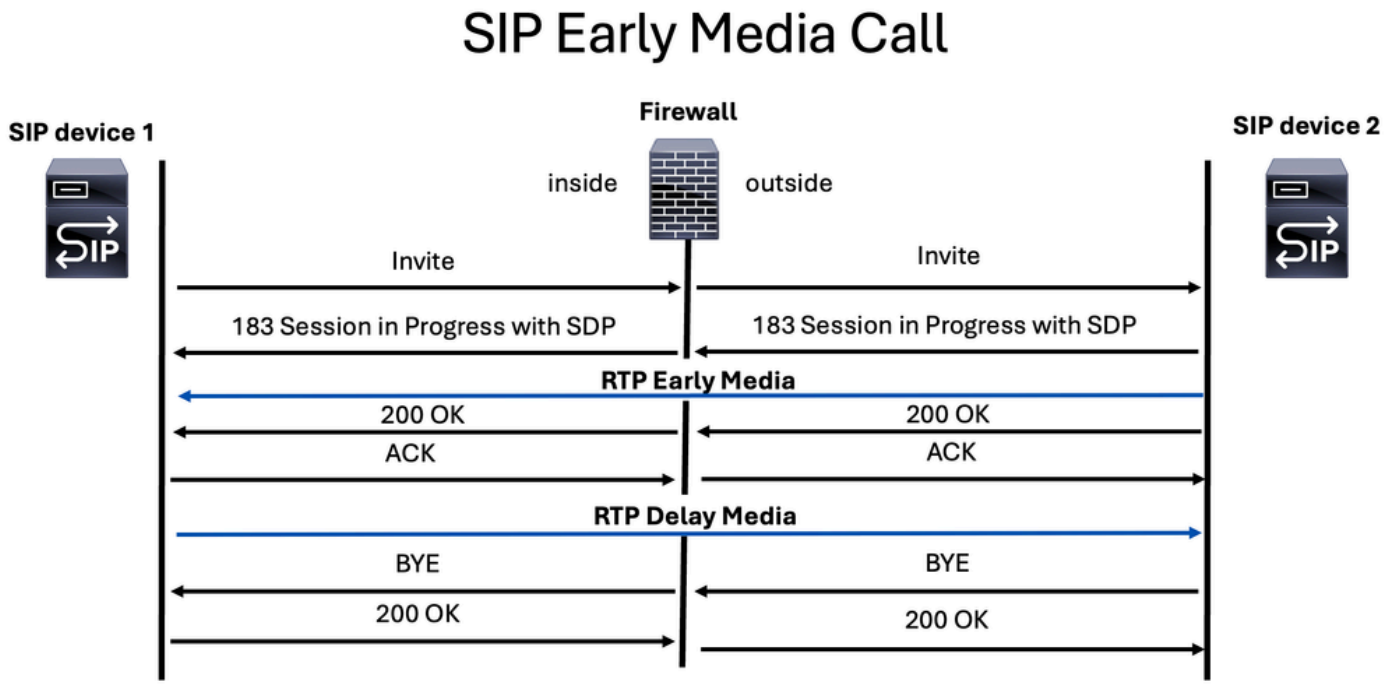
遅延オファー

この方式では、SDPは200 OKおよびACK SIPメッセージで検出されます。



初期メディア

早期メディアは、183 Session Progress応答と呼ばれる特定のSIPメッセージを介して送信されます。このメッセージには、着信側のメディアパラメータを含むSession Description Protocol（SDP；セッション記述プロトコル）が含まれています。一般に、コールが正式に接続される前に、自動ボイスメッセージまたはその他のメディアを発信者に送信するために、キャリアおよびSIPプロバイダーによって使用されます。

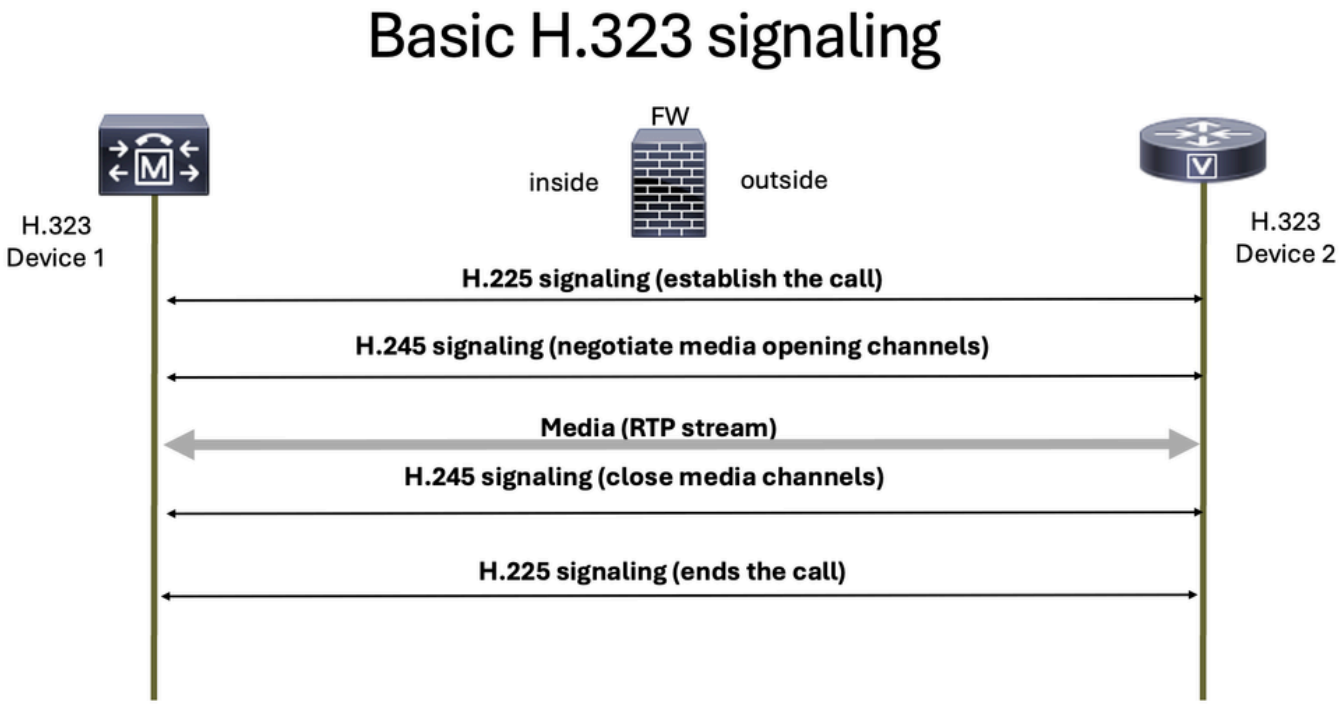


H.323

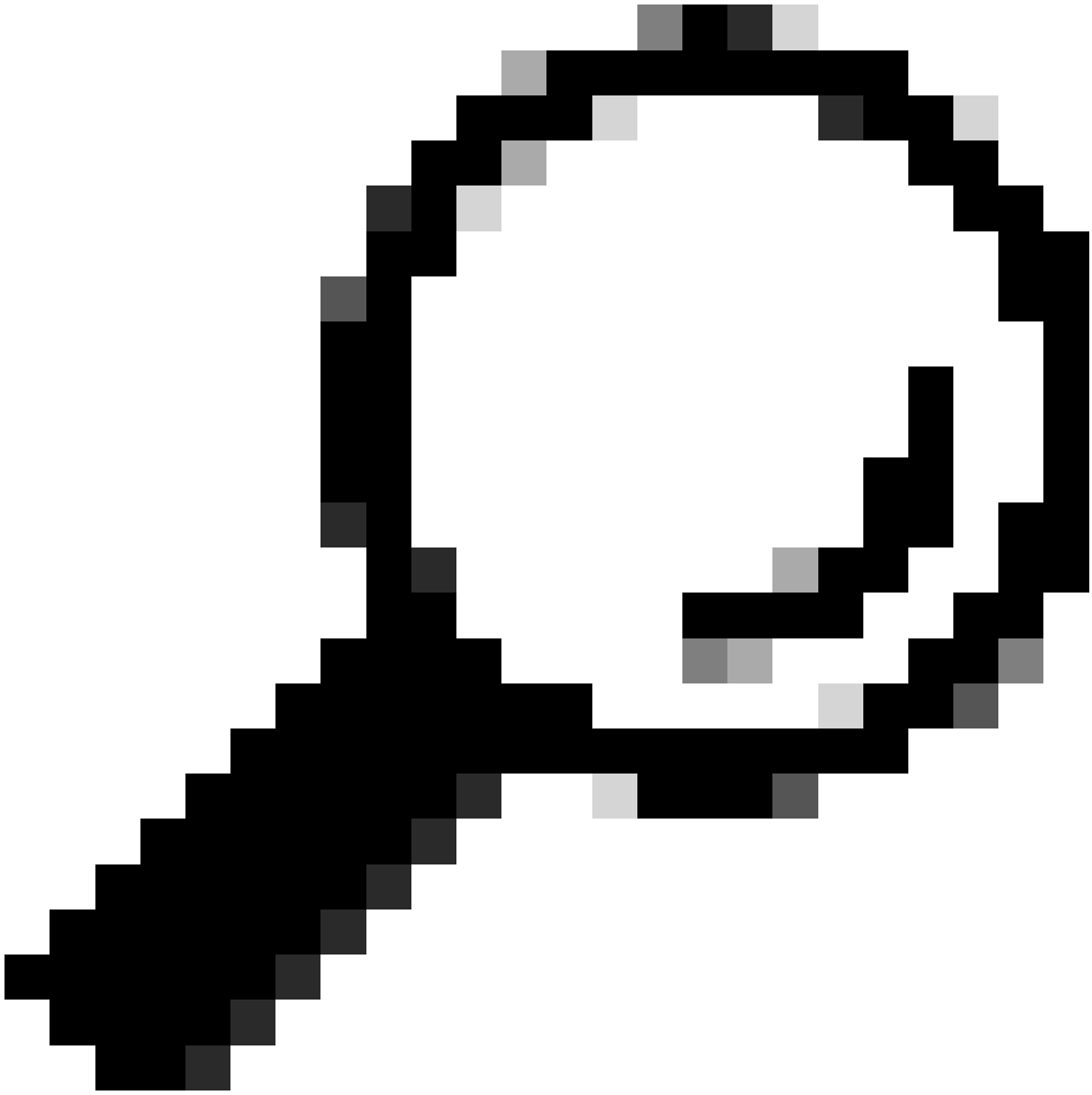
H.323は、インターネットなどのパケット交換ネットワークを介した音声、ビデオ、およびデータ通信用に、国際電気通信連合(ITU)によって定義されたプロトコルのセットです。

