

WHITE PAPER

SIP – uma introdução

Setembro 2024

Resumo

O Session Initiation Protocol (SIP) fornece uma interface adicional dedicada a integração a sistemas para produtos de segurança. O SIP é um padrão amplamente adotado no setor de telecomunicações e oferece mais flexibilidade em termos de interconectividade e uso diário. Interfaces abertas e padronizadas são exigidas por integradores de sistemas, desenvolvedores e usuários finais, aumentando o valor oferecido a eles, pois os produtos podem ser usados em diversos sistemas. Os produtos Axis compatíveis com SIP são feitos para uso em soluções de segurança e soluções de comunicação.

É muito fácil configurar um sistema SIP. No entanto, caso surjam topologias de rede complexas ou quando são exigidos recursos de gestão de chamadas adicionais, o servidor SIP e as técnicas de travessia de NAT precisam ser utilizados, o que exige um maior conhecimento técnico por parte do instalador ou do técnico.

Sumário

1	Introdução	4
2	Como funciona?	4
2.1	Configuração ponto a ponto – A maneira mais simples	4
2.2	Usar um servidor SIP (PBX) – Adicionar mais possibilidades	5
2.3	Usar um tronco SIP – atribuição de um número de telefone	5
3	Comunicações unificadas (UC)	6
4	Por dentro de uma chamada SIP normal	7
4.1	SDP – Negociação do formato a ser usado	7
4.2	Chamadas em uma infraestrutura SIP complexa	8
5	DTMF – Envio de comandos em chamadas SIP	8
6	Ambientes complexos e maior segurança	9
6.1	NAT Traversal – navegação em redes complexas	9
6.2	Usar criptografia com SIP	10
7	Terminologia SIP	11

1 Introdução

O Session Initiation Protocol (SIP) é usado para iniciar, manter e encerrar sessões multimídia entre diferentes entidades. Essas sessões geralmente são de áudio, mas às vezes também incluem vídeo. SIP é o protocolo padrão usado em aplicativos de Voice over IP (VoIP) e plataformas de comunicações unificadas (UC) (veja a Seção 3).

O SIP é uma nova forma de conectar, integrar e controlar seus produtos de rede Axis. Ele é compatível com todos os alto-falantes de rede Axis, todos os interfones de rede Axis e dispositivos de sistema Axis e câmeras Axis selecionados.

2 Como funciona?

Para se comunicar usando SIP, é necessário ter pelo menos dois clientes SIP. Um cliente SIP pode ser um hardphone ou um softphone SIP, um cliente móvel ou um produto Axis compatível com SIP.

Cada cliente SIP recebe seu próprio endereço SIP. Um endereço SIP é semelhante a um endereço de e-mail, mas com o prefixo "sip:"

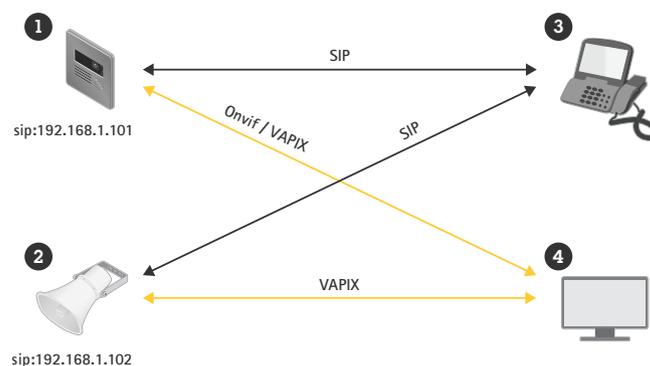
Por exemplo, sip:bob@axis.com [sip:<usuário@><provedor>]. Esse identificador pode ser usado em diversos dispositivos e funciona de maneira similar a um número de telefone vinculado a um cartão SIM que pode ser usado em vários dispositivos.

