Conozca los aspectos básicos de los protocolos de voz sobre IP para un firewall seguro

Contenido

Introducción

Este documento describe los fundamentos de varios protocolos VoIP para ayudar a los ingenieros en la resolución de problemas de manera eficaz en firewalls seguros.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento está pensado para su uso en situaciones de solución de problemas con estos dispositivos:

- Protección frente a amenazas de firewall (FTD)
- Dispositivo de seguridad adaptable (ASA) de firewall seguro

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

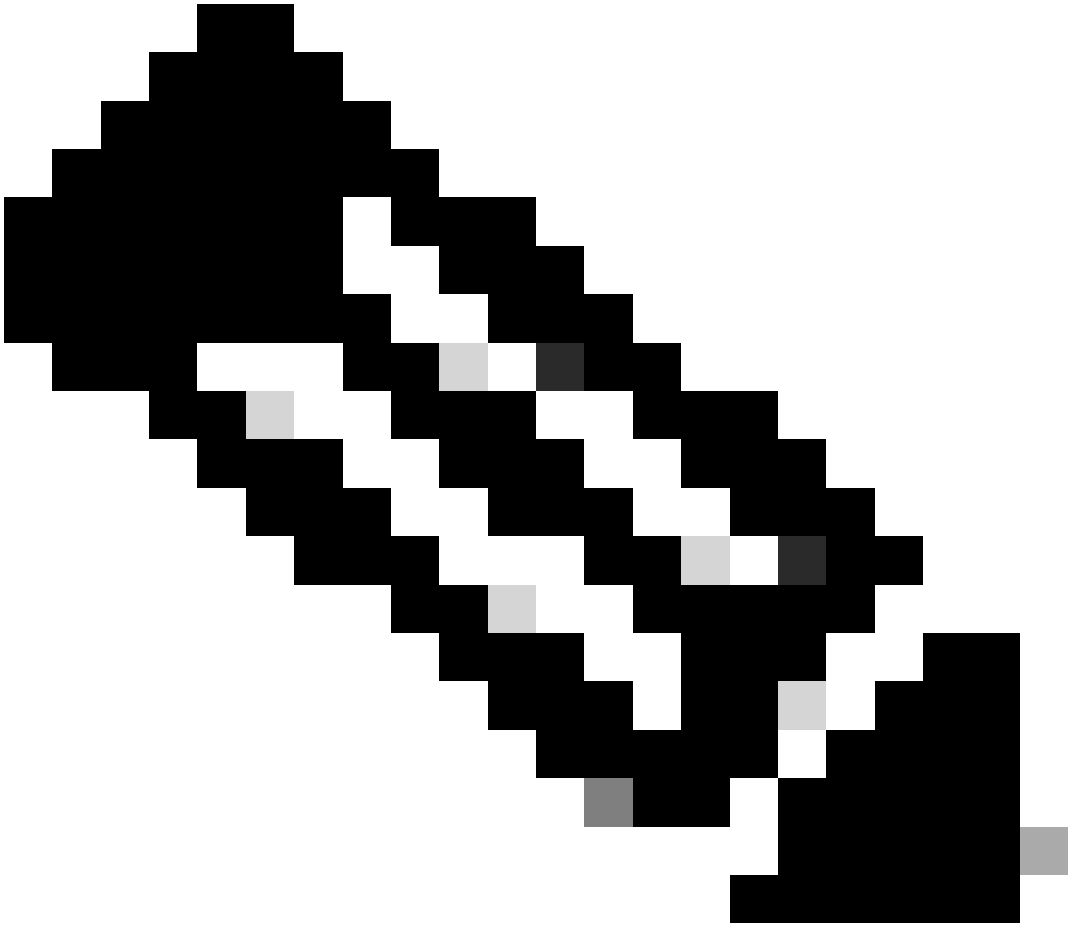
Conceptos básicos de VoIP

La comunicación es fundamental para las interacciones humanas. Los protocolos de voz sobre IP (VoIP) se han vuelto indispensables para la comunicación humana. Por ello, es importante conocer sus partes a la hora de solucionar problemas en un escenario que incluya un firewall (FW).

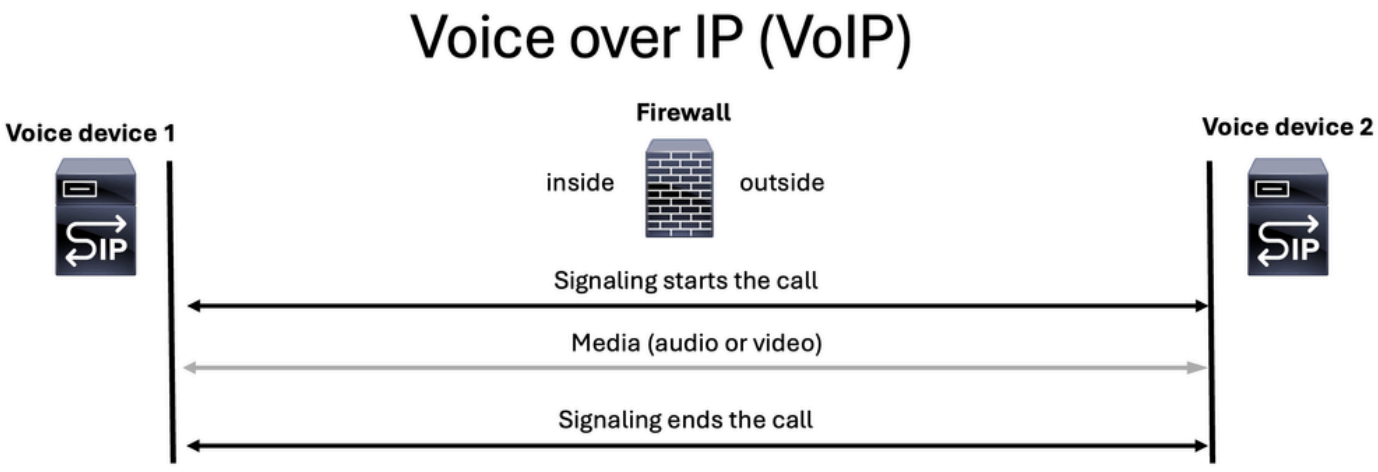
El VoIP se compone de dos partes:

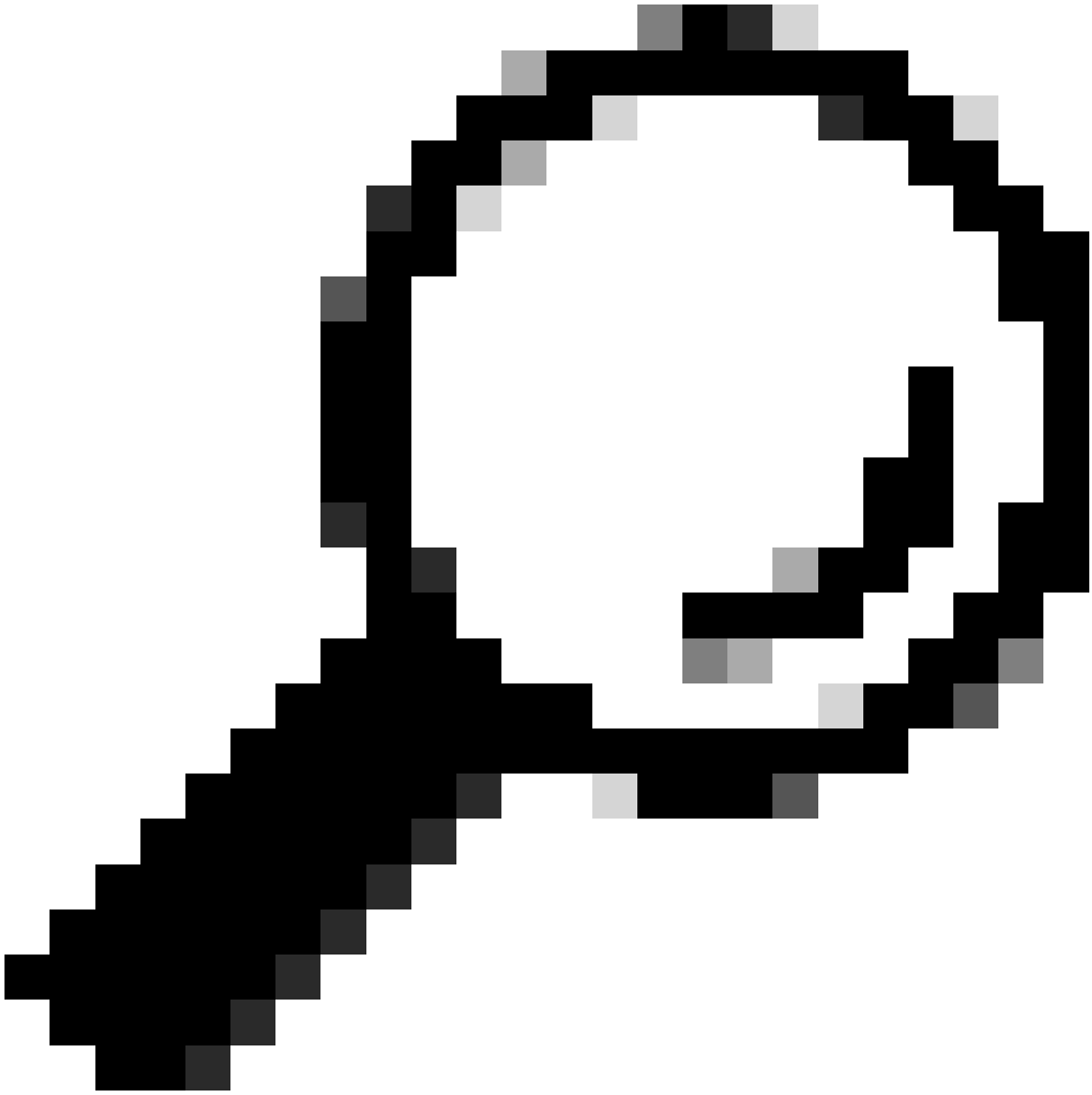
- Señalización
- Medios (voz o vídeo)

Las comunicaciones VoIP siempre comienzan con una parte de señalización para iniciar una llamada, a continuación, se transmiten los medios (voz o vídeo) y, finalmente, la señalización finaliza la llamada.

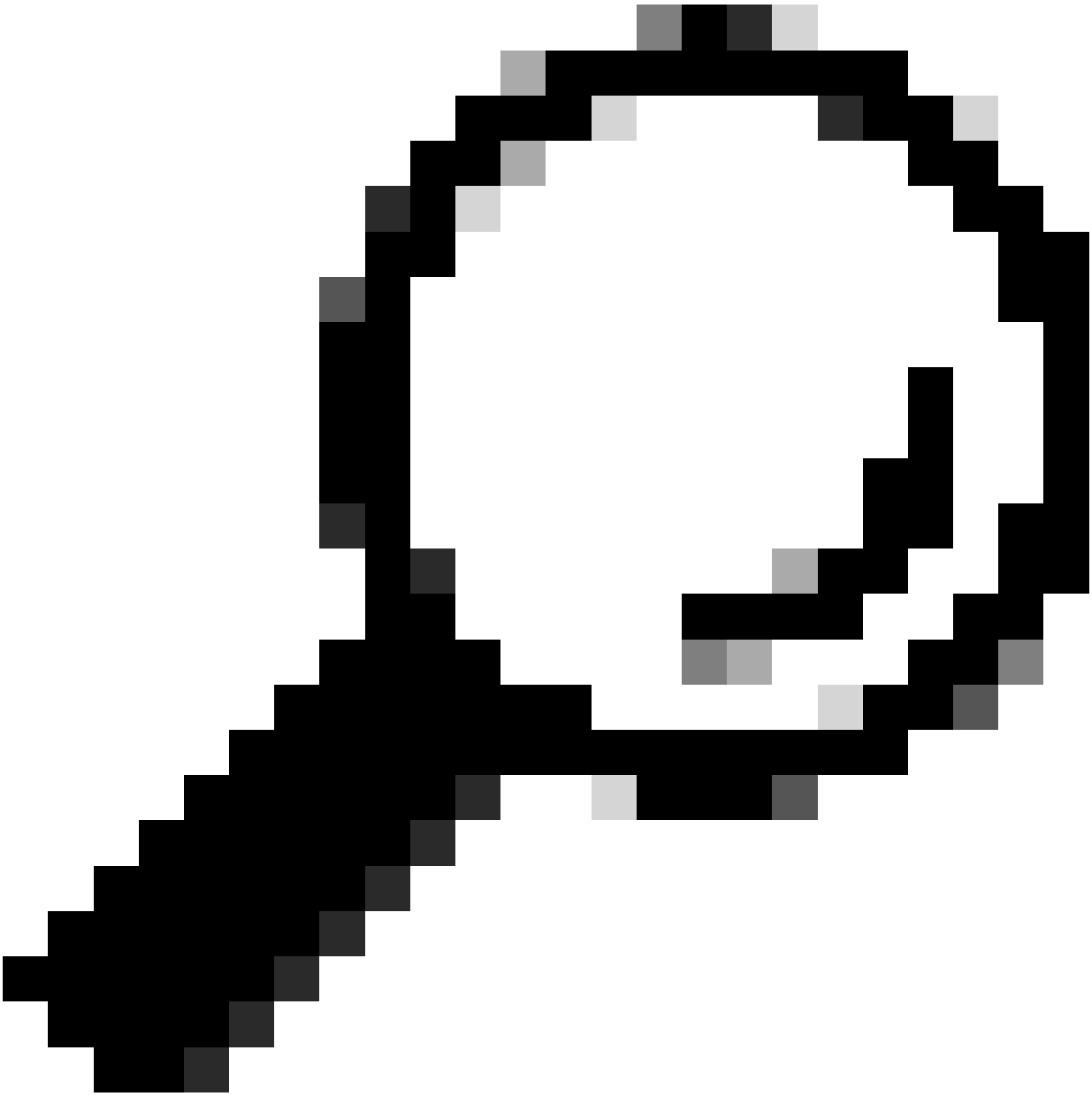


Nota: SIP es el protocolo más utilizado, por lo que se representa de forma coherente como el icono del servidor de voz SIP en muchos de los diagramas.





Consejo: Al solucionar un problema de voz para ASA o FTD, es crucial considerar el escenario desde la perspectiva del usuario. Debe determinar si la llamada se ha establecido o si no hay audio o audio unidireccional. Esta información proporciona pistas valiosas sobre si el problema reside en el protocolo de señalización o en el protocolo de medios (voz o vídeo).



Consejo: Un dispositivo de voz puede gestionar el tráfico del protocolo de transporte en tiempo real (RTP) de voz, el tráfico de señalización o ambos simultáneamente. Al solucionar problemas de voz, es esencial recordar estos conceptos principales:

++Servidores de señalización: Estos servidores son responsables de manejar solamente el tráfico de señalización.

++Servidores de medios: Estos servidores manejan tráfico RTP de voz exclusivamente.

++Algunos dispositivos pueden encargarse de ambas tareas.

Señalización

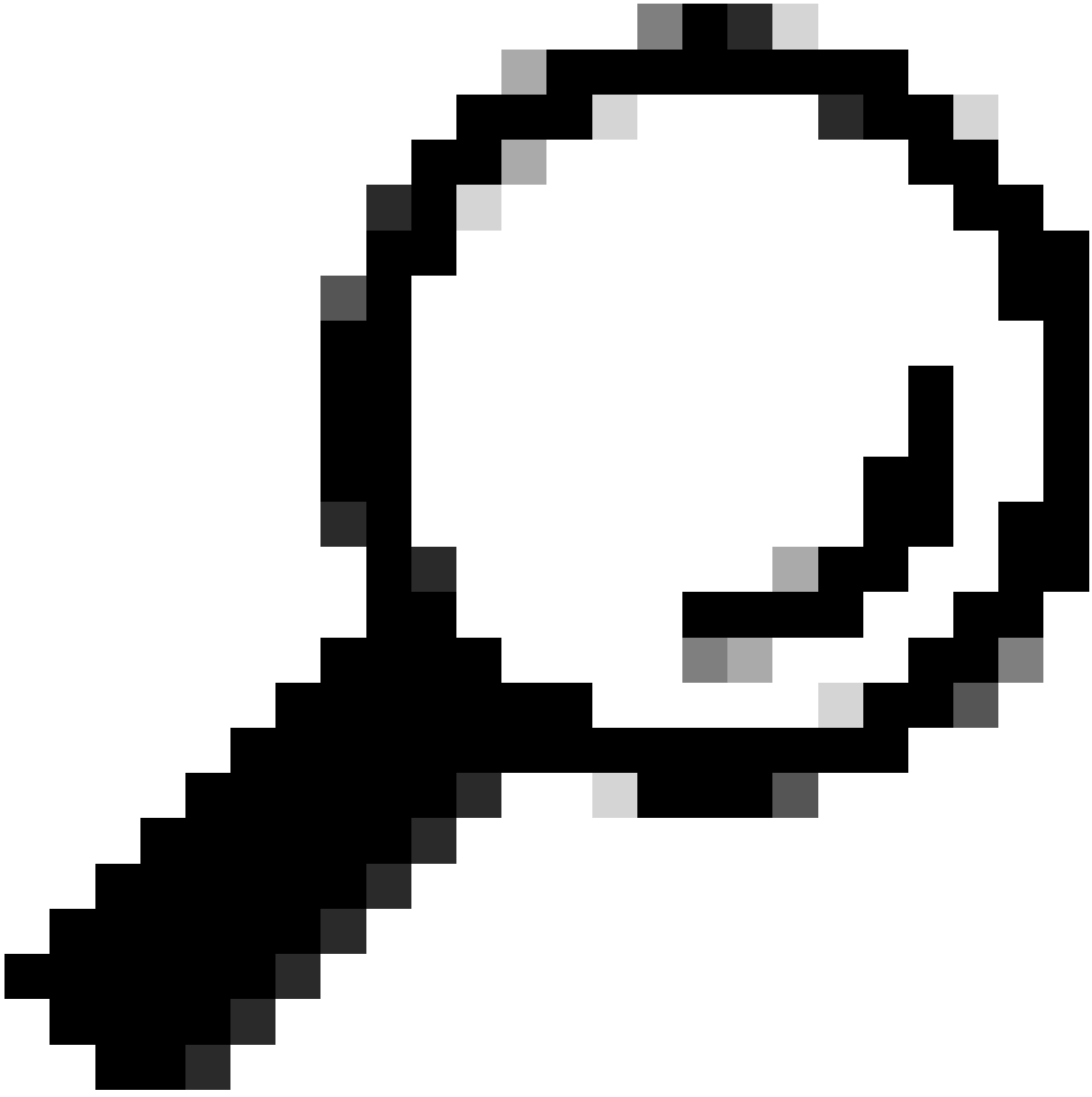
El protocolo de señalización es la parte de una llamada que inicia la comunicación de voz, pero

no solo eso, sino que también realiza estas funciones:

- Mantiene la comunicación.
- Modifica la comunicación.
- Finaliza la comunicación.

Los diferentes tipos de protocolos de señalización ayudan a establecer una llamada, y los más comunes incluyen:

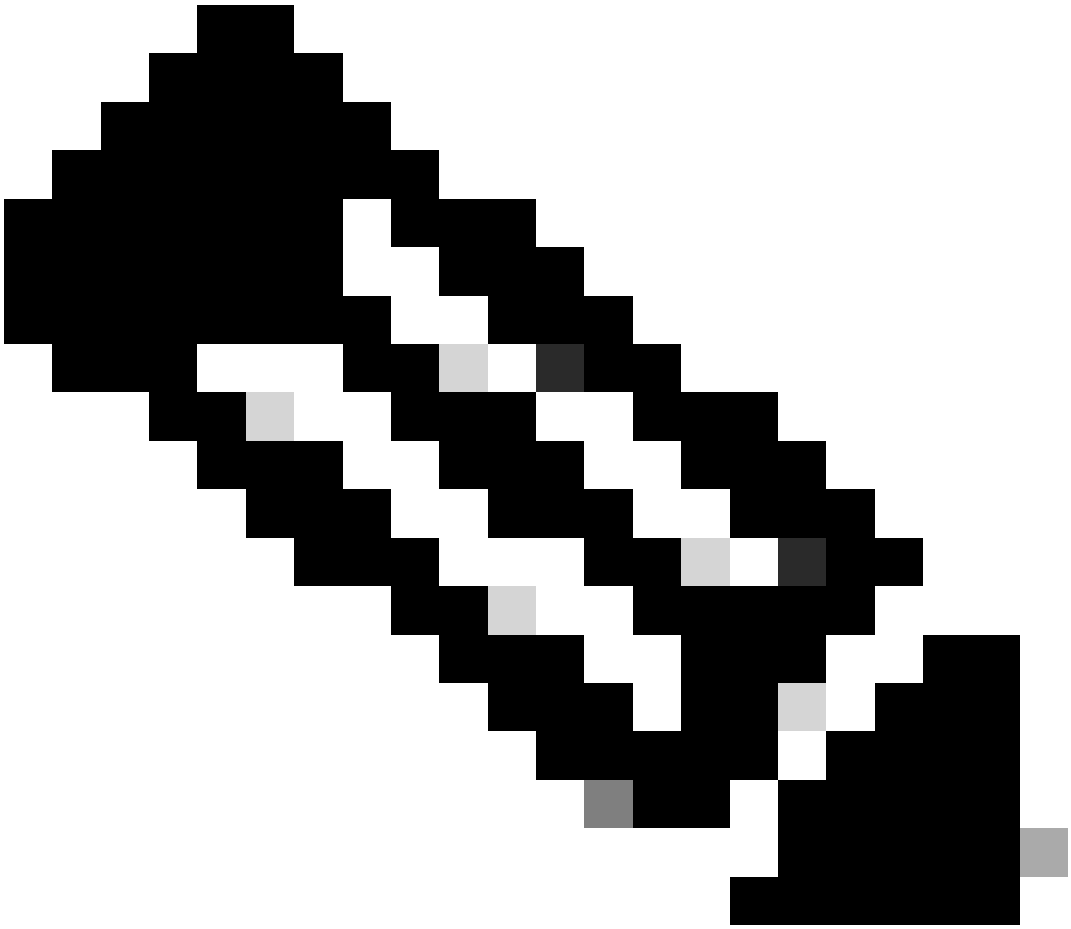
- Protocolo de inicio de sesión (SIP)
- H.323
- Protocolo de Control de Gateway de Medios (MGCP)
- Protocolo ligero de control de llamadas (SCCP)



Consejo: Es esencial identificar el protocolo de señalización en uso para determinar los

---

puertos apropiados para la captura de paquetes en ASA o FTD. Además, tener una topología de red y un flujo de llamadas es beneficioso para comprender la ruta de señalización.