H.323プロトコルは、次の2つの主要なコンポーネントで構成されています。

1. H.225：コールの設定と終了を含む、コールシグナリングを処理します。
2. H.245：機能交換と、音声およびビデオのチャネルの開閉を行います。



H.323シグナリングプロトコルで使用されるポートは、1718、1719、および1720です。

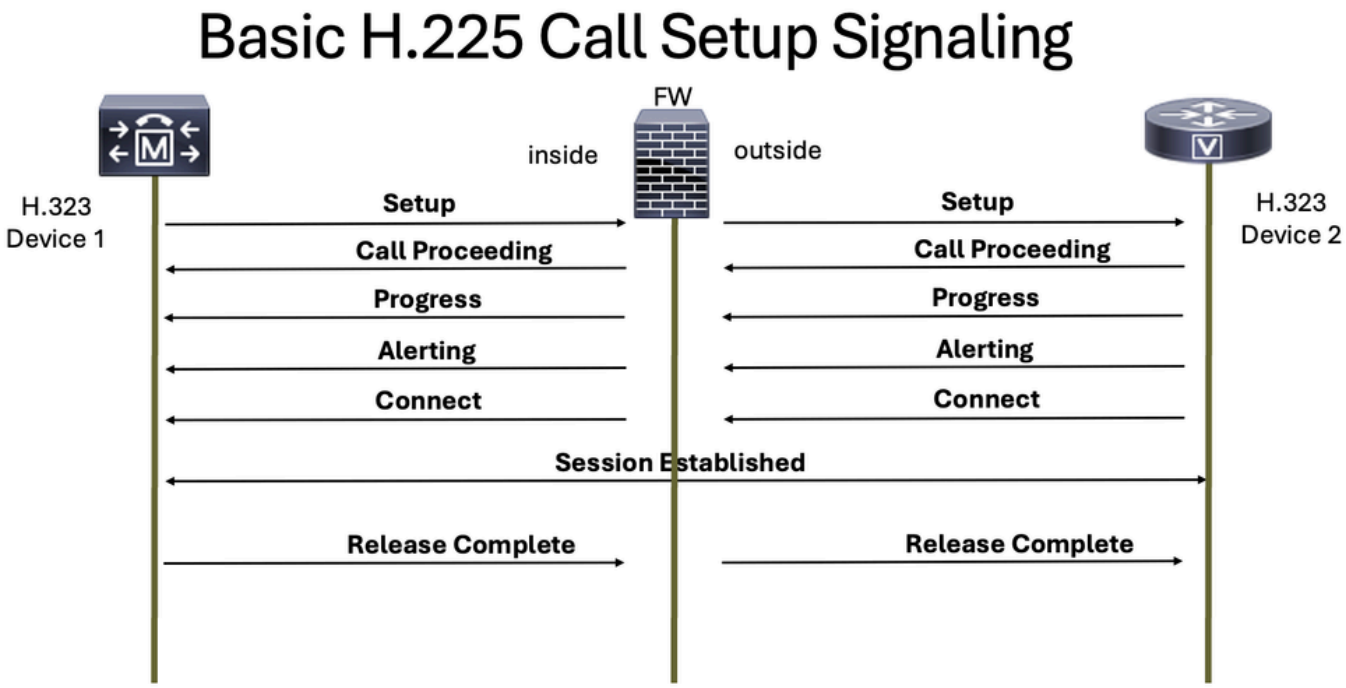


ヒント：安全なH.323プロトコル通信は、暗号化にTLSを使用するためにUDPからTCPへの切り替え時に問題が発生する可能性があり、ファイアウォールが疑わしいアクティビティとして接続を誤ってブロックする可能性があります。そのため、H.323エンドポイントまたはサーバのUDPトラフィックとTCPトラフィックの両方を許可するようにファイアウォールを設定することが重要です。

H.323は、スロースタートとファストスタートの2つの動作モードを持つプロトコルです。

H.225

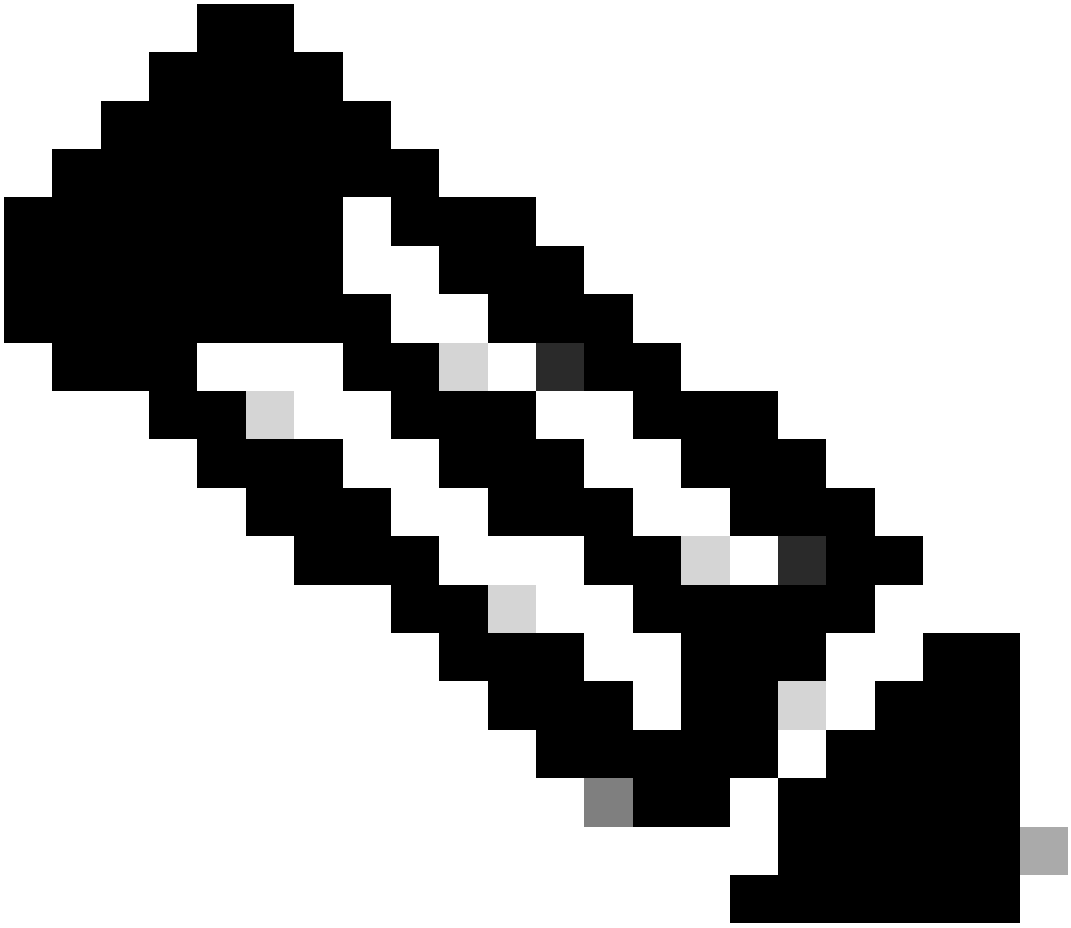
このプロトコルは、通話者のいずれかが電話を切ったときに、コールを設定し、音声コールを終了します。



H.245

H.245には次の機能があります。

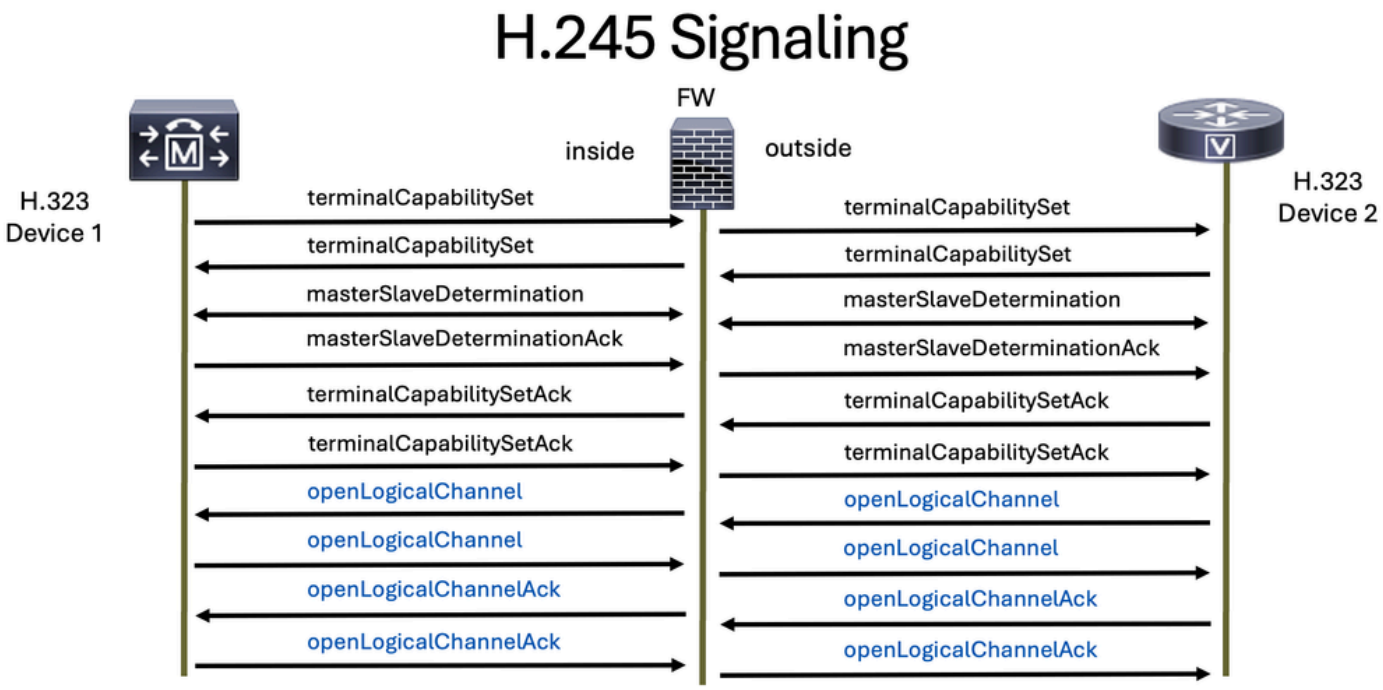
- 端末機能交換
- マスター/スレーブの決定
- 論理チャネルシグナリング



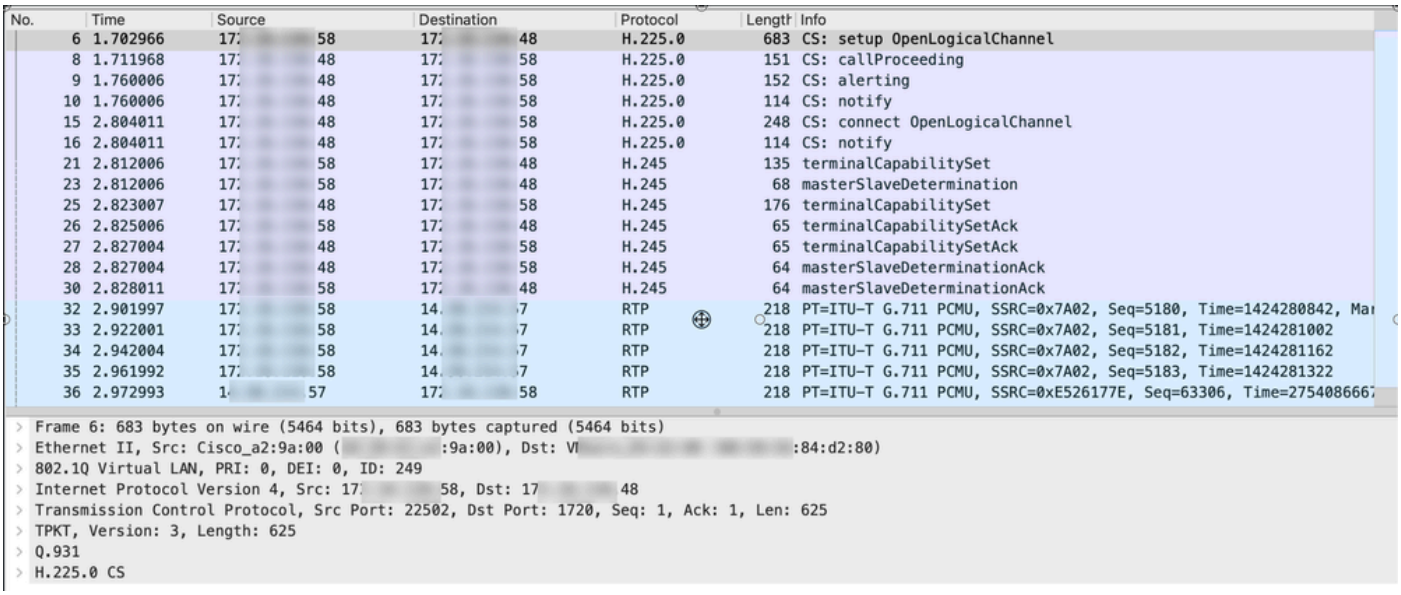
注：このドキュメントで使用されているマスターおよびスレーブという用語は、元のH.323プロトコルにハードコードされており、当社のポリシーまたは値を反映したものではありません。我々は，包摂的で丁寧な言葉を促進することにコミットしている。

H.245プロトコルは、H.225接続メッセージの受信後に送信されます。

このプロトコルは、RTPに使用される音声プロトコルの決定に役立ちます。このプロトコルは、論理チャネルを開始し、その論理チャネルのメッセージを閉じる際に指定されます。



