BIAŁA KSIĘGA

SIP — wprowadzenie

Wrzesień 2024

AXIS COMMUNICATIONS

Streszczenie

Protokół SIP (Session Initiation Protocol — protokół inicjowania sesji) jest dodatkowym interfejsem systemowej integracji produktów z obszaru bezpieczeństwa. SIP to standard powszechnie stosowany w branży telekomunikacyjnej, który zapewnia większą elastyczność w obszarach wzajemnych połączeń i codziennego użytkowania. Integratorzy systemów, programiści i użytkownicy domagają się otwartych, standardowych interfejsów, które zapewniają większe korzyści dzięki możliwości stosowania produktów w różnych systemach. Produkty Axis z obsługą protokołu SIP mogą być używane w rozwiązaniach z zakresu bezpieczeństwa i łączności.

System SIP może być stosunkowo łatwy w konfiguracji. Jednak w przypadku sieci o skomplikowanej topologii albo w sytuacji, gdy potrzebne są dodatkowe zabezpieczenia i funkcje obsługi połączeń, trzeba zastosować serwer SIP oraz techniki przechodzenia NAT, które od instalatora lub technika wymagają szerszej wiedzy technicznej.

Spis treści

1 Wprowadzenie

Protokół SIP (Session Initiation Protocol — protokół inicjowania sesji) służy do nawiązywania, utrzymywania i kończenia sesji multimedialnych między różnymi stronami. Zazwyczaj są to sesje dźwiękowe, ale czasem obejmują one również materiał wizyjny. SIP jest standardowym protokołem używanym w aplikacjach Voice over IP (VoIP) i na platformach Unified Communications (UC) (patrz sekcja 3).

Protokół SIP jest sposobem łączenia, integrowania i kontrolowania produktów sieciowych Axis. Obsługują go wszystkie głośniki sieciowe Axis, wszystkie interkomy sieciowe Axis oraz wybrane urządzenia systemowe i kamery Axis.

2 Zasada działania

Do komunikacji opartej na protokole SIP potrzeba co najmniej dwóch klientów SIP. Klientem SIP może być telefon IP lub aplikacja typu softphone, klient mobilny albo produkt Axis obsługujący protokół SIP.

Każdy klient SIP otrzymuje własny adres. Adres SIP przypomina adres e-mail, ale zaczyna się od prefiksu „sip:".

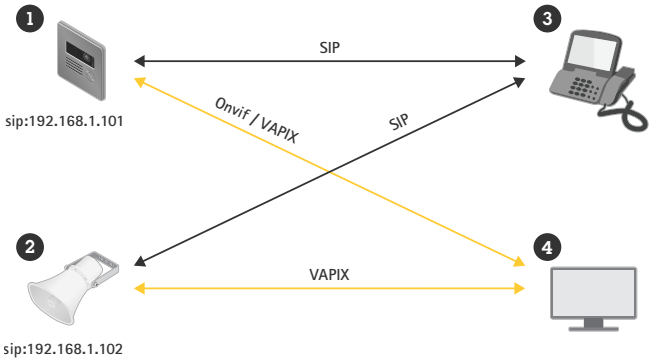
Na przykład: sip:robert@axis.com [sip:<użytkownik@]<dostawca>. Ten identyfikator może być używany na wielu urządzeniach i działa podobnie jak numer telefonu powiązany z kartą SIM, z którego można korzystać na wielu urządzeniach.

2.1 Konfiguracja peer-to-peer — najprostszy sposób

System SIP może mieć wiele postaci. W najprostszej z nich składa się z dwóch lub większej liczby agentów użytkowników SIP, którzy komunikują się ze sobą bezpośrednio. Jest to tzw. konfiguracja peer-to-peer, konfiguracja połączeń bezpośrednich lub konfiguracja lokalna. W takim przypadku typowy adres SIP ma postać sip:<ip-lokalny>, na przykład sip:192.168.0.90

Przykład: W przedstawionej prostej konfiguracji produkty Axis (1, 2) mogą używać protokołu SIP do zestawiania połączeń audio i/lub wideo z innymi urządzeniami SIP (3) w tej samej sieci, nie potrzebując do tego serwera ani centrali PBX.

