보안 방화벽을 위한 VoIP(Voice over IP) 프로토콜의 기본 정보 파악

목차

소개

이 문서에서는 엔지니어가 보안 방화벽에서 효과적으로 문제를 해결할 수 있도록 다양한 VoIP 프로토콜의 기본 사항에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 다음 장치와 관련된 문제 해결 시나리오에 사용하기 위한 것입니다.

- FTD(보안 방화벽 위협 방어)
- 보안 방화벽 ASA(Adaptive Security Appliance)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

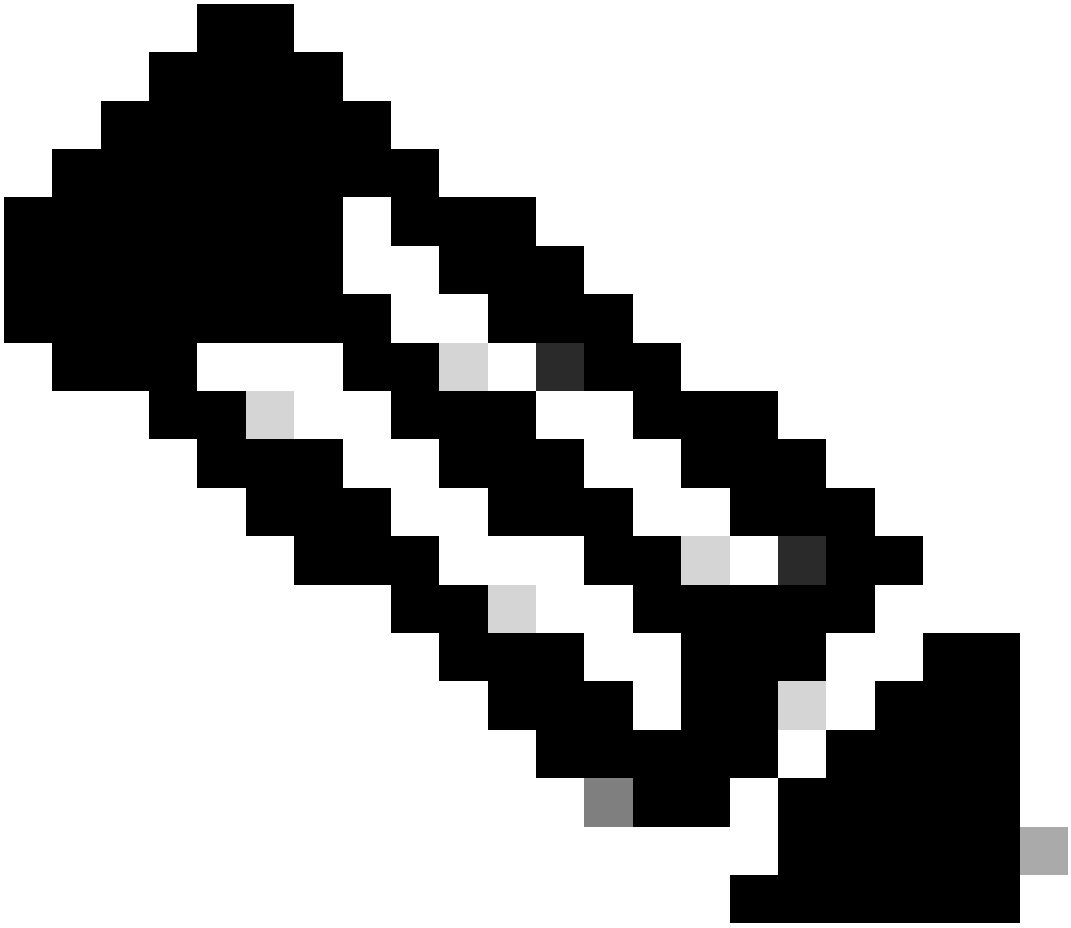
VoIP의 기초

커뮤니케이션은 사람의 상호작용에 필수적입니다. VoIP(Voice over IP) 프로토콜은 사람의 커뮤니케이션에 없어서는 안 될 요소가 되었습니다. 따라서 방화벽(FW)이 포함된 시나리오를 트러블슈팅할 때 해당 부분을 아는 것이 중요합니다.

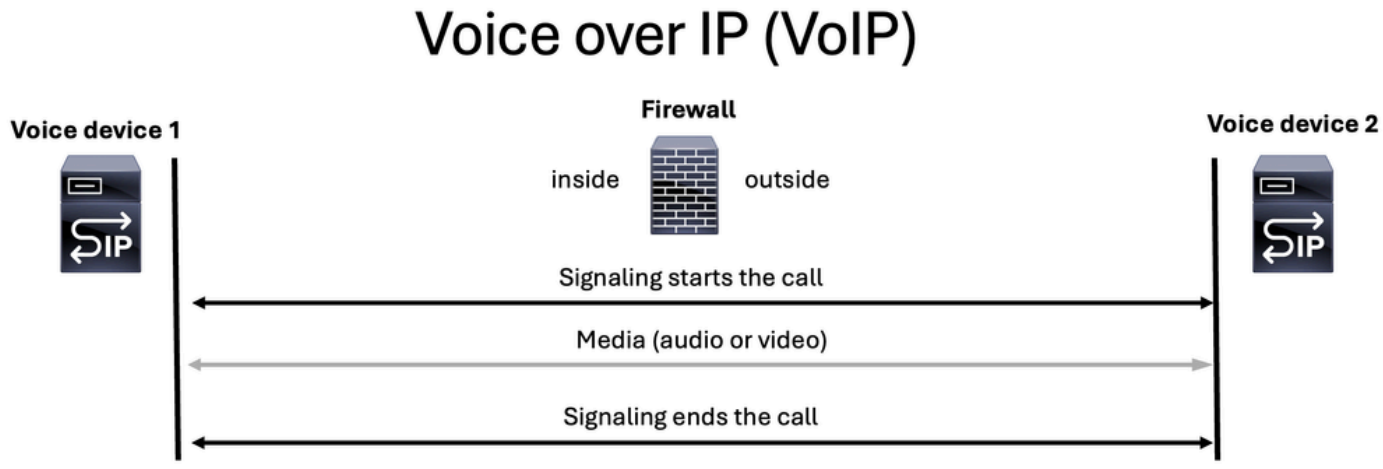
VoIP는 다음 두 부분으로 구성됩니다.

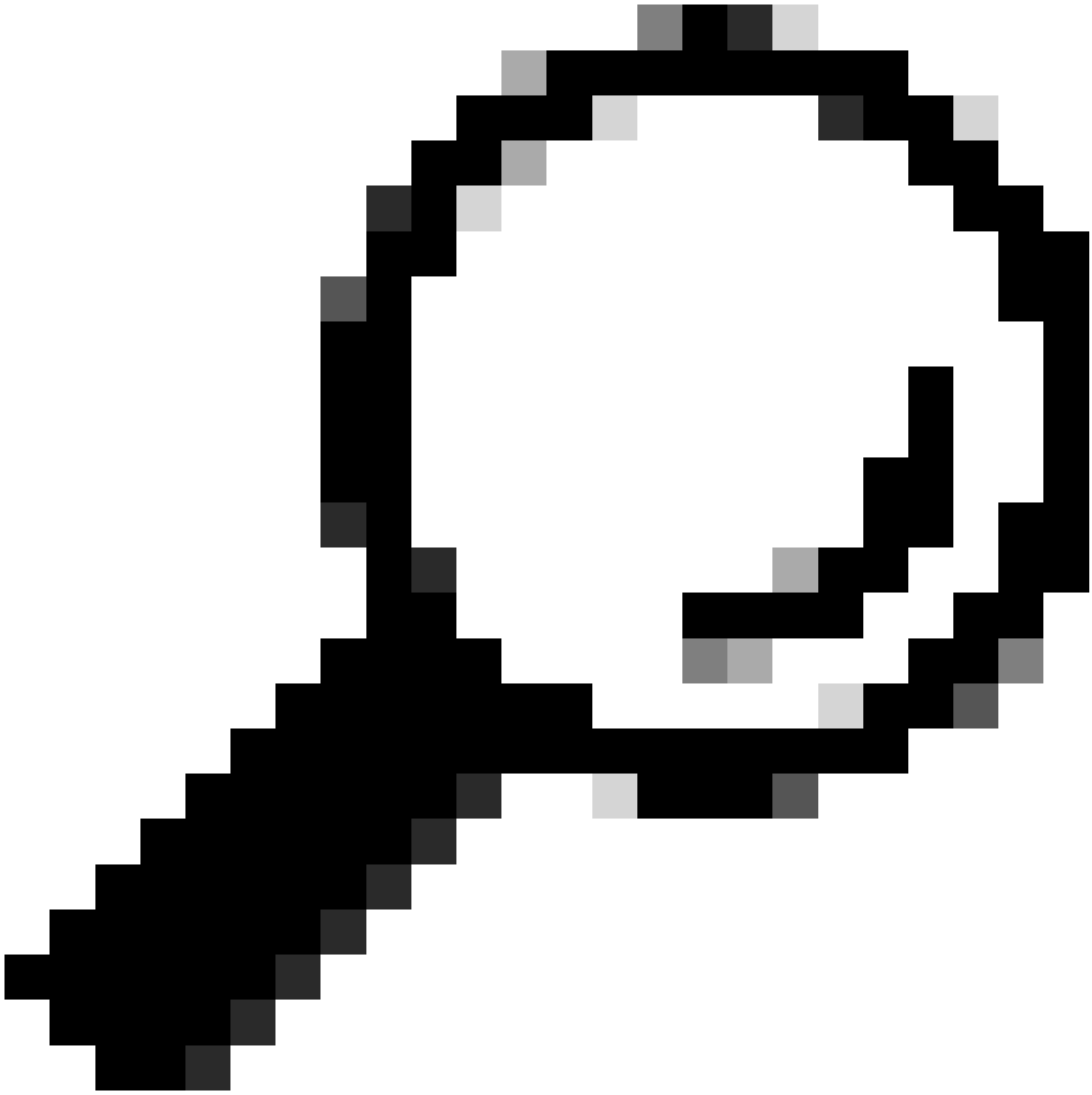
- 신호
- 미디어(음성 또는 비디오)

VoIP 통신은 항상 신호 부분으로 시작하여 통화를 시작한 다음 미디어(음성 또는 비디오)가 스트리밍되고, 마지막으로 신호 처리가 통화를 종료합니다.

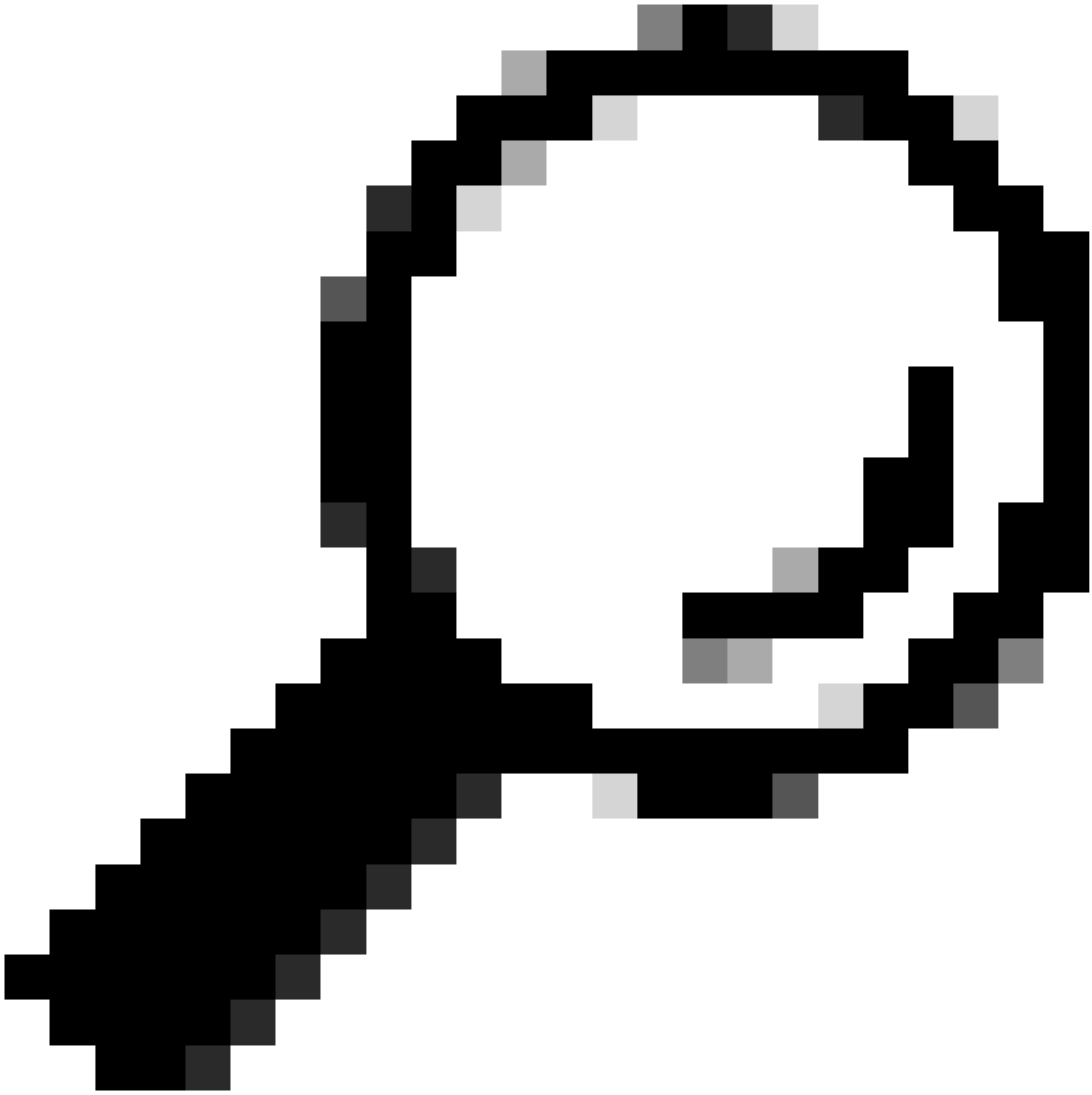


참고: SIP는 가장 널리 사용되는 프로토콜이므로 많은 다이어그램에서 SIP 음성 서버 아이콘으로 일관되게 표시됩니다.





팁: ASA 또는 FTD의 음성 문제를 해결할 때는 사용자의 관점에서 시나리오를 고려해야 합니다. 통화가 설정되었는지 또는 오디오 또는 단방향 오디오가 없는지 확인해야 합니다. 이 정보는 문제가 신호 프로토콜인지 미디어(음성 또는 비디오) 프로토콜인지에 대한 유용한 단서를 제공합니다.



팁: 음성 디바이스는 음성 RTP(Real-time Transport Protocol) 트래픽, 시그널링 트래픽 또는 둘 모두를 동시에 관리할 수 있습니다. 음성 문제를 해결할 때는 다음과 같은 주요 개념을 기억해야 합니다.

++신호 서버: 이러한 서버는 신호 트래픽만 처리합니다.

++미디어 서버: 이러한 서버는 음성 RTP 트래픽을 독점적으로 처리합니다.

++일부 디바이스는 두 작업을 모두 처리할 수 있습니다.

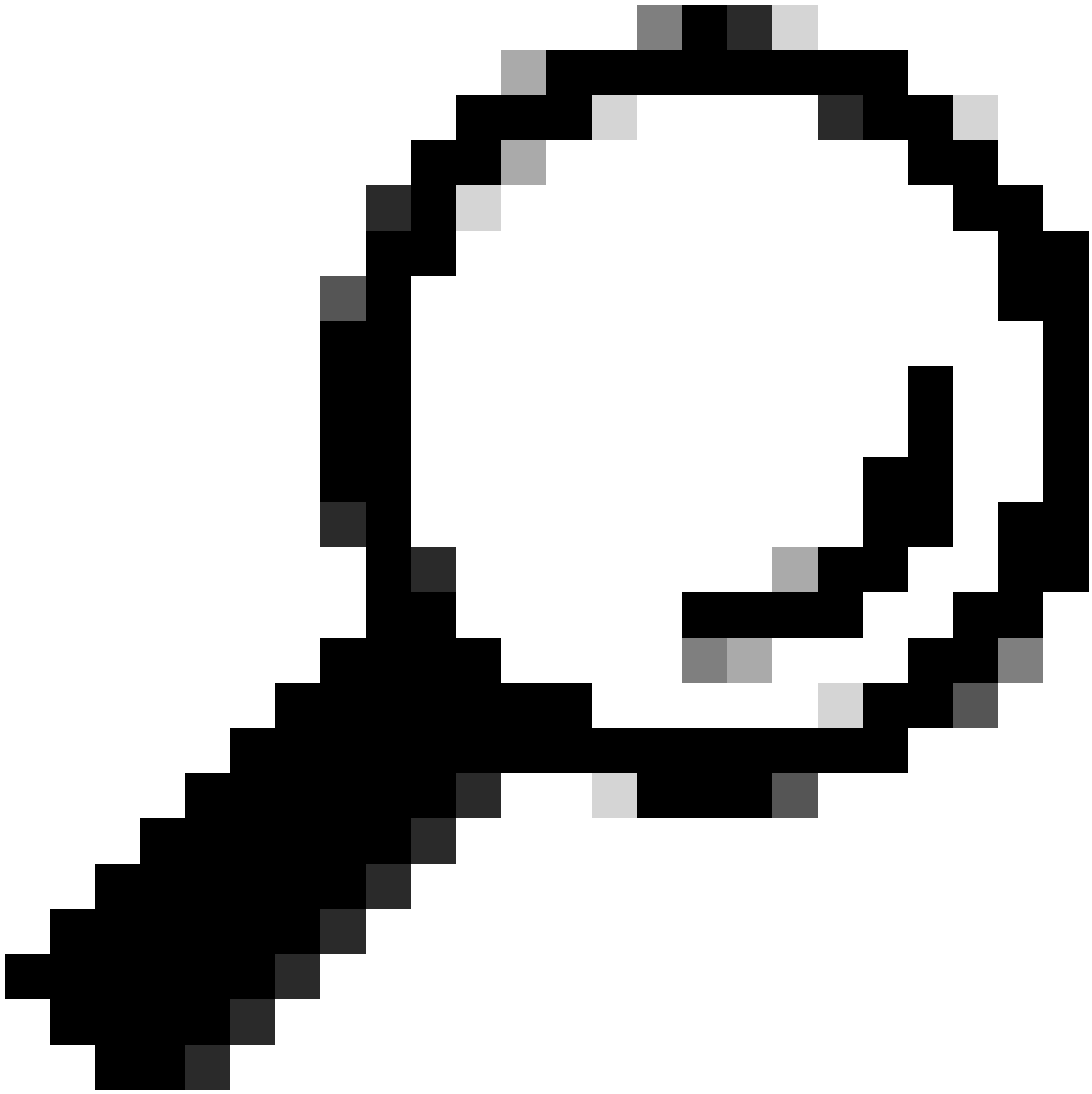
신호

신호 처리 프로토콜은 음성 통신을 시작하는 통화의 일부이지만, 그 뿐만 아니라 다음 기능도 수행합니다.

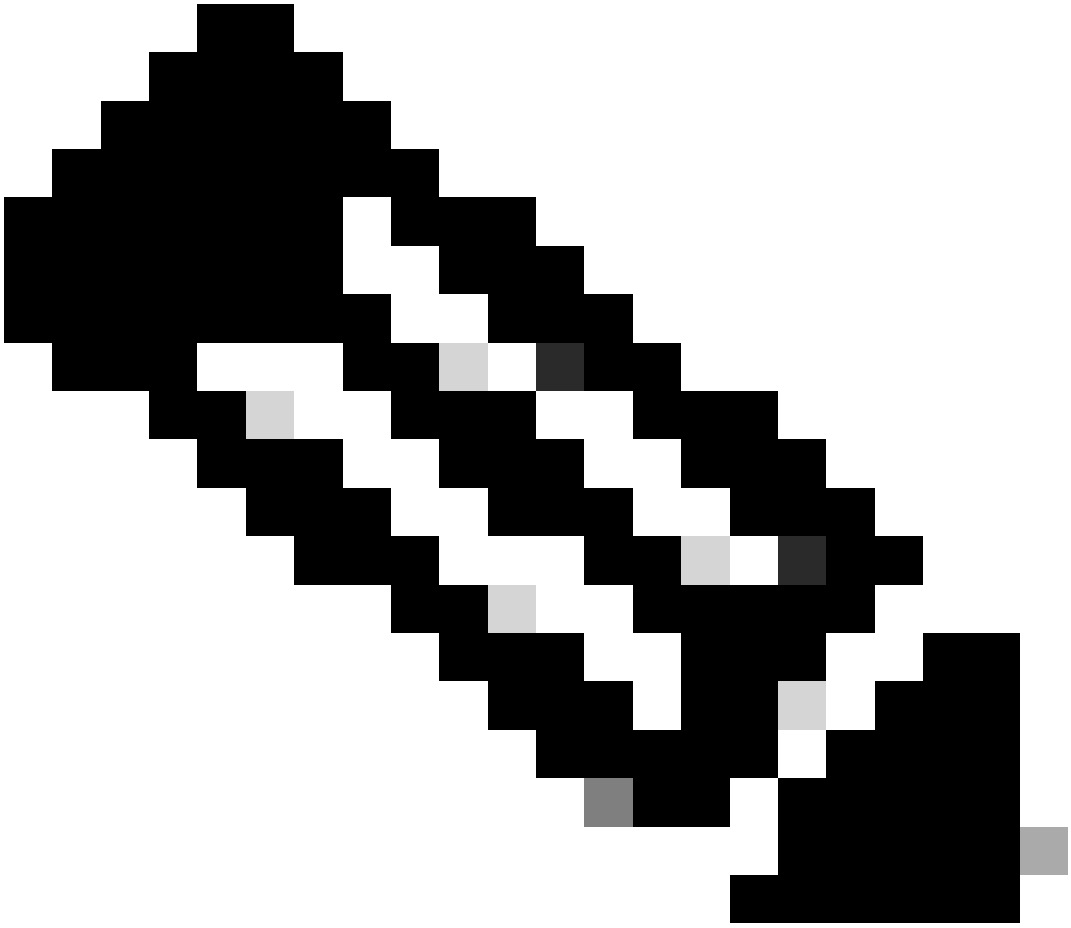
- 커뮤니케이션을 계속 가동합니다.
- 통신을 수정합니다.
- 통신을 종료합니다.

서로 다른 유형의 신호 처리 프로토콜을 사용하면 통화를 설정할 수 있으며, 가장 일반적인 방법은 다음과 같습니다.

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



팁: ASA 또는 FTD에서 패킷 캡처를 위한 적절한 포트를 확인하기 위해 사용 중인 시그널링 프로토콜을 식별해야 합니다. 또한 통화 흐름 및 네트워크 토폴로지를 확보하면 신호 경로를 파악하는 데 유용합니다.

