了解安全防火墙的IP语音协议基础知识

目录

简介

本文档介绍各种VoIP协议的基本原理，以帮助工程师在安全防火墙上有效地排除故障。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档适用于以下设备的故障排除场景：

- 安全防火墙威胁防御(FTD)
- 安全防火墙自适应安全设备(ASA)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

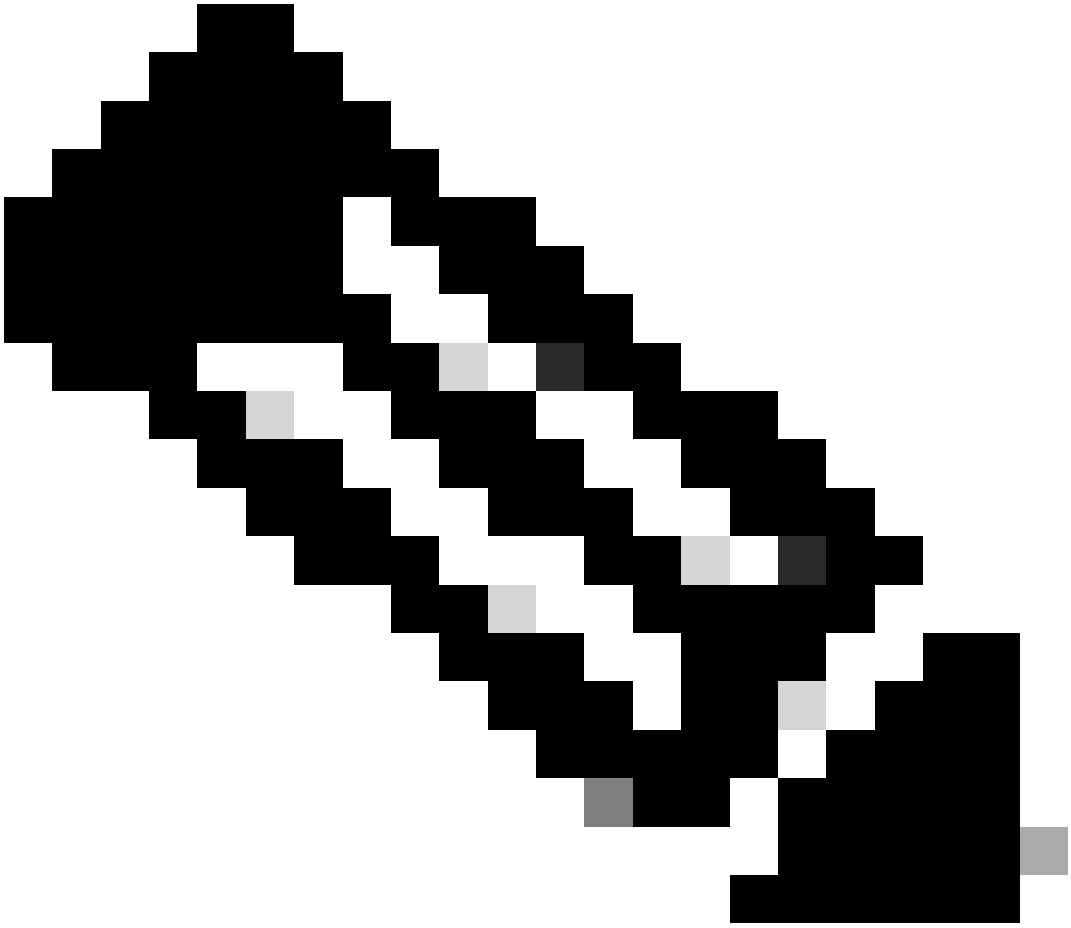
VoIP基础

通信是人类交互的基础，IP语音(VoIP)协议已成为人类通信不可或缺的一部分。因此，在排除包含防火墙(FW)的场景故障时，了解其组成部分非常重要。

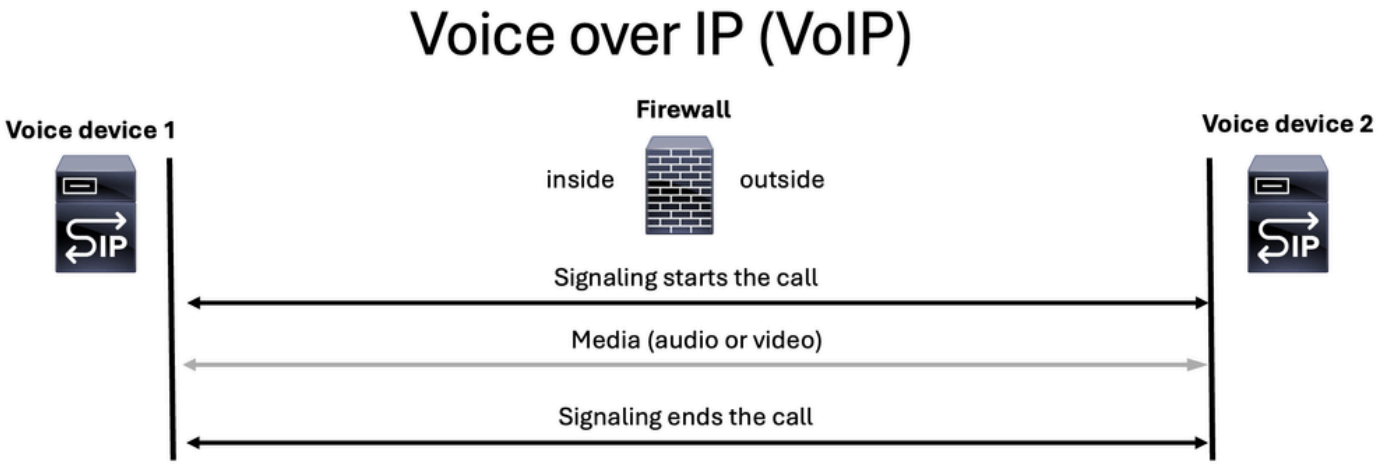
VoIP由两部分组成：

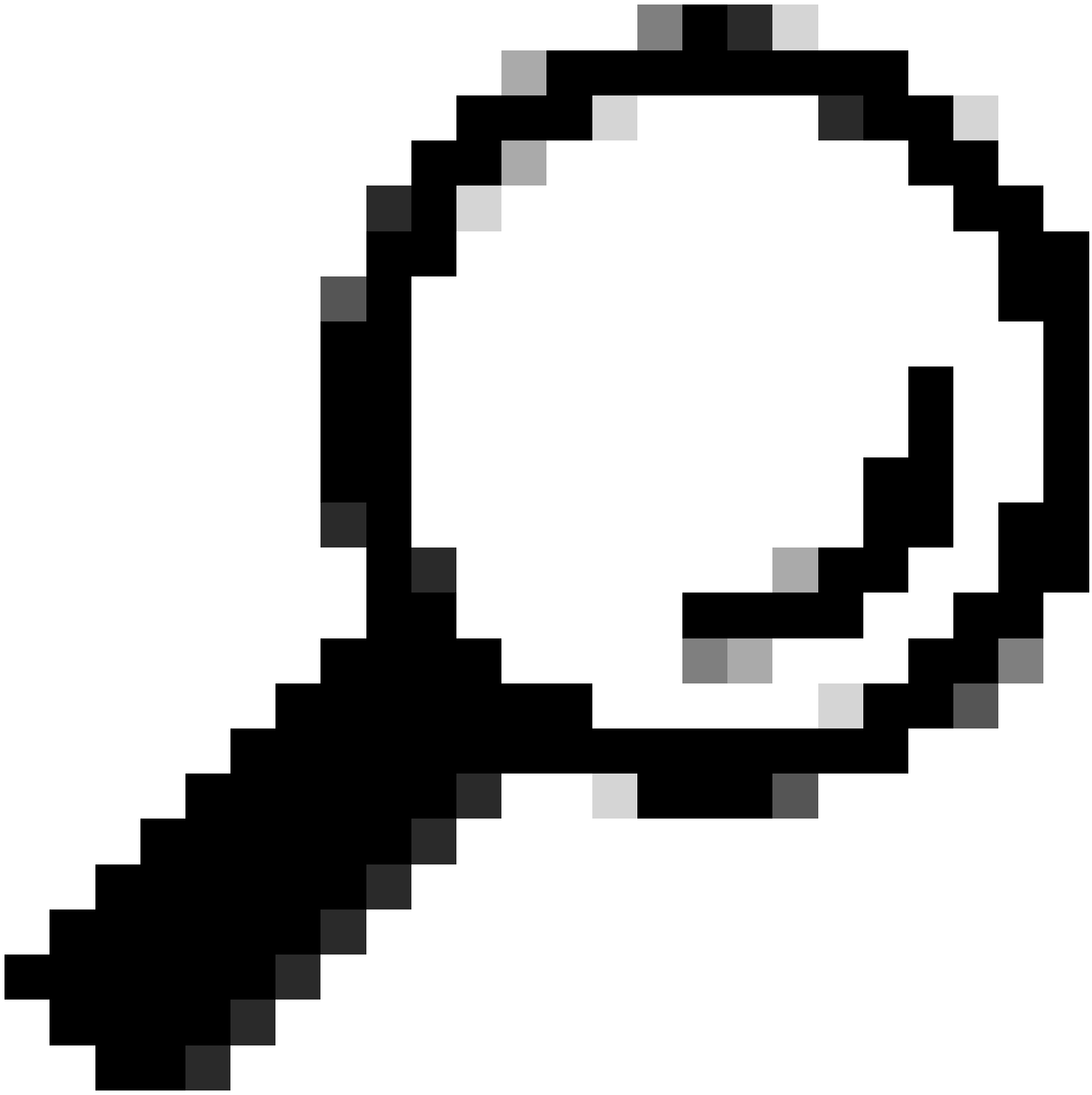
- 信令
- 媒体（语音或视频）

VoIP通信始终从发起呼叫的信令部分开始，然后对媒体（语音或视频）进行流传输，最后通过信令结束呼叫。

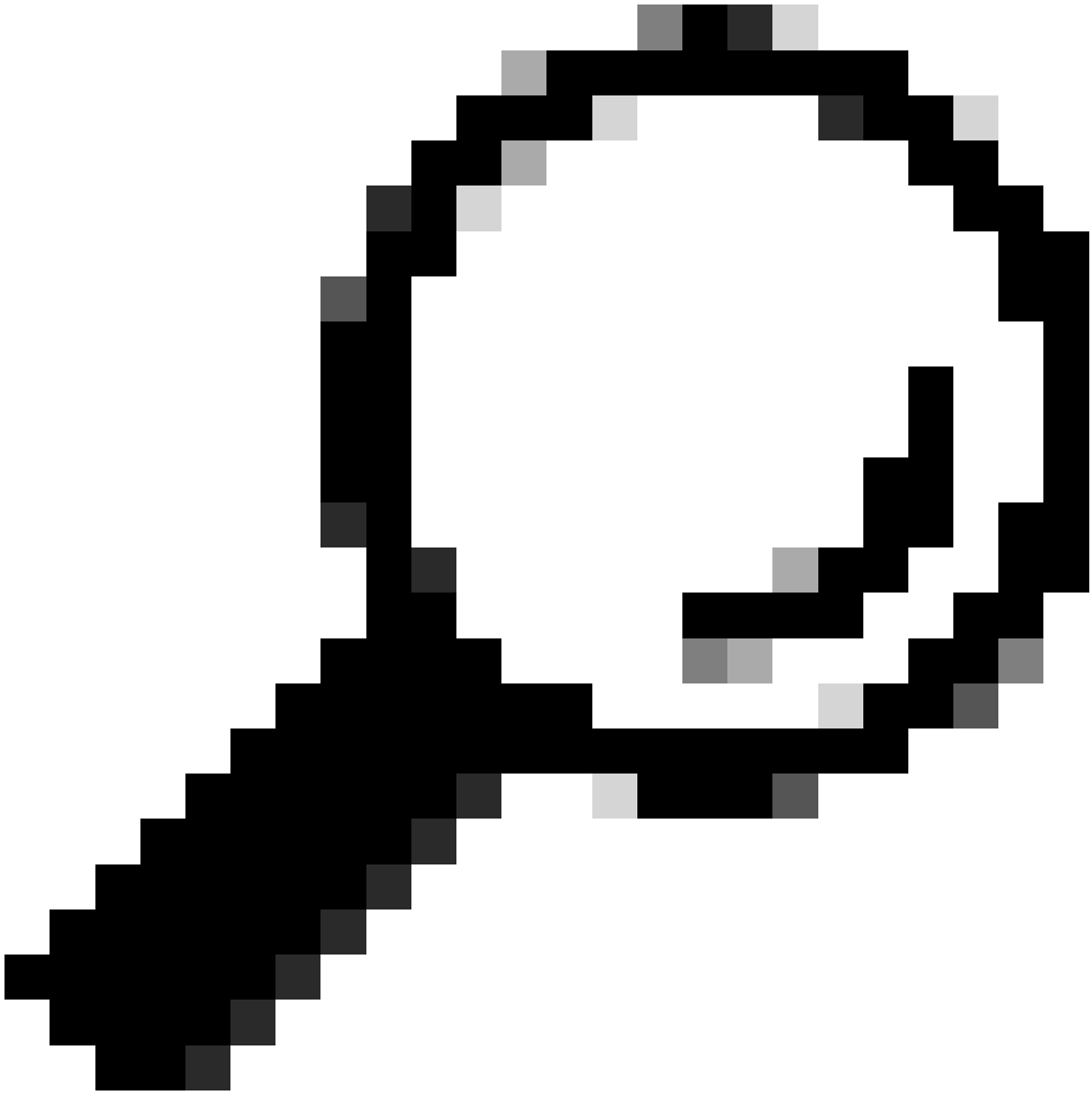


注意：SIP是最广泛使用的协议，因此在许多图中始终以SIP语音服务器图标表示。





提示：排除ASA或FTD的语音故障时，从用户的角度考虑场景至关重要。您需要确定呼叫是否已建立，或没有音频或单向音频。此信息提供有价值的线索，说明问题出在信令协议还是媒体（语音或视频）协议上。



提示：语音设备可以同时管理语音实时传输协议(RTP)流量和信令流量，也可以同时管理这两者。排除语音故障时，必须记住以下主要概念：

++信令服务器：这些服务器只负责处理信令流量。

++媒体服务器：这些服务器以独占方式处理语音RTP流量。

++有些设备可以处理这两个任务。

信令

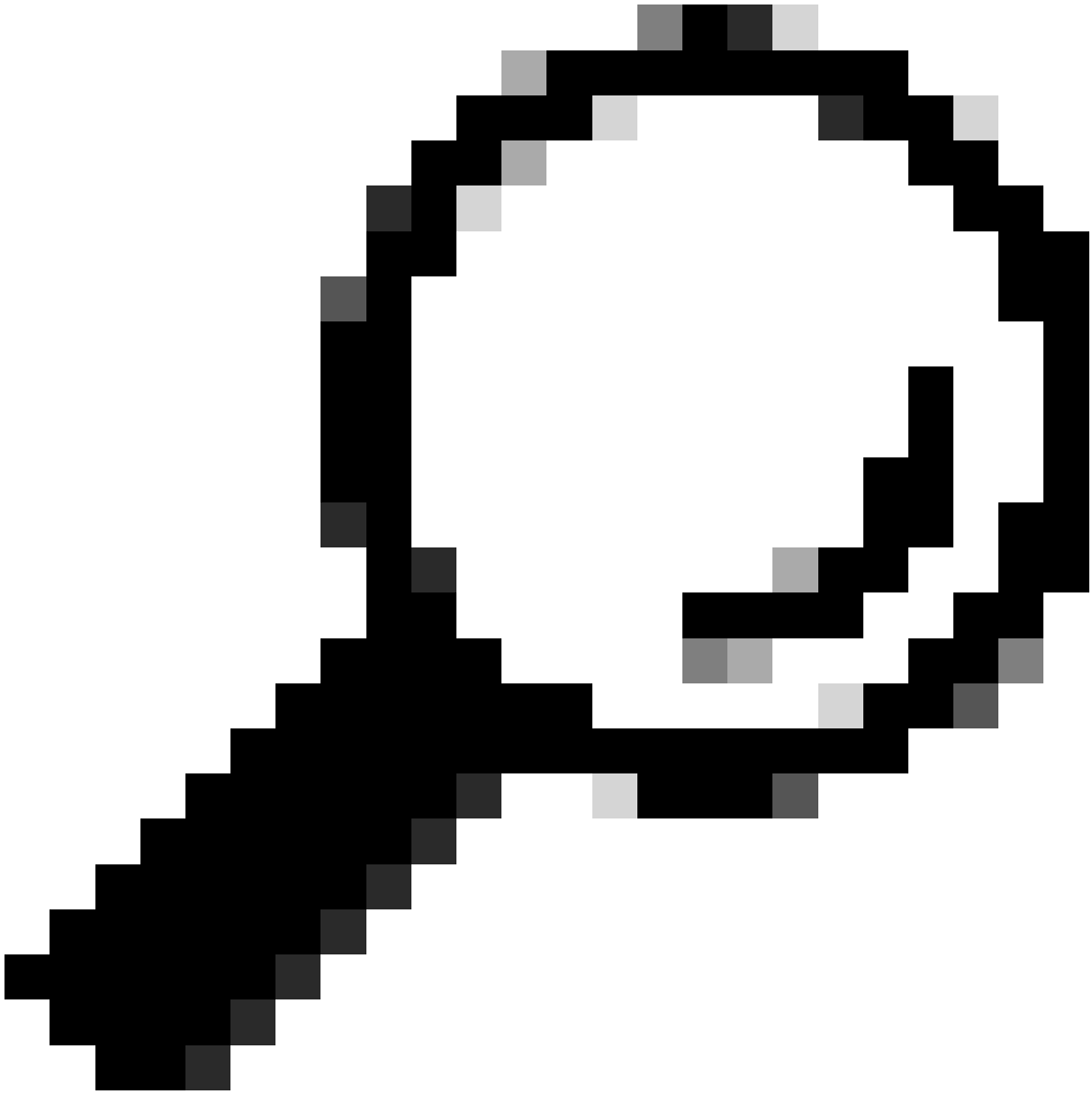
信令协议是启动语音通信的呼叫的一部分，但不仅如此，它还执行以下功能：

- 保持沟通。

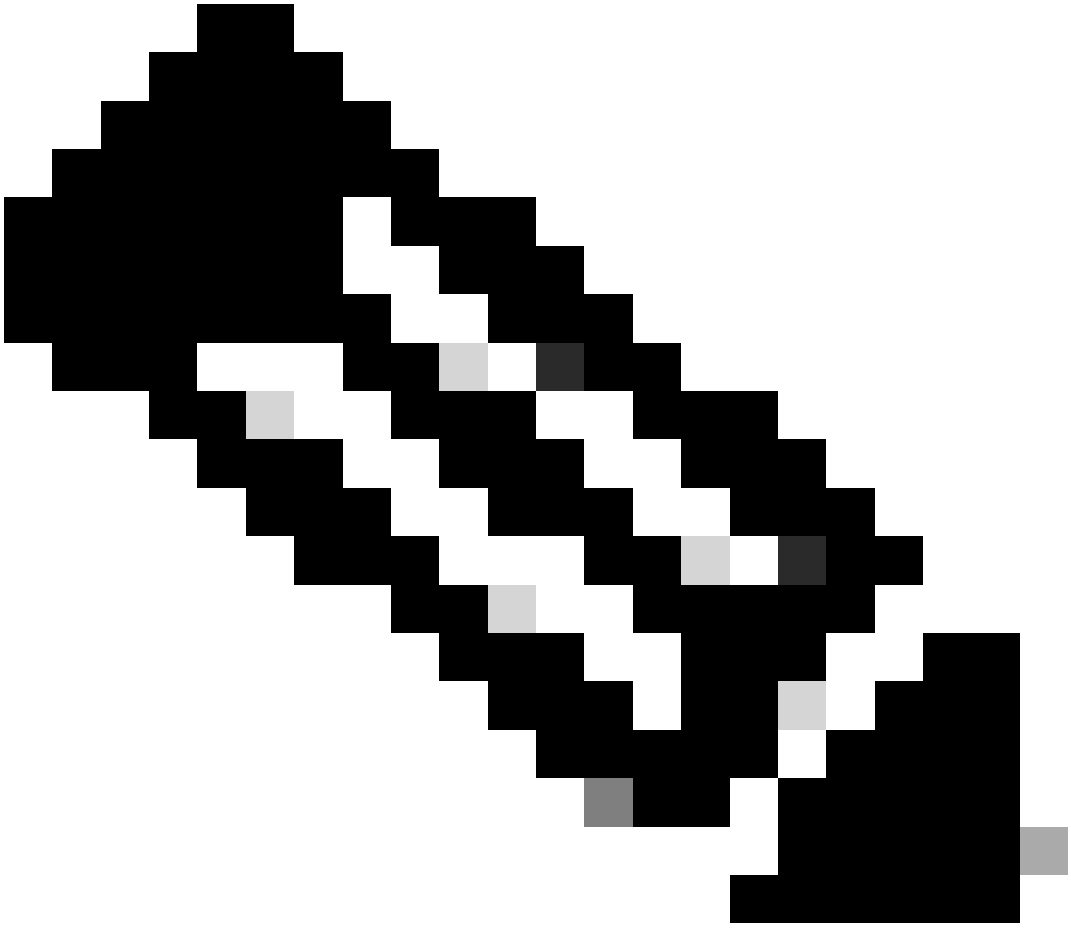
- 修改通信。
- 结束通信。

不同类型的信令协议可帮助建立呼叫，最常见协议包括：

- 会话初始协议 (SIP)
- H.323
- Media Gateway Control Protocol (MGCP)
- 瘦呼叫控制协议(SCCP)



