

瞭解安全防火牆的IP語音協定基礎知識

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[VoIP基礎](#)

[訊號](#)

[媒體](#)

[媒體流通](#)

[媒體週轉](#)

[作業階段啟始通訊協定\(SIP\)](#)

[SIP呼叫消息](#)

[SIP選項消息](#)

[SIP註冊消息](#)

[作業階段說明通訊協定\(SDP\)](#)

[提早發盤](#)

[延遲提供](#)

[早期媒體](#)

[H.323](#)

[H.225](#)

[H.245](#)

[慢啟動](#)

[快速啟動](#)

[SCCP](#)

[MGCP](#)

[最佳實踐](#)

[疑難排解](#)

[疑難排解防火牆上的訊號問題](#)

[對防火牆上的介質問題進行故障排除](#)

[排除SIP呼叫故障](#)

[相關資訊](#)

簡介

本文檔介紹各種VoIP協定的基本原理，以幫助工程師在安全防火牆上有效地排除故障。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案適用於以下裝置的疑難排解案例：

- 安全防火牆威脅防禦(FTD)
- 安全防火牆調適型安全裝置(ASA)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

VoIP基礎

通訊是人類互動的基礎，IP語音(VoIP)協定已成為人類通訊不可或缺的組成部分。因此，在排除包含防火牆(FW)的場景故障時，瞭解其部件非常重要。

VoIP由兩部分組成：

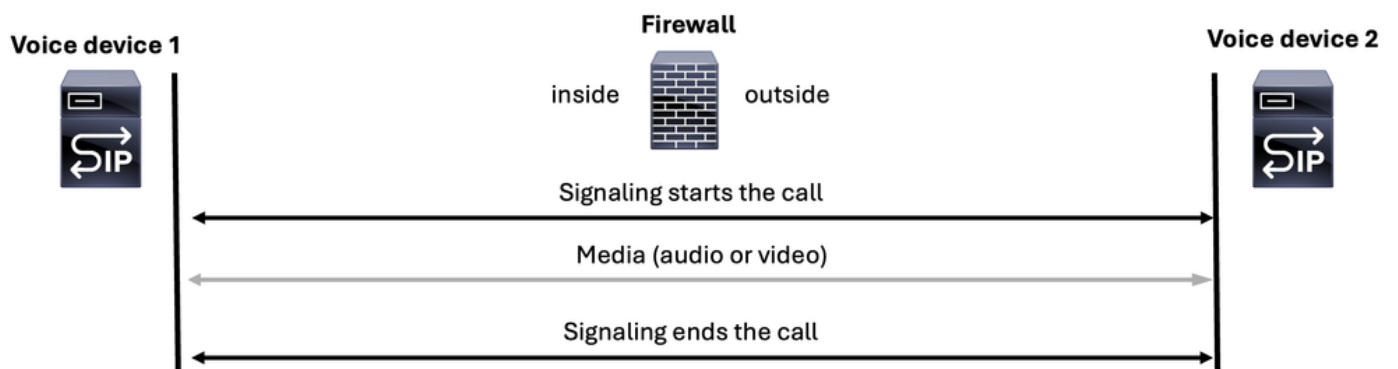
- 訊號
- 媒體 (語音或影片)

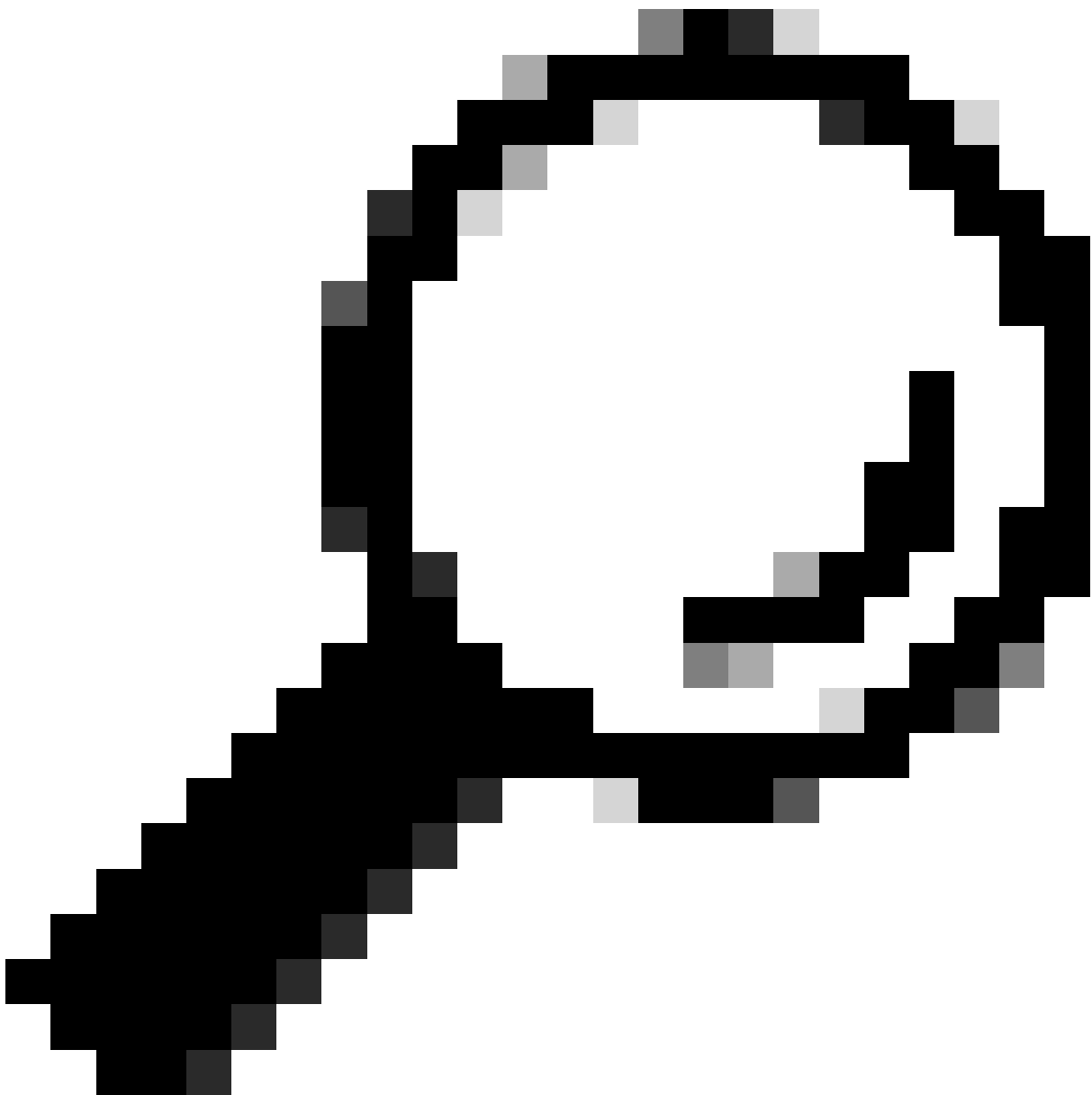
VoIP通訊總是從發起呼叫的信令部分開始，然後對媒體 (語音或影片) 進行流式傳輸，最後通過信令結束呼叫。



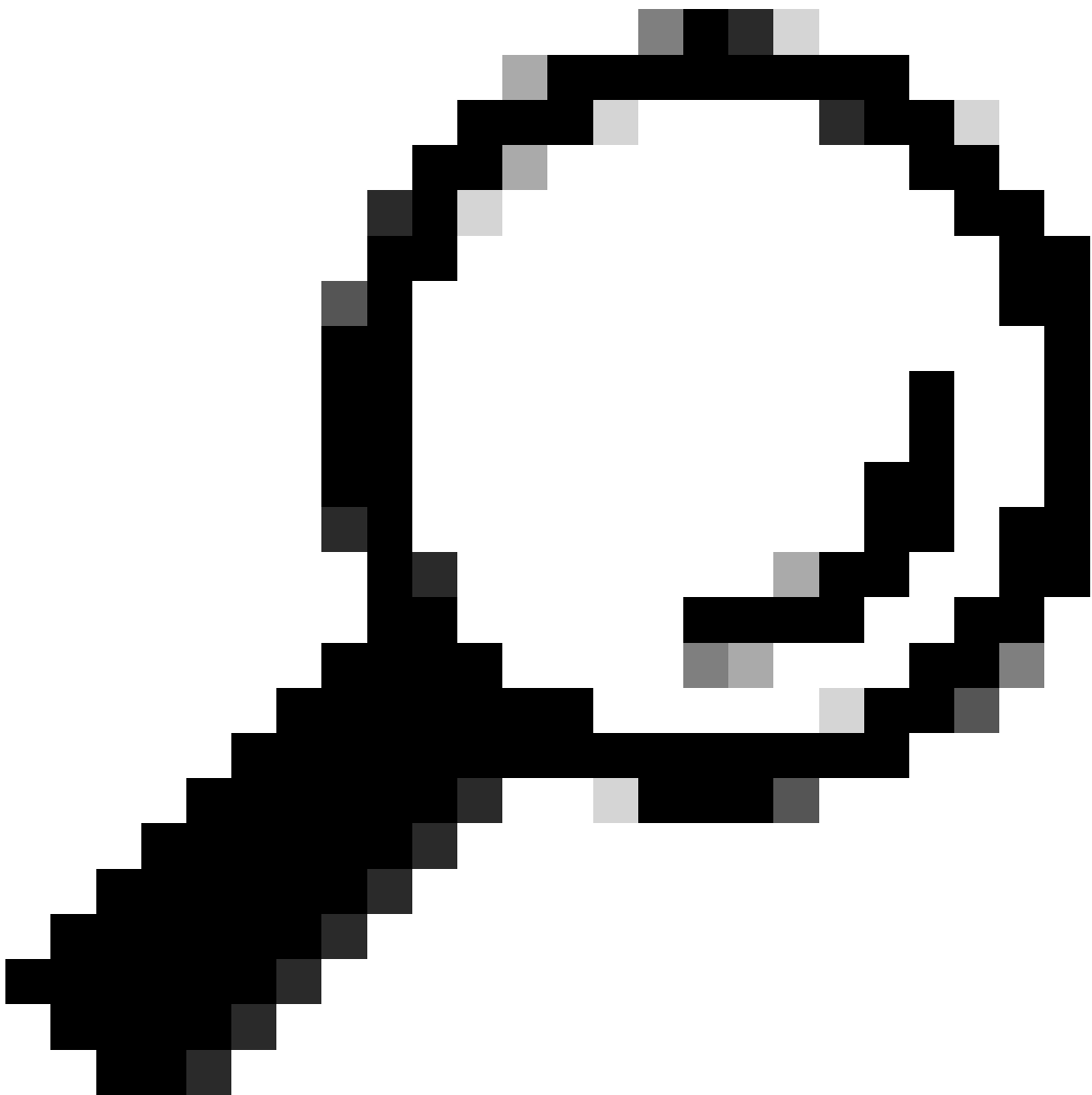
附註：SIP是使用最廣泛的協定，因此在許多圖表中始終以SIP語音伺服器圖示表示。

Voice over IP (VoIP)





提示：排查ASA或FTD的語音問題時，從使用者的角度考慮場景至關重要。您需要確定呼叫是否已建立，或沒有音訊或單向音訊。此資訊提供有關問題是屬於信令協定還是媒體（語音或影片）協定的重要線索。



提示：語音裝置可以同時管理語音即時傳輸協定(RTP)流量和信令流量，也可以同時管理這兩者。排除語音故障時，請務必記住以下主要概念：

++信令伺服器：這些伺服器僅負責處理訊號流量。

++媒體伺服器：這些伺服器以獨佔方式處理語音RTP流量。

++有些裝置可以同時處理這兩個任務。

訊號

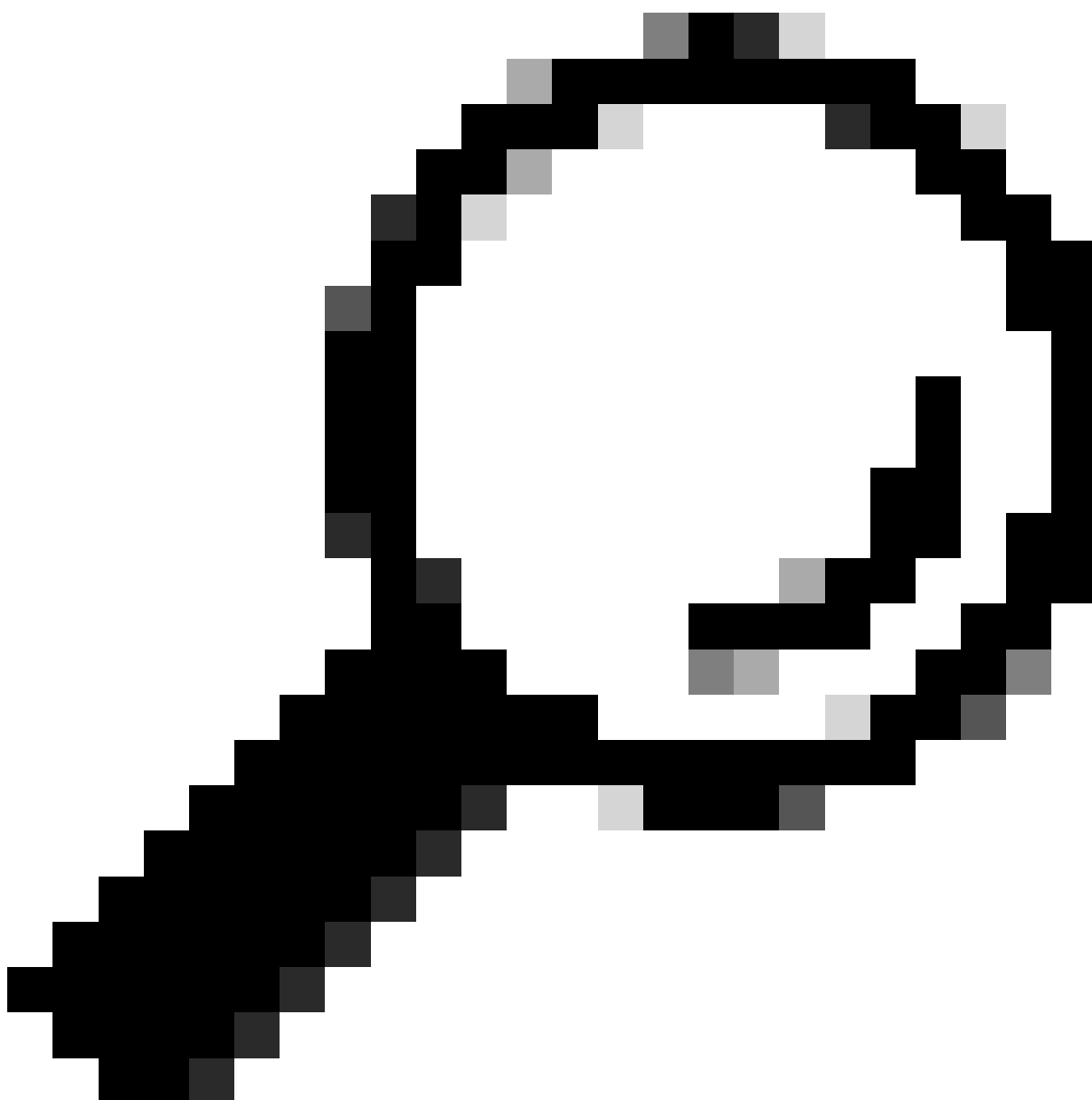
信令協定是啟動語音通訊的呼叫的一部分，但不僅如此，它還執行以下功能：

- 保持溝通。

- 修改通訊。
- 結束通訊。

不同型別的信令協定可幫助建立呼叫，最常見協定包括：

- 作業階段啟始通訊協定(SIP)
 - H.323
 - 媒體閘道控制通訊協定(MGCP)
 - 精簡型通話控制通訊協定(SCCP)
-



提示：確定正在使用的信令協定對於ASA或FTD上的資料包捕獲確定適當的埠至關重要。此外，具有呼叫流和網路拓撲有助於瞭解信令路徑。

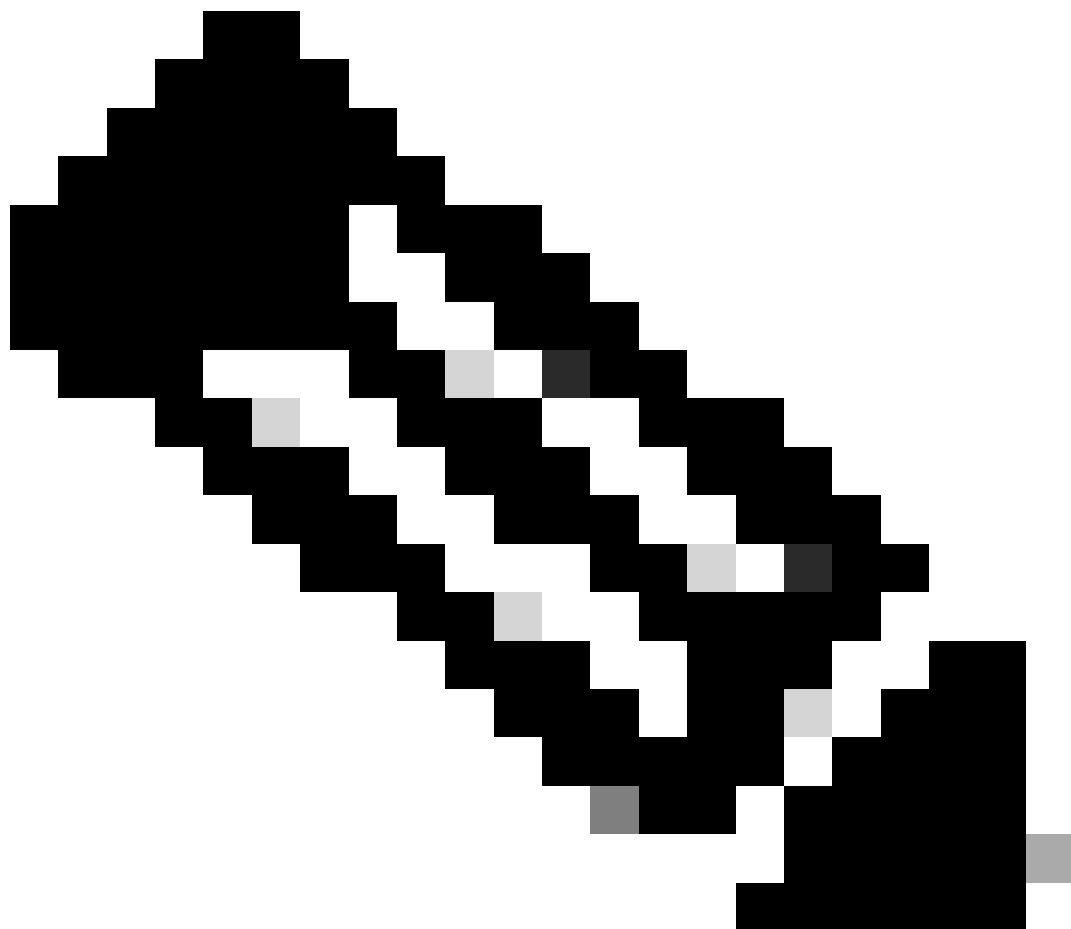
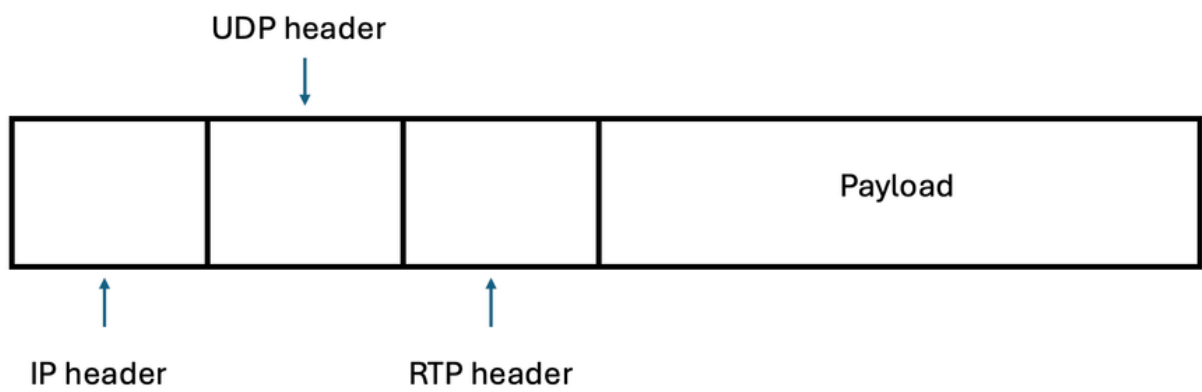