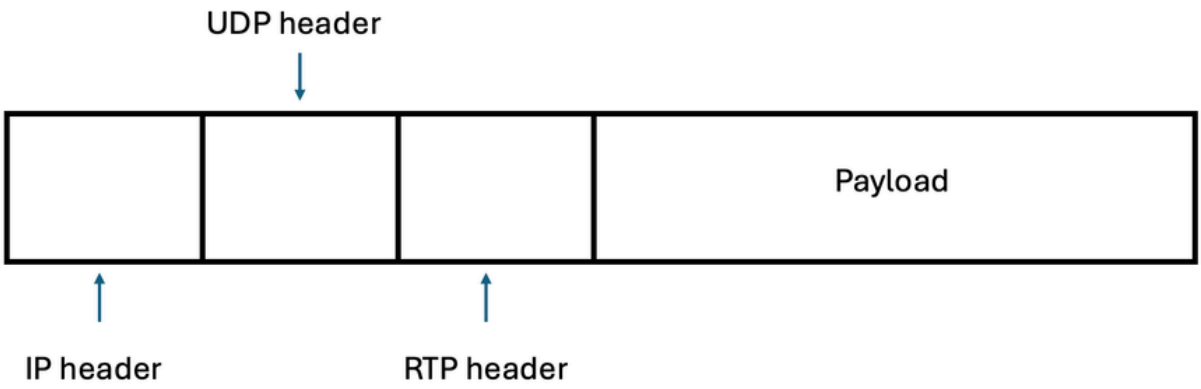


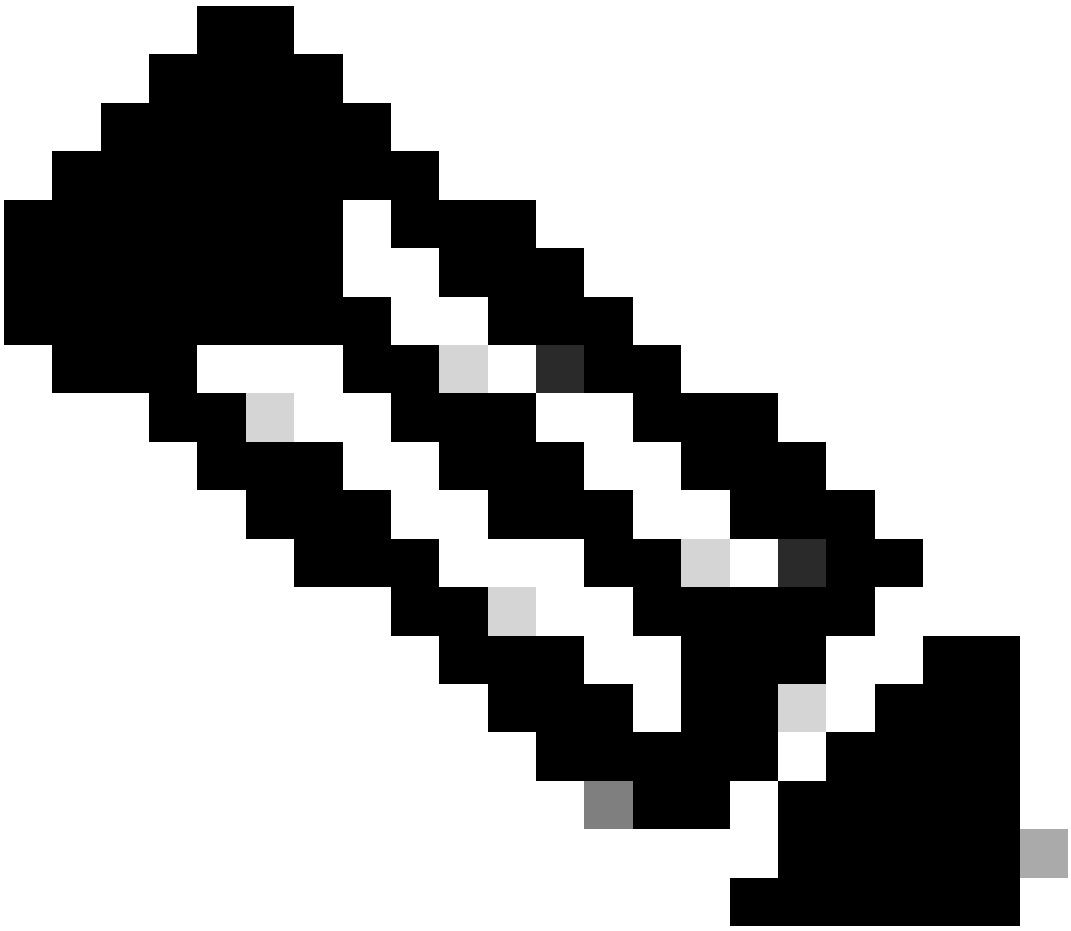
참고: 시그널링 패킷은 소스 및 목적지 IP 주소를 포함하여 RTP 미디어 스트림 전송 및 수신에 관여하는 당사자를 식별하는 데 도움이 됩니다.

미디어

신호 처리가 완료되고 신호 구성 요소(장치 또는 서버)가 미디어 유형에 동의하면 RTP(Real Time Protocol)가 재생되어 미디어(오디오 및/또는 비디오)를 관련된 모든 당사자에게 전송하기 시작합니다.

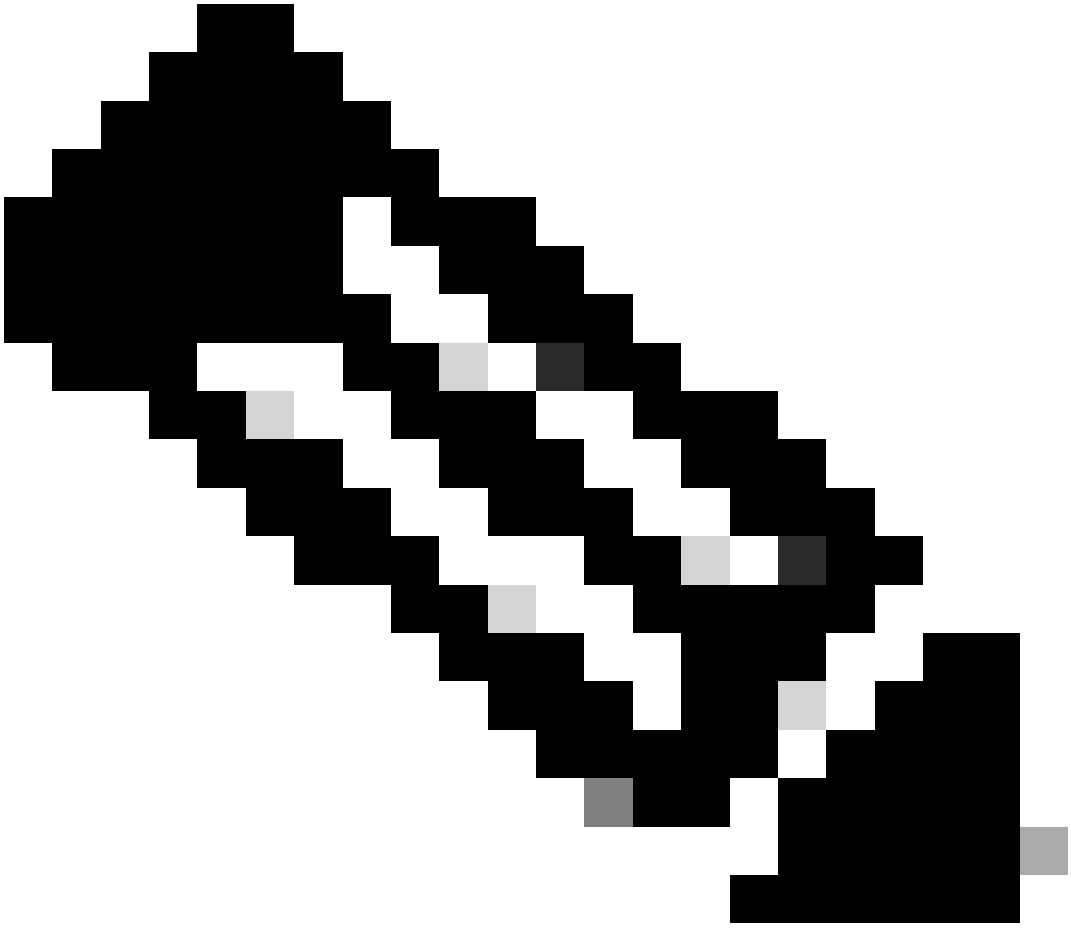
RTP는 통화가 설정된 후에만 전송되는 스트리밍 미디어에 사용되는 인터넷 프로토콜이며 UDP(User Datagram Protocol)를 통해 실행됩니다.



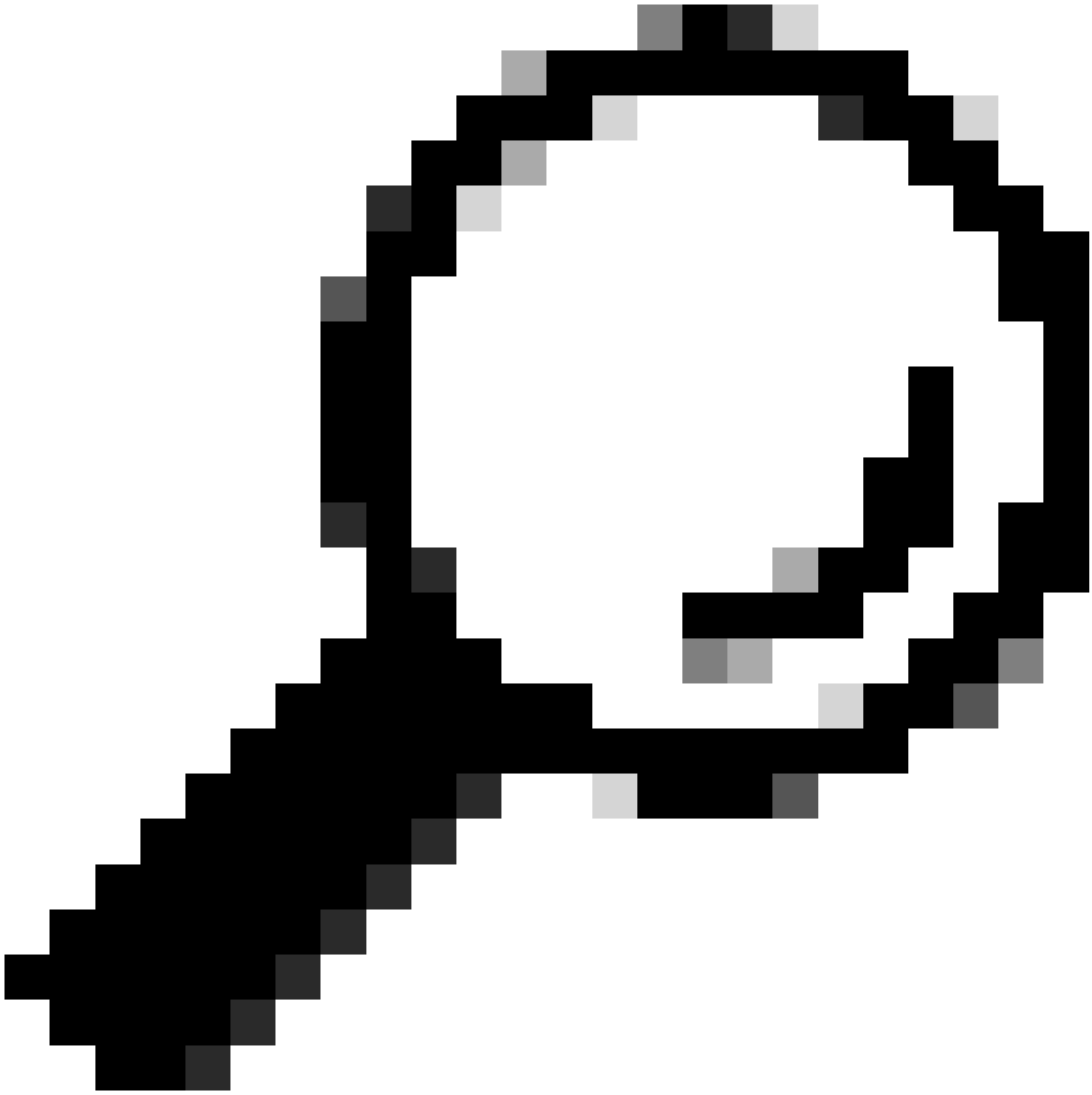


참고: 미디어는 음성 및/또는 비디오일 수 있으며 RTP 패킷 상에서 이동할 수 있습니다.

신호 구성 요소(장치 또는 서버)는 미디어(오디오 및/또는 비디오)를 보내거나 받는 데 사용되는 포트를 결정합니다. RTP의 가장 일반적인 포트 범위는 일반적으로 대부분의 디바이스에서 16384~32767 사이입니다.



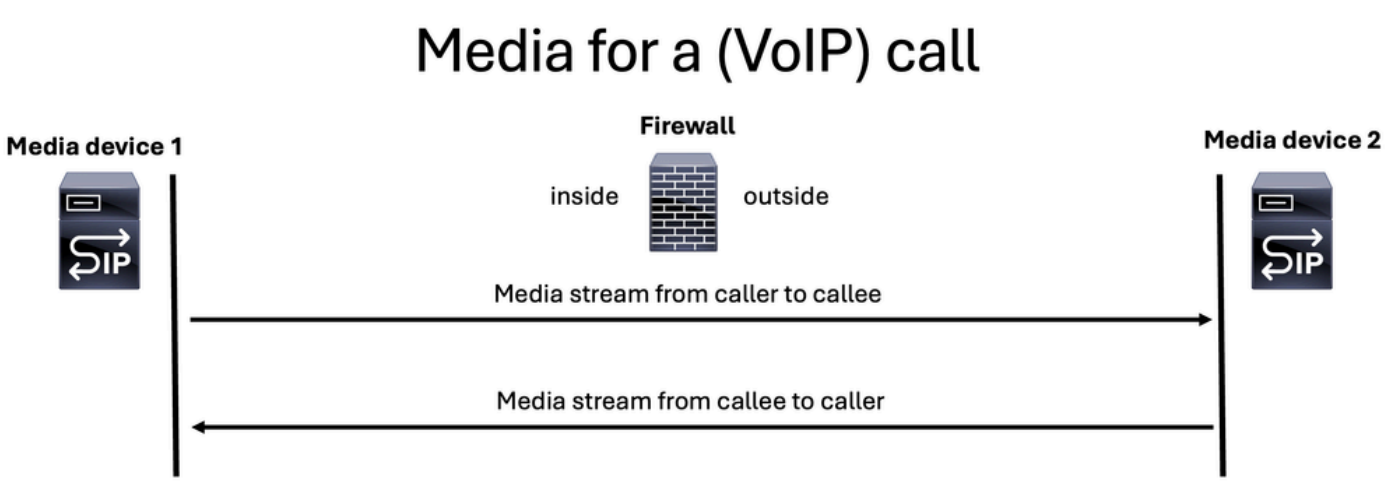
참고: ISR4K 플랫폼과 같은 ASR 및 ISR G3 플랫폼과 같은 특정 Cisco 장치는 표준화된 RTP 포트 범위 8000~48200을 사용합니다. 장치에 구성된 특정 RTP 포트 범위는 이러한 표준화된 값과 다를 수 있으며 서드파티 장치에 따라 다를 수 있으므로 이를 확인하는 것이 중요합니다.

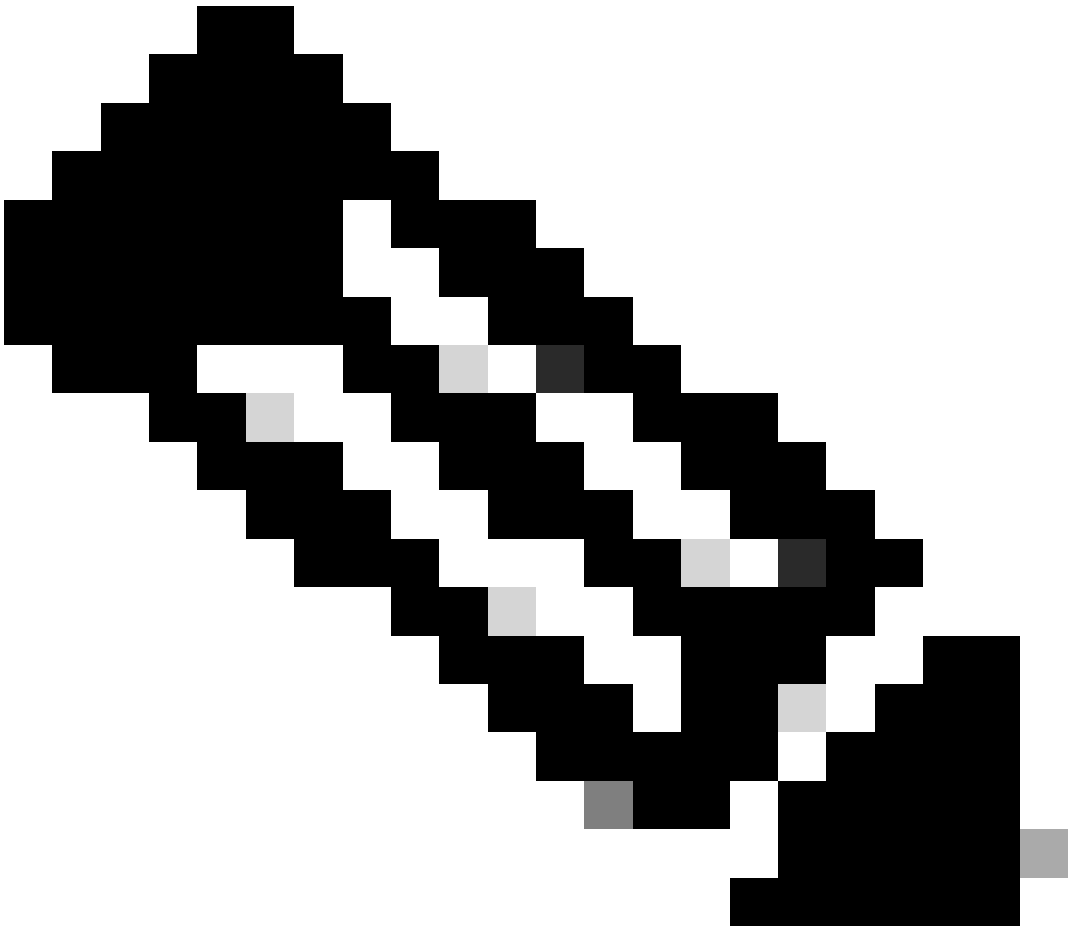


팁: RTP 경로가 신호 처리 경로와 다른 경우도 있으므로 음성 RTP 패킷을 보내고 받는 장치를 식별하는 것이 중요합니다. 이렇게 하면 ASA 또는 FTD를 통과하는 디바이스 간 UDP 트래픽을 캡처할 수 있습니다.

일반적인 음성 통화에서 생성되는 두 개의 미디어 스트림 또는 RTP 스트림이 있습니다.

1. 발신자에서 발신자로의 미디어 스트림 1개
2. 발신자에서 발신자로의 미디어 스트림 1개





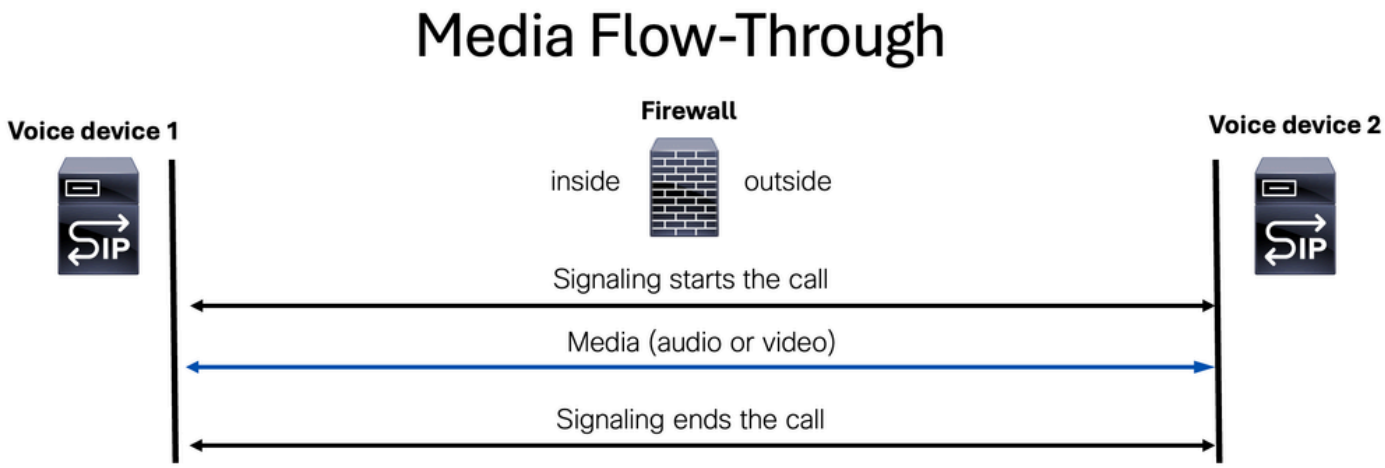
참고: 설명을 위해 SIP 서버 아이콘은 모든 이미지의 신호 서버 또는 미디어 서버를 나타내는 데 사용됩니다.

음성 통화에서 미디어 스트리밍에 대해 설명할 때 두 가지 주요 시나리오를 강조하는 것이 중요합니다.

1. Media Flow-Through
2. 미디어 흐름 중심

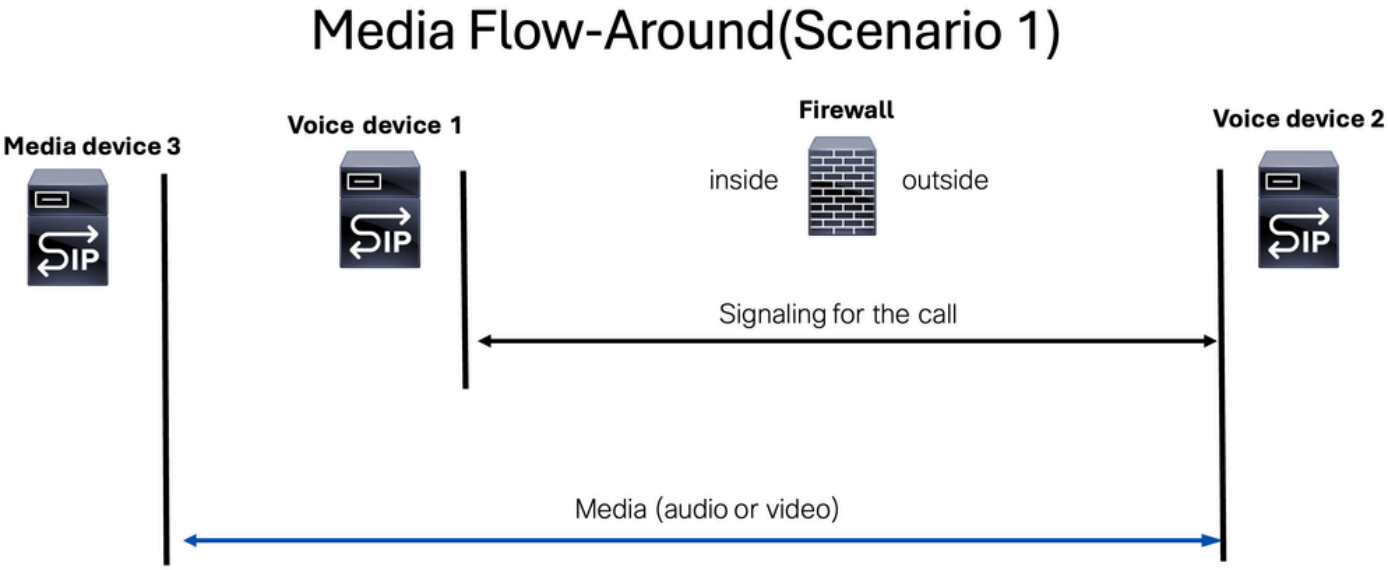
Media Flow-Through

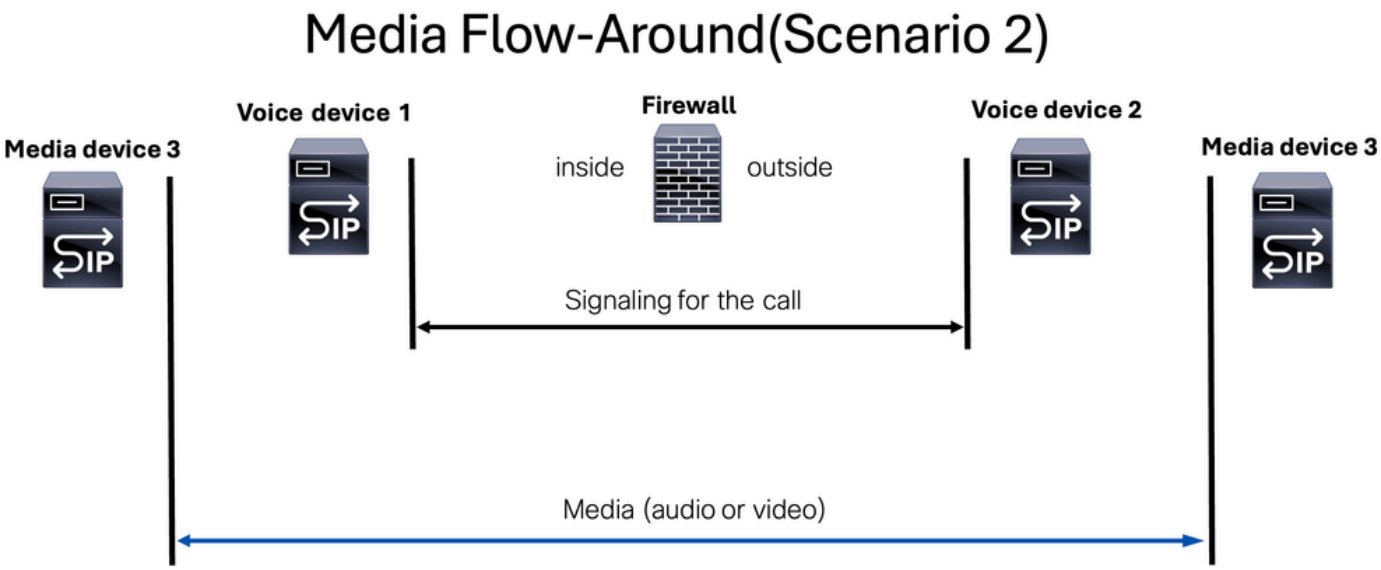
Media flow-through는 미디어(음성 및/또는 비디오)와 시그널링 패킷이 모두 동일한 디바이스에서 처리되는 모드입니다.



