WHITE PAPER

SIP — Un'Introduzione

Settembre 2024

Sommario

Il protocollo SIP (Session Initiation Protocol) fornisce un'interfaccia aggiuntiva per l'integrazione dei dispositivi di sicurezza nel sistema. SIP è uno standard largamente adottato nel settore delle telecomunicazioni e offre una maggiore flessibilità per l'interconnettività e l'uso quotidiano. Le interfacce aperte e standardizzate, richieste da integratori di sistemi, sviluppatori e utenti finali, aumentano il valore offerto perché i dispositivi si possono utilizzare in vari sistemi. I dispositivi Axis che supportano SIP sono concepiti per essere utilizzati sia nelle soluzioni di sicurezza che in quelle di comunicazione.

Configurare un sistema SIP può essere facile. Tuttavia, in caso di topologie di rete complesse, requisiti di sicurezza particolari e funzionalità supplementari di gestione delle chiamate, è necessario utilizzare server SIP e tecniche di attraversamento NAT, che richiedono competenze maggiori da parte dell'installatore o del tecnico.

Sommario

1 Introduzione

Il SIP (Session Initiation Protocol) viene utilizzato per avviare, mantenere e terminare sessioni multimediali tra diverse parti. Normalmente, le sessioni sono costituite da audio, ma a volte contengono anche video. SIP è il protocollo standard utilizzato dalle applicazioni Voice over IP (VoIP) e dalle piattaforme Unified Communications (UC) (vedere Capitolo 3).

SIP è un modo per collegare, integrare e controllare i tuoi dispositivi di rete Axis. È supportato da tutti gli altoparlanti di rete Axis, da tutti gli intercom di rete Axis e da alcuni dispositivi di sistema Axis e telecamere Axis.

2 Come funziona?

Per comunicare tramite SIP, sono necessari almeno due client SIP. Un client SIP può essere un telefono fisso SIP, un telefono virtuale, un client per dispositivi mobili, o un dispositivo Axis compatibile con SIP.

A ogni client SIP viene assegnato il proprio indirizzo SIP. Un indirizzo SIP è simile a un indirizzo email, ma con il prefisso "sip:".

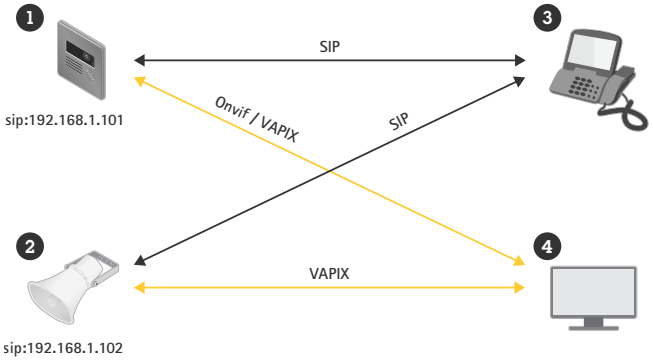
Ad esempio, sip:bob@axis.com [sip:<utente@]<provider>. Questo identificativo può essere utilizzato con vari dispositivi ed è analogo al numero di telefono di una scheda SIM, utilizzabile su diversi dispositivi.

2.1 Configurazione Peer-to-Peer: il metodo più semplice

Un sistema SIP può assumere molte forme. In quella più semplice, il sistema è costituito da due o più User Agent (UA) SIP che comunicano direttamente tra loro. Questa configurazione è detta peer-to-peer, a chiamata diretta o locale. In questo caso, un tipico indirizzo SIP assume il formato sip:<ip locale>, ad esempio, sip:192.168.0.90.

Esempio: In una configurazione semplice, i dispositivi Axis (1, 2) possono utilizzare il protocollo SIP per impostare una comunicazione audio e/o video con altri dispositivi SIP (3) nella stessa rete, senza la necessità di un server o un PBX.

Al tempo stesso, possono essere collegati come tutti gli altri dispositivi Axis al sistema di gestione video (4) utilizzando le API aperte VAPIX o ONVIF Profile S.