附註：信令資料包包括源IP地址和目的IP地址，有助於識別參與傳送和接收RTP媒體流的各方。

媒體

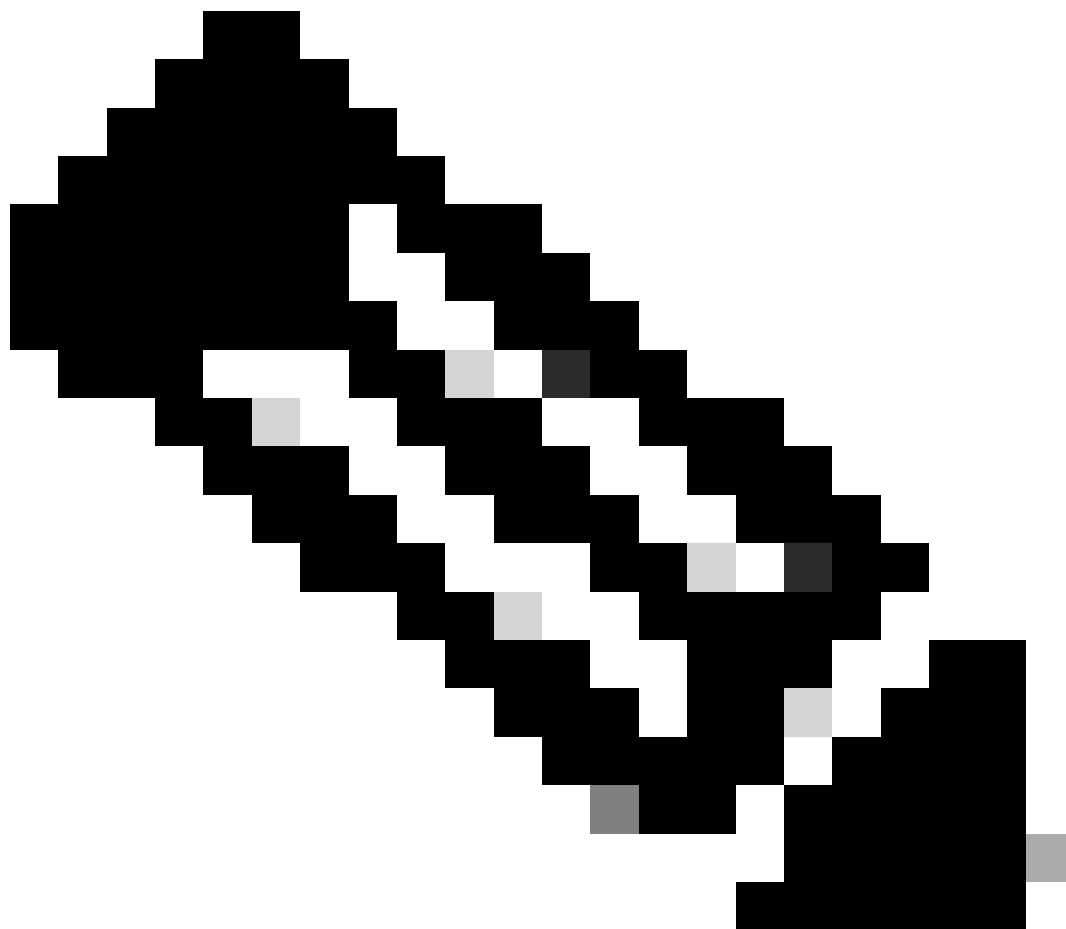
在信令完成且信令元件（裝置或伺服器）同意媒體型別後，即時協定(RTP)開始向相關各方傳送媒體（音訊和/或影片）。

RTP是用於流媒體的網際網路通訊協定，只有在建立通話後才會傳送，而且它透過使用者資料包通訊協定(UDP)執行。

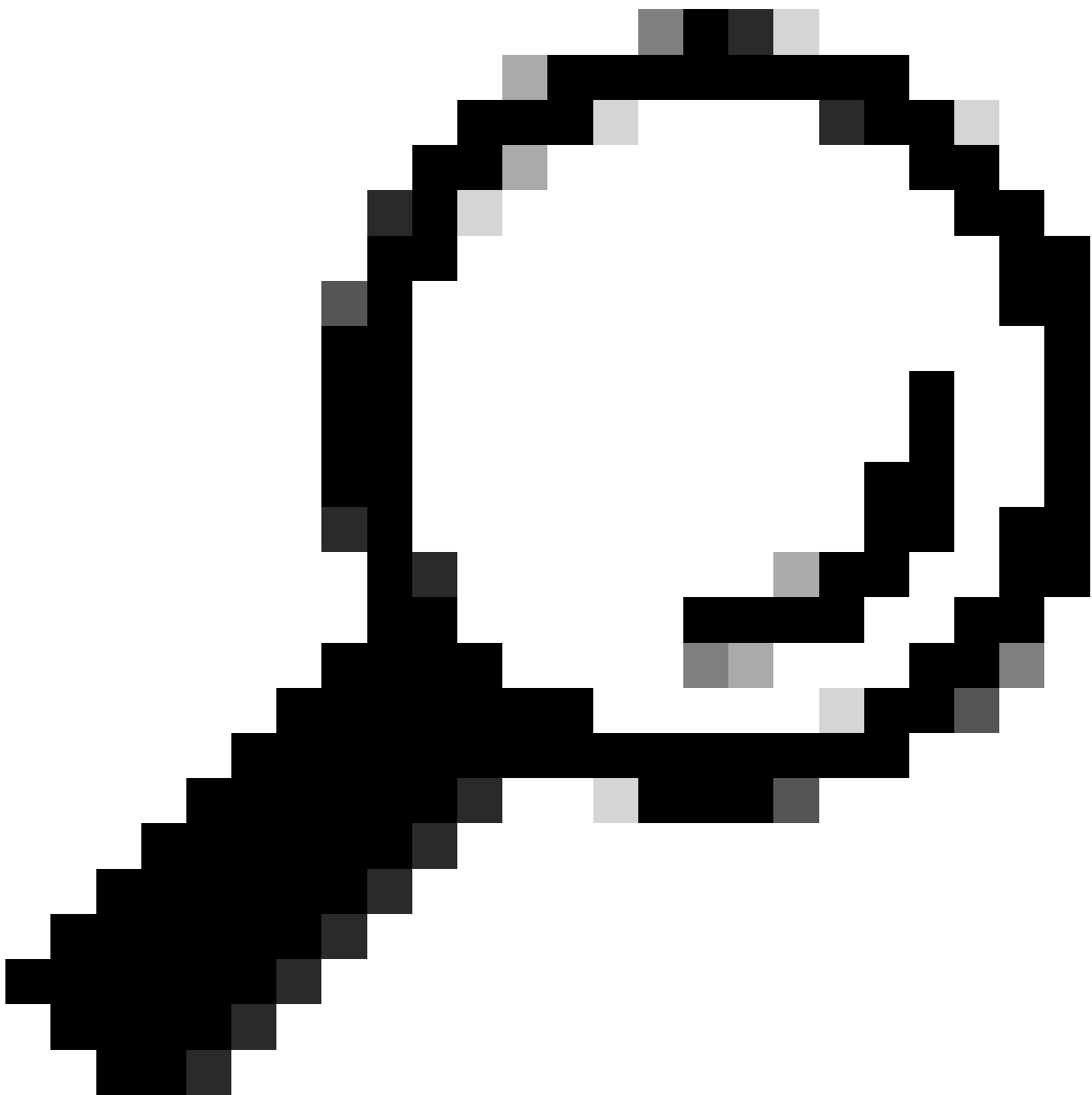


附註：介質可以是語音和/或影片，通過RTP資料包傳輸。

信令元件（裝置或伺服器）確定哪些埠用於傳送或接收媒體（音訊和/或影片）。對於大多數裝置而言，RTP最常見的埠範圍通常介於16384和32767之間。



附註：某些Cisco裝置（如ASR和ISR G3平台，如ISR4K平台）使用標準化的RTP埠範圍8000到48200。驗證裝置上配置的特定RTP埠範圍至關重要，因為它可能與這些標準化值不同，並且可能隨第三方裝置而變化。

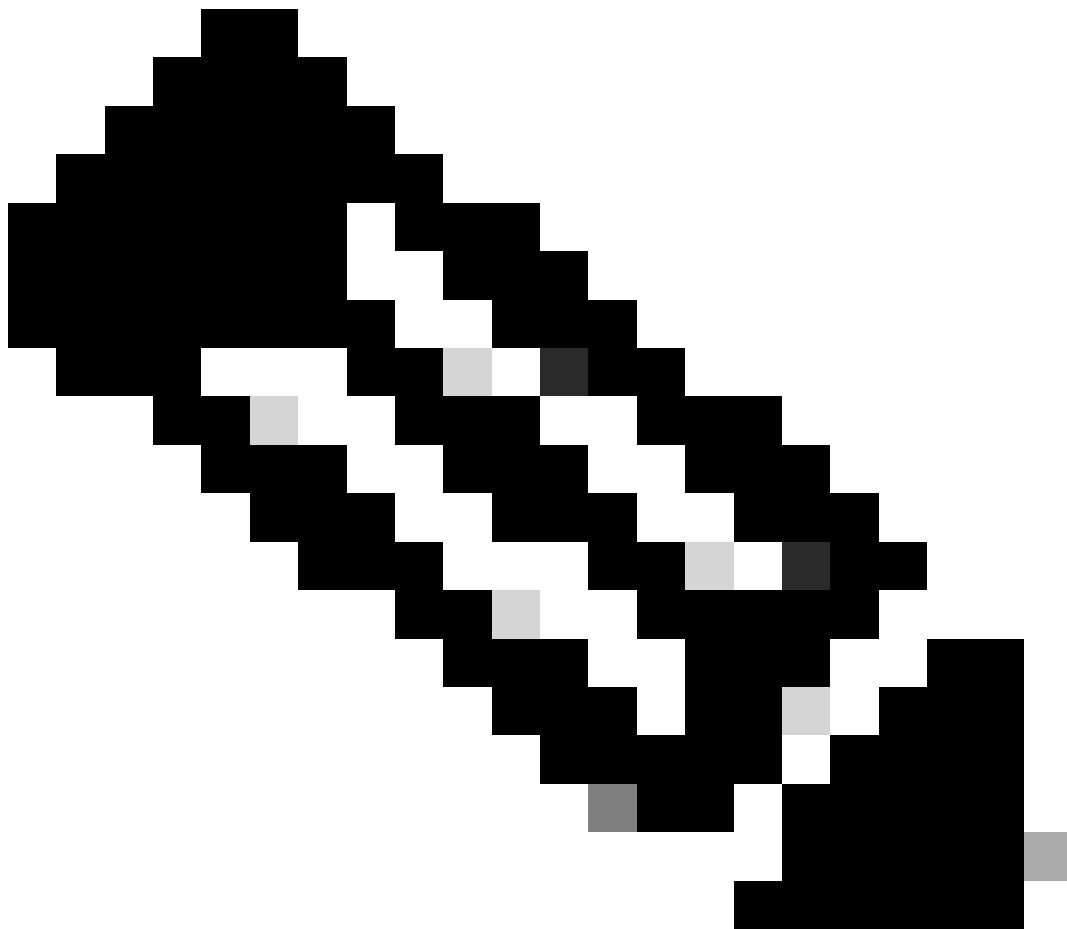
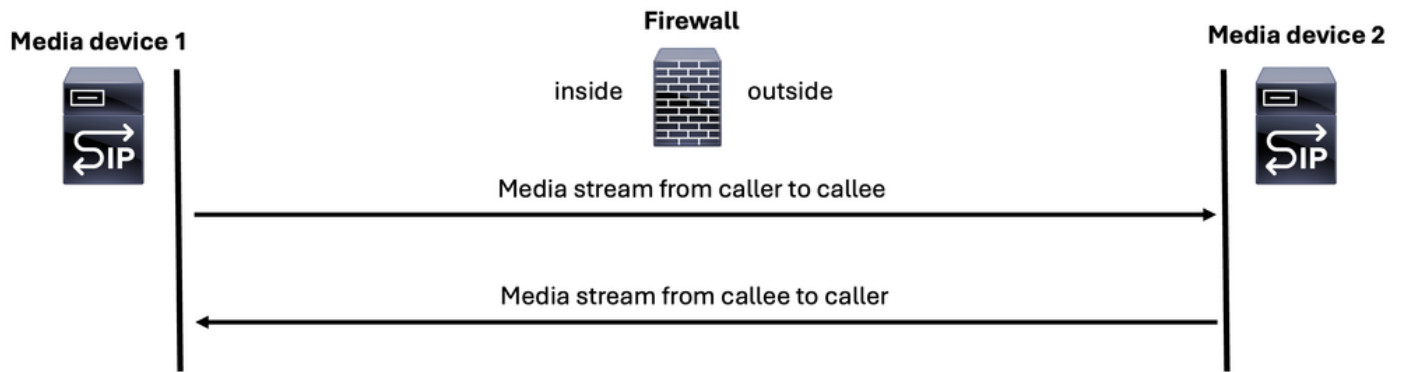


提示：有時RTP路徑與信令路徑不同，因此確定負責傳送和接收語音RTP資料包的裝置至關重要。這可確保捕獲通過ASA或FTD的裝置之間的UDP流量。

正常語音呼叫中生成兩個媒體流或RTP流：

1. 從呼叫方到被呼叫方的一個媒體流
2. 從被叫方到主叫方的一個媒體流

Media for a (VoIP) call



附註：為了便於說明，SIP伺服器圖示用於表示所有映像中的信令伺服器或媒體伺服器。

在語音呼叫中討論媒體流時，必須突出強調兩個關鍵場景：

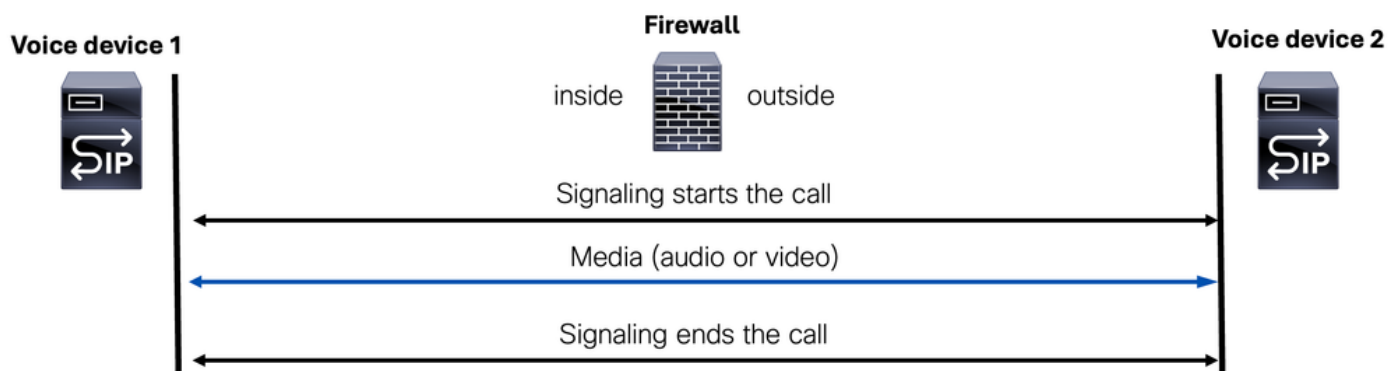
1. 媒體流通

2. 媒體週轉

媒體流通

媒體流傳輸是一種由同一裝置同時處理媒體（語音和/或影片）和信令資料包的模式。

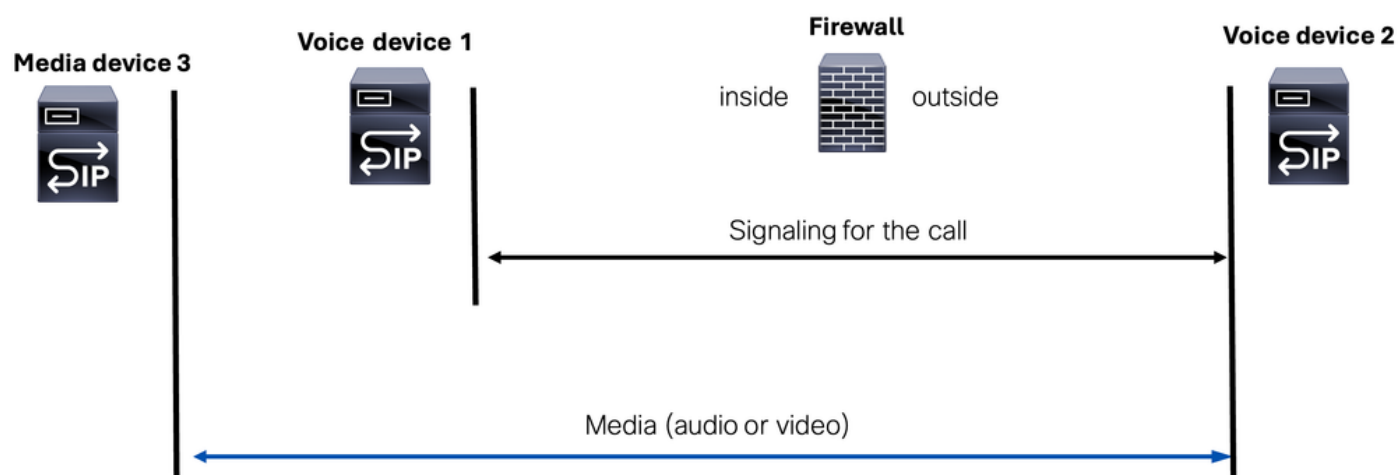
Media Flow-Through



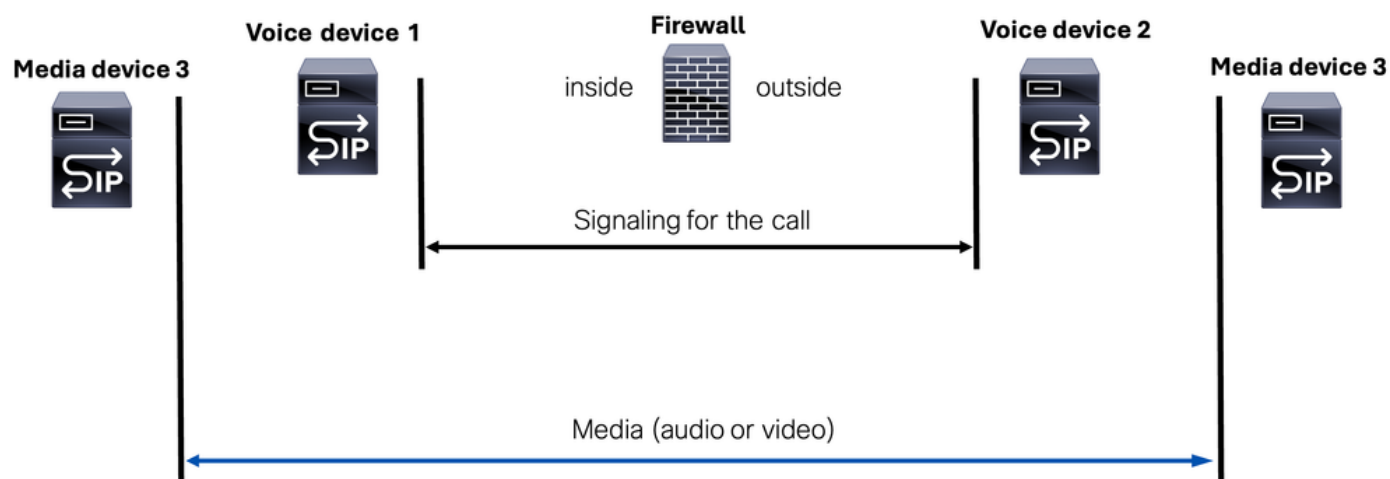
媒體週轉

媒體流繞流是一種模式，其中信令資料包由兩個獨立的信令元件（裝置或伺服器）處理，而媒體流（語音或影片）由稱為媒體裝置的第三裝置管理。

Media Flow-Around(Scenario 1)