2.1 Configuração ponto a ponto – A maneira mais simples

Um sistema SIP pode assumir muitas formas. Na sua forma mais simples, o sistema consiste em dois ou mais User Agents (UA) SIP comunicando-se diretamente entre si. Isso pode ser chamado de configuração ponto a ponto, configuração de chamada direta ou configuração local. Nesse caso, um endereço SIP típico teria a forma sip:<ip-local>, por exemplo, sip:192.168.0.90

Exemplo: Em uma configuração simples, esses produtos da Axis (1, 2) podem usar o SIP para configurar comunicação por áudio e/ou vídeo com outros dispositivos SIP (3) na mesma rede, sem a necessidade de ter um servidor ou um PBX.

Ao mesmo tempo, eles podem ser conectados como qualquer outro dispositivo da Axis ao sistema de gerenciamento de vídeo (4) usando as APIs abertas VAPIX ou ONVIF Profile S.



Para fazer uma chamada ponto a ponto de um UA para outro em uma rede local, basta usar o endereço SIP contendo o endereço IP da unidade.

2.2 Usar um servidor SIP (PBX) – Adicionar mais possibilidades

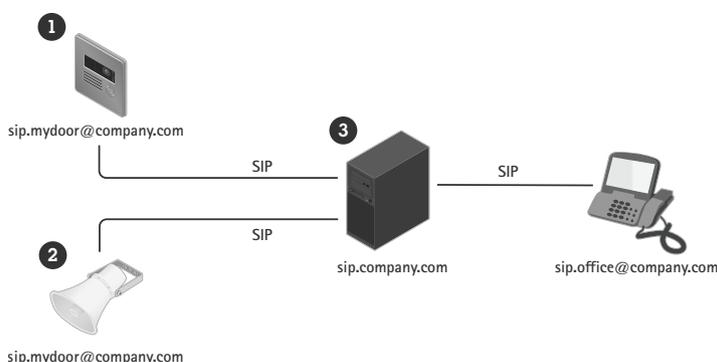
Uma infraestrutura VoIP baseada em SIP pode ser ampliada muito bem. O próximo passo em termos de tamanho é usar um servidor SIP ou Private Branch Exchange (PBX), como um hub central. Os UAs SIP registram-se no registrador do servidor e podem então entrar em contato com outros UAs simplesmente discando um ramal no PBX.

Nesse caso, um endereço SIP comum usaria o formato `sip:<usuário>@<domínio>`. Por outro lado, o formato pode ser `sip:<usuário>@<ip-do-registrador>`, por exemplo, `sip:6007@meuservidorIP.net`. Um PABX funciona como uma central telefônica tradicional, mostrando o status atual dos clientes, possibilitando transferências de chamadas, correio de voz, redirecionamentos e muito mais.

Um servidor SIP geralmente conta com as funcionalidades de proxy, registrador e redirecionamento. Os proxies roteiam as chamadas e fornecem lógica adicional às chamadas recebidas. Os registradores aceitam solicitações de registro e atuam como um serviço de localização para o domínio que ele gerencia. Os servidores de redirecionamento redirecionam o cliente para contatar um endereço SIP alternativo.

O servidor SIP pode ser configurado como uma entidade local ou pode estar localizado fora das instalações. Ele pode ser hospedado no local ou na nuvem. Ao fazer chamadas SIP entre instalações, normalmente as chamadas são roteadas inicialmente através de um conjunto de proxies SIP. Estes proxies consultam o local do endereço SIP que deve ser acessado.

Exemplo: Os produtos Axis (1, 2) podem se conectar a um servidor SIP (3) local ou externamente. O servidor se responsabiliza pela configuração e a finalização de chamadas entre dispositivos SIP na rede local ou pela Internet. Nessa configuração, o endereço SIP do dispositivo não depende do seu endereço IP e o servidor SIP torna o dispositivo acessível, desde que esteja registrado no servidor.