Jednocześnie można je połączyć tak jak każde inne urządzenie Axis z systemem zarządzania materiałem wizyjnym (4), korzystając z otwartych interfejsów API VAPIX lub profilu ONVIF S.



Aby jeden agent użytkownika mógł nawiązać połączenie peer-to-peer z drugim agentem w sieci lokalnej, wystarczy adres SIP zawierający adres IP odpowiedniego urządzenia.

2.2 Korzystanie z serwera SIP (centrali PBX) — dodatkowe możliwości

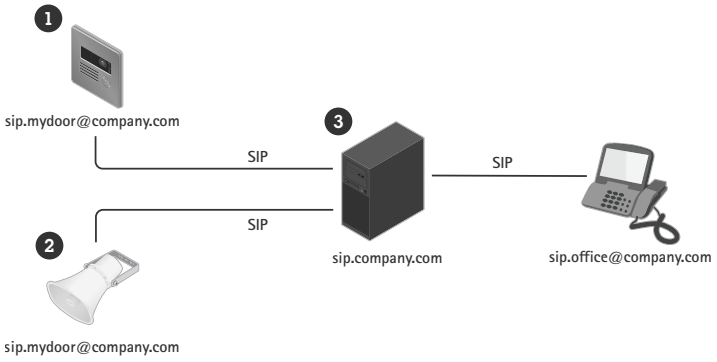
Infrastruktura VoIP oparta na protokole SIP umożliwia bardzo łatwe skalowanie. Kolejnym krokiem w rozbudowie systemu jest użycie serwera SIP lub centrali abonenckiej (Private Branch Exchange — PBX) jako swego rodzaju hubu komunikacyjnego. Wówczas agenci użytkowników SIP rejestrują się w rejestratorze serwera, a następnie mogą uzyskać dostęp do każdego innego agenta przez wybranie odpowiedniego numeru wewnętrznego w centrali PBX.

W takim przypadku typowy adres SIP ma postać sip:<użytkownik>@<domena>. Ewentualnie adres może mieć formę sip:<użytkownik>@<ip-rejestratora>, na przykład sip:6007@mojserwersip.net. Centrala PBX działa tak jak tradycyjna centrala telefoniczna, pokazując aktualny status klientów oraz udostępniając funkcje przekazywania połączeń, poczty głosowej, przekierowania i wiele innych.

Serwer SIP zazwyczaj obejmuje funkcje serwera proxy, rejestratora i przekierowywania połączeń. Serwer proxy trasuje połączenia i udostępnia dodatkowe funkcje logiczne do obsługi połączeń przychodzących. Rejestrator przyjmuje żądania rejestracji i działa jako usługa lokalizacji na potrzeby obsługiwanej przez siebie domeny. Serwer przekierowań przekierowuje klientów na alternatywny adres SIP.

Serwer SIP można skonfigurować jako urządzenie lokalne lub umieścić w lokalizacji zewnętrznej. Może on znajdować się w środowisku lokalnym lub w chmurze. Jeśli połączenie SIP jest wykonywane między lokalizacjami, w normalnych warunkach jest ono początkowo zestawiane przy użyciu kilku serwerów proxy SIP. Serwery te uzyskują informacje o lokalizacji docelowego adresu SIP.

Przykład: Produkty Axis (1, 2) mogą łączyć się z serwerem SIP (3) lokalnie lub poza siedzibą firmy. Serwer obsługuje zestawianie i kończenie połączeń między urządzeniami SIP w sieci lokalnej lub Internecie. W tej konfiguracji adres SIP urządzenia jest niezależny od jego adresu IP, a serwer SIP udostępnia urządzenie przez cały czas, w którym jest ono zarejestrowane na serwerze.