Media Flow-Around(Scenario 2)



此模式明確了相關裝置的角色，以及信令和媒體流或裝置之間的區別。

附註：在排除所建立的訪問清單可能允許信令元件（裝置或伺服器）時，這一點尤其重要，但如果媒體流使用其他媒體裝置，則我們需要允許它以及我們的FW裝置的訪問清單。

作業階段啟始通訊協定(SIP)

SIP是由Internet工程任務組(IETF)在RFC 3261中定義的應用層控制協定。

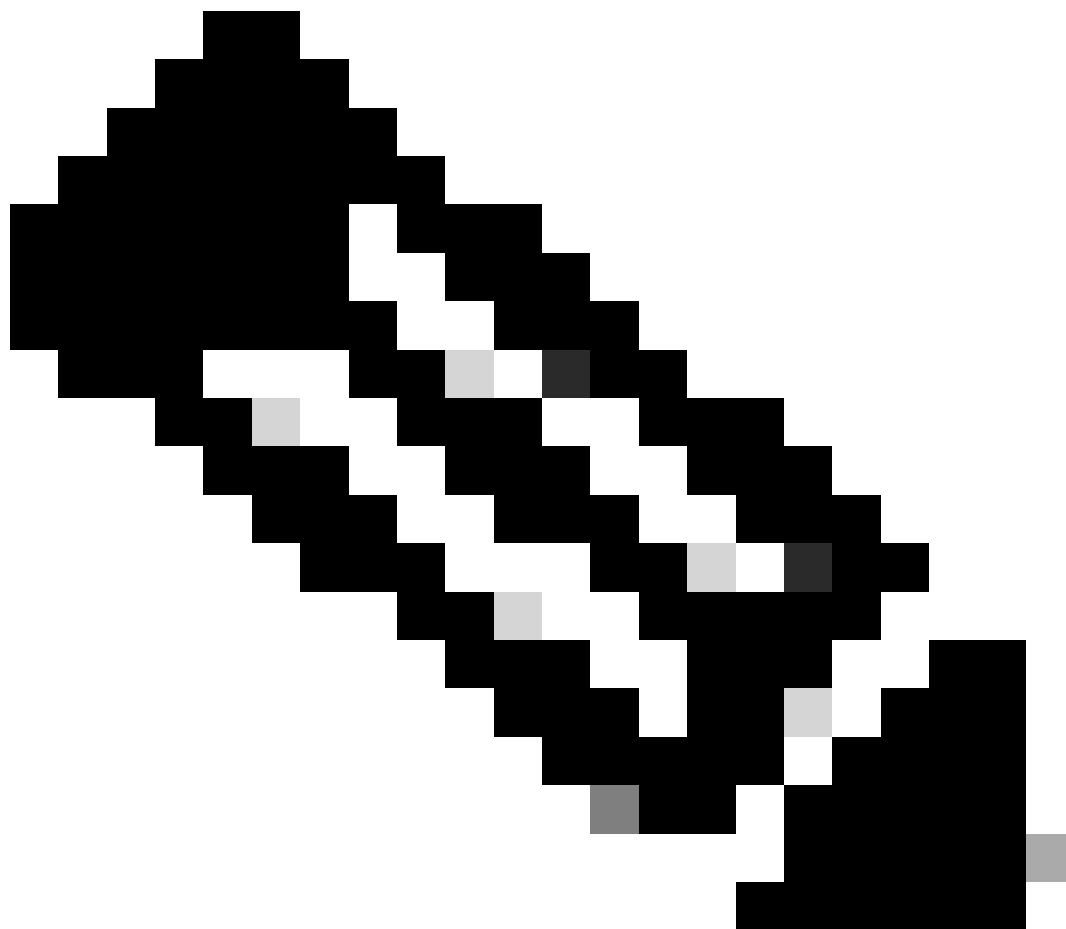
SIP是一種基於文本的協定。這意味著SIP消息由人類可讀的文本組成，類似於HTTP的運行方式。

SIP是專為處理封包電話網路中的訊號傳送和作業階段管理功能而設計的。

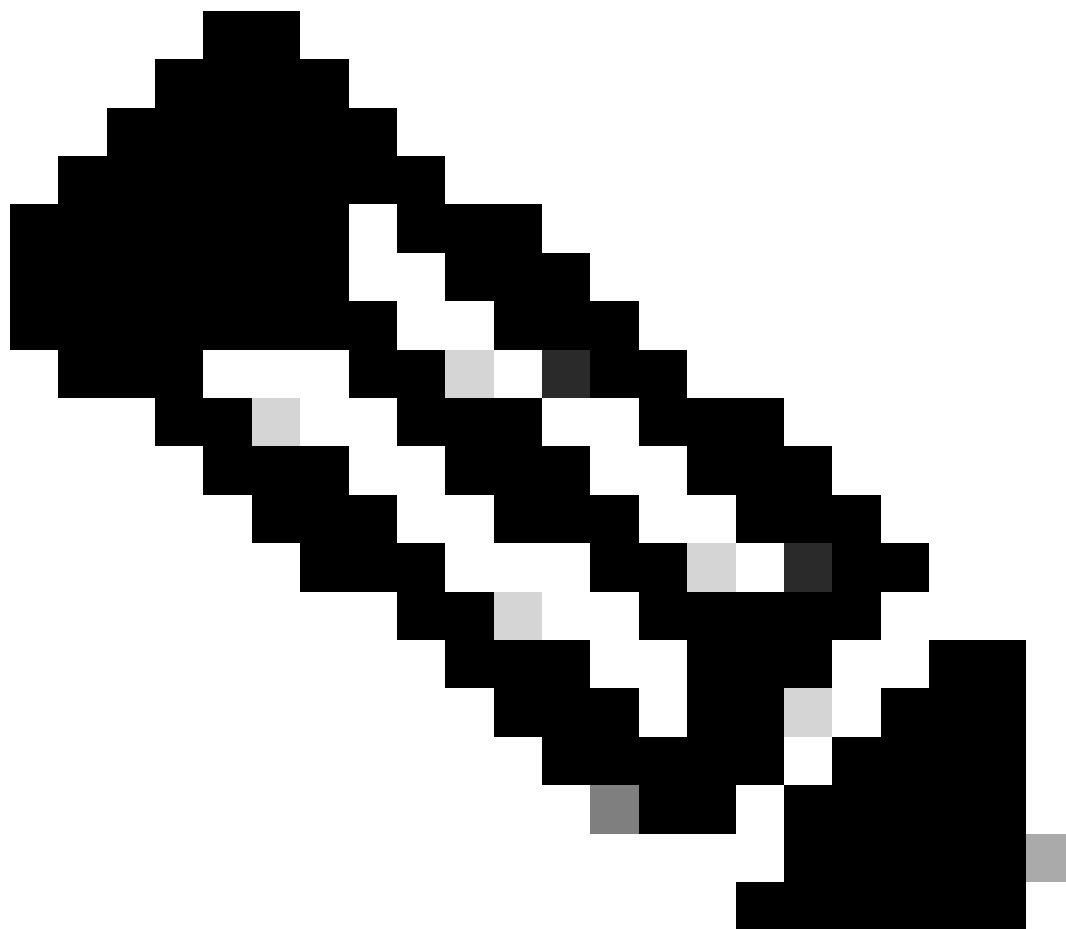
SIP可以：

- 建立呼叫
- 修改呼叫
- 終止呼叫

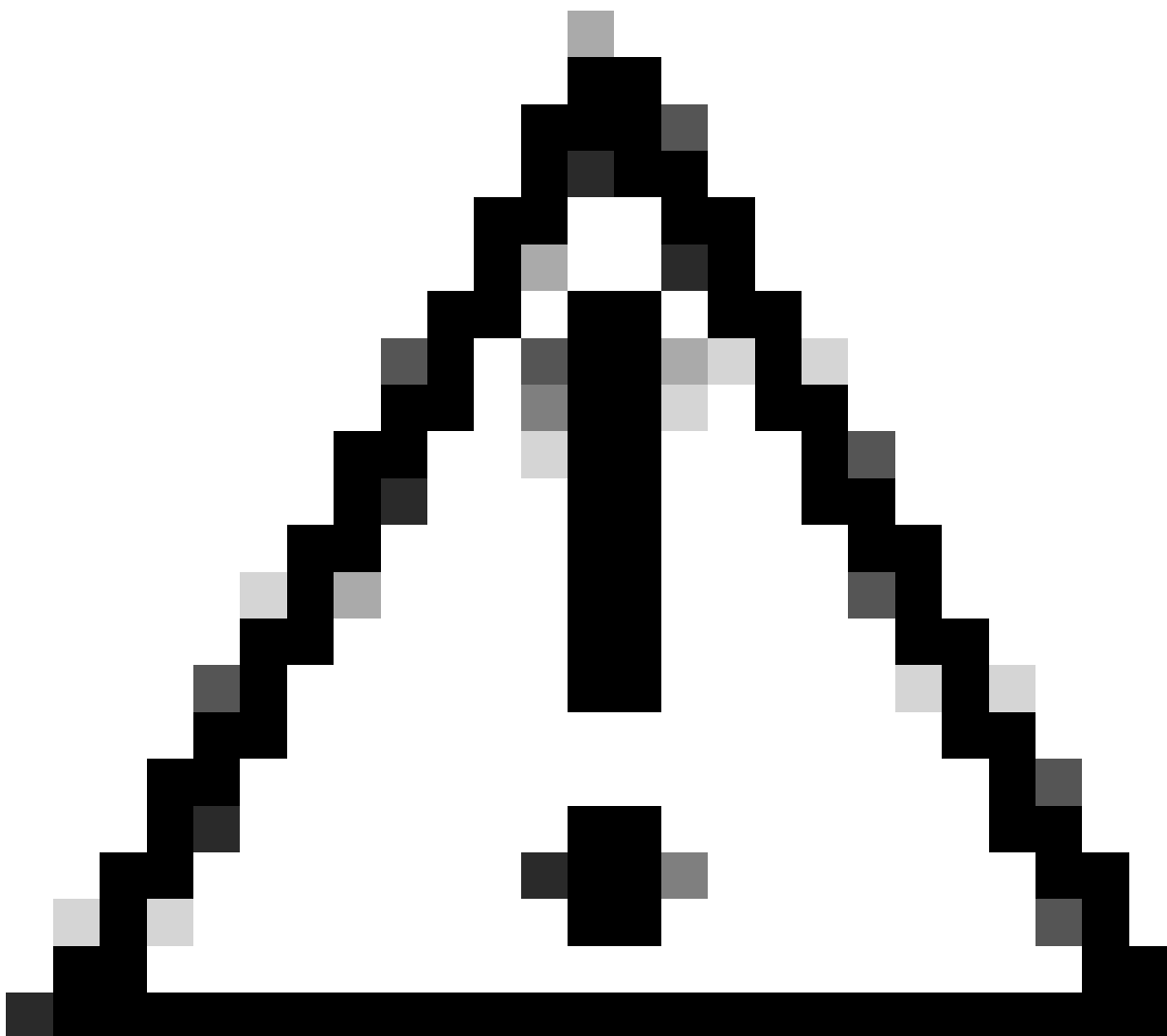
SIP可以在標準化埠5060上使用UDP或TCP。如果SIP是使用傳輸層安全(TLS)加密的，則可以使用標準埠5061。



附註：當SIP訊號經過加密時，在ASA或FTD裝置上的封包擷取中看不到實際的SIP封包。但是，您仍然能夠觀察SIP客戶端和SIP伺服器裝置之間的TCP握手和TLS握手。



附註：思科安全防火牆威脅防禦(FTD)和安全防火牆自適應安全裝置(ASA)預設啟用SIP檢測。



注意：請一律確認用來傳送訊號的連線埠。請記住，SIP協定通常使用埠5060或5061，但某些部署可能偏離這些標準，並且對SIP協定使用不同的埠。

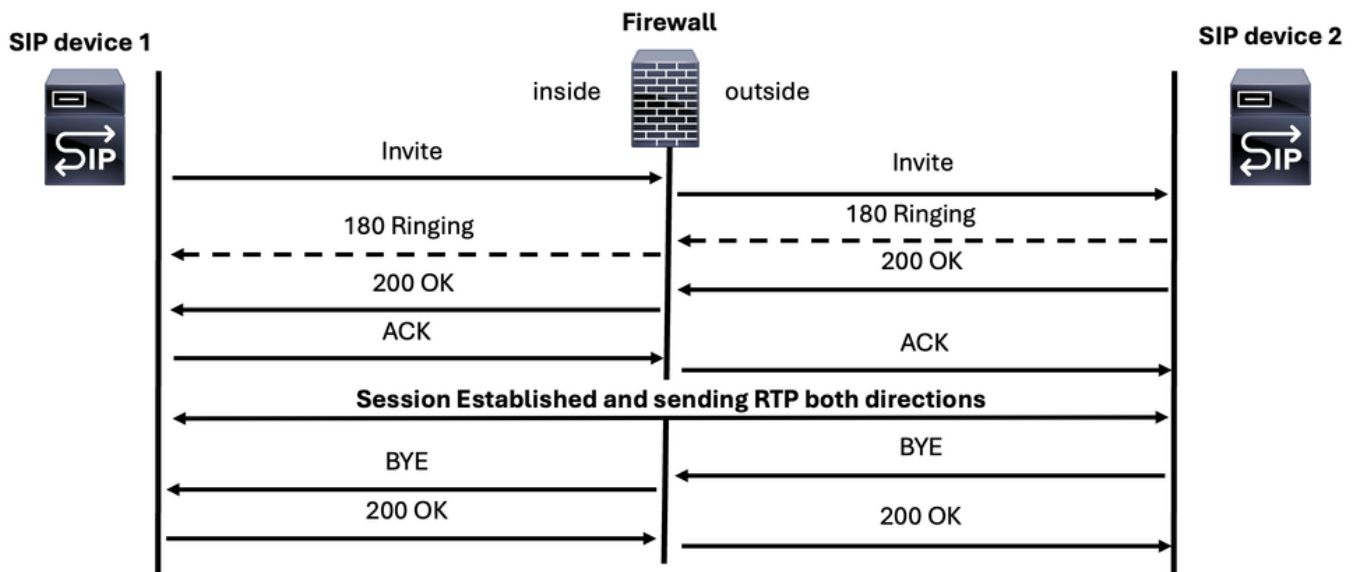
排除SIP信令問題時，可以找到三種方案：

- SIP呼叫信令消息
- SIP OPTION消息
- SIP註冊消息

SIP呼叫消息

用於建立和結束語音呼叫的主要SIP消息如下：

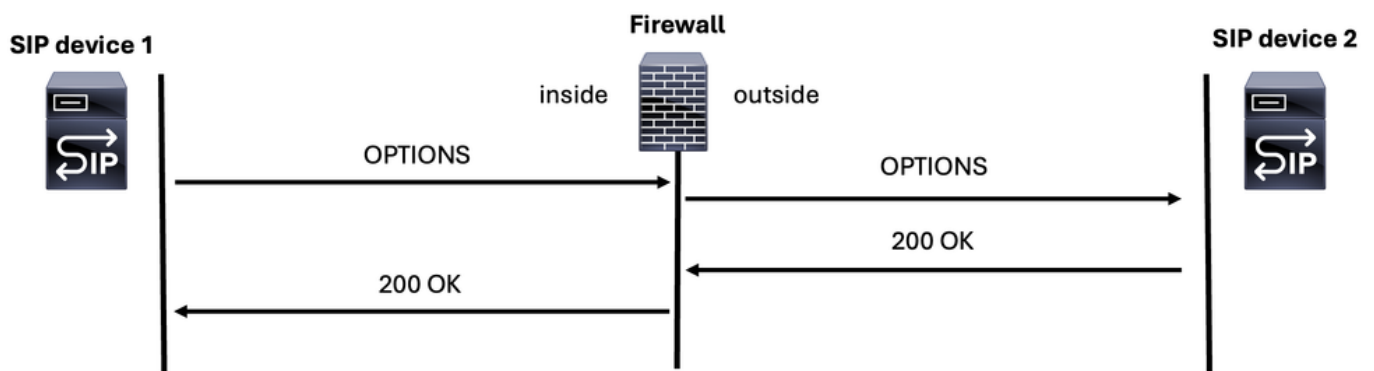
SIP Call messages



SIP選項消息

SIP OPTIONS消息對於確定SIP裝置是否線上並能夠響應非常重要。它類似於ping ICMP消息，但在SIP世界上。

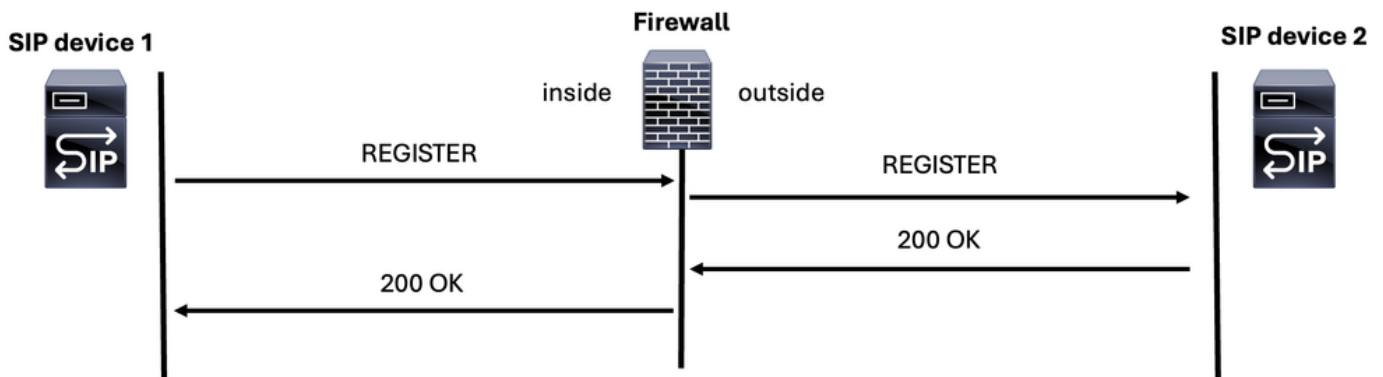
SIP OPTIONS Message



SIP註冊消息

在防火牆故障排除會話期間可以找到的另一條SIP消息是SIP REGISTER消息，它使裝置能夠向SIP伺服器註冊。

SIP REGISTER Message



此封包擷取顯示來自兩個SIP裝置的要求與回應，以及媒體（語音）流量：

No.	Time	Source	Destination	Protocol	Length	Info
4316	17.259331	208.10.1.52	10.0.0.99	SIP/SDP	1264	Request: INVITE sip:306@10.0.0.100:5060;transport=udp
4322	17.270515	10.0.0.99	208.10.1.52	SIP	669	Status: 100 Trying
4324	17.279166	10.0.0.99	208.10.1.52	SIP	1046	Status: 180 Ringing
4894	20.065503	10.0.0.99	208.10.1.52	SIP/SDP	1451	Status: 200 OK (INVITE)
4902	20.101588	208.10.1.52	10.0.0.99	SIP	873	Request: ACK sip:306@10.0.0.100:5060
4918	20.171759	208.10.1.52	10.0.0.99	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x2FA83E48, Seq=9514, Time=22816
4922	20.191646	208.10.1.52	10.0.0.99	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x2FA83E48, Seq=9515, Time=22976
4927	20.211818	208.10.1.52	10.0.0.99	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x2FA83E48, Seq=9516, Time=23136
4932	20.231744	208.10.1.52	10.0.0.99	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x2FA83E48, Seq=9517, Time=23296
4937	20.251687	208.10.1.52	10.0.0.99	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x2FA83E48, Seq=9518, Time=23456
4941	20.271675	208.10.1.52	10.0.0.99	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x2FA83E48, Seq=9519, Time=23616
4946	20.284842	10.0.0.99	208.10.1.52	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x8748B06B, Seq=27262, Time=1926491183, Mark
4947	20.284903	10.0.0.99	208.10.1.52	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x8748B06B, Seq=27263, Time=1926491343