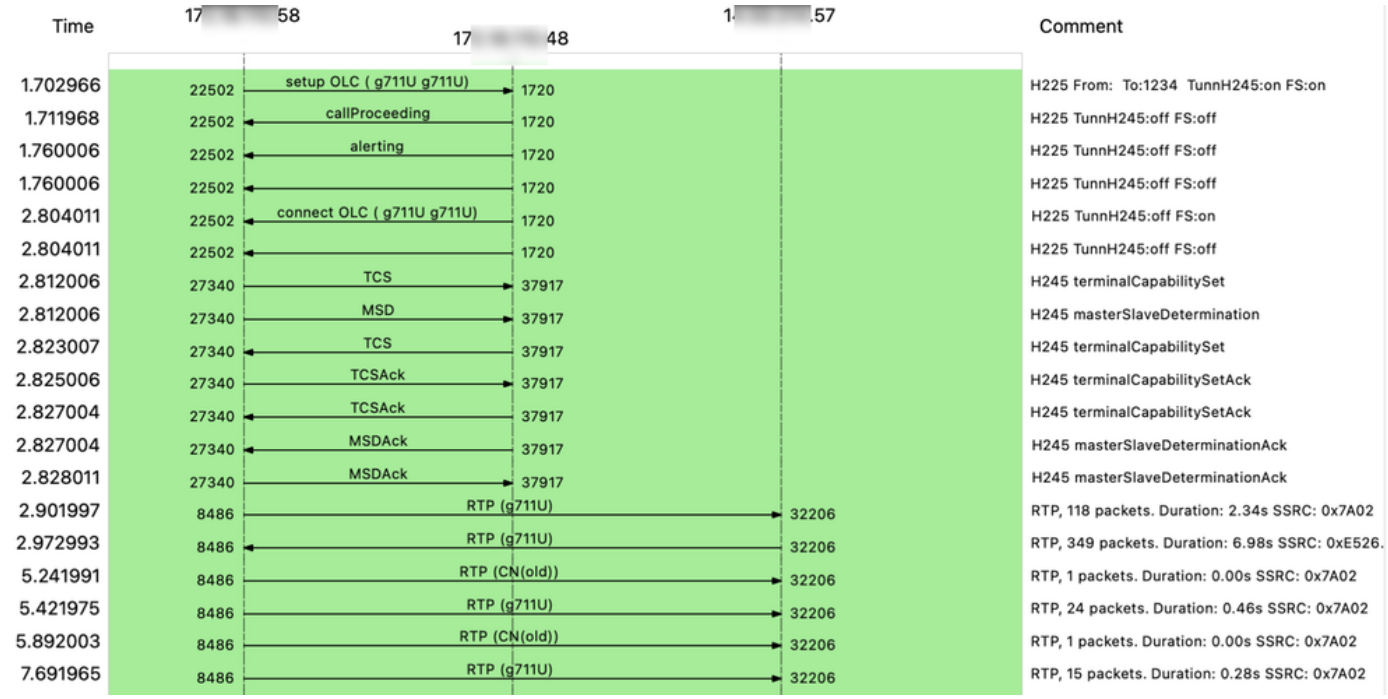
次のパケットキャプチャは、H.225およびH.245を搭載した2台のH.323デバイスからの要求と応答、およびメディア（音声）トラフィックを示しています。

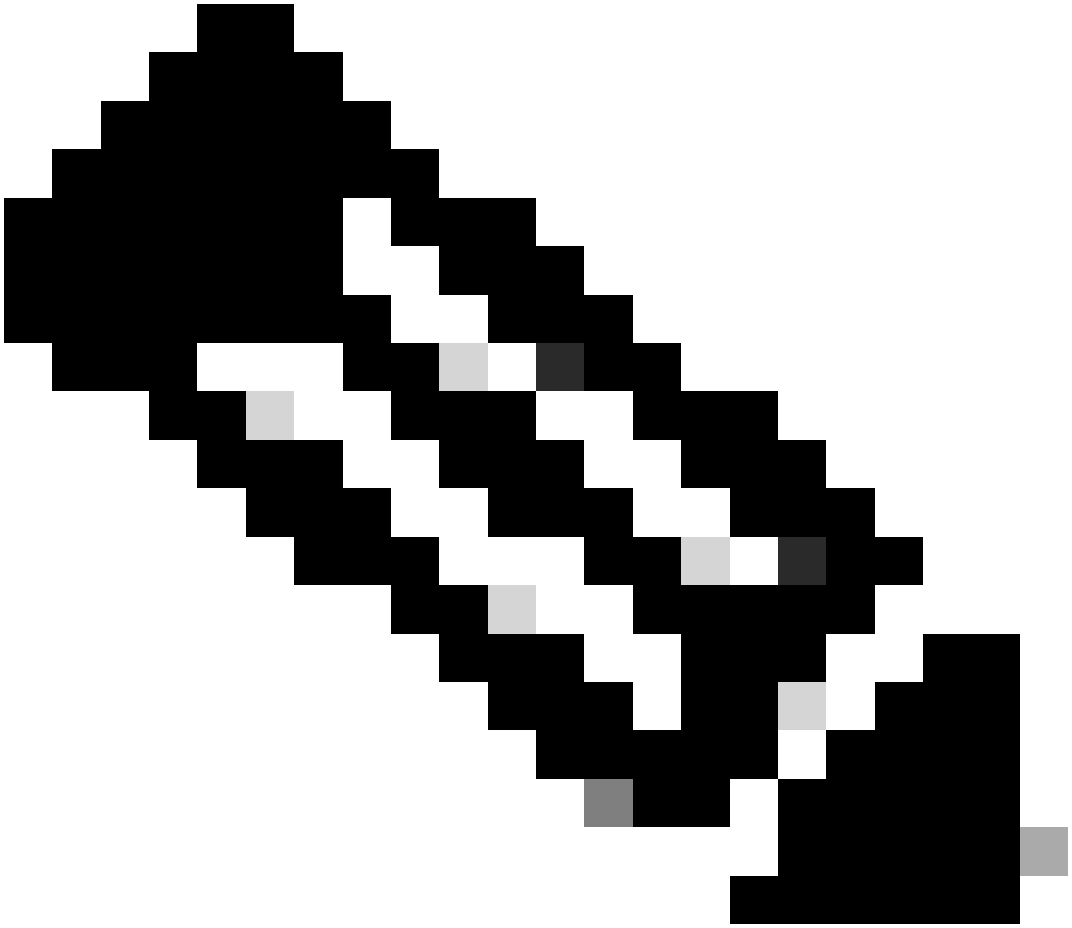


No.	Time	Source	Destination	Protocol	Length	Info
6	1.702966	17 58	17 48	H.225.0	683	CS: setup OpenLogicalChannel
8	1.711968	17 48	17 58	H.225.0	151	CS: callProceeding
9	1.760006	17 48	17 58	H.225.0	152	CS: alerting
10	1.760006	17 48	17 58	H.225.0	114	CS: notify
15	2.804011	17 48	17 58	H.225.0	248	CS: connect OpenLogicalChannel
16	2.804011	17 48	17 58	H.225.0	114	CS: notify
21	2.812006	17 58	17 48	H.245	135	terminalCapabilitySet
23	2.812006	17 58	17 48	H.245	68	masterSlaveDetermination
25	2.823007	17 48	17 58	H.245	176	terminalCapabilitySet
26	2.825006	17 58	17 48	H.245	65	terminalCapabilitySetAck
27	2.827004	17 48	17 58	H.245	65	terminalCapabilitySetAck
28	2.827004	17 48	17 58	H.245	64	masterSlaveDeterminationAck
30	2.828011	17 58	17 48	H.245	64	masterSlaveDeterminationAck
32	2.901997	17 58	14 7	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7A02, Seq=5180, Time=1424280842, Ma
33	2.922001	17 58	14 7	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7A02, Seq=5181, Time=1424281002
34	2.942004	17 58	14 7	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7A02, Seq=5182, Time=1424281162
35	2.961992	17 58	14 7	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7A02, Seq=5183, Time=1424281322
36	2.972993	1 57	17 58	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0xE526177E, Seq=63306, Time=2754086667

```
> Frame 6: 683 bytes on wire (5464 bits), 683 bytes captured (5464 bits)
> Ethernet II, Src: Cisco_a2:9a:00 ( :9a:00), Dst: V :84:d2:80)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 249
> Internet Protocol Version 4, Src: 17 58, Dst: 17 48
> Transmission Control Protocol, Src Port: 22502, Dst Port: 1720, Seq: 1, Ack: 1, Len: 625
> TPKT, Version: 3, Length: 625
> Q.931
> H.225.0 CS
```

次に、H.225とH.245を使用したH.323シグナリングと、RTPメディア（音声）の両方のフローの例を示します。

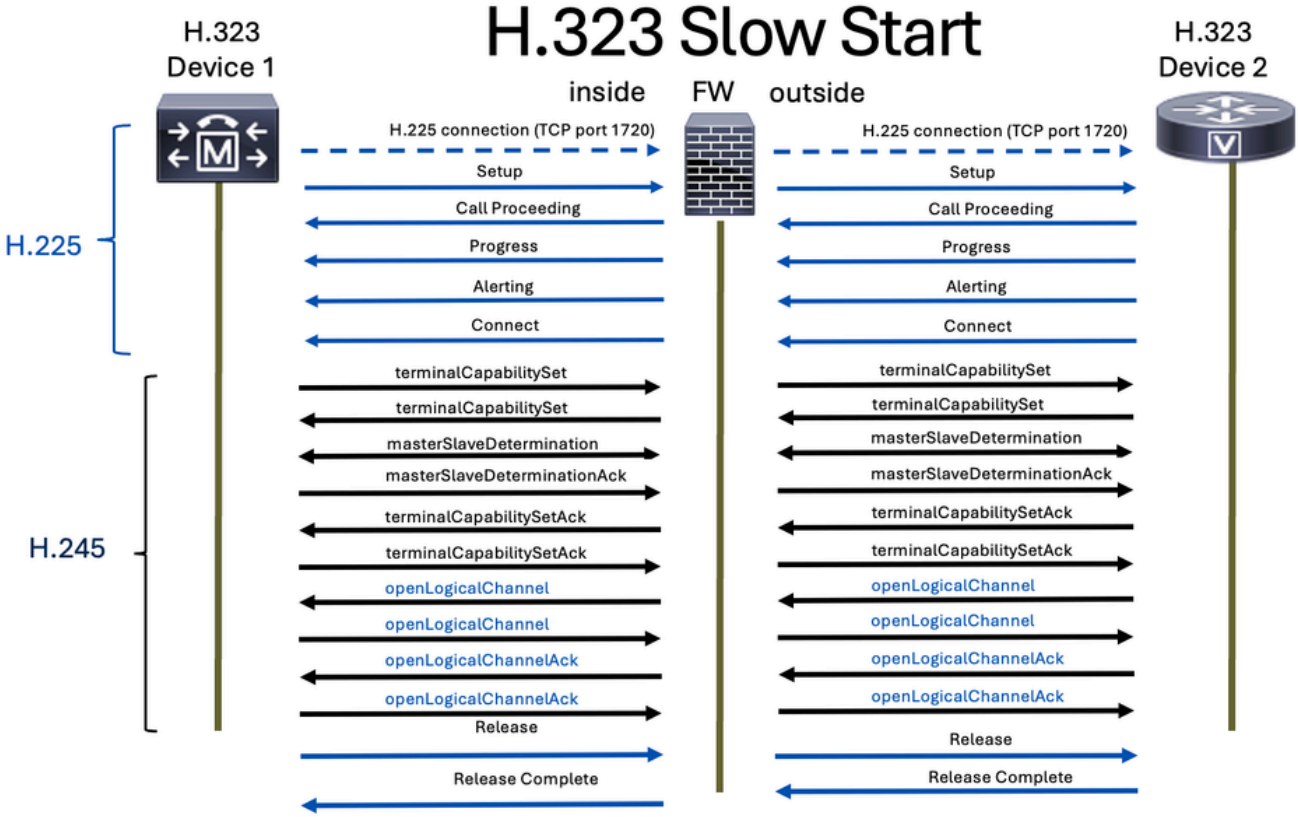

Time
Comment
1.702966 22502 setup OLC (g711U g711U) 1720 H225 From: To:1234 TunnH245:on FS:on
1.711968 22502 callProceeding 1720 H225 TunnH245:off FS:off
1.760006 22502 alerting 1720 H225 TunnH245:off FS:off
1.760006 22502 1720 H225 TunnH245:off FS:off
2.804011 22502 connect OLC (g711U g711U) 1720 H225 TunnH245:off FS:on
2.804011 22502 1720 H225 TunnH245:off FS:off
2.812006 27340 TCS 37917 H245 terminalCapabilitySet
2.812006 27340 MSD 37917 H245 masterSlaveDetermination
2.823007 27340 TCS 37917 H245 terminalCapabilitySet
2.825006 27340 TCSAck 37917 H245 terminalCapabilitySetAck
2.827004 27340 TCSAck 37917 H245 terminalCapabilitySetAck
2.827004 27340 MSDAck 37917 H245 masterSlaveDeterminationAck
2.828011 27340 MSDAck 37917 H245 masterSlaveDeterminationAck
2.901997 8486 RTP (g711U) 32206 RTP, 118 packets. Duration: 2.34s SSRC: 0x7A02
2.972993 8486 RTP (g711U) 32206 RTP, 349 packets. Duration: 6.98s SSRC: 0xE526.
5.241991 8486 RTP (CN(old)) 32206 RTP, 1 packets. Duration: 0.00s SSRC: 0x7A02
5.421975 8486 RTP (g711U) 32206 RTP, 24 packets. Duration: 0.46s SSRC: 0x7A02
5.892003 8486 RTP (CN(old)) 32206 RTP, 1 packets. Duration: 0.00s SSRC: 0x7A02
7.691965 8486 RTP (g711U) 32206 RTP, 15 packets. Duration: 0.28s SSRC: 0x7A02