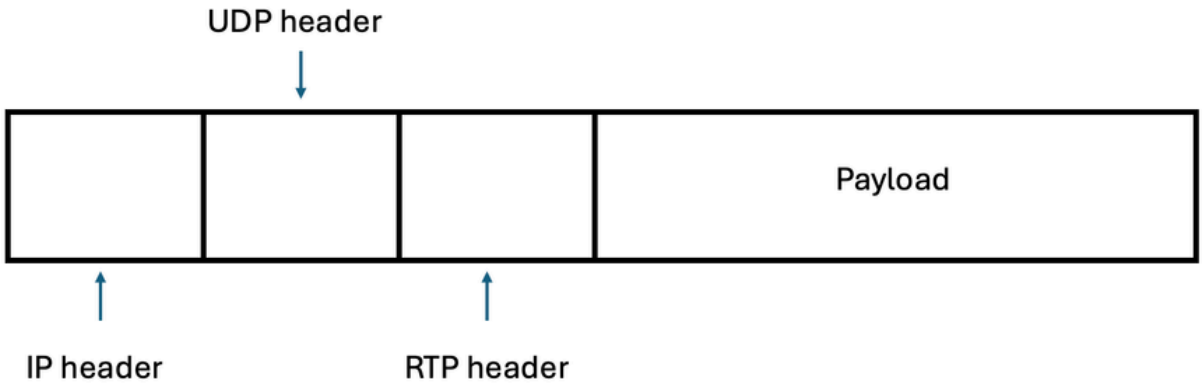
Nota: Los paquetes de señalización incluyen direcciones IP de origen y destino, que ayudan en la identificación de las partes involucradas en el envío y la recepción del flujo de medios RTP.

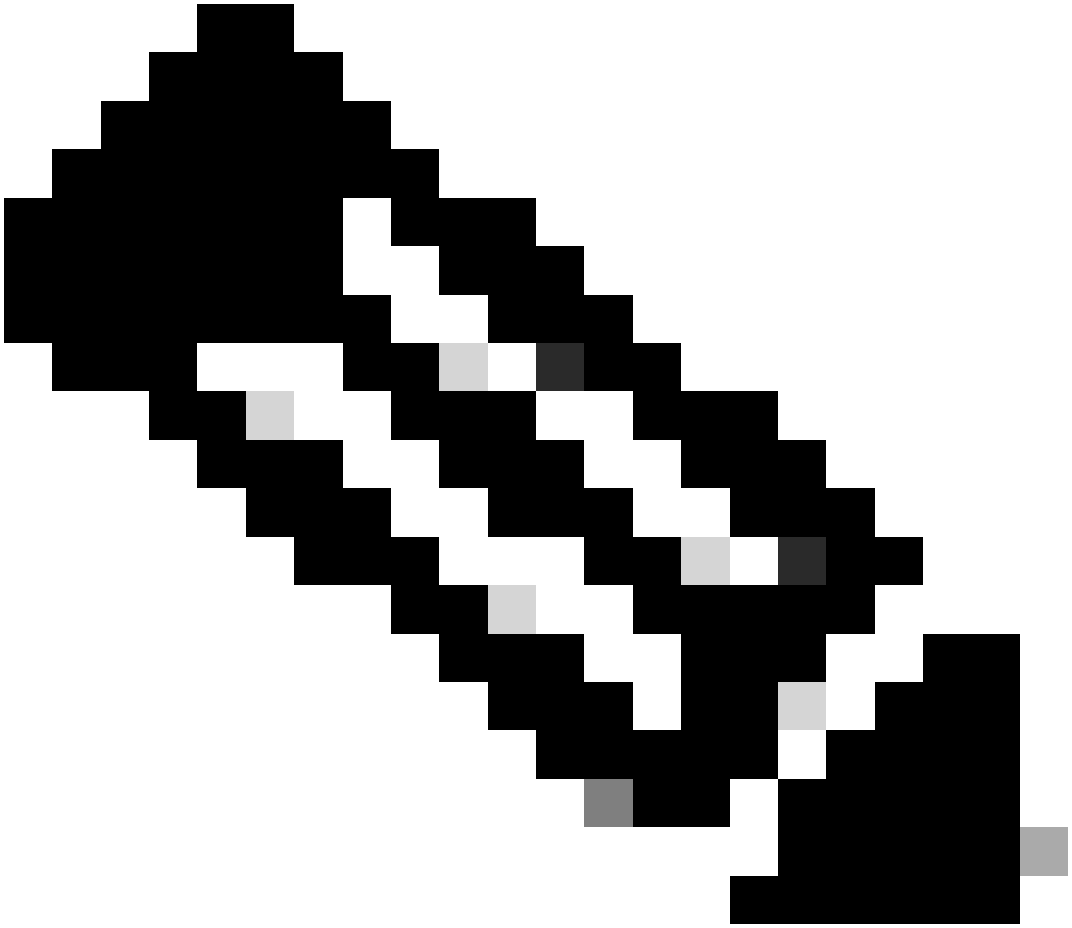
Medios

Una vez que se ha completado la señalización y los componentes de señalización (dispositivos o servidores) coinciden en el tipo de medio, entra en juego el protocolo en tiempo real (RTP) para comenzar a enviar medios (audio o vídeo) a todas las partes involucradas.

RTP es un protocolo de Internet que se utiliza para la transmisión multimedia que se envía solo después de establecer la llamada y que se ejecuta a través del protocolo de datagramas de

usuario (UDP).

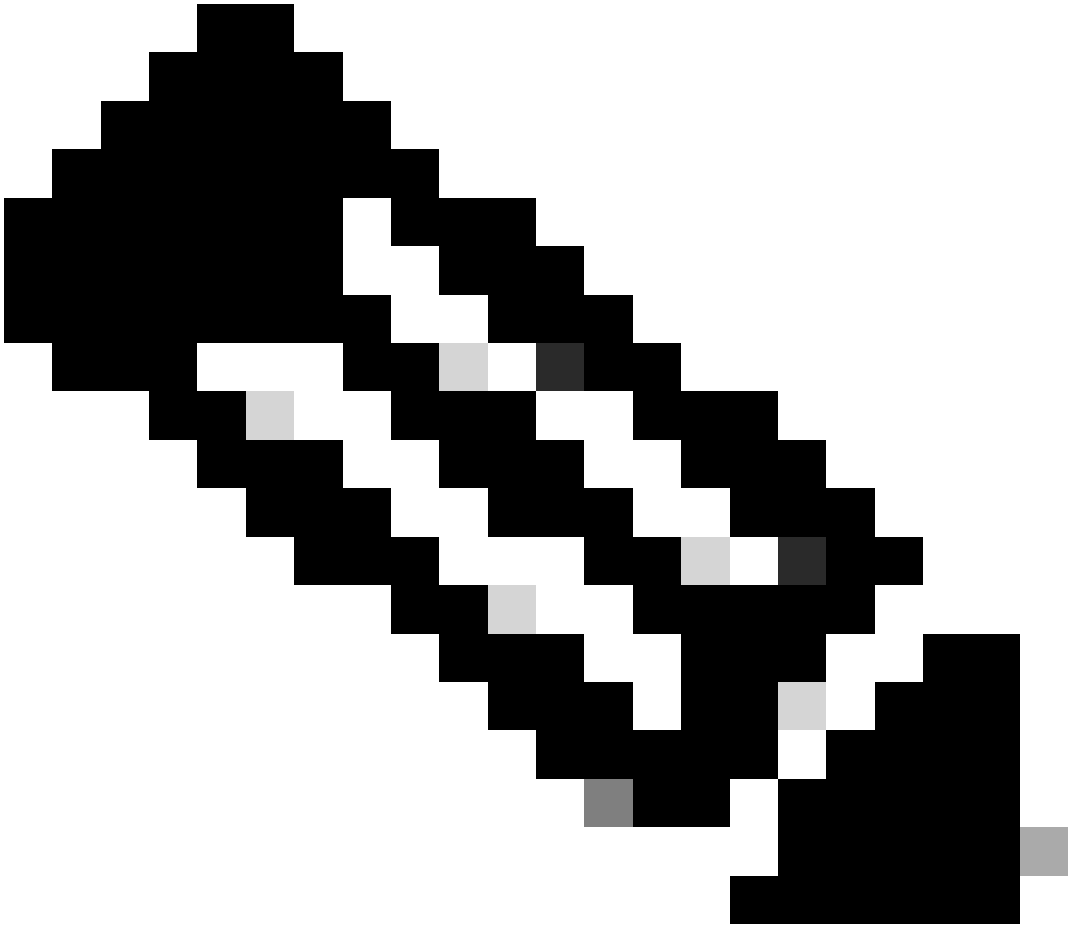




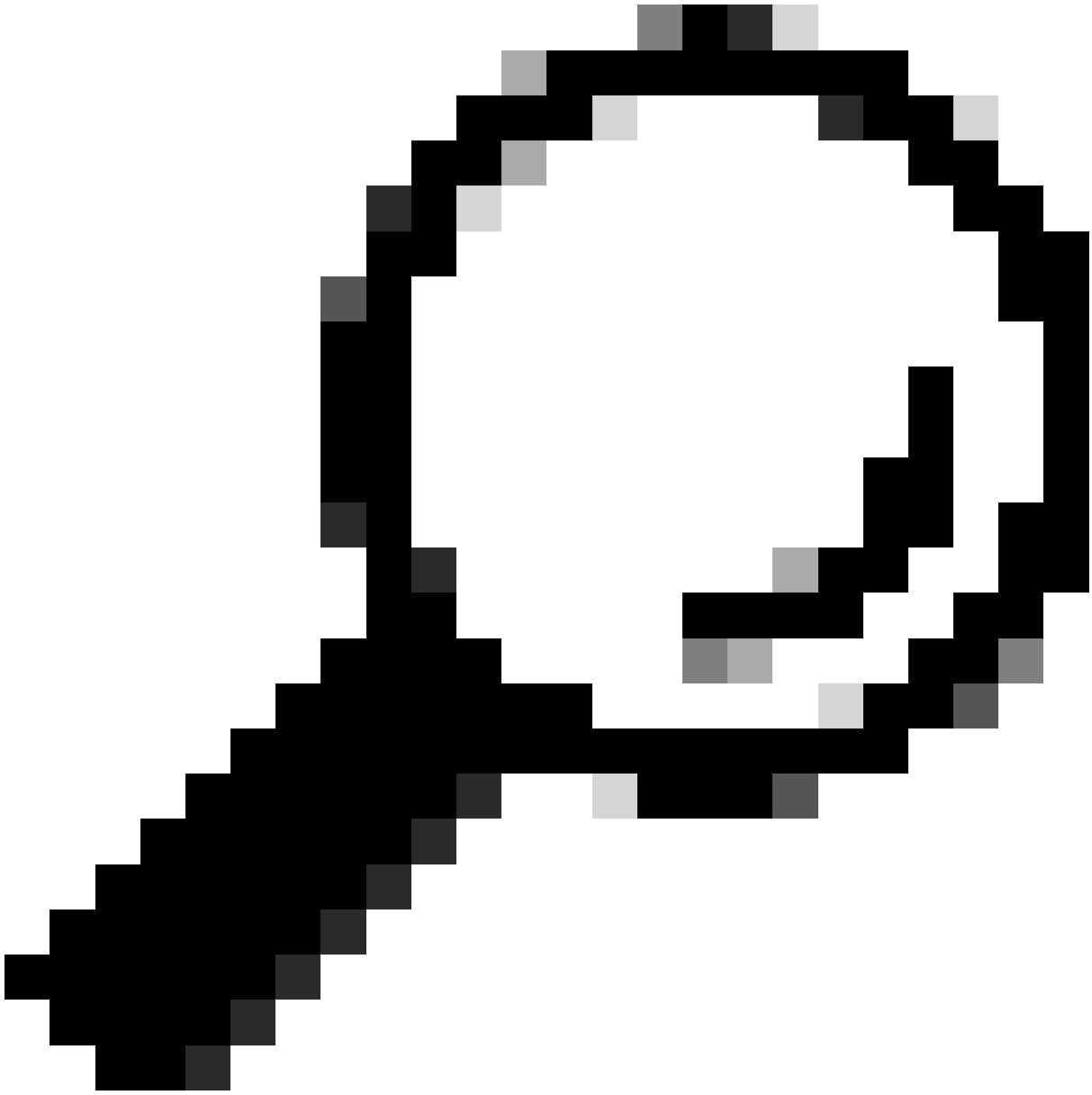
Nota: Los medios pueden ser voz y/o video y viajan en paquetes RTP.

Los componentes de señalización (dispositivos o servidores) determinan qué puertos se utilizan para enviar o recibir medios (audio o vídeo). El intervalo de puertos más común para RTP suele

estar entre 16384 y 32767 para la mayoría de los dispositivos.



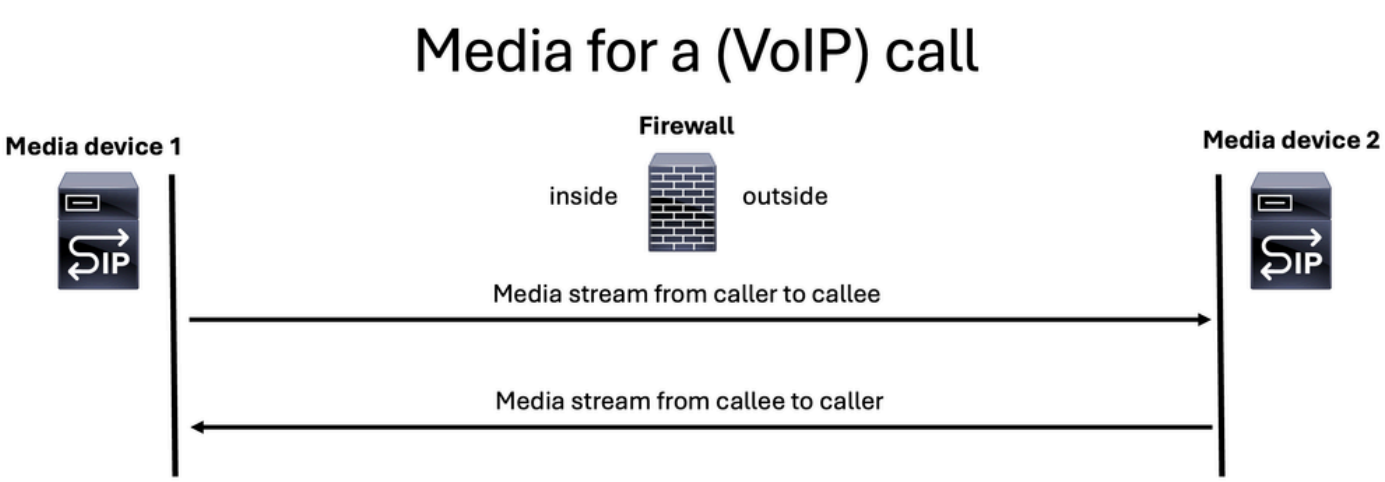
Nota: Ciertos dispositivos de Cisco, como las plataformas ASR e ISR G3, como la plataforma ISR4K, utilizan un intervalo de puertos RTP estandarizado de 8000 a 48200. Es fundamental verificar el intervalo de puertos RTP específico configurado en sus dispositivos, ya que puede diferir de estos valores estandarizados y puede variar entre dispositivos de terceros.

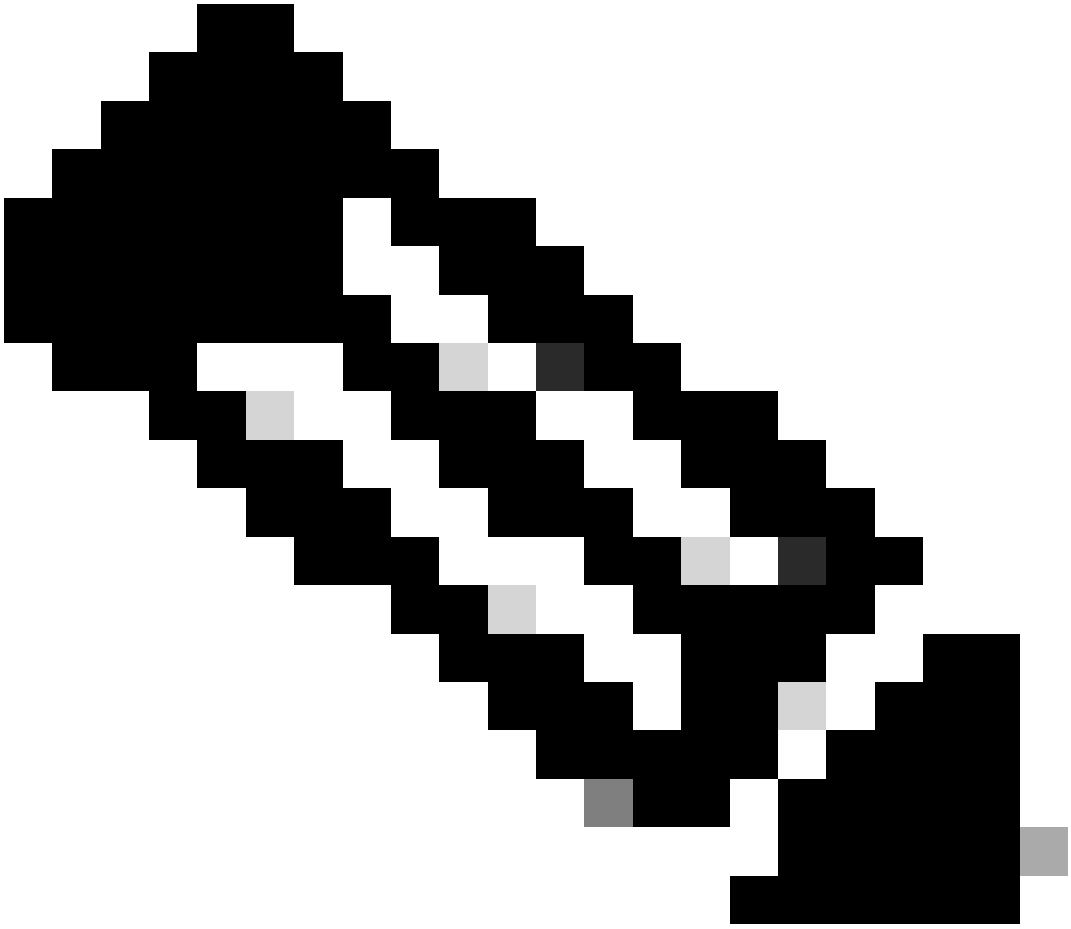


Consejo: A veces, la trayectoria RTP difiere de la trayectoria de señalización, por lo que es crucial identificar los dispositivos responsables del envío y la recepción de paquetes RTP de voz. Esto garantiza que se capture el tráfico UDP entre los dispositivos que atraviesan el ASA o FTD.

Hay dos flujos de medios o flujos RTP que se generan en una llamada de voz normal:

1. un flujo de medios de la persona que llama al destinatario
2. un flujo de medios del destinatario de la llamada al llamador





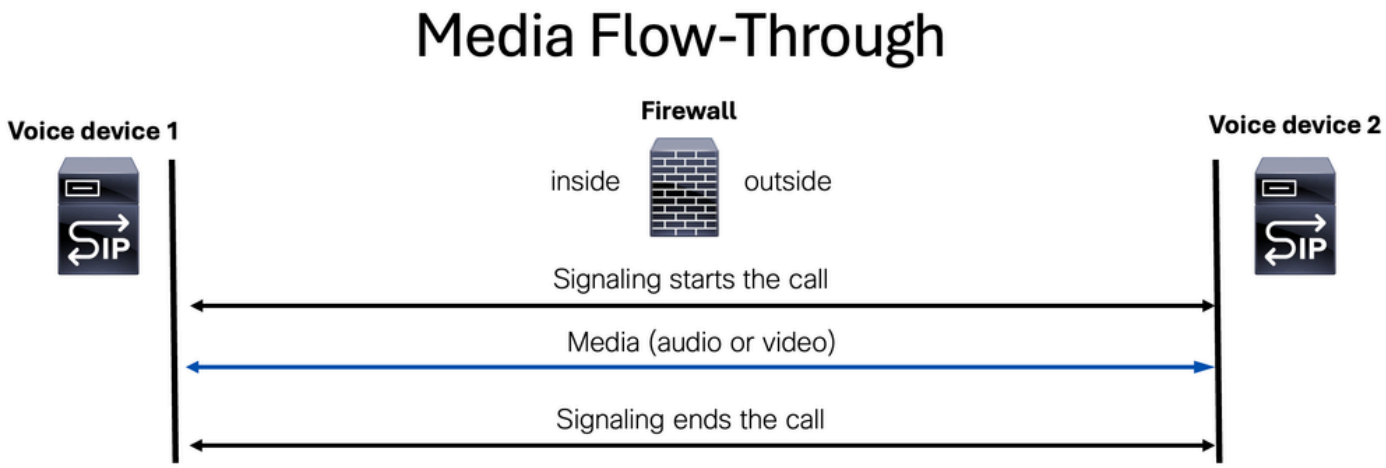
> Nota: A modo de ejemplo, el icono del servidor SIP se utiliza para representar un servidor de señalización o un servidor de medios en todas las imágenes.

Al hablar de la transmisión de medios en una llamada de voz, es importante destacar dos situaciones clave:

1. Flujo de medios
2. Flujo de medios

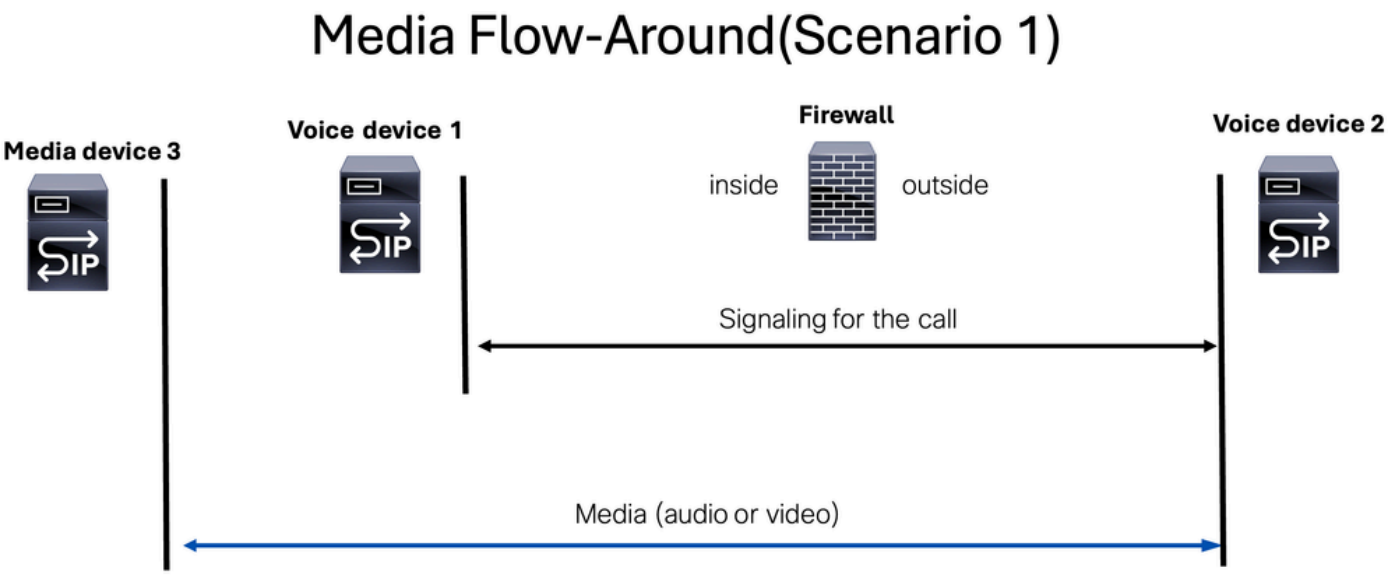
Flujo de medios

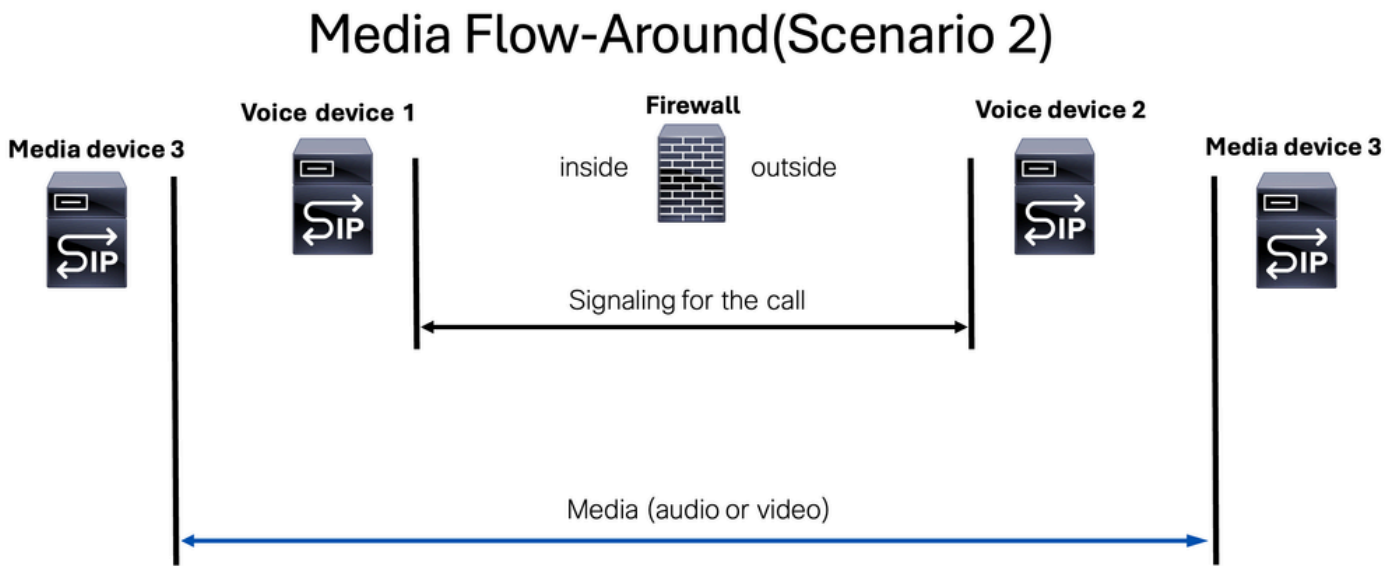
El flujo de medios es un modo en el que el mismo dispositivo procesa los paquetes de medios (voz y/o vídeo) y de señalización.