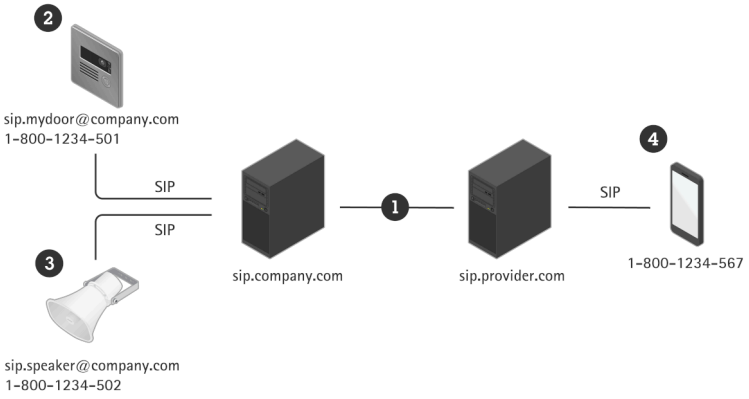
Aby umożliwić używanie urządzenia z serwerem SIP, należy utworzyć na serwerze konto za pomocą określonego identyfikatora użytkownika i hasła. Aby zarejestrować urządzenie na serwerze, należy na urządzeniu skonfigurować konto, wprowadzając adres serwera, identyfikator użytkownika i hasło.

2.3 Korzystanie z magistrali SIP — przypisywanie numeru telefonu

W przypadku korzystania z magistrali SIP agenci użytkowników SIP mogą być przełączani na tradycyjną sieć telefoniczną (PSTN). W ten sposób agentowi użytkownika SIP można przypisać zwykły numer telefoniczny.

Magistrale SIP oparte na chmurze to nowoczesne podejście, które wykorzystuje Internet do obsługi połączeń telefonicznych i dostarczania innych usług komunikacyjnych. Ta metoda eliminuje potrzebę stosowania fizycznych linii telefonicznych, ułatwiając integrację z rozwiązaniami chmurowymi i systemami VoIP.

Przykład: W przypadku korzystania z magistrali SIP (1) udostępnionej przez usługodawcę można przypisać zewnętrzne numery telefonów swoim urządzeniom (2, 3). Pozwala to nawiązywać połączenia między głośnikiem sieciowym lub interkomem sieciowym i zwykłymi telefonami (4).



Jeśli urządzenie jest używane z magistralą SIP, łączy się z serwerem w wyżej opisany sposób.

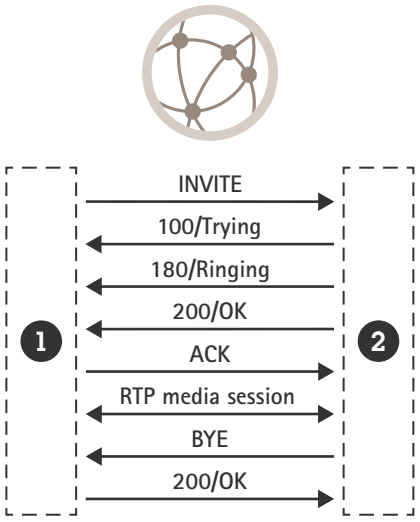
3 Unified Communications (UC)

Określenie Unified Communications (UC) odnosi się do integracji różnych narzędzi i technologii komunikacyjnych w jeden spójny system. Istotną rolę w platformach UC odgrywa protokół SIP, który umożliwia płynną interakcję między różnymi kanałami komunikacji, takimi jak głos, wideo, wiadomości błyskawiczne i informacje o obecności. Wykorzystując SIP, organizacja może stworzyć ujednolicone środowisko komunikacyjne, które usprawnia współpracę, zwiększa produktywność oraz zapewnia spójne wrażenia użytkowe na wielu urządzeniach i platformach.

Funkcje UC mogą być dostarczane lokalnie przez rozwiązania działające w siedzibie firmy lub za pośrednictwem rozwiązań chmurowych (UC as a service — UCaaS). Przykładowi usługodawcy w zakresie rozwiązań chmurowych to Cisco Webex, Microsoft Teams i Zoom.