注:H.323インスペクションは、Cisco Secure Firewall Threat Defense(FTD)およびSecure Firewall Adaptive Security Appliance(ASA)ではデフォルトで有効になっています。

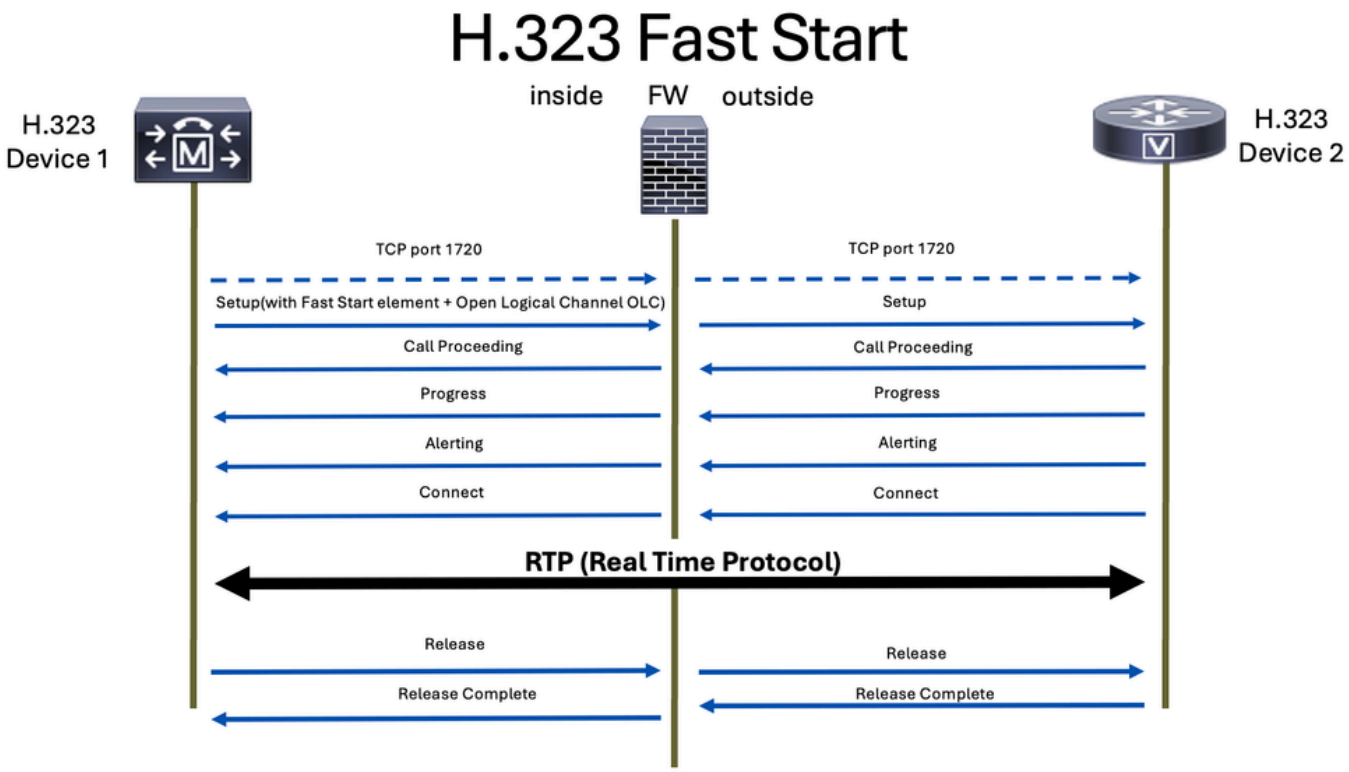
スロースタート

スロースタートモードでは、メディアチャネルが確立される前に、コールセットアッププロセスに複数のシグナリングステップが含まれます。手順には、セットアップ、呼処理、アラート、および接続が含まれます。これらの手順の後、H.245メディアネゴシエーションが個別に実行されます。つまり、メディアチャネルは最初のコールシグナリングが完了するまで確立されず、セットアップ時間が長くなる可能性があります。



Fast Start

これに対し、ファストスタートモードでは、初期セットアップメッセージ内でメディアネゴシエーションを行うことができます。つまり、最初のコールセットアップの一部としてネゴシエーションが行われるため、メディアチャネルをより迅速に確立できます。ファストスタートは、交換されるメッセージの数と、メディアチャネルが確立される前に必要な処理量を減らすことで、プロセスを合理化します。

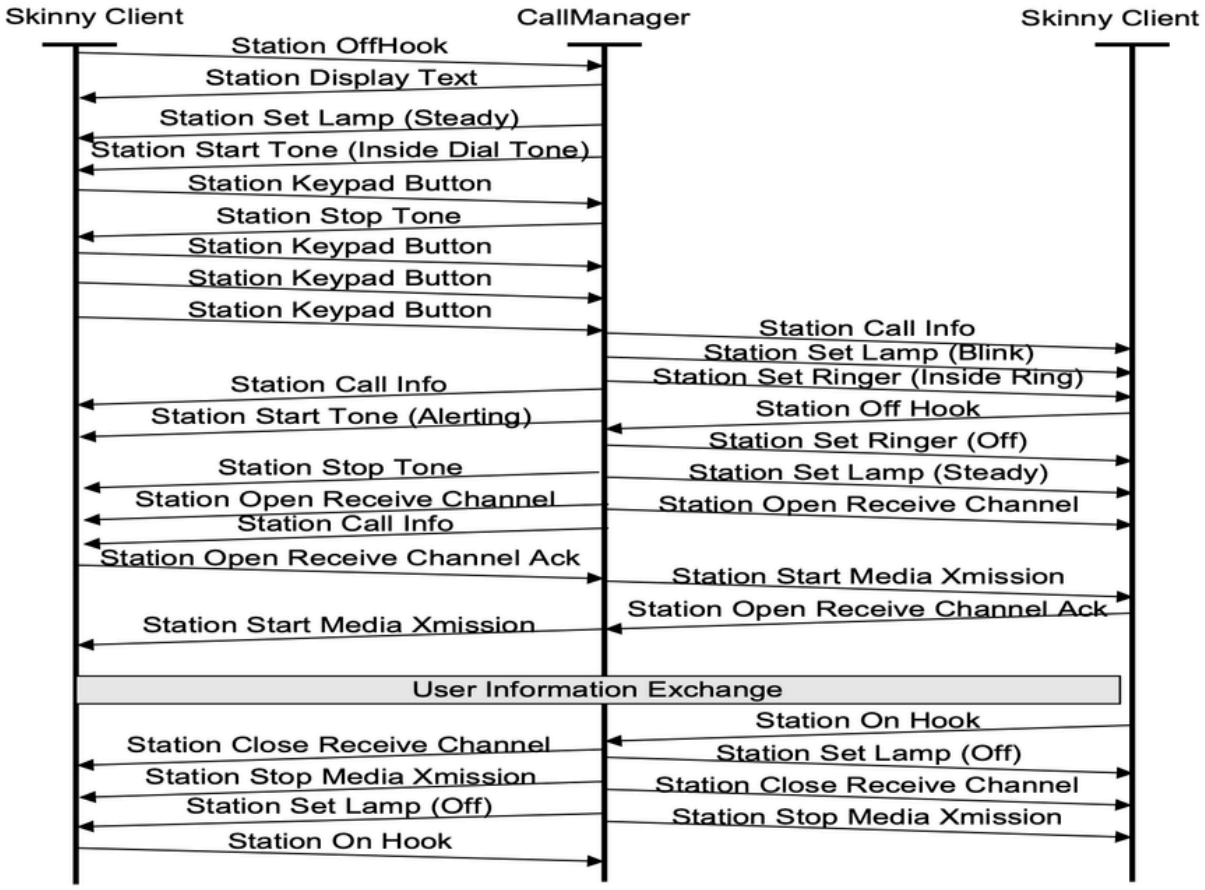


SCCP

Skinny Client Control Protocol(SCCP)は、シスコ独自のシグナリングプロトコルで、しばしば単にSkinnyと呼ばれます。主にCisco Unified Communications Manager(CUCM)、Cisco Unified Communications Manager Express(CME)ルータ、およびCisco IP Phoneで使用され、コールの設定と制御を容易にします。