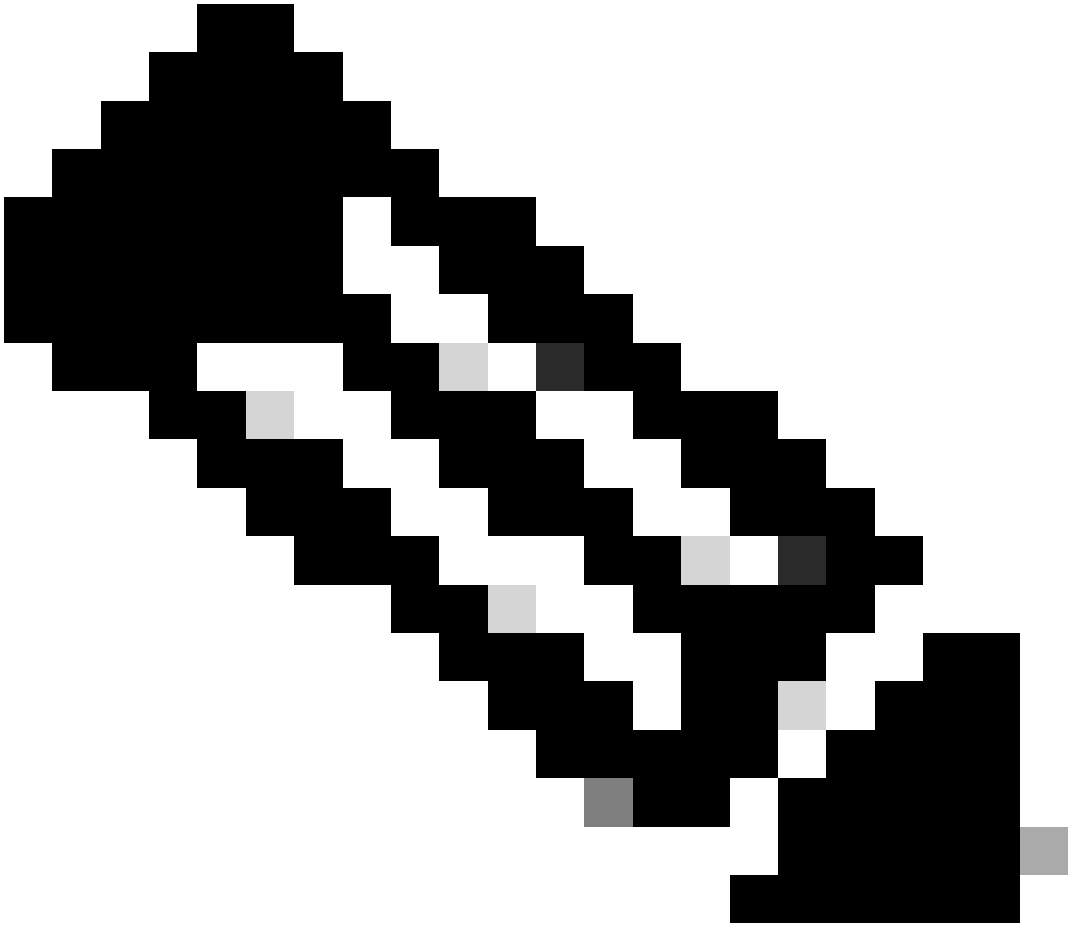
Flujo de medios

El flujo de flujo de medios es un modo en el que los paquetes de señalización se gestionan mediante dos componentes de señalización independientes (dispositivos o servidores), mientras que el flujo de medios (voz o vídeo) se gestiona mediante un tercer dispositivo conocido como dispositivo de medios.





Este modo aclara las funciones de los dispositivos implicados y la distinción entre la señalización y las transmisiones de medios o dispositivos.



Nota: Esto es especialmente importante mencionar cuando la resolución de problemas de la lista de acceso creada podría permitir los componentes de señalización (dispositivos o servidores), pero si el flujo de medios está utilizando otro dispositivo de medios, tenemos que permitirlo también en la lista de acceso de nuestro dispositivo FW.

Protocolo de inicio de sesión (SIP)

SIP es un protocolo de control de la capa de aplicación definido por el Grupo de trabajo de ingeniería de Internet (IETF) en RFC 3261.

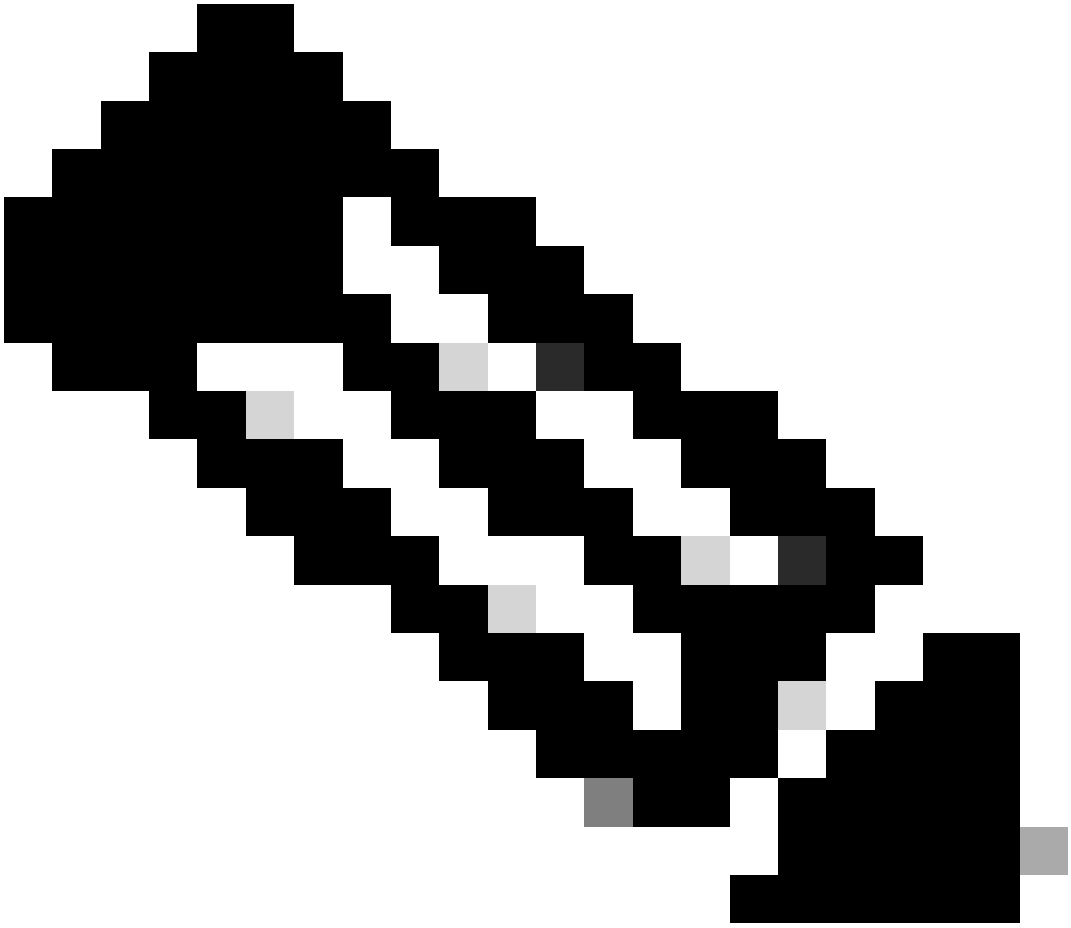
SIP es un protocolo basado en texto. Esto significa que los mensajes SIP están compuestos de texto legible por personas, de manera similar a como funciona HTTP.

SIP está diseñado para abordar las funciones de señalización y administración de sesiones dentro de una red de telefonía por paquetes.

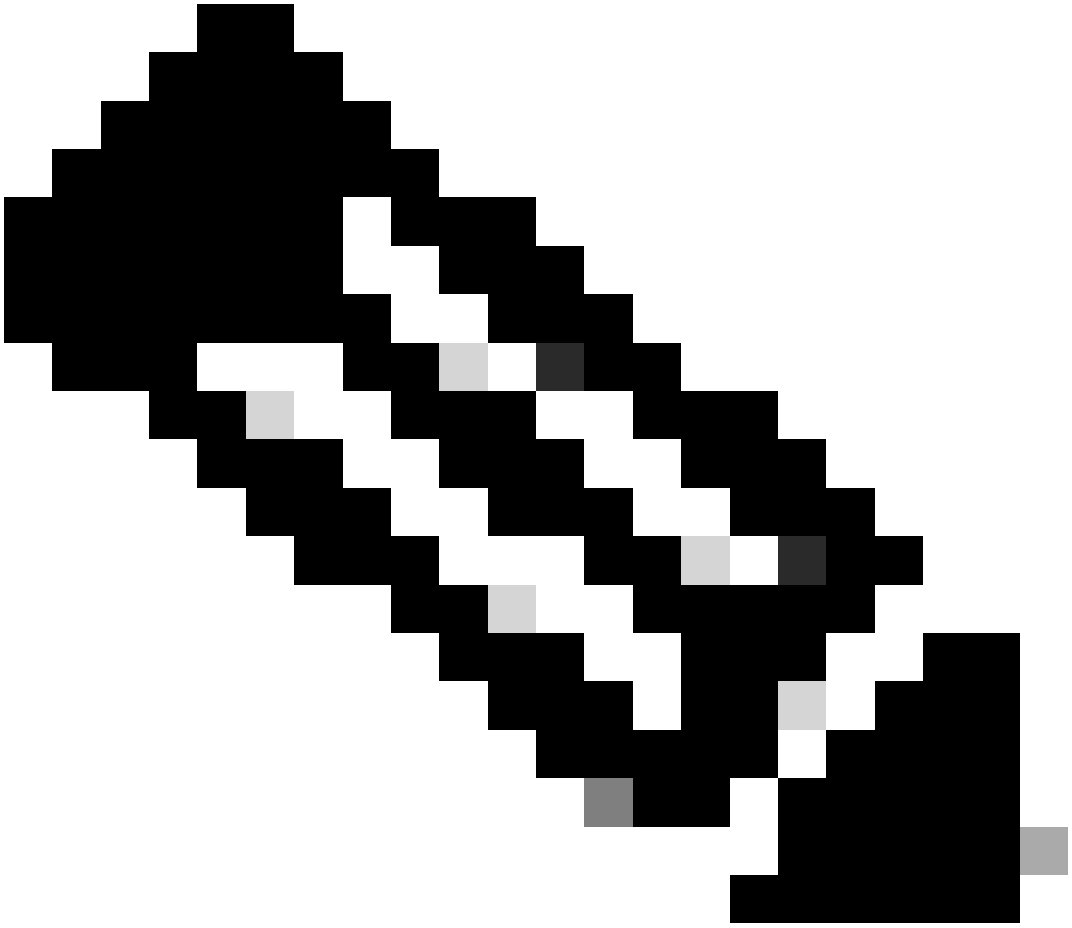
SIP puede:

- crear una llamada
- modificar una llamada
- terminar una llamada

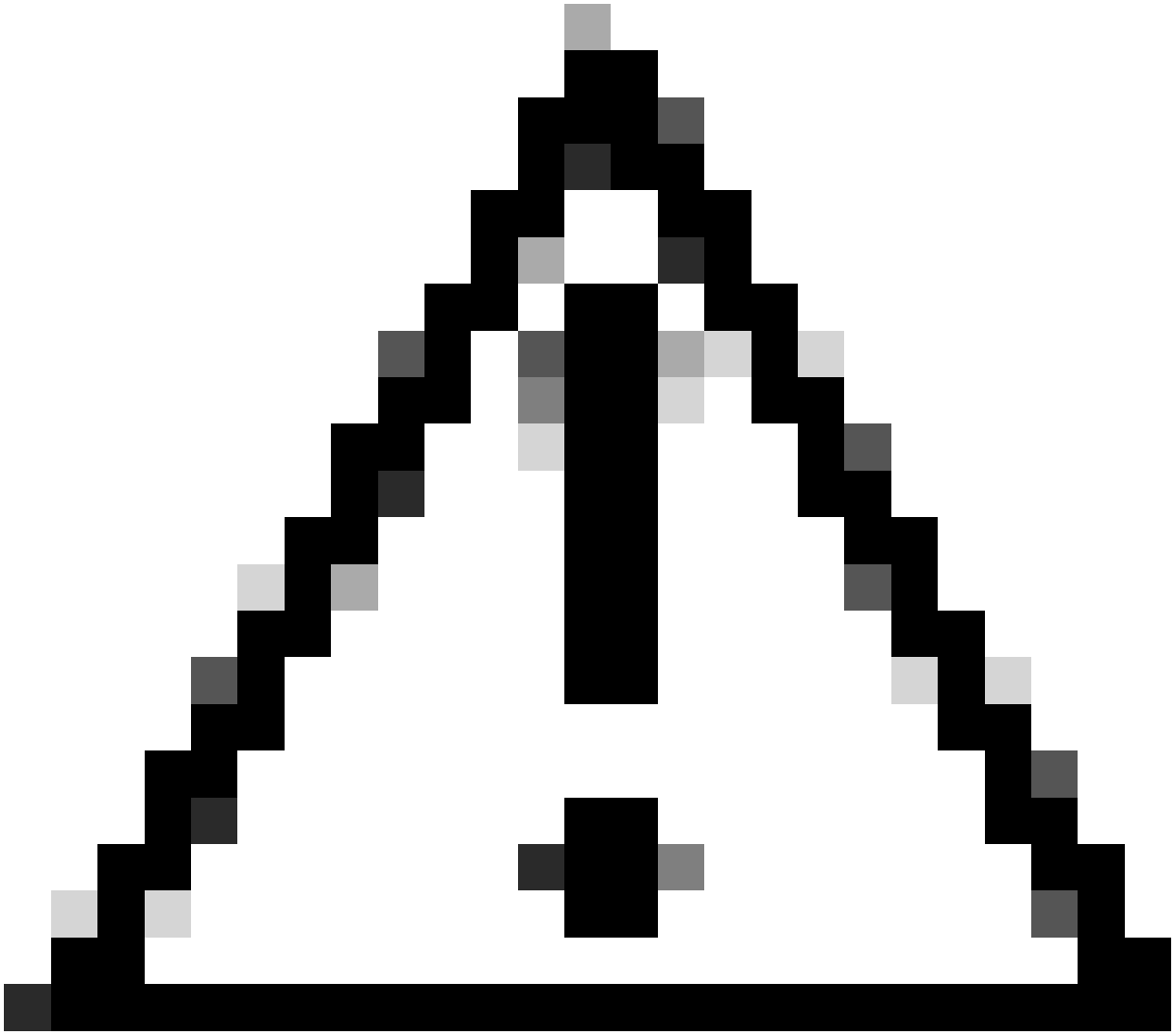
SIP se puede utilizar UDP o TCP en el puerto estandarizado 5060. Además, si el SIP se cifra mediante la seguridad de la capa de transporte (TLS), puede utilizar el puerto estandarizado 5061.



Nota: Cuando la señalización SIP está cifrada, los paquetes SIP reales no son visibles en las capturas de paquetes en dispositivos ASA o FTD. Sin embargo, aún puede observar el protocolo de enlace TCP seguido del protocolo de enlace TLS entre los clientes SIP y los dispositivos de servidor SIP.



Nota: La inspección de SIP está activada de forma predeterminada en Cisco Secure Firewall Threat Defense (FTD) y Secure Firewall Adaptive Security Appliance (ASA).



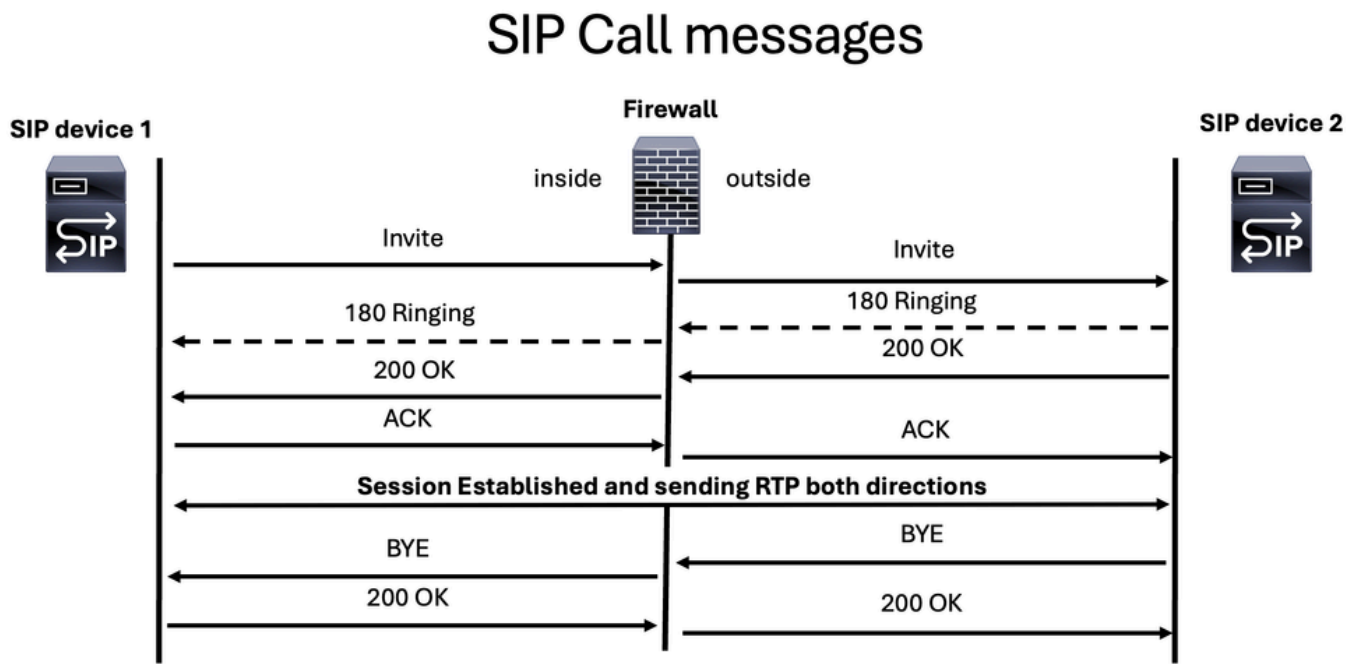
Precaución: Corroborar siempre qué puertos se utilizan para la señalización. Recuerde que el protocolo SIP suele utilizar los puertos 5060 o 5061, pero algunas implementaciones pueden desviarse de estos estándares y utilizar diferentes puertos para el protocolo SIP.

Hay tres situaciones que se pueden encontrar al resolver un problema de señalización SIP:

- Mensajes de señalización de llamadas SIP
- Mensajes SIP OPTION
- Mensajes SIP REGISTER

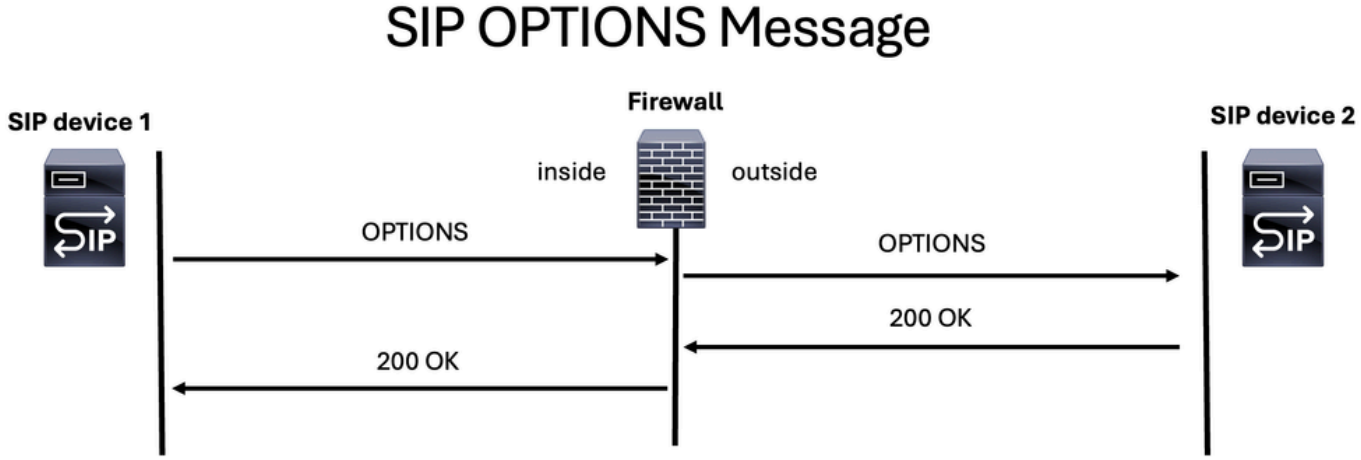
Mensajes de llamada SIP

Los mensajes SIP principales para establecer y finalizar una llamada de voz son los siguientes:



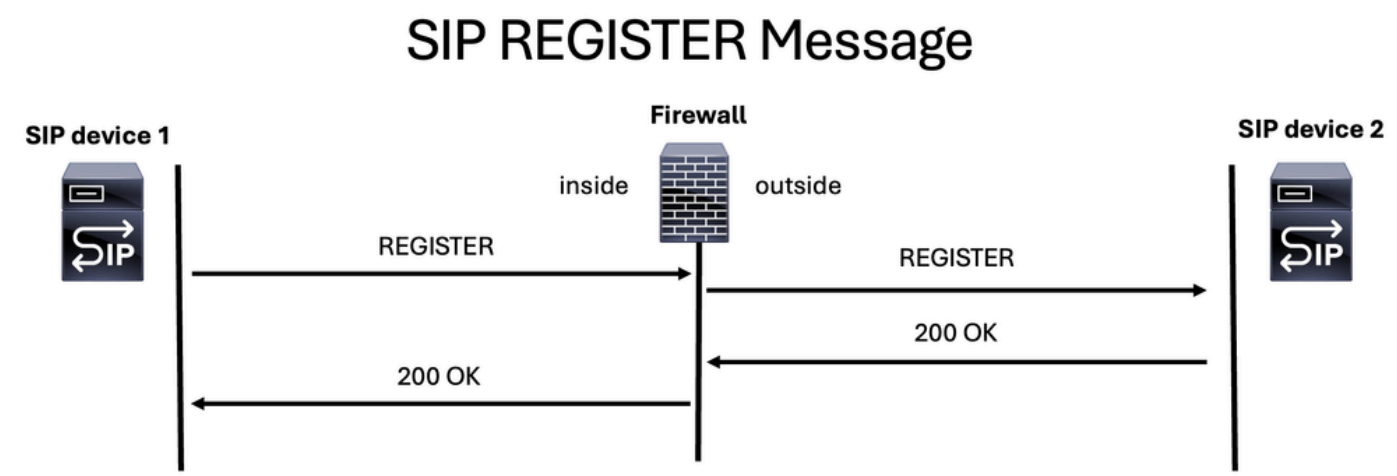
Mensajes de opciones SIP

Los mensajes de OPCIONES SIP son importantes para determinar si un dispositivo SIP está en línea y puede responder. Es como un mensaje de ping ICMP pero en el mundo SIP.