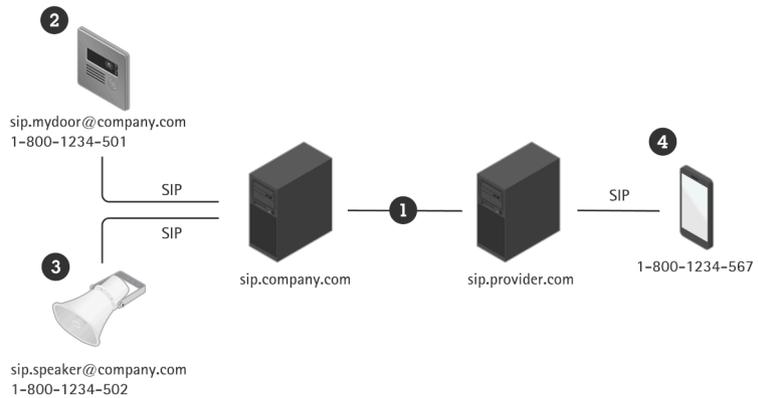
Para usar o seu dispositivo em conjunto com um servidor SIP, você precisa criar uma conta no servidor com um ID de usuário e senha especificados. Para registrar seu dispositivo no servidor, você precisa configurar uma conta no dispositivo, inserindo o endereço do servidor, o ID do usuário e a senha.

2.3 Usar um tronco SIP – atribuição de um número de telefone

Usando um tronco SIP, os UAs SIP podem ser alternados para a rede telefônica tradicional (PSTN). Assim, você pode até atribuir um número de telefone comum ao UA SIP.

O entroncamento SIP baseado em nuvem é uma abordagem moderna que aproveita a Internet para fornecer chamadas e outros serviços de comunicação. Esse método elimina a necessidade de linhas telefônicas físicas, facilitando a integração de soluções em nuvem e sistemas VoIP.

Exemplo: Usando um tronco SIP (1) com um provedor de serviços, você pode atribuir números de telefone externos aos seus dispositivos (2, 3). Assim, você pode fazer chamadas entre um alto-falante da rede ou um interfone de rede e telefones comuns (4).



Quando usado com um tronco SIP, o dispositivo se conecta ao servidor da maneira descrita acima.

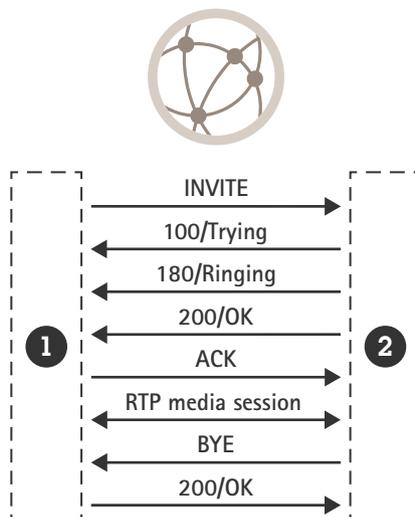
3 Comunicações unificadas (UC)

Comunicações unificadas (UC) refere-se à integração de várias ferramentas e tecnologias de comunicação em um sistema único e coeso. O SIP desempenha um papel vital nas UCs, ativando a interação perfeita entre diferentes canais de comunicação, como voz, vídeo, mensagens instantâneas e informações de presença. Ao aproveitar o SIP, as organizações podem criar um ambiente de comunicação unificado que aprimora a colaboração, melhora a produtividade e proporciona uma experiência consistente para o usuário em vários dispositivos e plataformas.

A UC pode ser fornecida localmente em soluções locais ou por meio de soluções em nuvem (UC como serviço - UCaaS). Exemplos de provedores de serviços para as soluções em nuvem: Cisco Webex, Microsoft Teams e Zoom.

4 Por dentro de uma chamada SIP normal

Para fazer uma chamada SIP, uma sequência de etapas é executada para trocar informações entre os UAs que iniciam e recebem a chamada.



Ao começar uma chamada, o UA iniciador (1) envia uma solicitação ou um INVITE para o endereço SIP do UA destinatário (2). O INVITE contém um corpo de Session Description Protocol (SDP) que descreve os formatos de mídia disponíveis e as informações de contato do iniciador da chamada.

Ao receber o INVITE, o destinatário confirma imediatamente respondendo a mensagem com uma resposta 100 TRYING.

O UA receptor então compara os formatos de mídia oferecidos descritos no SDP aos seus próprios formatos. Se um formato comum pode ser decidido, o UA alerta o destinatário de que há uma chamada chegando e envia uma resposta provisória de volta para o UA iniciador – 180 RINGING.