SCCPプロトコルは、非セキュアSCCPに対してはポート2000でTCPを使用し、セキュアSCCPに対してはポート2443を使用します。

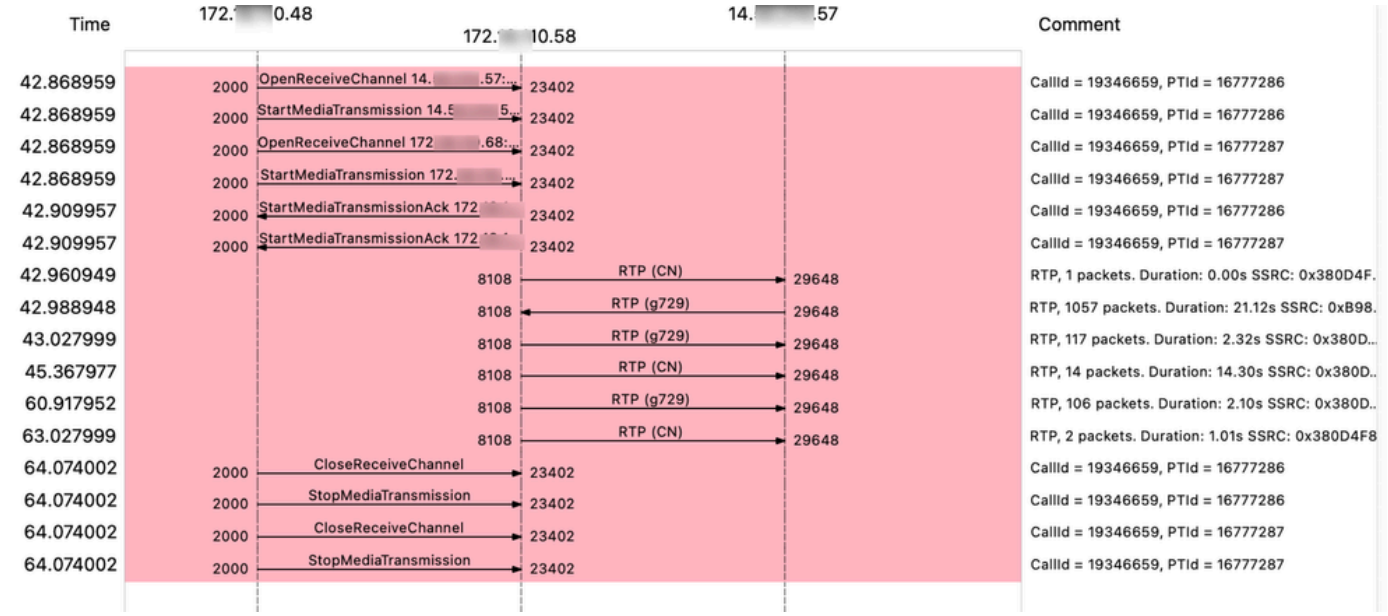
SCCPコールでよく見られるSCCPメッセージを次に示します。

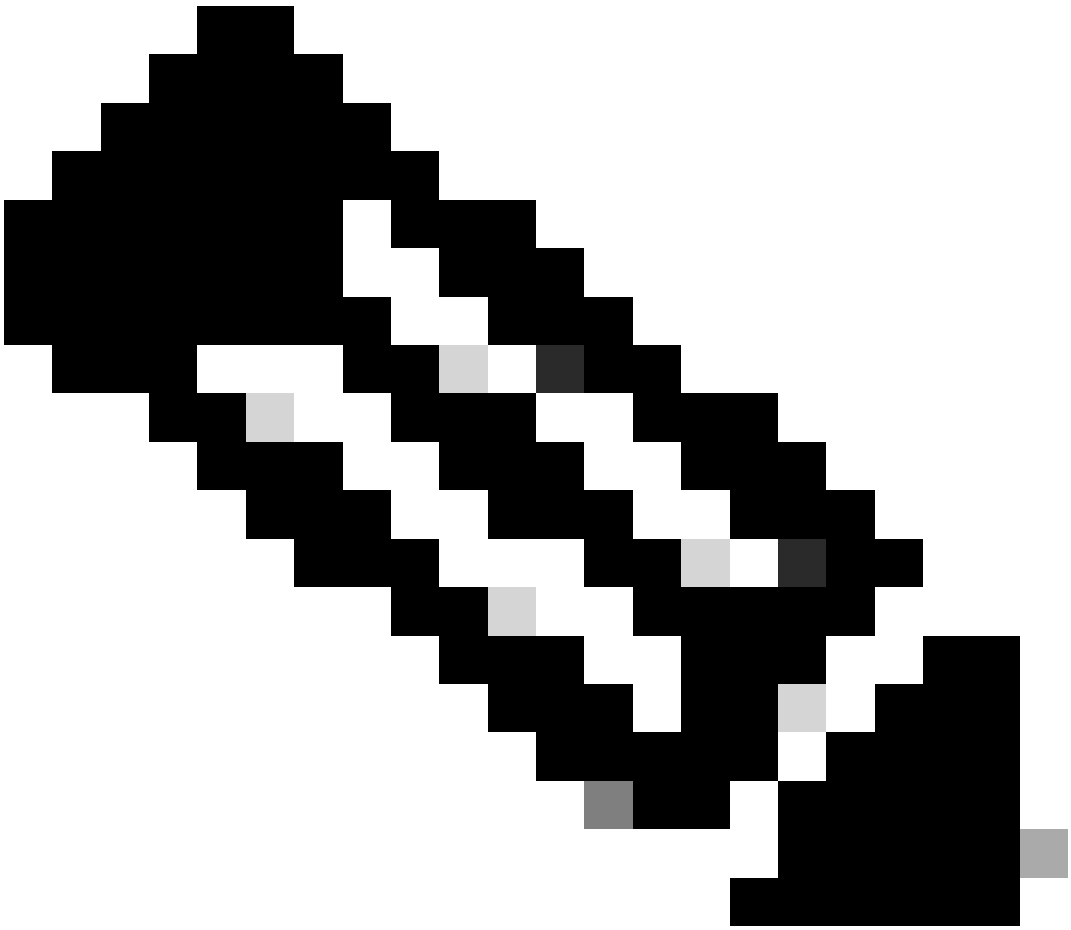


次のパケットキャプチャは、2台のSCCPデバイスからの要求と応答、およびメディア（音声）トラフィックを示しています。

No.	Time	Source	Destination	Protocol	Length	Info
42	11.170041	172. .0.48	172. 0.58	SKINNY/REQ	202	OpenReceiveChannel
58	13.307028	172. .0.48	172. 0.58	SKINNY/REQ	202	StartMediaTransmission
59	13.307028	172. .0.48	172. 0.58	SKINNY/REQ	202	OpenReceiveChannel
60	13.307028	172. .0.48	172. 0.58	SKINNY/REQ	202	StartMediaTransmission
62	13.309042	172. .0.58	172. 0.48	SKINNY/RESP	110	StartMediaTransmissionAck
64	13.309042	172. .0.58	172. 0.48	SKINNY/RESP	158	OpenReceiveChannelAck StartMediaTransmissionAck
66	13.390031	14.5 .57	172. 0.58	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7B4D4E5D, Seq=54086, Time=2101901655, Mark
67	13.409027	14.5 .57	172. 0.58	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7B4D4E5D, Seq=54087, Time=2101901815
68	13.429031	14.5 .57	172. 0.58	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7B4D4E5D, Seq=54088, Time=2101901975
69	13.451033	14.5 .57	172. 0.58	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7B4D4E5D, Seq=54089, Time=2101902135
70	13.453031	172. 0.58	14. .57	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x50, Seq=0, Time=585879569

次に、SCCPシグナリング（音声）とRTPメディア（音声）の両方のフローの例を示します。





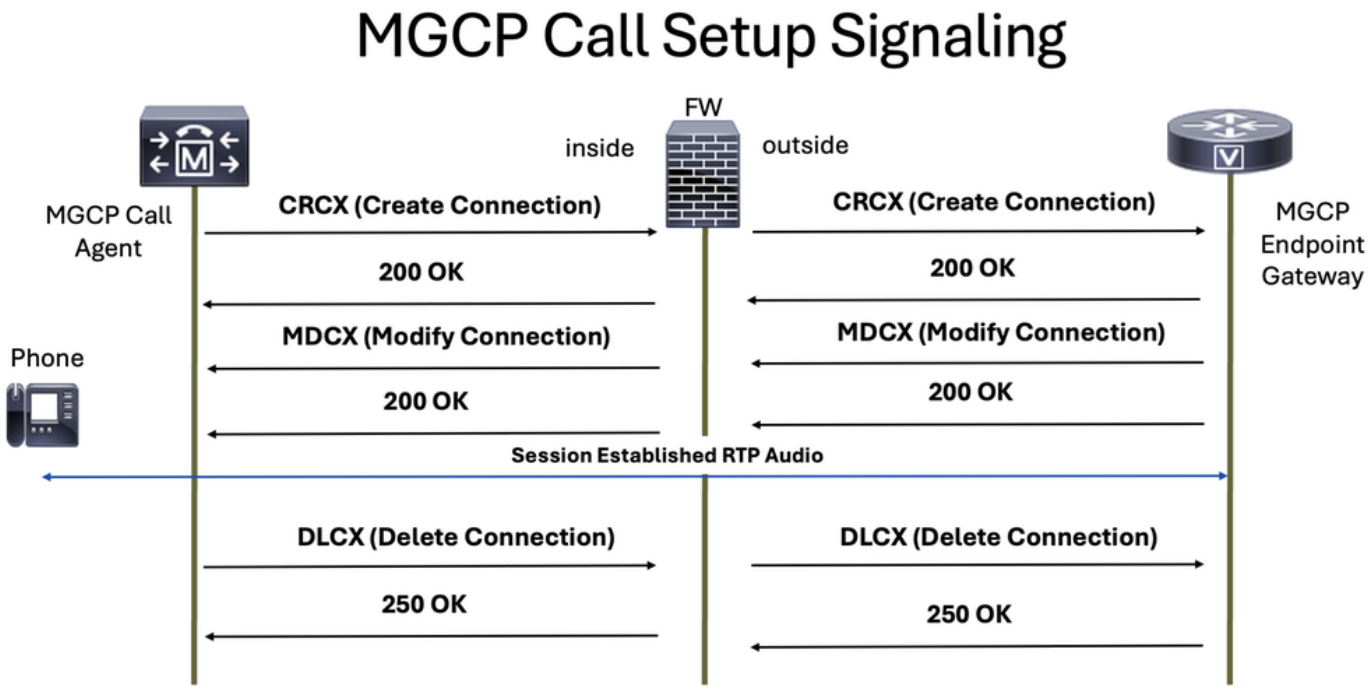
注:SCCPインスペクションは、Cisco Secure Firewall Threat Defense(FTD)およびSecure Firewall Adaptive Security Appliance(ASA)ではデフォルトで有効になっています。

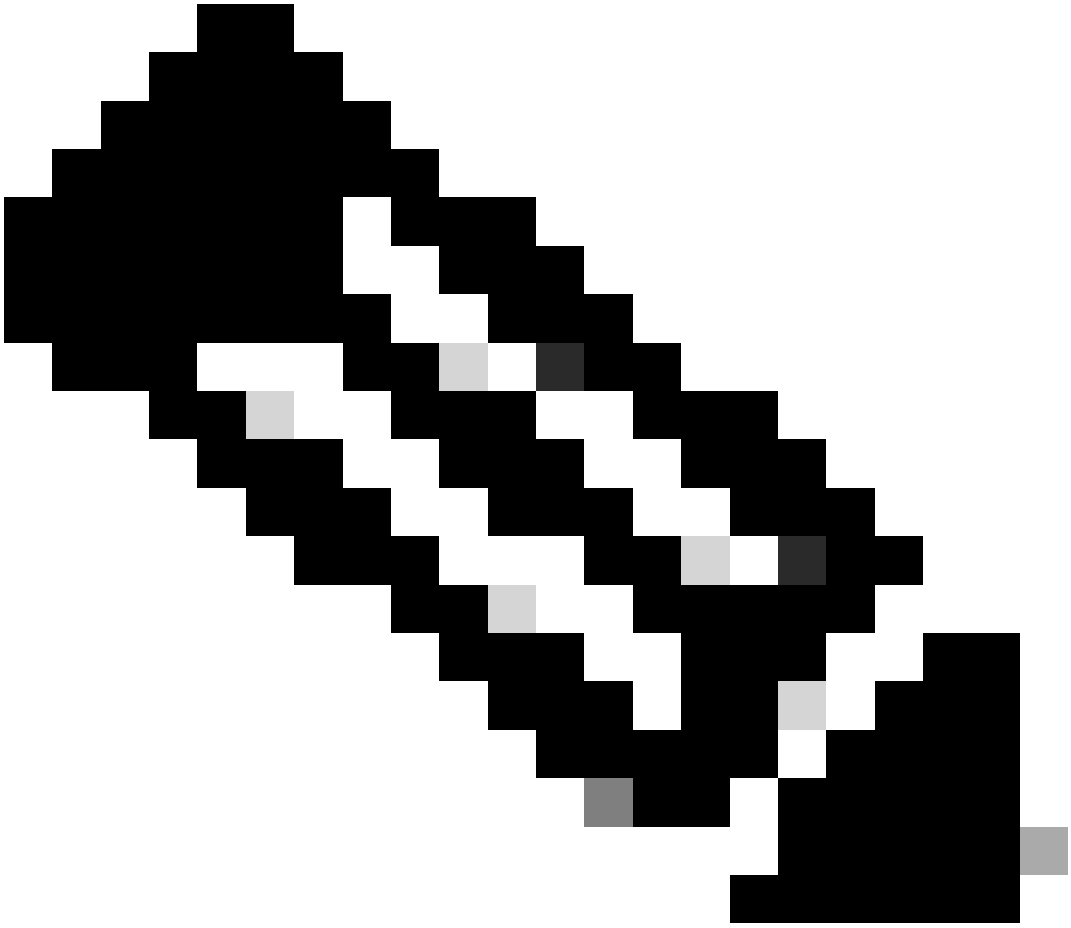
MGCP

メディアゲートウェイコントロールプロトコル(MGCP)は、コール制御デバイス（CUCMなど）によるVoIPコールの制御に使用されるプロトコルです。

MGCPシグナリングプロトコルはRFC 2705で定義されており、通信にTCPポート2428とUDPポート2427を使用します。

コール通信に対して期待されるMGCPの通常のパケットは次のとおりです。



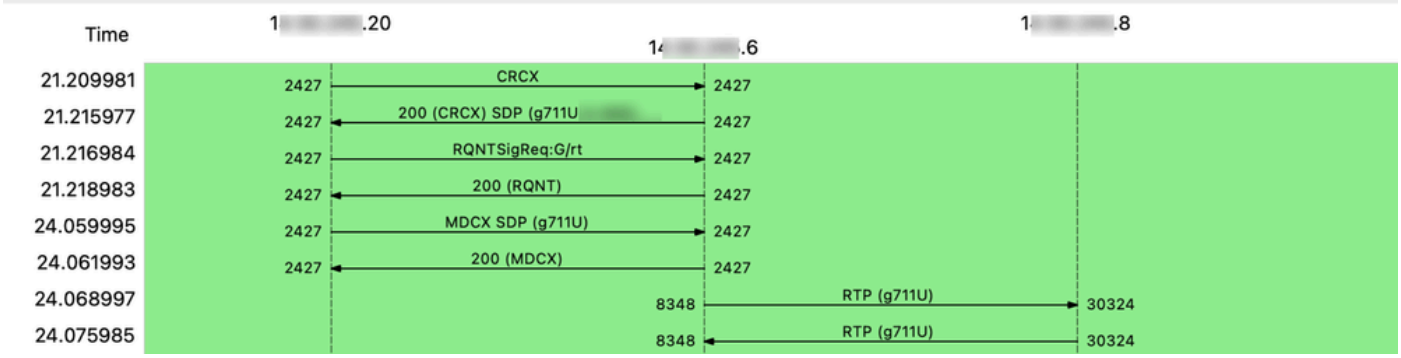


注：Cisco Secure Firewall Threat Defense(FTD)およびSecure Firewall Adaptive Security Appliance(ASA)のデフォルトのインスペクションポリシーでは、MGCPインスペクションは有効になっていません。そのため、このインスペクションが必要な場合は、MGCPインスペクションを有効にする必要があります。