提示：确定正在使用的信令协议对于确定ASA或FTD上用于数据包捕获的适当端口至关重要。此外，拥有呼叫流和网络拓扑有助于了解信令路径。

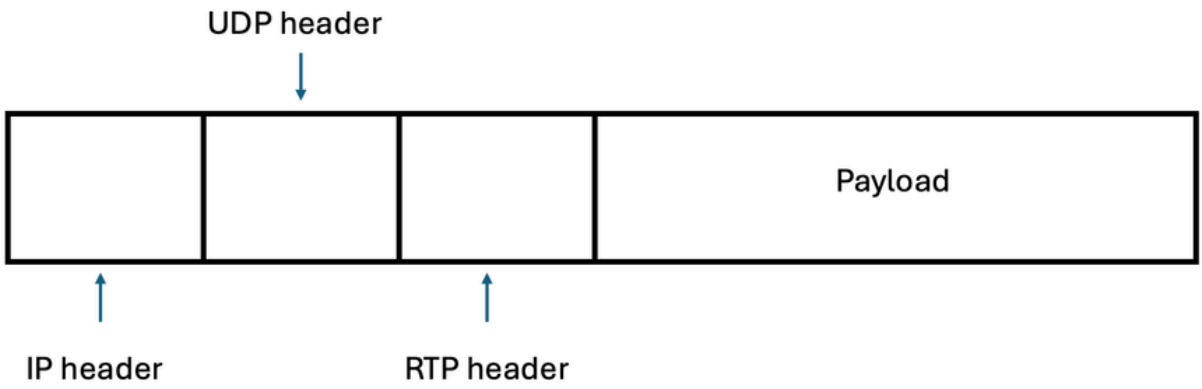


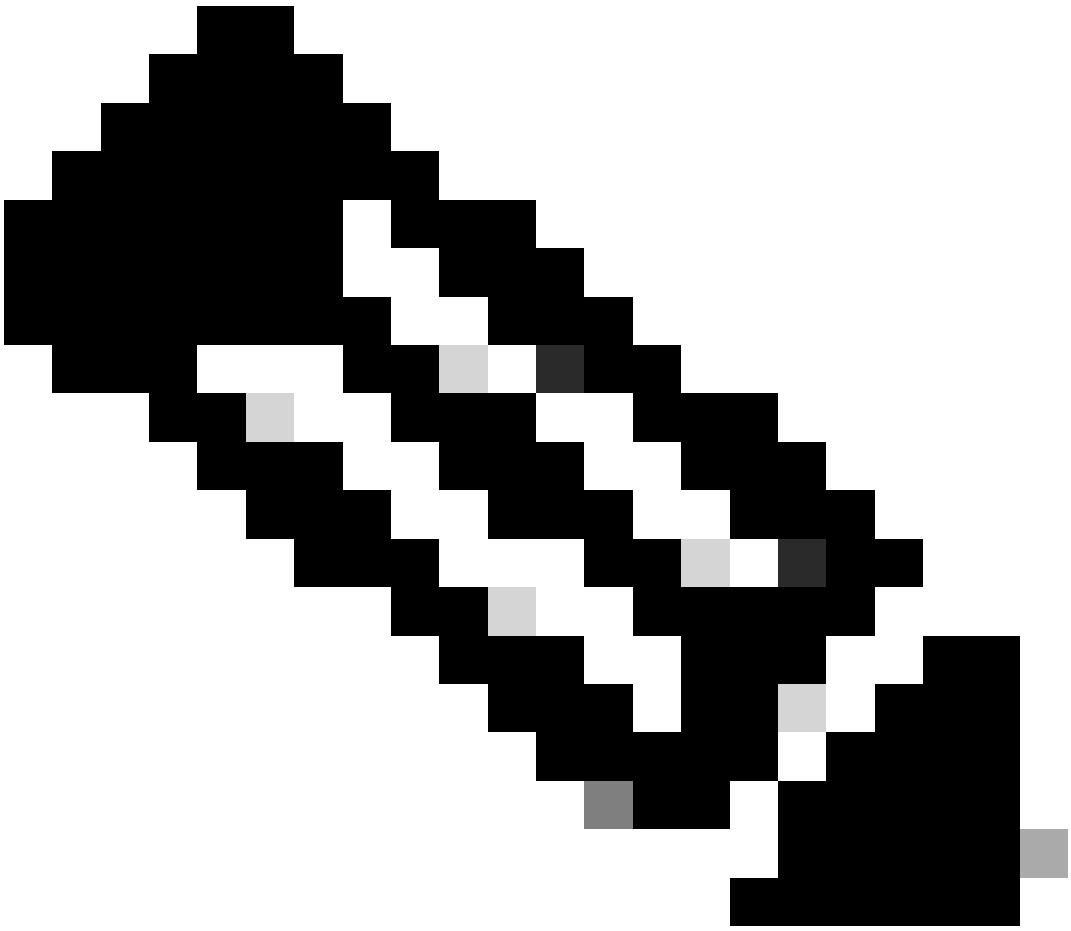
注意：信令数据包包括源IP地址和目的IP地址，有助于识别发送和接收RTP媒体流的相关方。

媒体

在信令完成且信令组件（设备或服务器）同意媒体类型后，将播放实时协议(RTP)以开始向相关各方发送媒体（音频和/或视频）。

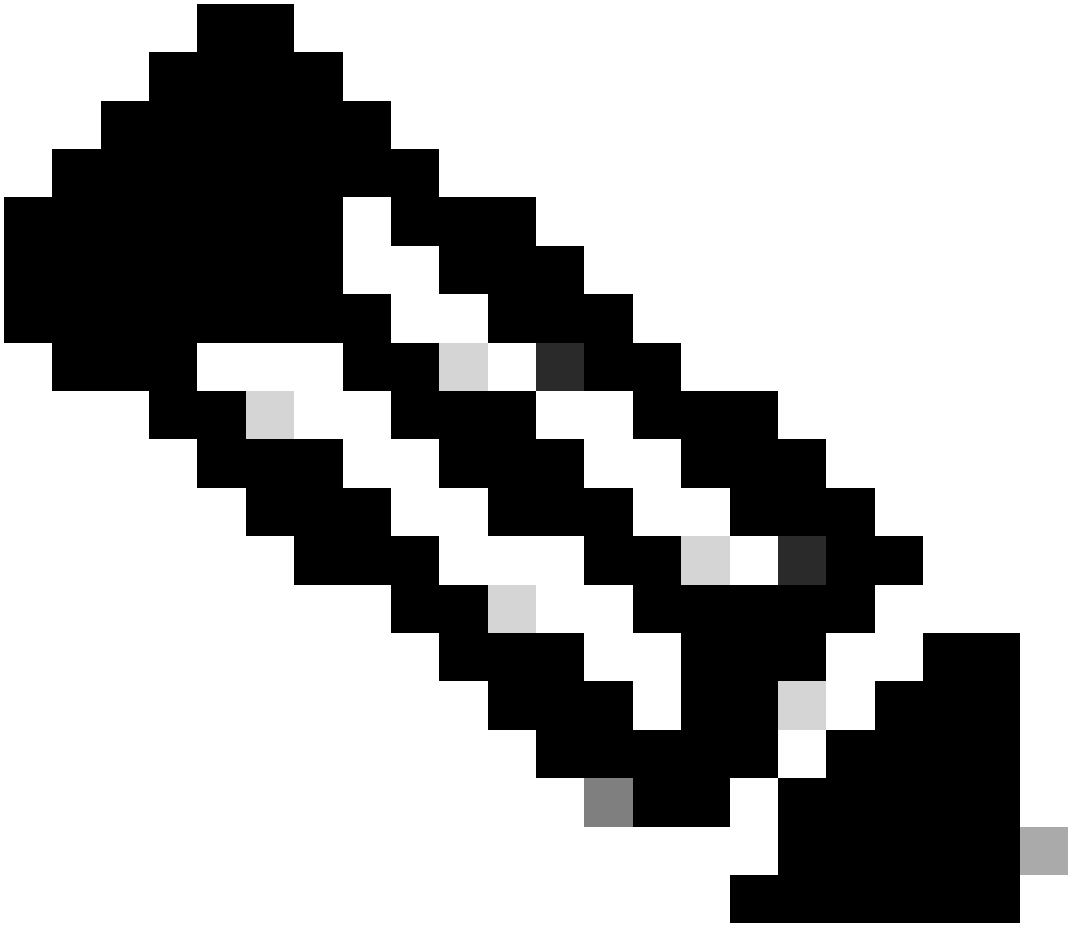
RTP是用于流媒体的互联网协议，仅在呼叫建立后发送，并且它通过用户数据报协议(UDP)运行。



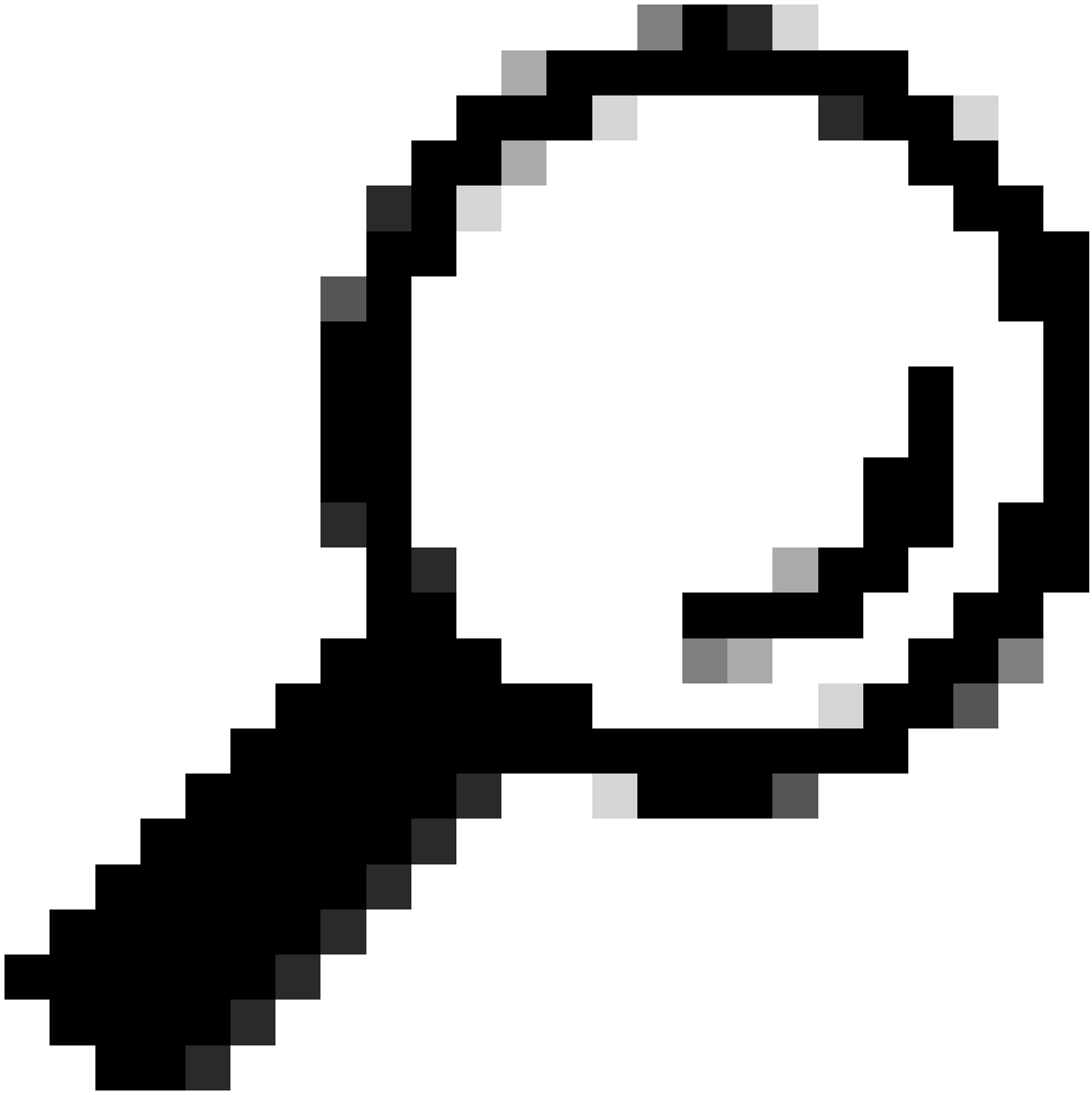


注意：介质可以是语音和/或视频，通过RTP数据包传输。

信令组件（设备或服务器）确定哪些端口用于发送或接收媒体（音频和/或视频）。 对于大多数设备，RTP最常见的端口范围通常介于16384和32767之间。



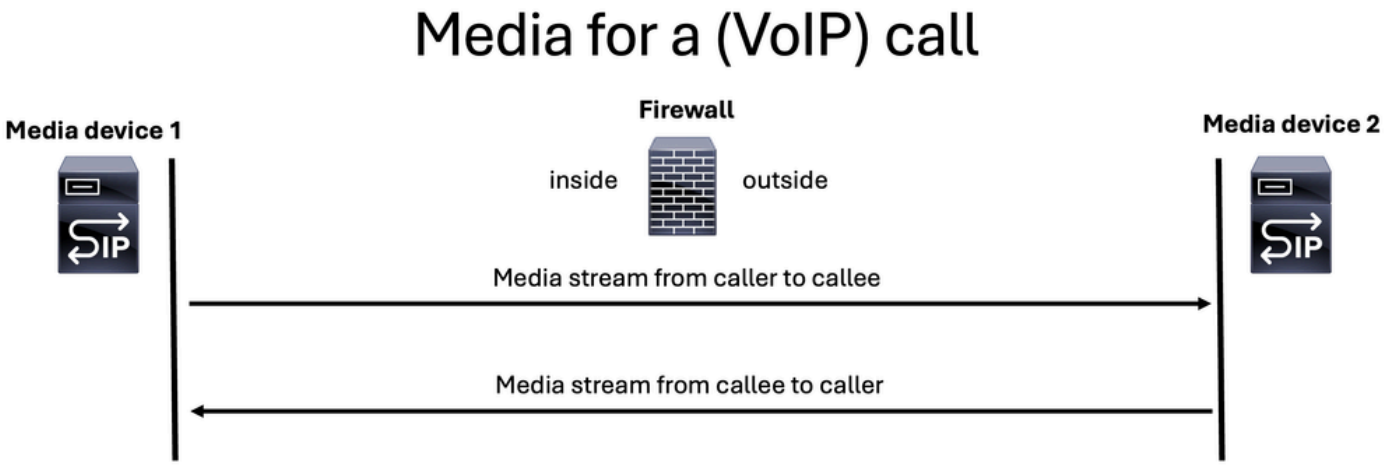
注意：某些Cisco设备（如ASR和ISR G3平台，如ISR4K平台）使用标准化的RTP端口范围8000到48200。验证设备上配置的特定RTP端口范围至关重要，因为它可能与这些标准化值不同，并且可能随第三方设备而变化。