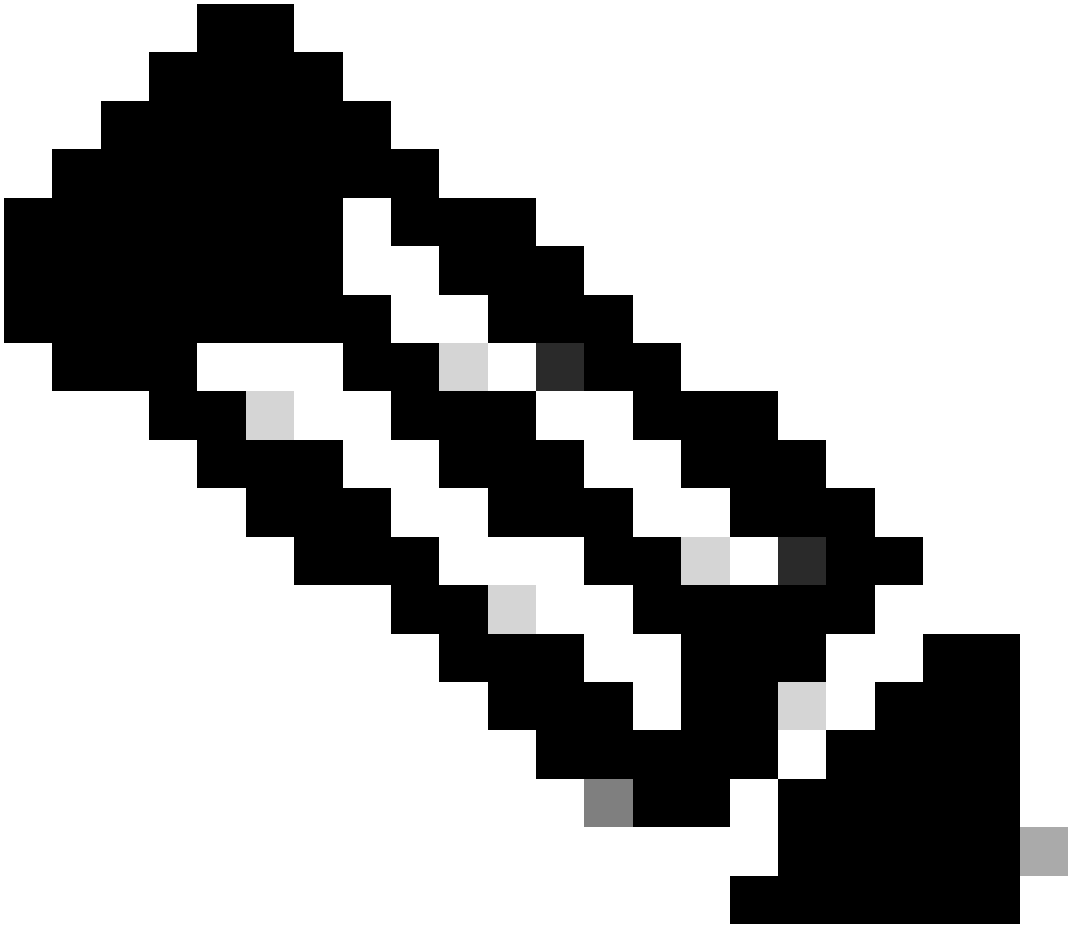
미디어 흐름 중심

미디어 스트림 플로우 어라운드(flow-around)는 시그널링 패킷이 두 개의 개별 시그널링 구성 요소(장치 또는 서버)에 의해 처리되는 모드이며, 미디어 스트림(음성 또는 비디오)은 미디어 장치라고 하는 세 번째 장치에 의해 관리됩니다.





이 모드는 관련된 장치의 역할 및 신호 처리와 미디어 스트림 또는 장치의 구별을 명확히 합니다.



참고: 생성된 액세스 목록을 트러블슈팅할 때 특히 중요한 사항으로서 시그널링 구성 요소(장치 또는 서버)를 허용할 수 있지만, 미디어 스트림이 다른 미디어 장치를 사용 중인 경우에는 FW 장치의 액세스 목록에서도 허용해야 합니다.

SIP(Session Initiation Protocol)

SIP는 RFC 3261의 IETF(Internet Engineering Task Force)에서 정의한 애플리케이션 레이어 제어 프로토콜입니다.

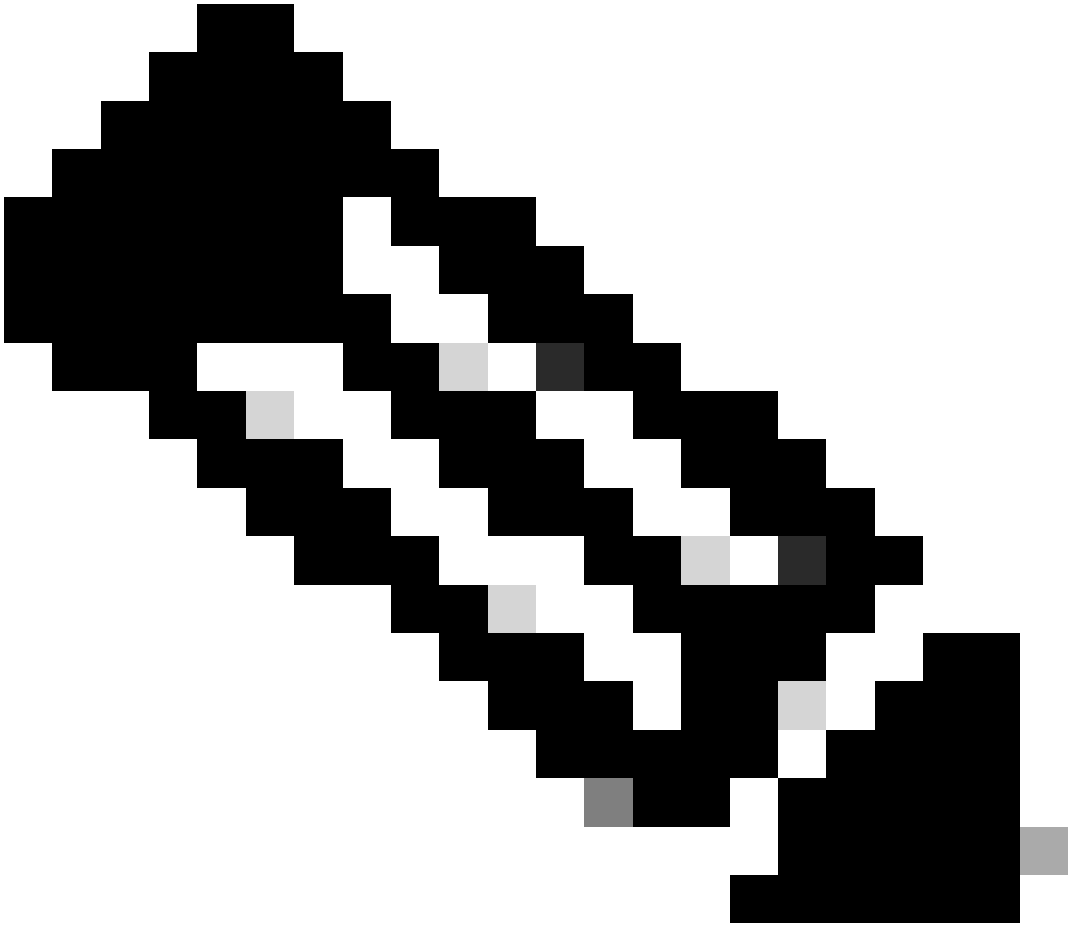
SIP는 텍스트 기반 프로토콜입니다. 즉, SIP 메시지는 HTTP 작동 방식과 유사하게 사람이 읽을 수 있는 텍스트로 구성됩니다.

SIP는 패킷 텔레포니 네트워크 내의 시그널링 및 세션 관리 기능을 처리하도록 설계되었습니다.

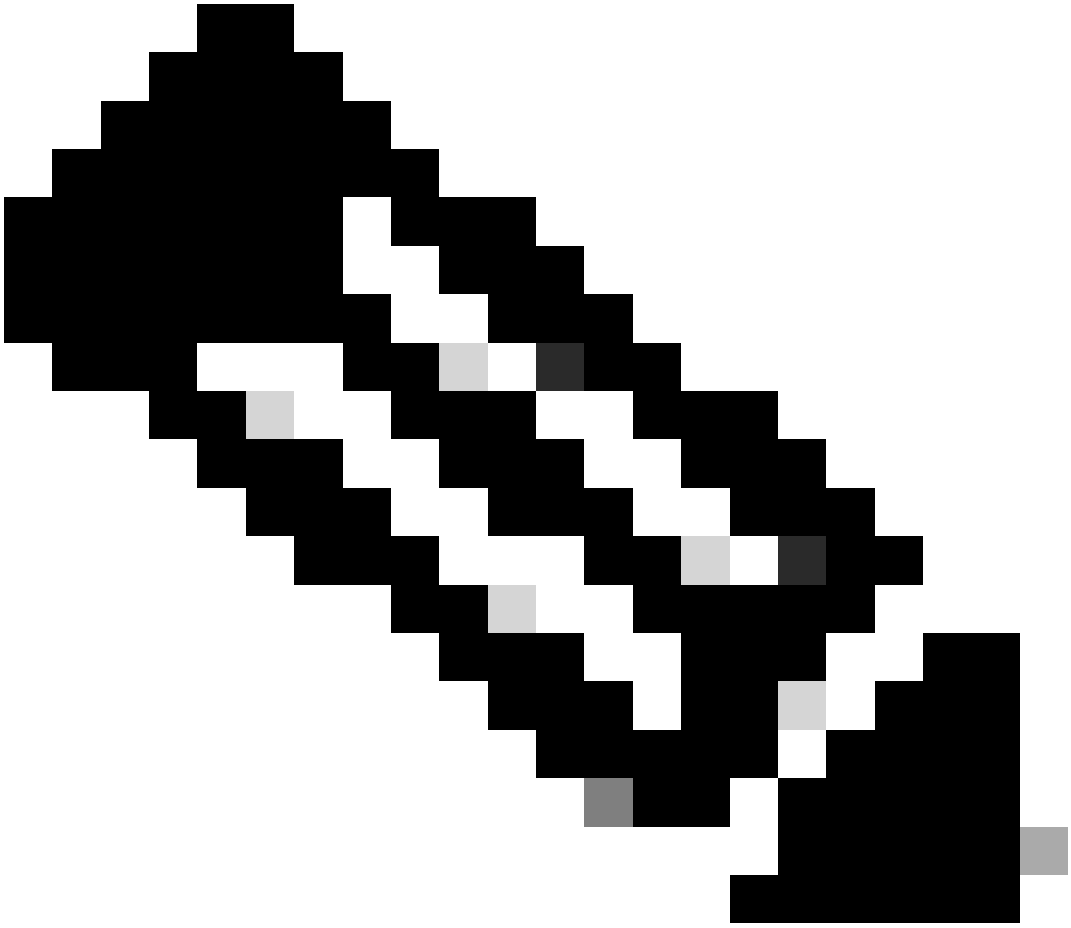
SIP는 다음을 수행할 수 있습니다.

- 통화 생성
- 통화 수정
- 통화 종료

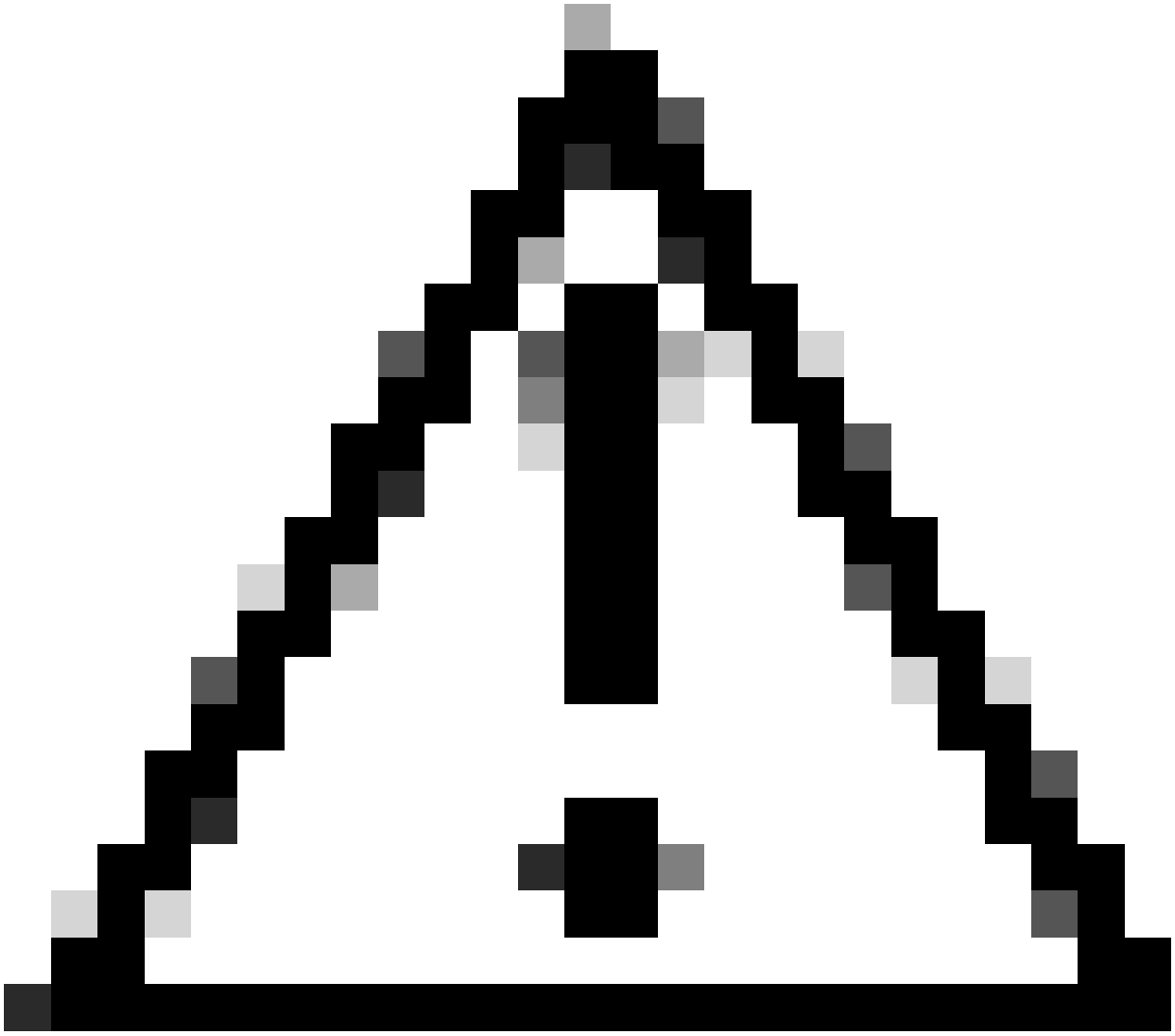
SIP는 표준화된 포트 5060에서 UDP 또는 TCP를 사용할 수 있습니다. 또한 SIP가 TLS(Transport Layer Security)를 사용하여 암호화된 경우 표준화된 포트 5061을 사용할 수 있습니다.



참고: SIP 시그널링이 암호화되면 ASA 또는 FTD 디바이스의 패킷 캡처에 실제 SIP 패킷이 표시되지 않습니다. 그러나 SIP 클라이언트와 SIP 서버 디바이스 간의 TLS 핸드셰이크 다음에 오는 TCP 핸드셰이크를 계속 관찰할 수 있습니다.



참고: SIP 검사는 Cisco FTD(Secure Firewall Threat Defense) 및 ASA(Secure Firewall Adaptive Security Appliance)에서 기본적으로 활성화됩니다.



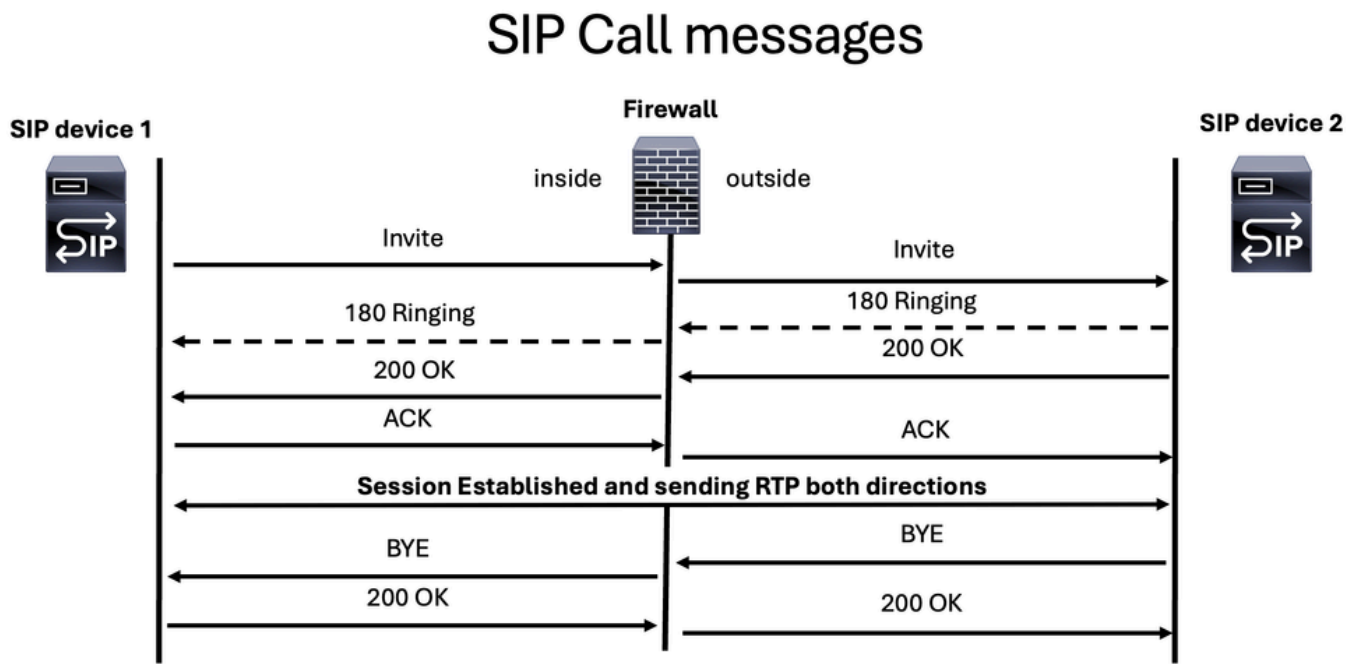
주의: 항상 신호에 사용되는 포트를 확인합니다. SIP 프로토콜은 일반적으로 포트 5060 또는 5061을 사용하지만, 일부 구축에서는 이러한 표준을 벗어나 SIP 프로토콜에 서로 다른 포트를 사용할 수 있습니다.

SIP 신호 처리 문제를 해결할 때 다음과 같은 세 가지 시나리오를 확인할 수 있습니다.

- SIP 통화 신호 메시지
- SIP 옵션 메시지
- SIP 등록 메시지

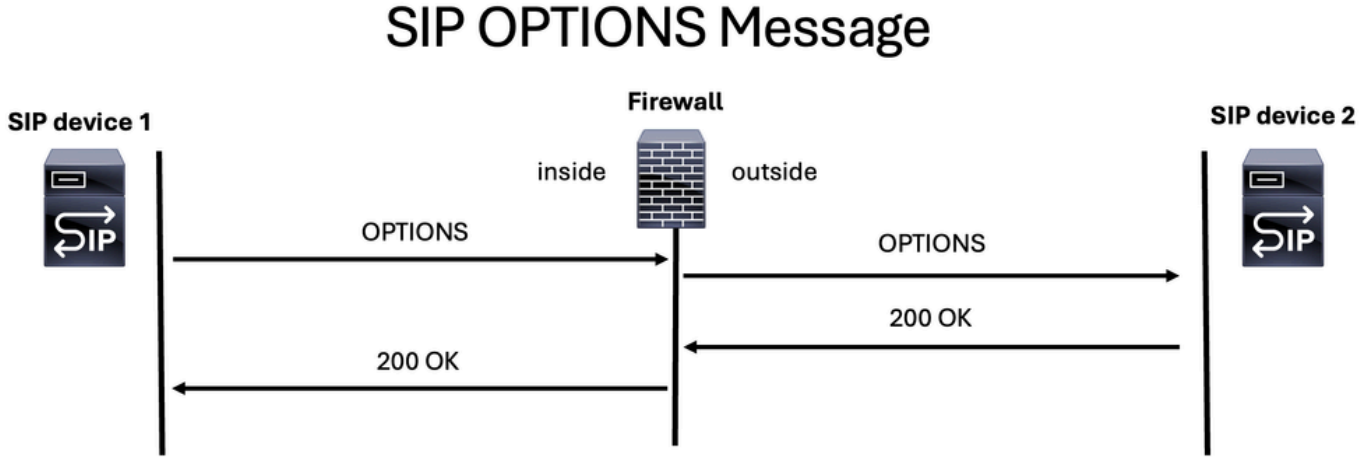
SIP 통화 메시지

음성 통화를 설정하고 종료하기 위한 기본 SIP 메시지는 다음과 같습니다.