4 Wnętrze normalnego połączenia SIP

W celu nawiązania połączenia SIP wykonywana jest pewna sekwencja kroków, które mają na celu wymianę informacji między agentem użytkownika inicjującym oraz odbierającym połączenie.



Na etapie inicjowania połączenia agent-inicjator (1) wysyła żądanie, czyli zaproszenie (INVITE), na adres SIP agenta-odbiorcy (2). Zaproszenie zawiera treść wiadomości SDP, która opisuje dostępne formaty multimediów i podaje dane kontaktowe inicjatora połączenia.

Po otrzymaniu zaproszenia odbiorca natychmiast ją potwierdza, wysyłając odpowiedź 100 TRYING (próba).

Następnie agent odbierający porównuje proponowane formaty multimediów wymienione w wiadomości SDP z własnymi. Jeśli można uzgodnić wspólny format, agent użytkownika powiadamia odbiorcę o połączeniu przychodzącym i wysyła tymczasową odpowiedź 180 RINGING (dzwonienie) do agenta inicjującego.

Gdy odbiorca faktycznie odbierze połączenie, do inicjatora wysyłana jest odpowiedź 200 OK, która potwierdza nawiązanie połączenia. Odpowiedź ta zawiera wynegocjowaną wiadomość SDP, która wskazuje inicjatorowi, jakich formatów multimediów powinien używać i gdzie ma wysyłać strumienie multimedialne.

Wynegocjowane strumienie multimedialne są zestawiane przy użyciu protokołu RTP (Real-time Transport Protocol) z parametrami opartymi na wynegocjowanej wiadomości SDP, a multimedia są przekazywane bezpośrednio między obiema stronami. Inicjator wysyła za pośrednictwem protokołu SIP potwierdzenie (ACK), że zestawił strumienie multimedialne w uzgodniony sposób. Sesja SIP pozostaje aktywna, ale nie jest już wykorzystywana do transferu multimediów.

Gdy jedna ze stron postanowi zakończyć połączenie, wysyła nowe żądanie, czyli BYE. Po jego otrzymaniu odbiorca potwierdza ten fakt komunikatem 200 OK, co powoduje zatrzymanie strumieni multimedialnych RTP.

4.1 SDP — negocjowanie właściwego formatu

SDP (Session Description Protocol — protokół opisu sesji) to format opisu parametrów służących do inicjowania sesji strumieniowego przesyłania multimediów. Treść wiadomości SDP zawiera informacje na

temat formatów multimediów (czyli kodeków) obsługiwanych przez klientów oraz preferowanej przez klientów kolejności wyboru kodeków.

Do typowych kodeków audio używanych podczas połączeń SIP należą PCMU, PCMA, G.722, G.726 i L16. Jeśli inicjator i odbiorca obsługują wiele kodeków, w normalnych warunkach wybierany jest kodek o najwyższym priorytecie po stronie odbiorcy. Wybór kodeków ostatecznie przekłada się na przepustowość, więc należy się nad nim dobrze zastanowić, aby zapewnić zgodność z innymi agentami użytkowników SIP i spełnić wymagania dotyczące przepustowości, które wiążą się z danym zastosowaniem. Przykładowo w sieci lokalnej, w której wszyscy klienci obsługują format L16, uzasadniony będzie wybór nieskompresowanego audio. Jeśli jednak dostęp do agenta użytkownika SIP ma być uzyskiwany przez Internet przy użyciu telefonu komórkowego, lepszym wyborem będzie format PCMU.

4.2 Połączenia w złożonej infrastrukturze SIP

W infrastrukturze SIP o bardziej złożonej konfiguracji inicjowanie wygląda nieco inaczej, ponieważ sesja jest zestawiana krok po kroku dla każdego przeskoku. Jednak po zestawieniu sesji SIP ruch zazwyczaj nie jest trasowany, ale przepływa bezpośrednio między poszczególnymi stronami, tak jak w poprzednim przykładzie.