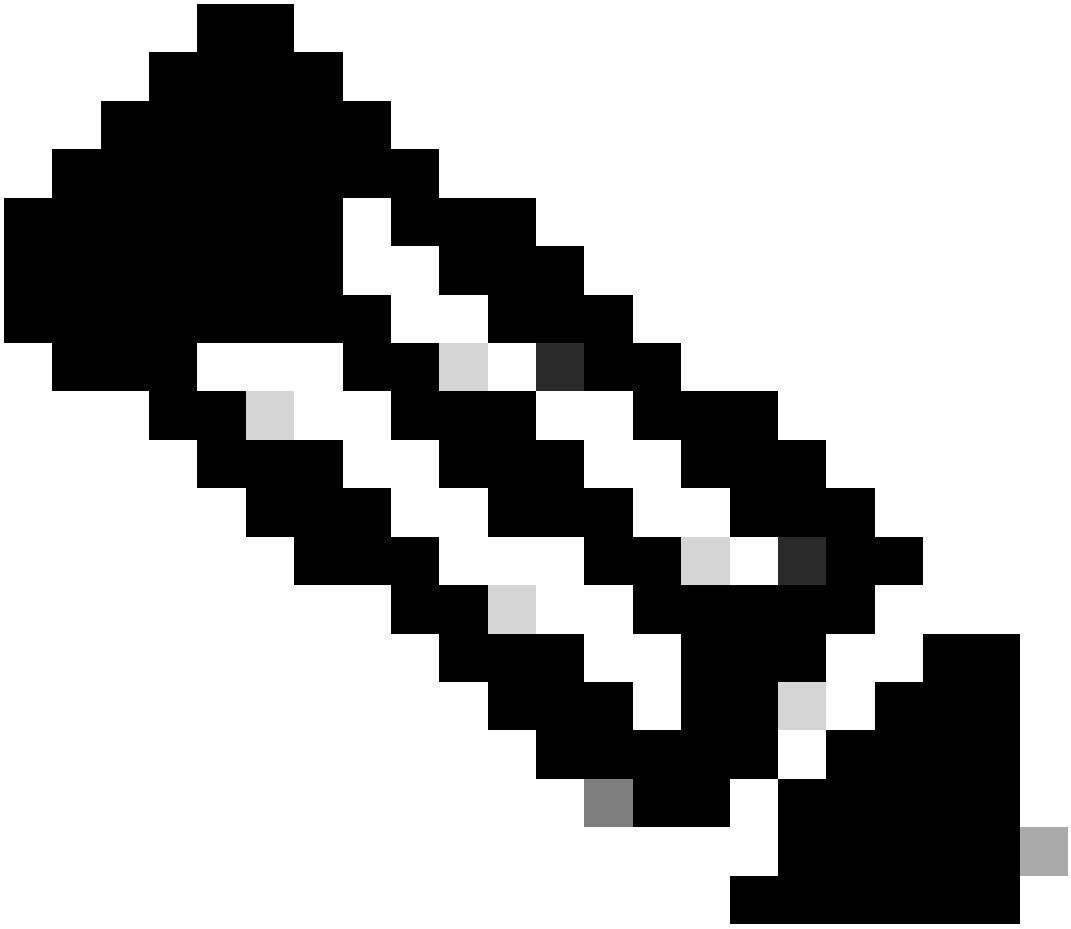


提示：有时，RTP路径与信令路径不同，因此确定负责发送和接收语音RTP数据包的设备至关重要。这可确保捕获穿越ASA或FTD的设备之间的UDP流量。

正常语音呼叫中生成两个媒体流或RTP流：

1. 从主叫方到被叫方的一个媒体流
2. 从被叫方到主叫方的一个媒体流





注意：为了便于说明，SIP服务器图标用于表示所有映像中的信令服务器或媒体服务器。

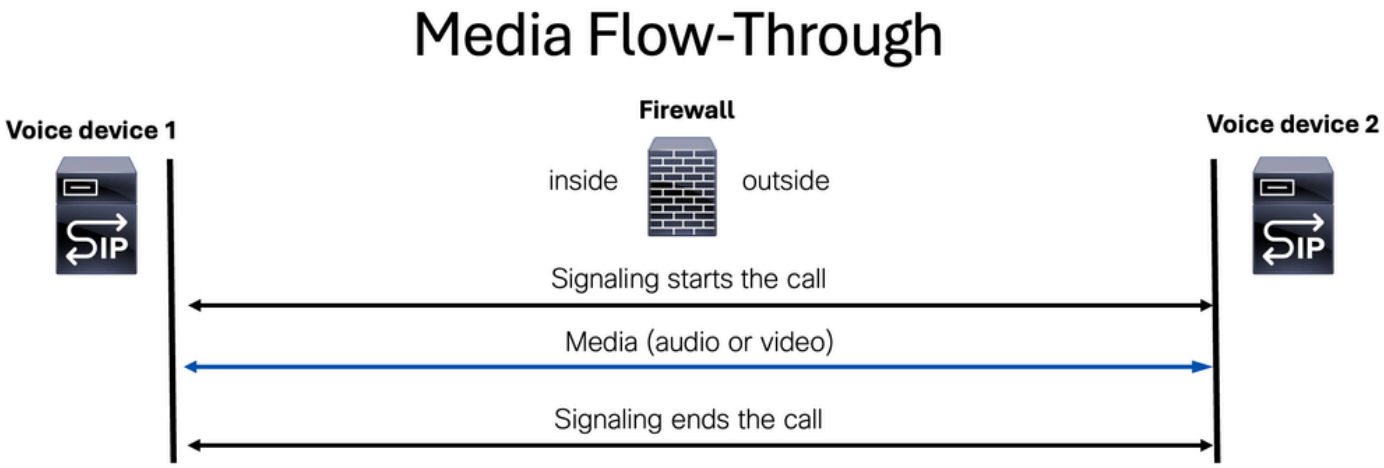
在语音呼叫中讨论媒体流时，必须突出两个关键场景：

1. 媒体流通

2. 介质绕流

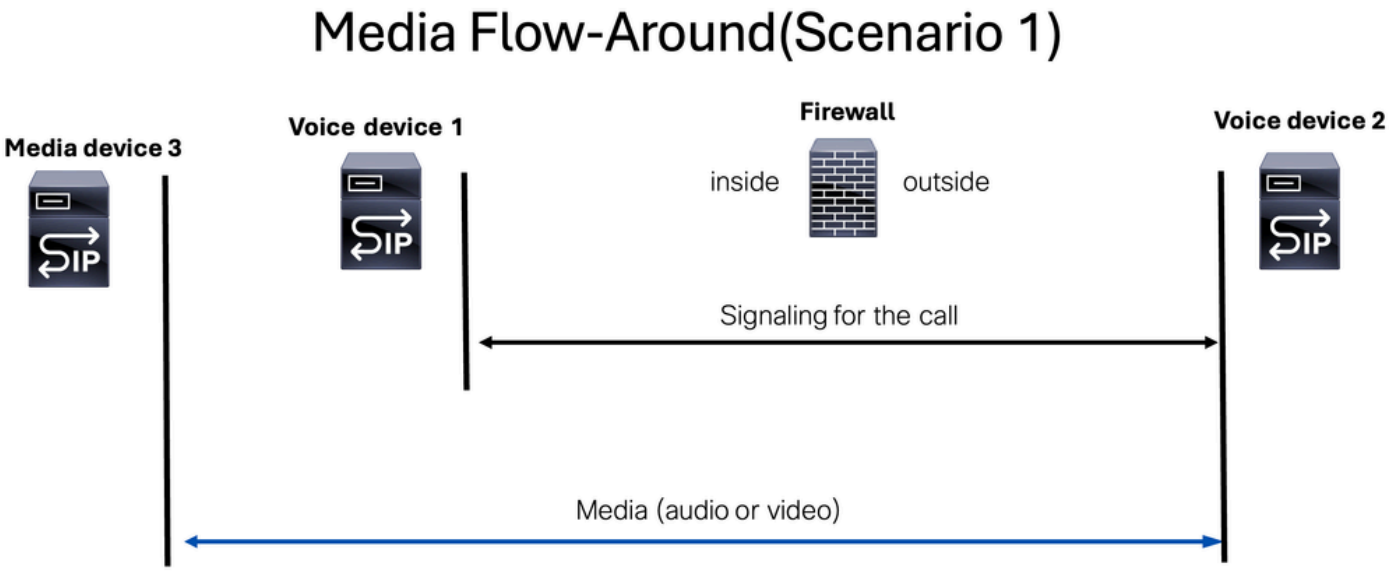
媒体流通

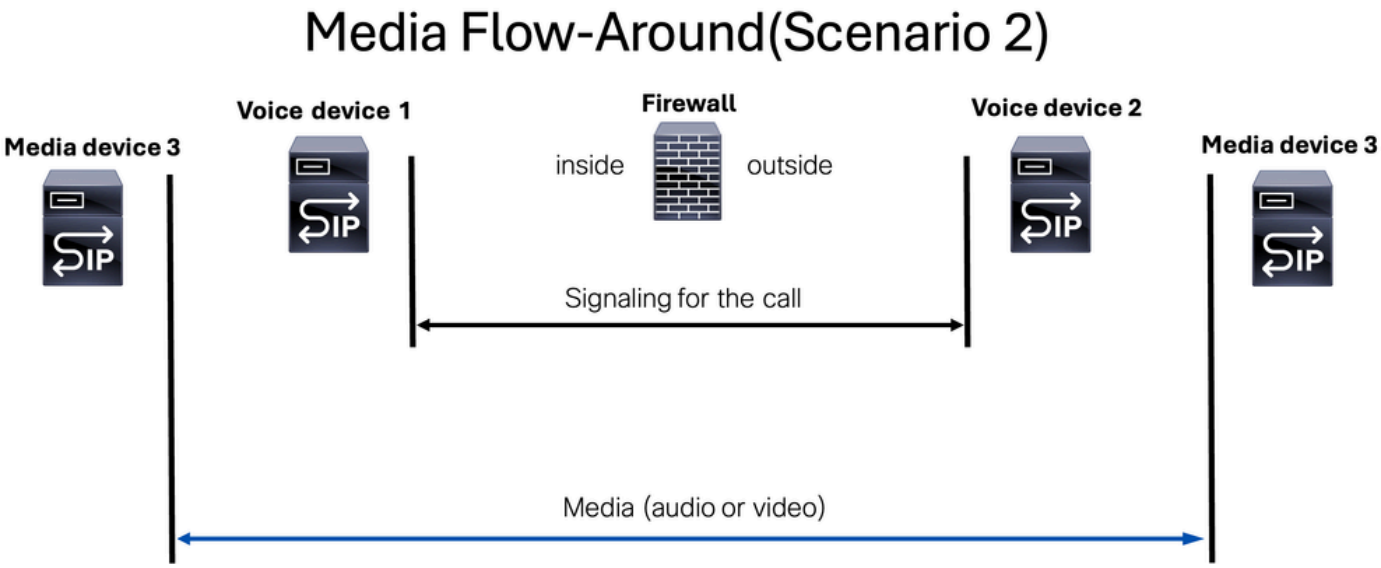
媒体流是指媒体（语音和/或视频）和信令数据包均由同一设备处理的模式。



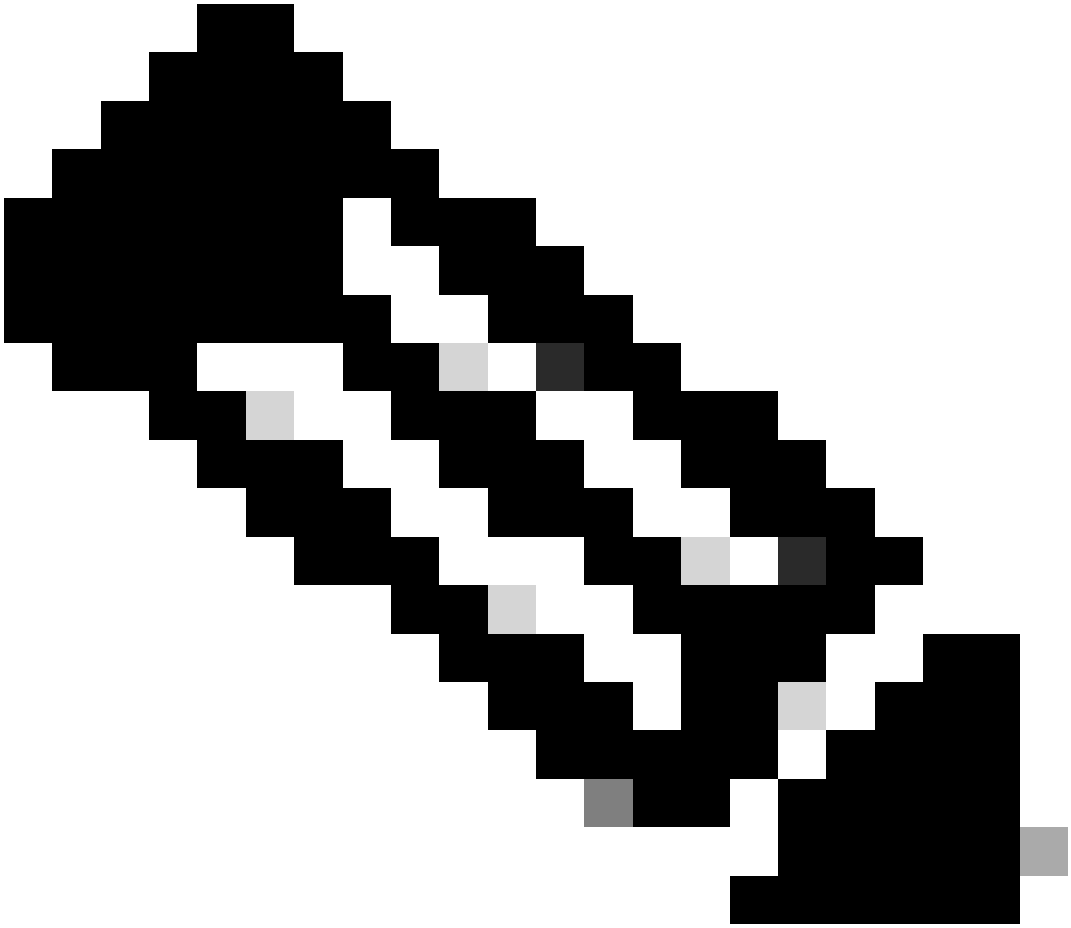
介质绕流

媒体流绕流是一种模式，其中信令数据包由两个独立的信令组件（设备或服务器）处理，而媒体流（语音或视频）由称为媒体设备的第三台设备管理。





此模式明确了相关设备的角色以及信令和媒体流或设备之间的区别。



注意：在排除创建的访问列表可能允许信令组件（设备或服务器）的故障时，这一点尤其重要，但如果媒体流使用其他媒体设备，我们需要允许它以及防火墙设备的访问列表。

会话初始协议 (SIP)

SIP是由Internet工程任务组(IETF)在RFC 3261中定义的应用层控制协议。

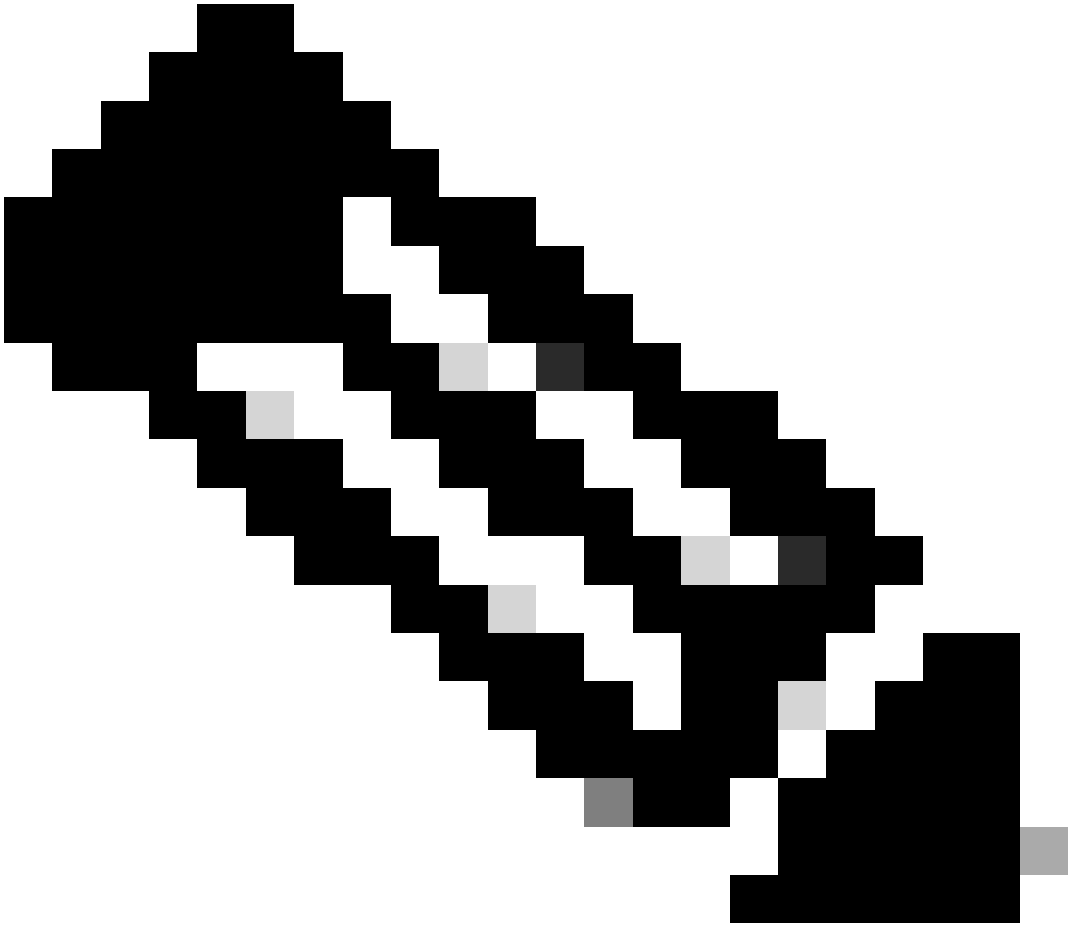
SIP是基于文本的协议。这意味着SIP消息由人类可读的文本组成，类似于HTTP的工作原理。

SIP旨在解决数据包电话网络中的信令和会话管理功能。

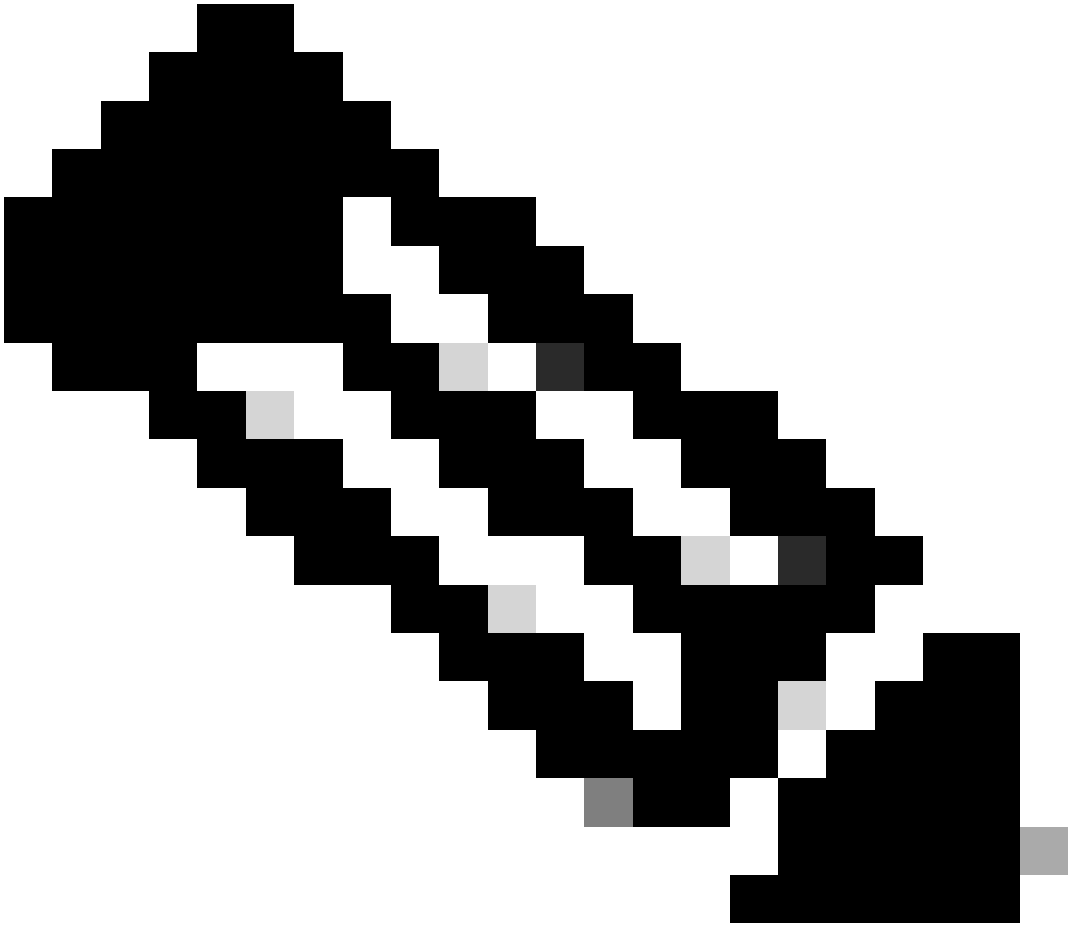
SIP可以：

- 创建呼叫
- 修改呼叫
- 终止呼叫

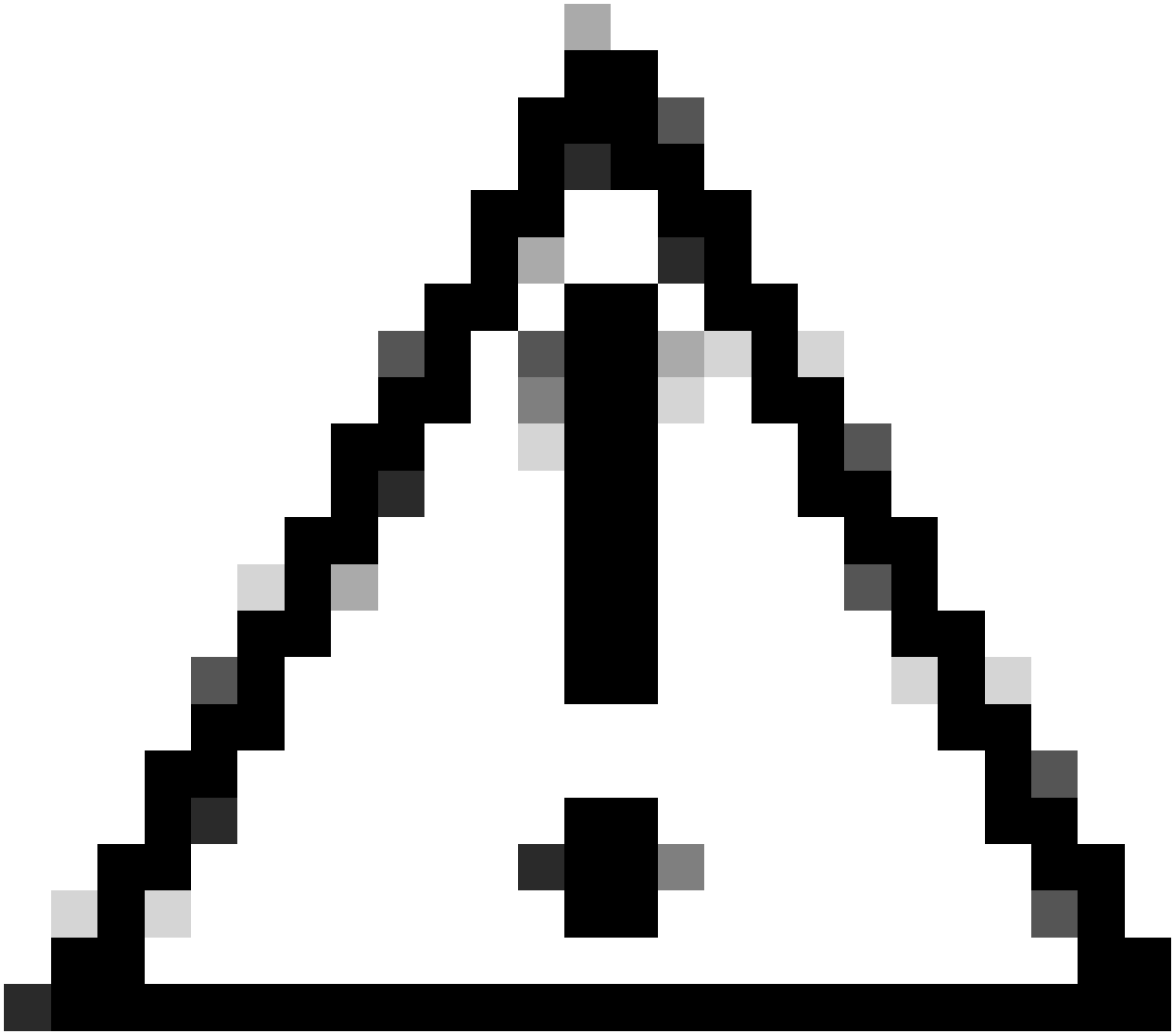
SIP可以在标准化端口5060上使用UDP或TCP。如果SIP使用传输层安全(TLS)加密，则可以使用标准化端口5061。



注意：当SIP信令加密时，实际SIP数据包在ASA或FTD设备上的数据包捕获中不可见。但是，您仍然能够观察SIP客户端和SIP服务器设备之间的TCP握手和TLS握手。



注意：默认情况下，思科安全防火墙威胁防御(FTD)和安全防火墙自适应安全设备(ASA)上启用SIP检测。



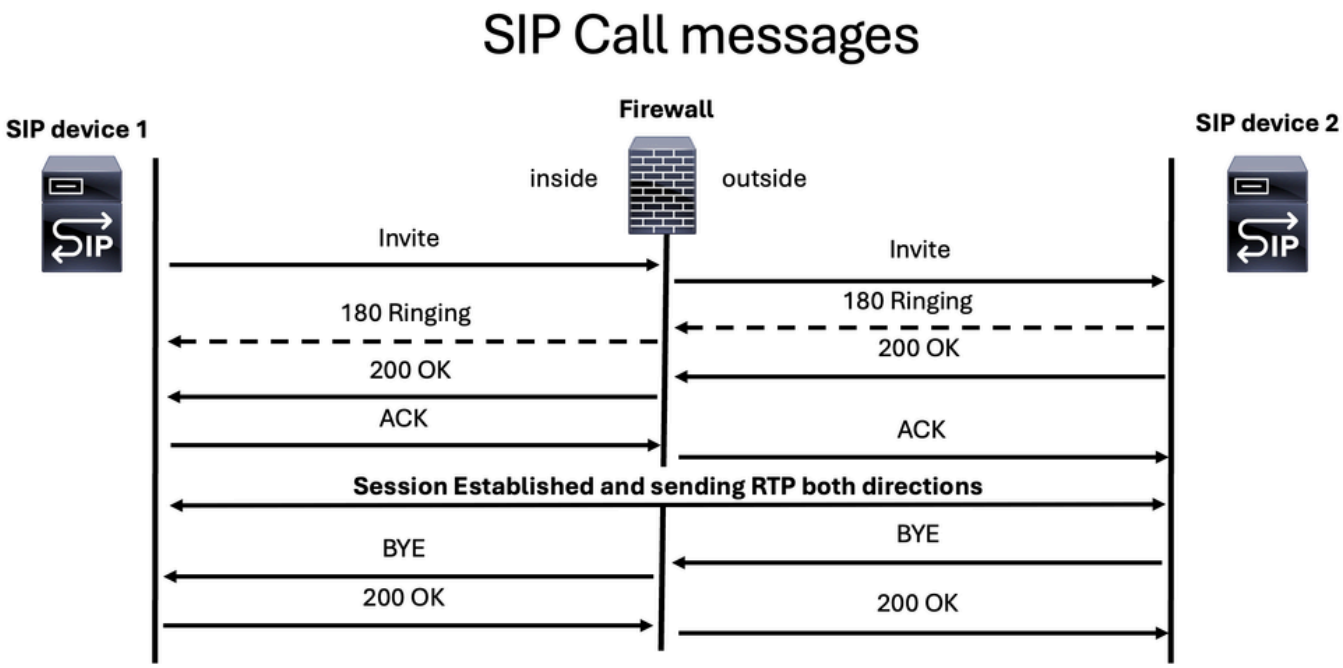
警告：请始终证实用于信令的端口。请记住，SIP协议通常使用端口5060或5061，但某些部署可能偏离这些标准，并且对SIP协议使用不同的端口。