Per effettuare una chiamata peer-to-peer da un UA all'altro su una rete locale, è sufficiente avere l'indirizzo SIP contenente l'indirizzo IP dell'unità.

2.2 Uso di un server SIP (PBX) – aggiunta di possibilità

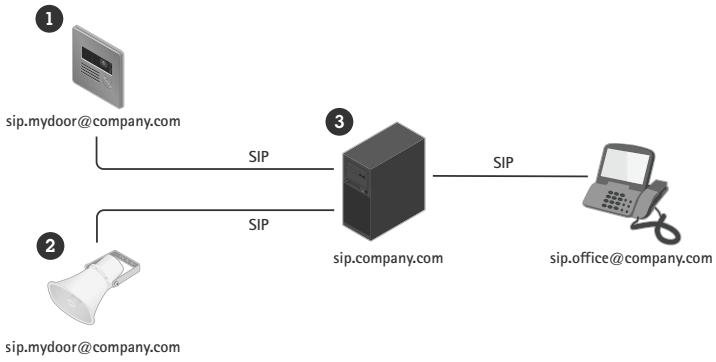
Un'infrastruttura VoIP basata su SIP è molto scalabile. Il passo successivo in termini di dimensioni, è l'utilizzo di un server SIP, o Private Branch Exchange (PBX), come hub centrale. Gli UA SIP si registrano con il registrar server e possono quindi raggiungere l'altro UA semplicemente componendo un interno sul PBX.

In questo caso, un normale indirizzo SIP assumerebbe la forma sip:<utente>@<dominio>. In alternativa, potrebbe essere sip:<utente>@<ip registrar>, ad esempio sip:6007@ mysipserver.net. Un PBX funziona come un tradizionale centralino: mostra lo stato attuale dei client, consentendo i trasferimenti di chiamata, la segreteria telefonica, i reindirizzamenti e molto altro.

Di norma, un server SIP include funzionalità proxy, registrar e di reindirizzamento. I proxy instradano le chiamate e applicano una logica supplementare alle chiamate in arrivo. I registrar accettano le richieste di registrazione e fungono da servizio di localizzazione per il dominio che gestiscono. I server di reindirizzamento reindirizzano il client per contattare un indirizzo SIP alternativo.

Il server SIP può essere configurato come entità locale o off-site. Può essere ospitato localmente o nel cloud. Quando si effettuano chiamate SIP tra siti diversi, all'inizio le chiamate vengono instradate normalmente tramite una serie di proxy SIP. I proxy eseguono una query sulla posizione dell'indirizzo SIP da raggiungere.

Esempio: I prodotti Axis (1, 2) possono collegarsi a un server SIP (3) locale o esterno. Il server gestisce l'impostazione e la terminazione delle chiamate tra dispositivi SIP sulla rete locale o su Internet. Con questa configurazione, l'indirizzo SIP del dispositivo è indipendente dal suo indirizzo IP e il server SIP rende accessibile il dispositivo finché è registrato sul server.



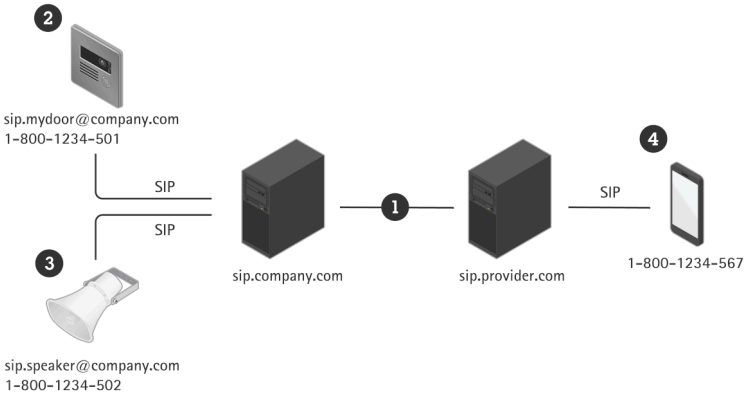
Per utilizzare un dispositivo con un server SIP, è necessario creare un account sul server con un ID utente e una password specifici. Per registrare il dispositivo sul server, è necessario configurare un account sul dispositivo inserendo l'indirizzo del server, l'ID utente e la password.