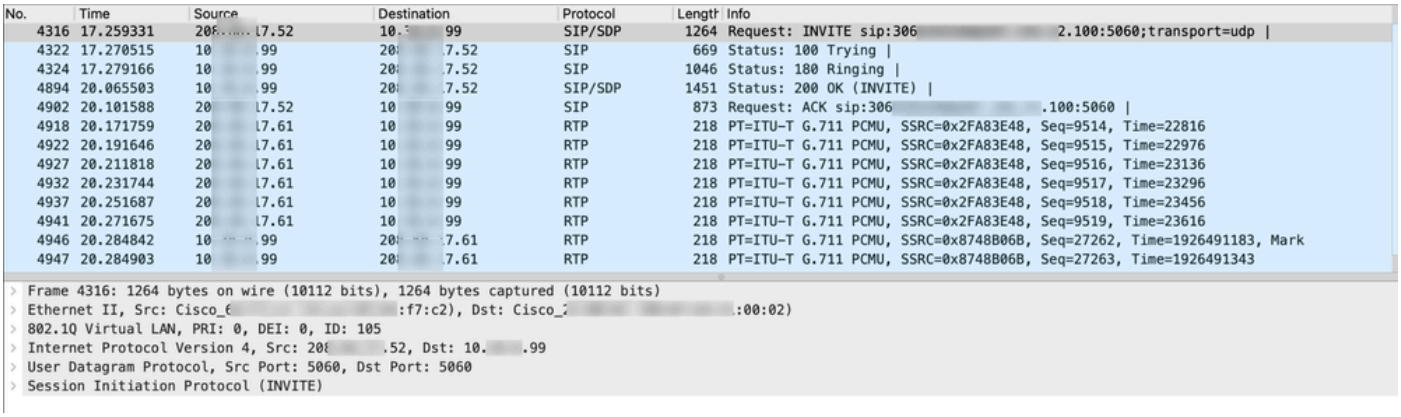


Mensaje SIP REGISTER

Otro mensaje SIP que puede encontrar durante una sesión de solución de problemas del firewall es el mensaje SIP REGISTER, que permite que un dispositivo se registre en un servidor SIP.



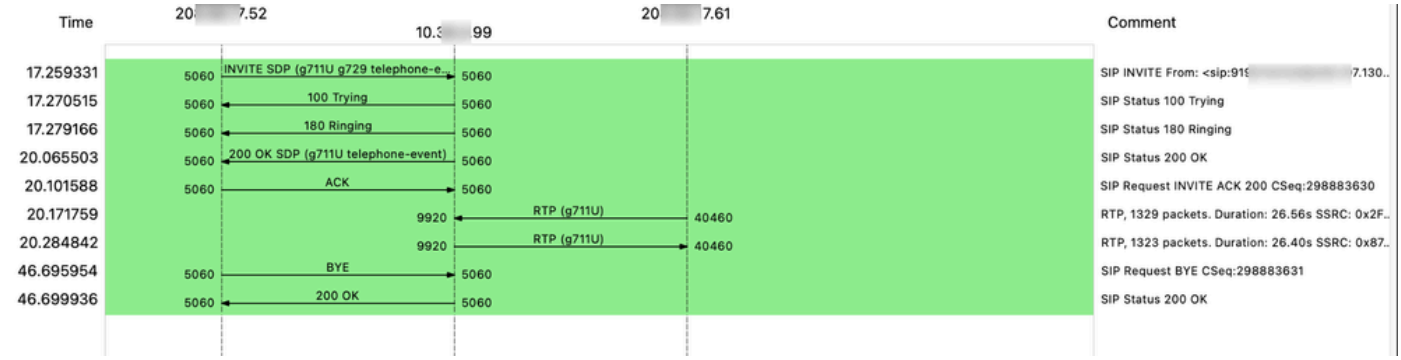
Esta captura de paquetes muestra las solicitudes y respuestas de dos dispositivos SIP y también el tráfico de medios (voz):



No.	Time	Source	Destination	Protocol	Length	Info
4316	17.259331	20[redacted]7.52	10.[redacted]99	SIP/SDP	1264	Request: INVITE sip:306[redacted]2.100:5060;transport=udp |
4322	17.270515	10[redacted].99	20[redacted]7.52	SIP	669	Status: 100 Trying |
4324	17.279166	10[redacted].99	20[redacted]7.52	SIP	1046	Status: 180 Ringing |
4894	20.065503	10[redacted].99	20[redacted]7.52	SIP/SDP	1451	Status: 200 OK (INVITE) |
4902	20.101588	20[redacted]7.52	10[redacted]99	SIP	873	Request: ACK sip:306[redacted].100:5060 |
4918	20.171759	20[redacted]7.61	10[redacted]99	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x2FA83E48, Seq=9514, Time=22816
4922	20.191646	20[redacted]7.61	10[redacted]99	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x2FA83E48, Seq=9515, Time=22976
4927	20.211818	20[redacted]7.61	10[redacted]99	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x2FA83E48, Seq=9516, Time=23136
4932	20.231744	20[redacted]7.61	10[redacted]99	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x2FA83E48, Seq=9517, Time=23296
4937	20.251687	20[redacted]7.61	10[redacted]99	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x2FA83E48, Seq=9518, Time=23456
4941	20.271675	20[redacted]7.61	10[redacted]99	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x2FA83E48, Seq=9519, Time=23616
4946	20.284842	10[redacted].99	20[redacted]7.61	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x8748B06B, Seq=27262, Time=1926491183, Mark
4947	20.284903	10[redacted].99	20[redacted]7.61	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x8748B06B, Seq=27263, Time=1926491343

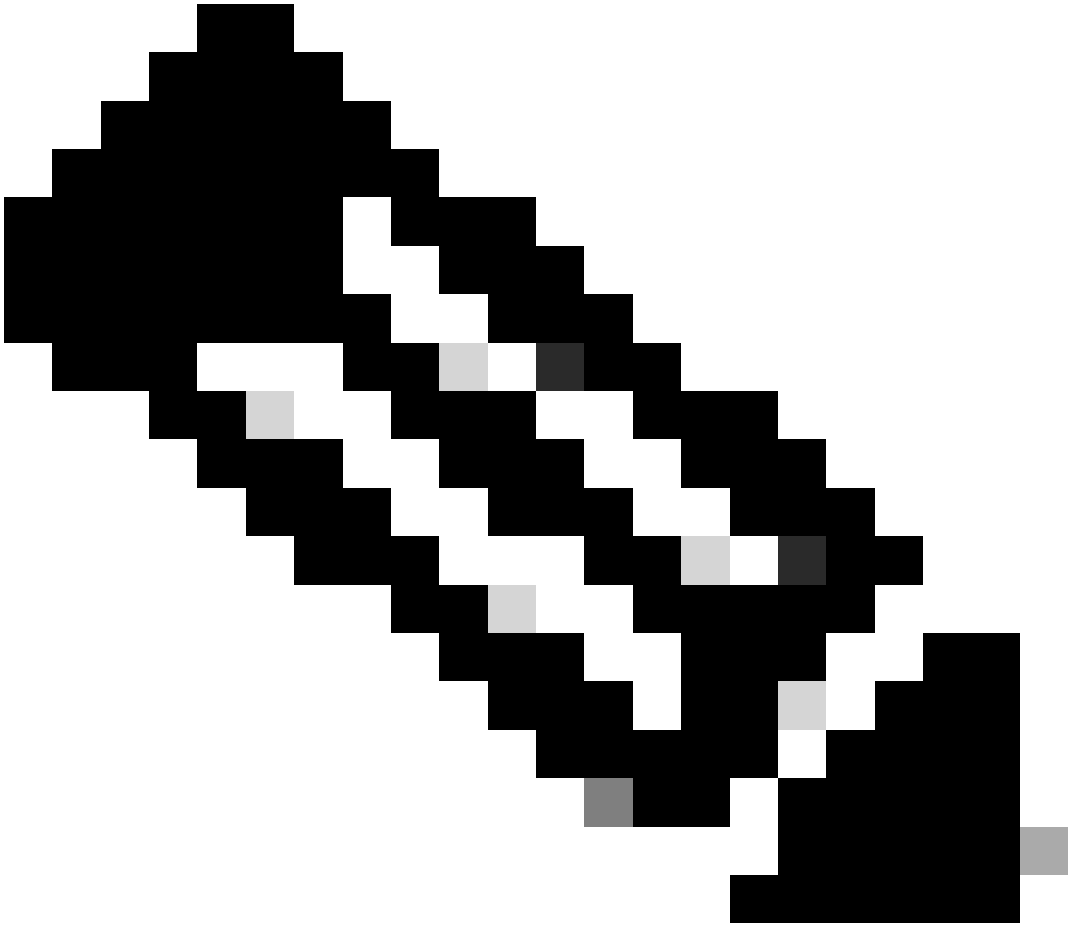
```
> Frame 4316: 1264 bytes on wire (10112 bits), 1264 bytes captured (10112 bits)
> Ethernet II, Src: Cisco_[redacted]:f7:c2), Dst: Cisco_[redacted]:00:02)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 105
> Internet Protocol Version 4, Src: 20[redacted].52, Dst: 10.[redacted].99
> User Datagram Protocol, Src Port: 5060, Dst Port: 5060
> Session Initiation Protocol (INVITE)
```

Este es un ejemplo de un flujo de señalización SIP y medios RTP (voz):



Protocolo de descripción de sesión (SDP)

El protocolo de descripción de sesión (SDP) es una representación estándar que se utiliza para describir transmisiones de medios para sesiones multimedia. No transporta medios en sí, pero se utiliza para negociar el tipo de medios y el formato entre los terminales. SDP se utiliza junto con el protocolo de inicio de sesión (SIP) para administrar y negociar las características multimedia de una sesión.

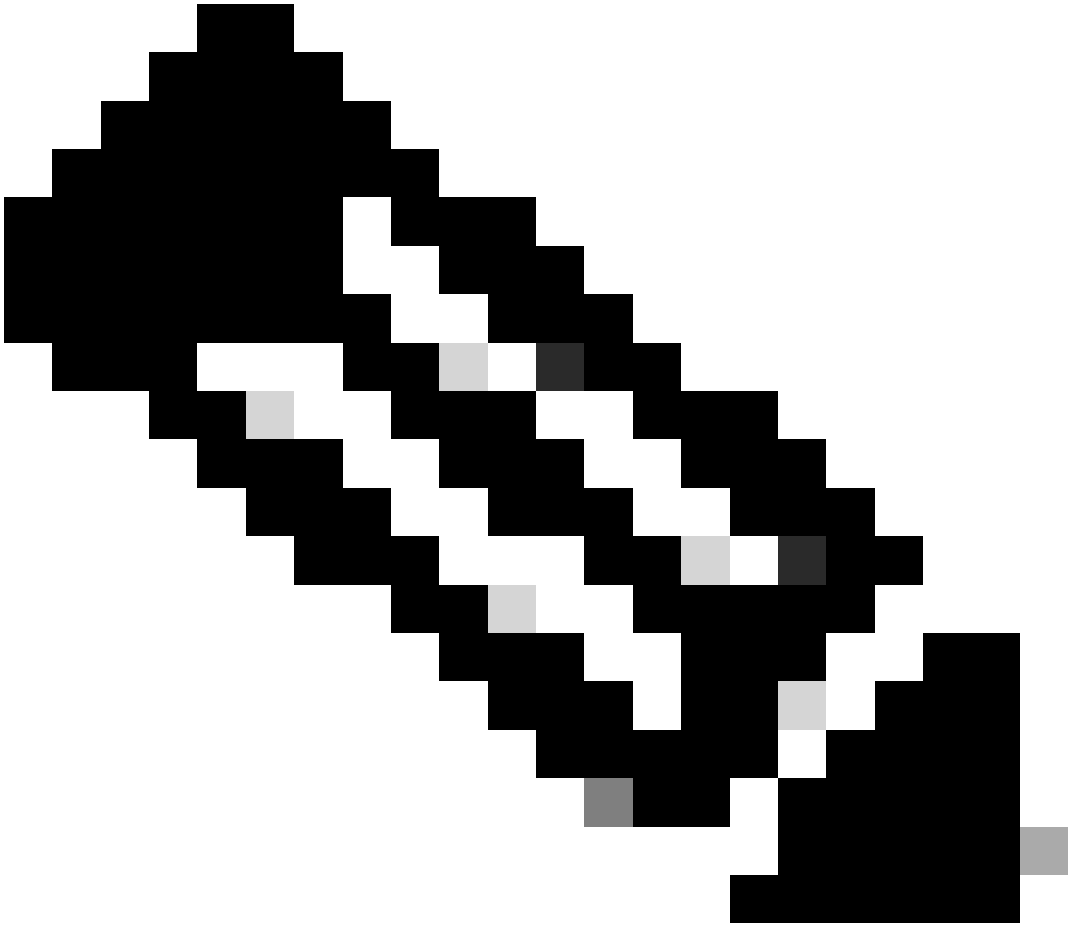


Nota: MGCP incorpora el concepto de SDP, que se utiliza para el mismo propósito.

Este es un ejemplo de mensaje SDP dentro de un protocolo SIP:

```
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
```



Nota: Algunos de los mensajes SDP contienen estos parámetros en el ejemplo:

++c-IN IP4: Dirección IP del servidor de medios

++m=audio: Esto indica que el tipo de medio es audio.

826 ++: Este es el número de puerto en el que se enviará la secuencia de audio.

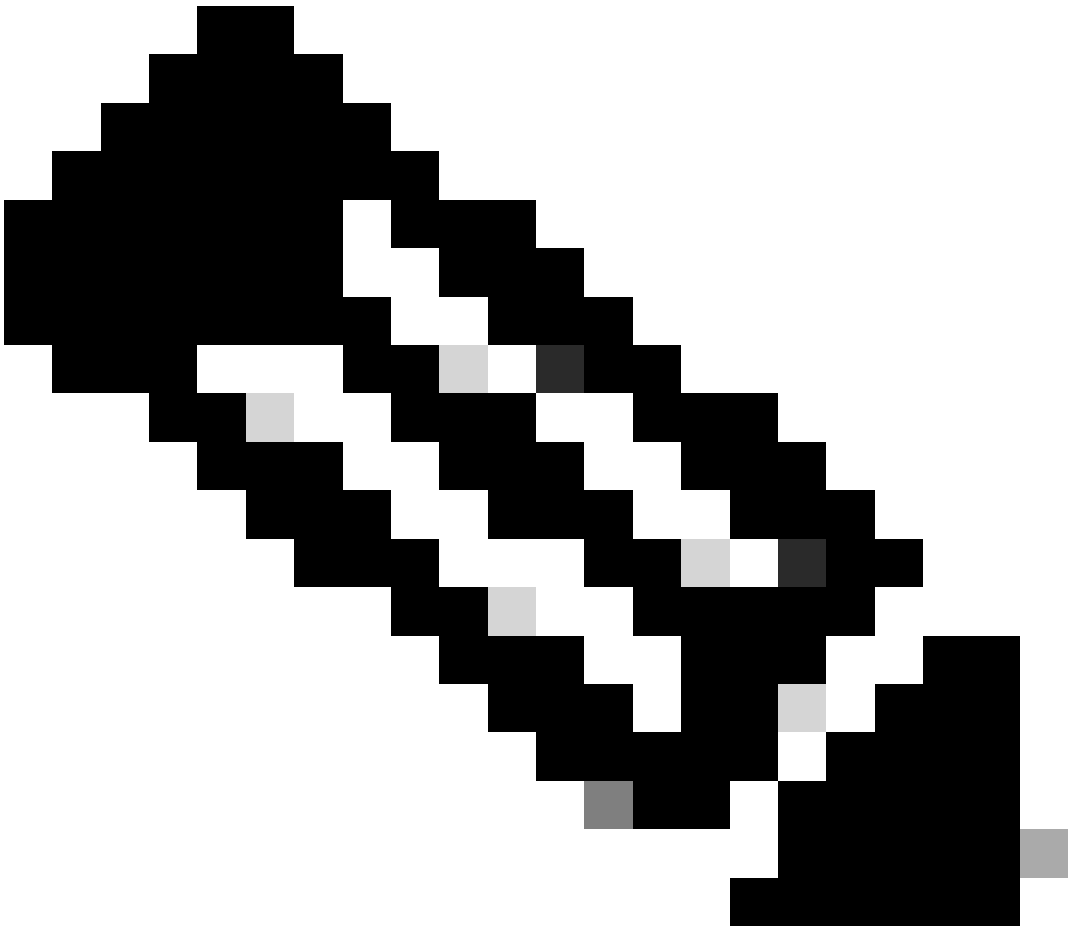
++RTP/AVP: Especifica el protocolo de transporte, que es RTP con el perfil de audio y vídeo (AVP).

18 127 ++: Estos son los tipos de carga útil para los códecs de audio. El tipo de carga útil 18 corresponde normalmente al códec G.729 y 127 es un tipo de carga útil dinámica que se puede asignar a un códec según la negociación entre los extremos.

El protocolo de descripción de sesión (SDP) se puede encontrar dentro de varios mensajes SIP como: INVITACIÓN, 183 sesiones en curso, 200 OK, ACK, etc. SDP sirve como método de respuesta para intercambiar capacidades de voz o vídeo entre las partes. A la hora de solucionar

problemas de llamadas, es fundamental comprender tres conceptos principales:

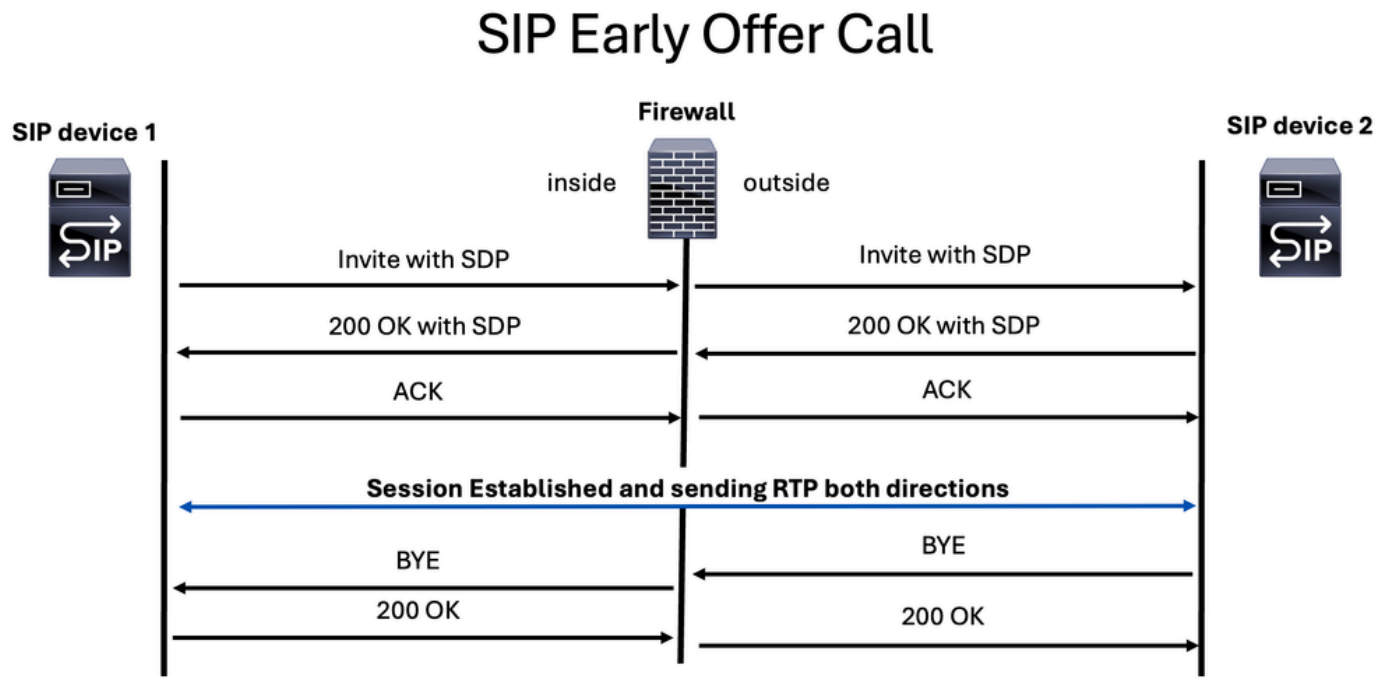
1. Oferta anticipada
2. Demorar oferta
3. Medios tempranos



> Nota: Es fundamental comprender el destino de los mensajes SDP, ya que la función de inspección del firewall puede modificar las direcciones IP no solo dentro de los encabezados SIP, sino también en la sección SDP.