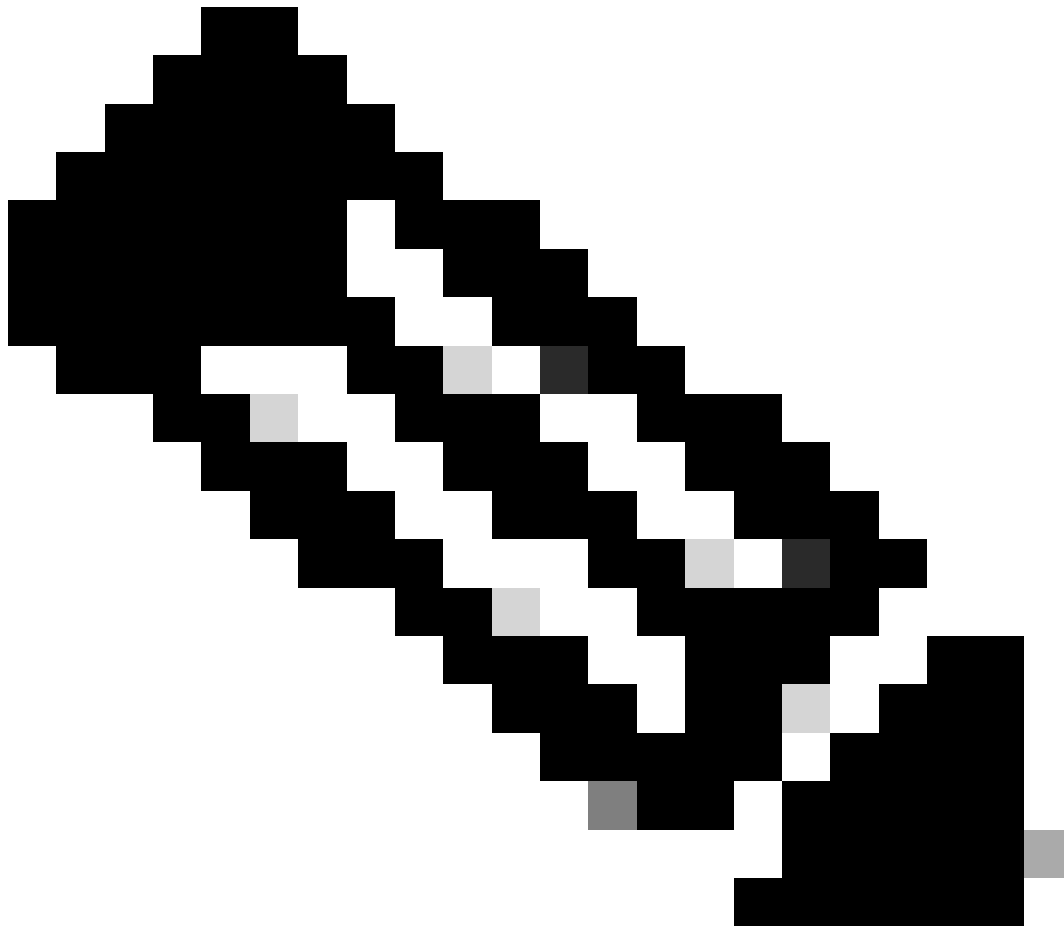
> Frame 4316: 1264 bytes on wire (10112 bits), 1264 bytes captured (10112 bits) on 0
> Ethernet II, Src: Cisco_68:05:20:10:10:10, Dst: Cisco_08:00:20:10:10:10
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 105
> Internet Protocol Version 4, Src: 208.10.1.52, Dst: 10.0.0.99
> User Datagram Protocol, Src Port: 5060, Dst Port: 5060
> Session Initiation Protocol (INVITE)

以下是SIP訊號傳送和RTP媒體（語音）流量的範例：

Time	208.10.1.52	10.0.0.99	208.10.1.52	Comment
17.259331	5060	5060	5060	SIP INVITE From: <sip:916@10.0.0.100> To: <sip:306@10.0.0.100>
17.270515	5060	5060	5060	SIP Status 100 Trying
17.279166	5060	5060	5060	SIP Status 180 Ringing
20.065503	5060	5060	5060	SIP Status 200 OK
20.101588	5060	5060	5060	SIP Request INVITE ACK 200 CSeq:298883630
20.171759	9920	9920	40460	RTP, 1329 packets. Duration: 26.56s SSRC: 0x2FA83E48
20.284842	9920	9920	40460	RTP, 1323 packets. Duration: 26.40s SSRC: 0x8748B06B
46.695954	5060	5060	5060	SIP Request BYE CSeq:298883631
46.699936	5060	5060	5060	SIP Status 200 OK

作業階段說明通訊協定(SDP)

作業階段說明通訊協定(SDP)是一種標準表示，用於說明多媒體作業階段的媒體流。它本身不傳輸介質，但用於在端點之間協商介質型別和格式。SDP與作業階段啟始通訊協定(SIP)結合使用，用於管理和交涉作業階段的媒體特徵。



附註：MGCP包含了SDP的概念，用於同樣的目的。

以下是SIP協定中的SDP消息示例：

```
INVITE sip:2003@192.168.245.9:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.245.6:5060;branch=z9hGXX5763
Remote-Party-ID:
```

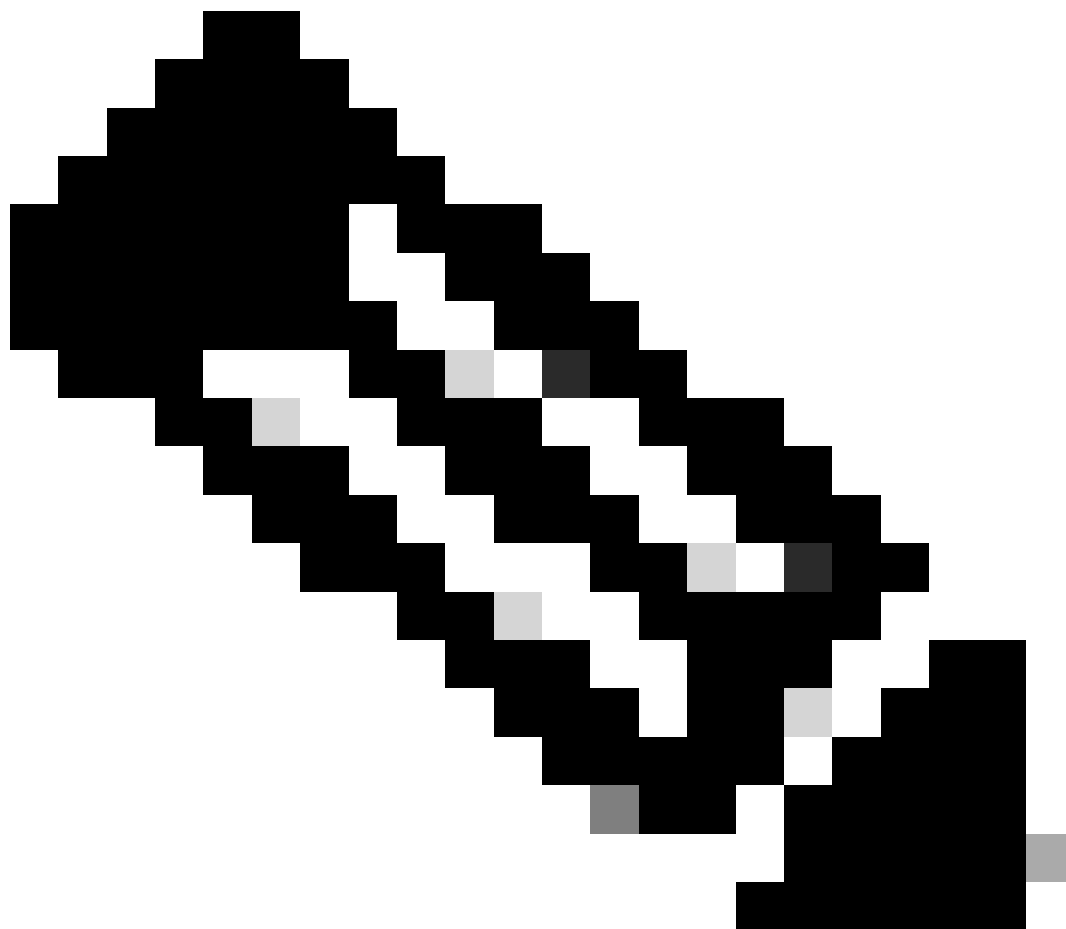
```
      ;party=calling;screen=no;privacy=off
From:
```

```
      ;tag=4E3XXC-A9F
To:
```

Date: Thu, 17 Aug 2025 13:48:52 GMT
Call-ID: 2A7BE22B-XXXXXXXX-XXXXXXXX-F940DC75@192.168.245.6
Supported: 100rel,timer,resource-priority,replaces,sdp-anat
Min-SE: 1800
Cisco-Guid: 0350227076-XXXXXXXX-XXXXXXXX-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



附註：在示例中，某些SDP消息包含以下引數：

++c-IN IP4:媒體伺服器的IP地址

++m=音訊：這表示媒體型別為音訊。

++8266:這是用於傳送音訊流的埠號。

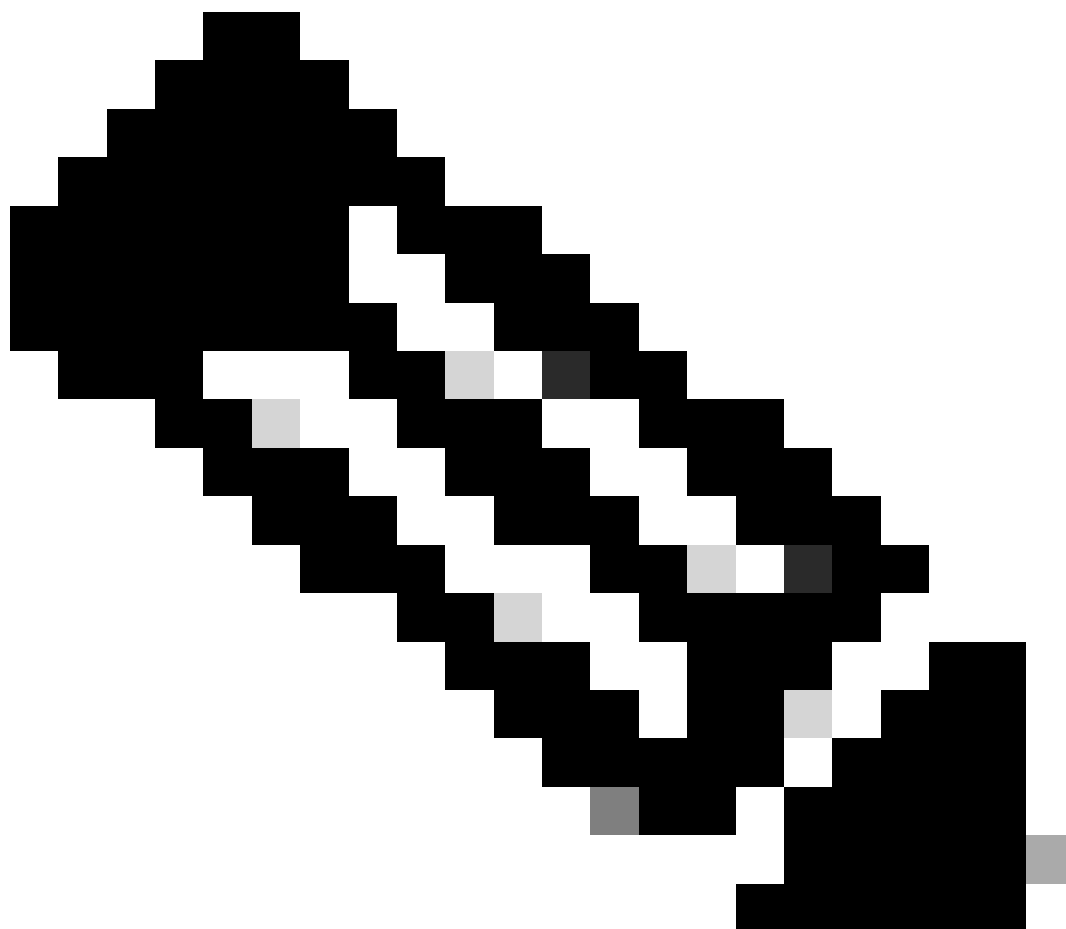
++RTP/AVP:這指定傳輸協定，即使用音訊/影片配置檔案(AVP)的RTP。

++18 127:以下是音訊編解碼器的負載型別。負載型別18通常對應於G.729編解碼器，而127是動態負載型別，可以根據終端之間的協商分配給編解碼器。

可以在以下幾種SIP消息中找到會話描述協定(SDP):INVITE、183 Session in Progress、200 OK、ACK等。SDP充當各方之間交換語音和/或影片功能的應答方法。在排查呼叫問題時，必須瞭解三個主要概念：

1. 提早發盤

2. 延遲提供
 3. 早期媒體
-

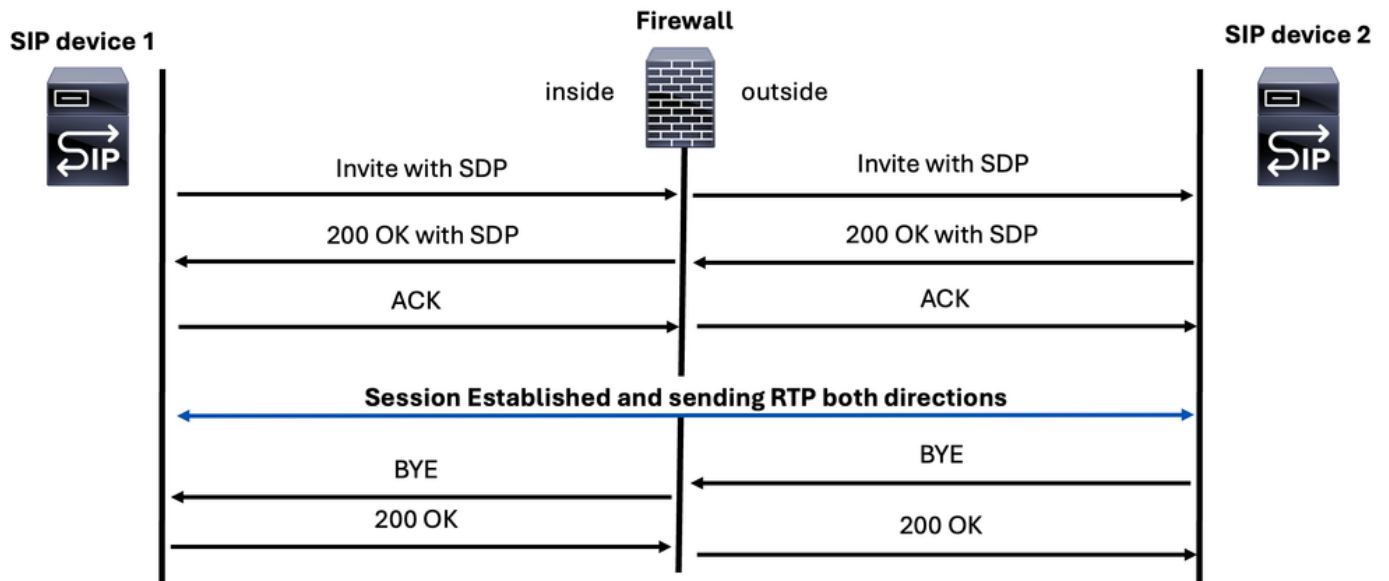


附註：瞭解SDP消息的目標至關重要，因為防火牆上的檢查功能不僅可以修改SIP報頭中的IP地址，而且還可以修改SDP部分中的IP地址。

提早發盤

在INVITE和200 OK SIP消息中找到SDP上的媒體引數。

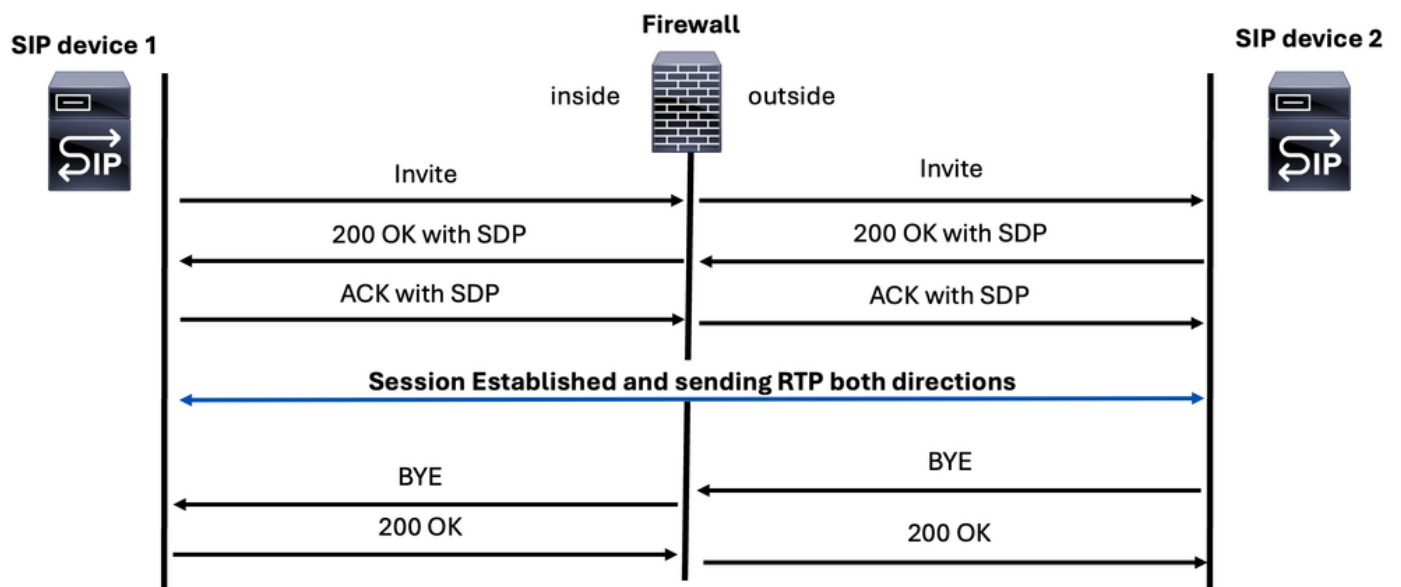
SIP Early Offer Call



延遲提供

在此方法中，在200 OK和ACK SIP消息上找到SDP。

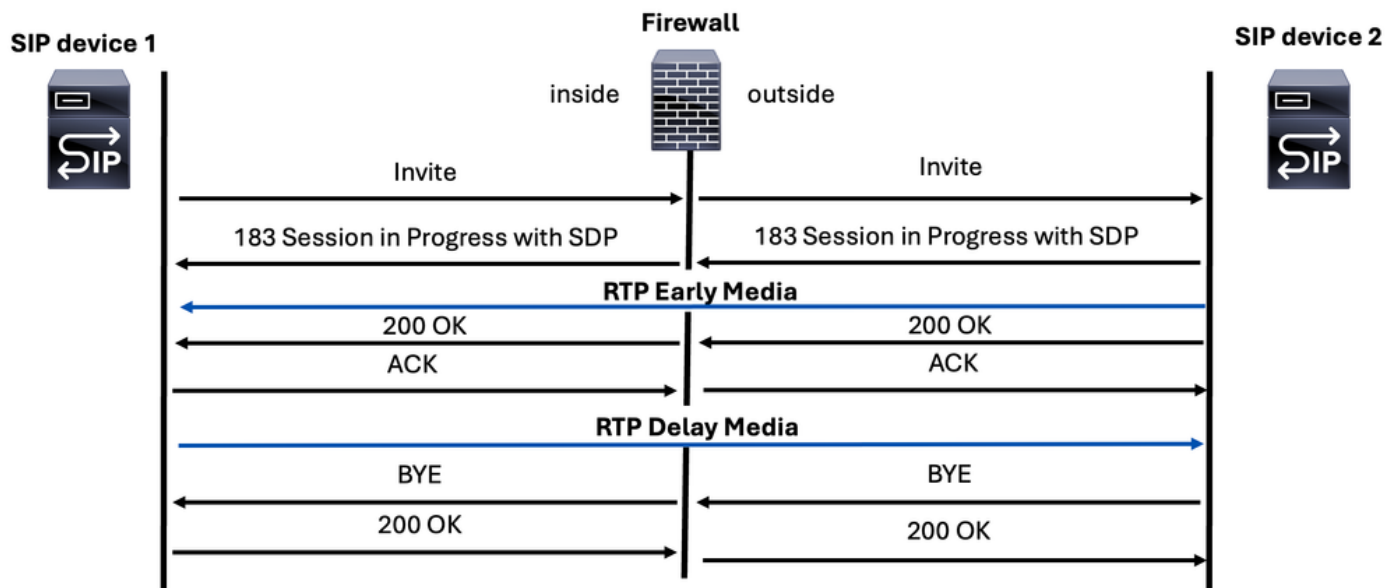
SIP Delay Offer Call



早期媒體

早期介質通過稱為「183會話進度」響應的特定SIP消息傳輸。此消息包含會話描述協定(SDP)，其中包含被叫方的媒體引數。在呼叫正式連線之前，運營商和SIP提供商通常使用它向呼叫者傳送自動語音消息或其他媒體。