排除SIP信令故障时，可以找到以下三种场景：

- SIP呼叫信令消息
- SIP选项消息
- SIP注册消息

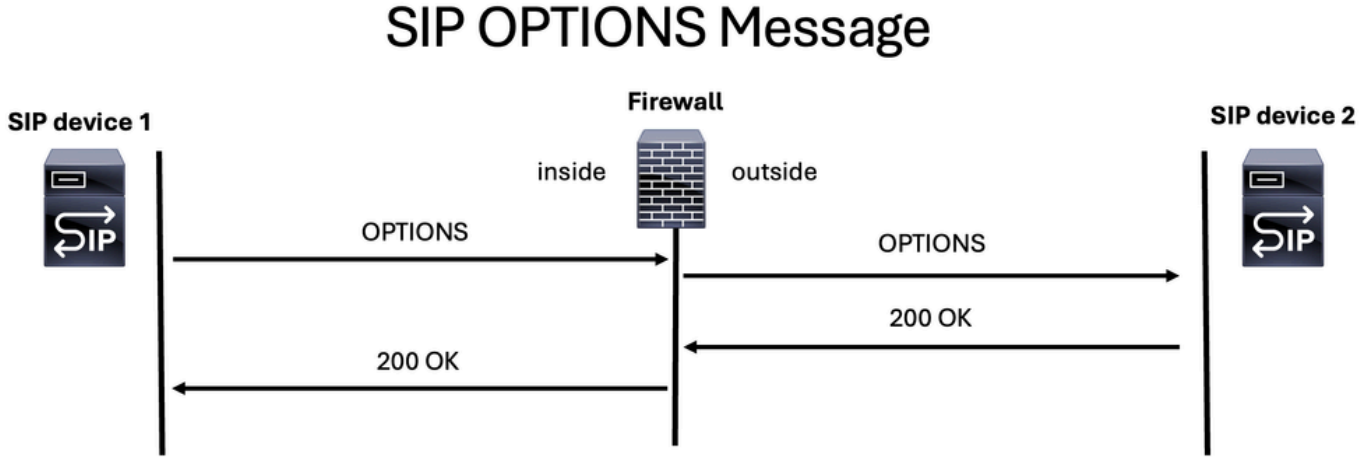
SIP呼叫消息

用于建立和结束语音呼叫的主要SIP消息如下：



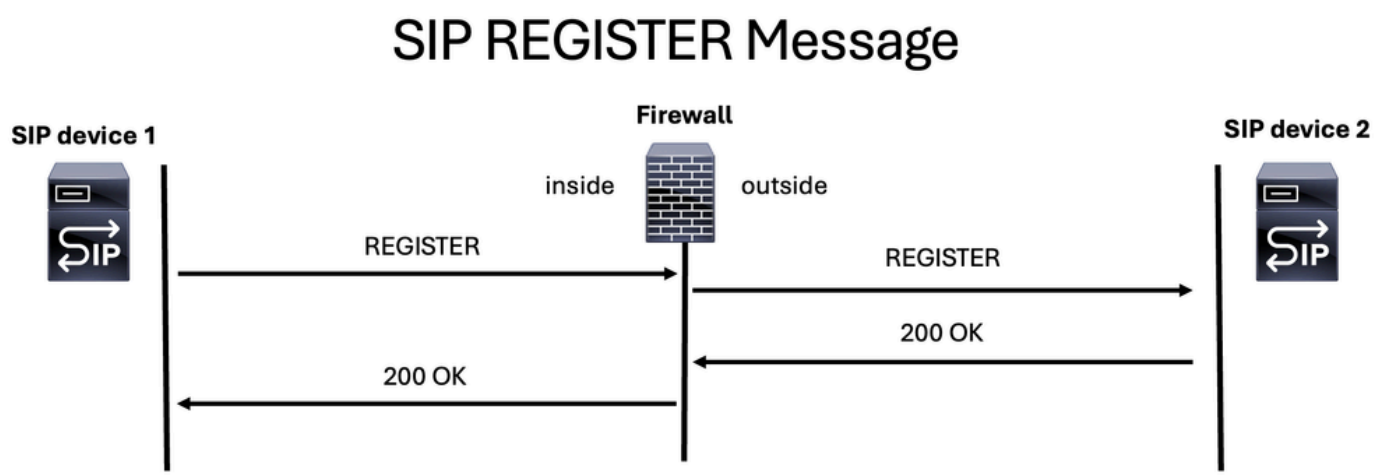
SIP选项消息

SIP OPTIONS消息对于确定SIP设备是否在线以及是否可以响应非常重要。它类似于ping ICMP消息，但在SIP世界上。

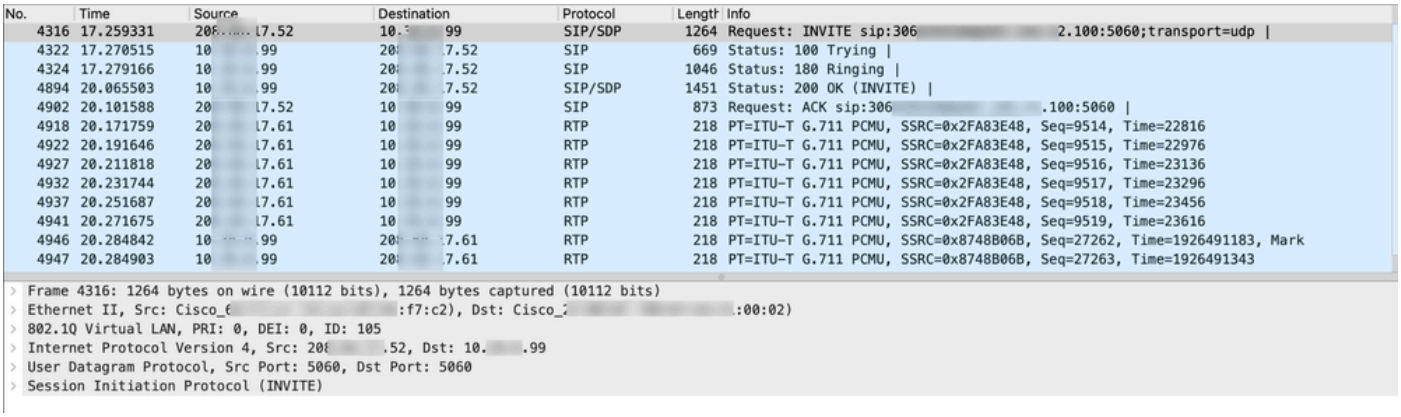


SIP注册消息

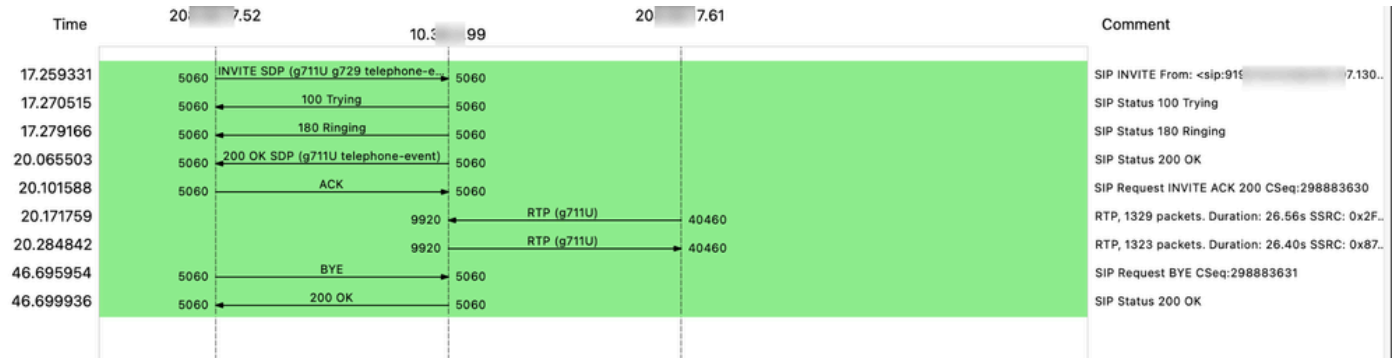
在防火墙故障排除会话期间可以找到的另一条SIP消息是SIP REGISTER消息，它使设备能够向SIP服务器注册。



此数据包捕获显示来自两个SIP设备的请求和响应，以及媒体（语音）流量：

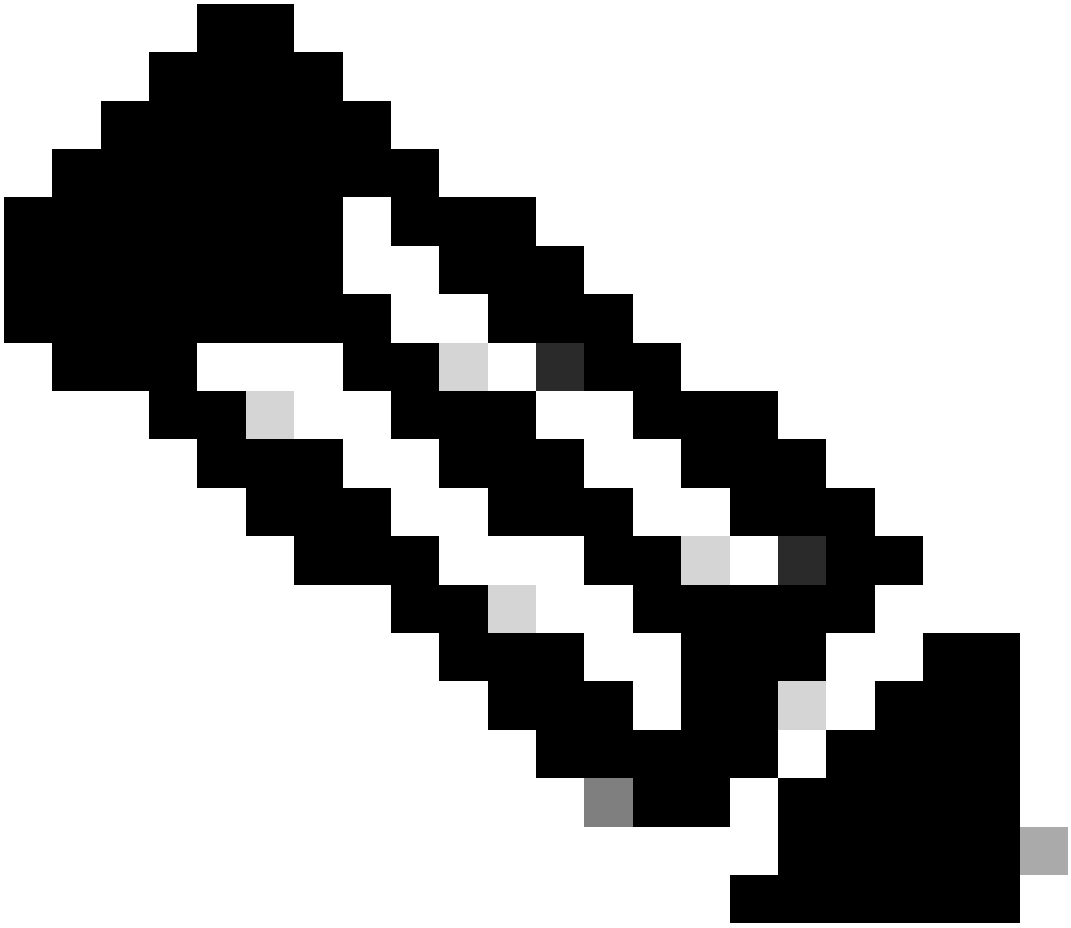


以下是SIP信令和RTP媒体（语音）流的示例：



会话描述协议(SDP)

会话描述协议(SDP)是一种用于描述多媒体会话的媒体流的标准表示方式。它本身不传输介质，但用于在终端之间协商介质类型和格式。SDP与会话发起协议(SIP)配合使用，用于管理和协商会话的媒体特征。