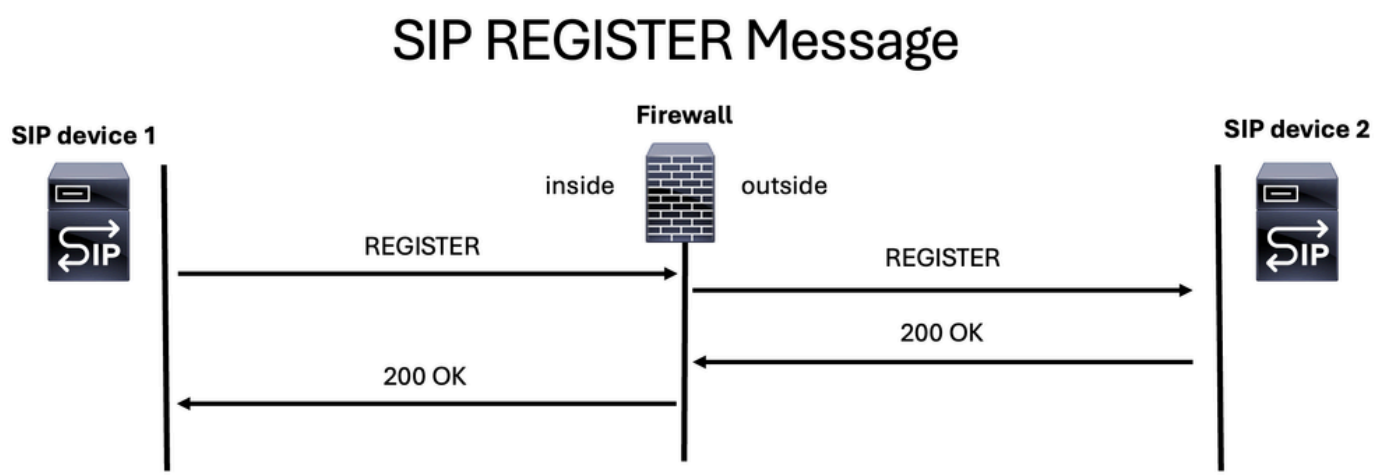
SIP 옵션 메시지

SIP OPTIONS 메시지는 SIP 장치가 온라인 상태이고 응답할 수 있는지 여부를 확인하는 데 중요합니다. 이는 ICMP 메시지를 ping하는 것과 같지만 SIP 세상입니다.

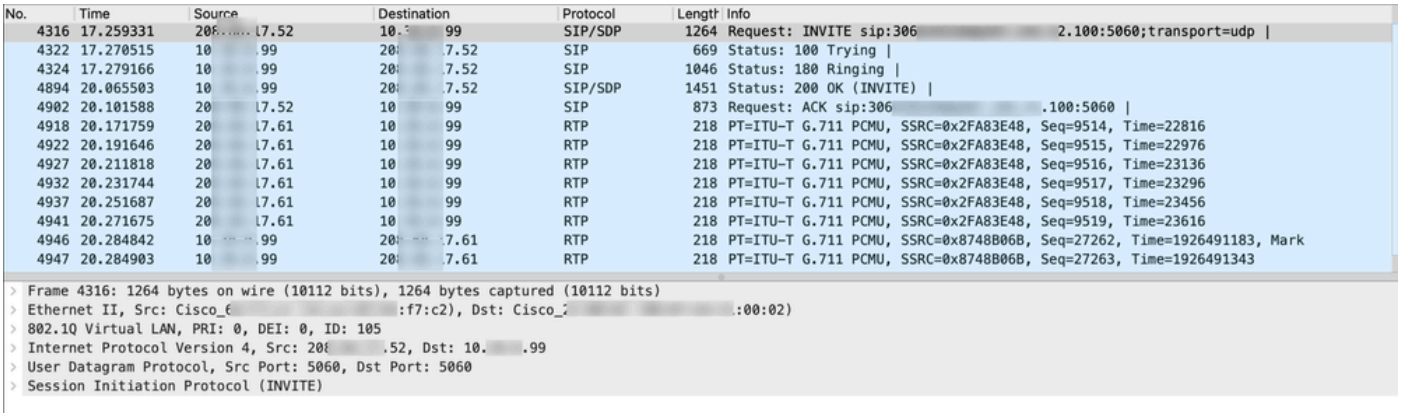


SIP 등록 메시지

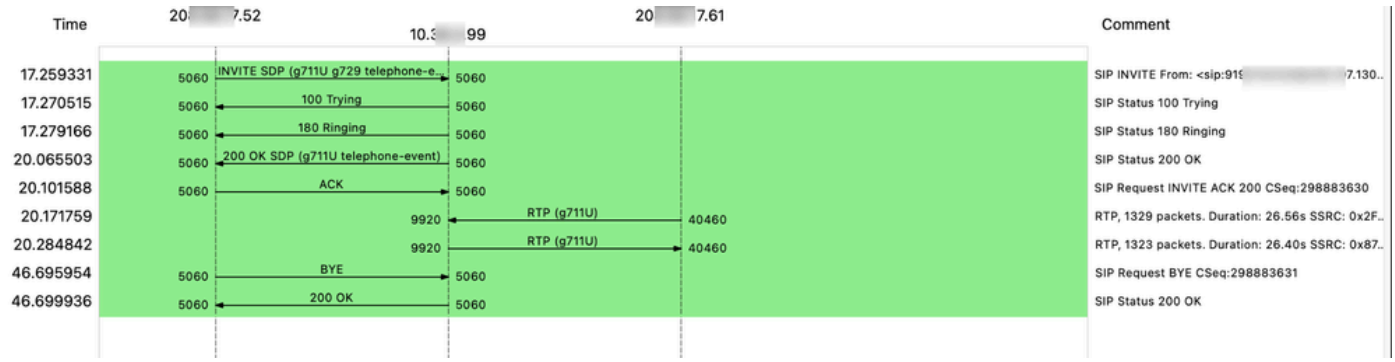
방화벽 트러블슈팅 세션 중에 찾을 수 있는 또 다른 SIP 메시지는 SIP REGISTER 메시지로, 디바이스를 SIP 서버에 등록할 수 있습니다.



이 패킷 캡처는 2개의 SIP 디바이스 및 미디어(음성) 트래픽의 요청과 응답을 보여줍니다.

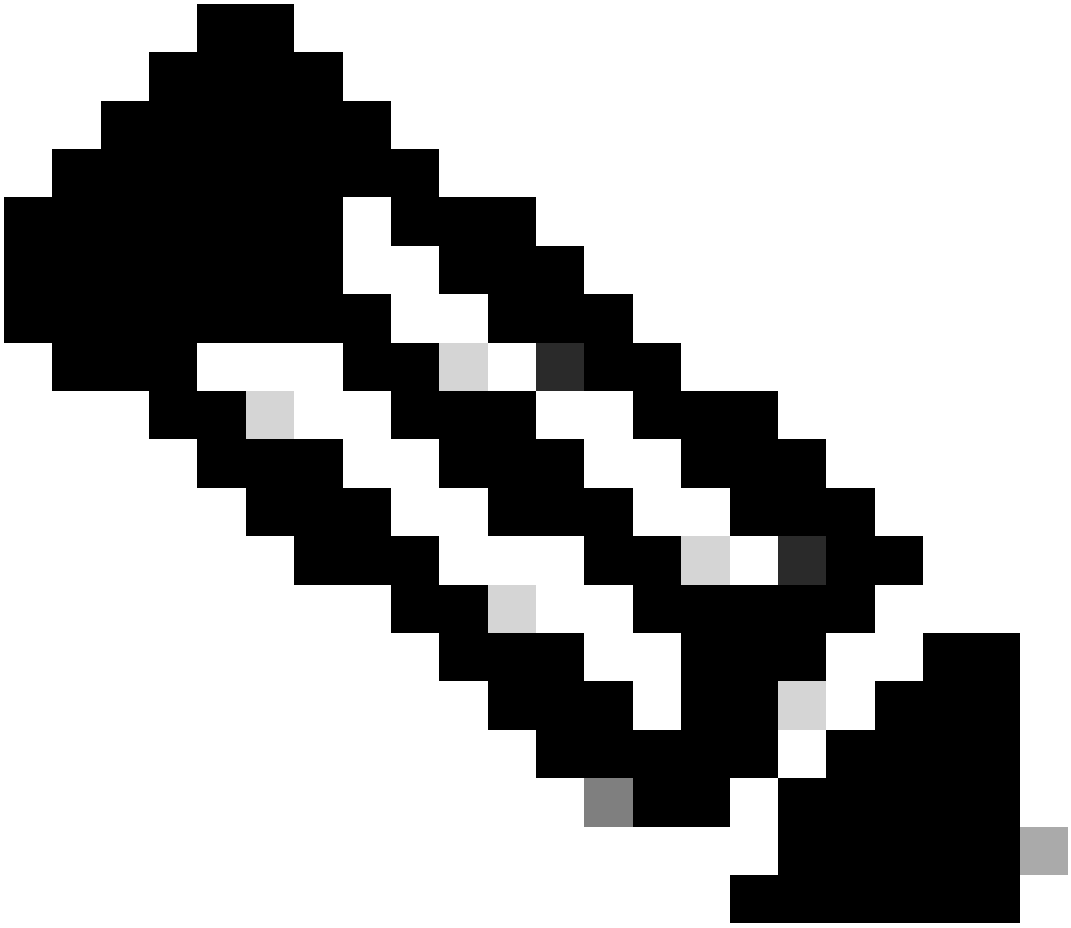


다음은 SIP 시그널링 및 RTP 미디어(음성) 플로우의 예입니다.



SDP(Session Description Protocol)

SDP(Session Description Protocol)는 멀티미디어 세션에 대한 미디어 스트림을 설명하는 데 사용되는 표준 표현입니다. 미디어 자체는 전달하지 않지만 엔드포인트 간에 미디어 유형 및 형식을 협상하는 데 사용됩니다. SDP는 SIP(Session Initiation Protocol)와 함께 사용되어 세션의 미디어 특성을 관리하고 협상합니다.

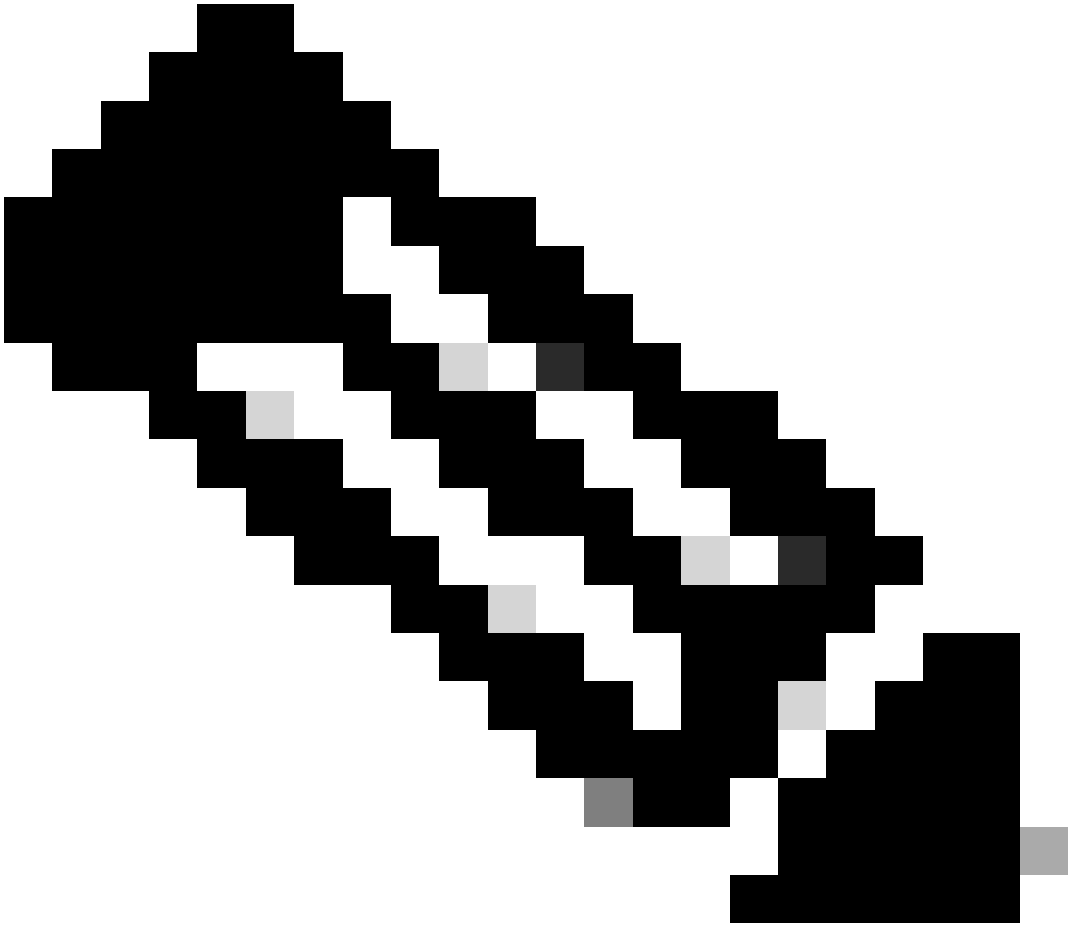


참고: MGCP는 동일한 목적으로 활용되는 SDP의 개념을 통합하고 있다.

다음은 SIP 프로토콜 내의 SDP 메시지의 예입니다.

```
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
```



참고: SDP 메시지 중 일부에는 이 예에서 다음 매개변수가 포함됩니다.

++c-IN IP4: 미디어 서버의 IP 주소

++m=오디오: 미디어 유형이 오디오임을 나타냅니다.

++8266: 오디오 스트림이 전송되는 포트 번호입니다.

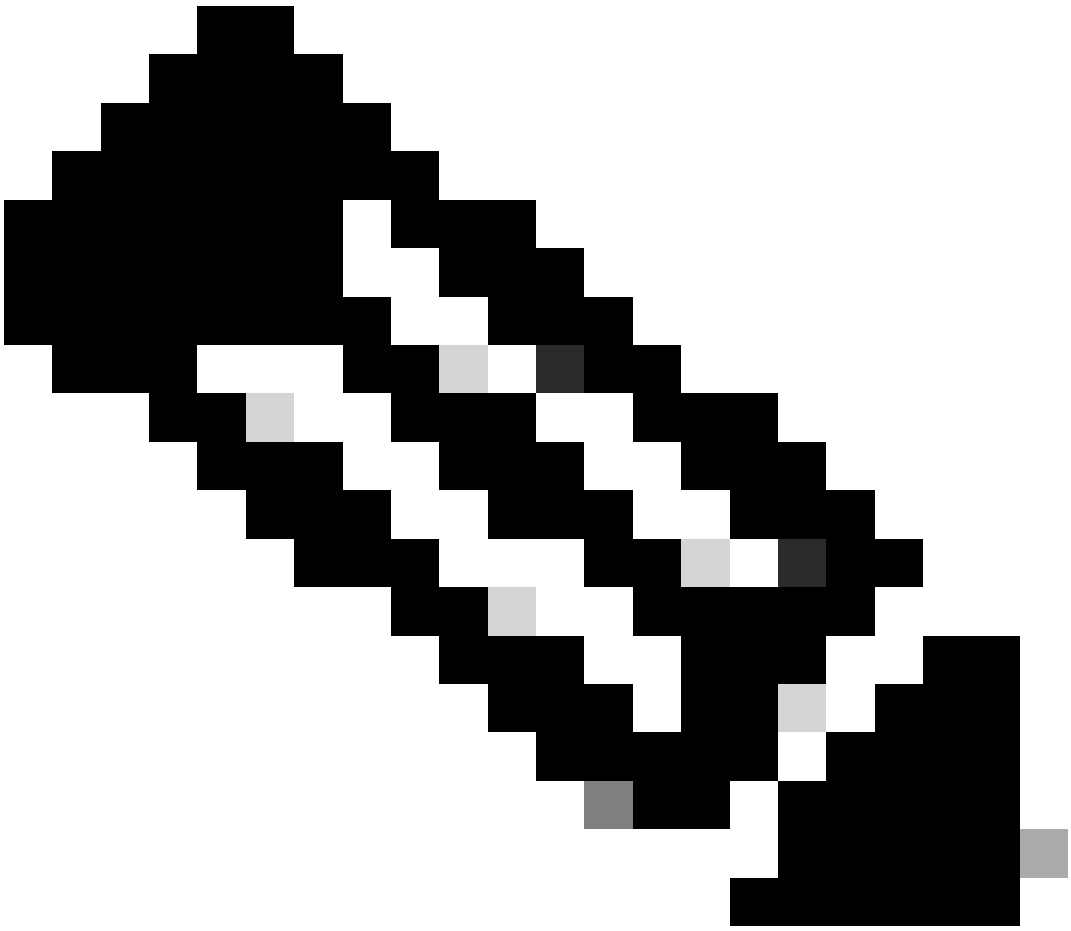
++RTP/AVP: 이는 AVP(Audio/Video Profile)를 사용하는 RTP인 전송 프로토콜을 지정합니다.

++18 127: 오디오 코덱의 페이로드 유형입니다. 페이로드 유형 18은 일반적으로 G.729 코덱에 해당하며, 127은 엔드포인트 간의 협상에 따라 코덱에 할당할 수 있는 동적 페이로드 유형입니다.

SDP(Session Description Protocol)는 다음과 같은 여러 SIP 메시지에서 찾을 수 있습니다. INVITE, 183 Session in Progress, 200 OK, ACK 등이 있습니다. SDP는 당사자 간에 음성 및/또는 비디오 기능을 교환하는 응답 방법 역할을 합니다. 통화 문제를 해결할 때 세 가지 주요 개념을 이해하는 것이

중요합니다.

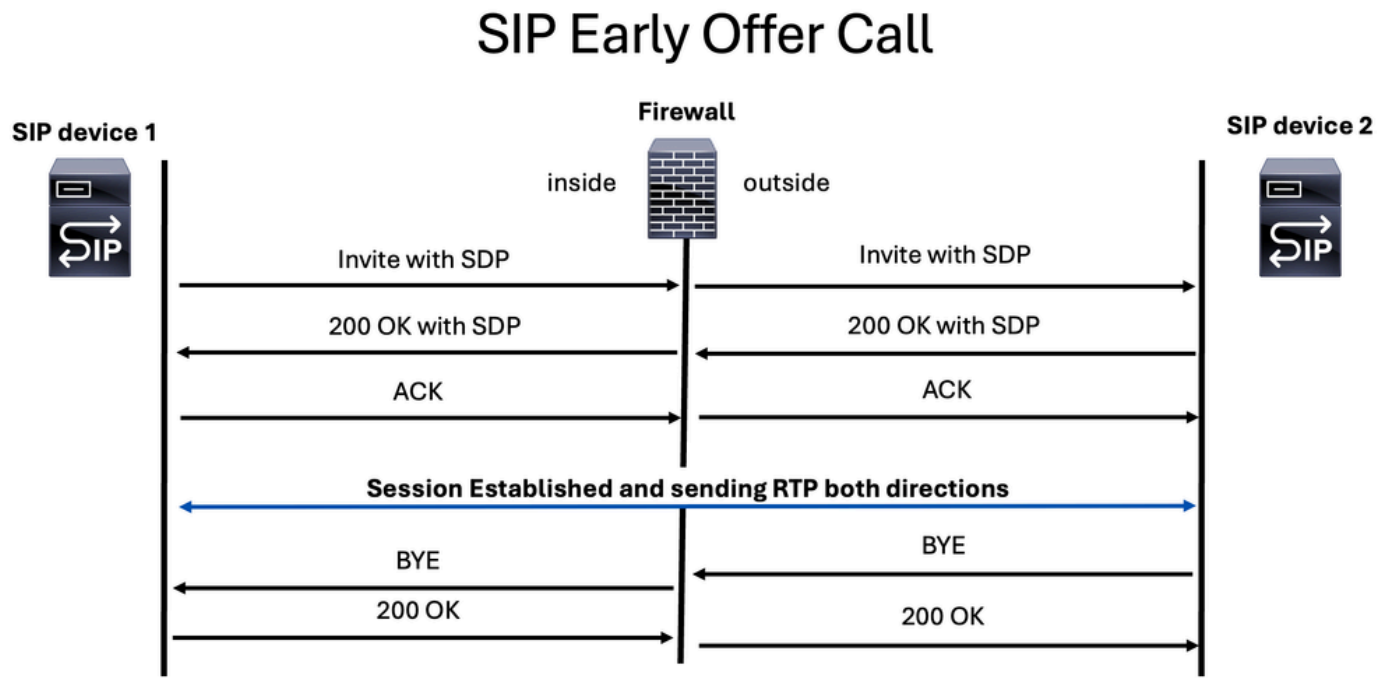
1. 조기 제안
2. 제안 연기
3. 초기 미디어



> 참고: 방화벽의 검사 기능은 SIP 헤더 내뿐만 아니라 SDP 섹션에서 IP 주소를 수정할 수 있으므로 SDP 메시지의 대상을 이해하는 것이 중요합니다.

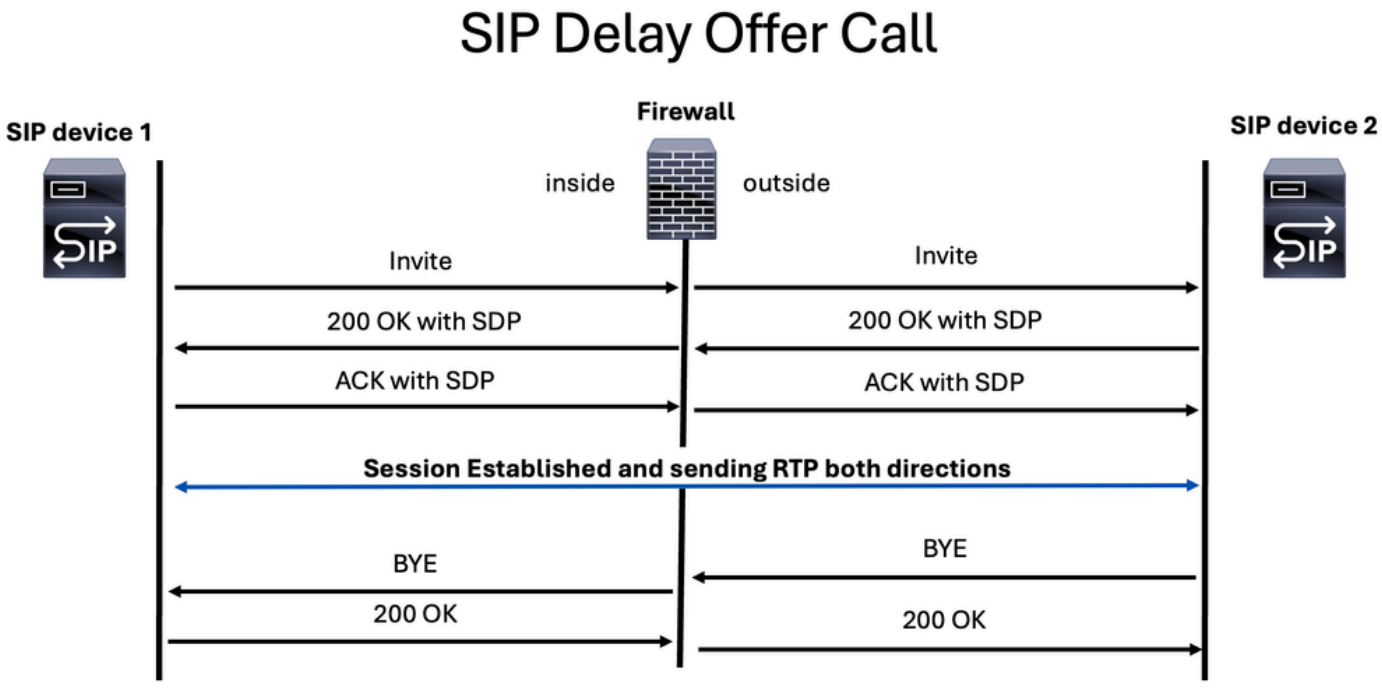
조기 제안

여기서 SDP의 미디어 매개변수는 INVITE 및 200 OK SIP 메시지에 있습니다.