SIP Early Media Call



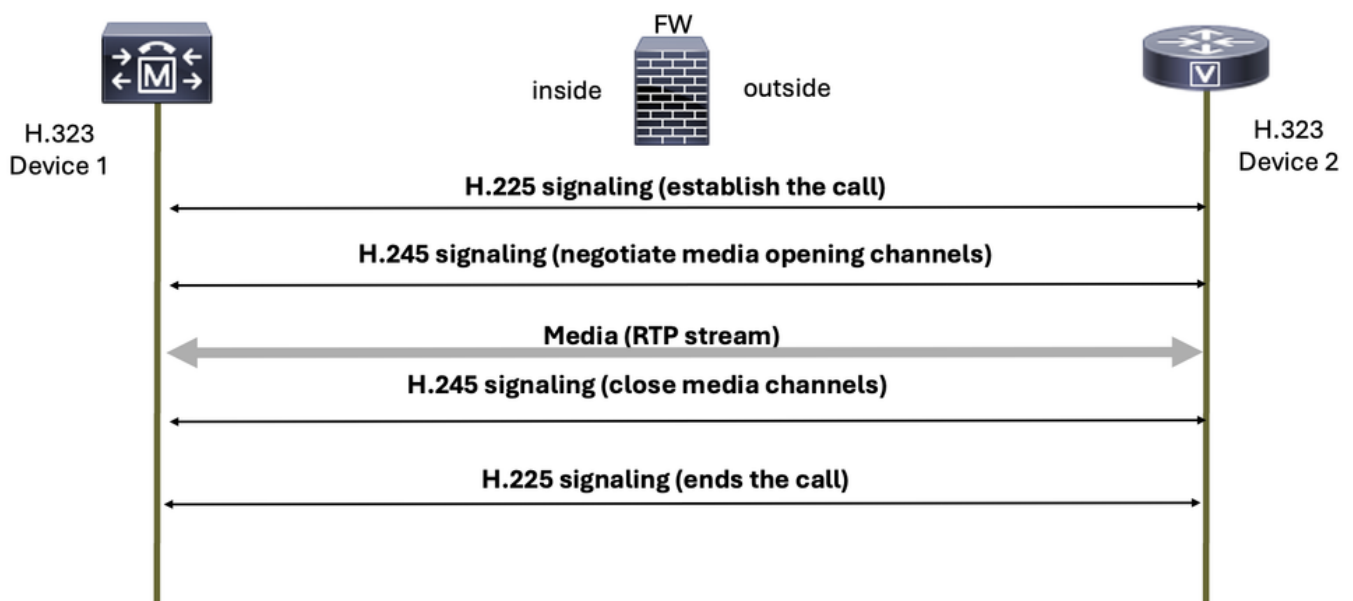
H.323

H.323是由國際電信聯盟(ITU)定義的一組通訊協定，用於透過封包交換網路（例如網際網路）進行語音、視訊和資料通訊。

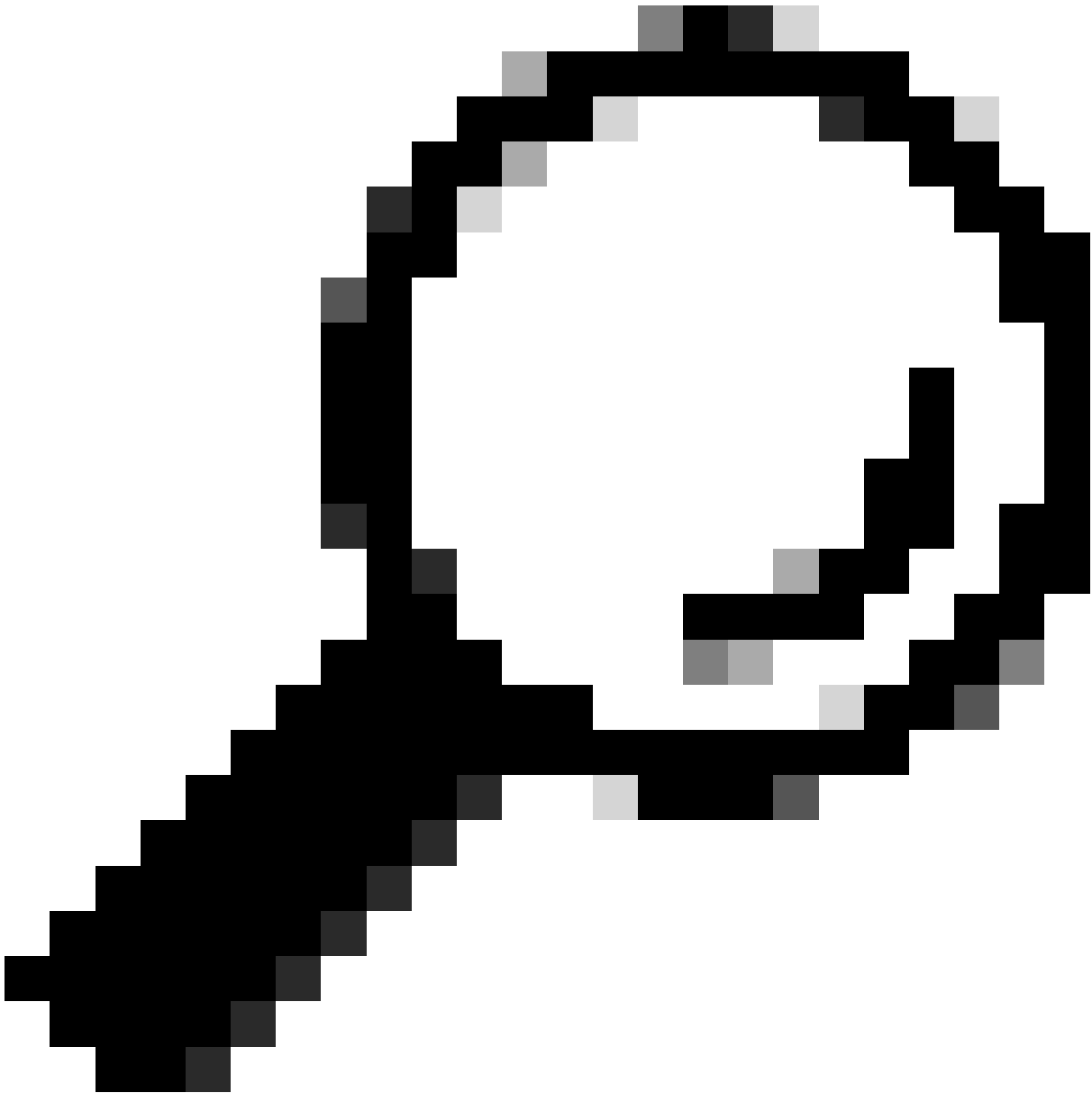
H.323協定由兩個主要元件組成：

1. H.225:這處理呼叫信令，包括呼叫的設定和終止。
2. H.245:負責能力交換以及音訊和影片通道的開啟和關閉。

Basic H.323 signaling



H.323信令協定使用的埠是1718、1719和1720。



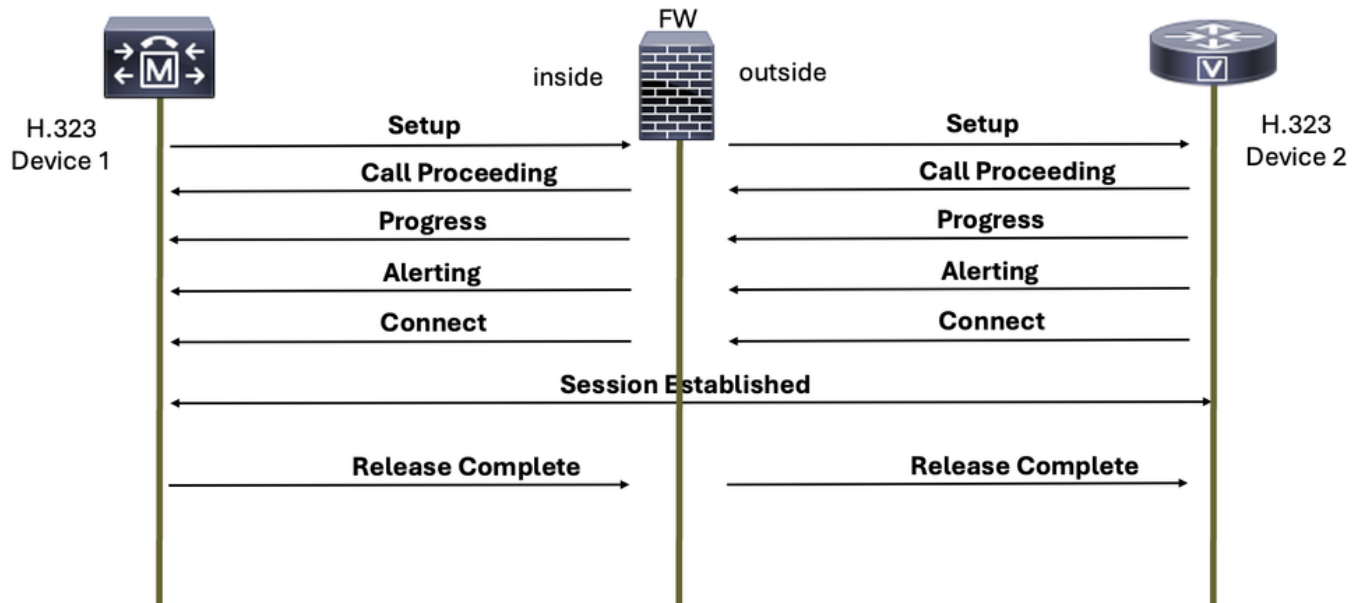
提示：由於使用TLS進行加密，因此安全H.323協定通訊在從UDP切換到TCP時可能會遇到問題，這會導致防火牆錯誤地阻止連線為可疑活動，因此將防火牆配置為允許H.323端點或伺服器的UDP和TCP流量至關重要。

H.323協定有兩種工作模式：啟動慢啟動快。

H.225

此協定負責建立呼叫並在其中一方掛斷時終止語音呼叫。

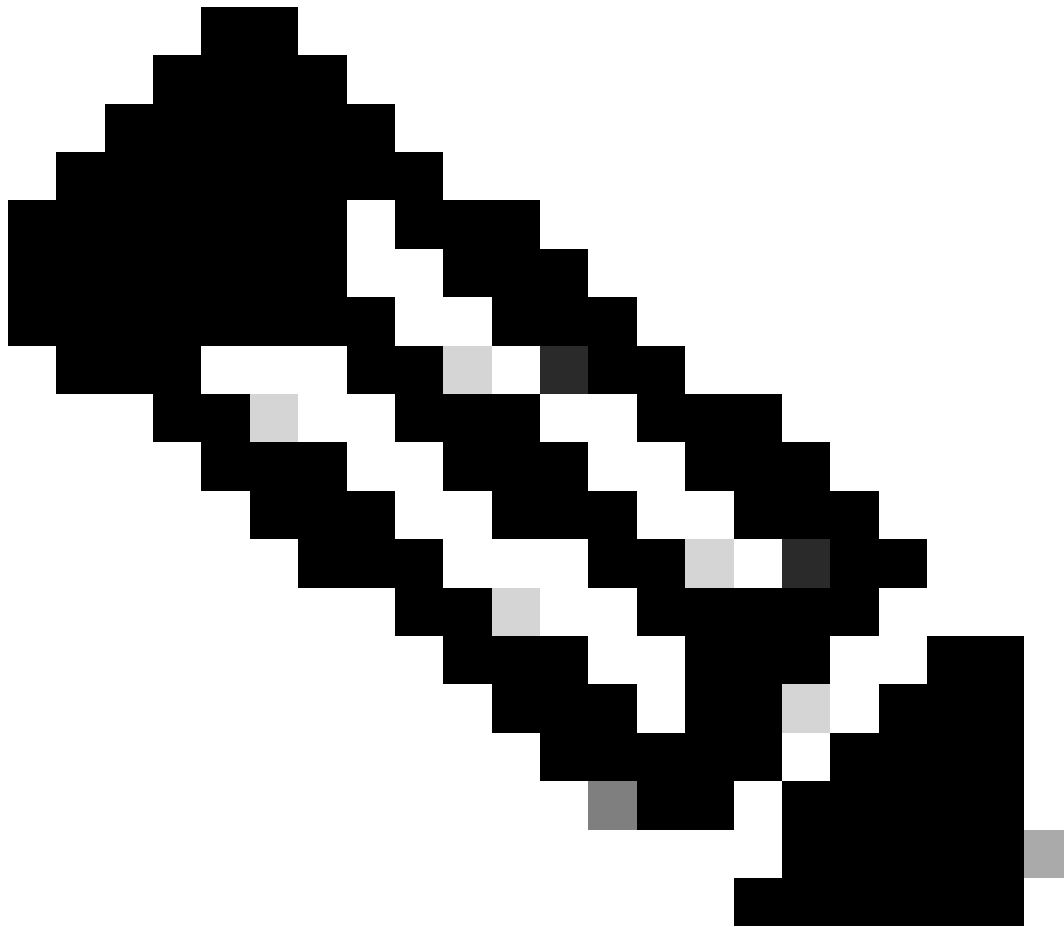
Basic H.225 Call Setup Signaling



H.245

H.245提供以下功能：

- 終端功能交換
- 主/從確定
- 邏輯通道訊號

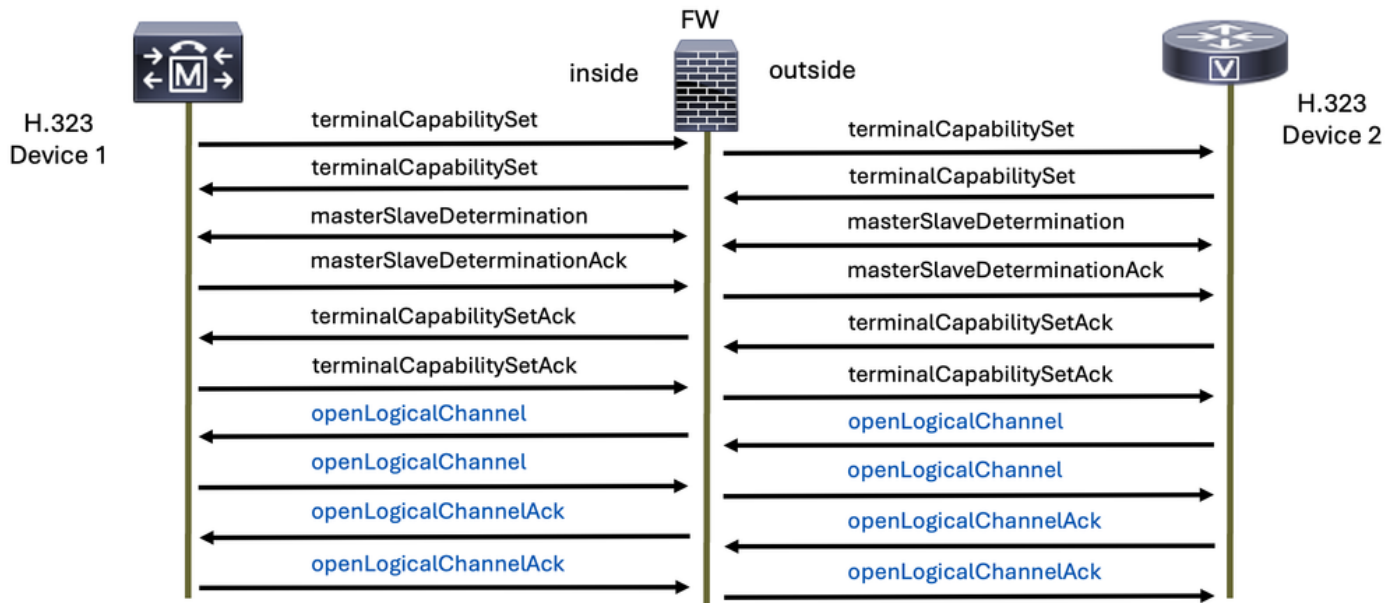


附註：本文檔中使用的「主和從」一詞已硬編碼為原始H.323協定，並不反映公司的策略或價值。我們致力於促進包容和尊重的語言。

在收到H.225連線消息後傳送H.245協定。

此協定有助於確定哪個語音協定用於RTP，並且它是在為其開啟邏輯通道和關閉邏輯通道消息時指定的。

H.245 Signaling



此封包擷取顯示來自兩台H.225和H.245的H.323裝置的要求與回應，以及媒體（語音）流量：

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	terminalCapabilitySetAck
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, Mar
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	17: 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: Vi :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