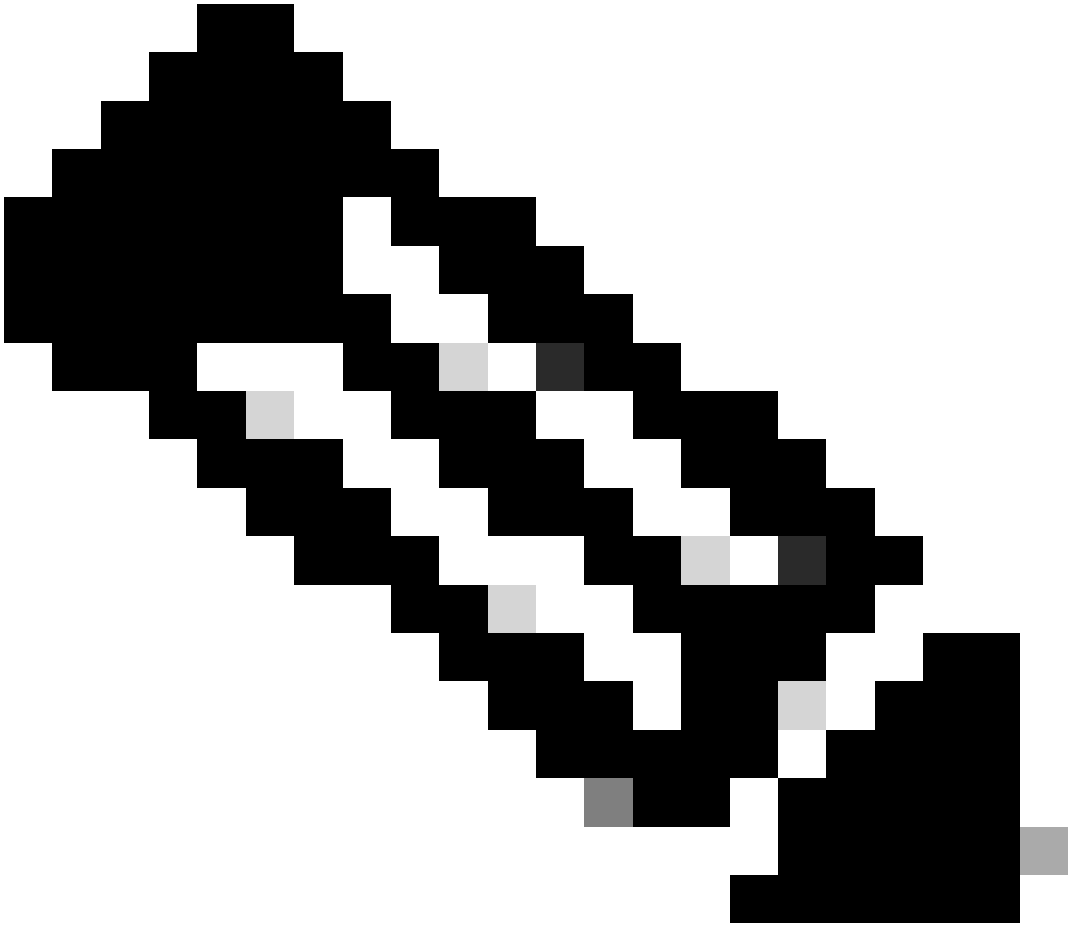


注意：MGCP包含了SDP的概念，SDP也用于同样的目的。

以下是SIP协议中的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=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
```



注意：在示例中，某些SDP消息包含以下参数：

++c-IN IP4:媒体服务器的IP地址

++m=音频：这表示媒体类型为音频。

++8266:这是发送音频流的端口号。

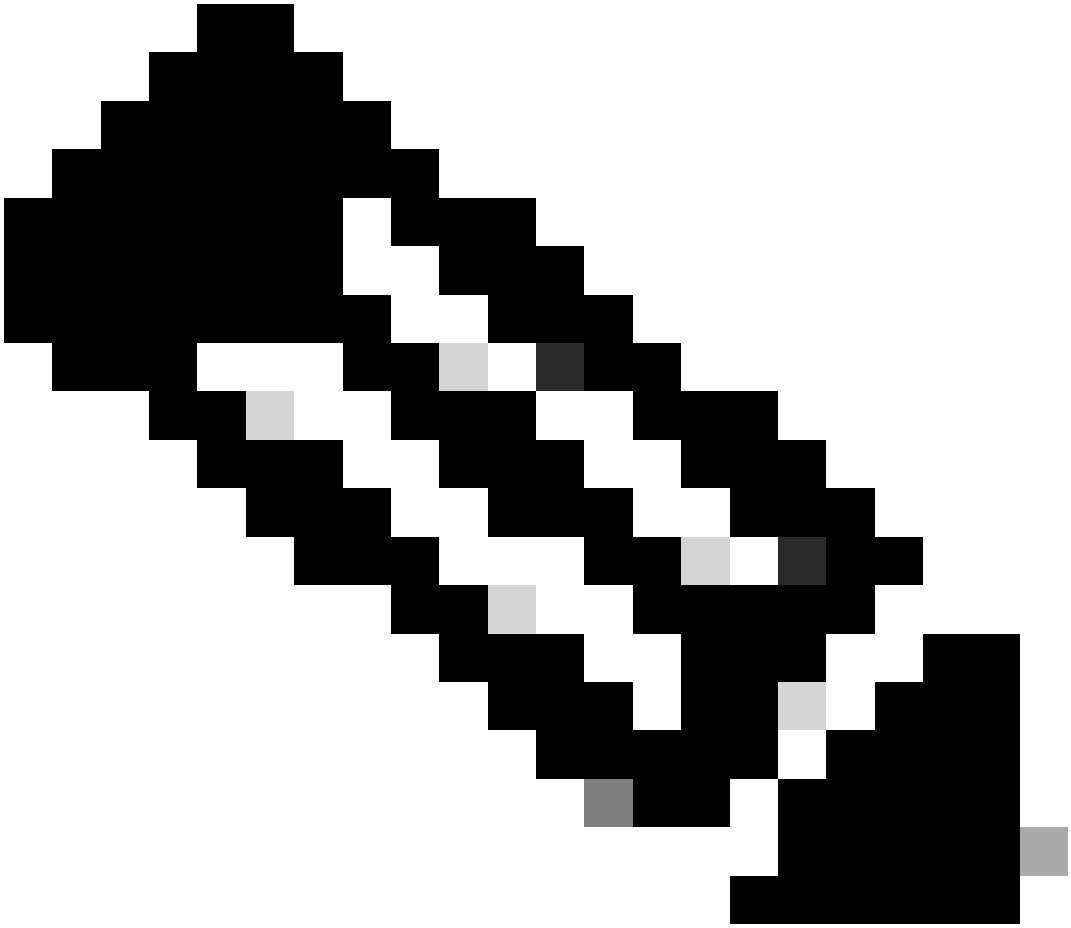
++RTP/AVP:这指定传输协议，即使用音频/视频配置文件(AVP)的RTP。

++18 127:这些是音频编解码器的负载类型。负载类型18通常对应于G.729编解码器，而127是动态负载类型，可以根据终端之间的协商分配给编解码器。

会话描述协议(SDP)可以在几条SIP消息中找到，例如：INVITE、183 Session in Progress、200 OK、ACK等。SDP是各方之间交换语音和/或视频功能的应答方法。排除呼叫故障时，必须了解三个主要概念：

1. 早期提供

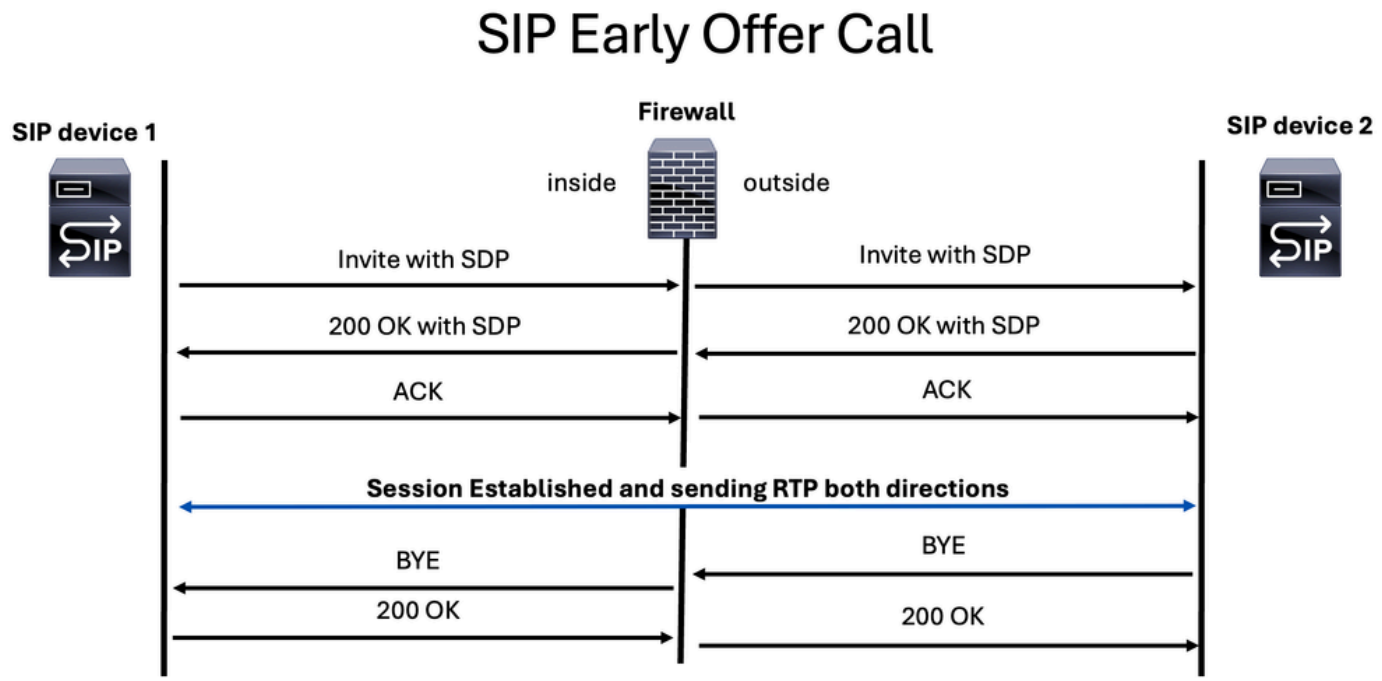
2. 延迟提供
3. 早期媒体



注意：了解SDP消息的目标至关重要，因为防火墙上的检查功能不仅可以修改SIP报头中的IP地址，还可以修改SDP部分中的IP地址。

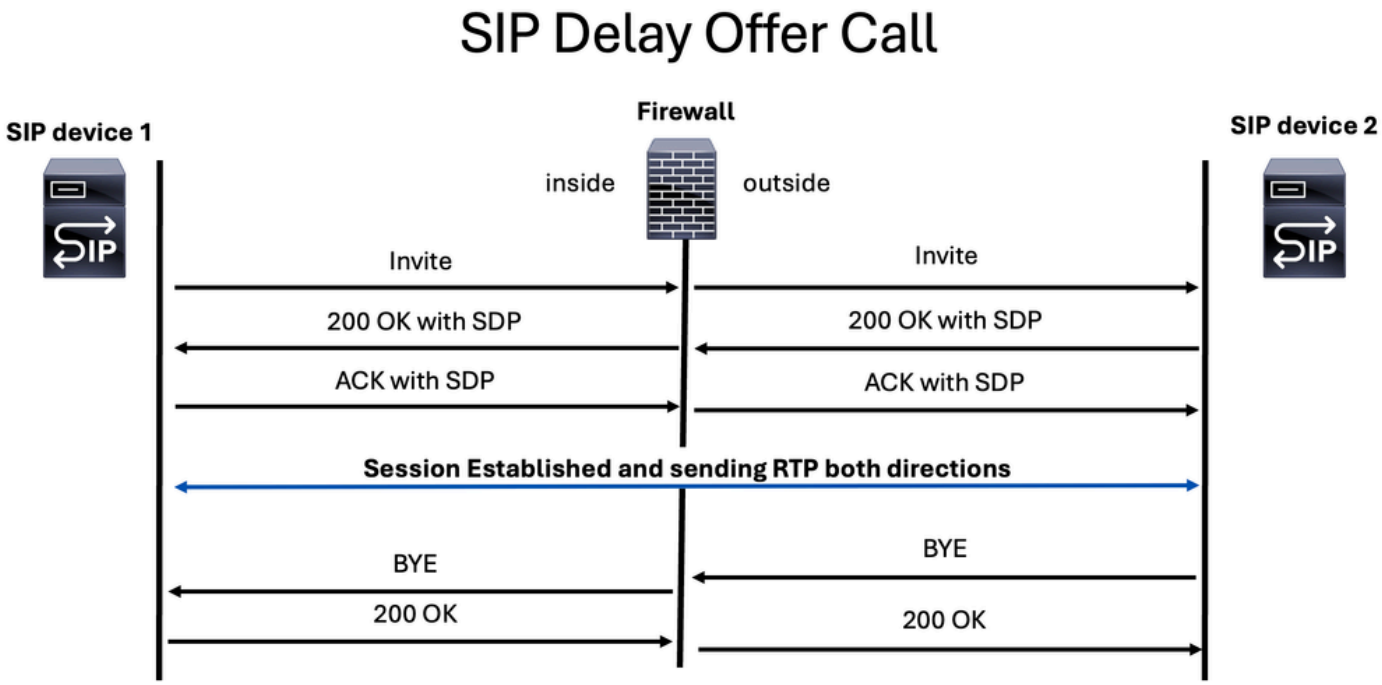
早期提供

SDP上的媒体参数位于INVITE和200 OK SIP消息中。



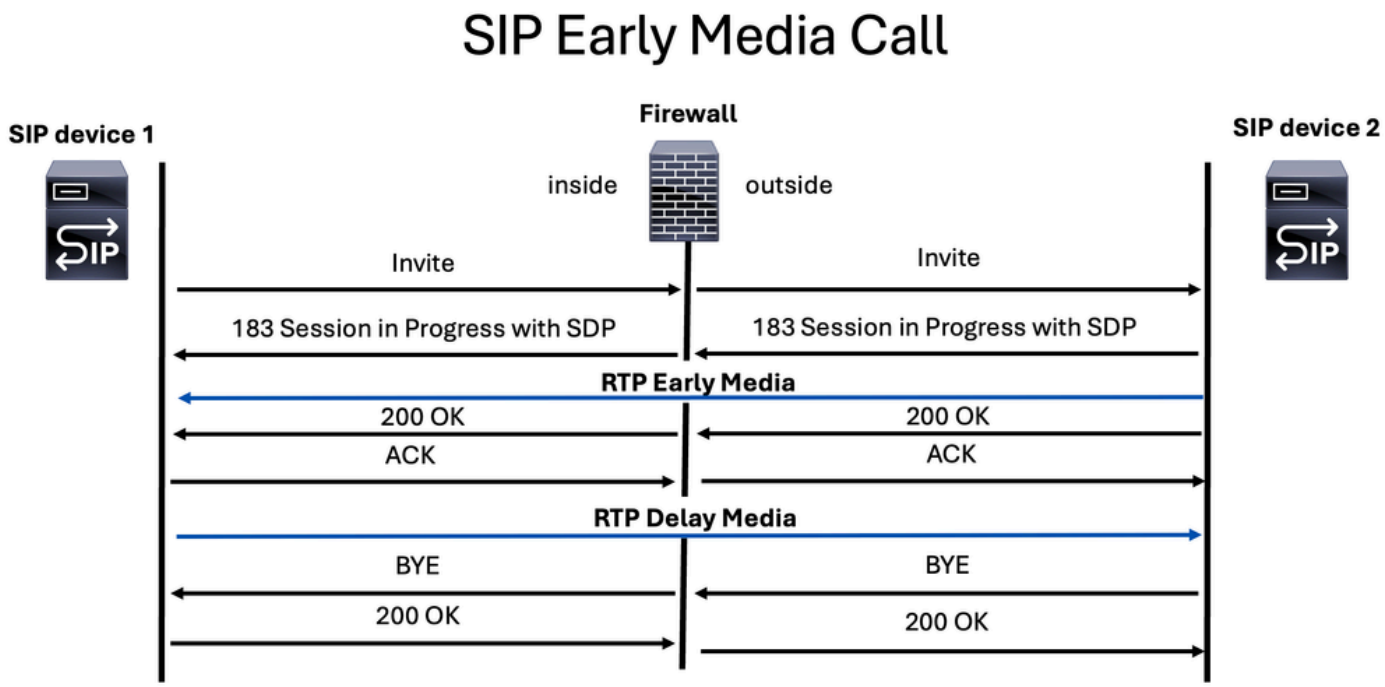
延迟提供

在此方法中，在200 OK和ACK SIP消息上找到SDP。



早期媒体

早期媒体通过称为“183会话进度”响应的特定SIP消息传输。此消息包括会话描述协议(SDP)，其中包含被叫方的媒体参数。在呼叫正式接通之前，运营商和SIP提供商通常使用它向呼叫者发送自动语音消息或其他媒体。

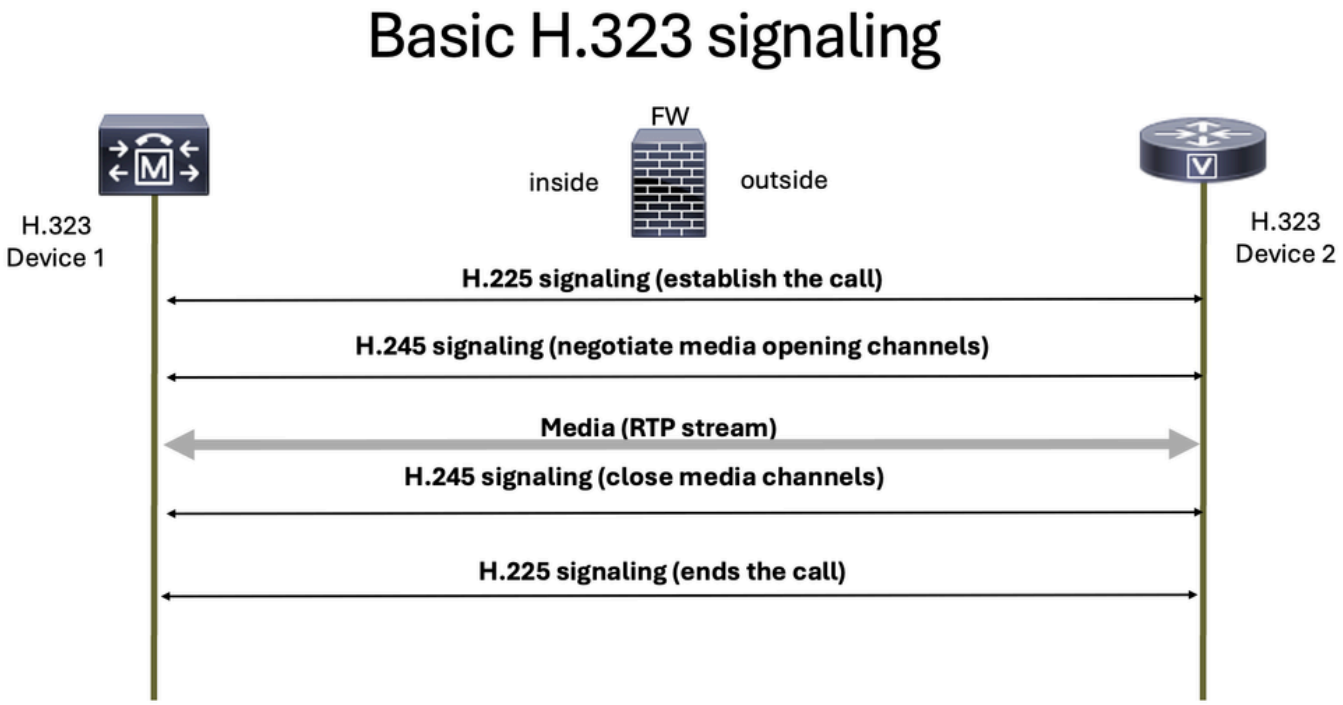


H.323

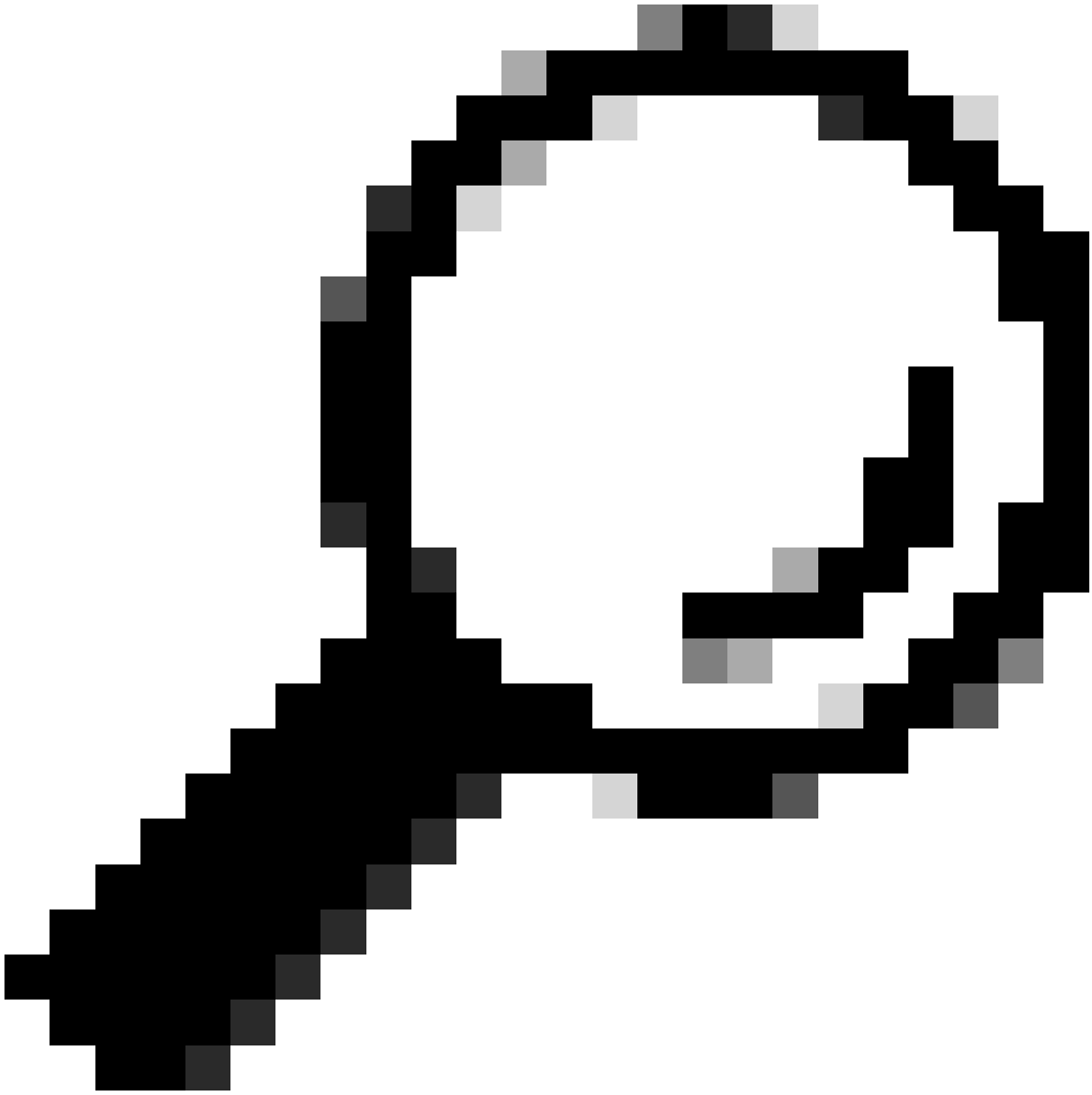
H.323是由国际电信联盟(ITU)定义的一组协议，用于通过分组交换网络（例如Internet）进行语音、视频和数据通信。

H.323协议由两个主要组件组成：

1. H.225:这将处理呼叫信令，包括呼叫的建立和终止。
2. H.245:负责能力交换以及音频和视频频道的打开和关闭。



H.323信令协议使用的端口是1718、1719和1720。

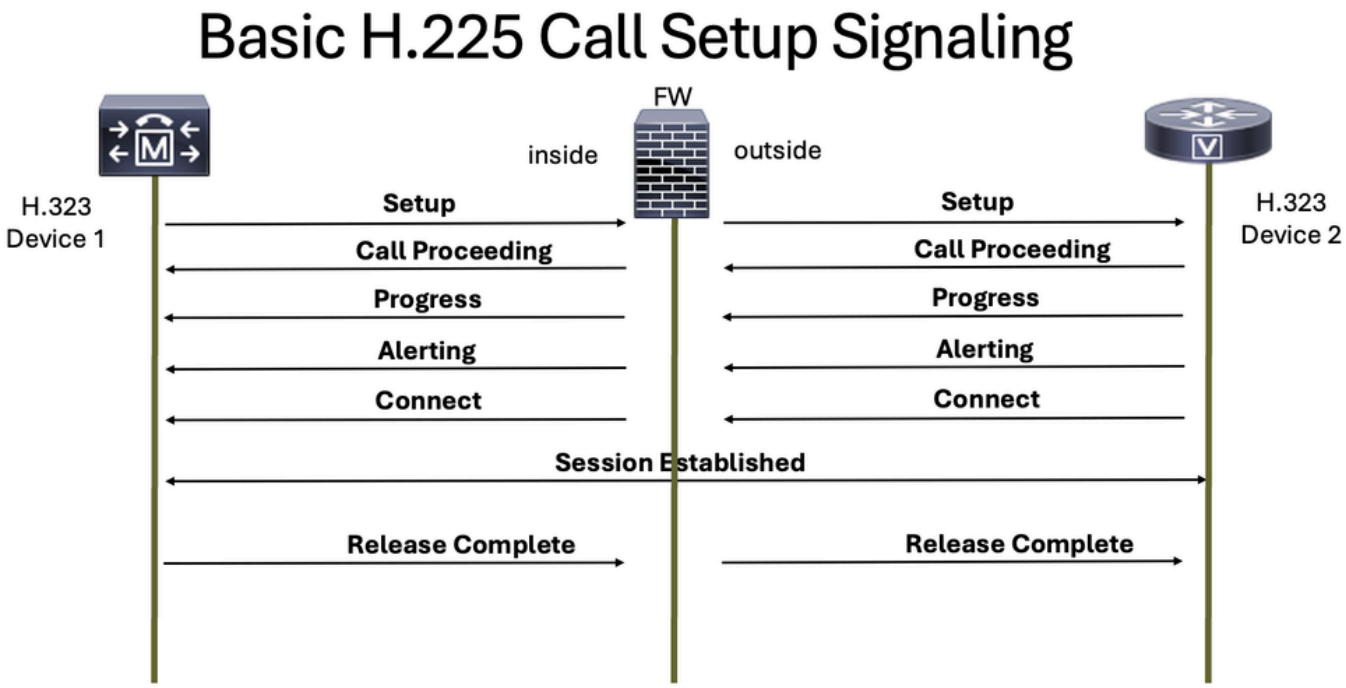


提示：由于使用TLS进行加密，在从UDP切换到TCP时，安全H.323协议通信可能会遇到问题，这会导致防火墙错误地阻止连接作为可疑活动，因此将防火墙配置为允许H.323终端或服务器的UDP和TCP流量至关重要。

H.323协议具有两种操作模式：缓慢启动和快速启动。

H.225

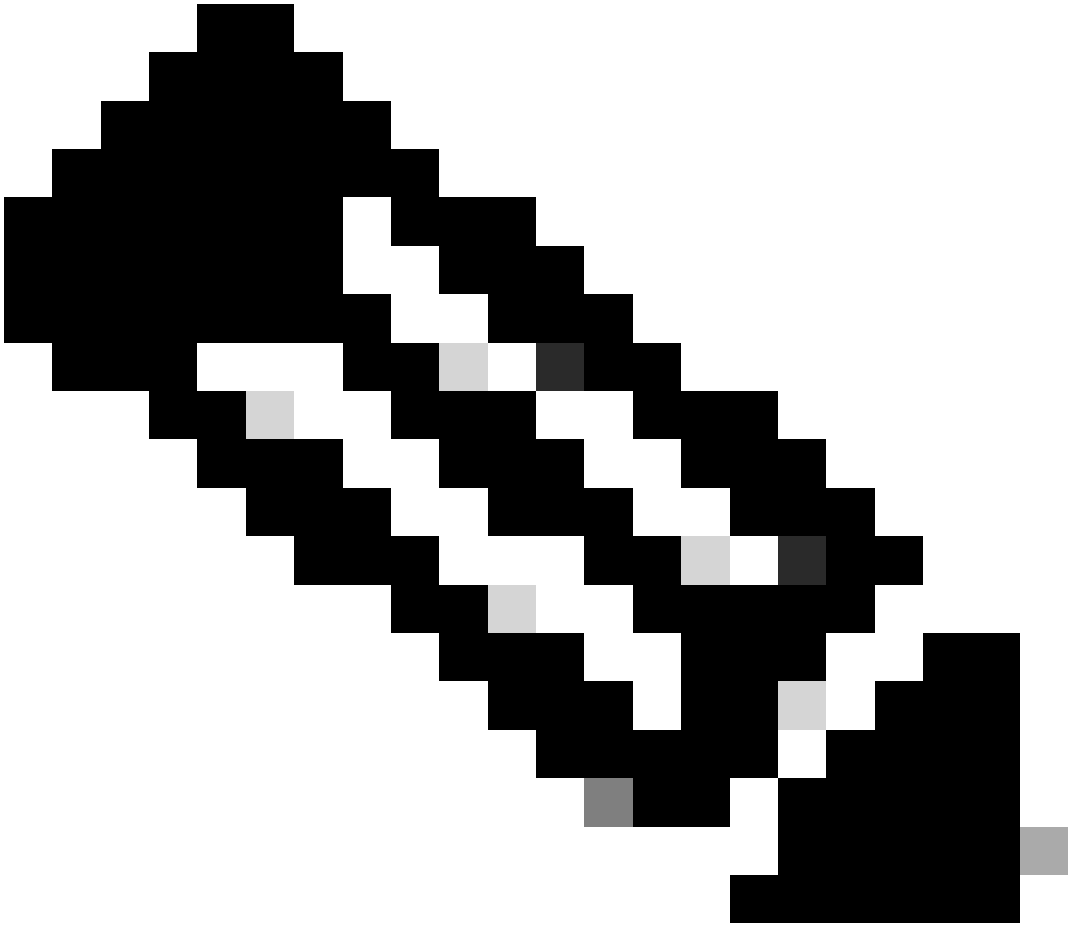
当其中一方挂断电话时，此协议负责建立呼叫和结束语音呼叫。



H.245

H.245提供以下功能：

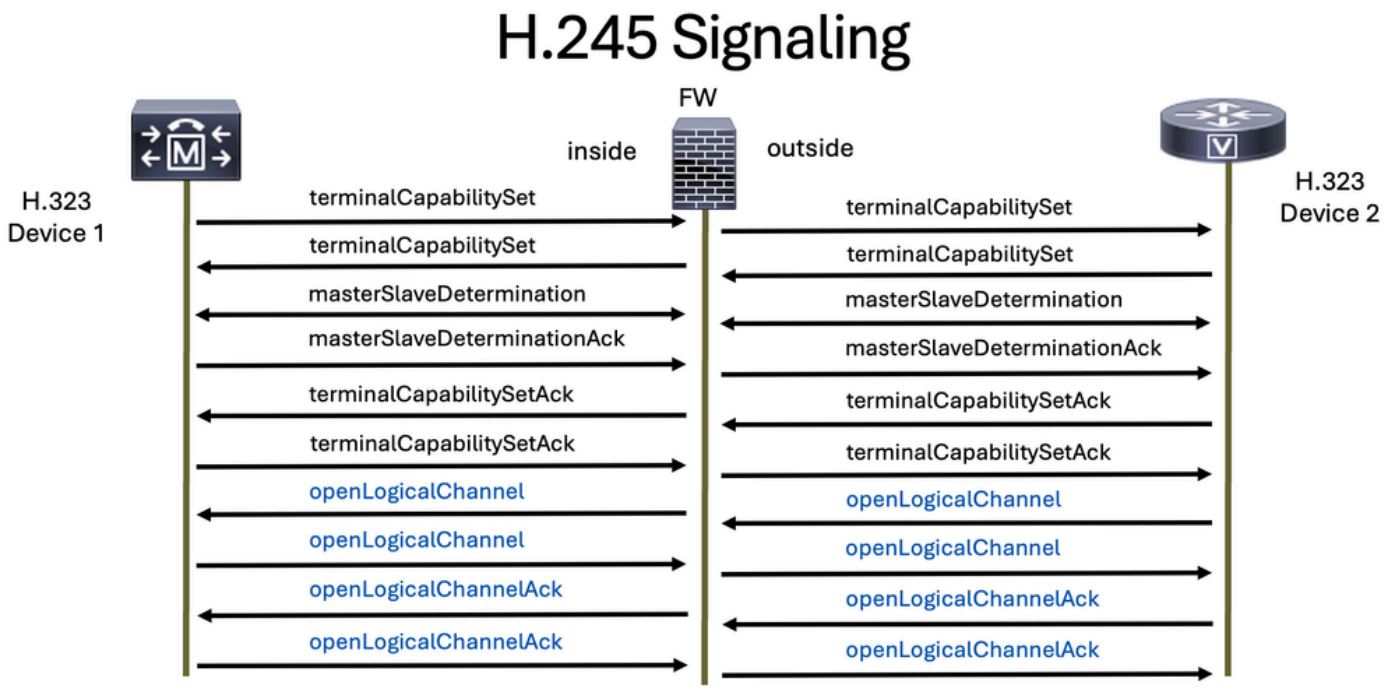
- 终端功能交换
- 主/从确定
- 逻辑信道信令



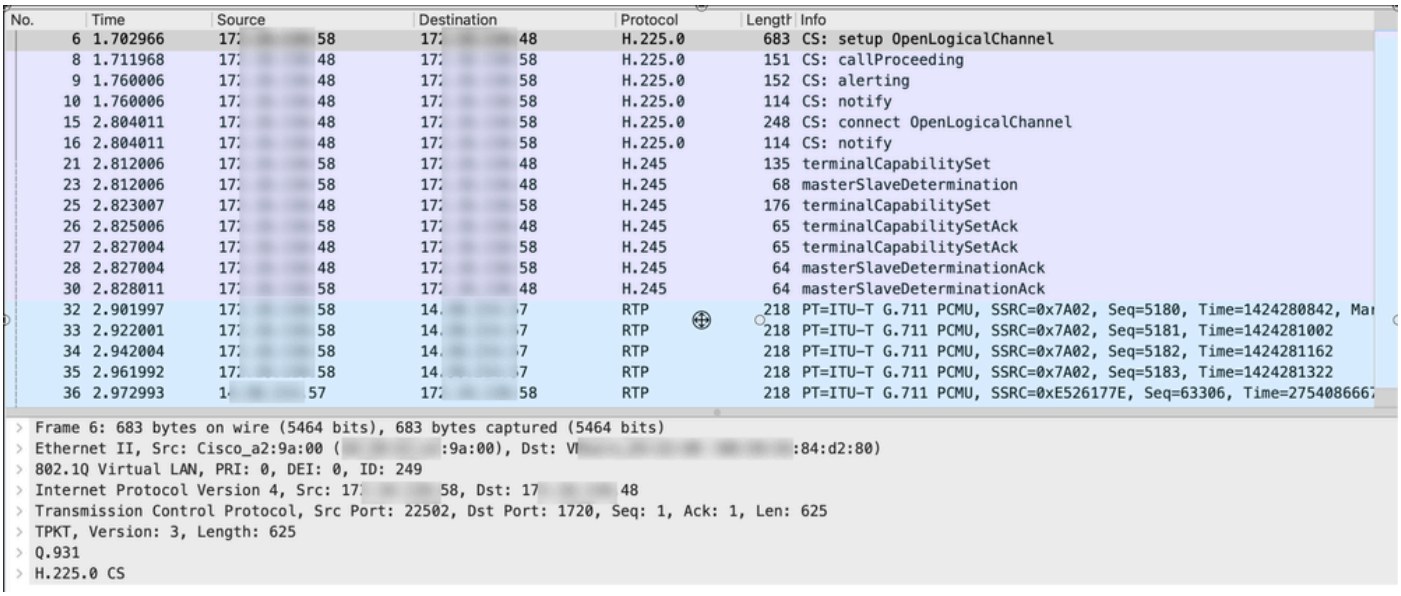
注意：本文档中使用的“主设备”和“从设备”术语硬编码为原始H.323协议，并不反映公司的策略或价值。我们致力于促进包容和尊重的语言。

H.245协议在收到H.225连接消息后发送。

此协议有助于确定哪个语音协议用于RTP，并且它是在为其打开逻辑信道和关闭逻辑信道消息时指定的。



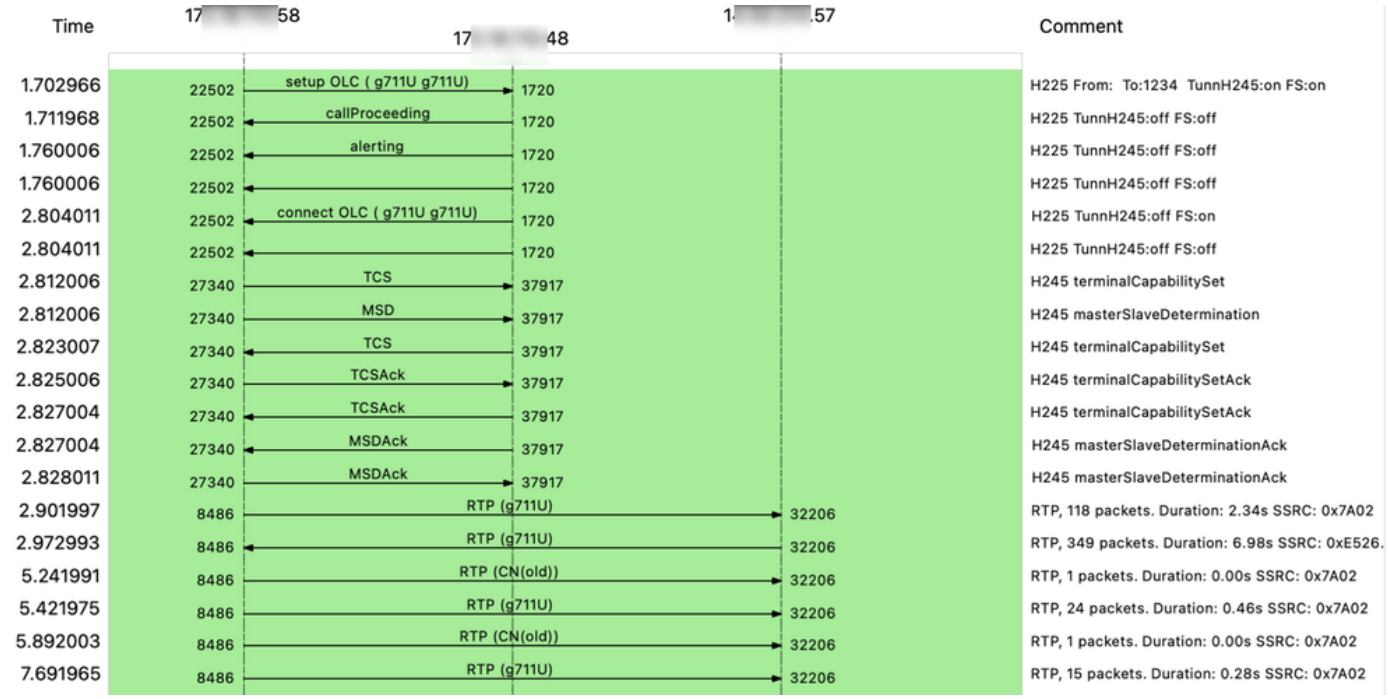
此数据包捕获显示来自H.225和H.245的两个H.323设备的请求和响应，以及媒体（语音）流量：

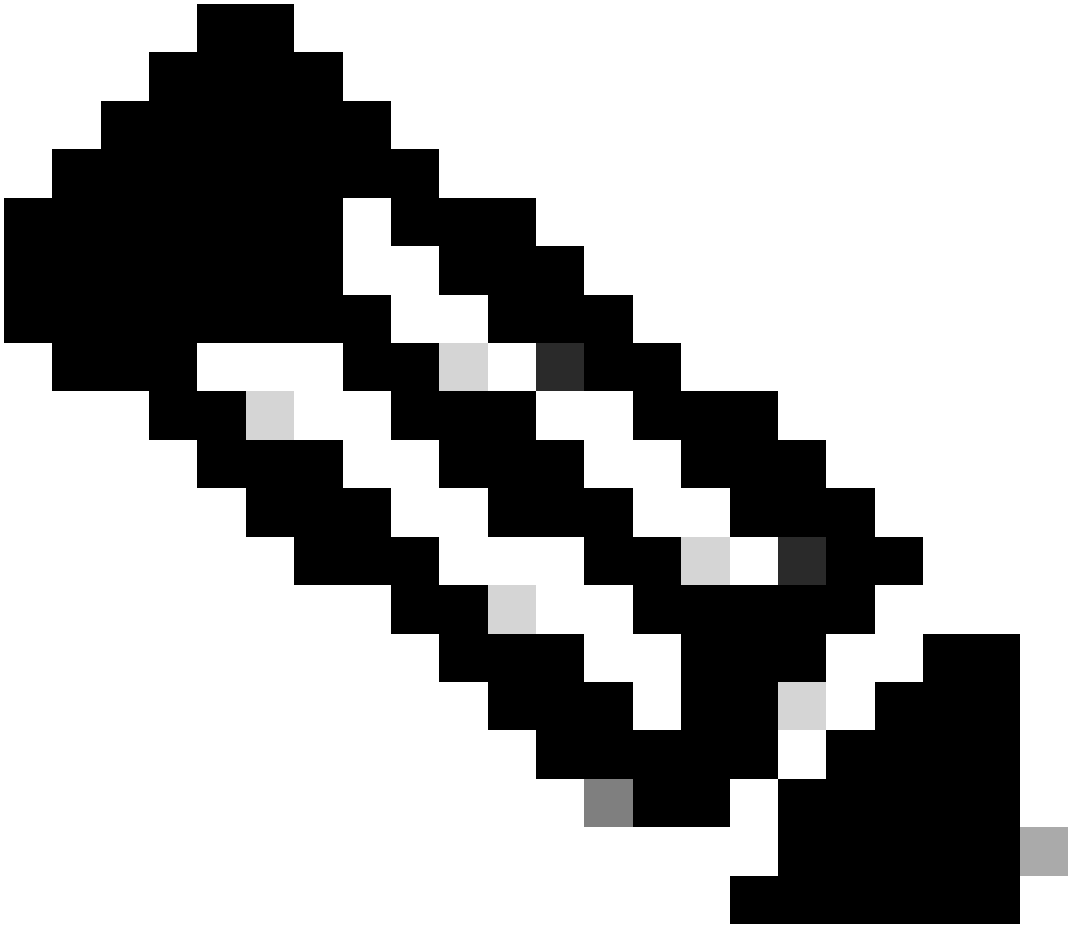


No.	Time	Source	Destination	Protocol	Length	Info
6	1.702966	17 58	17 48	H.225.0	683	CS: setup OpenLogicalChannel
8	1.711968	17 48	17 58	H.225.0	151	CS: callProceeding
9	1.760006	17 48	17 58	H.225.0	152	CS: alerting
10	1.760006	17 48	17 58	H.225.0	114	CS: notify
15	2.804011	17 48	17 58	H.225.0	248	CS: 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	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
```