2.3 Uso di un trunk SIP – assegnazione di un numero di telefono

Utilizzando un trunk SIP, gli UA SIP possono essere commutati sulla rete telefonica tradizionale (PSTN). In questo modo è anche possibile assegnare un numero di telefono regolare all'UA SIP.

Il trunk SIP basato su cloud è un approccio moderno che sfrutta Internet per fornire chiamate e altri servizi di comunicazione. Questo metodo elimina la necessità di linee telefoniche fisiche, facilitando l'integrazione con soluzioni cloud e sistemi VoIP.

Esempio: Utilizzando un trunk SIP (1) con un service provider, è possibile assegnare numeri di telefono esterni ai dispositivi (2, 3). In questo modo, è possibile effettuare chiamate tra un altoparlante o un intercom di rete e i normali telefoni (4).



Se utilizzato con un trunk SIP, il dispositivo si connette al server come descritto sopra.

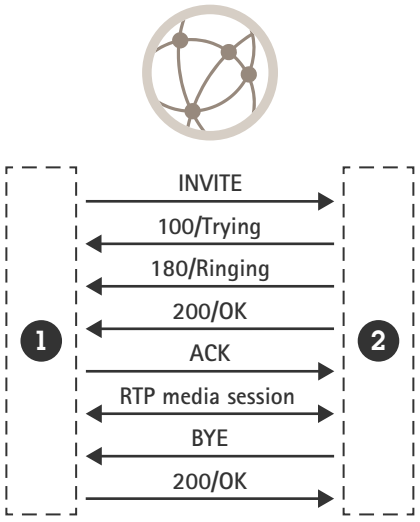
3 Unified Communications (UC)

Le Unified Communications (UC) si riferiscono all'integrazione di vari strumenti e tecnologie di comunicazione in un unico sistema coeso. Il SIP svolge un ruolo fondamentale nelle UC, in quanto consente la perfetta interazione di diversi canali di comunicazione, come voce, video, messaggistica istantanea e informazioni sulla presenza. Sfruttando il SIP, le società possono creare un ambiente di comunicazione unificato che migliora la collaborazione, aumenta la produttività e offre un'esperienza utente coerente su più dispositivi e piattaforme.

Le UC possono essere fornite in soluzioni locali o tramite cloud (UC as a service - UCaaS). Esempi di service provider per le soluzioni cloud sono Cisco Webex, Microsoft Teams e Zoom.

4 Funzionamento di una chiamata SIP normale

Per effettuare una chiamata SIP viene eseguita una sequenza di passaggi per lo scambio di informazioni tra l'UA che inizia e quello riceve la chiamata.



Quando si avvia una chiamata, l'UA di inizio (1) invia una richiesta (o INVITE) all'indirizzo SIP dell'UA destinatario (2). L'INVITE contiene un corpo SDP (Session Description Protocol) che descrive i formati multimediali disponibili e le informazioni di contatto per l'iniziatore della chiamata.

Dopo aver ricevuto l'INVITE, il destinatario lo riconosce immediatamente e risponde con 100 TRYING.

Quindi, l'UA ricevente confronta i formati multimediali offerti e descritti nell'SDP con i propri. Se è possibile decidere un formato comune, l'UA avverte il destinatario che è in arrivo una chiamata e invia una risposta provvisoria all'UA di inizio - 180 RINGING.

Quando il destinatario risponde alla chiamata, viene inviata una risposta all'iniziatore (200 OK) per confermare che è stata stabilita una connessione. La risposta contiene un SDP negoziato che indica all'iniziatore i formati multimediali da utilizzare e dove inviare i flussi multimediali.

Ora, i flussi multimediali negoziati sono configurati utilizzando il protocollo RTP (Real-Time Transport Protocol) con parametri basati sull'SDP negoziato e i media viaggiano direttamente tra le due parti. L'iniziatore invia una conferma (ACK) tramite SIP per attestare che ha configurato i flussi multimediali come concordato. La sessione SIP è ancora attiva ma non è più coinvolta nel trasferimento multimediale.