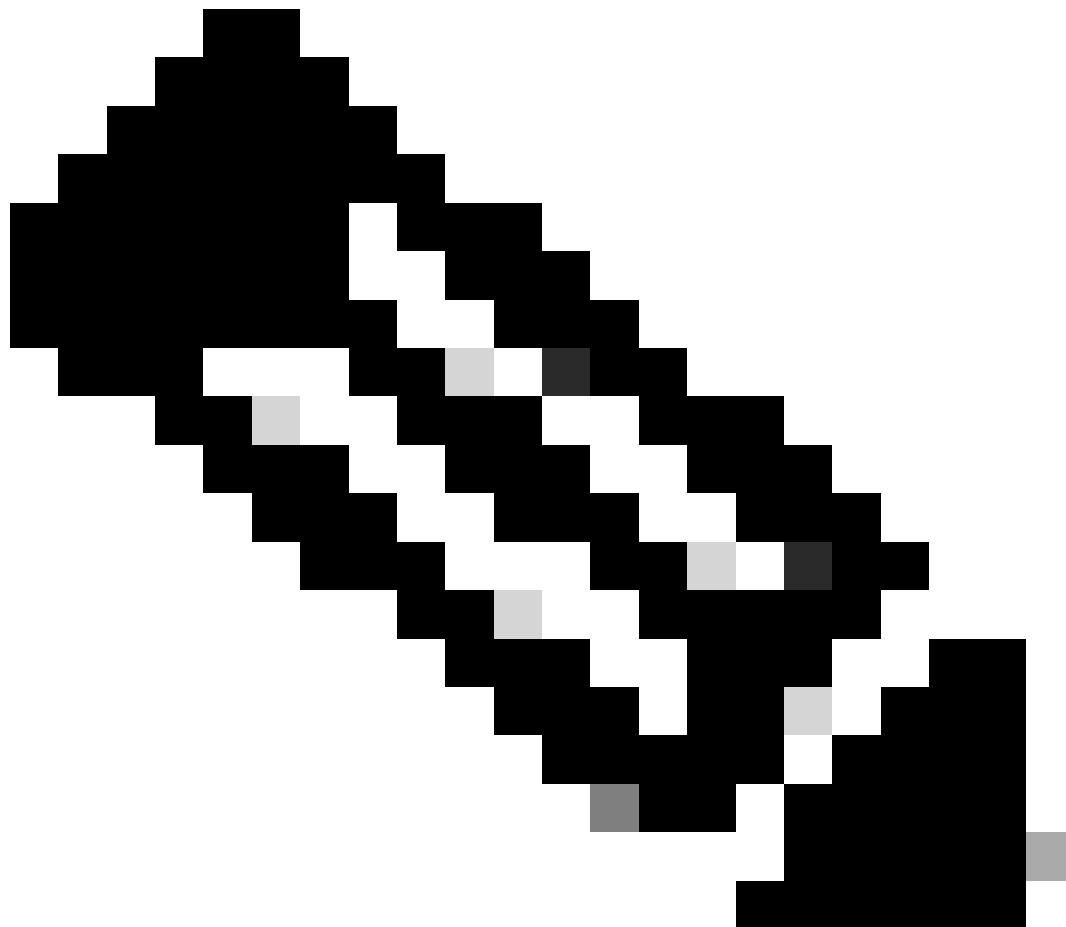
> TPKT, Version: 3, Length: 625

> Q.931

> H.225.0 CS

以下是使用H.225和H.245以及RTP媒體（語音）的H.323訊號傳送流量的範例：

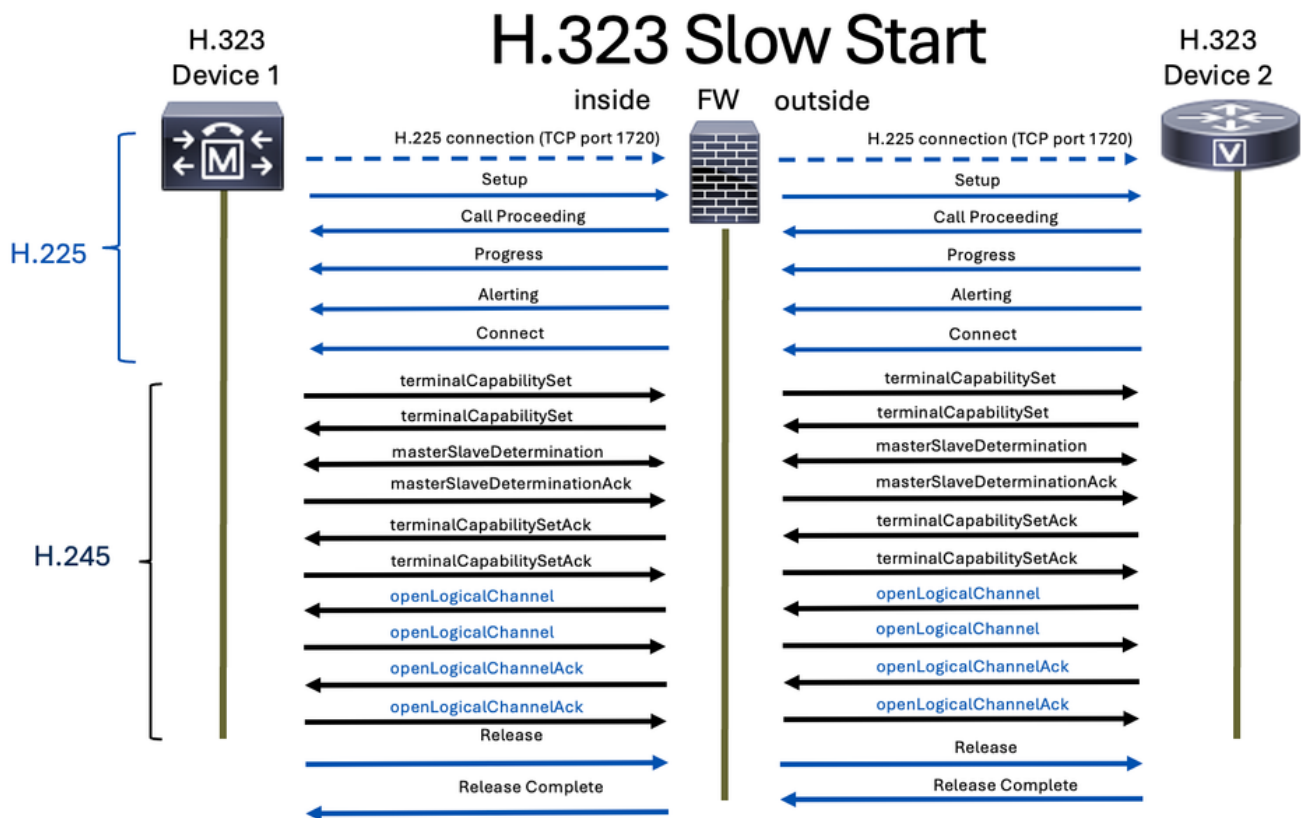
Time	17	58	17	48	1	.57	Comment
1.702966	22502	setup OLC (g711U g711U)	→	1720			H225 From: To:1234 TunnH245:on FS:on
1.711968	22502	callProceeding	←	1720			H225 TunnH245:off FS:off
1.760006	22502	alerting	←	1720			H225 TunnH245:off FS:off
1.760006	22502		←	1720			H225 TunnH245:off FS:off
2.804011	22502	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



附註：思科安全防火牆威脅防禦(FTD)和安全防火牆自適應安全裝置(ASA)預設啟用H.323檢測。

慢啟動

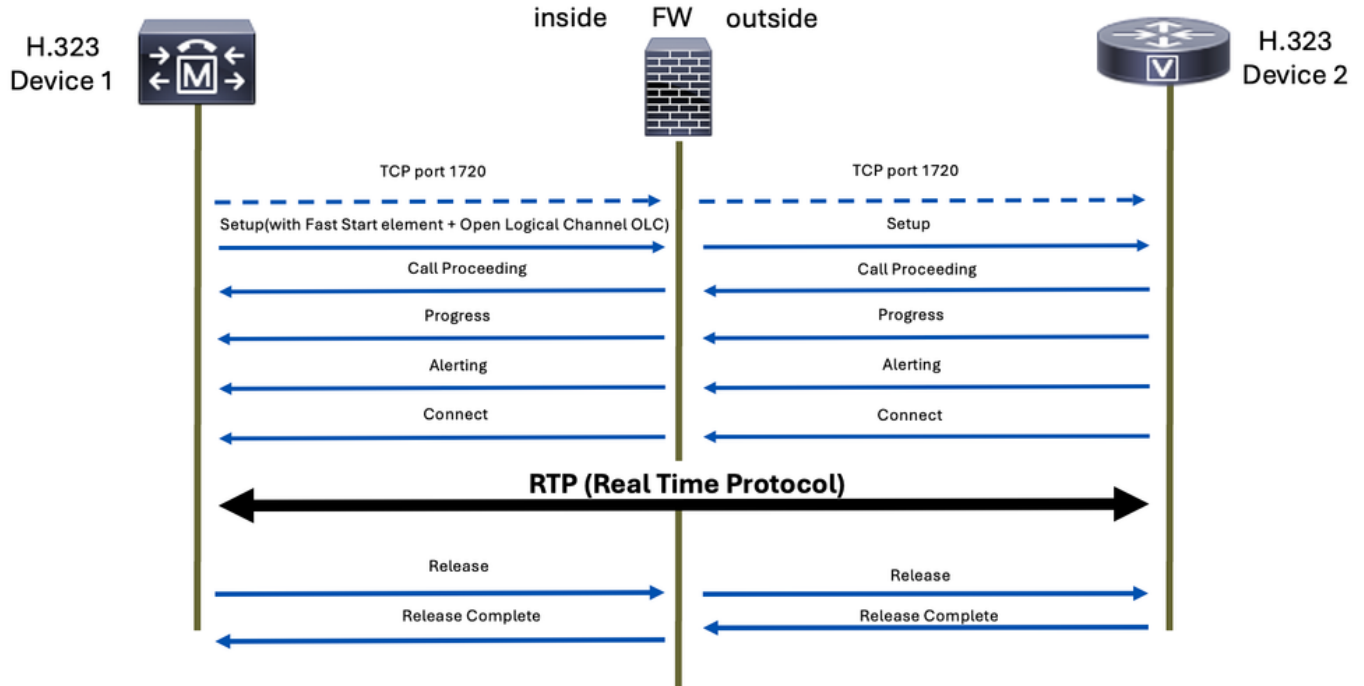
在慢啟動模式中，呼叫建立過程涉及建立媒體通道之前的數個信令步驟。步驟包括設定、呼叫繼續、警報和連線。執行完這些步驟後，H.245媒體協商會單獨執行。這意味著在初始呼叫信令完成之前不會建立媒體通道，這可能導致設定時間更長。



快速啟動

相反，快速啟動模式允許在初始設定消息內進行媒體協商。這意味著可以更快地建立媒體通道，因為協商是在初始呼叫建立過程中完成的。Fast start通過減少交換的消息數以及在建立媒體通道之前所需的處理量來簡化流程。

H.323 Fast Start

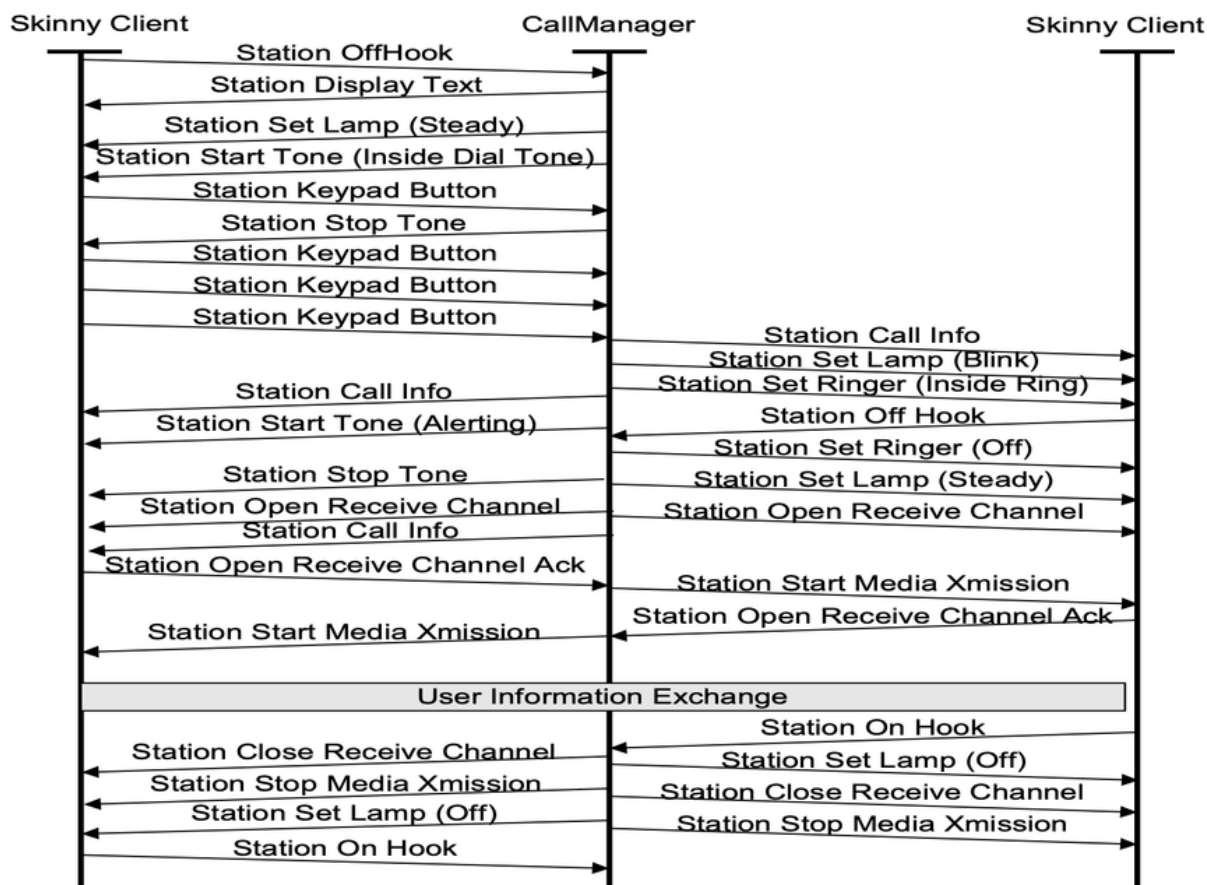


SCCP

瘦客戶端控制協定(SCCP) (通常簡稱為Skinny) 是思科專有的信令協定。它主要由Cisco Unified Communications Manager(CUCM)、Cisco Unified Communications Manager Express(CME)路由器和Cisco IP電話使用，用於促進呼叫的設定和控制。

SCCP協定在埠2000上將TCP用於非安全SCCP，在埠2443上使用安全SCCP。

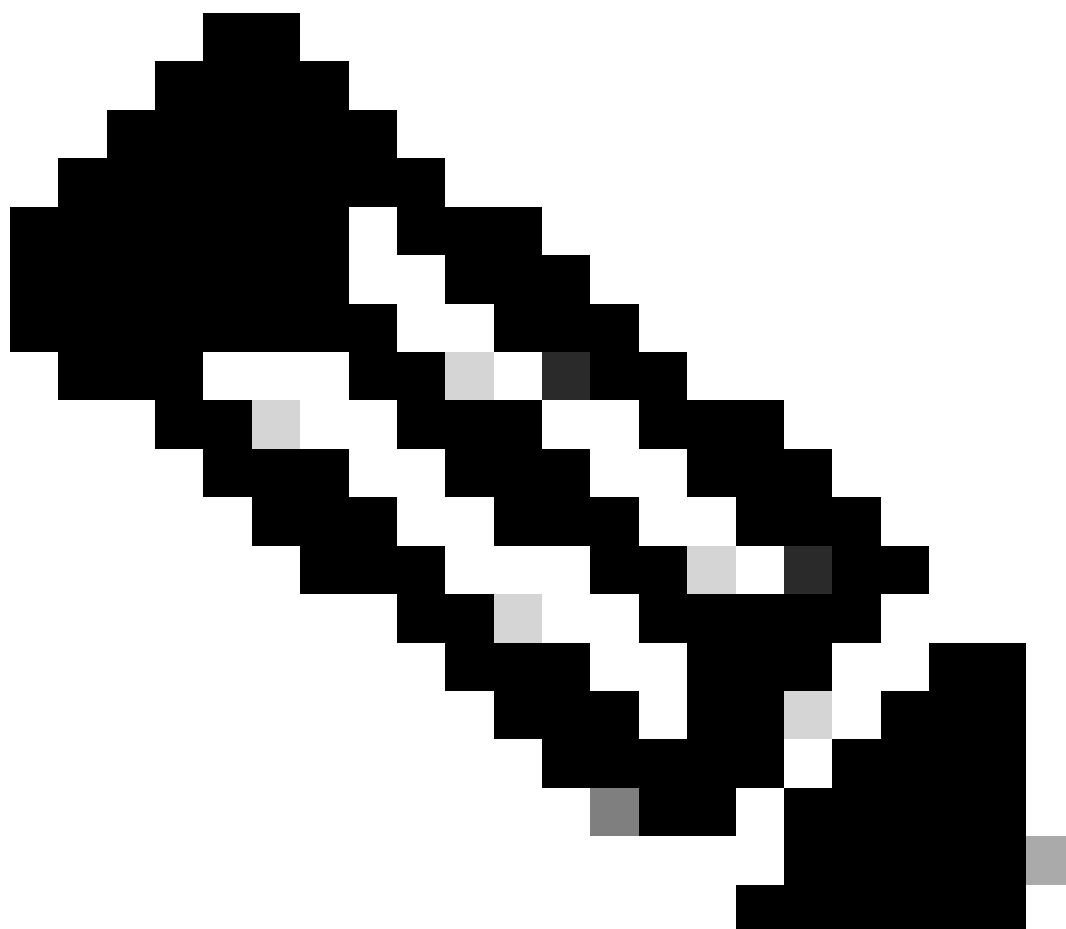
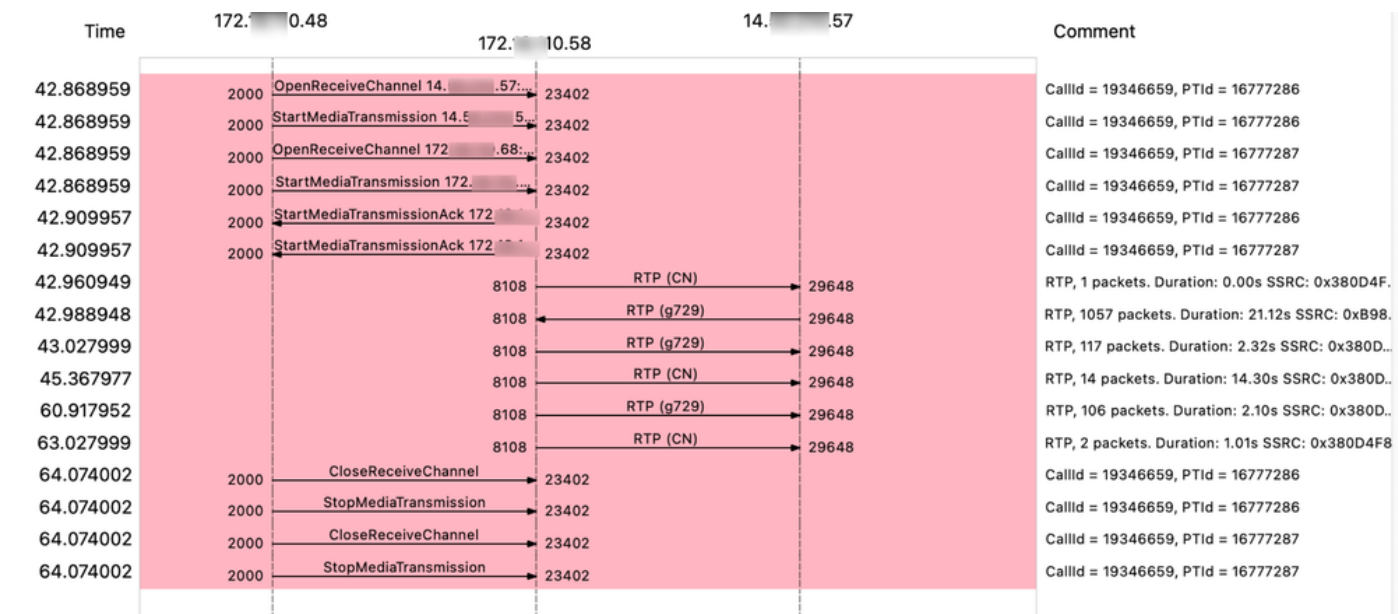
以下是可以在SCCP呼叫中找到的常見SCCP消息：



此封包擷取顯示來自兩個SCCP裝置的要求及回應，以及媒體（語音）流量：

No.	Time	Source	Destination	Protocol	Length	Info
42	11.170041	172.17.0.48	172.17.0.58	SKINNY/REQ	202	OpenReceiveChannel
58	13.307028	172.17.0.48	172.17.0.58	SKINNY/REQ	202	StartMediaTransmission
59	13.307028	172.17.0.48	172.17.0.58	SKINNY/REQ	202	OpenReceiveChannel
60	13.307028	172.17.0.48	172.17.0.58	SKINNY/REQ	202	StartMediaTransmission
62	13.309042	172.17.0.58	172.17.0.48	SKINNY/RESP	110	StartMediaTransmissionAck
64	13.309042	172.17.0.58	172.17.0.48	SKINNY/RESP	158	OpenReceiveChannelAck StartMediaTransmissionAck
66	13.390031	14.51.0.57	172.17.0.58	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7B4D4E5D, Seq=54086, Time=2101901655, Mark
67	13.409027	14.51.0.57	172.17.0.58	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7B4D4E5D, Seq=54087, Time=2101901815
68	13.429031	14.51.0.57	172.17.0.58	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7B4D4E5D, Seq=54088, Time=2101901975
69	13.451033	14.51.0.57	172.17.0.58	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7B4D4E5D, Seq=54089, Time=2101902135
70	13.453031	172.17.0.58	14.51.0.57	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x50, Seq=0, Time=585879569