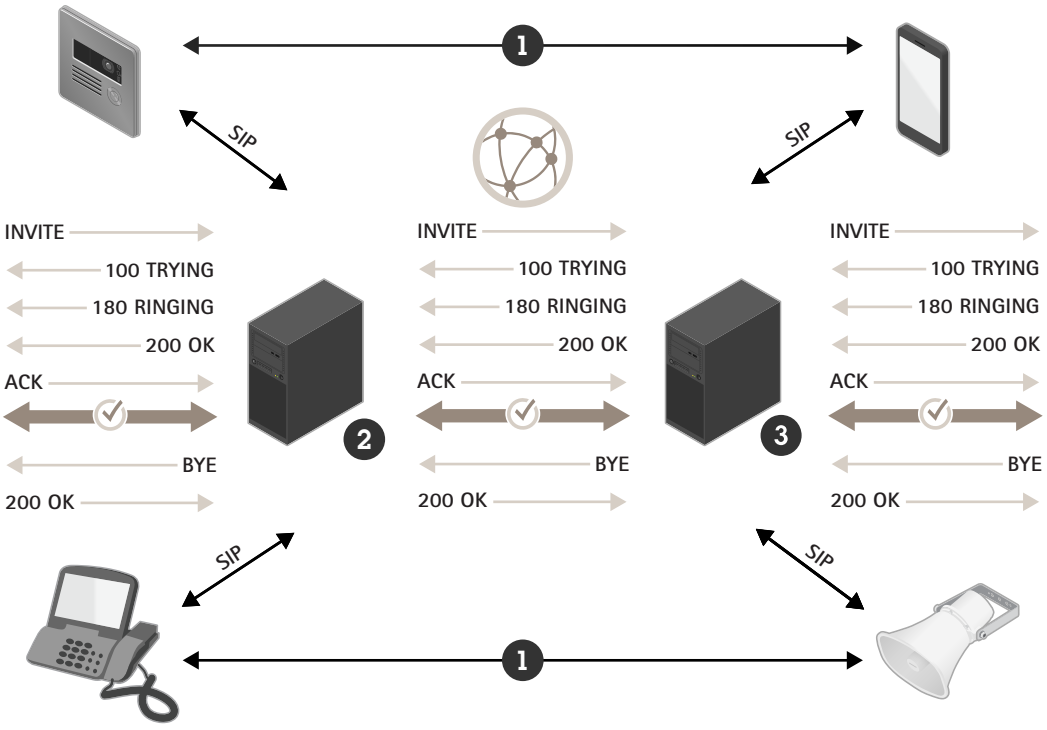


Figure 1. Połączenie zestawione w złożonej infrastrukturze SIP. Strumienie multimedialne RTP (1) przepływają bezpośrednio między stronami po zestawieniu sesji SIP między inicjatorem (2) a odbiorcą (3).

5 DTMF — wysyłanie poleceń w połączeniach SIP

DTMF (Dual-Tone Multiple-Frequency) to format używany do wysyłania informacji w ramach połączeń telefonicznych. Sygnały DTMF mogą być też wysyłane w połączeniach SIP w celu przekazywania poleceń urządzeniom SIP. Pula znaków DTMF obejmuje cyfry 0–9, litery A–D oraz symbole * i #.

Przykładowo podczas połączenia z interkomem SIP można z klawiatury telefonu wysłać znak DTMF „5", który odbiornik zgodnie ze swoją konfiguracją zinterpretuje jako polecenie otwarcia drzwi.

Istnieją trzy sposoby wysyłania sygnałów DTMF w ramach połączenia SIP:

- Tradycyjna metoda wewnątrzpasmowa, gdzie sygnał jest po prostu impulsem dźwiękowym wplecionym w strumień audio. Jest to jednak metoda zawodna, która działa tylko z nieskompresowanymi kodekami.
- Metoda SIP INFO, gdzie znak DTMF jest wysyłany w wiadomości SIP w ramach strumienia sygnalizacji. Jest to metoda bardzo niezawodna i pozapasmowa, ale jej wsparcie jest ograniczone.
- Metoda RTP (RFC2833), gdzie znak DTMF jest kodowany jako pakiet RTP i wysyłany poza pasmem. Ta metoda jest de facto standardem i cieszy się szerokim wsparciem.