Quando una delle parti decide di terminare la chiamata, invia una nuova richiesta – BYE. Dopo aver ricevuto il BYE, la parte ricevente conferma con 200 OK e i flussi multimediali RTP vengono interrotti.

4.1 SDP – negoziazione del formato da utilizzare

Session Description Protocol (SDP) è un formato che descrive i parametri di inizializzazione dei media in streaming. Il corpo dell'SDP contiene informazioni sui formati multimediali (ovvero i codec) supportati dai client e sull'ordine di selezione dei codec preferito dai client.

I codec audio più comuni utilizzati per le chiamate SIP sono PCMU, PCMA, G.722, G.726 e L16. Se l'iniziatore e il destinatario supportano più codec sovrapposti, in genere viene selezionato il codec con la priorità più alta sul lato del destinatario. Poiché la scelta dei codec influisce sulla larghezza di banda, occorre un'attenta valutazione per soddisfare i requisiti di compatibilità con altri UA SIP e per mantenere la larghezza di banda necessaria per l'applicazione. Ad esempio, se in una rete locale tutti i client supportano L16, scegliere l'audio non compresso offre buoni risultati. Tuttavia, se occorre accedere a un UA SIP via Internet tramite un telefono cellulare, è meglio scegliere PCMU.

4.2 Chiamate in infrastrutture SIP complesse

In un'infrastruttura SIP più complessa, l'inizio è leggermente diverso perché la sessione SIP viene impostata passo dopo passo per ciascun hop. Tuttavia, una volta impostata la sessione SIP, normalmente il traffico non viene instradato, ma viaggia direttamente tra le varie parti come nell'esempio precedente.

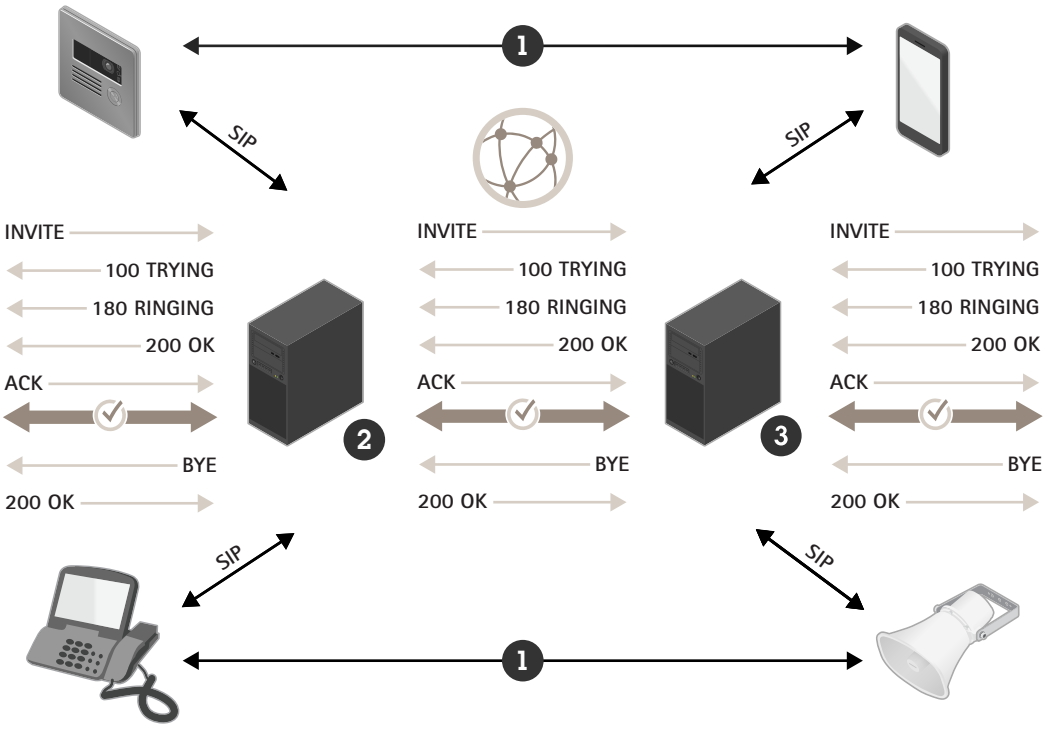


Figure 1. Configurazione di una chiamata in un'infrastruttura SIP complessa. I flussi multimediali RTP (1) viaggiano direttamente tra le parti una volta impostata la sessione SIP tra l'iniziatore (2) e il destinatario (3).