次のパケットキャプチャは、2台のMGCPデバイスからの要求と応答、およびメディア（音声）トラフィックを示しています。

No.	Time	Source	Destination	Protocol	Length	Info
12	21.209981	1[redacted].20	1[redacted].6	MGCP	213	CRCX 509 S0/SU1/DS1-0/1@[redacted] MGCP 0.1
13	21.215977	1[redacted].6	1[redacted].20	MGCP/SDP	213	200 509 OK
14	21.216984	1[redacted].20	1[redacted].6	MGCP	144	RQNT 511 S0/SU1/DS1-0/1@[redacted] MGCP 0.1
18	21.218983	1[redacted].6	1[redacted].20	MGCP	57	200 511 OK
20	24.059995	1[redacted].20	1[redacted].6	MGCP/SDP	342	MDCX 513 S0/SU1/DS1-0/1@[redacted] MGCP 0.1
21	24.061993	1[redacted].6	1[redacted].20	MGCP	57	200 513 OK
22	24.068997	1[redacted].6	1[redacted].8	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7AE2, Seq=5377, Time=584785512
23	24.075985	1[redacted].8	1[redacted].6	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0xF22F508, Seq=39645, Time=128207581
24	24.088985	1[redacted].6	1[redacted].8	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7AE2, Seq=5378, Time=584785672
25	24.095988	1[redacted].8	1[redacted].6	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0xF22F508, Seq=39646, Time=128207741
26	24.108988	1[redacted].6	1[redacted].8	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7AE2, Seq=5379, Time=584785832
27	24.115991	1[redacted].8	1[redacted].6	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0xF22F508, Seq=39647, Time=128207901

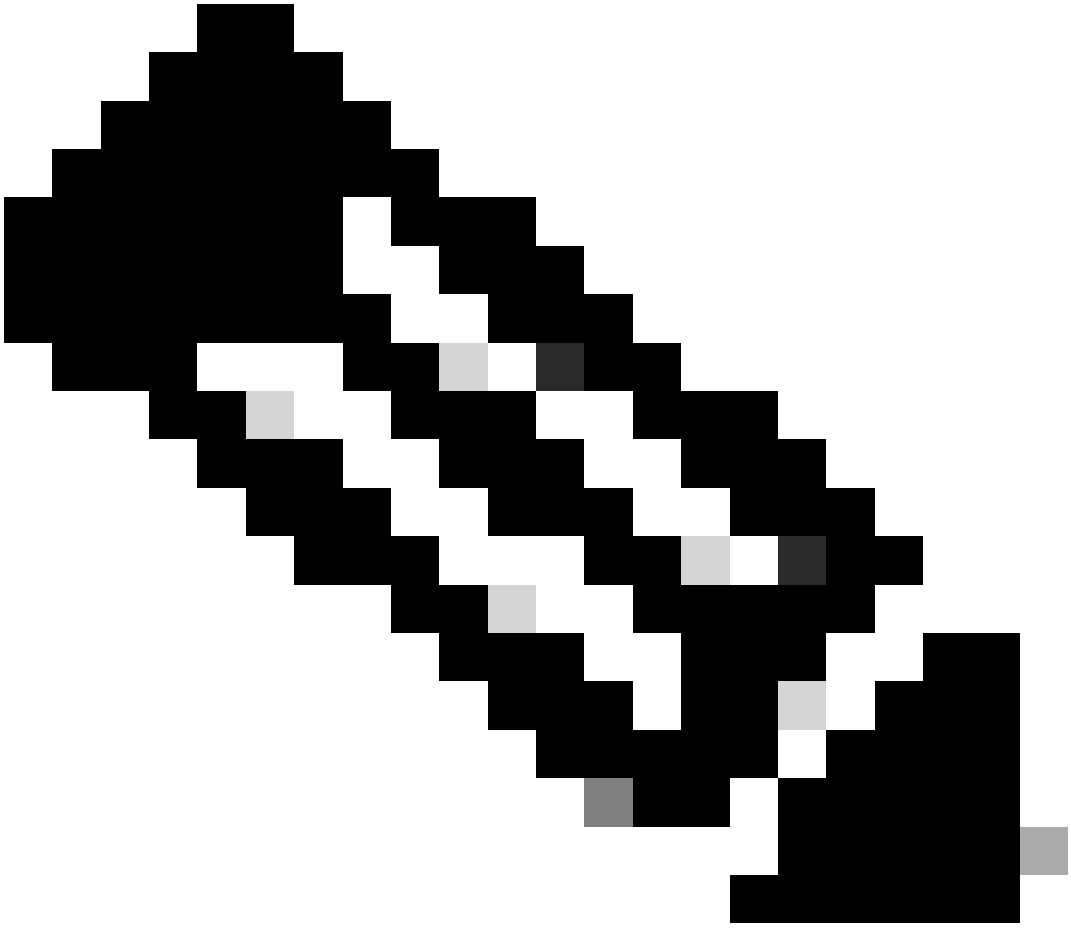
次に、MGCPシグナリング（音声）とRTPメディア（音声）の両方のフローの例を示します。



ベスト プラクティス

ASAの場合：

- 2つのシグナリングコンポーネント（デバイスまたはサーバ）との間で送受信されるトラフィックを許可する許可ルールを使用します。 これは、指定されたシグナリングVoIPプロトコルで使用されるポートによって制限される可能性があります。
- オーディオストリームまたはビデオストリームを送受信できるメディアデバイス間でRTPポートの範囲を許可します。



注：これらのオーディオデバイスまたはメディアデバイスは、シグナリングコンポーネント（デバイスまたはサーバ）とは異なる場合があることに注意してください。

FTDの場合：

- シグナリングコンポーネント（デバイスまたはサーバ）のプレフィルタルールを定義し、特定のシグナリングプロトコルのトラフィックだけを制限するように特定のポートを定義します。
- オーディオおよびビデオのRTPプロトコルのプレフィルタを設定します。

トラブルシュート

音声の問題のトラブルシューティングを行う際には、問題がシグナリングとメディア（音声またはビデオ）、またはその両方のいずれであるかを知る必要があります。次に、この問題を区別するための例をいくつか示します。

シグナリング問題の例：

++コールが確立されていないとユーザから報告されました。

++ユーザは他のユーザまたは番号にコールできません。

++OPTIONS sipメッセージが応答を受信していないため、SIPトランクは起動しません。

++デバイスを登録できません。

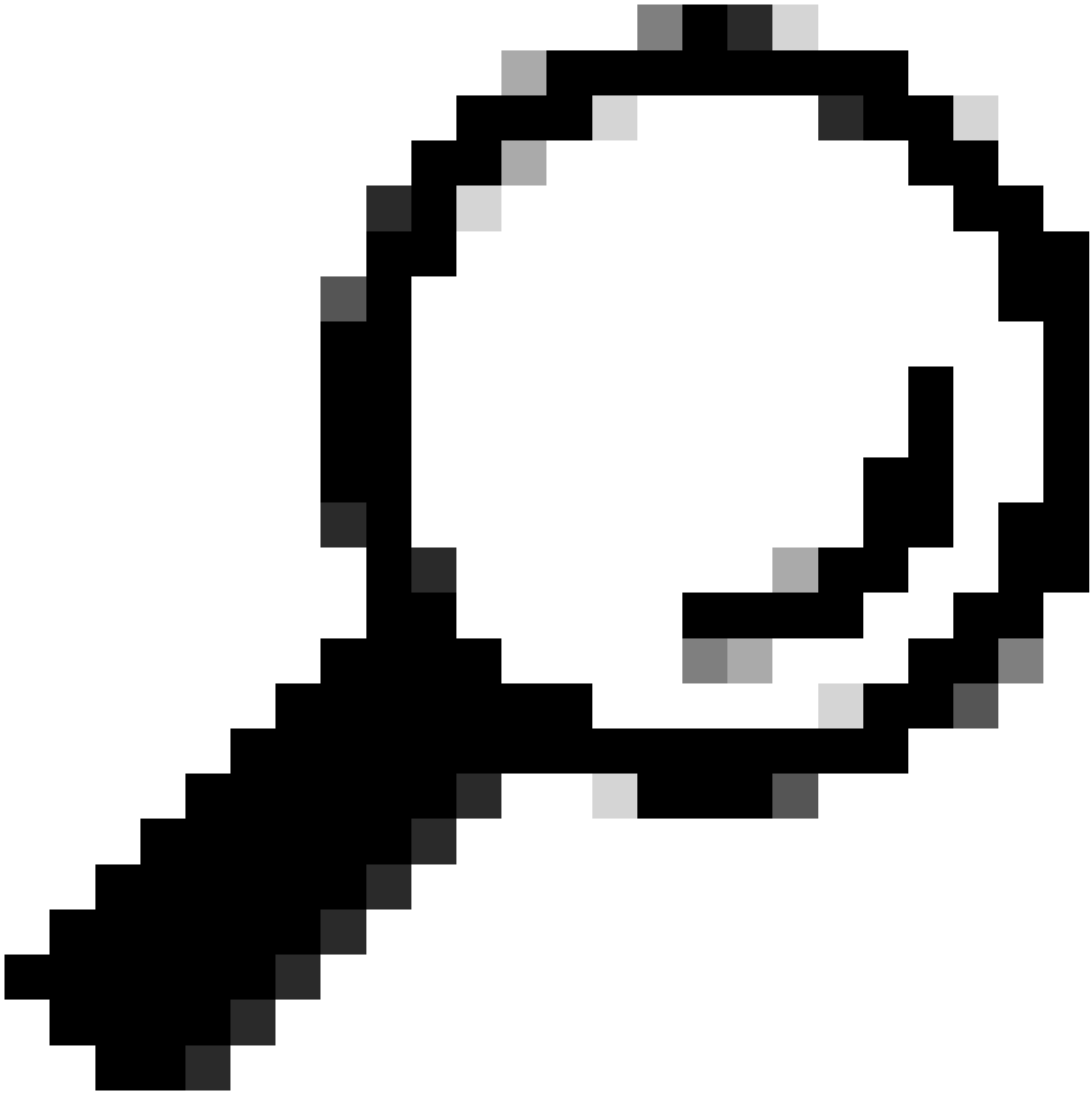
メディア（音声またはビデオ）の問題の例：

++片通話の問題があります。

++通話に音声がありません。

++画像が全く表示されない。

++コールがサイレントになります。



ヒント：ビデオコール中に、SDPはオーディオ、ビデオ、およびイメージの3つのメディア回線（m回線）までネゴシエートできます。 各m回線は、コールレッグごとに個別のReal-Time Transport Protocol(RTP)ストリームに対応します。つまり、コールレッグごとに最大3つの個別のRTPストリーム（メディアタイプごとに1つ）を作成できます。