6 Złożone środowiska i większe bezpieczeństwo

Złożone środowiska sieciowe, na przykład sieci firmowe, mogą utrudniać stosowanie protokołu SIP. To samo dotyczy korzystania z szyfrowania.

6.1 Przechodzenie przez NAT — poruszanie się po złożonych sieciach

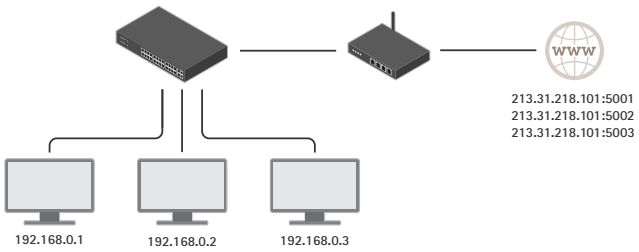
W bardziej złożonym środowisku sieciowym może wystąpić potrzeba skorzystania z techniki tłumaczenia adresów sieciowych (Network Address Translation — NAT). Zapewnia ona publiczną reprezentację adresów IP znajdujących się w prywatnej sieci lokalnej. W takim przypadku wszystkie jednostki znajdujące się w podsieci prywatnej korzystają ze wspólnego prefiksu adresu IP, na przykład 192.168.1.XXX. Takim adresem posługują się we wzajemnej komunikacji. W przypadku komunikacji z inną siecią adres ten jest tłumaczony na adres publiczny routera oraz jest do niego dołączane mapowanie portu.

- 192.168.1.24 => 184.13.12.33:44221
- 192.168.1.121 => 184.13.12.33:24325 itd.

Ponieważ tabela tłumaczenia adresów jest przechowywana w routerze, w większości przypadków użytkownik z zewnątrz nie jest w stanie poznać adresu urządzenia objętego mechanizmem NAT. Podczas komunikacji opartej na protokole SIP może to doprowadzić do jednego z następujących problemów:

- Brak możliwości zainicjowania, zaktualizowania lub zakończenia sesji, czyli nawiązania, wstrzymania lub zakończenia połączenia
- Brak strumieni multimedialnych
- Jednokierunkowe strumienie multimedialne

Przechodzenie przez NAT: funkcja NAT zmienia adres źródłowy każdego pakietu na publiczny adres IP z innym portem źródłowym.



W odpowiedzi na te problemy w protokole SIP wprowadzono obsługę trzech technik NAT:

- STUN. W tej technice do serwera znajdującego się w znanej lokalizacji kierowane jest pytanie o publiczny adres danej jednostki. Serwer STUN zwraca publiczny adres IP i mapowanie portu użyte w żądaniu. Otrzymany wynik jest następnie używany w sygnalizacji i transferze multimediów, co sprawdza się w większości sytuacji.
- TURN. Jeśli używana jest technika TURN, cały ruch jest przekazywany poprzez znany serwer. Generuje to dodatkowe obciążenie, ponieważ komputer obsługujący serwer TURN musi być wystarczająco wydajny, aby kierować wszystkie multimedia dla każdego klienta korzystającego z tej usługi. To rozwiązanie jest droższe, ale działa w pewnych sytuacjach, w których nie sprawdza się STUN.
- ICE. Protokół ICE zbiera wszystkie możliwe do znalezienia adresy IP związane z określonym agentem użytkownika SIP, a następnie próbuje obliczyć, którego z nich należy użyć. Jeśli ta metoda jest używana w połączeniu z technikami STUN i TURN zarówno w inicjującym, jak i odbierającym agencie użytkownika SIP, zwiększa skuteczność zestawiania połączeń SIP.

6.2 Używanie szyfrowania z protokołem SIP

Dane sygnalizacyjne SIP zazwyczaj są przesyłane przy użyciu bezpołączeniowego protokołu UDP. Mogą też być wysyłane za pośrednictwem protokołu TCP i wówczas dodatkowo szyfrowane przy użyciu protokołu TLS.