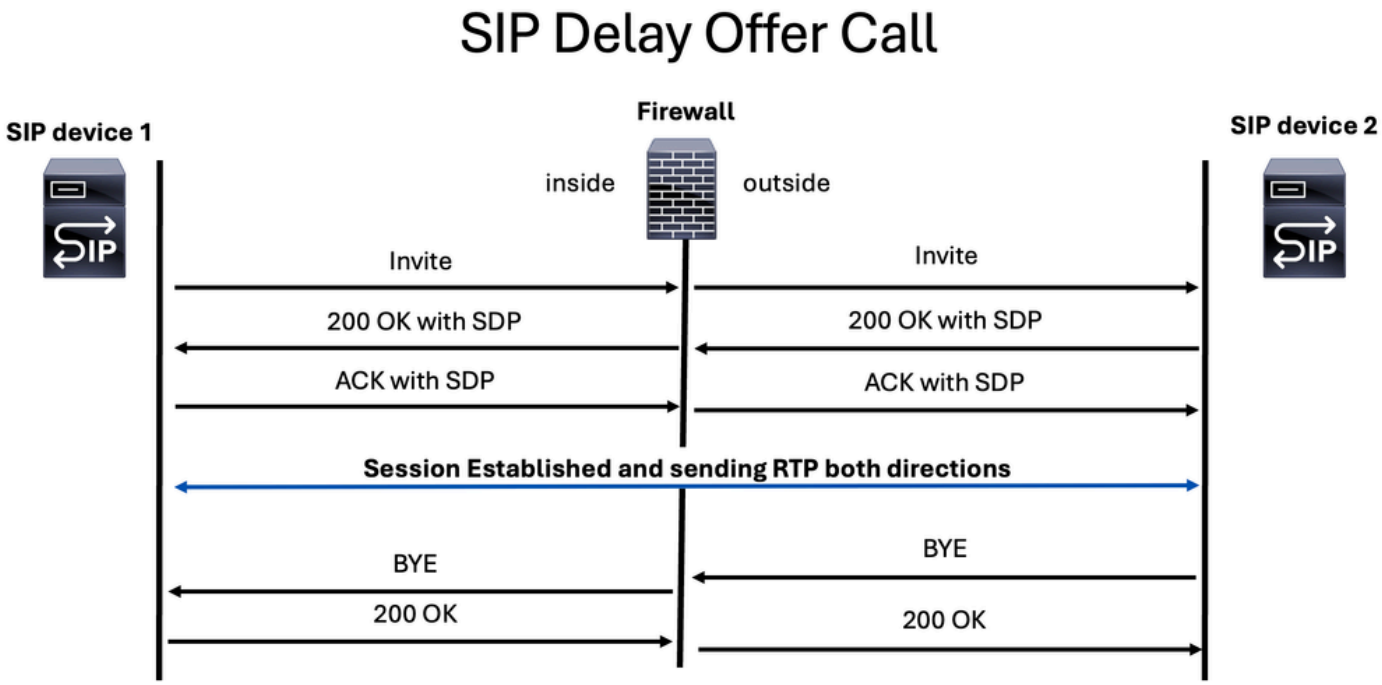
Oferta anticipada

Aquí, los parámetros de medios en SDP se encuentran dentro de los mensajes SIP INVITE y 200 OK.



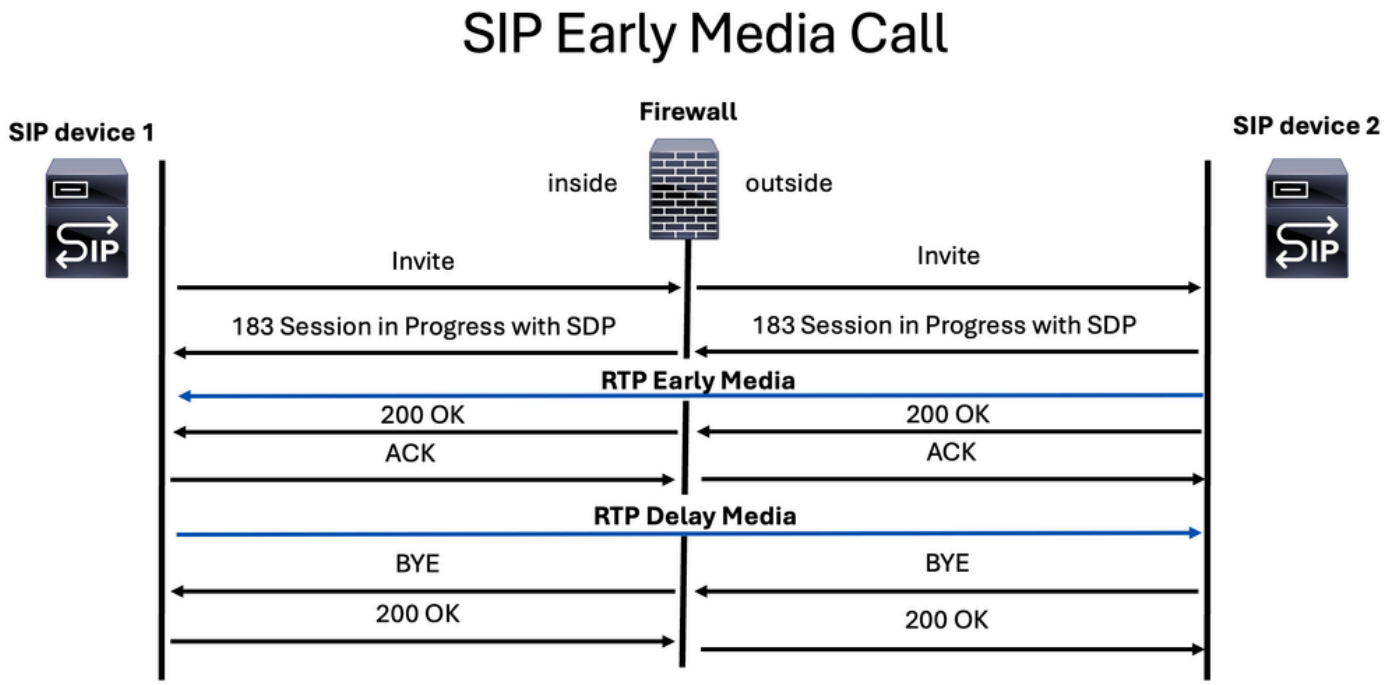
Demorar oferta

En este método, el SDP se encuentra en 200 mensajes SIP OK y ACK.



Medios tempranos

Los medios tempranos se transmiten a través de un mensaje SIP específico conocido como respuesta de progreso de sesión 183. Este mensaje incluye el protocolo de descripción de sesión (SDP) que contiene los parámetros de medios para la parte llamada. Los operadores y los proveedores de SIP lo utilizan habitualmente para enviar mensajes de voz automatizados u otros medios a la persona que llama antes de que la llamada se conecte oficialmente.

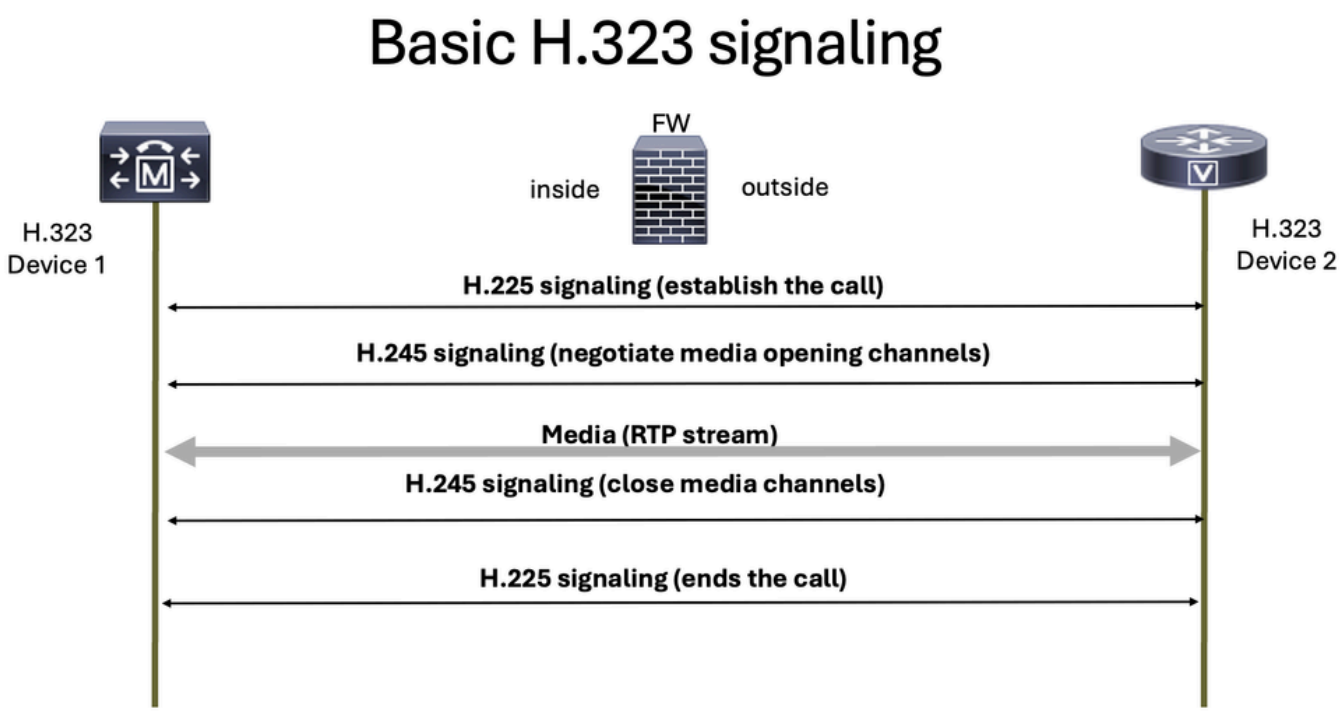


H.323

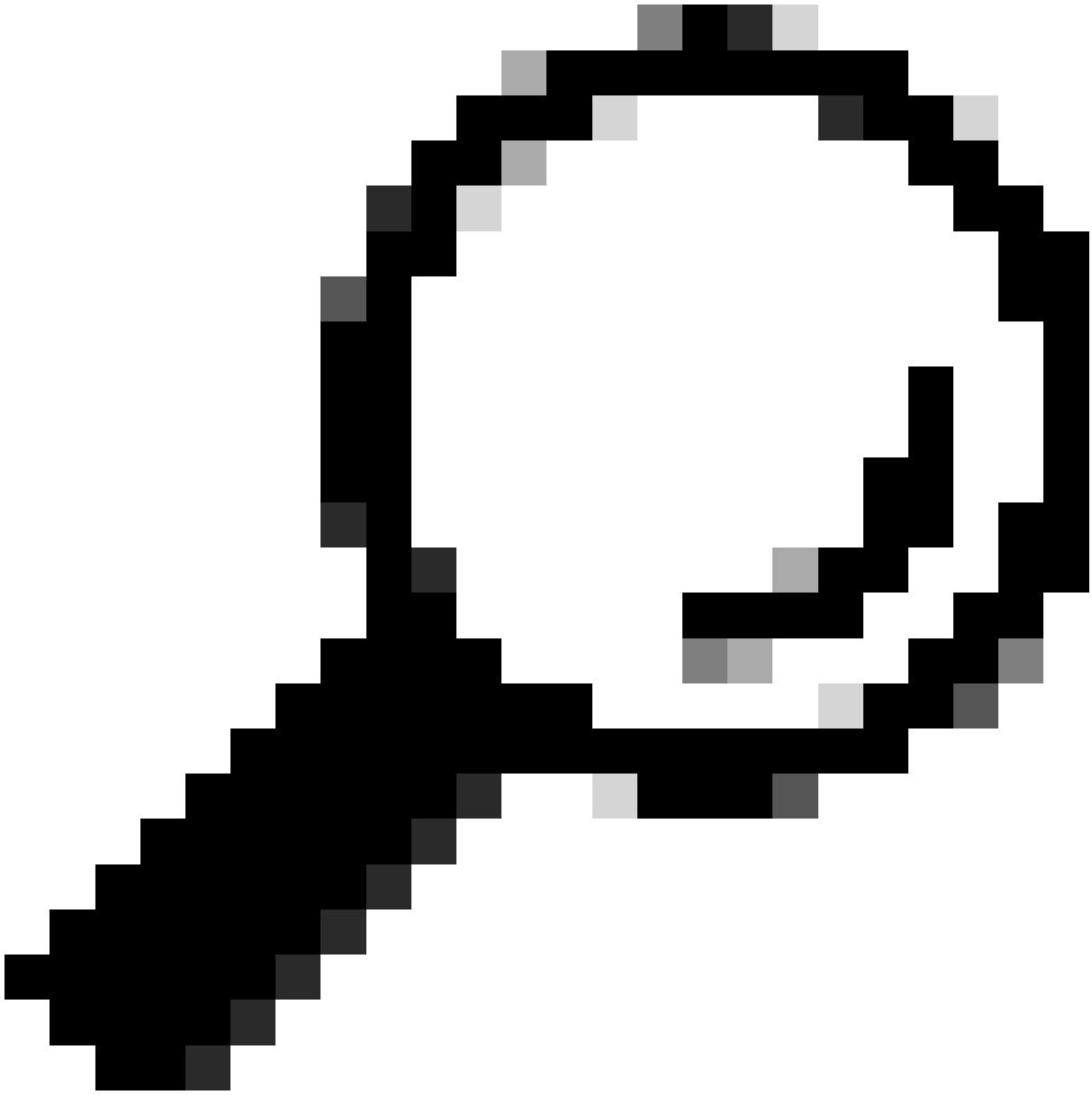
H.323 es un conjunto de protocolos definidos por la Unión Internacional de Telecomunicaciones (ITU) para las comunicaciones de voz, vídeo y datos a través de redes conmutadas por paquetes, como Internet.

El protocolo H.323 se compone de dos componentes principales:

1. H.225 Esto gestiona la señalización de llamadas, incluida la configuración y terminación de llamadas.
2. H.245: Es responsable del intercambio de capacidades y de la apertura y el cierre de canales de audio y vídeo.



Los puertos utilizados por el protocolo de señalización H.323 son 1718, 1719 y 1720.

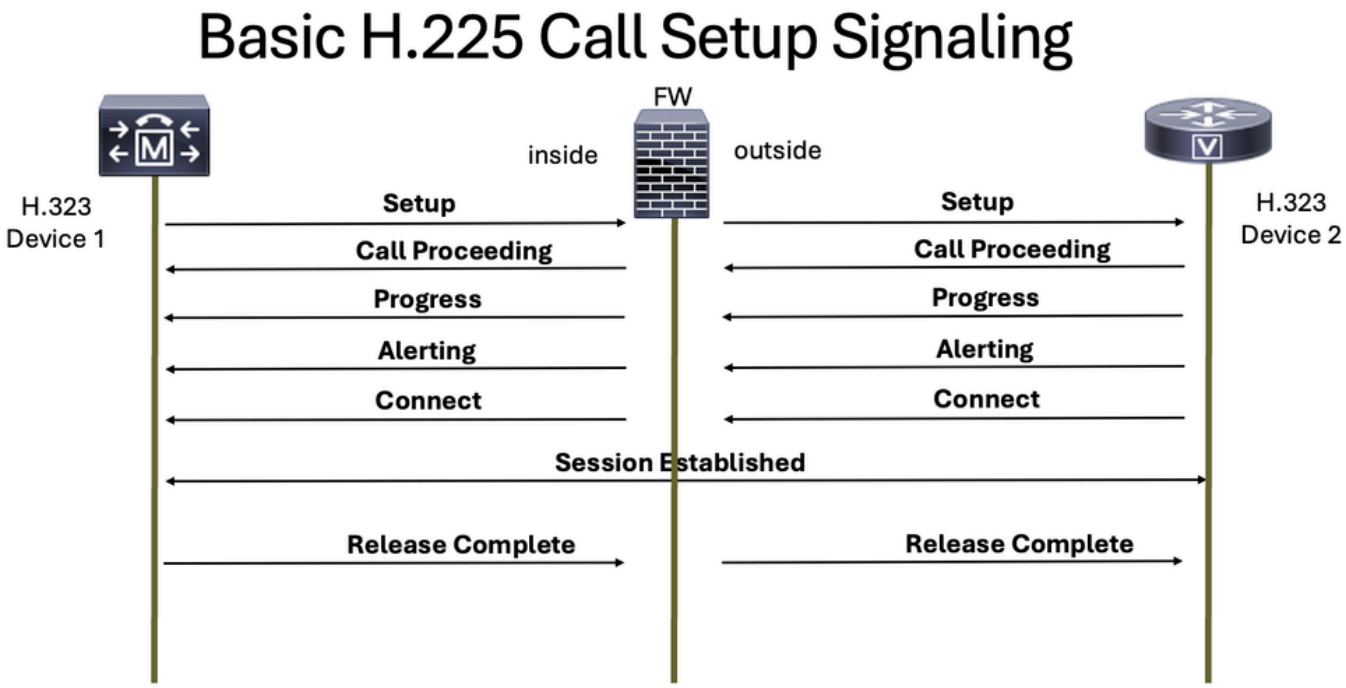


Consejo: Las comunicaciones de protocolo H.323 seguras pueden encontrar problemas al cambiar de UDP a TCP debido al uso de TLS para cifrado, lo que puede hacer que un firewall bloquee erróneamente la conexión como actividad sospechosa, por lo que es crucial configurar el firewall para permitir el tráfico UDP y TCP para los terminales o servidores H.323.

H.323 es un protocolo que tiene dos modos de operación: arranque lento y arranque rápido.

H.225

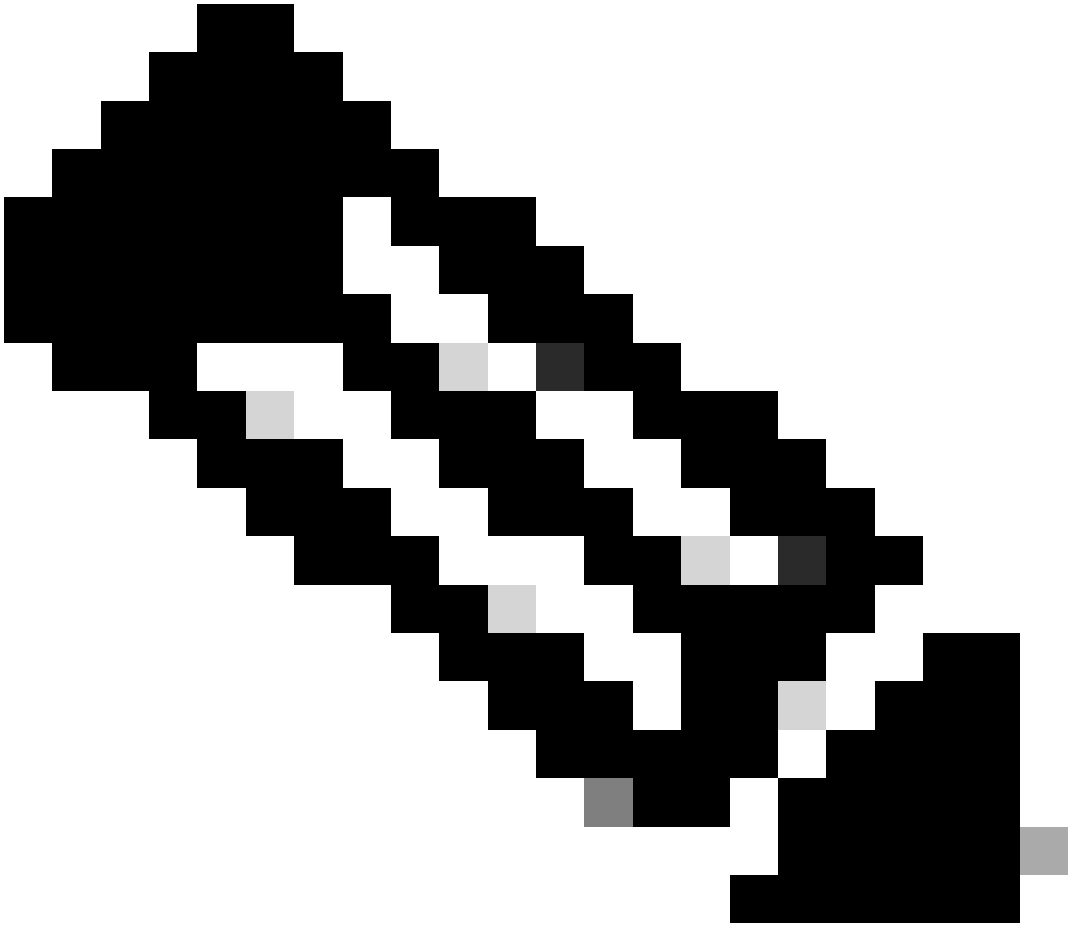
Este protocolo es responsable de configurar la llamada y finalizar una llamada de voz cuando una de las partes cuelga.



H.245

H.245 proporciona estas funcionalidades:

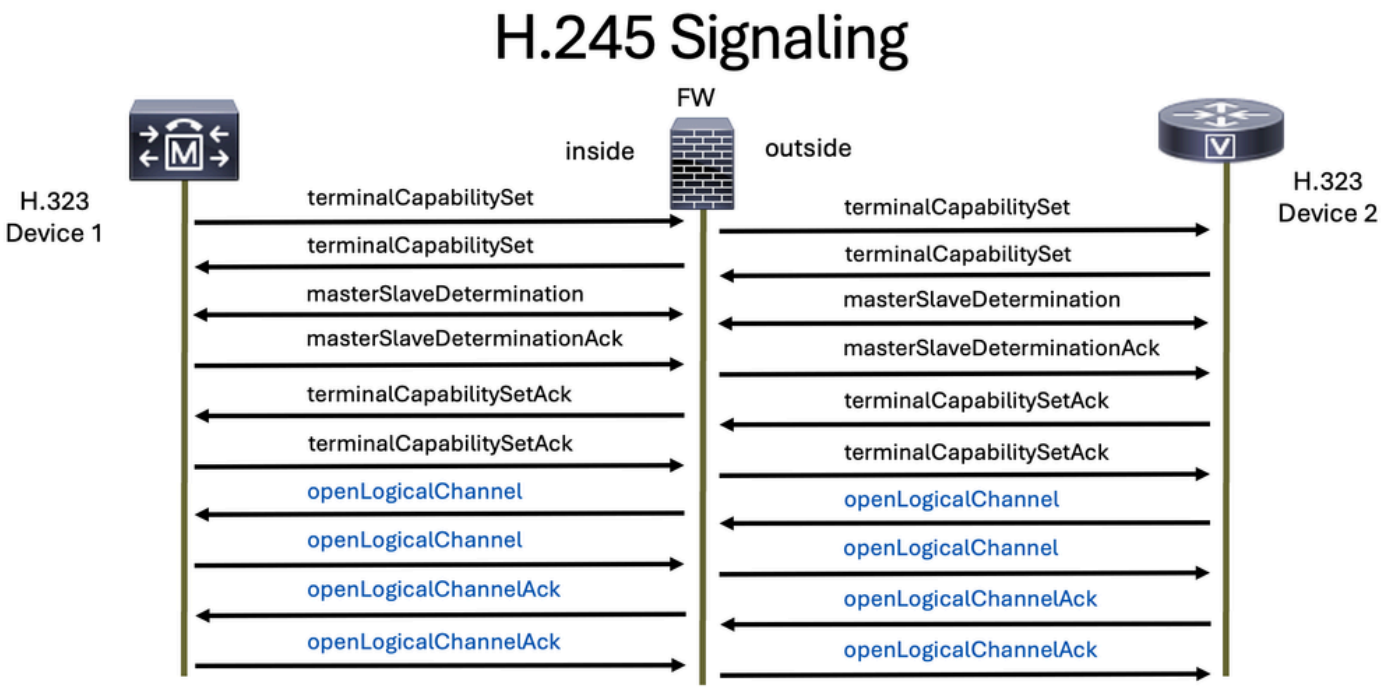
- Intercambio de capacidad de terminal
- Determinaciones de maestro/esclavo
- Señalización de canales lógicos



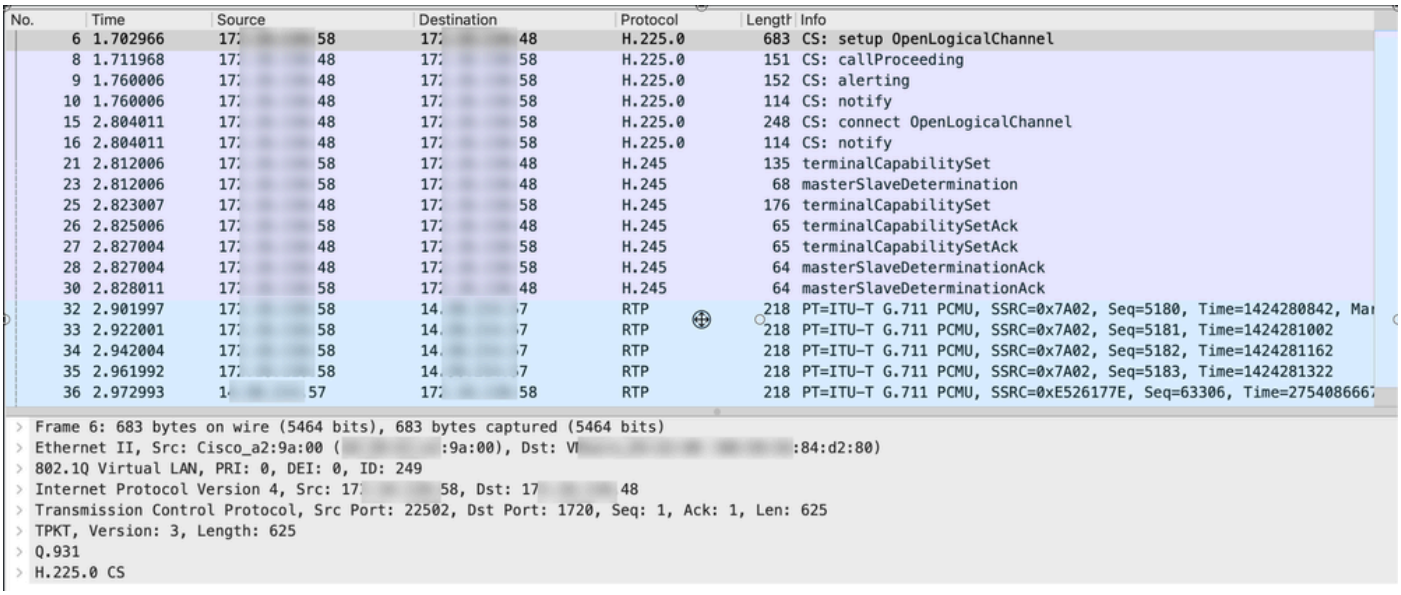
> Nota: Los términos Master y Slave utilizados en este documento están codificados en el protocolo H.323 original y no reflejan las políticas o valores de nuestra empresa. Estamos comprometidos con la promoción de un lenguaje inclusivo y respetuoso.