5 DTMF: invio di comandi nelle chiamate SIP

Dual-Tone Multiple-Frequency (DTMF) è un formato utilizzato per inviare informazioni su una connessione telefonica. I segnali DTMF possono essere inviati nelle chiamate SIP ed essere utilizzati per dare istruzioni a un dispositivo SIP. L'intervallo di caratteri DTMF è costituito da numeri (0-9), lettere (A-D), * e #.

Ad esempio, in una chiamata a un interfono compatibile con SIP, dalla tastiera del telefono può essere inviato il carattere DTMF "5", che può essere configurato affinché il ricevente lo interpreti come comando di apertura della porta.

Esistono tre modi per inviare DTMF in una chiamata SIP:

- Il metodo tradizionale in banda, in cui il segnale è in realtà un impulso audio miscelato con il flusso audio. Tuttavia, questo metodo non è affidabile e funziona solo con i codec non compressi.
- Il metodo SIP INFO, in cui il carattere DTMF viene inviato in un messaggio SIP nel flusso di segnalazione. Questo metodo è molto affidabile e fuori banda, ma è supportato solo limitatamente.
- Il metodo RTP (RFC2833), in cui il carattere DTMF viene codificato come pacchetto RTP e inviato fuori banda. È lo standard de facto e gode di un ampio supporto.

6 Ambienti complessi e maggiore sicurezza

Gli ambienti di rete complessi, come le reti aziendali, possono rendere difficoltoso l'uso di SIP. Lo stesso vale se si desidera utilizzare la crittografia.

6.1 Attraversamento NAT: navigazione in reti complesse

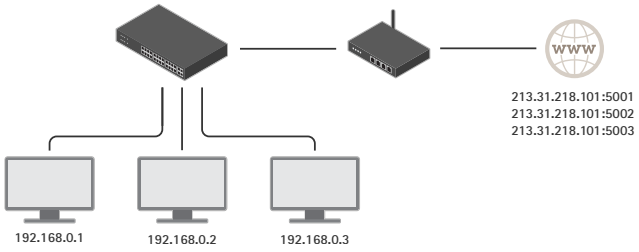
In un ambiente di rete più complesso, può essere necessario utilizzare NAT (Network Address Translation), una tecnica che rappresenta pubblicamente gli indirizzi IP ubicati su una rete locale privata. Questo significa che tutte le unità di una sottorete privata hanno un prefisso comune dell'indirizzo IP, ad esempio 192.168.1.XXX: si tratta dell'indirizzo che utilizzano quando comunicano tra loro. Quando comunicano con un'altra rete, questo indirizzo viene convertito nell'indirizzo pubblico del router, al quale viene aggiunta una mappatura delle porte.

- 192.168.1.24 => 184.13.12.33:44221
- 192.168.1.121 => 184.13.12.33:24325, e così via.

Poiché la tabella di traduzione è memorizzata nel router, nella maggior parte dei casi non è possibile che un utente esterno conosca l'indirizzo di un dispositivo NAT:ed. Quando si comunica tramite SIP, questo può causare uno dei seguenti problemi:

- Impossibile iniziare, aggiornare o terminare una sessione, ovvero non è possibile chiamare, mettere in attesa o riagganciare.
- Nessun flusso multimediale.
- Flussi multimediali unidirezionali.

Attraversamento NAT: NAT converte l'indirizzo di origine di ciascun pacchetto in un indirizzo IP pubblico con diverse porte di origine.