以下是使用H.225和H.245以及RTP媒体（语音）的H.323信令流的示例：

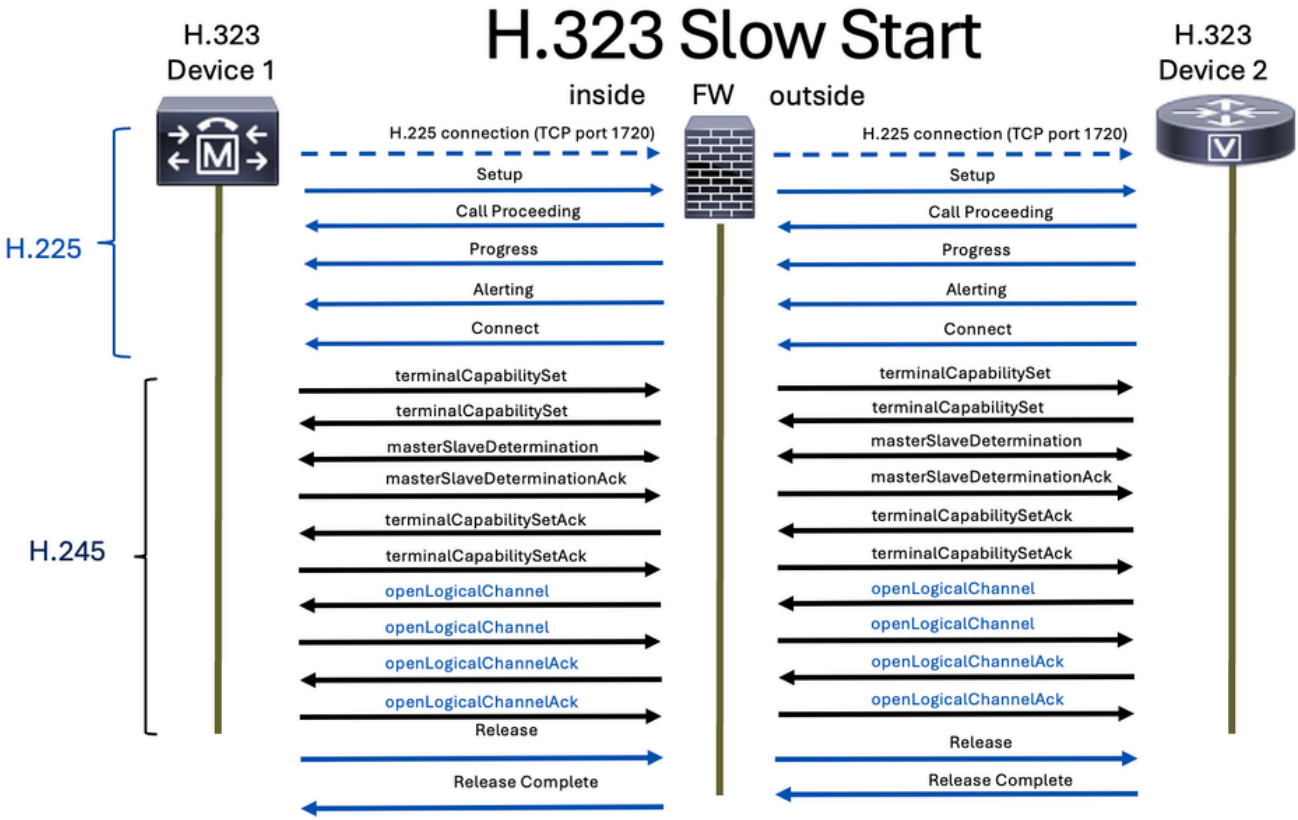

Time
Comment
1.702966 22502 setup OLC (g711U g711U) 1720 H225 From: To:1234 TunnH245:on FS:on
1.711968 22502 callProceeding 1720 H225 TunnH245:off FS:off
1.760006 22502 alerting 1720 H225 TunnH245:off FS:off
1.760006 22502 1720 H225 TunnH245:off FS:off
2.804011 22502 connect OLC (g711U g711U) 1720 H225 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



注意：默认情况下，思科安全防火墙威胁防御(FTD)和安全防火墙自适应安全设备(ASA)上启用H.323检测。

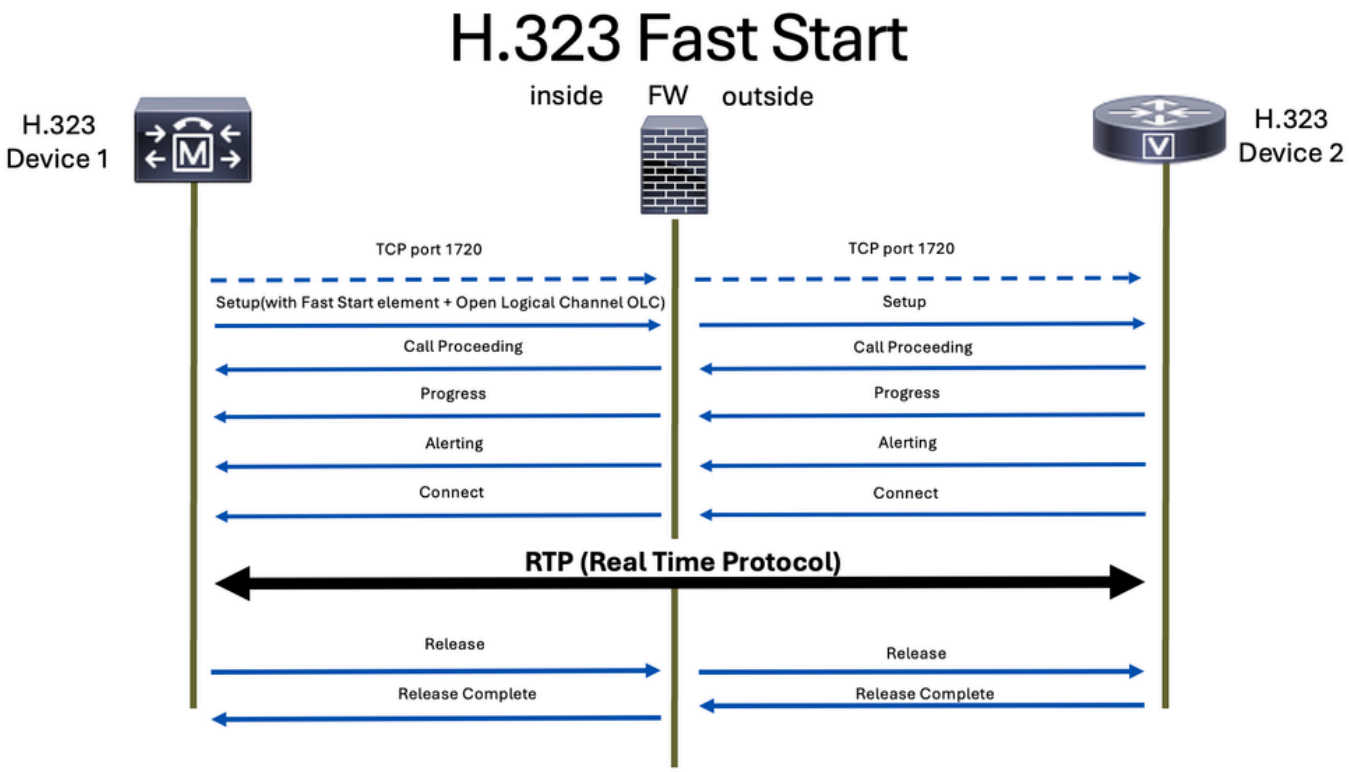
缓慢启动

在慢启动模式下，呼叫建立过程涉及建立媒体信道之前的数个信令步骤。步骤包括设置、呼叫继续、警报和连接。完成这些步骤后，H.245媒体协商将单独执行。这意味着在初始呼叫信令完成之前不会建立媒体信道，这会导致设置时间较长。



快速启动

相反，快速启动模式允许在初始设置消息内进行媒体协商。这意味着可以更快地建立媒体通道，因为协商是在初始呼叫建立过程中进行的。Fast start通过减少交换的消息数量和建立媒体通道之前所需的处理量来简化流程。

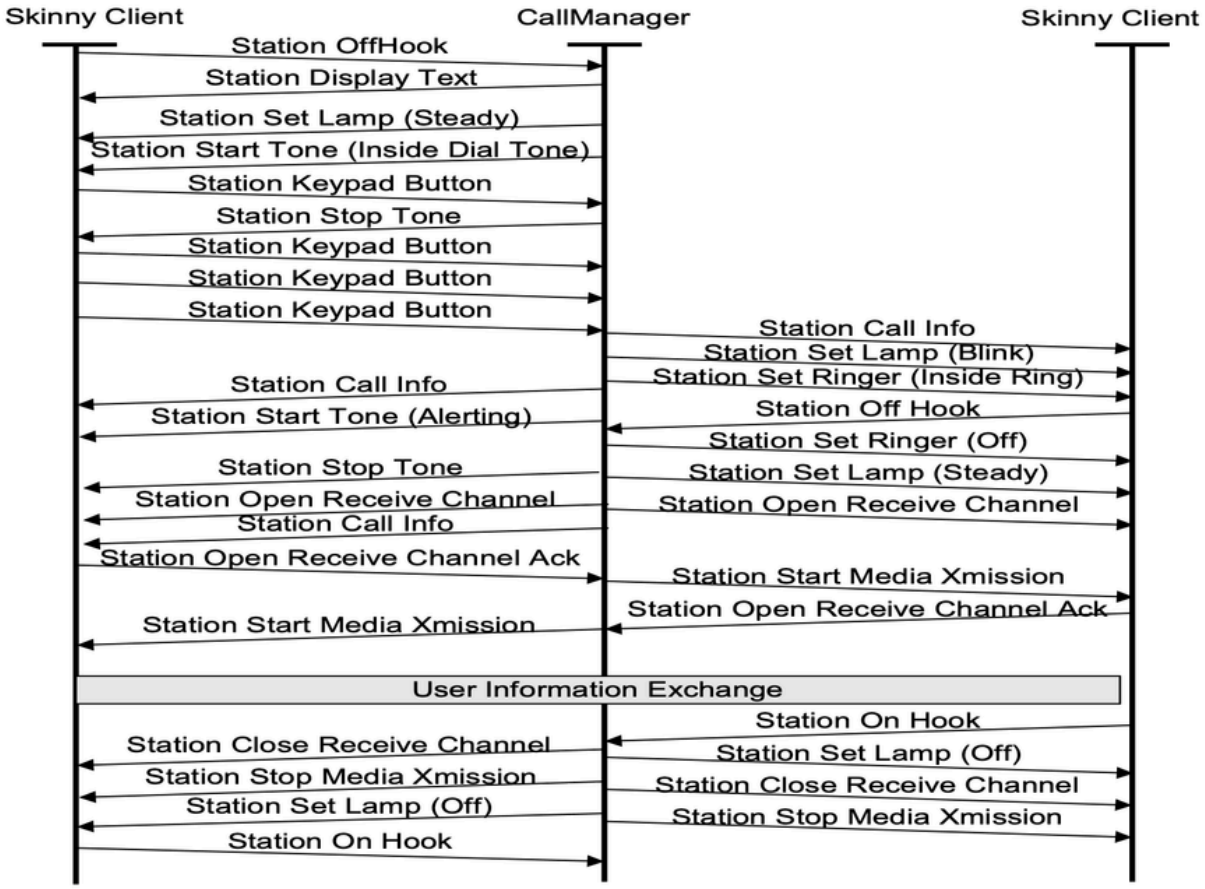


SCCP

瘦客户端控制协议(SCCP)，通常简称为Skinny，是思科专有信令协议。它主要由Cisco Unified Communications Manager(CUCM)、Cisco Unified Communications Manager Express(CME)路由器和Cisco IP电话用于促进呼叫设置和控制。