El protocolo H.245 se envía después de recibir el mensaje de conexión H.225.

Este protocolo ayuda a determinar qué protocolo de voz se utiliza para RTP y se especifica en los mensajes de canal lógico de apertura y cierre para él.



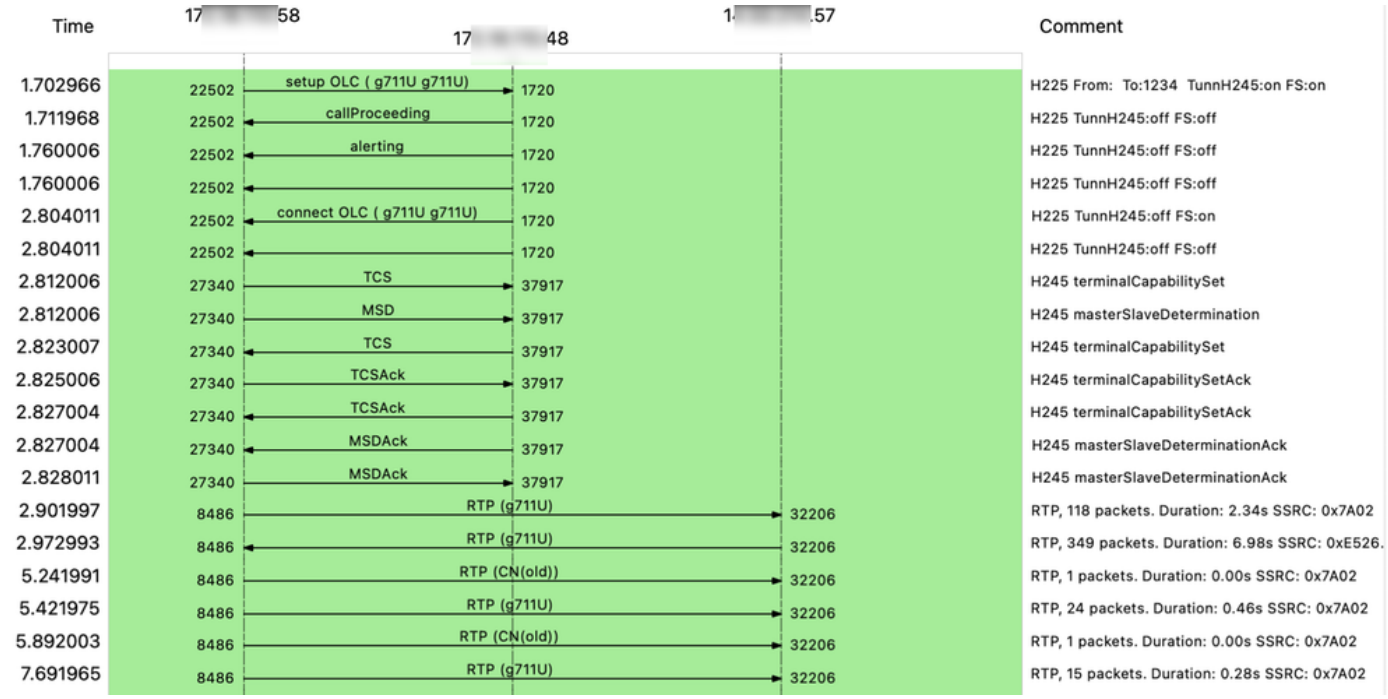
Esta captura de paquetes muestra las solicitudes y respuestas de dos dispositivos H.323 con H.225 y H.245 y también el tráfico de medios (voz):

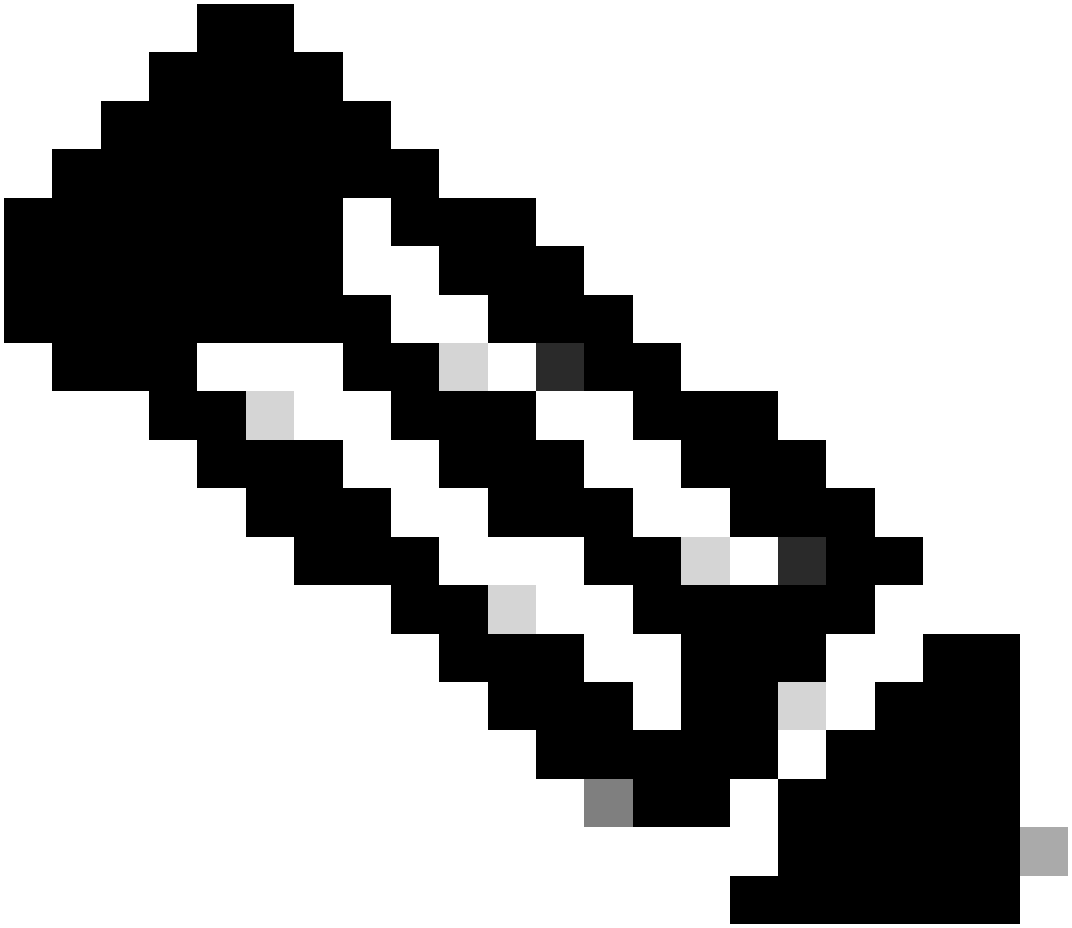


No.	Time	Source	Destination	Protocol	Length	Info
6	1.702966	17. 58	17. 48	H.225.0	683	CS: setup OpenLogicalChannel
8	1.711968	17. 48	17. 58	H.225.0	151	CS: callProceeding
9	1.760006	17. 48	17. 58	H.225.0	152	CS: alerting
10	1.760006	17. 48	17. 58	H.225.0	114	CS: notify
15	2.804011	17. 48	17. 58	H.225.0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

Este es un ejemplo de un flujo de señalización H.323 con medios H.225 y H.245 y RTP (voz):

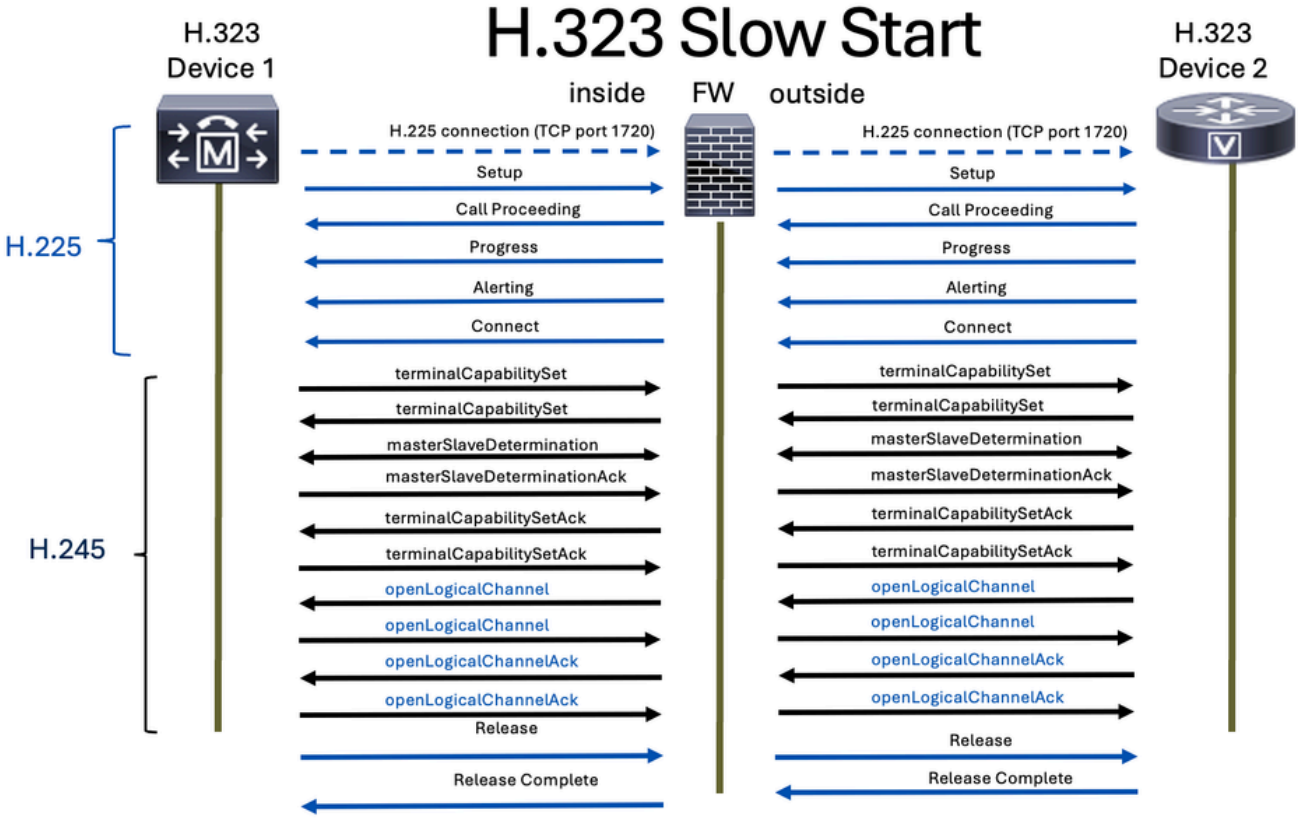

Time
Comment
1.702966 22502 setup OLC (g711U g711U) 1720 H225 From: To:1234 TunnH245:on FS:on
1.711968 22502 callProceeding 1720 H225 TunnH245:off FS:off
1.760006 22502 alerting 1720 H225 TunnH245:off FS:off
1.760006 22502 1720 H225 TunnH245:off FS:off
2.804011 22502 connect OLC (g711U g711U) 1720 H225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



Nota: La inspección H.323 está activada de forma predeterminada en Cisco Secure Firewall Threat Defense (FTD) y Secure Firewall Adaptive Security Appliance (ASA).

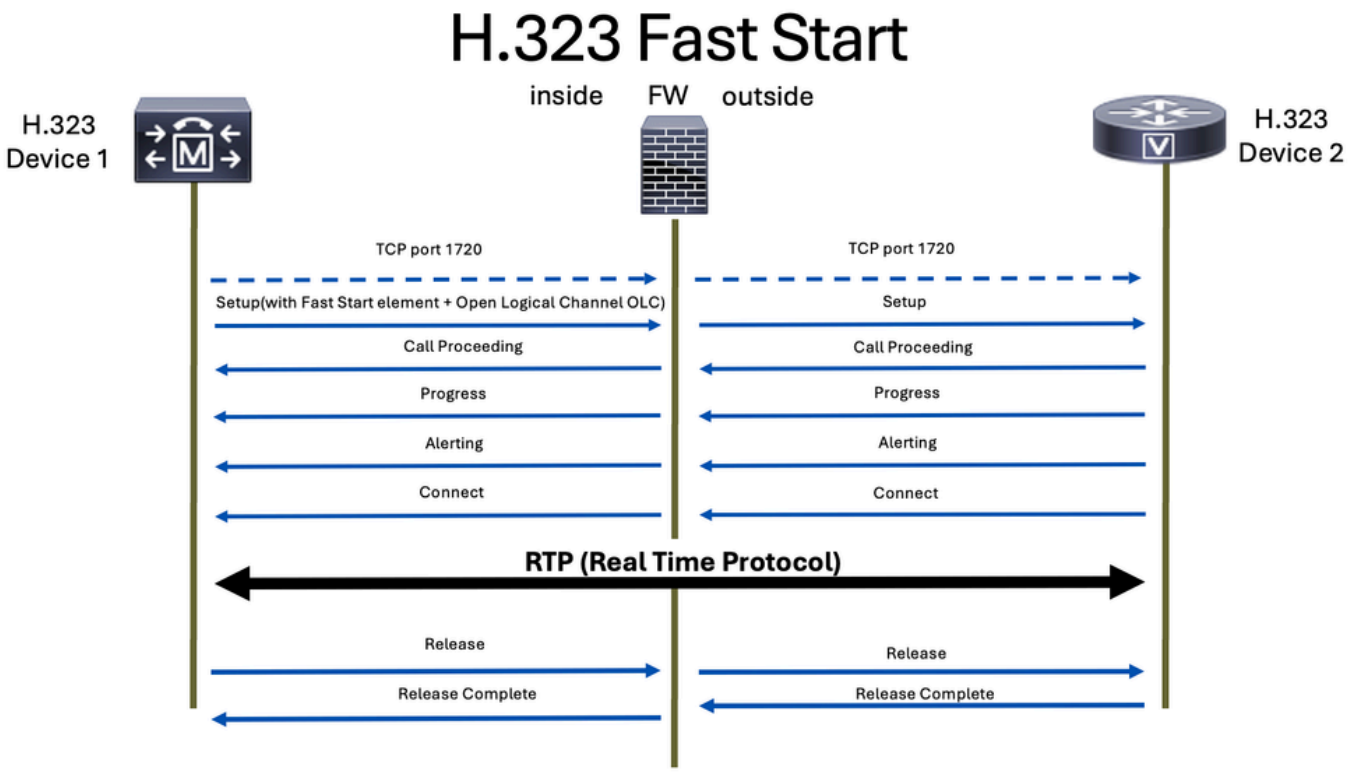
Slow Start

En el modo de inicio lento, el proceso de configuración de la llamada implica varios pasos de señalización antes de que se establezcan los canales de medios. Entre los pasos se incluyen Setup (Configuración), Call Proceeding (Procedimiento de llamada), Alerting (Alerta) y Connect (Conectar). Después de estos pasos, la negociación de medios H.245 se realiza por separado. Esto significa que los canales de medios no se establecen hasta después de que se haya completado la señalización de llamada inicial, lo que puede resultar en un tiempo de configuración más largo.



Inicio rápido

Por el contrario, el modo de inicio rápido permite que se produzca la negociación de medios dentro del mensaje de configuración inicial. Esto significa que los canales de medios se pueden establecer más rápidamente, ya que la negociación se realiza como parte de la configuración de llamada inicial. Fast Start simplifica el proceso al reducir el número de mensajes intercambiados y la cantidad de procesamiento necesario antes de establecer los canales de medios.

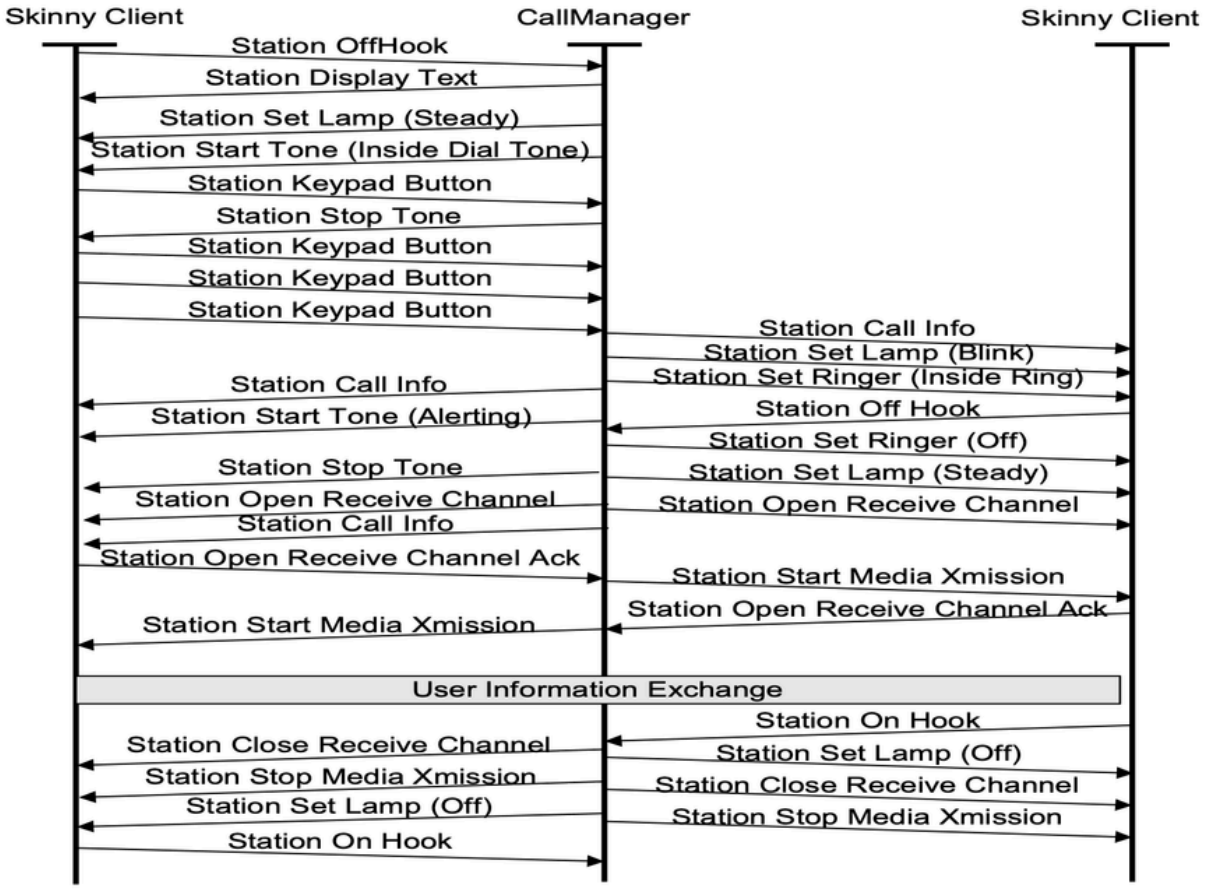


SCCP

El protocolo de control de clientes (SCCP) Skinny, a menudo denominado simplemente Skinny, es un protocolo de señalización propiedad de Cisco. Los utilizan principalmente Cisco Unified Communications Manager (CUCM), los routers Cisco Unified Communications Manager Express (CME) y los Cisco IP Phones para facilitar la configuración y el control de las llamadas.

El protocolo SCCP utiliza TCP en el puerto 2000 para SCCP no seguro y utiliza el puerto 2443 para SCCP seguro.