ファイアウォールのシグナリング問題のトラブルシューティング

シグナリング部分のトラブルシューティングでは、次のことを確認する必要があります。

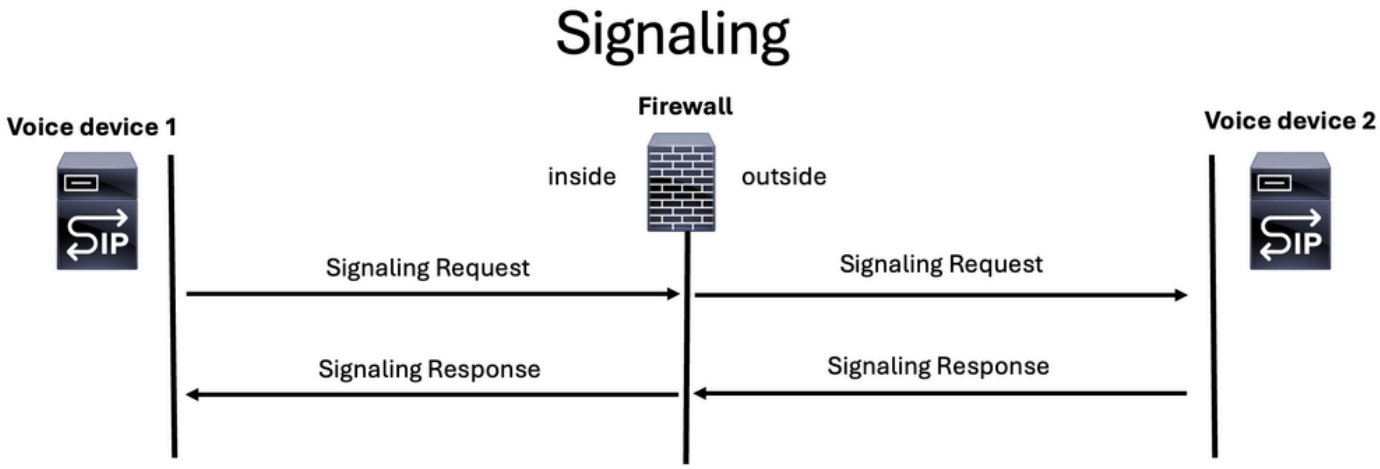
++入力インターフェイスと出力インターフェイスの両方からのコールに関係するすべてのシグナリングコンポーネント（デバイスまたはサーバ）を特定し、いずれかのSecure FWのCLIでパケットキャプチャに対して適切な一致基準を設定します。

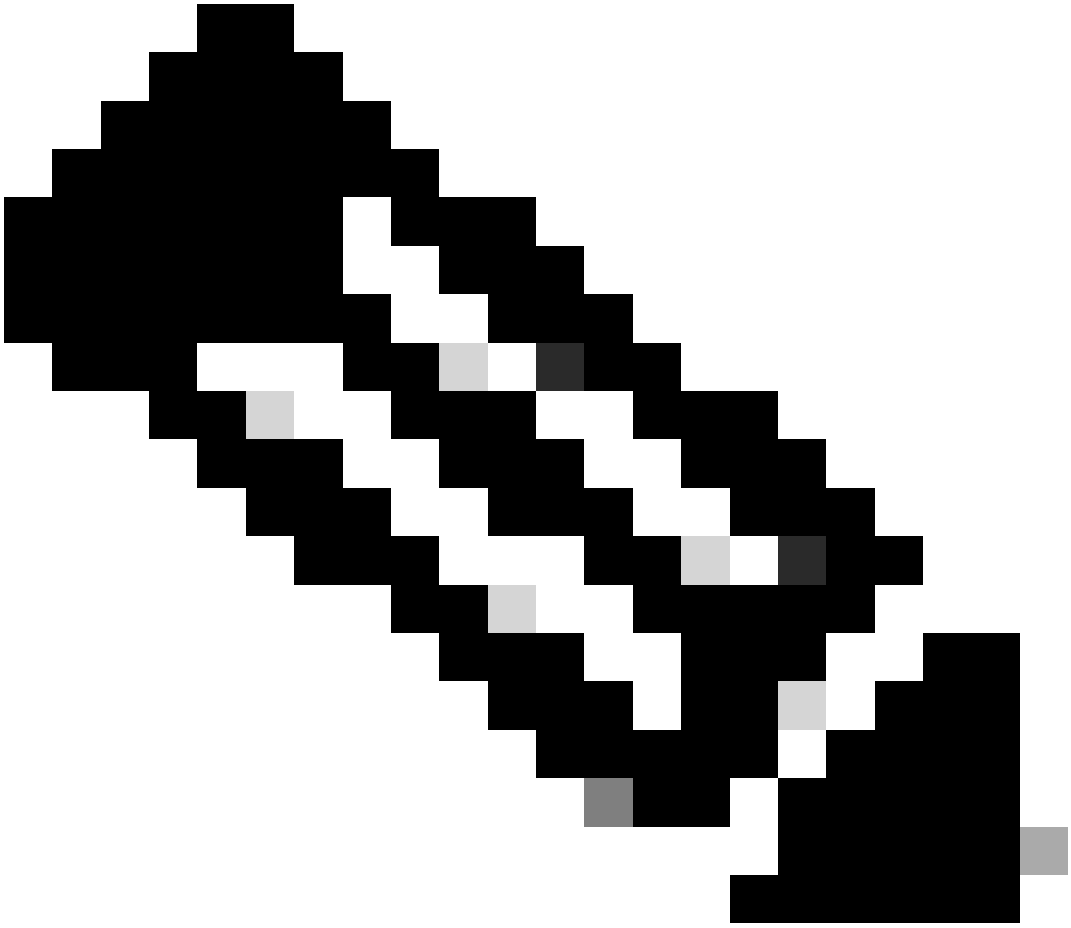
++入力インターフェイスのシグナリングメッセージの数は、出力インターフェイスと一致する必

要があることに注意してください。

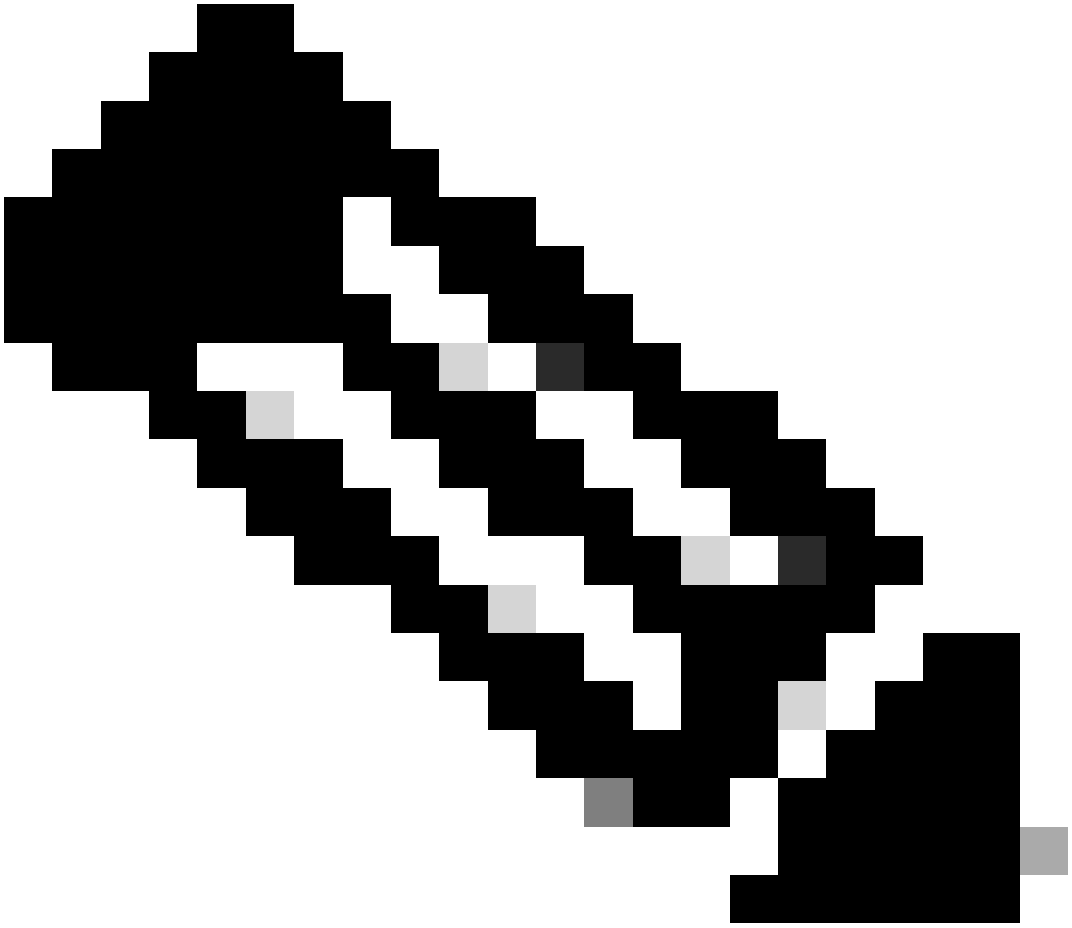
++シグナリングプロトコルでTCPとUDPのどちらを使用するかを指定し、予期されるポート番号をフィルタリングすることによって、パケットキャプチャの効率を高めることができます。すべてのシグナリングプロトコルはIP上で動作するため、CLIでこれらのフィルタを適用すると、キャプチャで表示されるトラフィックの量を制限するのに役立ちます。

++出力インターフェイスの場合のみ、発信トラフィックに割り当てられたNAT IPアドレスがパケットキャプチャフィルタで指定されていることを確認してください。これにより、出力インターフェイスに表示される正しいトラフィックを確実にキャプチャできます。





注：音声に使用するシグナリングプロトコルに関係なく、要求と応答が常に存在し、入力インターフェイスと出力インターフェイスの両方で一貫している必要があることに注意してください。