SCCP协议使用端口2000上的TCP作为非安全SCCP，使用端口2443作为安全SCCP。

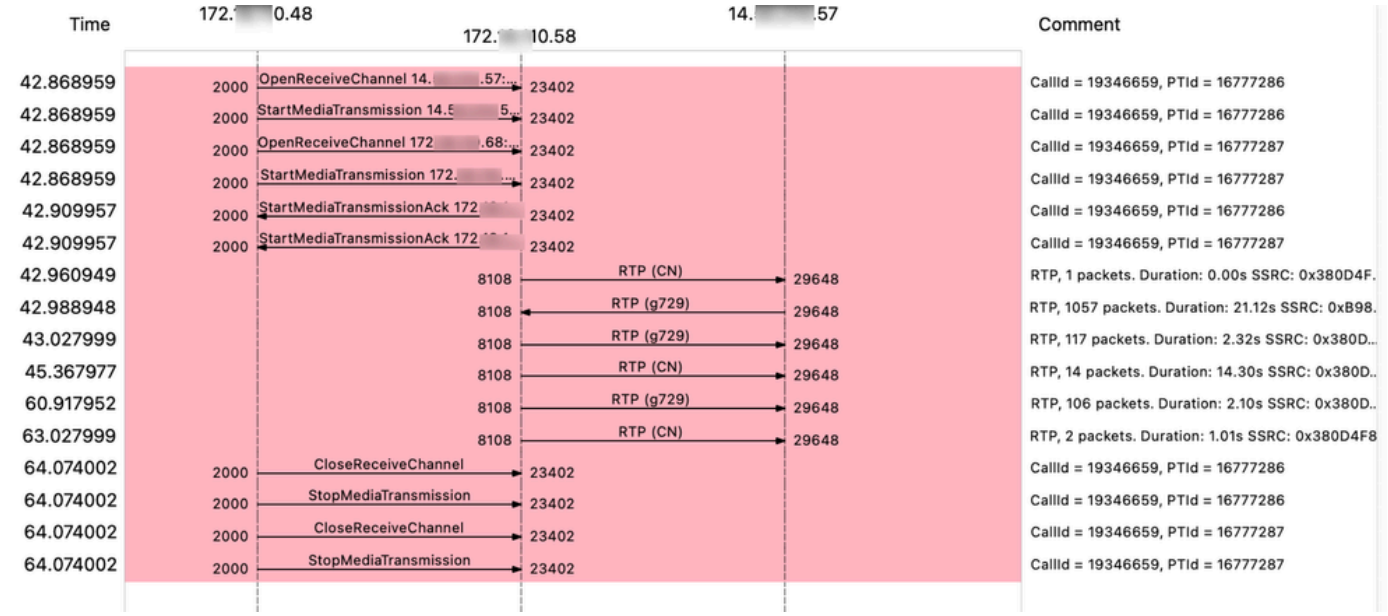
以下是可以在SCCP呼叫中找到的常见SCCP消息：

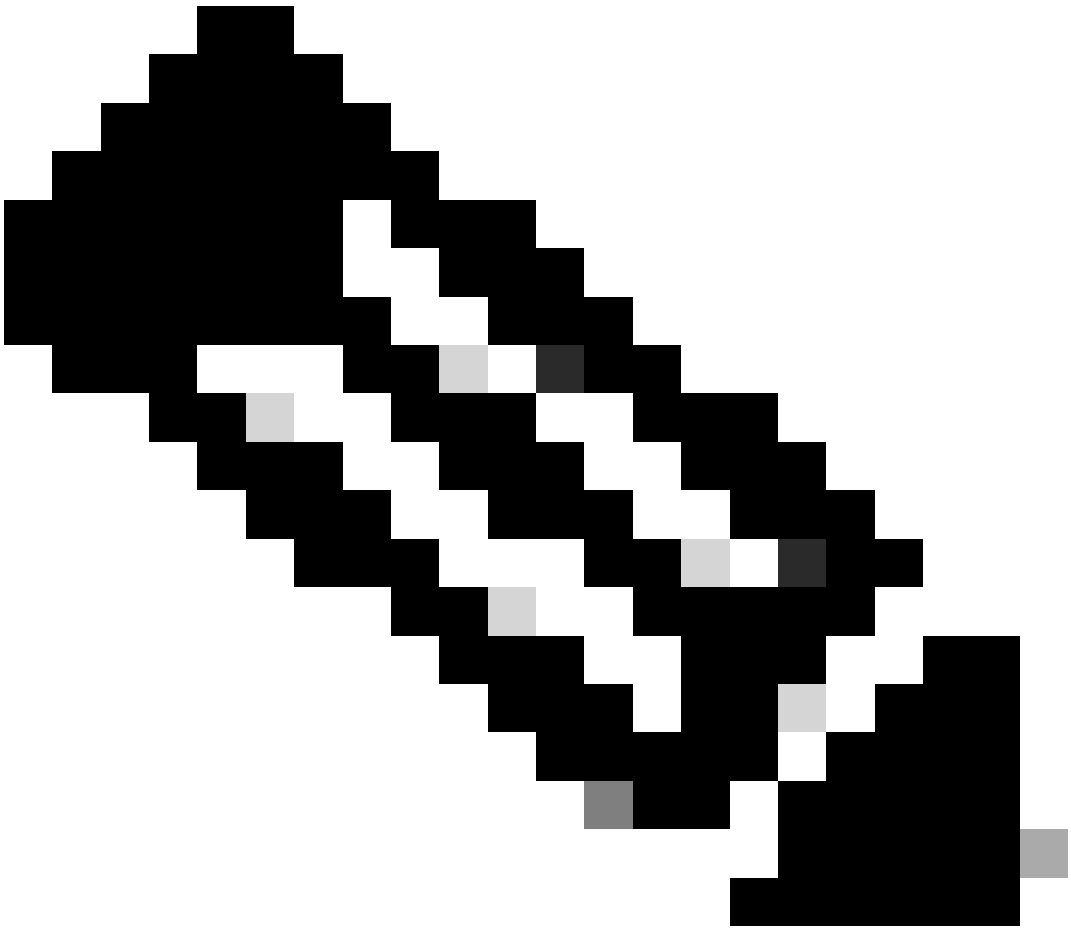


此数据包捕获显示来自两个SCCP设备的请求和响应，以及媒体（语音）流量：

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

以下是SCCP信令和RTP媒体（语音）流的示例：





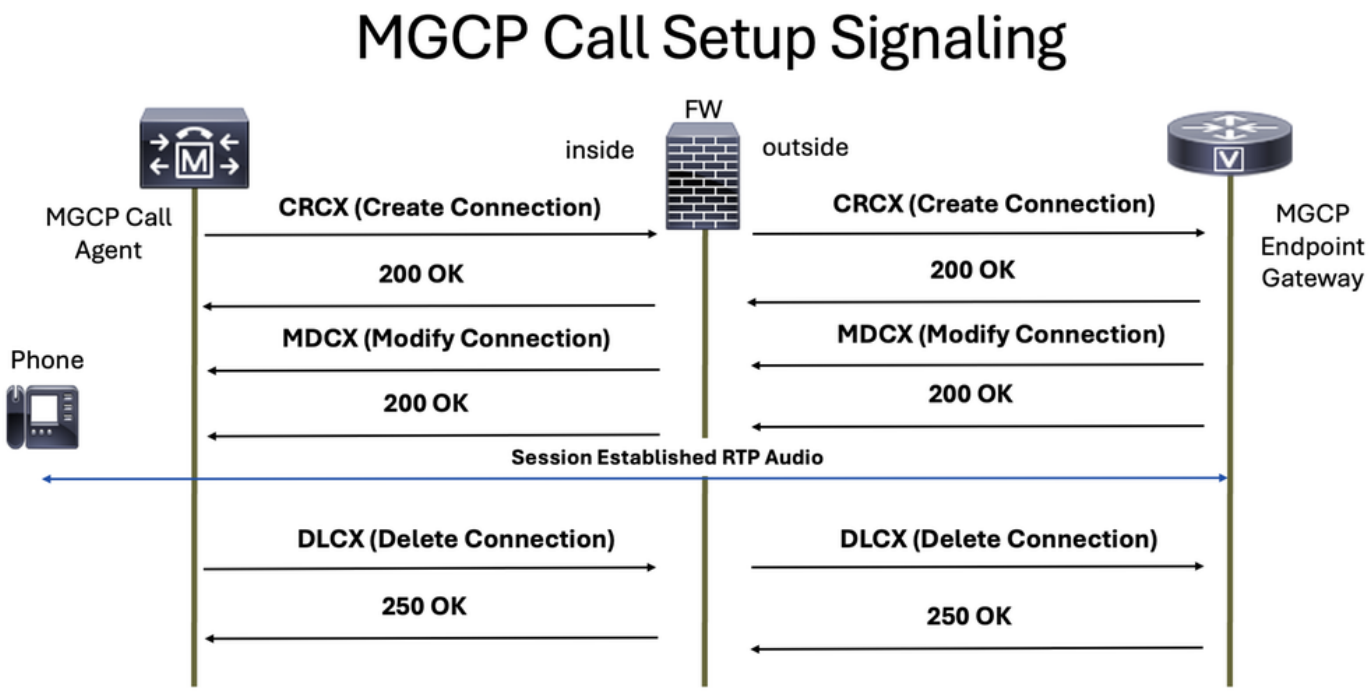
注意：默认情况下，思科安全防火墙威胁防御(FTD)和安全防火墙自适应安全设备(ASA)上启用SCCP检测。

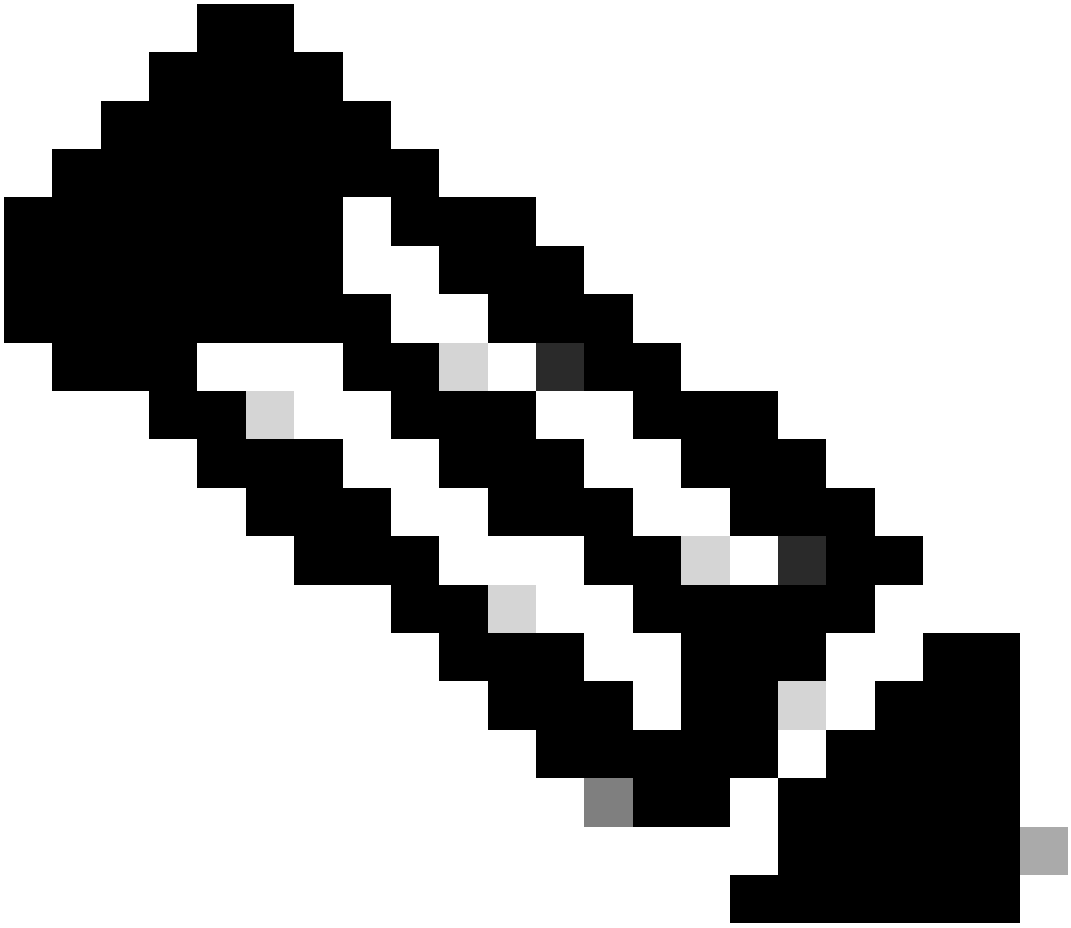
MGCP

媒体网关控制协议(MGCP)是呼叫控制设备（例如CUCM）用于控制VoIP呼叫的协议。

MGCP信令协议在RFC 2705中定义，使用TCP端口2428和UDP端口2427进行通信。

您期望呼叫通信的MGCP正常数据包是：



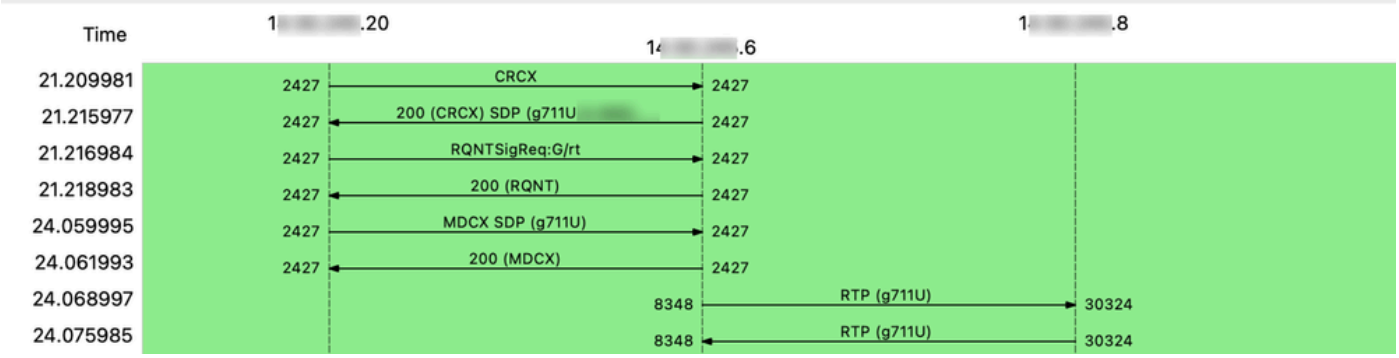


注意：思科安全防火墙威胁防御(FTD)和安全防火墙自适应安全设备(ASA)的默认检测策略中未启用MGCP检测，因此，如果需要此检测，必须启用它。

此数据包捕获显示来自两个MGCP设备的请求和响应，以及媒体（语音）流量：

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

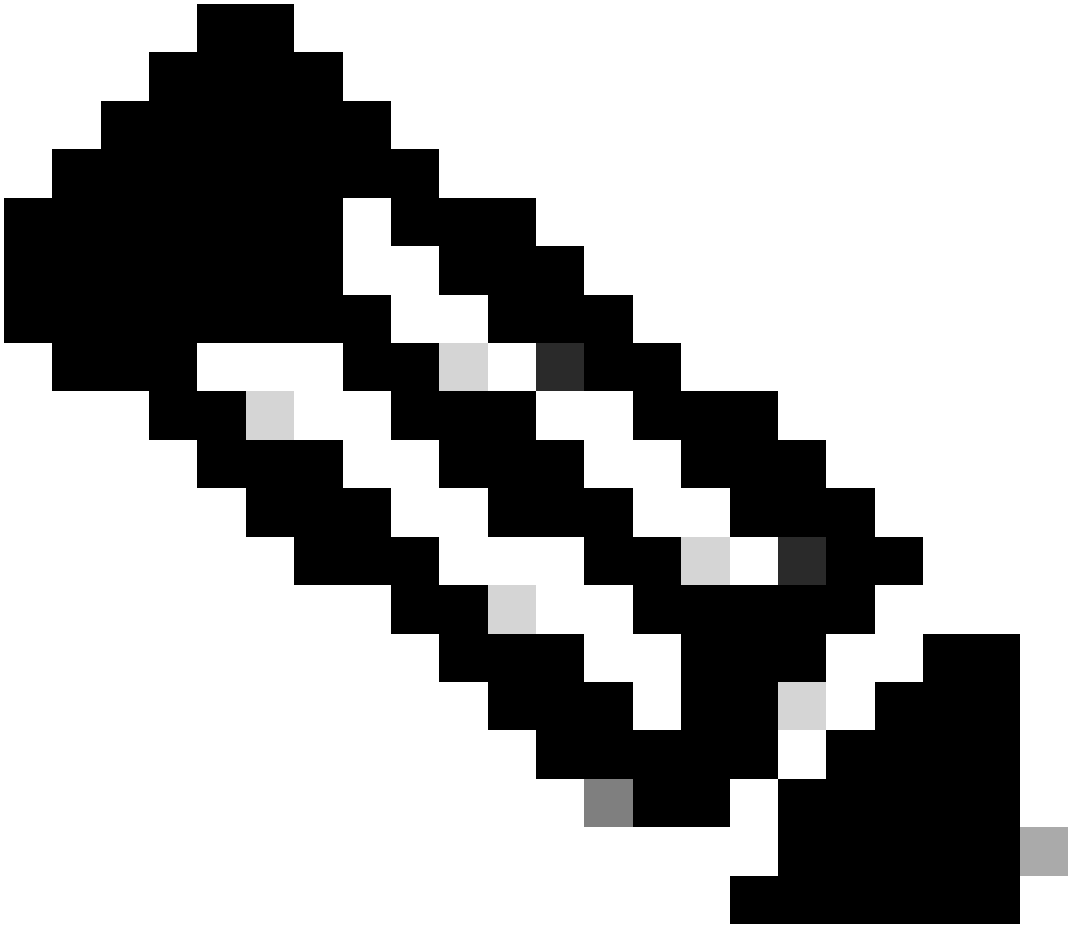
以下是MGCP信令和RTP媒体（语音）流的示例：



最佳实践

对于ASA:

- 使用允许流量进出两个信令组件（设备或服务器）的允许规则。 这可以受指定信令VoIP协议上使用的端口的限制。
- 允许可发送和/或接收音频和/或视频流的媒体设备之间的RTP端口范围。



注意：请记住，这些音频或媒体设备可能与信令组件（设备或服务器）不同。

对于FTD:

- 定义信令组件（设备或服务器）的预过滤器规则，并定义特定端口以仅限制指定信令协议的流量。
- 配置音频和/或视频RTP协议的预过滤器。

故障排除

排除语音故障时，您需要知道问题是信令还是媒体（语音或视频）还是两者，下面是一些示例，可帮助您区分以下情况：

信令问题示例：

++用户报告呼叫未建立。

++用户无法呼叫其他用户或号码。

++SIP中继未启动，因为OPTIONS sip消息未收到响应。

++我的设备无法注册。

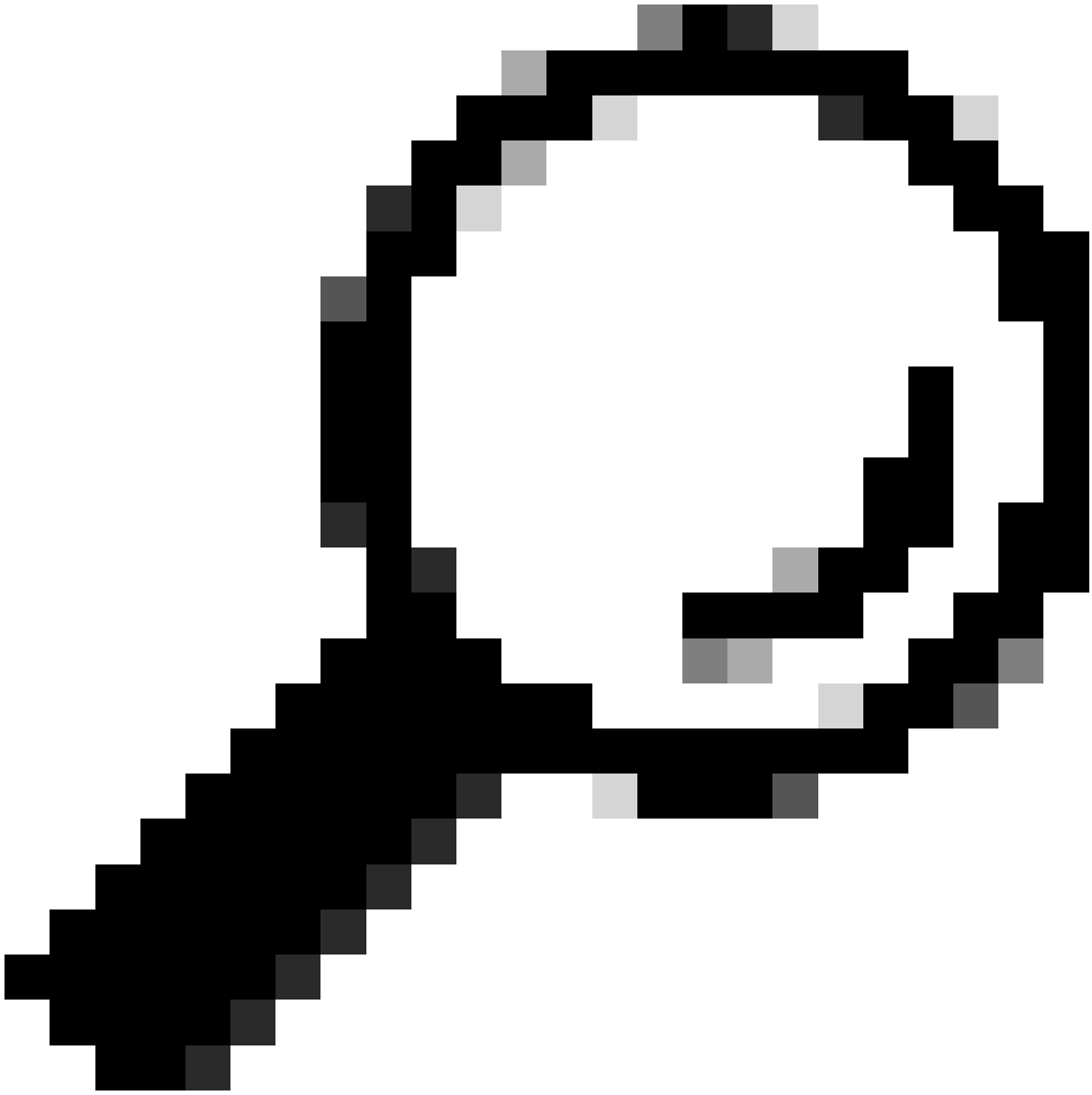
媒体（语音或视频）问题示例：

++存在单向音频问题。

++没有通话中的音频。

++根本就没有视频。

++呼叫保持静音。



提示：在视频呼叫期间，SDP可以协商最多三条媒体线路（m条线路）：音频、视频和图像。每个m线路对应于每个呼叫段的一个单独的实时传输协议(RTP)流，这意味着在呼叫的每个段上最多可以有三个不同的RTP流（每种媒体类型一个）。