Quando o destinatário atende à chamada, uma resposta 200 OK é enviada para o iniciador para confirmar que uma conexão foi estabelecida. Essa resposta contém um SDP negociado indicando para o iniciador quais formatos de mídia devem ser usados e para onde os streams de mídia devem ser enviados.

Os streams de mídia negociados agora são configurados usando o Real-time Transport Protocol (RTP) com parâmetros baseados no SDP negociado e a mídia viaja diretamente entre as duas partes. O iniciador envia uma confirmação (ACK) via SIP para confirmar que ele configurou os streams de mídia conforme acordado. A sessão SIP ainda está ativa, mas não está mais envolvida na transferência de mídia.

Quando uma das partes decide encerrar a chamada, ela envia uma nova solicitação: BYE. Ao receber um BYE, a parte receptora reconhece isso com um 200 OK e os fluxos de mídia RTP são interrompidos.

4.1 SDP – Negociação do formato a ser usado

O Session Description Protocol (SDP) é um formato usado para descrever parâmetros de inicialização de mídias de streaming. O corpo do SDP contém informações sobre quais formatos de mídia (ou seja, codecs) são suportados pelos clientes e sobre a ordem de seleção de codecs preferida dos clientes.

Os codecs de áudio comumente usados para chamadas SIP são: PCMU, PCMA, G.722, G.726 e L16. Se o iniciador e o destinatário suportarem vários codecs sobrepostos, normalmente, o codec com a prioridade mais alta no lado do destinatário será selecionado. No fim, a escolha dos codecs afeta a largura de banda, portanto, o uso deles deve ser cuidadosamente pensado para atender aos requisitos de compatibilidade de outros UAs SIP e respeitar o requisito de largura de banda adequado ao caso de uso. Por exemplo, em uma rede local onde todos os clientes são compatíveis com L16, escolher usar áudio não compactado é algo que funciona bem. Entretanto, se a ideia é que o UA SIP seja acessado pela internet por meio de um celular, o PCMU é a melhor opção.

4.2 Chamadas em uma infraestrutura SIP complexa

Em uma infraestrutura de SIP mais complexa, o processo de iniciação é um pouco diferente, já que a sessão de SIP é configurada passo a passo para cada salto. No entanto, depois que a sessão SIP é configurada, o tráfego geralmente não é roteado, mas trafega diretamente entre as diferentes partes, como no exemplo anterior.