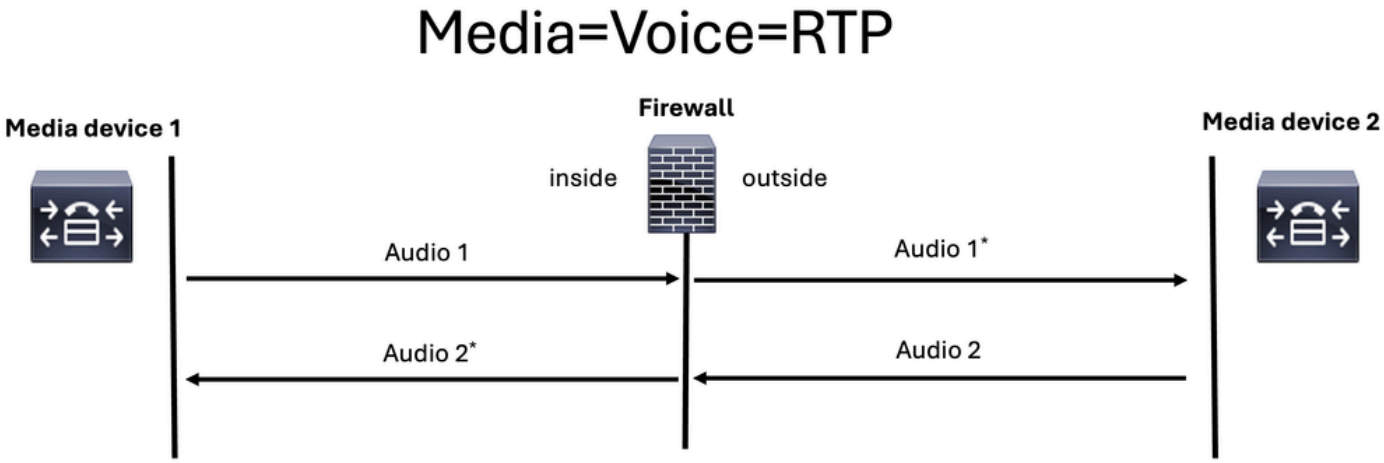


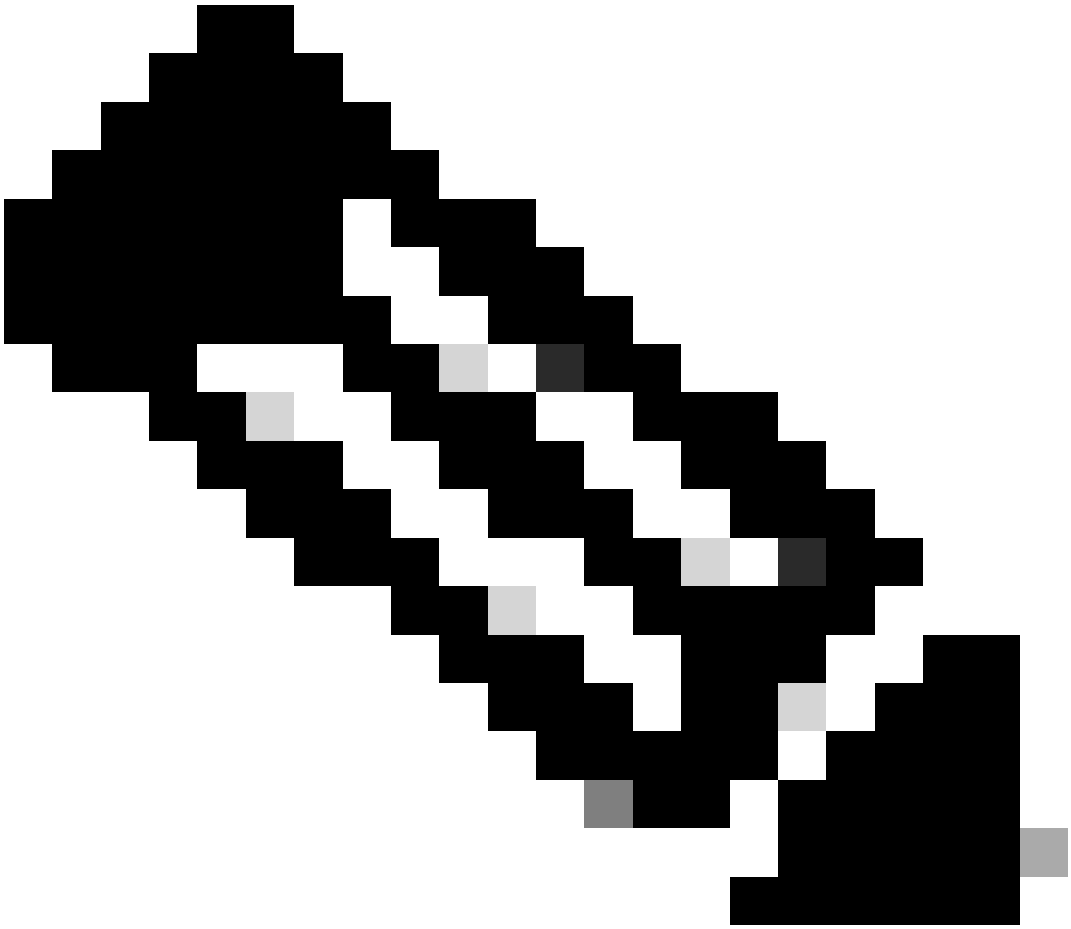
注：可能な限り、通信パスにファイアウォールが1つだけ含まれるようにしてください。一部の導入では、音声シグナリングとメディアストリームが別々のファイアウォールを通過できます。このような場合は、トラブルシューティングプロセスに関連するすべてのファイアウォールを含めてください

ファイアウォールのメディア問題のトラブルシューティング

FWの観点からは、片通話、両通話、または無音声の問題をトラブルシューティングする際に分析する必要がある4つのストリームがあります。

1. 発信者から着信者（入力インターフェイス）へのRTPストリーム。
2. 発信者から着信者（出力インターフェイス）へのRTPストリーム。
3. 呼び出し先から発信者（出力インターフェイス）へのRTPストリーム。
4. 呼び出し先から発信者（入力インターフェイス）へのRTPストリーム。



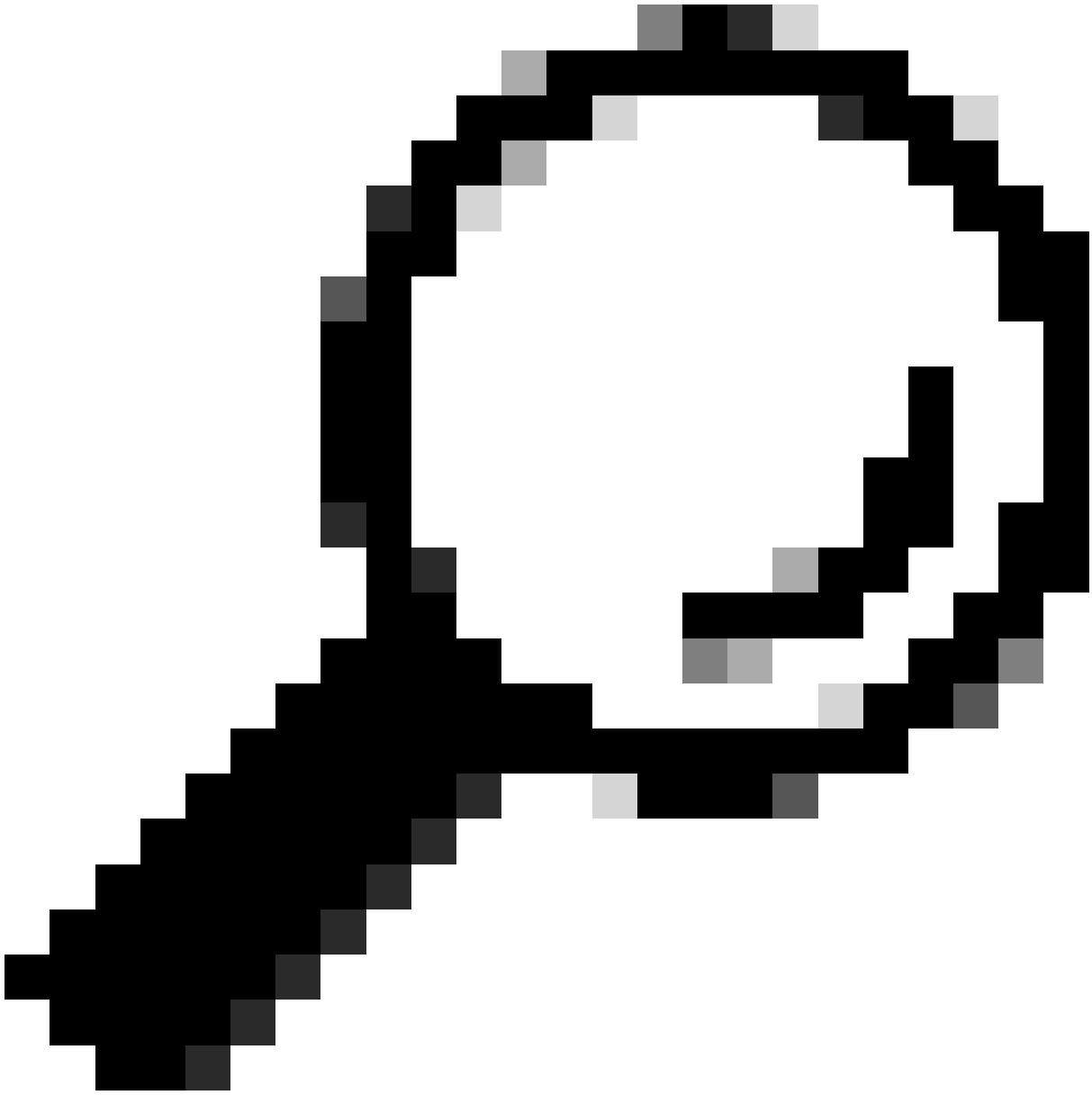


注:FTDのASAまたはLINAモードでCLIパケットキャプチャを使用する場合は、トラブルシューティングを実行してください。これにより、単一のパケットキャプチャで複数の一致を適用する柔軟性が向上します。

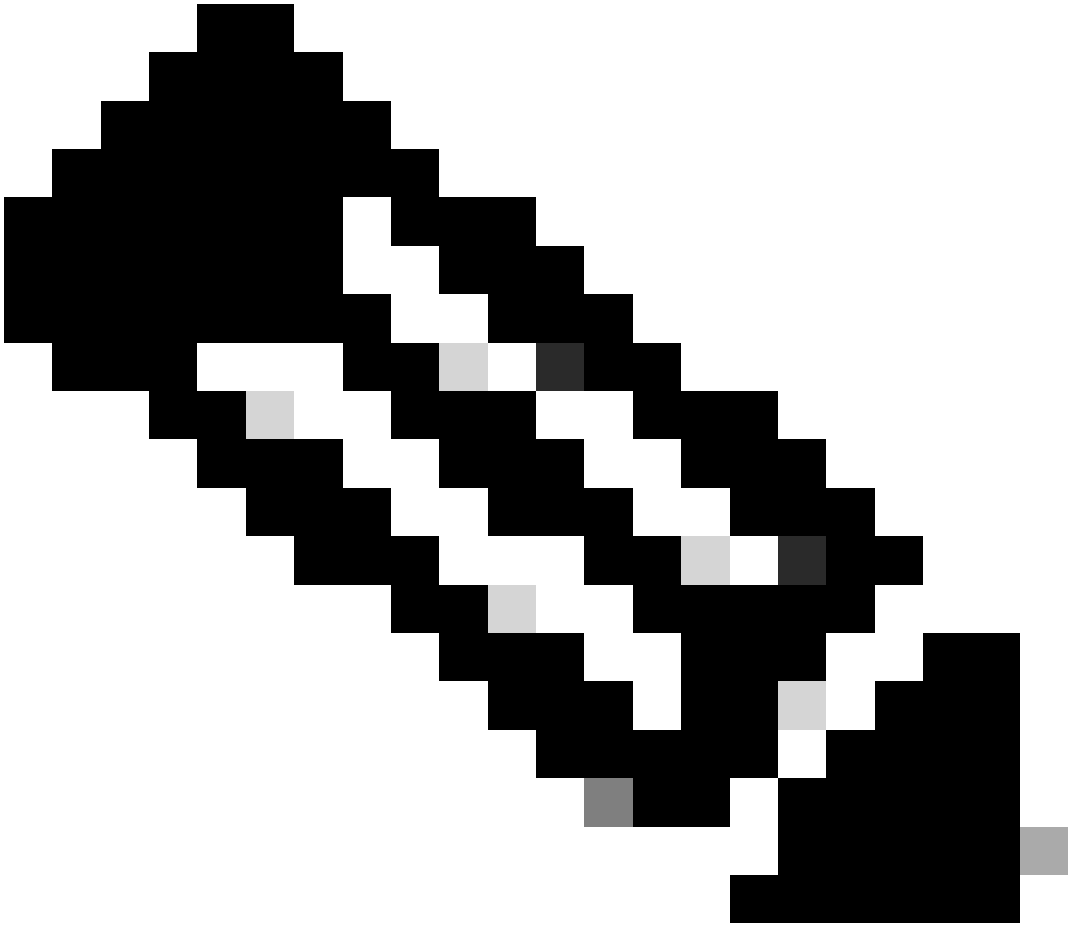
SIPコールのトラブルシューティング

セキュアFW（ASAまたはFTD）の音声の問題をトラブルシューティングする場合は、次の手順を実行する必要があります。

1. コールフローとトポロジダイアグラムがあることを確認します。
2. ユーザの観点から問題を理解していることを確認します。
3. シグナリングプロトコルのパスを理解する。
4. メディアRTPプロトコルのパスを理解します。
5. 入力インターフェイスと出力インターフェイスの両方でパケットキャプチャを取得します。
6. 設定ACLルールとNATルールを復習します。
7. SIPシグナリングトラフィックがファイアウォールによってブロックされていないことを確認します。また、入力インターフェイスと出力インターフェイスを比較して、音声トラフィックフローを分析します。
8. 入力インターフェイスと出力インターフェイスのトラフィックフローを比較して、RTPメディアトラフィックがファイアウォールによってブロックされていないことを確認します。
9. シグナリングデバイスがインスペクションをサポートしていることを確認します。サポートしていない場合は、インスペクションを無効にします。



ヒント:FWに入るSIPシグナリングメッセージは、FWから出るメッセージと同じでなければなりません。



注:SIPのトラブルシューティングのヒントは、H.323、MGCP、およびSCCPプロトコルにも適用できます。

関連情報

- CLIによるASAパケットキャプチャの設定
- Firepower Threat Defense(FTD)キャプチャの使用

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。