排除防火墙上的信令问题

要对信令部分进行故障排除，需要确保：

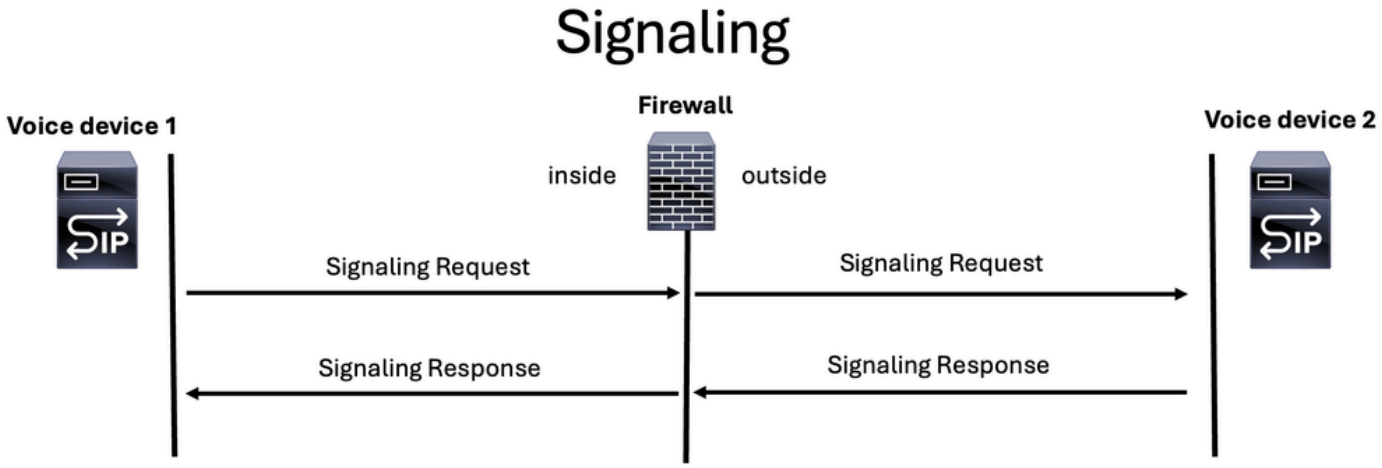
++从入口和出口接口确定呼叫中涉及的所有信令组件（设备或服务器），并在任一安全防火墙的CLI上配置数据包捕获的适当匹配条件。

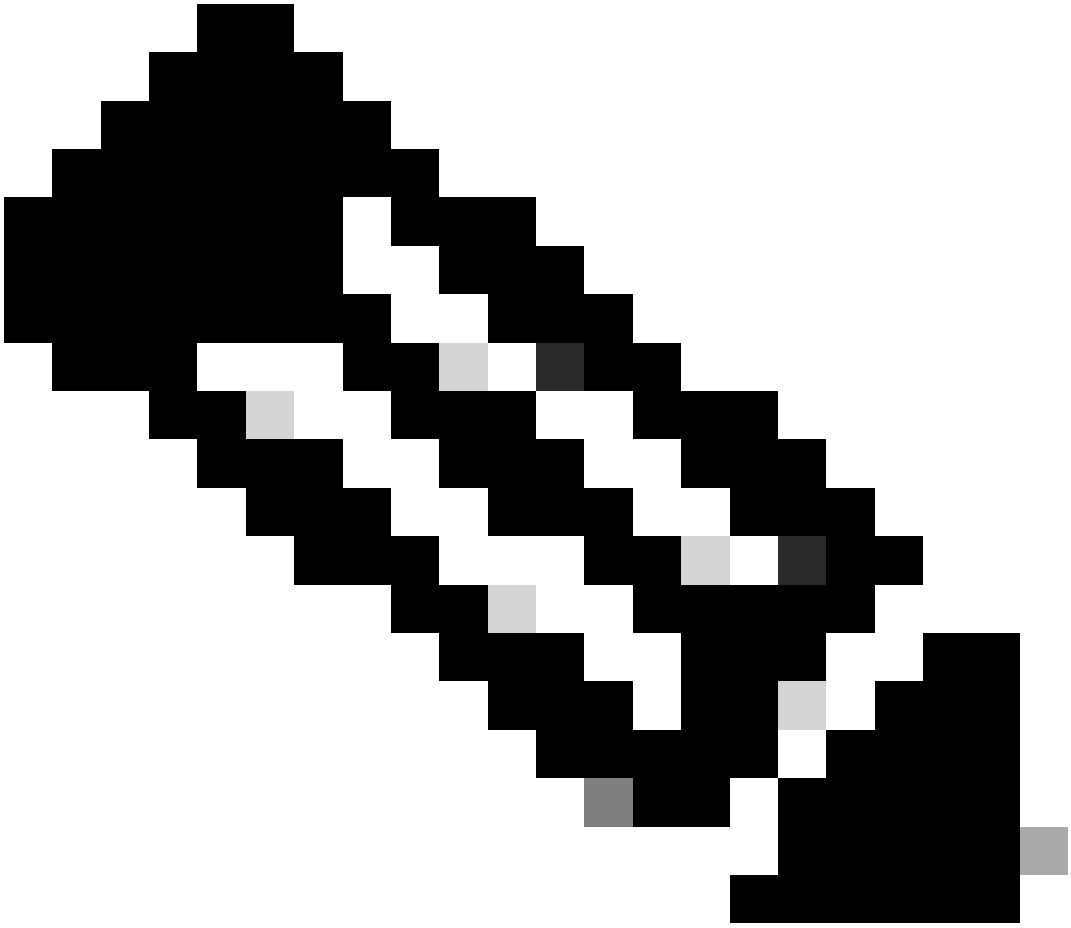
++请记住，入口接口的信令消息数必须与出口接口匹配。

++通过指定信令协议使用TCP还是UDP以及过滤预期端口号，数据包捕获可以更加高效。由于所有

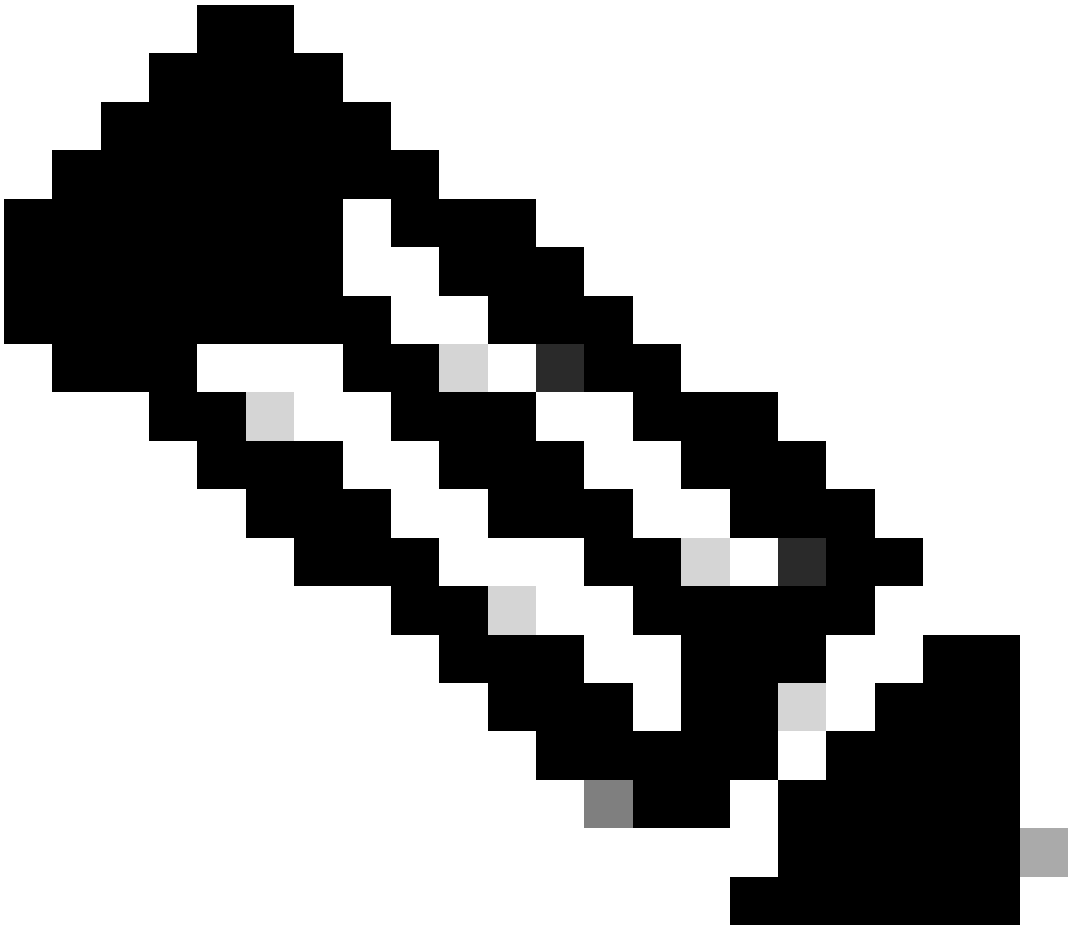
信令协议都通过IP运行，因此在CLI上应用这些过滤器有助于限制您在捕获中看到的流量。

++仅对于出口接口，确保在数据包捕获过滤器中指定分配给出站流量的NAT IP地址。这样可以确保捕获显示在出口接口上的正确流量。





注意：请记住，无论使用哪种信令协议进行语音，都必须始终存在请求和响应，并且必须在入口和出口接口上保持一致。



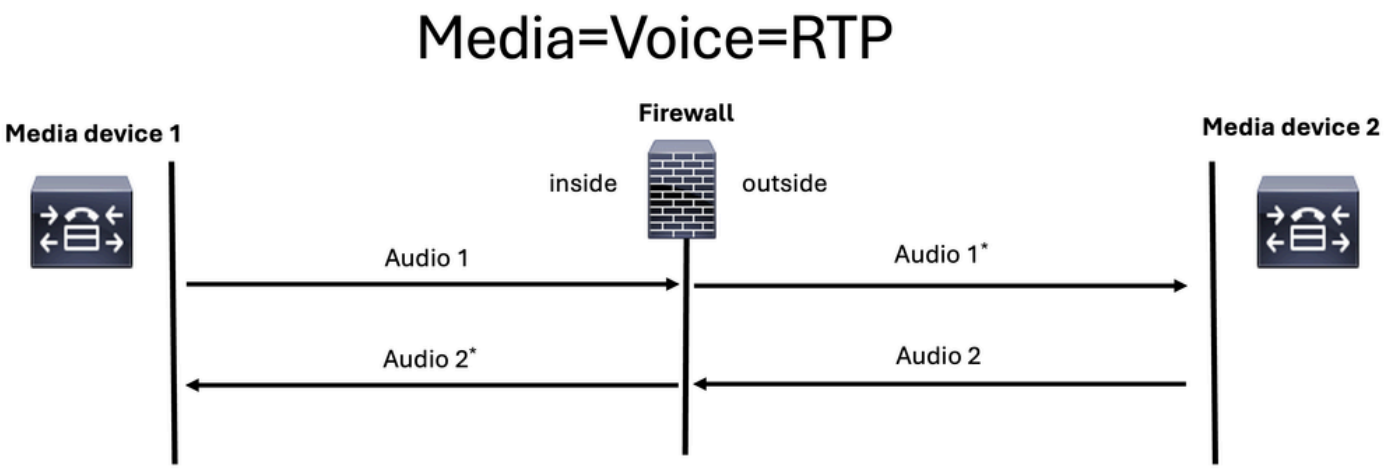
注意：尽可能确保通信路径中仅涉及一个防火墙。在某些部署中，语音信令和媒体流可以穿越单独的防火墙。在这些情况下，请确保在故障排除过程中包含所有相关防火墙

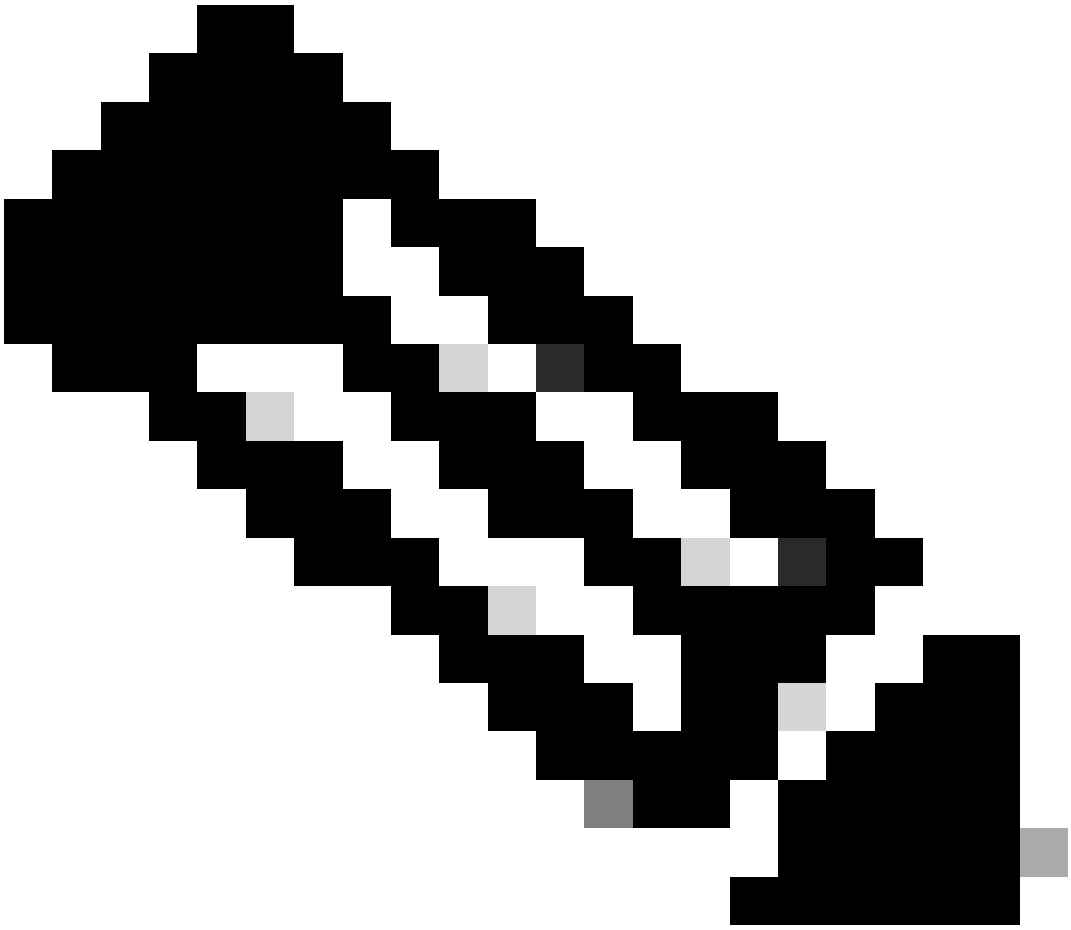
排除防火墙上的介质问题

从FW的角度来看，排除单向音频、双向音频问题或无音频故障时，必须分析4个流：

1. 从主叫方到被叫方的RTP流（入口接口）。
2. 从主叫方到被叫方的RTP流（出口接口）。
3. 从被叫方到主叫方的RTP流（出口接口）。

4. 从被叫方到主叫方（入口接口）的RTP流。



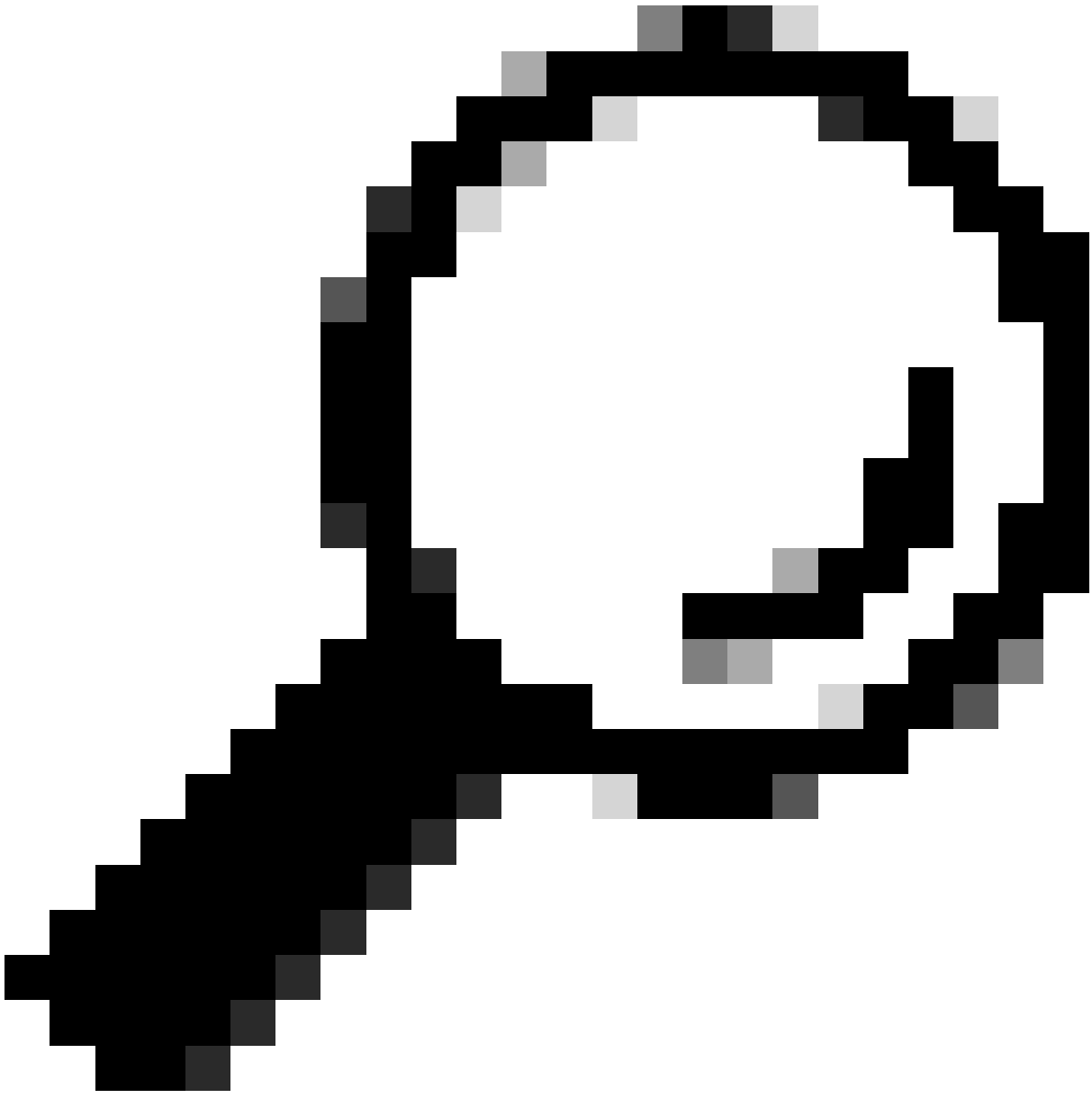


注意：确保在ASA或FTD的LINA模式下使用CLI数据包捕获执行故障排除，因为这样可以在单个数据包捕获内更灵活地应用多个匹配。

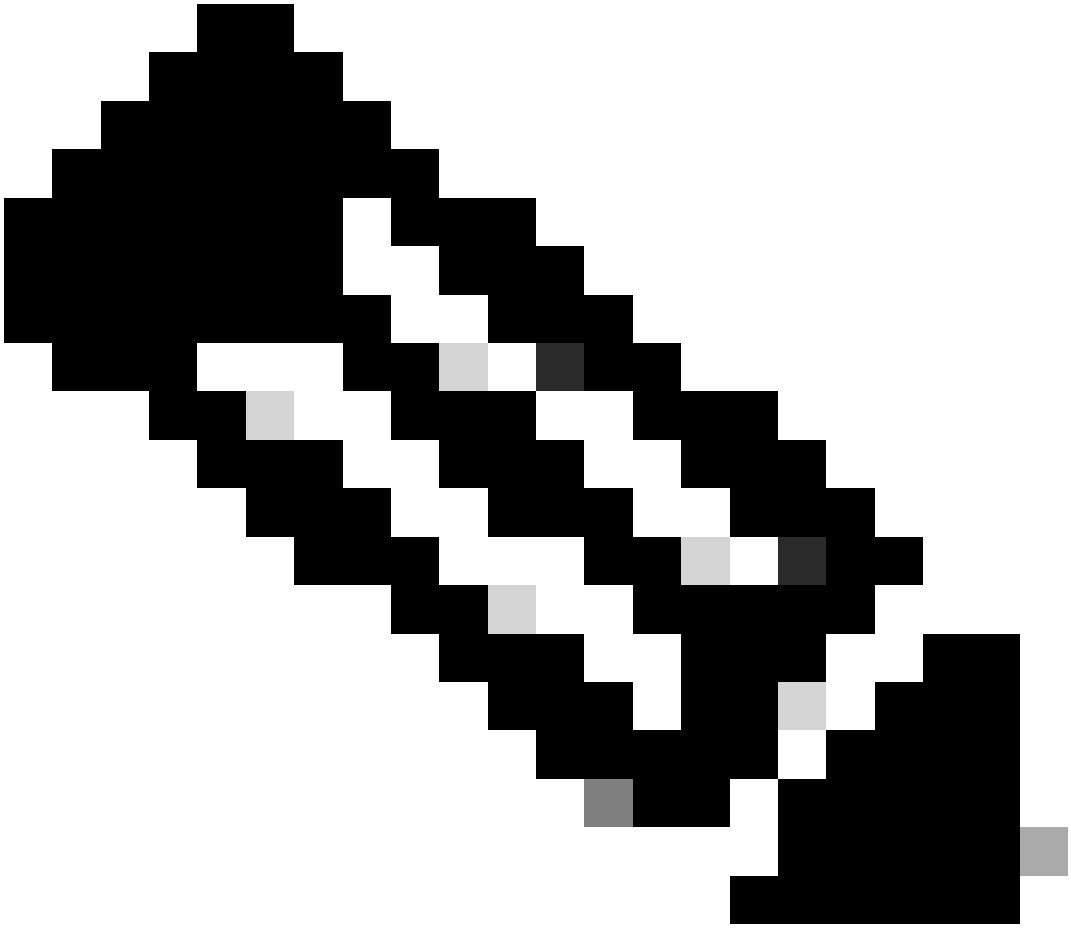
排除SIP呼叫故障

在排除安全防火墙（ASA或FTD）上的语音故障时，您需要执行以下步骤：

1. 确保您有呼叫流程和拓扑图。
2. 确保您从用户的角度理解问题。
3. 了解信令协议的路径。
4. 了解媒体RTP协议的路径。
5. 在入口和出口接口上捕获数据包。
6. 检查配置ACL规则和NAT规则。
7. 验证SIP信令流量未被防火墙阻止。此外，比较入口和出口接口以分析语音流量。
8. 通过比较入口和出口接口上的流量流，验证防火墙未阻止RTP媒体流量。
9. 确保信令设备支持检测，如果不禁用该检测。



提示：进入防火墙的SIP信令消息也必须与离开防火墙相同。



注意：SIP的故障排除提示也可以应用于H.323、MGCP和SCCP协议。

相关信息

- 使用CLI配置ASA数据包捕获
- 使用Firepower威胁防御捕获

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。