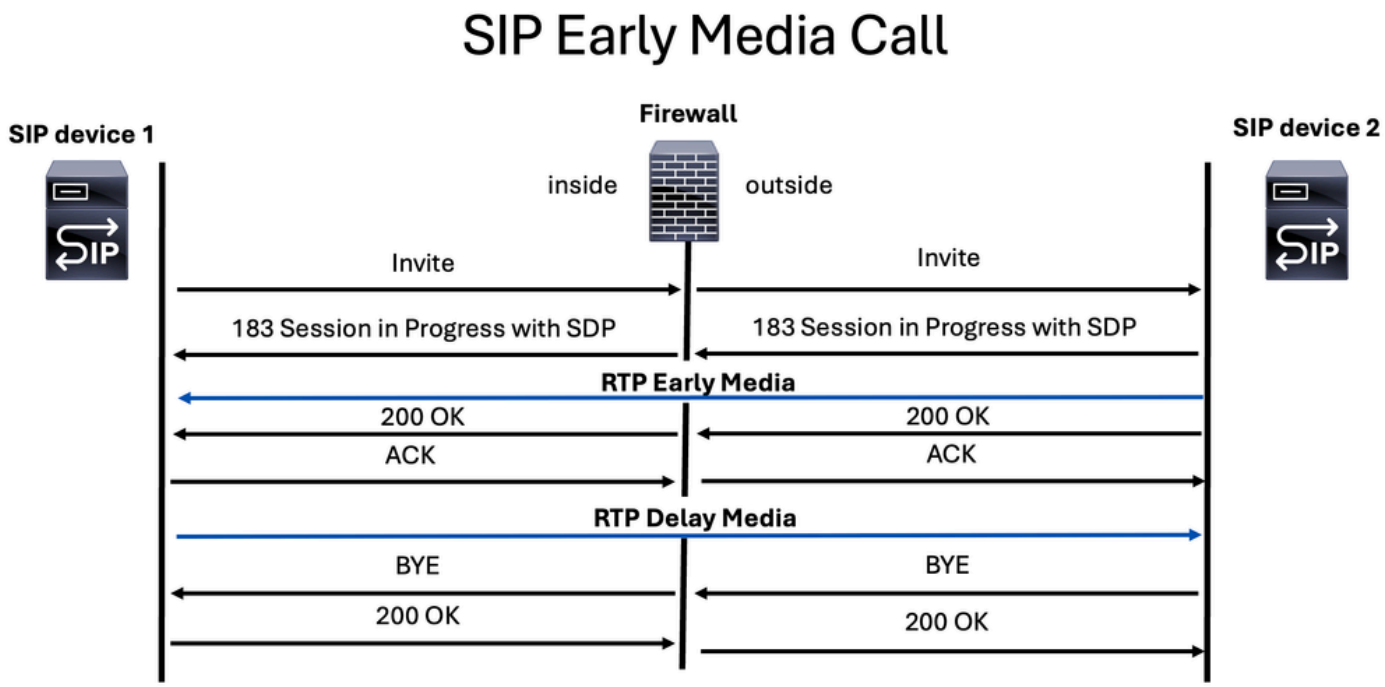
제안 연기

이 방법에서 SDP는 200 OK 및 ACK SIP 메시지에 있습니다.



초기 미디어

초기 미디어는 183 Session Progress 응답이라고 하는 특정 SIP 메시지를 통해 전송됩니다. 이 메시지에는 수신자에 대한 미디어 매개 변수를 포함하는 SDP(Session Description Protocol)가 포함되어 있습니다. 일반적으로 통신사 및 SIP 공급자는 통화가 공식적으로 연결되기 전에 발신자에게 자동 음성 메시지 또는 기타 미디어를 보내는 데 사용합니다.

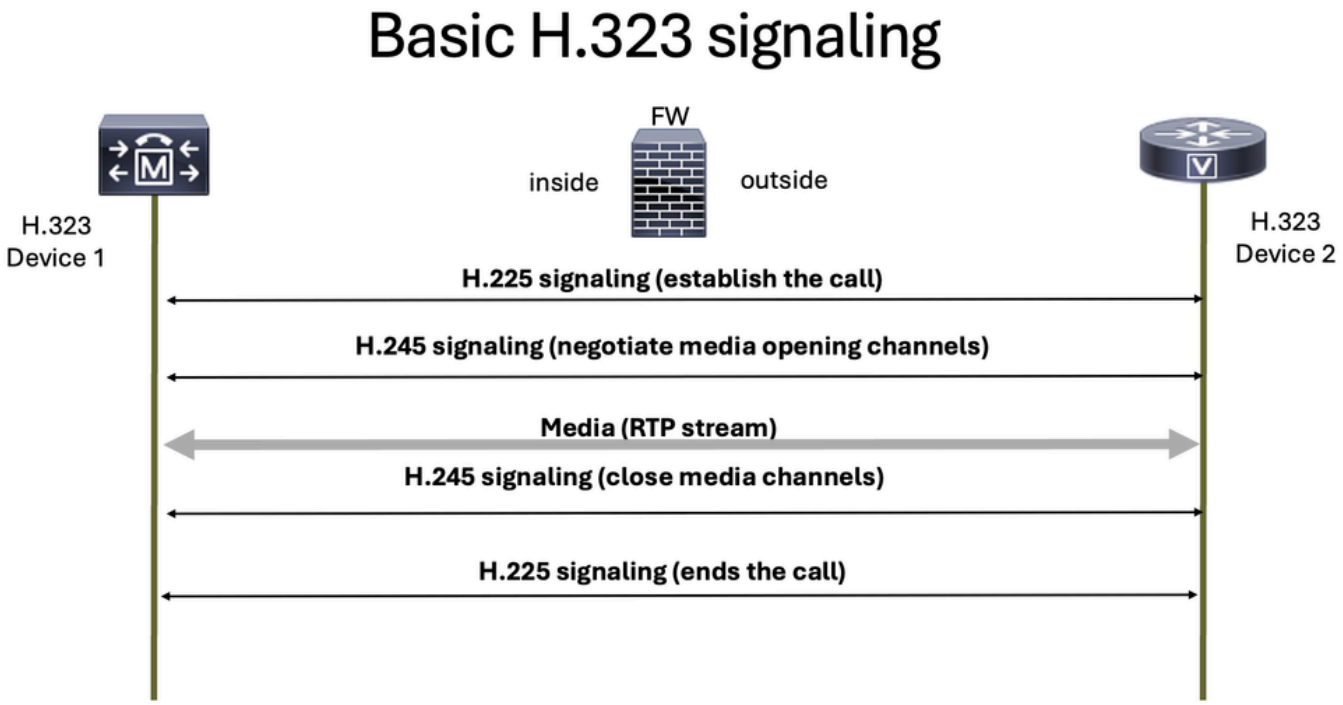


H.323

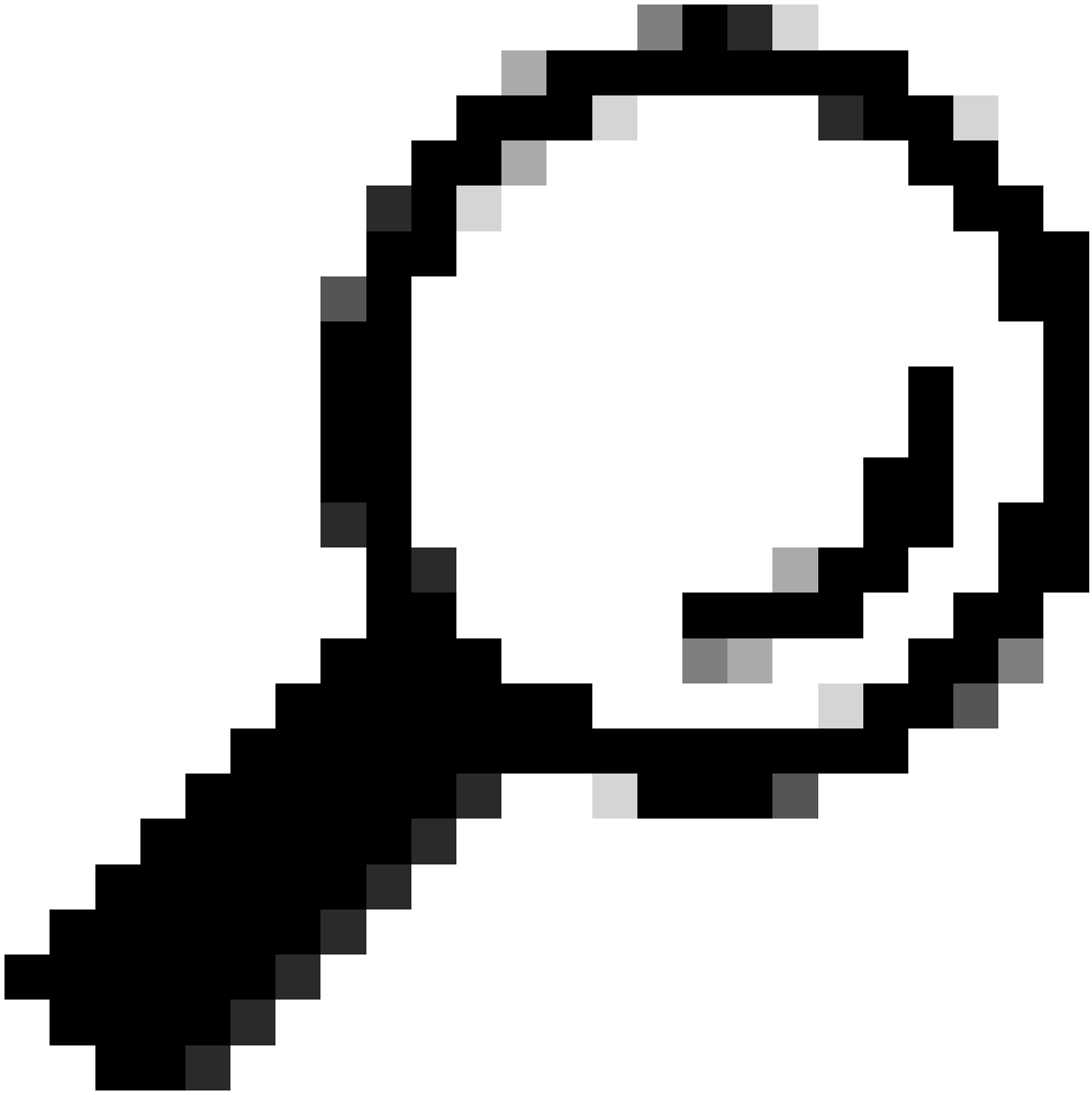
H.323은 인터넷과 같은 패킷 교환 네트워크를 통한 음성, 비디오 및 데이터 통신을 위해 ITU(International Telecommunication Union)에서 정의한 프로토콜 집합입니다.

H.323 프로토콜은 두 가지 주요 구성 요소로 구성됩니다.

1. H.225 이는 통화 설정 및 종료를 비롯한 통화 신호 처리를 처리합니다.
2. H.245 이는 기능 교환 및 오디오 및 비디오 채널 개폐를 담당합니다.



H.323 신호 처리 프로토콜에서 사용되는 포트는 1718, 1719 및 1720입니다.

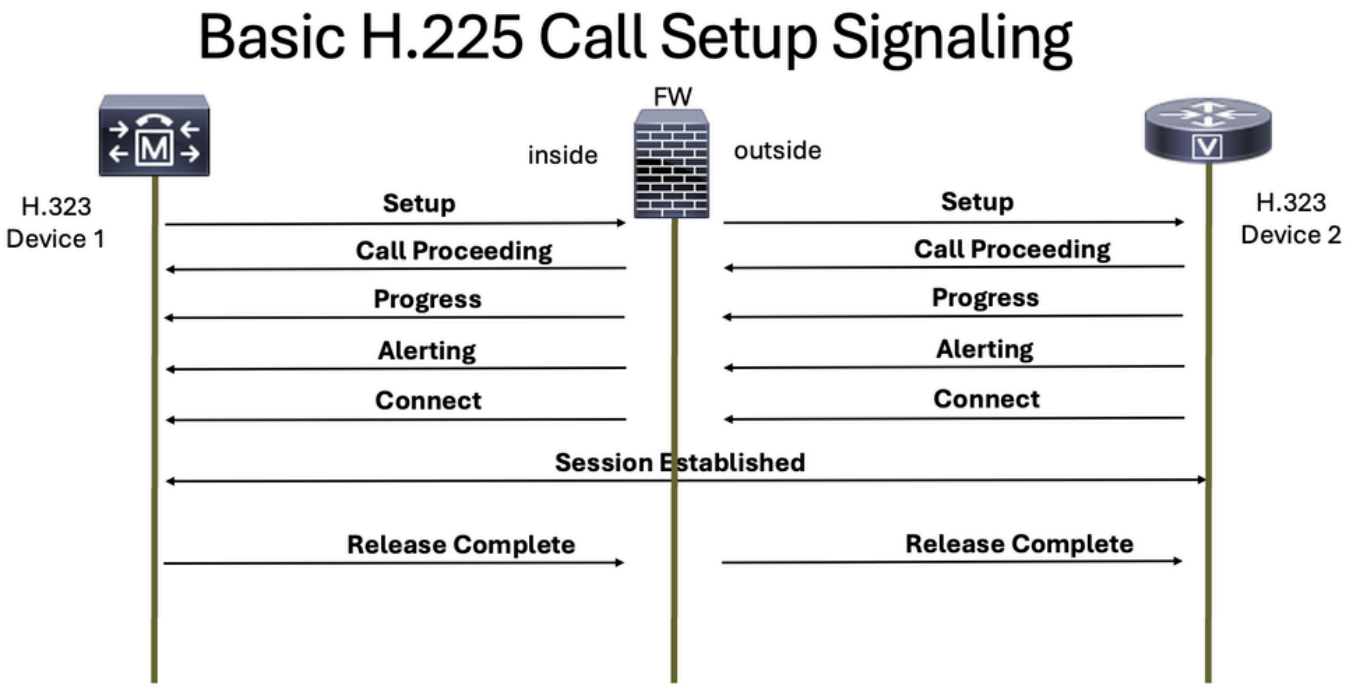


팁: 보안 H.323 프로토콜 통신은 암호화를 위해 TLS를 사용하여 UDP에서 TCP로 전환할 때 문제가 발생할 수 있으며, 이로 인해 방화벽에서 연결을 의심스러운 활동으로 잘못 차단할 수 있습니다. 따라서 H.323 엔드포인트 또는 서버의 UDP 및 TCP 트래픽을 모두 허용하도록 방화벽을 구성하는 것이 중요합니다.

H.323은 두 가지 작동 모드를 갖는 프로토콜입니다. 느린 시작과 빠른 시작.

H.225

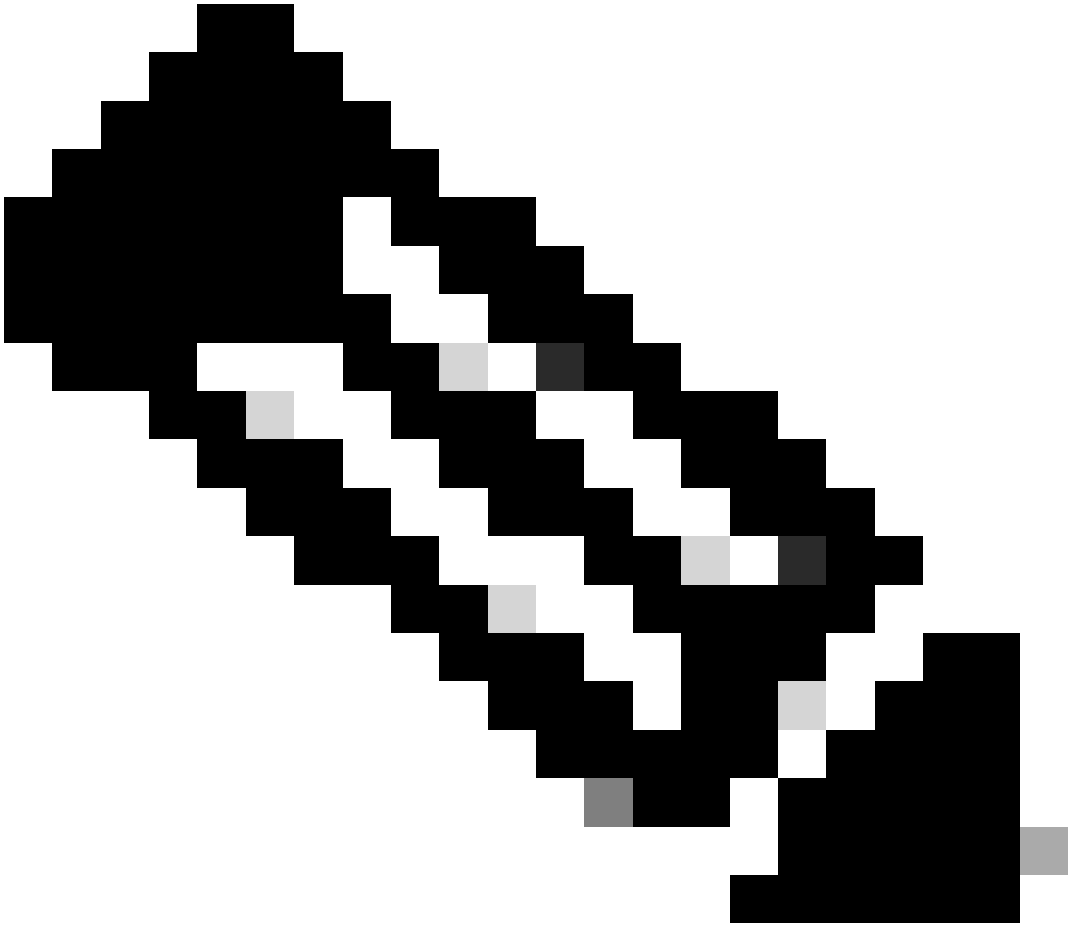
이 프로토콜은 통화를 설정하고 당사자 중 하나가 전화를 끊을 때 음성 통화를 끝냅니다.



H.245

H.245는 다음과 같은 기능을 제공합니다.

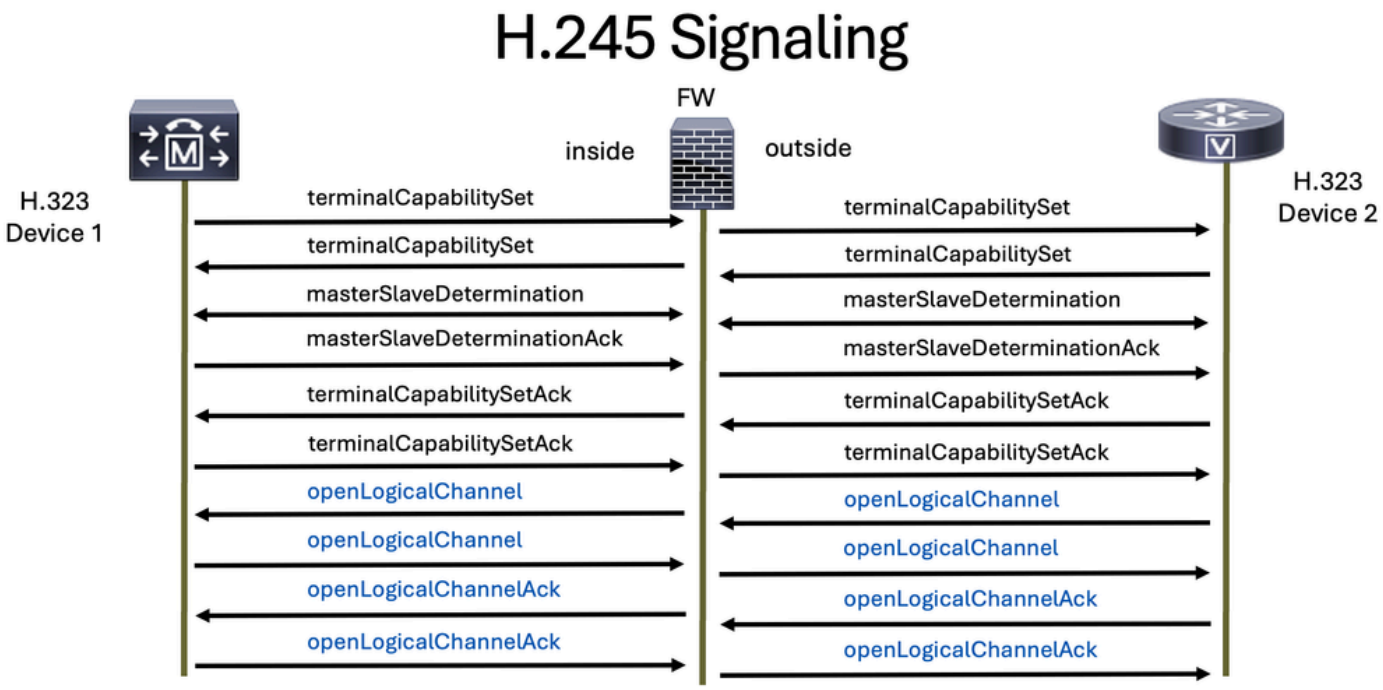
- 터미널 기능 교환
- 마스터/슬레이브 결정
- 논리적 채널 시그널링



참고: 이 문서에서 사용된 마스터 및 슬레이브라는 용어는 원래 H.323 프로토콜로 하드코딩되며 당사의 정책 또는 가치를 반영하지 않습니다. 우리는 포용적이고 존중하는 언어를 장려하기 위해 최선을 다하고 있다.

H.245 프로토콜은 H.225 연결 메시지를 수신한 후 전송됩니다.

이 프로토콜은 어떤 음성 프로토콜이 RTP에 사용되는지 확인하는 데 도움이 되며, 논리 채널을 열고 논리 채널 메시지를 닫는 데 지정됩니다.