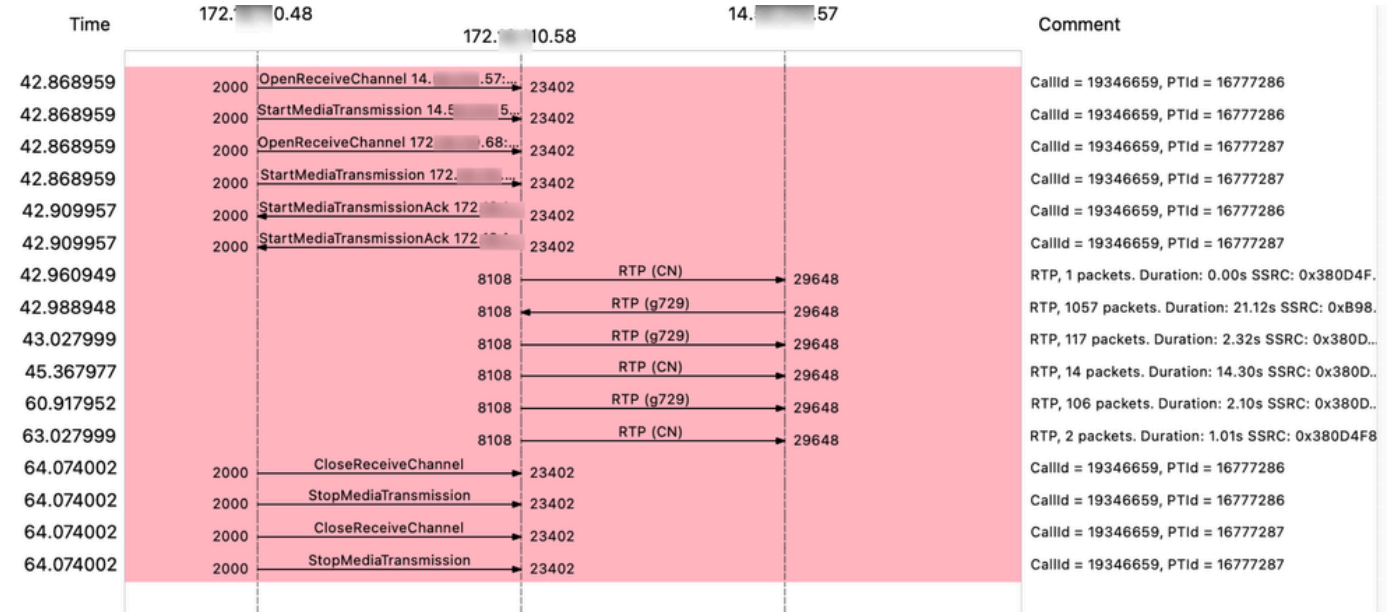
Estos son los mensajes SCCP comunes que puede encontrar en una llamada SCCP:

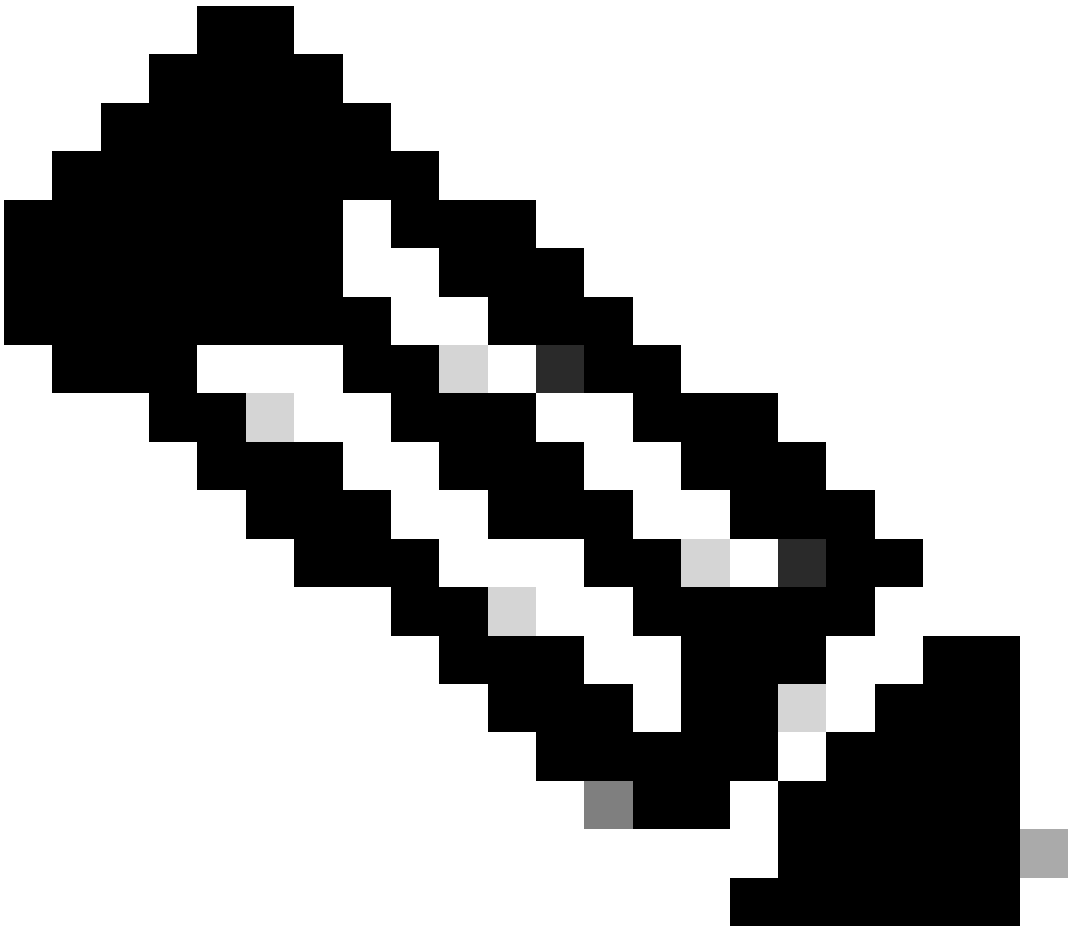


Esta captura de paquetes muestra las solicitudes y respuestas de dos dispositivos SCCP y también el tráfico de medios (voz):

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

Este es un ejemplo de un flujo de señalización SCCP y medios RTP (voz):





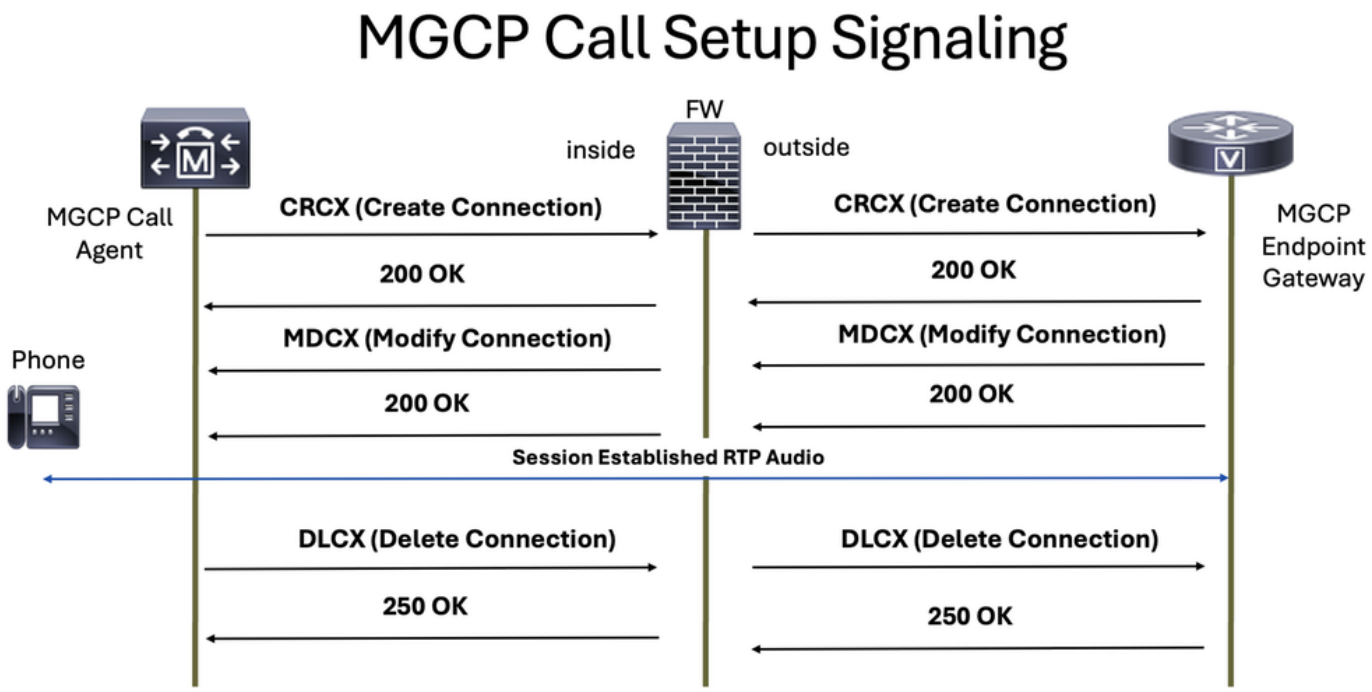
Nota: La inspección SCCP está activada de forma predeterminada en Cisco Secure Firewall Threat Defense (FTD) y Secure Firewall Adaptive Security Appliance (ASA).

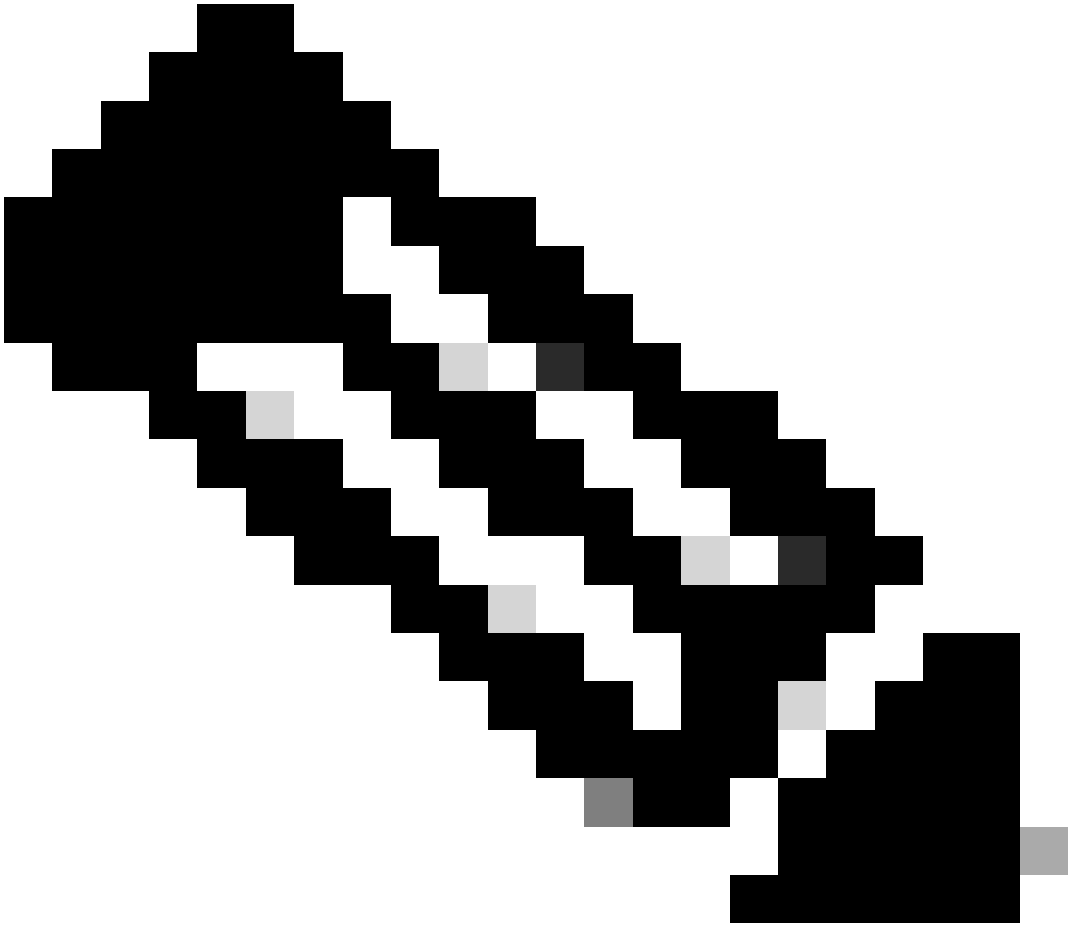
MGCP (Protocolo de control de gateway de medios)

El protocolo de control de gateway de medios (MGCP) es un protocolo utilizado para el control de llamadas VoIP por un dispositivo de control de llamadas, por ejemplo, CUCM.

El protocolo de señalización MGCP se define en RFC 2705 y utiliza el puerto TCP 2428 y el puerto UDP 2427 para la comunicación.

Los paquetes normales MGCP que se esperan para una comunicación de llamada son:



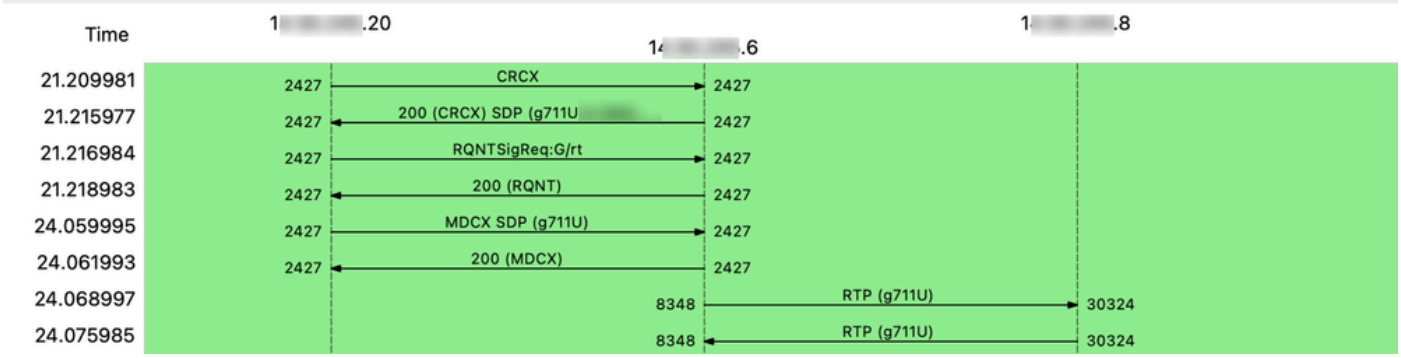


> Nota: La inspección MGCP no está habilitada en la política de inspección predeterminada en Cisco Secure Firewall Threat Defense (FTD) y Secure Firewall Adaptive Security Appliance (ASA), por lo que debe habilitarla si necesita esta inspección.

Esta captura de paquetes muestra las solicitudes y respuestas de dos dispositivos MGCP y también el tráfico de medios (voz):

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

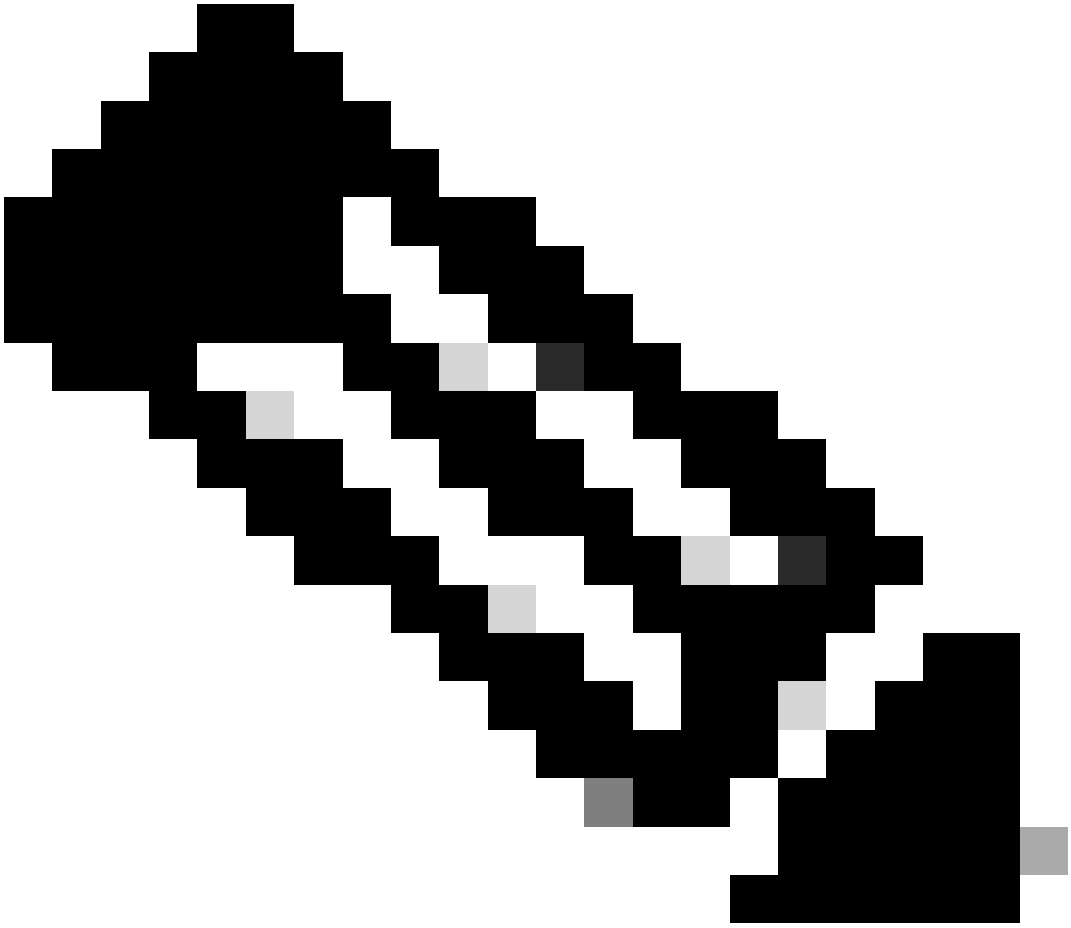
Este es un ejemplo de un flujo de señalización MGCP y medios RTP (voz):



Mejores medidas

Para ASA:

- Utilice una regla de permiso que permita el tráfico hacia y desde los dos componentes de señalización (dispositivos o servidores). Esto puede estar limitado por los puertos utilizados en el protocolo VoIP de señalización especificado.
- Permite el intervalo de puertos RTP entre los dispositivos de medios que pueden enviar o recibir transmisiones de audio o vídeo.



Nota: Recuerde que estos dispositivos de audio o medios podrían ser diferentes de los componentes de señalización (dispositivos o servidores).

Para FTD:

- Defina reglas de prefiltrado para los componentes de señalización (dispositivos o servidores) y defina el puerto específico para limitar sólo el tráfico para el protocolo de señalización especificado.
- Configure el filtro previo para el protocolo RTP de audio y/o vídeo.

Troubleshoot

Al solucionar problemas de voz, debe saber si el problema es de señalización o multimedia (voz o vídeo) o ambos. A continuación, se incluyen algunos ejemplos que pueden guiarle para diferenciarlo:

Ejemplo de problemas de señalización:

++El usuario informa de que no se ha establecido la llamada.

++El usuario no puede llamar a otros usuarios o números.

++El troncal SIP no aparece, porque el mensaje SIP OPTIONS no recibe respuesta.

++Mi dispositivo no se puede registrar.

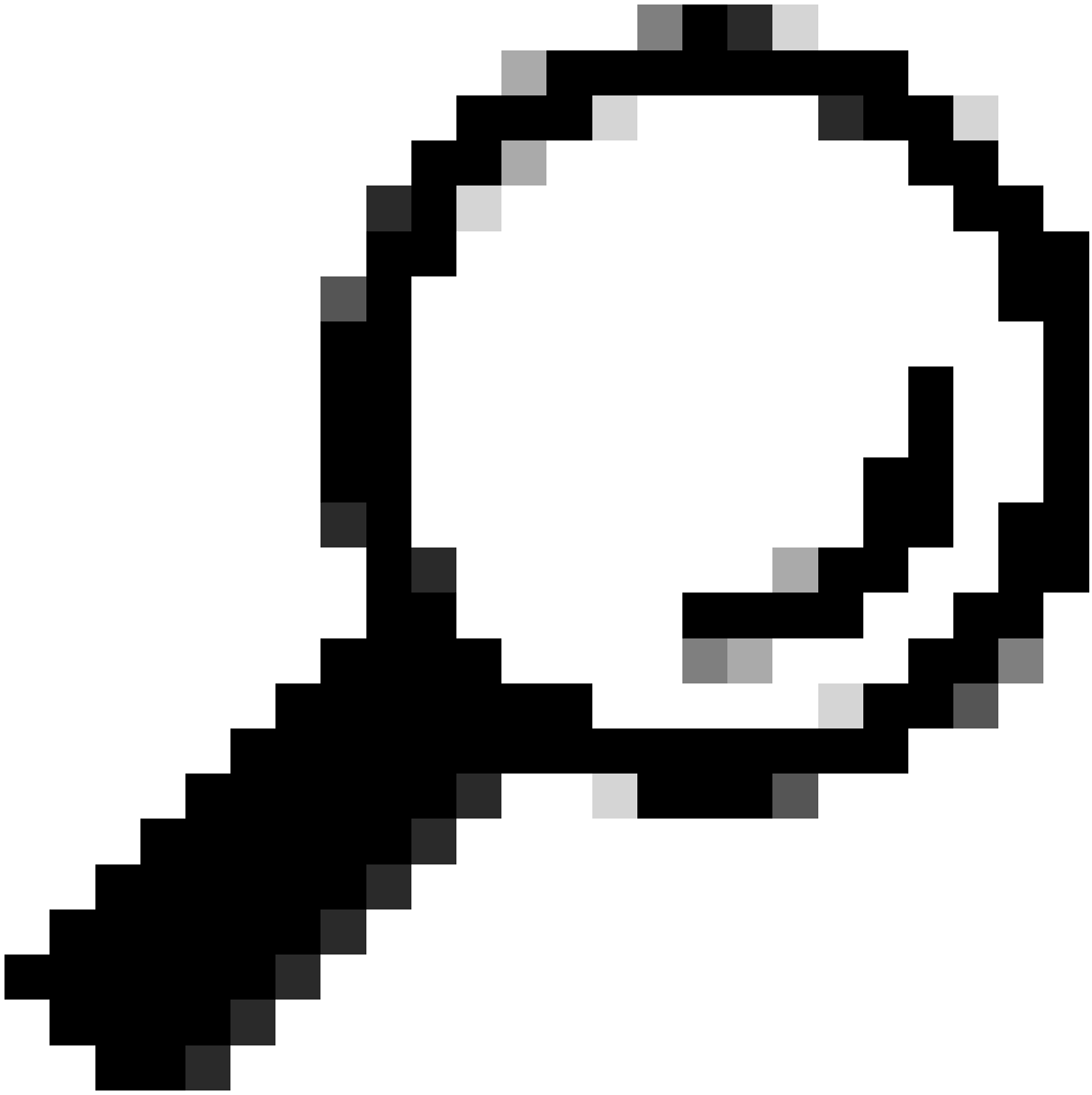
Ejemplo de problemas de medios (voz o vídeo):

++Hay un problema de audio unidireccional.

++No hay audio en la llamada.

++No hay vídeo en absoluto.

++La llamada se silencia.



Consejo: Durante una videollamada, el SDP puede negociar hasta tres líneas de medios (líneas m): audio, vídeo e imagen. Cada línea m corresponde a una secuencia independiente de protocolo de transporte en tiempo real (RTP) por segmento de llamada, lo que significa que puede haber hasta tres transmisiones RTP distintas (una para cada tipo de medio) en cada segmento de la llamada.