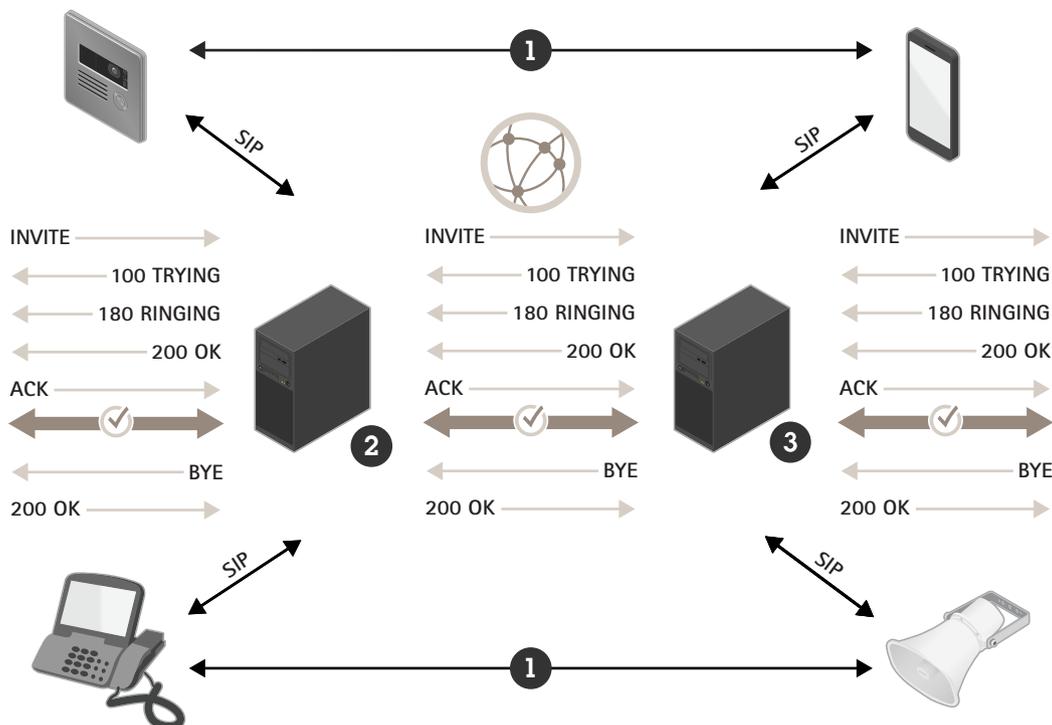


Figure 1. Configuração de chamada em uma infraestrutura de SIP complexa. Streams RTP de mídia (1) viajam diretamente entre as partes assim que a sessão SIP é configurada entre o iniciador (2) e o destinatário (3).

5 DTMF – Envio de comandos em chamadas SIP

Dual-Tone Multiple-Frequency (DTMF) é um formato usado para enviar informações via conexão telefônica. Os sinais DTMF podem ser enviados em chamadas SIP e ser usados para dar instruções a um dispositivo SIP. O intervalo de caracteres DTMF é formado por dígitos de 0 a 9, as letras A a D, * e #.

Por exemplo, em uma chamada para um interfone com SIP, o caractere DTMF "5" pode ser enviado do teclado do telefone, que pode ser configurado para ser interpretado pelo receptor como o comando que desbloqueia porta.

Há três maneiras diferentes de enviar DTMF em uma chamada SIP:

- O método tradicional in-band, no qual o sinal é na verdade um pulso de áudio intercalado com o stream de áudio. No entanto, esse método não é confiável e só funciona com codecs não compactados.
- O método SIP INFO, no qual o caractere DTMF é enviado em uma mensagem SIP no stream de sinalização. Esse método é muito confiável e out-of-band, porém, é pouco suportado.
- O método RTP (RFC2833), no qual o caractere DTMF é codificado como um pacote RTP e enviado out-of-band. Esse é o padrão realmente usado e conta com amplo suporte.

6 Ambientes complexos e maior segurança

Ambientes de rede complexos, como redes corporativas, podem causar dificuldades quando você usa SIP. O mesmo vale se você deseja usar criptografia.

6.1 NAT Traversal – navegação em redes complexas

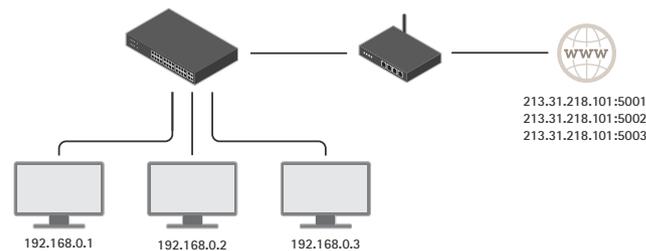
Em um ambiente de rede mais complexo, pode ser necessário utilizar Network Address Translation (NAT). NAT é uma maneira de representar publicamente endereços IP localizados em uma rede local privada. Isso significa que todas as unidades em uma sub-rede privada compartilham um prefixo de endereço IP comum, como 192.168.1.XXX. Esse é o endereço usado quando eles se comunicam entre si. Quando eles se comunicam com outra rede, esse endereço é traduzido para o endereço público do roteador e acrescido de um mapeamento de portas

- 192.168.1.24 => 184.13.12.33:44221
- 192.168.1.121 => 184.13.12.33:24325 e assim por diante.

Como a tabela de tradução é armazenada no roteador, na maioria dos casos é impossível um usuário externo saber o endereço de um dispositivo com NAT. Em uma comunicação via SIP, o resultado pode ser um dos seguintes problemas:

- Não é possível iniciar, atualizar ou encerrar uma sessão, ou seja, não é possível ligar, deixar em espera ou desligar.
- Sem streams de mídia.
- Streams de mídia unidirecionais.

NAT Traversal: o NAT altera o endereço de origem de cada pacote para um endereço IP público com diferentes portas de origem.