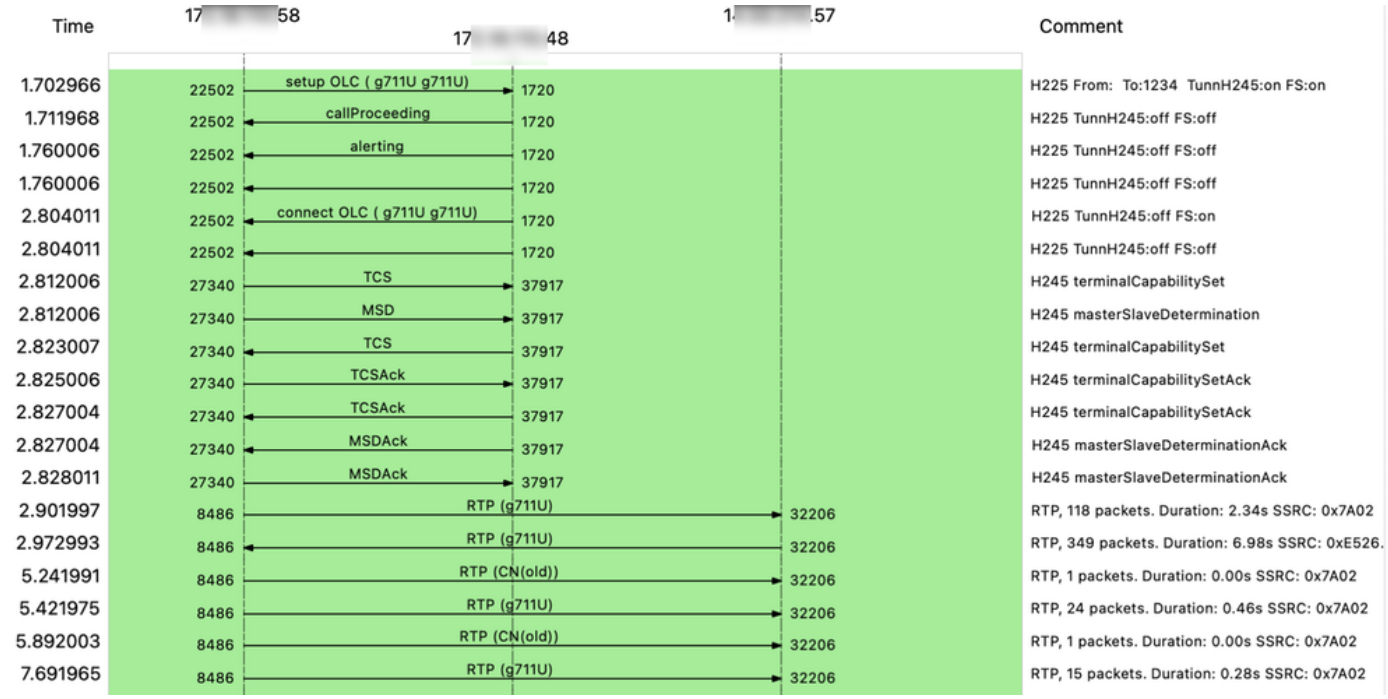


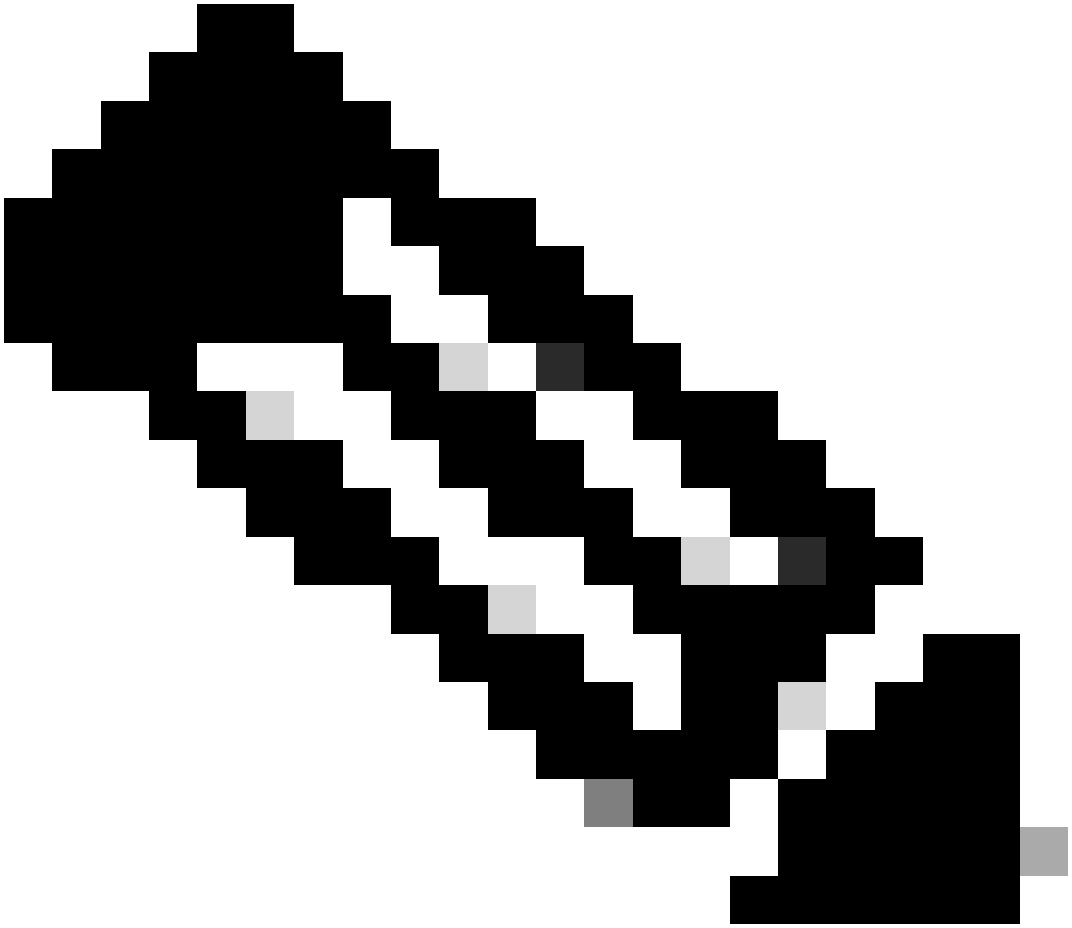
이 패킷 캡처는 H.225 및 H.245가 있는 두 H.323 디바이스 및 미디어(음성) 트래픽의 요청 및 응답을 보여줍니다.