Per risolvere questi problemi, SIP supporta tre tecniche NAT:

- STUN - Metodo utilizzato per chiedere a un server in una posizione nota l'indirizzo pubblico dell'unità. Il server STUN restituisce l'IP pubblico e la mappatura delle porte utilizzati per effettuare la richiesta. Quindi, il risultato viene utilizzato nella segnalazione e nel trasferimento multimediale: questa tecnica funziona nella maggior parte dei casi.
- TURN: utilizzando TURN, tutto il traffico viene inoltrato tramite un server noto. Questo impone un carico aggiuntivo, perché la macchina che ospita il server TURN deve avere una potenza sufficiente da instradare tutti i media per ogni client che utilizza il servizio. La soluzione è più costosa, ma può essere utile in alcuni casi quando STUN non funziona.
- ICE – Il protocollo ICE raccoglie tutti gli indirizzi IP che riesce a trovare e che sono correlati a un UA SIP, quindi prova a calcolare quale utilizzare. Se utilizzato in combinazione con STUN e TURN sia sull'UA SIP di inizio che su quello ricevente, aumenta le possibilità di effettuare le chiamate SIP.

6.2 Uso della crittografia con SIP

Normalmente, il traffico di segnalazione SIP viene inviato tramite il protocollo UDP senza connessione. Può anche essere inviato tramite TCP; in questo caso può anche essere crittografato mediante TLS (Transport Layer Security).

Per garantire l'uso di una connessione protetta per una chiamata, il protocollo SIP utilizza uno schema di indirizzamento denominato Secure SIP (SIPS), che richiede l'impostazione della modalità di trasporto su TLS. Quando si effettua una chiamata, l'indirizzo SIP composto è preceduto da "sips:" anziché "sip", ad esempio sips:bob@biloxi.ex.com invece di sip:bob@biloxi.ex.com. Questo impone che ogni hop sia protetto mediante TLS e che l'estremità ricevente utilizzi lo stesso livello di sicurezza. La chiamata a un indirizzo con prefisso sip quando si utilizza TLS garantisce solo che il primo hop sia crittografato.

Per ottenere il massimo livello di sicurezza, occorre adottare le seguenti misure:

- La modalità di trasporto deve essere impostata su TLS.
- Deve sempre essere utilizzato il prefisso sips.
- È necessario utilizzare SIP INFO per inviare toni DTMF, che seguono un canale crittografato.

Nota: non tutti i client supportano Secure SIP.

7 SIP: terminologia

API	Application Programming Interface
Codec	COdificatore-DECofidicatore
Telefono fisico	Hardware che effettua chiamate telefoniche, ovvero un telefono
ICE	Interactive Connectivity Establishment
IP	Internet Protocol
Client mobile	Programma software su dispositivo mobile che effettua chiamate telefoniche
NAT	Network Address Translation
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network, ovvero la normale rete telefonica

RTP	Real-time Transport Protocol
SDP	Session Description Protocol
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
Server SIP	Componente principale di un IP PBX. Gestisce l'impostazione e la chiusura delle chiamate. È anche detto proxy o registrar SIP.
SIPS	Secure SIP
URI SIP (indirizzo SIP)	Uniform Resource Identifier. Indirizzo univoco dell'UA SIP.
Telefono virtuale	Programma software che effettua chiamate telefoniche
STUN	Session Traversal Utilities for NAT
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TURN	Traversal Using Relays around NAT
UA	User agent. I due endpoint di una sessione di comunicazione.
UC	Unified Communications
UDP	User Datagram Protocol
VoIP	Voice over IP

T10175991/IT/M4.6/2409

Informazioni su Axis Communications

Axis consente un mondo più intelligente e più sicuro creando soluzioni per migliorare la sicurezza e le prestazioni aziendali. Come società di tecnologie di rete e leader nel settore, Axis offre soluzioni nella videosorveglianza, controllo degli accessi, interfono e sistemi audio. Queste sono ottimizzate da applicazioni di analisi intelligente e supportate da formazione di alta qualità.

Axis ha circa 4.000 impiegati dedicati in più di 50 paesi e collabora con partner di tecnologia e integrazione di sistema in tutto il mondo per offrire soluzioni di clienti. Fondata nel 1984, Axis e con sede a Lund, in Svezia