Para resolver esses problemas, o SIP oferece suporte a três técnicas NAT diferentes:

- STUN – É uma maneira de perguntar a um servidor em um local conhecido qual é o endereço público da unidade. O servidor STUN retorna o IP público e o mapeamento de porta usado para fazer a solicitação. Depois, o resultado é usado na sinalização e na transferência de mídia, o que funciona na maioria das situações.
- TURN – Ao usar TURN, todo o tráfego é retransmitido por meio de um servidor conhecido. Isso cria uma sobrecarga extra, pois a máquina que hospeda o servidor TURN deve ser poderosa o suficiente para rotear todas as mídias para cada cliente usando o serviço. Essa é uma solução mais cara, mas pode funcionar em algumas situações que fogem do escopo do STUN.
- ICE – O protocolo ICE reúne todos os endereços IP que consegue encontrar relacionados a um UA SIP e, em seguida, tenta calcular qual deles deve ser usado. Quando usado em combinação com STUN e TURN tanto no UA SIP inicial quanto no receptor, aumenta as chances de estabelecer chamadas SIP com sucesso.

6.2 Usar criptografia com SIP

O tráfego de sinalização SIP normalmente é enviado pelo protocolo UDP sem conexão. Também pode ser enviado por TCP e, nesse caso, pode também ser criptografado com Transport Layer Security (TLS).

Para garantir que uma conexão segura seja usada em uma chamada, o protocolo SIP usa um esquema de endereçamento chamado Secure SIP (SIPS), que exige que o modo de transporte seja definido como TLS. Ao fazer uma chamada, o endereço SIP discado recebe o prefixo "sips:" em vez de "sip". Por exemplo: sips:bob@biloxi.ex.com em vez de sip:bob@biloxi.ex.com. Isso exige que cada salto seja protegido com TLS e que a extremidade receptora aplique o mesmo nível de segurança. Chamar um endereço com prefixo sip usando TLS garante apenas que o primeiro salto seja criptografado.

Para obter o mais alto nível de segurança, as seguintes medidas devem ser adotadas:

- O modo de transporte deve ser definido como TLS.
- O prefixo sips deve ser usado em todos os momentos.
- SIP INFO deve ser usado para enviar tons DTMF, pois isso é enviado no canal criptografado.

Observe que nem todos os clientes oferecem suporte a Secure SIP.

7 Terminologia SIP

API	Interface de programação de aplicativo
Codec	Codificador-decodificador
Hardphone	Hardware que faz ligações telefônicas, ou seja, um telefone
ICE	Interactive Connectivity Establishment
IP	Internet Protocol
Cliente móvel	Software em um dispositivo móvel que faz chamadas telefônicas
NAT	Network Address Translation
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network, ou seja, uma rede telefônica comum
RTP	Real-time Transport Protocol
SDP	Session Description Protocol
SIM	Subscriber Identity Module
SIP	Protocolo de iniciação de sessão
Servidor SIP	Componente principal de um IP PBX. Responsável pela configuração e finalização de chamadas. Também é chamado de SIP proxy ou de registrador.
SIPS	Secure SIP
URI SIP (endereço SIP)	Uniform Resource Identifier. O endereço exclusivo do UA SIP.
Softphone	Software que faz chamadas telefônicas
STUN	Session Traversal Utilities for NAT
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TURN	Traversal Using Relays around NAT
UA	User agent. As duas extremidades de uma sessão de comunicação.
UC	Comunicações unificadas
UDP	User Datagram Protocol
VoIP	Voice over IP

Sobre a Axis Communications

A Axis torna possível um mundo mais inteligente e seguro criando soluções para melhorar a segurança e o desempenho dos negócios. Como empresa de tecnologia de rede e líder do setor, a Axis oferece soluções em videomonitoramento, controle de acesso, intercomunicação e áudio. Nossas soluções são aprimoradas por aplicativos de análise inteligentes e apoiados por treinamento de alta qualidade.

A Axis tem cerca de 4.000 funcionários dedicados em mais de 50 países e colabora com parceiros de tecnologia e integração de sistemas em todo o mundo para fornecer soluções aos clientes. A Axis foi fundada em 1984 e tem sede em Lund, Suécia