No.	Time	Source	Destination	Protocol	Length	Info
6	1.702966	17[redacted]58	17[redacted]48	H.225.0	683	CS: setup OpenLogicalChannel
8	1.711968	17[redacted]48	17[redacted]58	H.225.0	151	CS: callProceeding
9	1.760006	17[redacted]48	17[redacted]58	H.225.0	152	CS: alerting
10	1.760006	17[redacted]48	17[redacted]58	H.225.0	114	CS: notify
15	2.804011	17[redacted]48	17[redacted]58	H.225.0	248	CS: connect OpenLogicalChannel
16	2.804011	17[redacted]48	17[redacted]58	H.225.0	114	CS: notify
21	2.812006	17[redacted]58	17[redacted]48	H.245	135	terminalCapabilitySet
23	2.812006	17[redacted]58	17[redacted]48	H.245	68	masterSlaveDetermination
25	2.823007	17[redacted]48	17[redacted]58	H.245	176	terminalCapabilitySet
26	2.825006	17[redacted]58	17[redacted]48	H.245	65	terminalCapabilitySetAck
27	2.827004	17[redacted]48	17[redacted]58	H.245	65	terminalCapabilitySetAck
28	2.827004	17[redacted]48	17[redacted]58	H.245	64	masterSlaveDeterminationAck
30	2.828011	17[redacted]58	17[redacted]48	H.245	64	masterSlaveDeterminationAck
32	2.901997	17[redacted]58	14[redacted]7	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7A02, Seq=5180, Time=1424280842, Ma
33	2.922001	17[redacted]58	14[redacted]7	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7A02, Seq=5181, Time=1424281002
34	2.942004	17[redacted]58	14[redacted]7	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7A02, Seq=5182, Time=1424281162
35	2.961992	17[redacted]58	14[redacted]7	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7A02, Seq=5183, Time=1424281322
36	2.972993	1[redacted]57	17[redacted]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 ([redacted]:9a:00), Dst: V[redacted]:84:d2:80)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 249
> Internet Protocol Version 4, Src: 17[redacted]58, Dst: 17[redacted]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
```

다음은 H.225 및 H.245와 RTP 미디어(음성)를 사용한 H.323 신호 흐름의 예입니다.

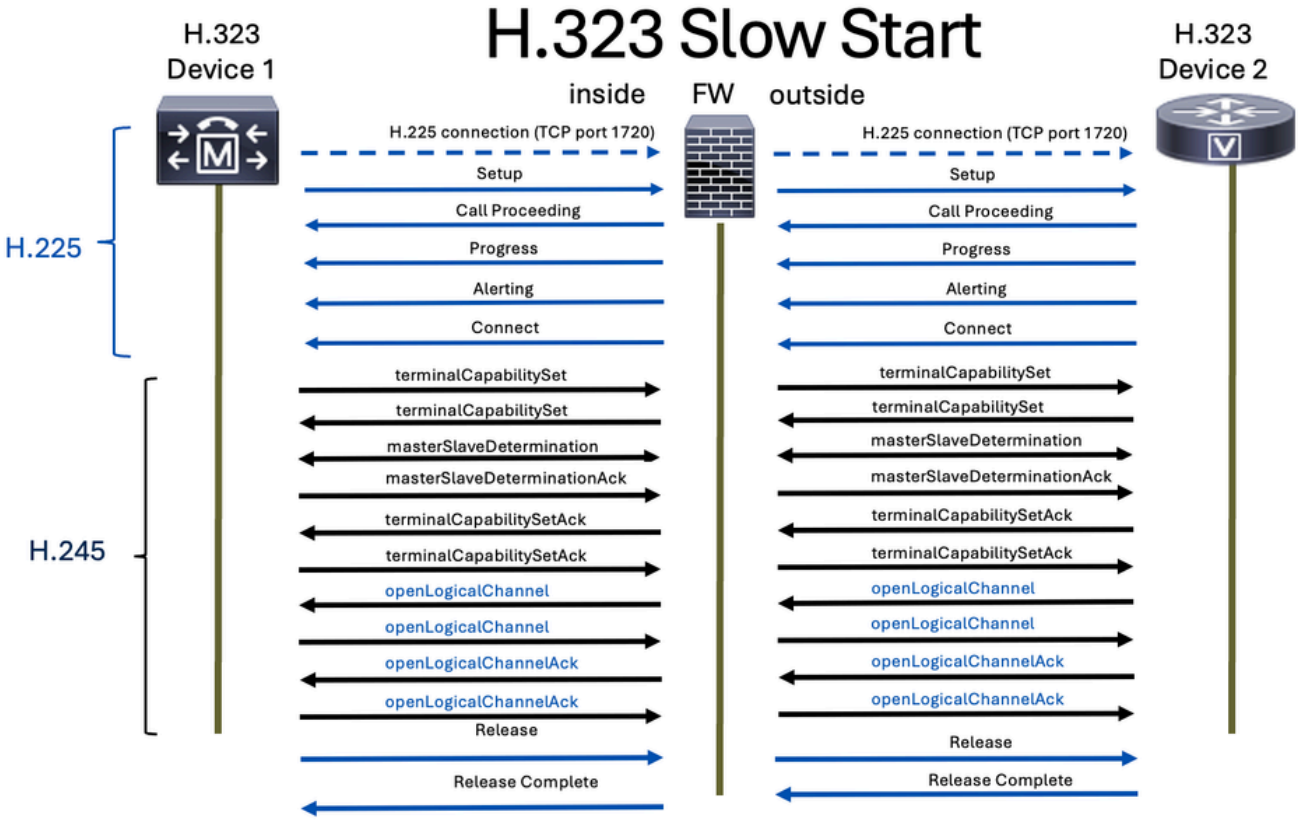

Time
Comment
1.702966 22502 setup OLC (g711U g711U) 1720 H225 From: To:1234 TunnH245:on FS:on
1.711968 22502 callProceeding 1720 H225 TunnH245:off FS:off
1.760006 22502 alerting 1720 H225 TunnH245:off FS:off
1.760006 22502 1720 H225 TunnH245:off FS:off
2.804011 22502 connect OLC (g711U g711U) 1720 H225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



참고: H.323 검사는 Cisco FTD(Secure Firewall Threat Defense) 및 ASA(Secure Firewall Adaptive Security Appliance)에서 기본적으로 활성화됩니다.

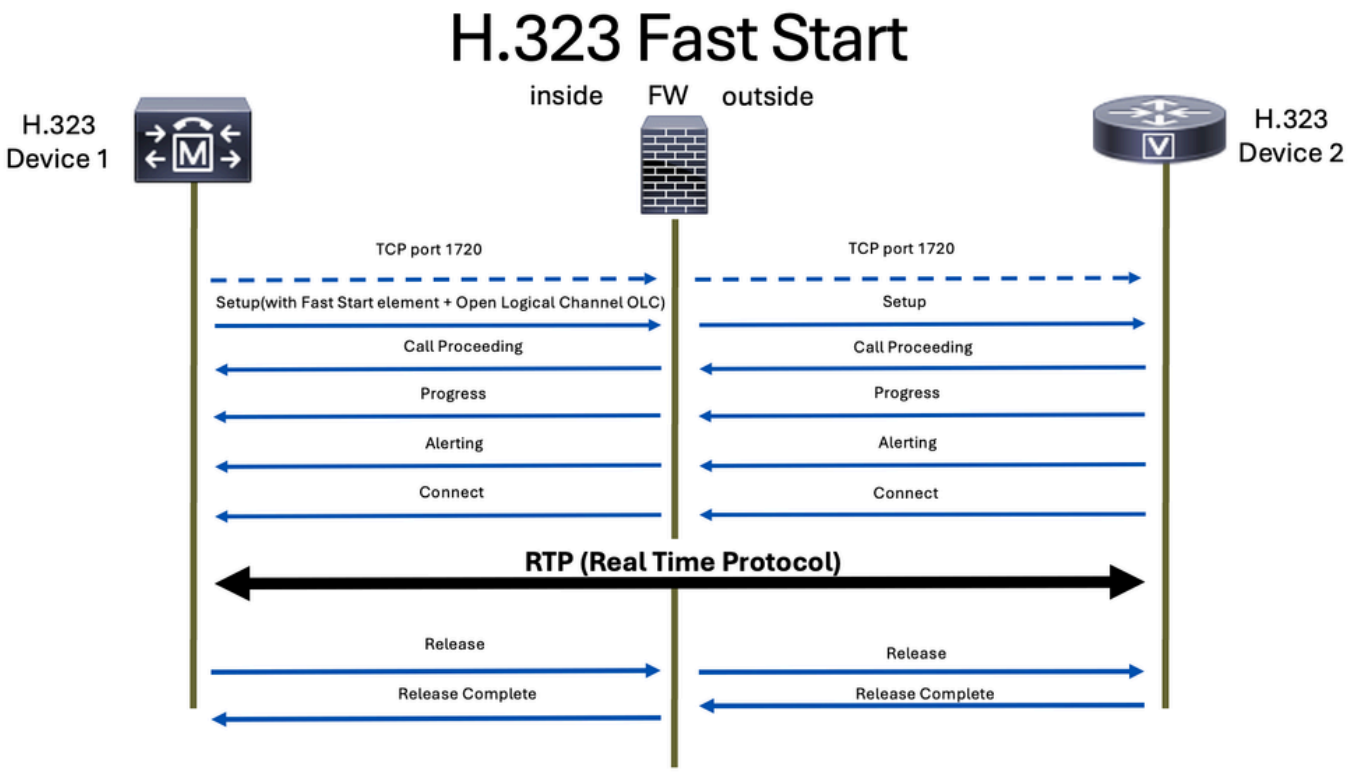
느린 시작

느린 시작 모드에서 통화 설정 프로세스에는 미디어 채널이 설정되기 전에 여러 신호 처리 단계가 포함됩니다. 단계에는 설정, 통화 진행, 알림 및 연결이 포함됩니다. 이 단계 이후에는 H.245 미디어 협상이 별도로 수행됩니다. 이는 최초 통화 신호 처리가 완료될 때까지 미디어 채널이 설정되지 않기 때문에 설정 시간이 더 길어질 수 있습니다.



빠른 시작

반면, 빠른 시작 모드에서는 초기 설정 메시지 내에서 미디어 협상이 발생할 수 있습니다. 이는 협상이 초기 호 설정의 일부로 이루어지기 때문에 미디어 채널을 보다 빠르게 설정할 수 있음을 의미한다. Fast Start는 미디어 채널이 설정되기 전에 교환되는 메시지 수 및 필요한 처리 양을 줄여 프로세스를 간소화합니다.

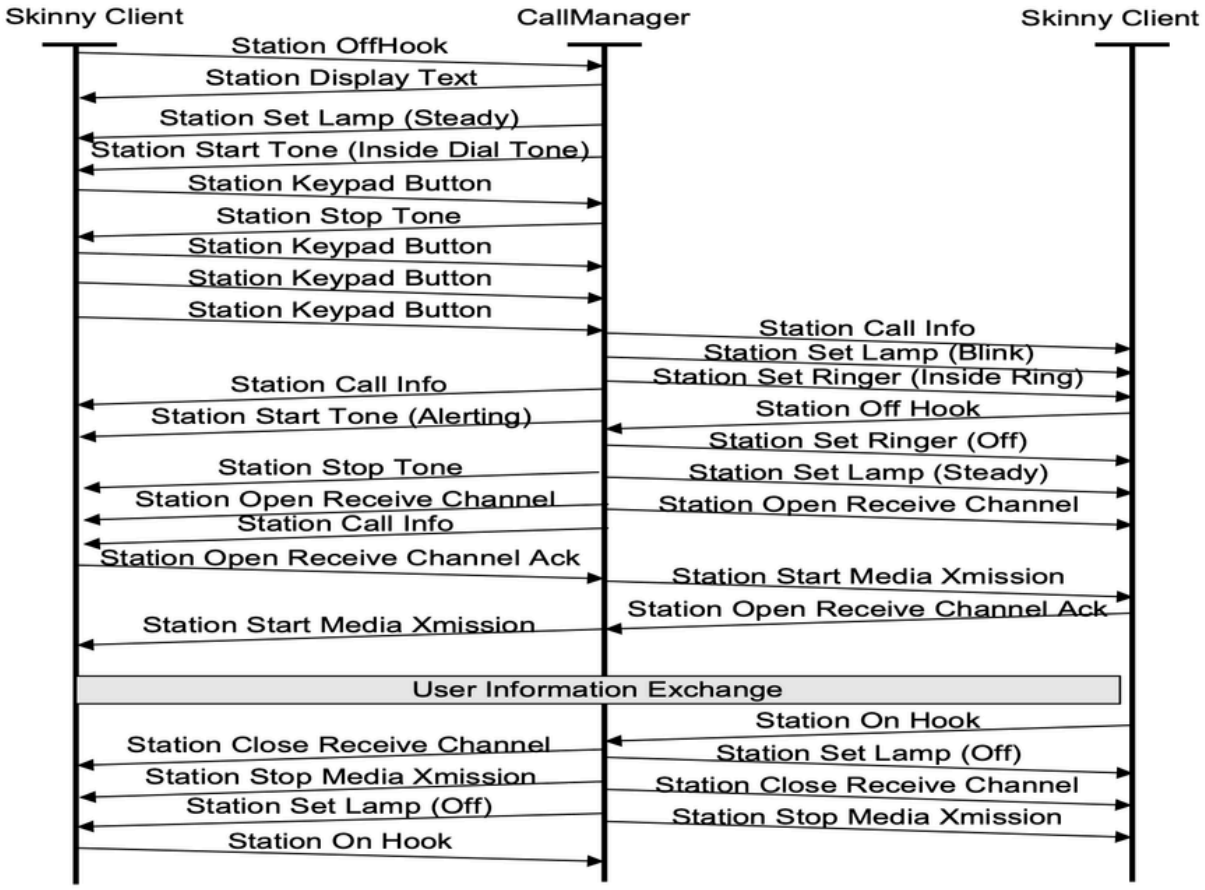


SCCP

Skinny라고도 하는 SCCP(Skinny Client Control Protocol)는 Cisco 독점 시그널링 프로토콜입니다. CUCM(Cisco Unified Communications Manager), Cisco CME(Unified Communications Manager Express) 라우터 및 Cisco IP Phone에서 통화 설정 및 제어를 용이하게 하기 위해 주로 사용됩니다.

SCCP 프로토콜은 비보안 SCCP에 포트 2000의 TCP를 사용하고 보안 SCCP에 포트 2443을 사용합니다.

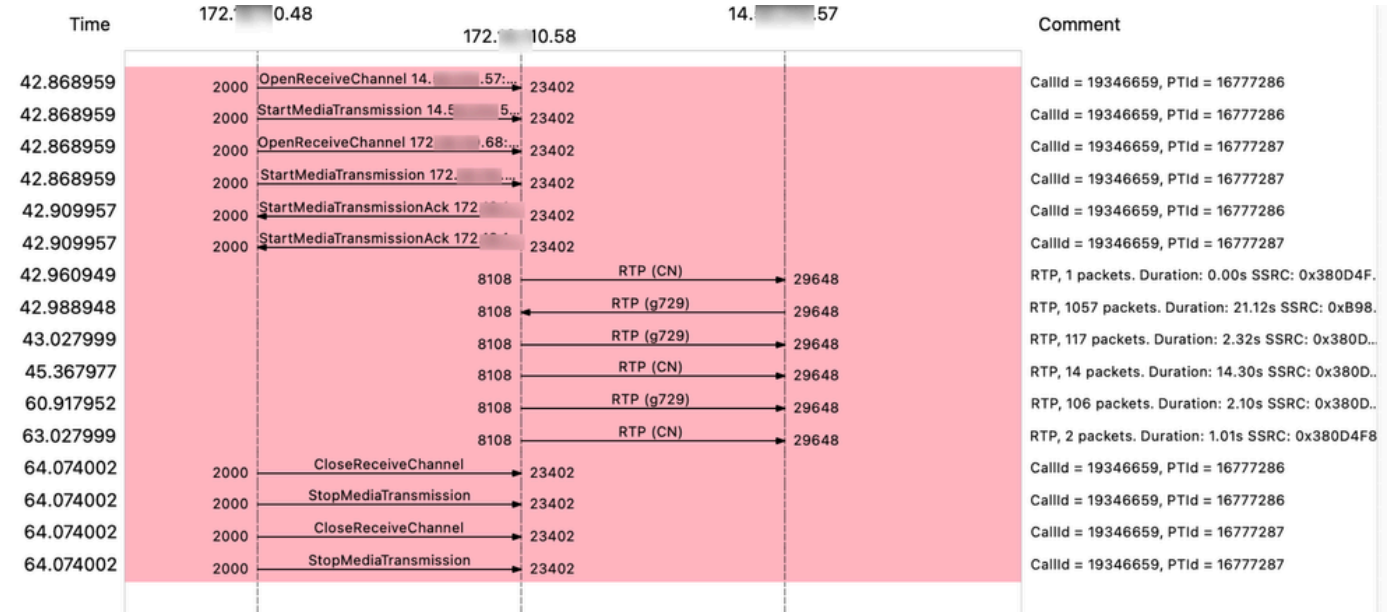
다음은 SCCP 통화에서 찾을 수 있는 일반적인 SCCP 메시지입니다.



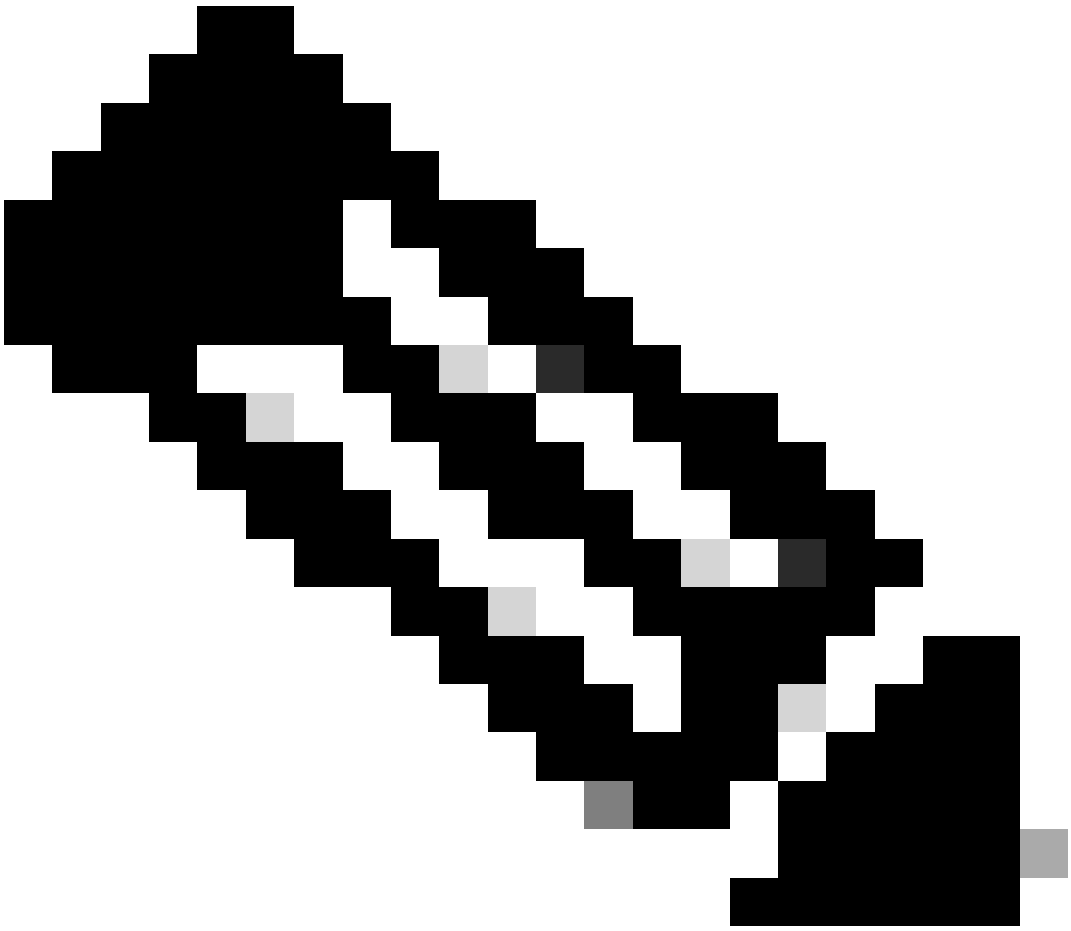
이 패킷 캡처는 2개의 SCCP 디바이스 및 미디어(음성) 트래픽의 요청 및 응답을 보여줍니다.

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

이것은 SCCP 시그널링 및 RTP 미디어(음성) 모두의 플로우의 예입니다.



Time	172.[redacted]0.48		172.[redacted]10.58	14.[redacted].57	Comment
42.868959	2000	OpenReceiveChannel 14.[redacted].57:...	23402		CallId = 19346659, PTId = 16777286
42.868959	2000	StartMediaTransmission 14.5[redacted]5...	23402		CallId = 19346659, PTId = 16777286
42.868959	2000	OpenReceiveChannel 172[redacted].68:...	23402		CallId = 19346659, PTId = 16777287
42.868959	2000	StartMediaTransmission 172.[redacted]...	23402		CallId = 19346659, PTId = 16777287
42.909957	2000	StartMediaTransmissionAck 172.[redacted]	23402		CallId = 19346659, PTId = 16777286
42.909957	2000	StartMediaTransmissionAck 172.[redacted]	23402		CallId = 19346659, PTId = 16777287
42.960949		8108 RTP (CN)		29648	RTP, 1 packets. Duration: 0.00s SSRC: 0x380D4F.
42.988948		8108 RTP (g729)		29648	RTP, 1057 packets. Duration: 21.12s SSRC: 0xB98.
43.027999		8108 RTP (g729)		29648	RTP, 117 packets. Duration: 2.32s SSRC: 0x380D...