以下是SCCP訊號傳送和RTP媒體（語音）流量的範例：



附註：思科安全防火牆威脅防禦(FTD)和安全防火牆自適應安全裝置(ASA)預設啟用 SCCP檢測。

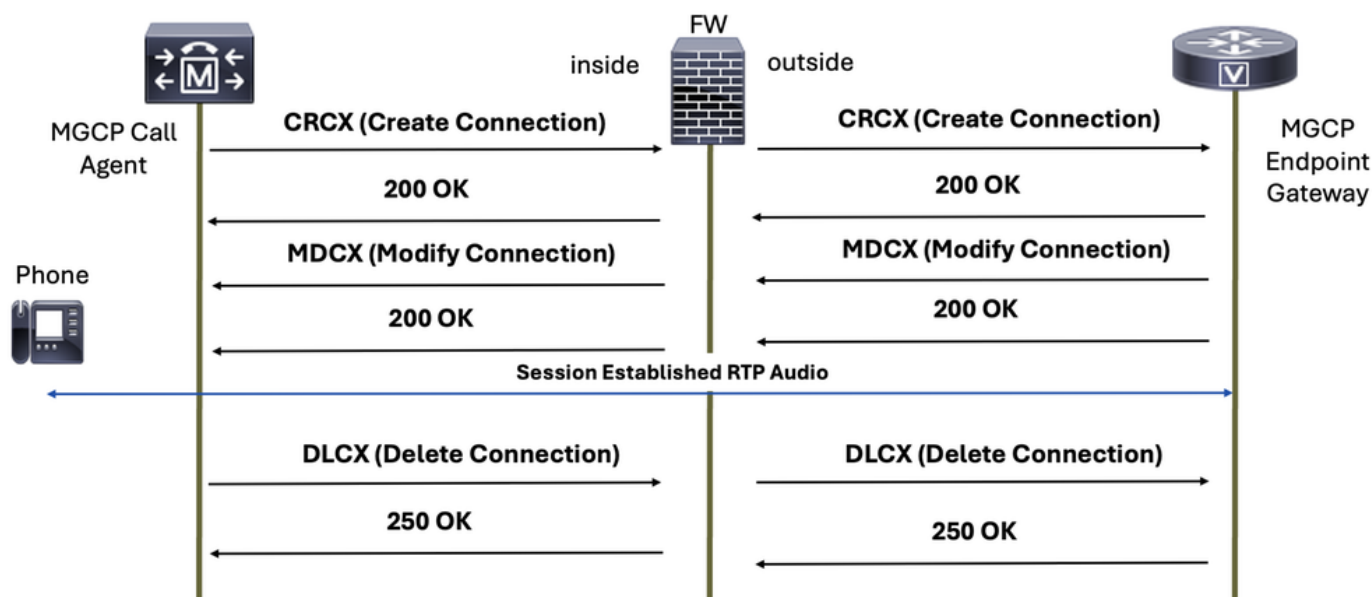
MGCP

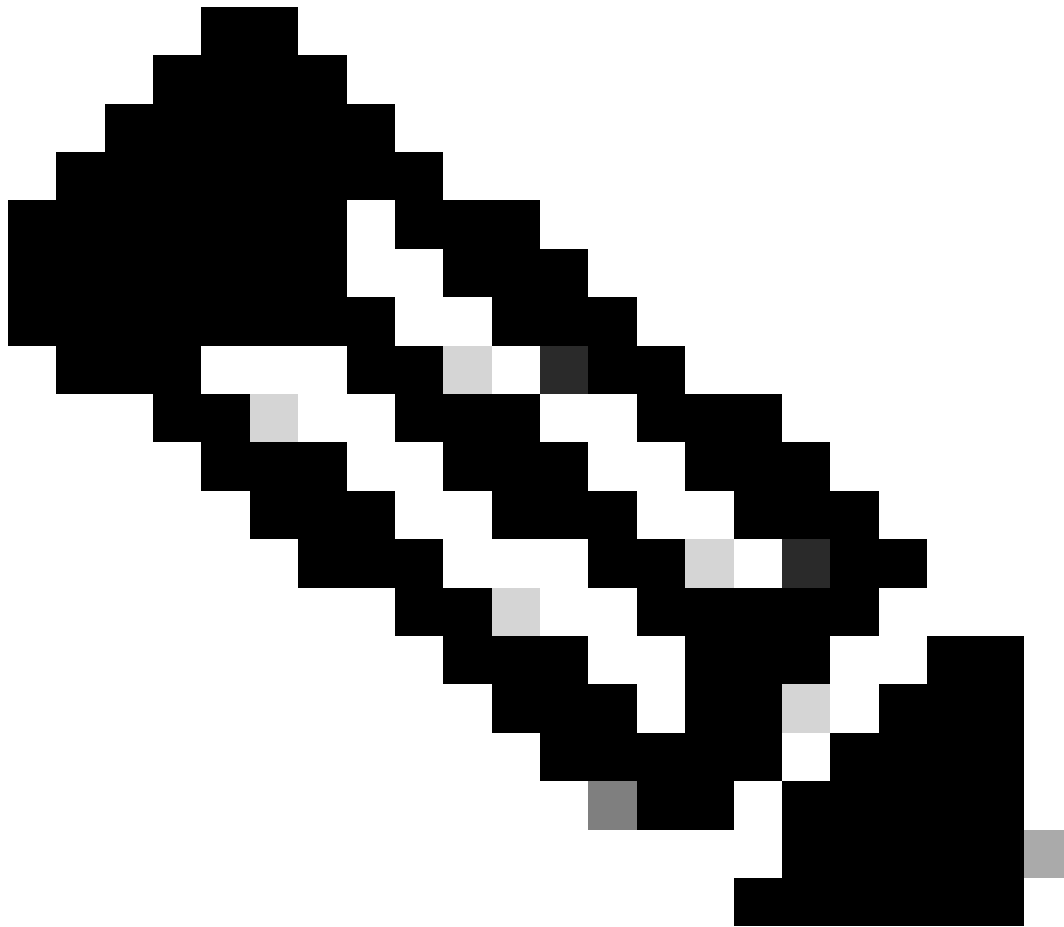
媒體閘道控制通訊協定(MGCP)是用來由通話控制裝置 (例如CUCM) 控制VoIP通話的通訊協定。

MGCP信令協定在RFC 2705中定義，使用TCP埠2428和UDP埠2427進行通訊。

您期望呼叫通訊的MGCP正常資料包為：

MGCP Call Setup Signaling



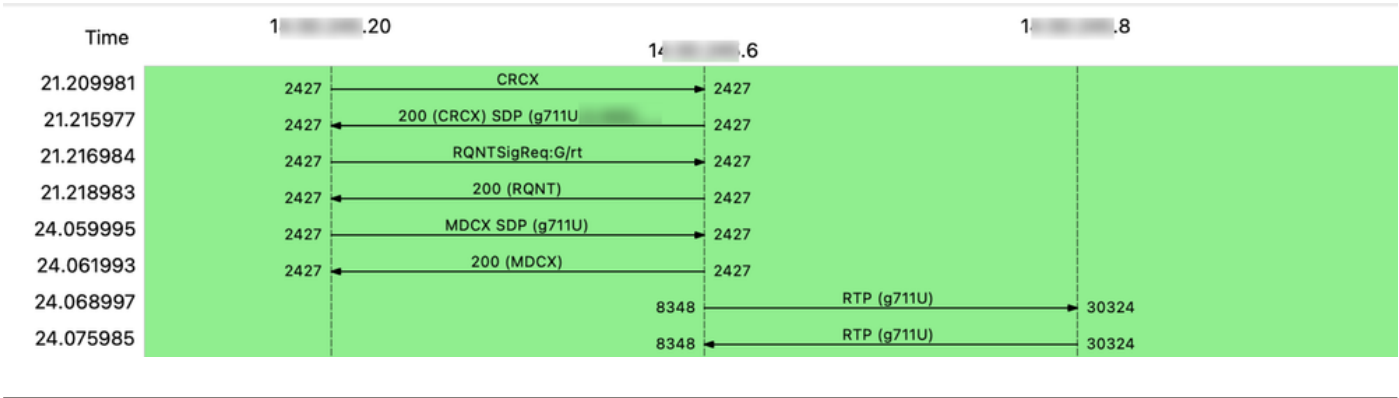


附註：思科安全防火牆威脅防禦(FTD)和安全防火牆自適應安全裝置(ASA)上的預設檢查策略中未啟用MGCP檢查，因此，如果需要此檢查，必須啟用它。

此封包擷取顯示來自兩個MGCP裝置的要求及回應，以及媒體（語音）流量：

No.	Time	Source	Destination	Protocol	Length	Info
12	21.209981	10.10.10.20	10.10.10.6	MGCP	213	CRCX 509 S0/SU1/DS1-0/1@ MGCP 0.1
13	21.215977	10.10.10.6	10.10.10.20	MGCP/SDP	213	200 509 OK
14	21.216984	10.10.10.20	10.10.10.6	MGCP	144	RQNT 511 S0/SU1/DS1-0/1@ MGCP 0.1
18	21.218983	10.10.10.6	10.10.10.20	MGCP	57	200 511 OK
20	24.059995	10.10.10.20	10.10.10.6	MGCP/SDP	342	MDCX 513 S0/SU1/DS1-0/1@ MGCP 0.1
21	24.061993	10.10.10.6	10.10.10.20	MGCP	57	200 513 OK
22	24.068997	10.10.10.6	10.10.10.8	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0xF22F508, Seq=5377, Time=584785512
23	24.075985	10.10.10.8	10.10.10.6	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0xF22F508, Seq=39645, Time=128207581
24	24.088985	10.10.10.6	10.10.10.8	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0xF22F508, Seq=5378, Time=584785672
25	24.095988	10.10.10.8	10.10.10.6	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0xF22F508, Seq=39646, Time=128207741
26	24.108988	10.10.10.6	10.10.10.8	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0xF22F508, Seq=5379, Time=584785832
27	24.115991	10.10.10.8	10.10.10.6	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0xF22F508, Seq=39647, Time=128207901

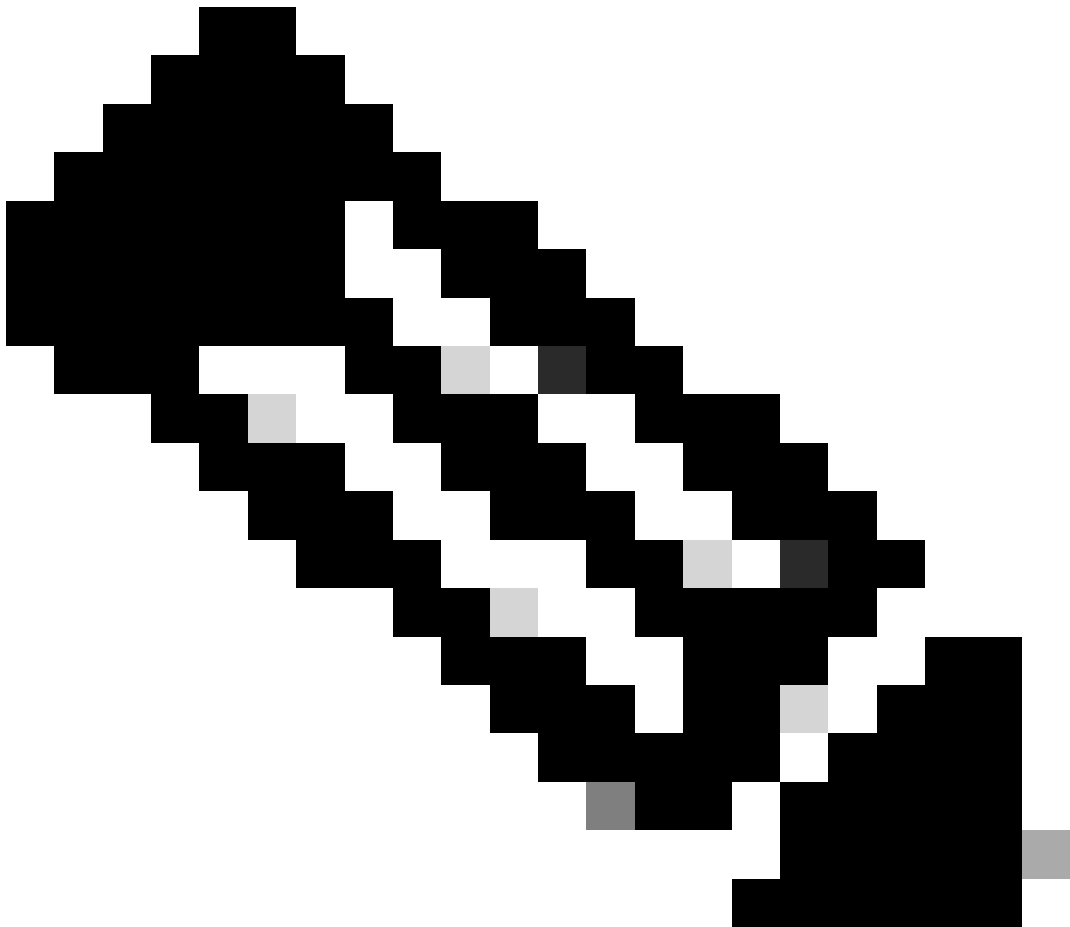
以下是MGCP訊號傳送和RTP媒體（語音）流量的範例：



最佳實踐

對於ASA:

- 使用允許流量進出兩個信令元件（裝置或伺服器）的允許規則。這可以受到指定信令VoIP協定上使用的埠的限制。
- 允許可以傳送和/或接收音訊和/或影片流的媒體裝置之間的RTP埠範圍。



附註：請記住，這些音訊或媒體裝置可能與信令元件（裝置或伺服器）不同。

對於FTD:

- 為信令元件（裝置或伺服器）定義預過濾器規則，並定義特定埠以僅限制指定信令協定的流量。
- 為音訊和/或影片RTP協定配置預過濾器。

疑難排解

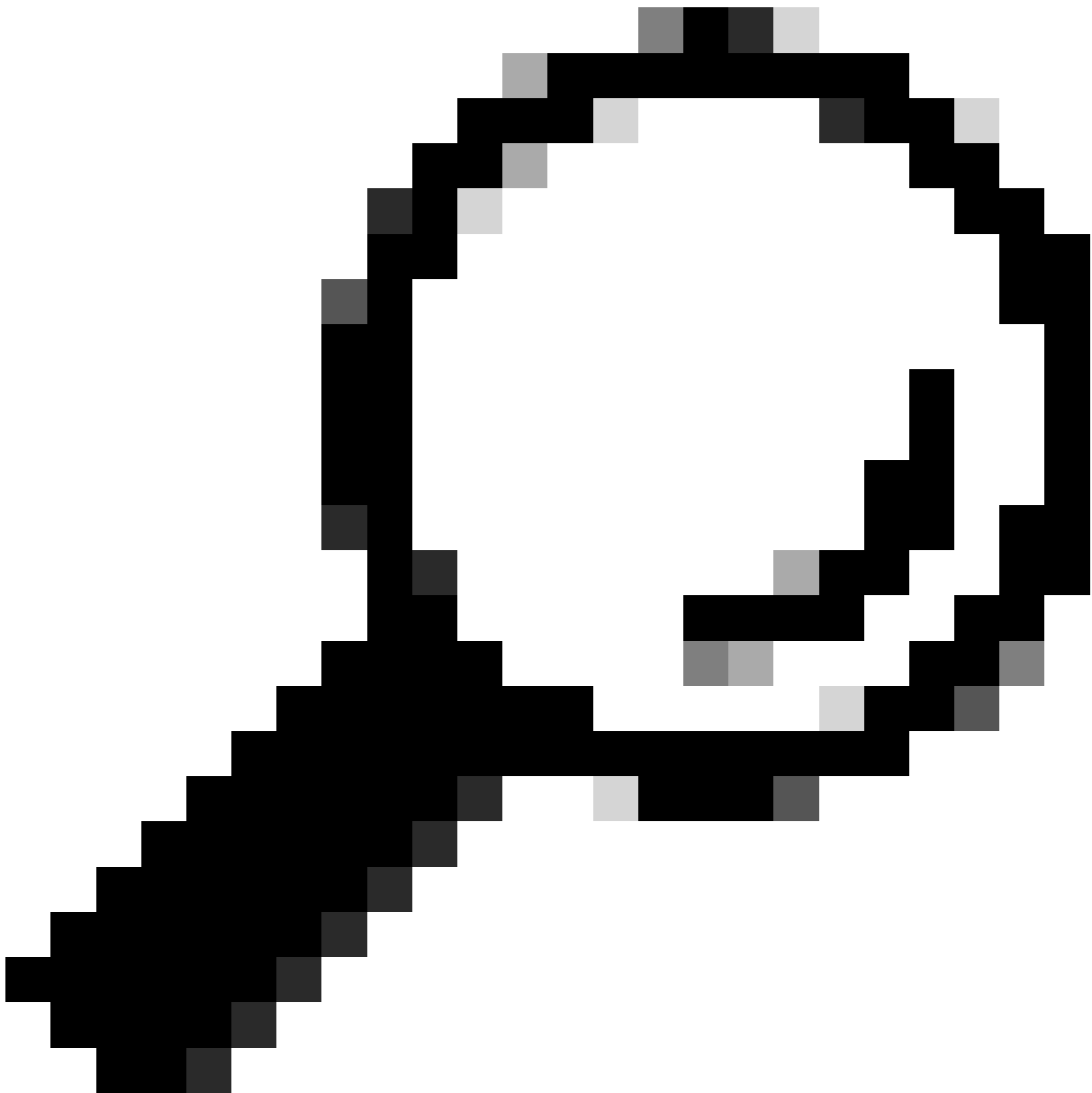
在排查語音問題時，您需要知道問題是信令還是媒體（語音或影片）還是兩者都存在，下面是一些示例可以指導您對此加以區分：

信令問題示例：

- ++使用者報告呼叫未建立。
- ++使用者無法呼叫其他使用者或號碼。
- ++SIP中繼沒有啟動，因為選項SIP消息沒有收到響應。
- ++我的裝置無法註冊。

媒體（語音或影片）問題示例：

- ++存在單向音訊問題。
- ++沒有通話音訊。
- ++完全沒有影片。
- ++呼叫保持靜默。



提示：在影片呼叫期間，SDP最多可以協商三條媒體線路（m條線路）：音訊、影片和影象。每個m行對應於每個呼叫段的一個單獨的即時傳輸協定(RTP)流，這意味著在呼叫的每個段上最多可以有三個不同的RTP流（每種媒體型別各一個）。

疑難排解防火牆上的訊號問題

要排除信令部分的故障，您需要確保：

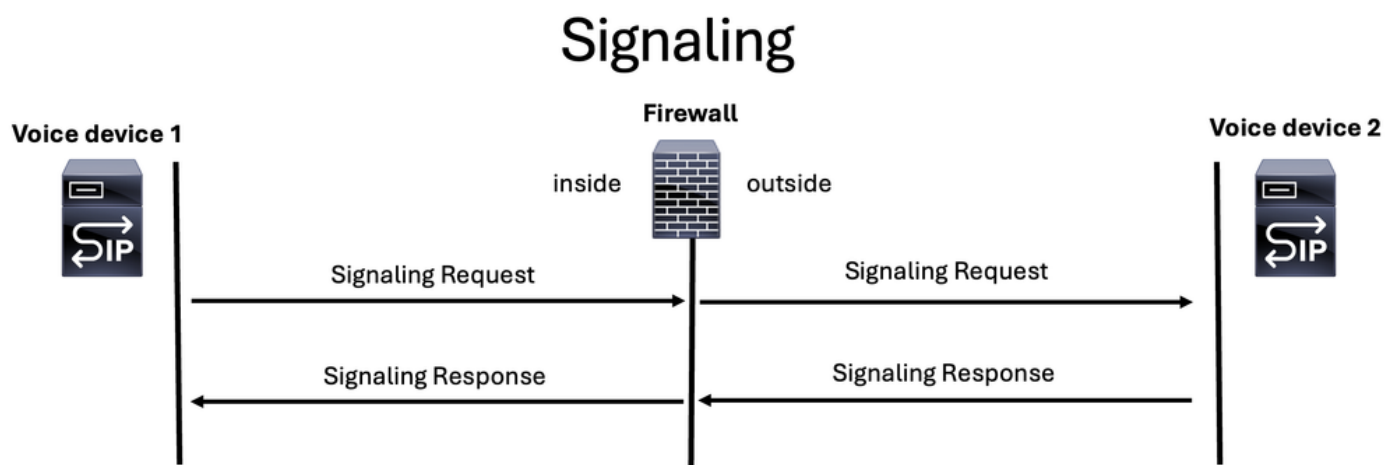
++從入口和出口介面確定呼叫中涉及的所有信令元件（裝置或伺服器），並在安全防火牆的CLI上配置資料包捕獲的相應匹配條件。