Aby zapewnić, że na potrzeby połączenia komunikacyjnego zostanie użyte bezpieczne połączenie sieciowe, protokół SIP używa schematu adresowania pod nazwą Secure SIP (SIPS), który wymaga ustawienia trybu transportu TLS. Podczas nawiązywania połączenia wybierany adres SIP otrzymuje prefiks „sips:", a nie „sip", na przykład sips:robert@biloxi.wew.com, a nie sip:robert@biloxi.wew.com. Wskazuje to, że każdy przeskok musi być zabezpieczony przy użyciu protokołu SIP, i wymaga od odbiorcy zastosowania tego samego poziomu zabezpieczeń. W przypadku korzystania z protokołu TLS zainicjowanie połączenia z adresem o prefiksie sip zapewnia wyłącznie zaszyfrowanie pierwszego przeskoku.

Aby uzyskać najwyższy poziom bezpieczeństwa, należy stosować następujące środki:

- Należy ustawiać tryb transportu TLS.
- Należy zawsze używać prefiksu sips.
- Do wysyłania tonów DTMF należy używać metody SIP INFO, ponieważ korzysta ona z kanału zaszyfrowanego.

Należy pamiętać, że nie wszyscy klienci obsługują schemat Secure SIP.

7 Terminologia związana z protokołem SIP

API	Application Programming Interface (interfejs programowania aplikacji)
Kodek	Koder-dekoder
Telefon IP	Urządzenie fizyczne umożliwiające nawiązywanie połączeń telefonicznych (telefon)
ICE	Interactive Connectivity Establishment (środowisko łączności interaktywnej)
IP	Internet Protocol (protokół internetowy)
Klient mobilny	Oprogramowanie na urządzeniu mobilnym umożliwiające nawiązywanie połączeń telefonicznych
NAT	Network Address Translation (tłumaczenie adresów sieciowych)
PBX	Private Branch Exchange (centrala abonencka)
PSTN	Public Switched Telephone Network (publiczna komutowana sieć telefoniczna), czyli zwykła sieć telefoniczna
RTP	Real-time Transport Protocol
SDP	Session Description Protocol
SIM	Subscriber Identity Module (moduł identyfikacyjny abonenta)
SIP	Session Initiation Protocol
Serwer SIP	Główny element centrali PBX IP. Obsługuje zestawianie i kończenie połączeń. Nazywany także rejestratorem lub serwerem proxy SIP.
SIPS	Secure SIP (bezpieczny protokół SIP)
SIP URI (adres SIP)	Uniform Resource Identifier (jednolity identyfikator zasobu). Unikatowy adres agenta użytkownika SIP.
Softphone	Oprogramowanie umożliwiające nawiązywanie połączeń telefonicznych
STUN	Session Traversal Utilities dla NAT (protokół)
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TURN	Traversal Using Relays around NAT (protokół)
Agent użytkownika (UA)	Nazywany także agentem. Każdy z punktów końcowych sesji komunikacyjnej.
UC	Unified Communications
UDP	User Datagram Protocol
VoIP	Voice over IP

T10175991/PL/M4.6/2409

O firmie Axis Communications

Axis umożliwia tworzenie mądrzejszego i bezpieczniejszego świata, tworząc rozwiązania zwiększające bezpieczeństwo i wydajność biznesową. Jako firma z branży technologicznej będąca liderem na rynku, Axis oferuje systemy dozoru wizyjnego, kontroli dostępu, domofonowe i rozwiązania audio. Rozwiązania te są wzbogacone o inteligentne aplikacje analityczne i wysokiej jakości szkolenia

Firma Axis zatrudnia około 4000 zaangażowanych pracowników w ponad 50 krajach i współpracuje z partnerami z sektora technologii oraz integracji systemów na całym świecie, aby dostarczać rozwiązania dla klientów. Firma Axis powstała w 1984 roku, a jej siedziba znajduje się w Lund w Szwecji