45.367977		8108 RTP (CN)		29648	RTP, 14 packets. Duration: 14.30s SSRC: 0x380D..
60.917952		8108 RTP (g729)		29648	RTP, 106 packets. Duration: 2.10s SSRC: 0x380D..
63.027999		8108 RTP (CN)		29648	RTP, 2 packets. Duration: 1.01s SSRC: 0x380D4F8
64.074002	2000	CloseReceiveChannel	23402		CallId = 19346659, PTId = 16777286
64.074002	2000	StopMediaTransmission	23402		CallId = 19346659, PTId = 16777286
64.074002	2000	CloseReceiveChannel	23402		CallId = 19346659, PTId = 16777287
64.074002	2000	StopMediaTransmission	23402		CallId = 19346659, PTId = 16777287



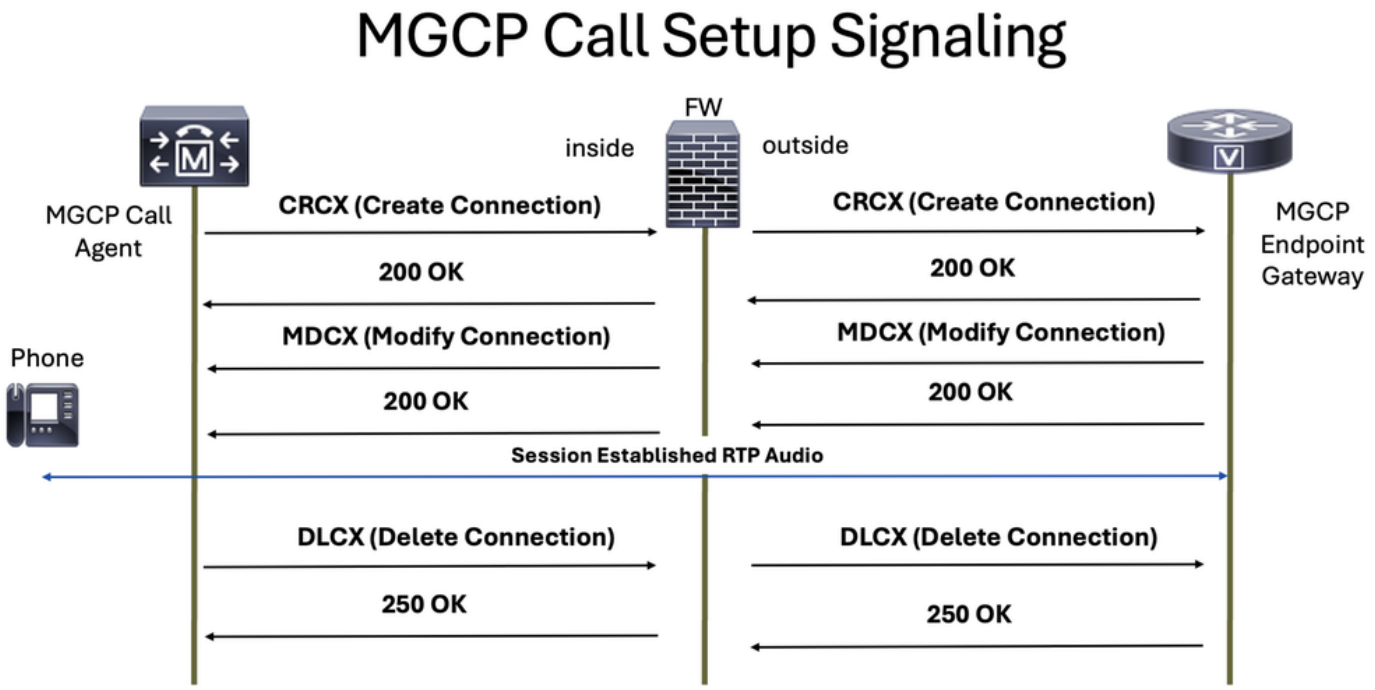
참고: SCCP 검사는 Cisco FTD(Secure Firewall Threat Defense) 및 ASA(Secure Firewall Adaptive Security Appliance)에서 기본적으로 활성화됩니다.

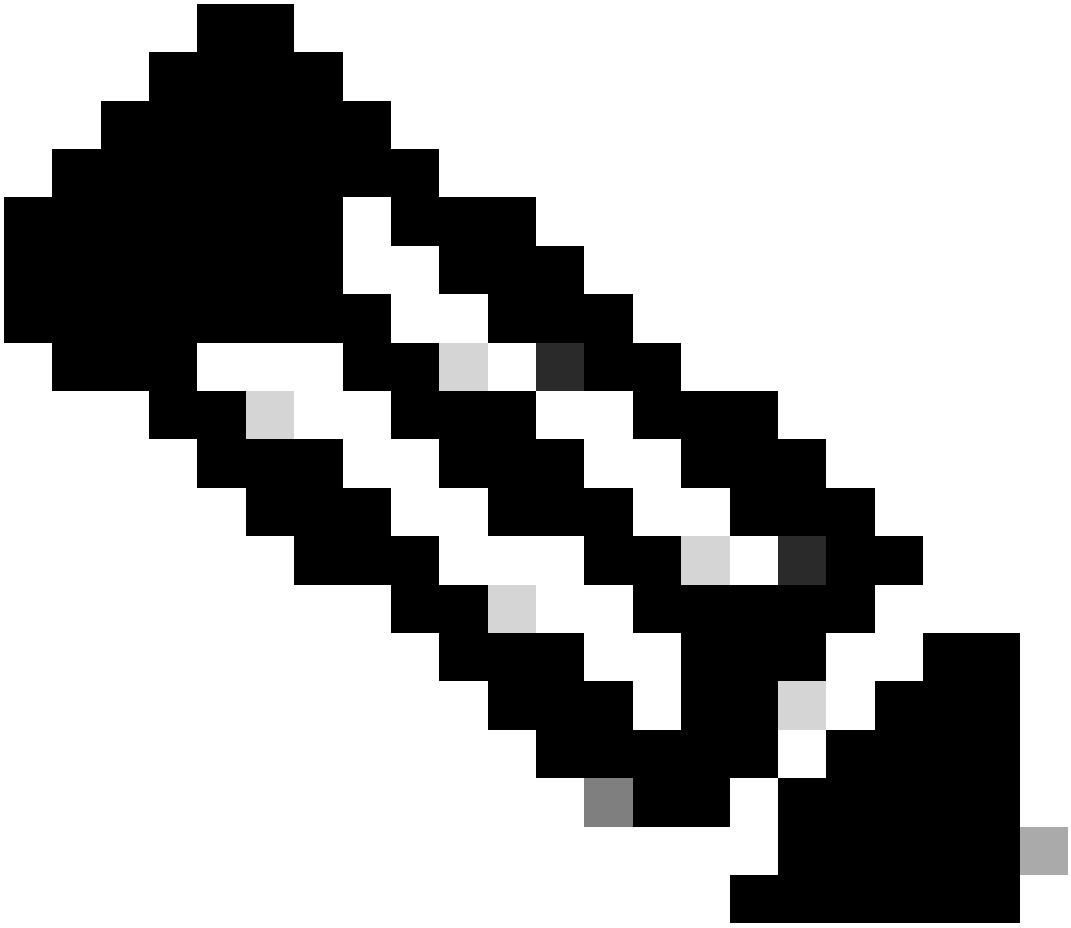
MGCP

MGCP(Media Gateway Control Protocol)는 통화 제어 장치(예: CUCM)가 VoIP 통화를 제어하는 데 사용되는 프로토콜입니다.

MGCP 시그널링 프로토콜은 RFC 2705에서 정의되며 통신에 TCP 포트 2428 및 UDP 포트 2427을 사용합니다.

통화 통신에 필요한 MGCP 일반 패킷은 다음과 같습니다.



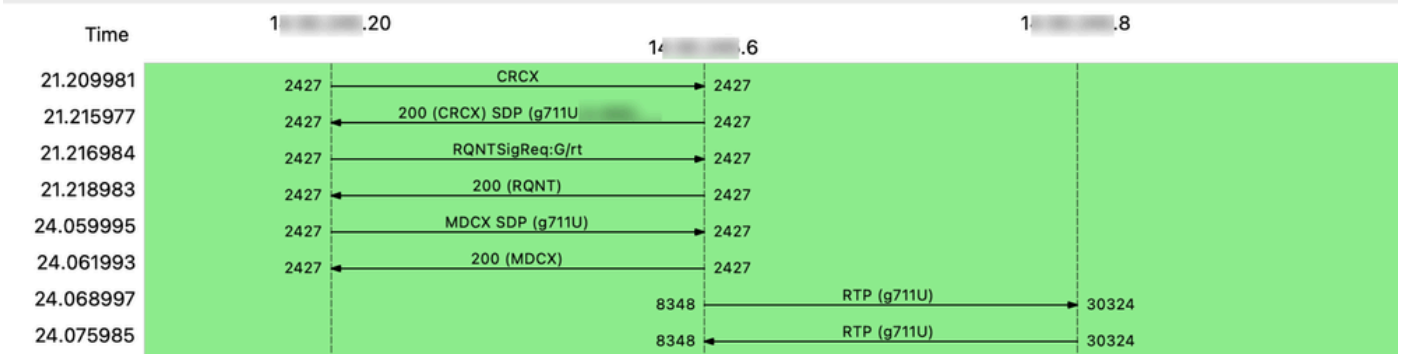


참고: MGCP 검사는 Cisco FTD(Secure Firewall Threat Defense) 및 ASA(Secure Firewall Adaptive Security Appliance)의 기본 검사 정책에서 활성화되지 않으므로 이 검사가 필요한 경우 활성화해야 합니다.

이 패킷 캡처는 두 MGCP 디바이스 및 미디어(음성) 트래픽의 요청 및 응답을 보여줍니다.

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

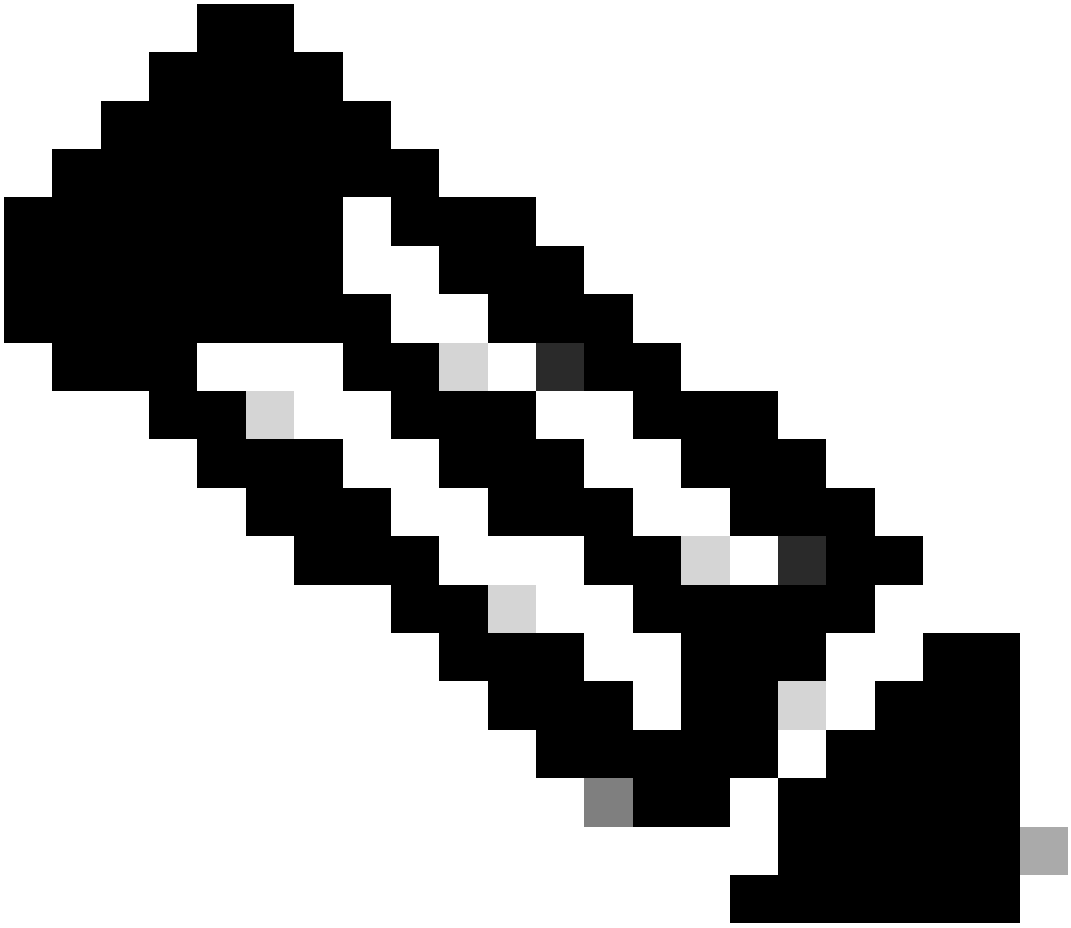
다음은 MGCP 시그널링 및 RTP 미디어(음성) 모두의 흐름의 예입니다.



모범 사례

ASA의 경우

- 트래픽이 두 신호 구성 요소(디바이스 또는 서버)를 오가는 것을 허용하는 허용 규칙을 사용합니다. 이는 지정된 시그널링 VoIP 프로토콜에 사용되는 포트에 의해 제한될 수 있습니다.
- 오디오 및/또는 비디오 스트림을 보내고 받을 수 있는 미디어 장치 간의 RTP 포트 범위를 허용합니다.



참고: 이러한 오디오 또는 미디어 장치는 신호 구성 요소(장치 또는 서버)와 다를 수 있다는 점을 기억하십시오.

FTD:

- 신호 구성 요소(장치 또는 서버)에 대한 프리필터 규칙을 정의하고 특정 포트를 정의하여 지정된 신호 프로토콜에 대한 트래픽만 제한합니다.
- 오디오 및/또는 비디오 RTP 프로토콜에 대한 사전 필터를 구성합니다.

문제 해결

음성 문제를 트러블슈팅할 때, 문제가 신호인지 미디어(음성 또는 비디오)인지 아니면 둘 다인지 알아야 합니다. 다음은 이를 차별화하는 데 도움이 되는 몇 가지 예입니다.

신호 문제의 예:

++사용자가 통화가 설정되지 않았다고 보고합니다.

++사용자가 다른 사용자 또는 번호로 전화를 걸 수 없습니다.

++OPTIONS sip 메시지가 응답을 받지 못하기 때문에 SIP 트렁크가 작동하지 않습니다.

++장치가 등록할 수 없습니다.

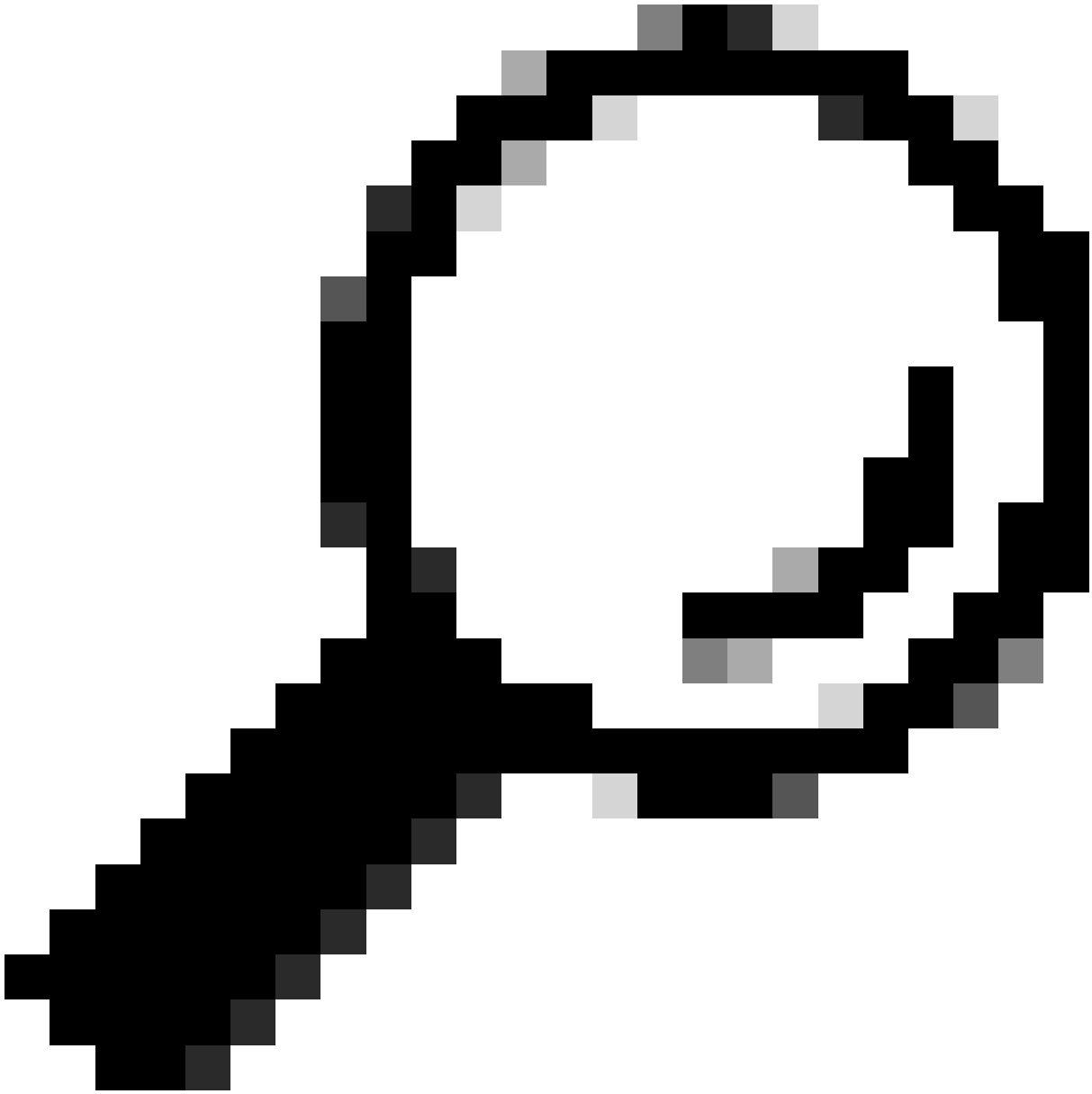
미디어(음성 또는 비디오) 문제의 예:

++단방향 오디오 문제가 있습니다.

++통화 중인 오디오가 없습니다.

++비디오가 전혀 없습니다.

++통화가 침묵됩니다.



팁: 비디오 통화 중에 SDP는 최대 3개의 미디어 라인(m-라인)을 협상할 수 있습니다. 오디오, 비디오 및 이미지. 각 m-라인은 통화 레그당 별도의 RTP(Real-Time Transport Protocol) 스트림에 해당합니다. 즉, 통화의 각 레그에 최대 3개의 개별 RTP 스트림(미디어 유형별로 하나씩)이 있을 수 있습니다.

방화벽의 신호 문제 해결

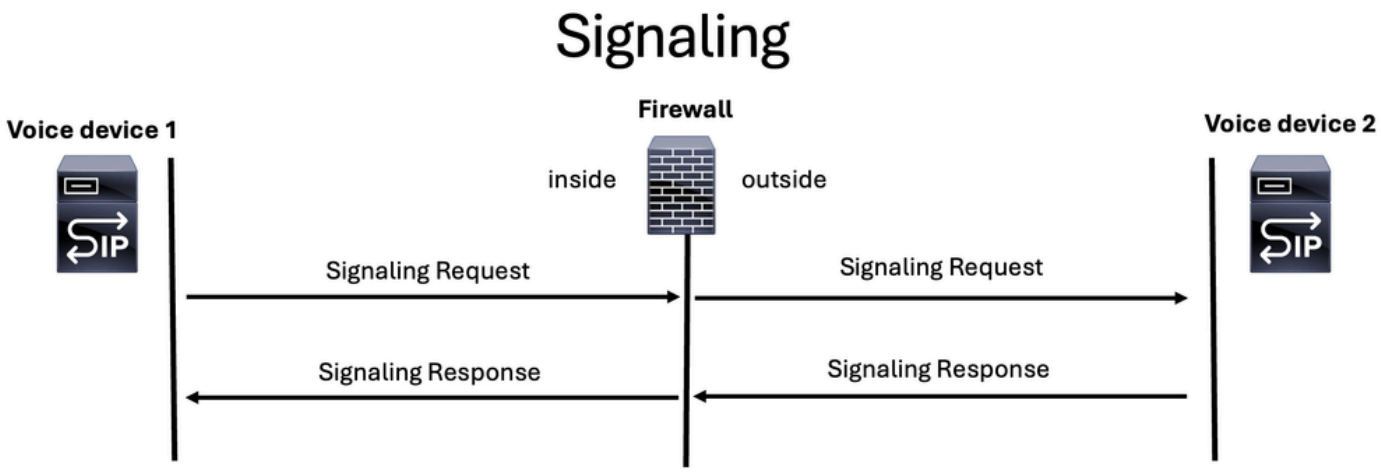
신호 부분을 트러블슈팅하려면 다음을 확인해야 합니다.

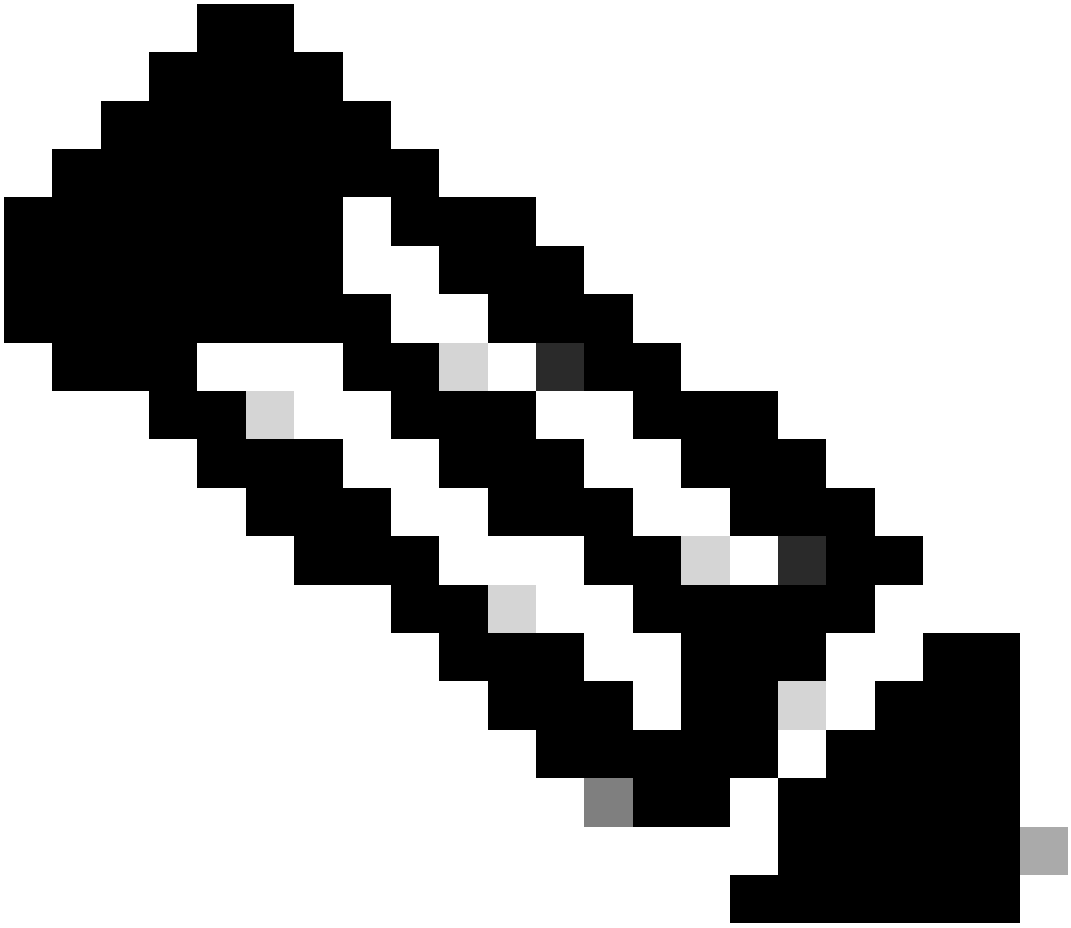
++인그레스 및 이그레스 인터페이스에서 통화와 관련된 모든 신호 구성 요소(디바이스 또는 서버)를 식별하고 보안 FW의 CLI에서 패킷 캡처에 적절한 일치 기준을 구성합니다.

++인그레스 인터페이스의 시그널링 메시지 수는 이그레스 인터페이스와 일치해야 합니다.

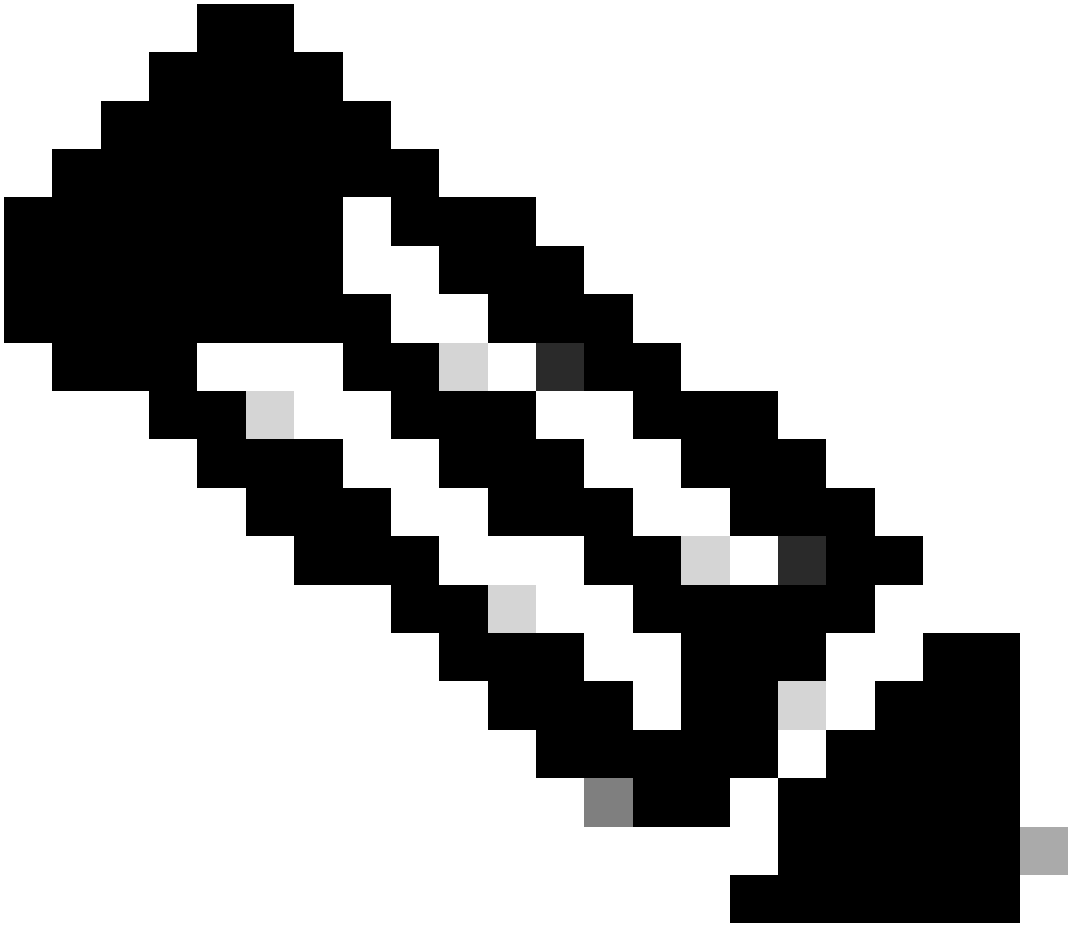
++시그널링 프로토콜에서 TCP를 사용하는지 UDP를 사용하는지 지정하고 예상 포트 번호를 필터링하여 패킷 캡처를 보다 효율적으로 만들 수 있습니다. 모든 시그널링 프로토콜은 IP를 통해 작동하므로 CLI에서 이러한 필터를 적용하면 캡처에 표시되는 트래픽의 양을 제한할 수 있습니다.

++이그레스 인터페이스의 경우 아웃바운드 트래픽에 할당된 NAT IP 주소가 패킷 캡처 필터에 지정되어 있는지 확인합니다. 이렇게 하면 이그레스 인터페이스에 나타나는 정확한 트래픽을 캡처할 수 있습니다.





참고: 음성에 어떤 시그널링 프로토콜이 사용되든 항상 요청과 응답이 있어야 하며 인그레스 및 이그레스 인터페이스에서 일관성이 있어야 합니다.

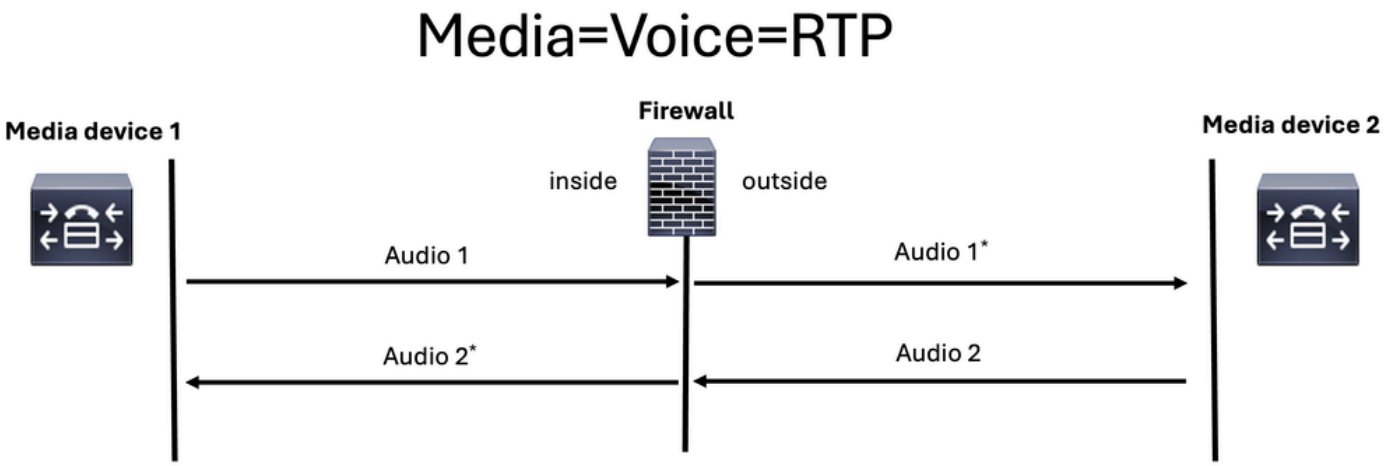


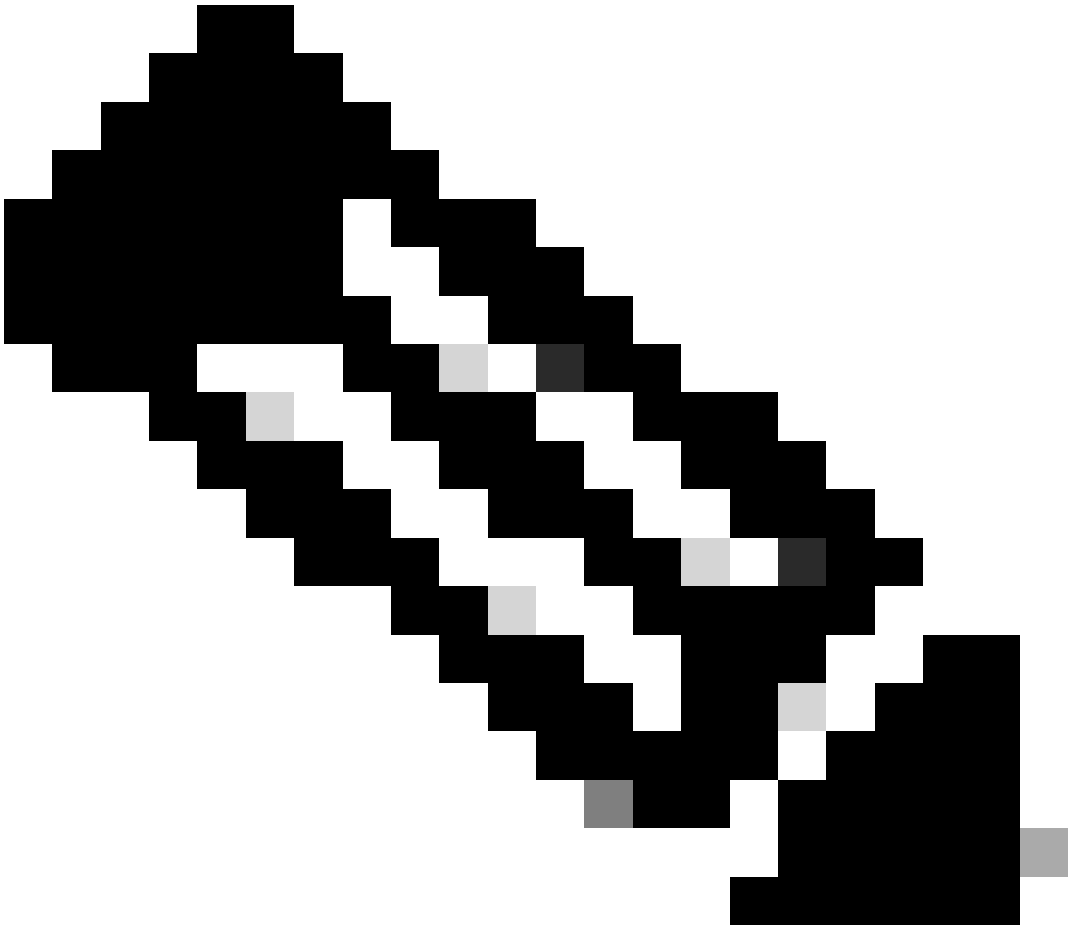
참고: 가능한 경우 통신 경로에 방화벽이 하나만 있는지 확인하십시오. 일부 구축에서는 음성 신호 및 미디어 스트림이 별도의 방화벽을 통과할 수 있습니다. 이러한 경우 트러블슈팅 프로세스에 모든 관련 방화벽을 포함해야 합니다

방화벽의 미디어 문제 해결

FW의 관점에서 보면 단방향 오디오, 양방향 오디오 문제 또는 오디오를 사용하지 않을 때 분석해야 하는 4개의 스트림이 있습니다.

1. 발신자에서 발신자로의 RTP 스트림(인그레스 인터페이스).
2. 발신자에서 수신자(이그레스 인터페이스)로의 RTP 스트림.
3. 피호출자에서 발신자로 전송되는 RTP 스트림(이그레스 인터페이스).
4. 발신자에서 발신자로의 RTP 스트림(인그레스 인터페이스).



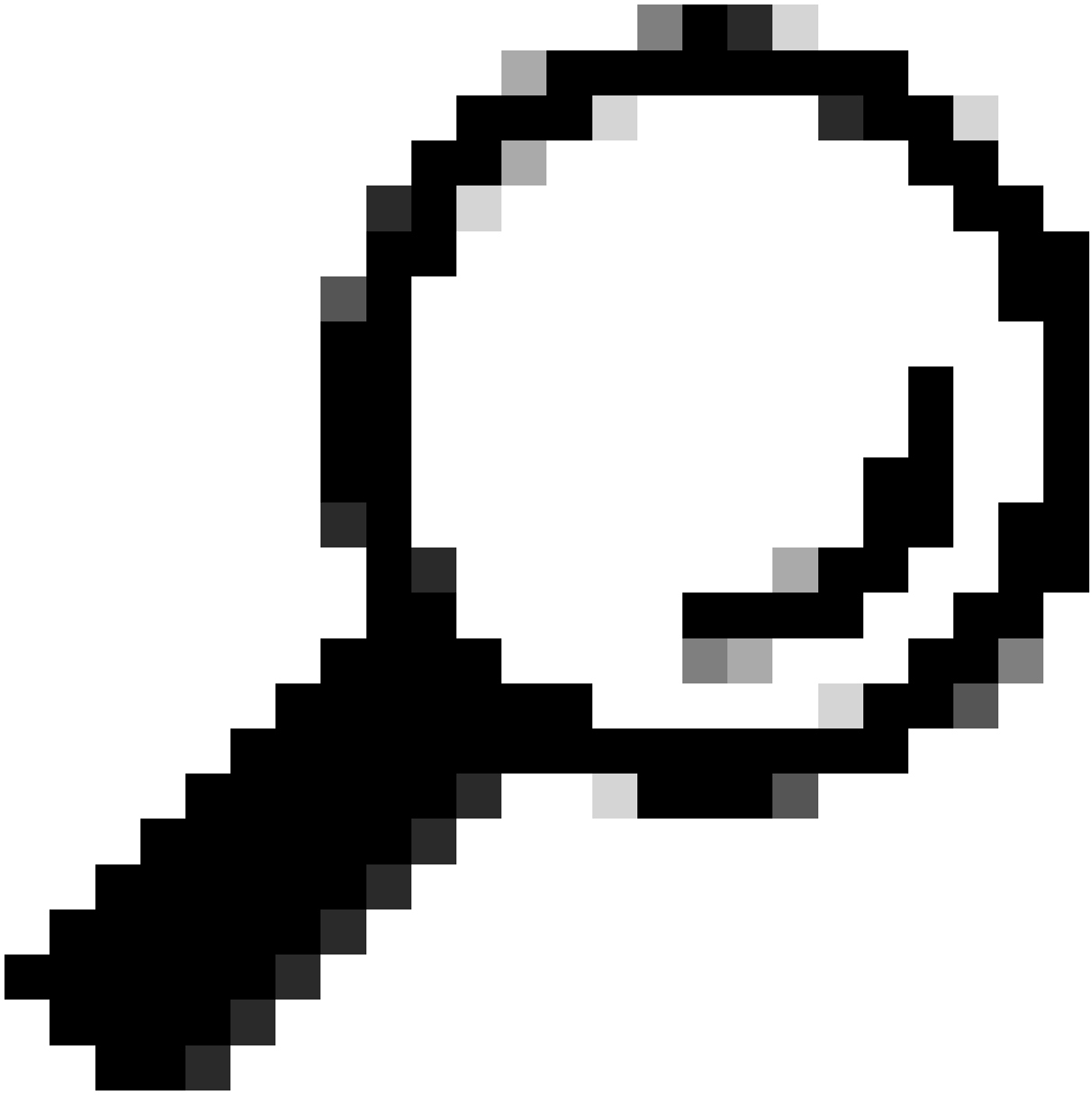


참고: FTD의 ASA 또는 LINA 모드에서 CLI 패킷 캡처를 사용하여 트러블슈팅을 수행할 수 있습니다. 이는 단일 패킷 캡처 내에서 여러 일치를 적용할 수 있는 더 큰 유연성을 제공합니다.

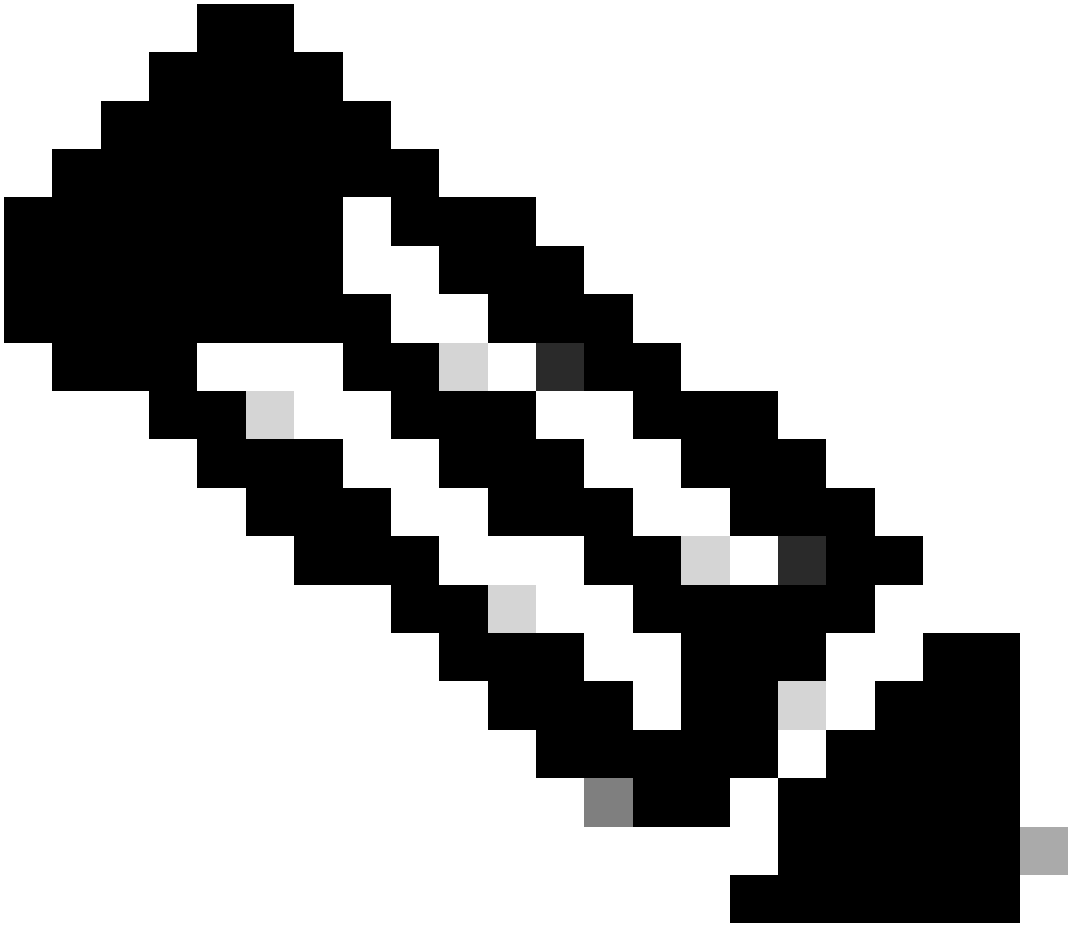
SIP 통화 문제 해결

Secure FW(ASA 또는 FTD)에서 음성 문제를 해결할 때 다음 단계를 수행해야 합니다.

1. 통화 흐름 및 토폴로지 다이어그램이 있는지 확인합니다.
2. 사용자의 관점에서 문제를 파악해야 합니다.
3. 신호 프로토콜의 경로를 파악합니다.
4. 미디어 RTP 프로토콜의 경로를 이해합니다.
5. 인그레스 및 이그레스 인터페이스에서 패킷 캡처를 수행합니다.
6. 컨피그레이션 ACL 규칙 및 NAT 규칙을 검토합니다.
7. SIP 시그널링 트래픽이 방화벽에 의해 차단되고 있지 않은지 확인합니다. 또한 인그레스(ingress) 및 이그레스(egress) 인터페이스를 비교하여 음성 트래픽 흐름을 분석합니다.
8. 인그레스 및 이그레스 인터페이스의 트래픽 흐름을 비교하여 RTP 미디어 트래픽이 방화벽에 의해 차단되지 않는지 확인합니다.
9. 신호 장치가 검사를 지원하는지 확인하고 비활성화하지 않으면 비활성화합니다.



팁: FW에 들어오는 SIP 시그널링 메시지는 FW를 떠나는 것과 동일해야 합니다.



참고: SIP에 대한 문제 해결 팁은 H.323, MGCP 및 SCCP 프로토콜에도 적용할 수 있습니다.

관련 정보

- CLI로 ASA 패킷 캡처 구성
- firepower Threat Defense 캡처 사용

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.