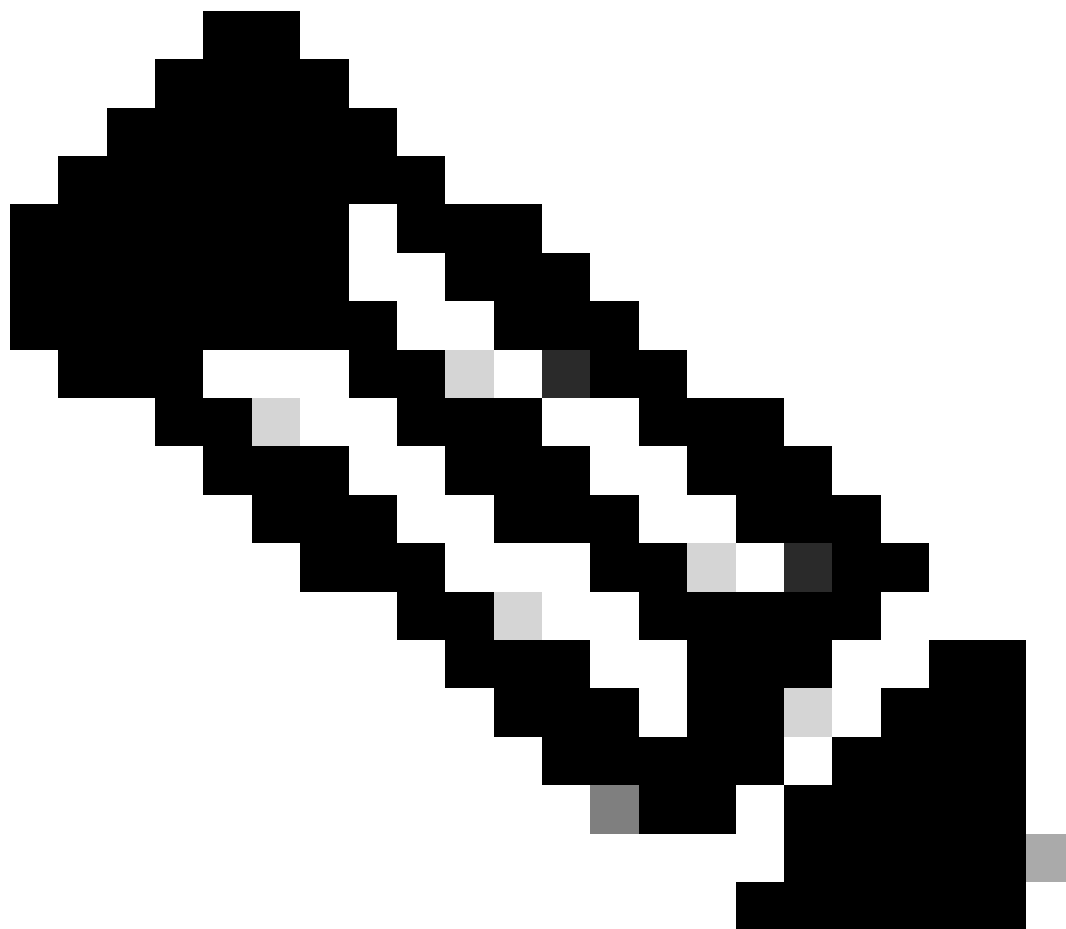
++請記住，輸入介面上的訊號傳送訊息數量必須與輸出介面相符。

++通過指定信令協定使用TCP還是UDP，以及對預期埠號進行過濾，可以使資料包捕獲更加高效。

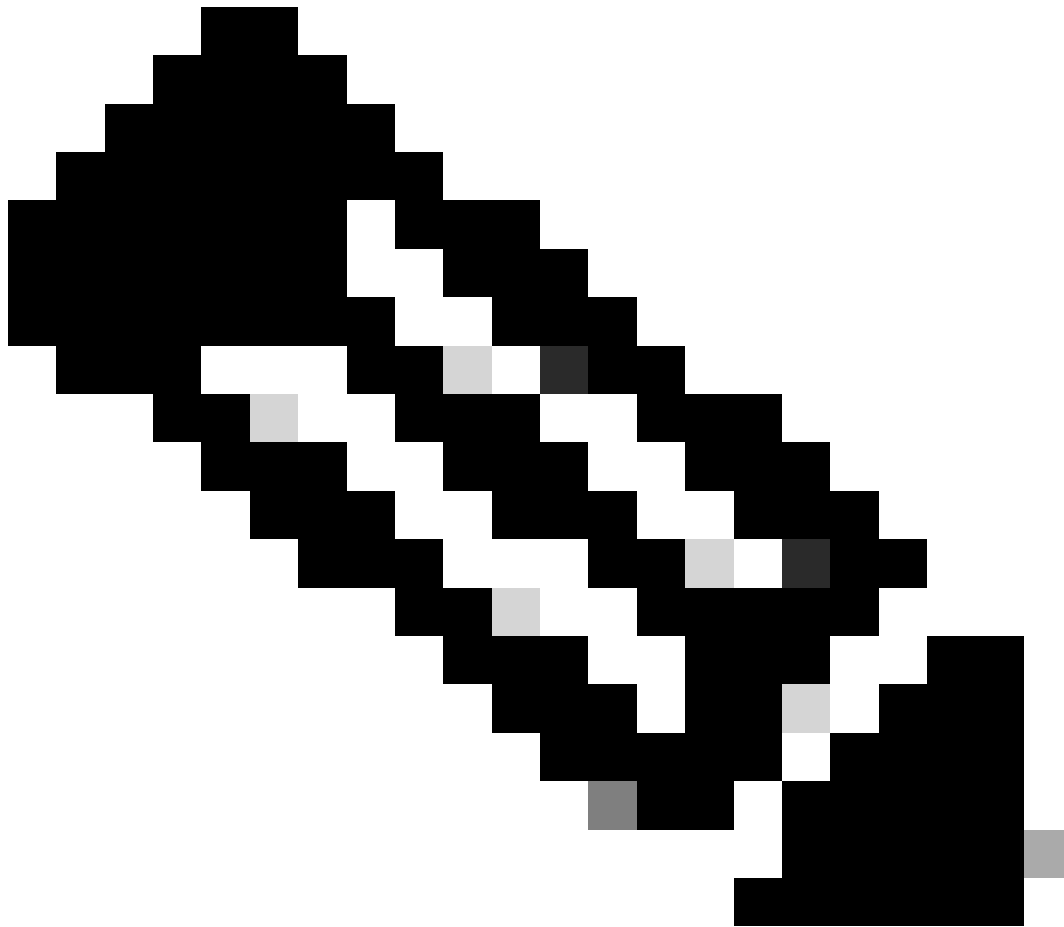
由於所有訊號通訊協定都是透過IP執行，因此在CLI上應用這些過濾器有助於限制您在擷取中看到的流量量。

++僅對於出口介面，確保在資料包捕獲過濾器中指定分配給出站流量的NAT IP地址。這可確保您擷取輸出介面上顯示的正確流量。





注意：請記住，無論使用哪種信令協定進行語音，都必須始終存在請求和響應，並且必須在入口和出口介面上保持一致。



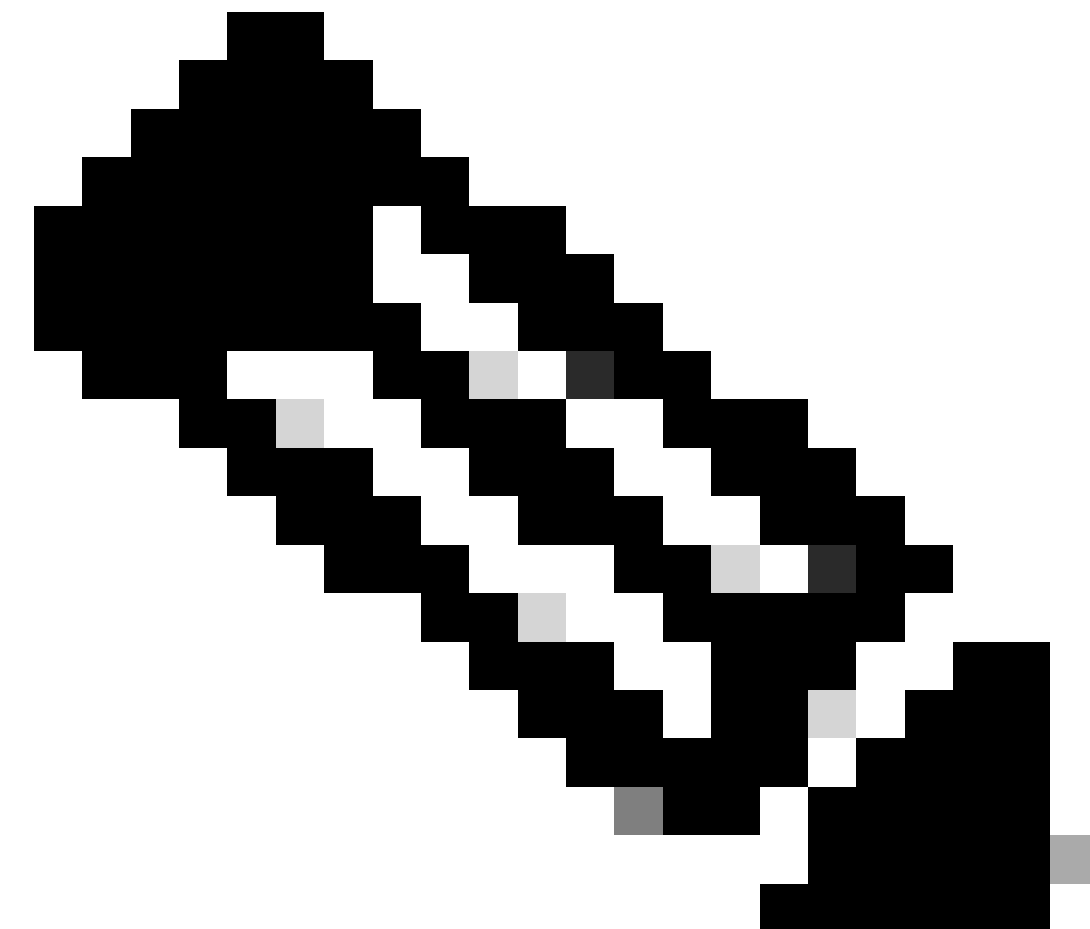
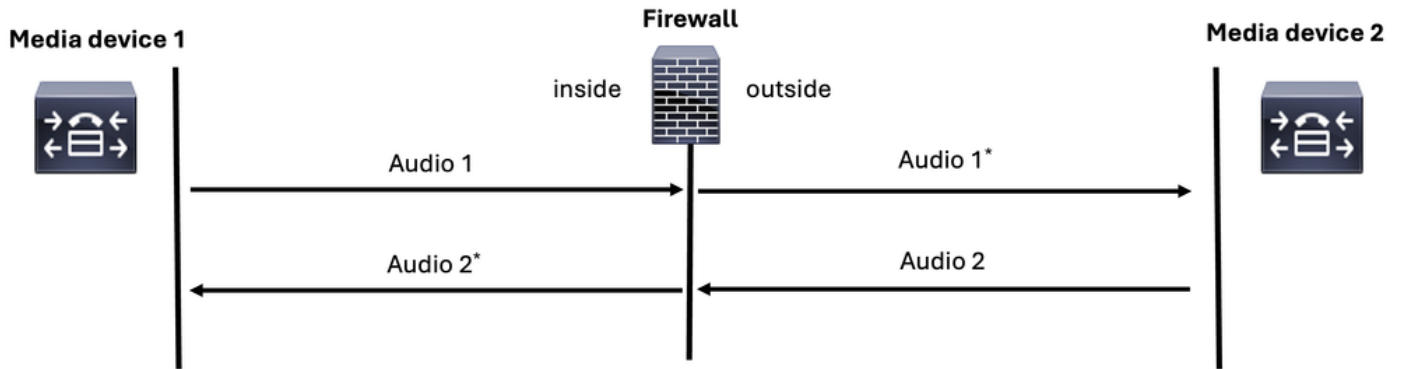
注意：儘可能確保通訊路徑中僅涉及一個防火牆。在某些部署中，語音信令和媒體流可以穿過單獨的防火牆。在這些情況下，請確保在疑難排解過程中包含所有相關防火牆

對防火牆上的介質問題進行故障排除

從防火牆的角度來看，在排除單向音訊、雙向音訊問題或無音訊故障時，必須分析4個流：

1. 從呼叫者到被呼叫者的RTP流（輸入介面）。
2. 從呼叫者到被呼叫者的RTP流（輸出介面）。
3. 從被叫方到主叫方的RTP流（輸出介面）。
4. 從被呼叫者到呼叫者的RTP流（輸入介面）。

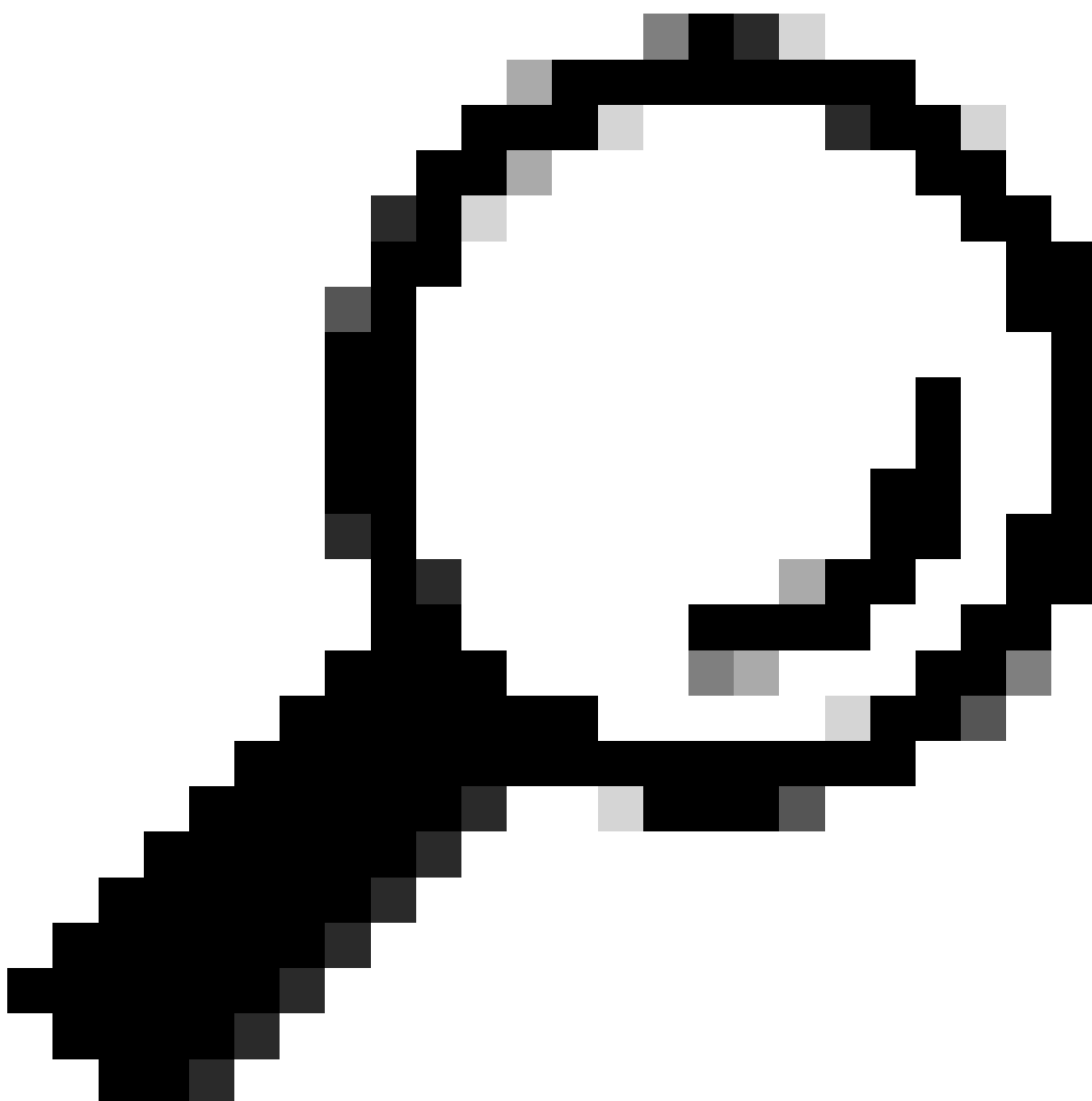
Media=Voice=RTP



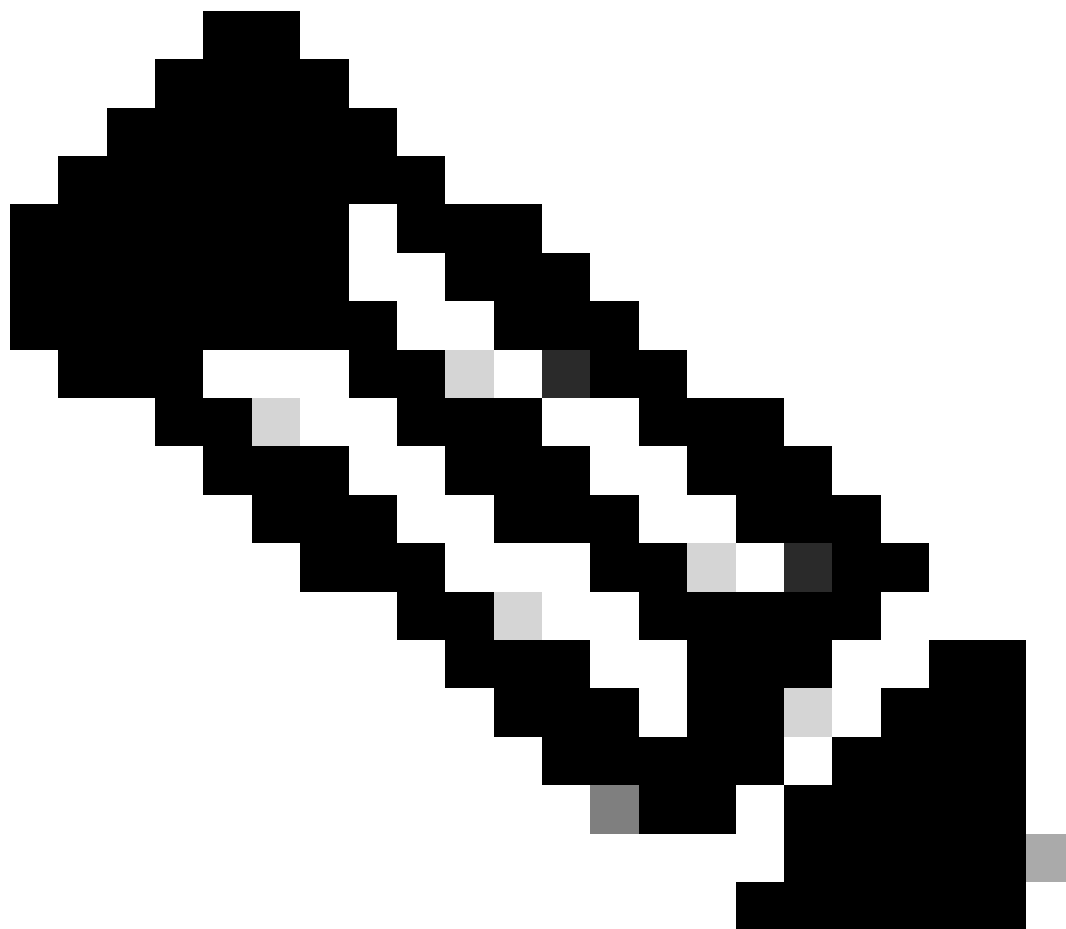
附註：確保您在FTD的ASA或LINA模式下使用CLI封包擷取執行疑難排解，因為這樣可以在單一封包擷取中更靈活地套用多個相符專案。

排除安全防火牆 (ASA或FTD) 上的語音故障時，您需要執行以下步驟：

1. 確保您有呼叫流程和拓撲圖。
2. 確保從使用者的角度理解問題。
3. 瞭解訊號通訊協定的路徑。
4. 瞭解媒體RTP協定的路徑。
5. 在入口和出口介面上捕獲資料包。
6. 檢查配置ACL規則和NAT規則。
7. 驗證防火牆是否未阻止SIP信令流量。此外，比較入口和出口介面以分析語音流量。
8. 通過比較入口和出口介面上的流量來驗證防火牆是否未阻止RTP媒體流量。
9. 確保信令裝置支援檢測，如果不禁用該檢測。



提示：進入FW的SIP信令消息也必須與離開FW相同。



附註：SIP故障排除提示也可應用於H.323、MGCP和SCCP協定。

相關資訊

- [使用CLI配置ASA資料包捕獲](#)
- [使用Firepower威脅防禦捕獲](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。