Resolución de problemas de señalización en firewall

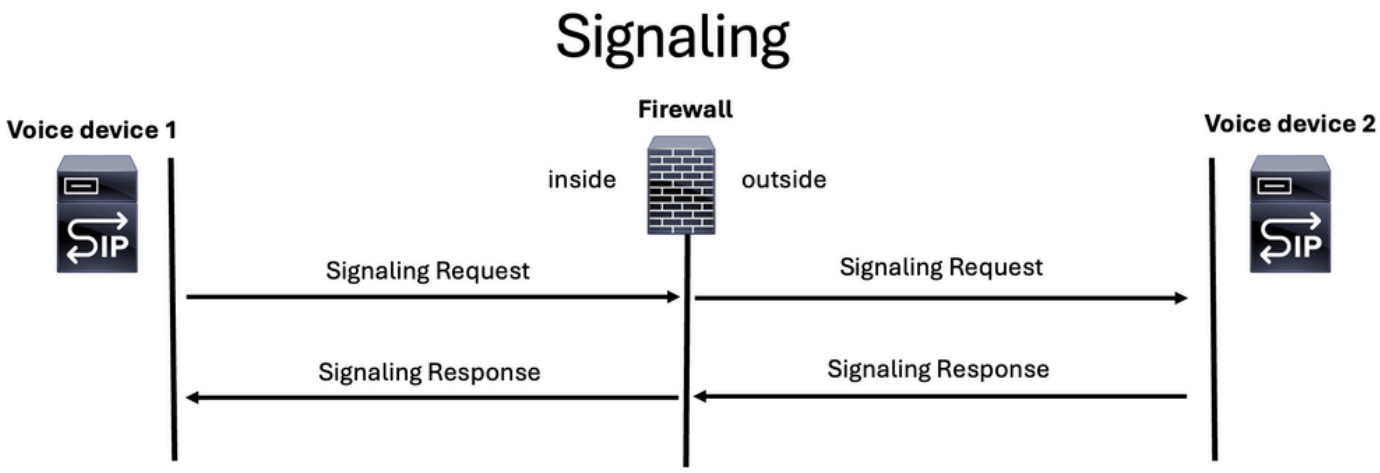
Para la resolución de problemas de la parte de señalización debe asegurarse de:

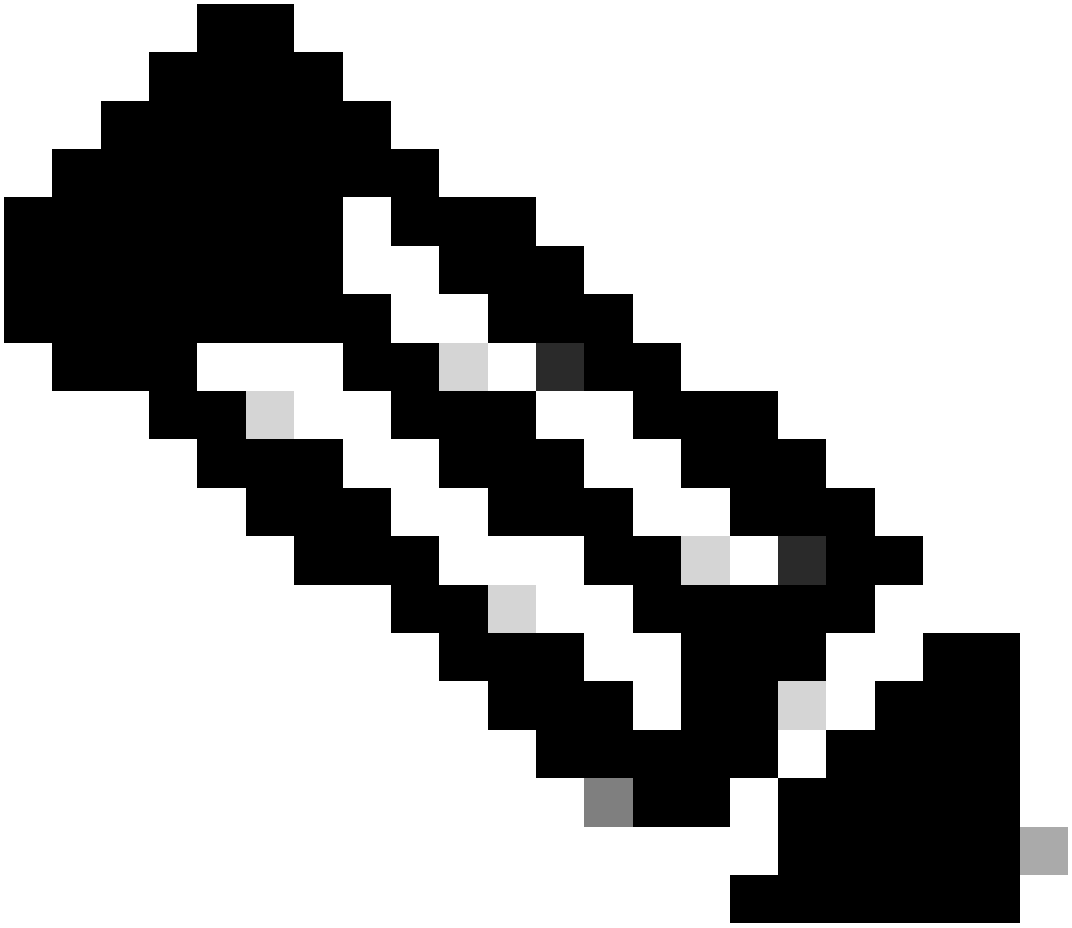
++Identifique todos los componentes de señalización (dispositivos o servidores) involucrados en la llamada desde la interfaz de ingreso y egreso y configure los criterios de coincidencia apropiados en las capturas de paquetes en CLI de cualquiera de los FW seguros.

++Recuerde que el número de mensajes de señalización en la interfaz de ingreso debe coincidir con la interfaz de egreso.

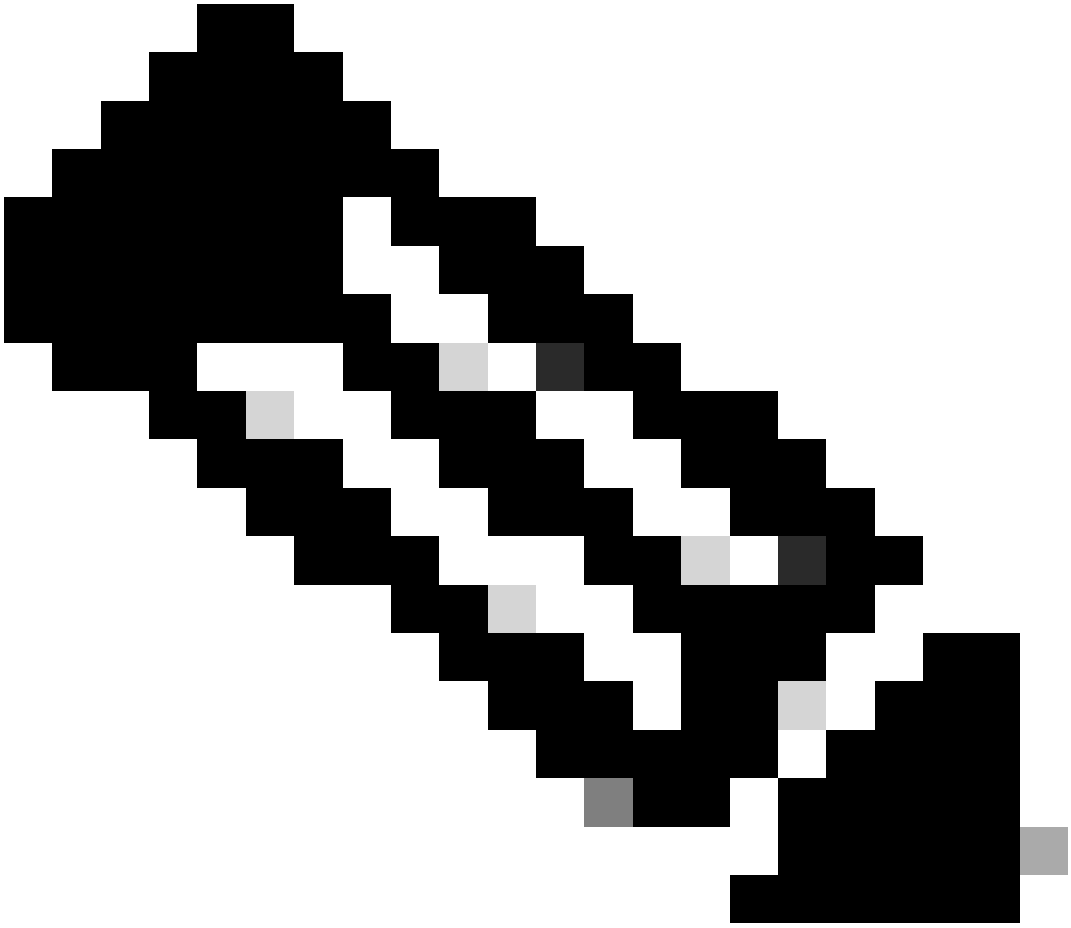
++La captura de paquetes se puede hacer más eficiente especificando si el protocolo de señalización utiliza TCP o UDP y filtrando el número de puerto esperado. Dado que todos los protocolos de señalización funcionan sobre IP, la aplicación de estos filtros en la CLI ayuda a restringir la cantidad de tráfico que ve en las capturas.

++Sólo para interfaces de salida, asegúrese de que la dirección IP de NAT asignada al tráfico saliente se especifica en el filtro de captura de paquetes. Esto garantiza que está capturando el tráfico correcto tal como aparece en la interfaz de salida.





Nota: Recuerde que, independientemente del protocolo de señalización que se utilice para la voz, siempre debe haber una solicitud y una respuesta, y debe ser consistente tanto en las interfaces de ingreso como de egreso.

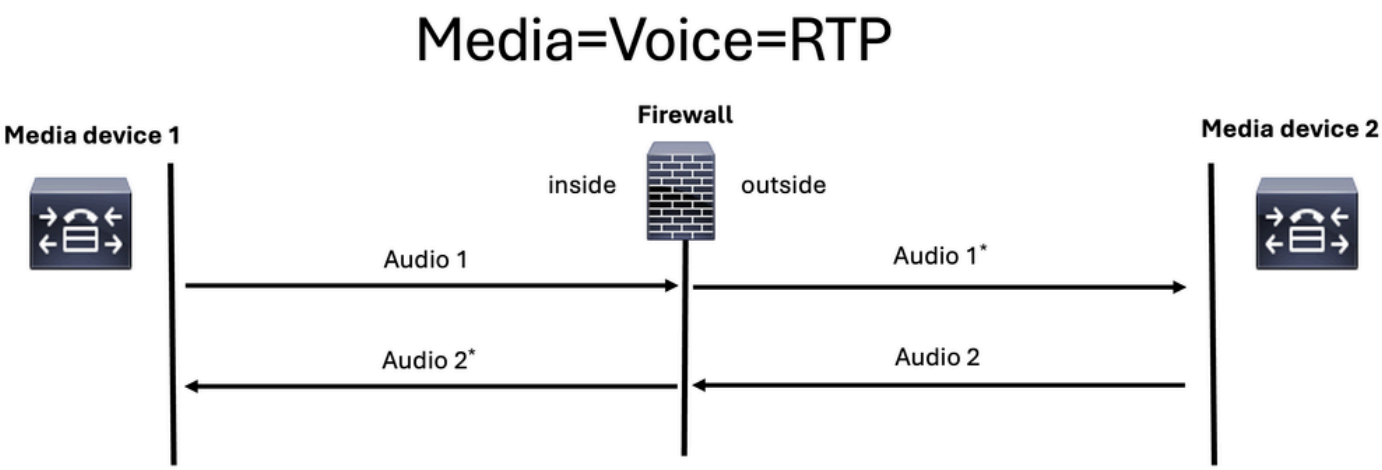


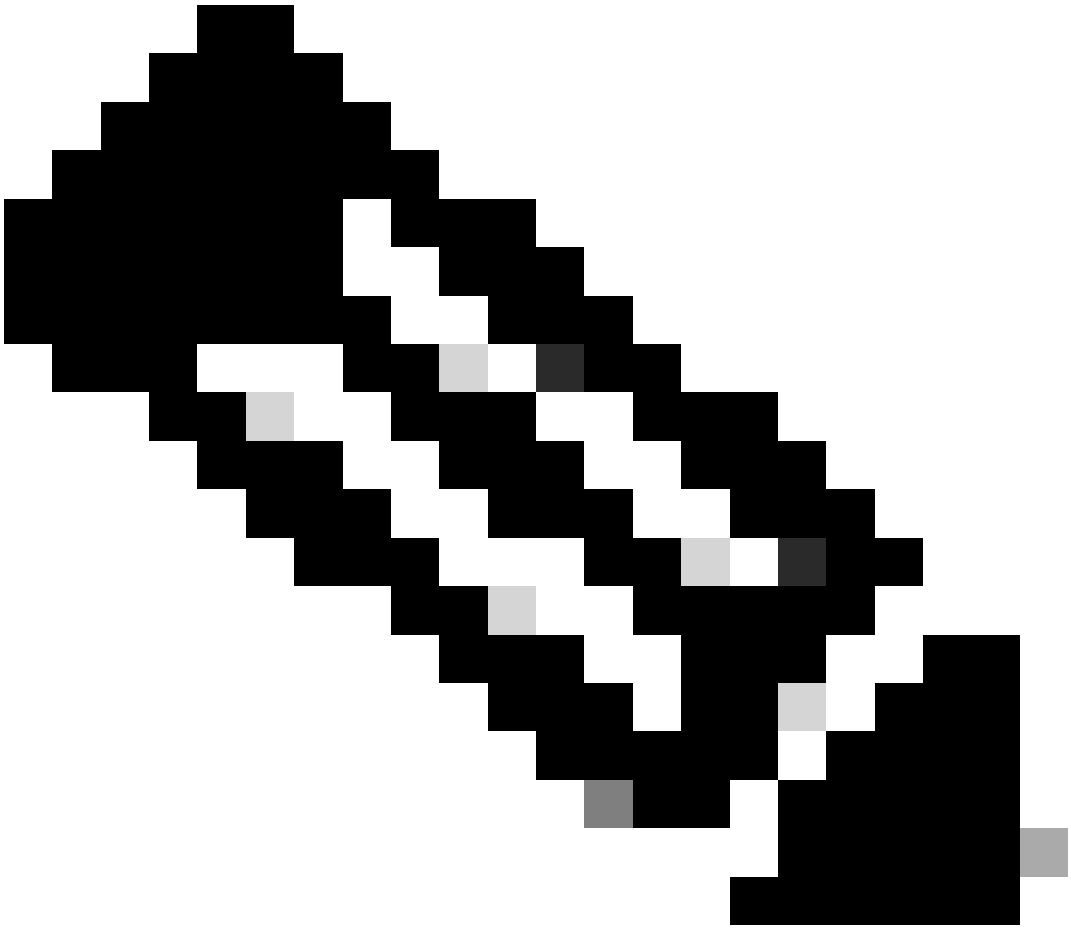
Nota: siempre que sea posible, asegúrese de que solo haya un firewall involucrado en la ruta de comunicación. En algunas implementaciones, la señalización de voz y las transmisiones multimedia pueden atravesar firewalls independientes. En estos casos, asegúrese de incluir todos los firewalls relevantes en el proceso de solución de problemas

Solución de problemas de medios en firewall

Desde la perspectiva de FW, habrá 4 flujos que se deben analizar al resolver problemas de audio unidireccional, problemas de audio bidireccional o sin audio:

1. Flujo RTP de la persona que llama a la persona que llama (interfaz de entrada).
2. Flujo RTP de la persona que llama a la persona que llama (interfaz de salida).
3. Flujo RTP de la persona que llama a la que llama (interfaz de salida).
4. Flujo RTP de la persona que llama a la que llama (interfaz de entrada).



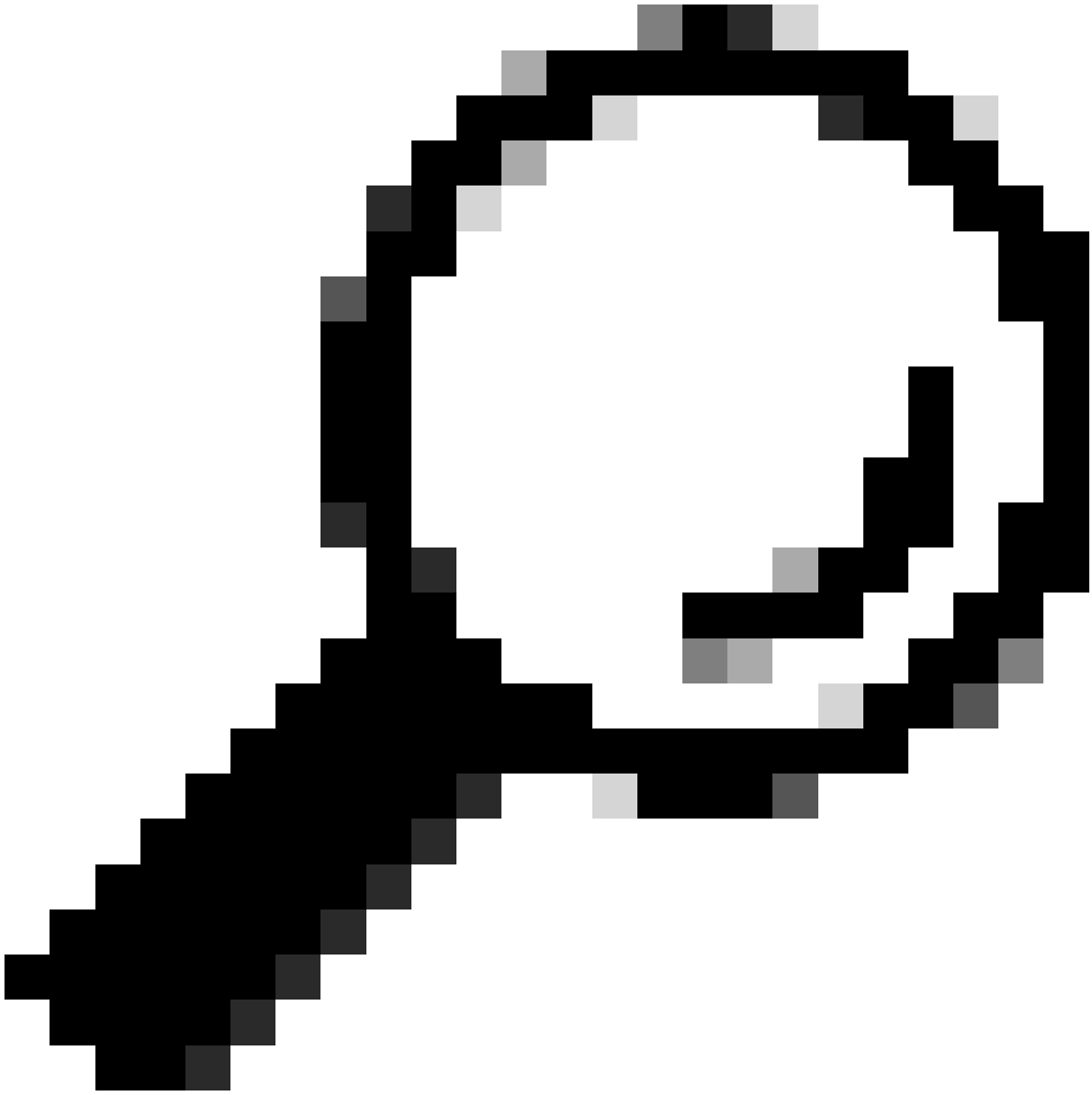


Nota: Asegúrese de realizar la resolución de problemas mediante capturas de paquetes CLI en el modo ASA o LINA en el FTD, ya que esto proporciona una mayor flexibilidad para aplicar varias coincidencias dentro de una sola captura de paquetes.

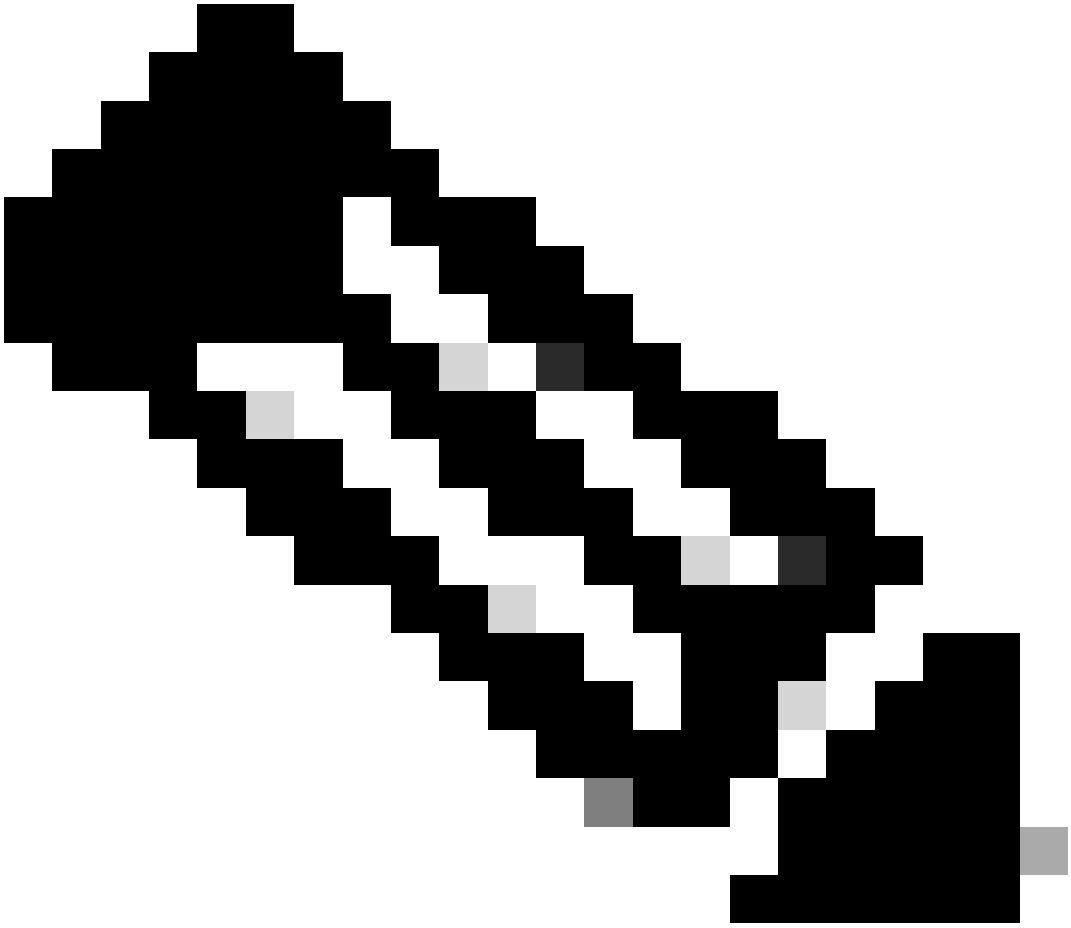
Solución de problemas de llamadas SIP

Al solucionar problemas de voz en Secure FW (ASA o FTD), debe llevar a cabo estos pasos:

1. Asegúrese de tener el flujo de llamadas y el diagrama de topología.
2. Asegúrese de comprender el problema desde la perspectiva del usuario.
3. Comprender la ruta del protocolo de señalización.
4. Comprender la ruta del protocolo RTP de medios.
5. Tome capturas de paquetes en las interfaces de ingreso y egreso.
6. Revise las reglas de configuración ACL y las reglas NAT.
7. Verifique que el tráfico de señalización SIP no esté siendo bloqueado por el firewall. Además, compare las interfaces de entrada y salida para analizar el flujo del tráfico de voz.
8. Verifique que el firewall no esté bloqueando el tráfico de medios RTP comparando el flujo de tráfico en las interfaces de entrada y salida.
9. Asegúrese de que los dispositivos de señalización admitan la inspección y, si no es así, inhabilite esa inspección.



Consejo: Los mensajes de señalización SIP que ingresan al FW también deben ser los mismos que los que salen del FW.



Nota: Las sugerencias de solución de problemas para SIP también se pueden aplicar a los protocolos H.323, MGCP y SCCP.

Información Relacionada

- Configuración de capturas de paquetes ASA con CLI
- Utilice capturas de Firepower Threat Defence

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).