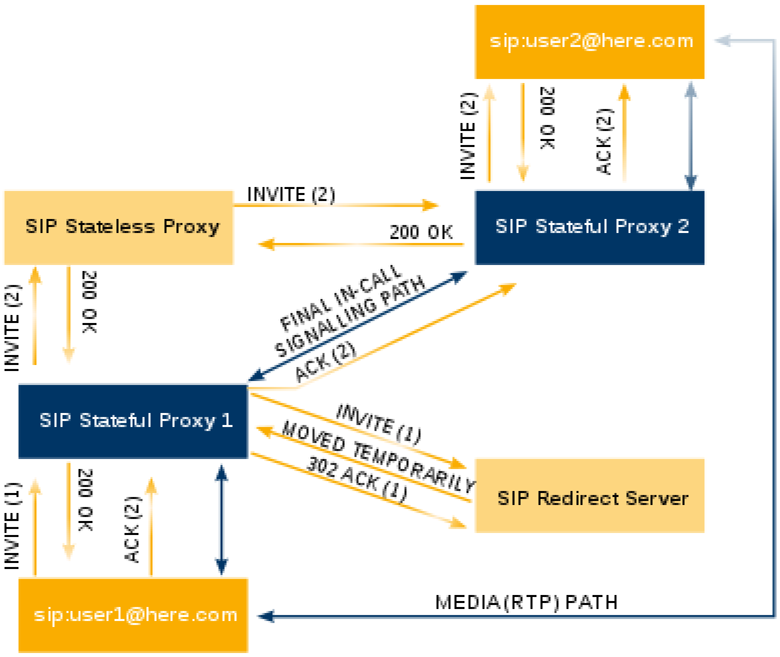
# SIP - Session Initiation Protocol

In contrast to H.323, **SIP** was developed by the IETF (Internet Engineering Taskforce) with the Internet in mind and is therefore oriented towards the architecture of common Internet applications.

From the beginning, attention was paid to easy implementability, scalability, expandability and flexibility. **SIP** can be used to manage any number of sessions with one or several participants. However, it is not limited to **Voice over IP** as sessions can be any number of multimedia streams or conferences.

The security standard **SIPS** not only prevents eavesdropping and message manipulation, but also ensures the proxy server about the identity of the snom client phone and protects against identity spoofing.

Through the use of **AES (Advanced Encryption Standard)** in the counter mode for secure **RTP** one single key stream emerges for each **RTP** packet, which makes it practically impossible to retrieve an original **RTP** stream and abuse it.



To make an Internet phone call, you need more than just SIP, because it only serves to agree or negotiate the communication modalities - the actual data for the communication must be exchanged via other, suitable protocols. The Session Description Protocol (SDP, RFC 4566, the translation from the English "Session Description Protocol" is not commonly used) is often embedded in SIP to negotiate the details of the video and/or audio transmission. The devices tell each other which methods of video and audio transmission they master (the so-called codecs), with which protocol they want to do this and at which network address they want to send and receive.

This media negotiation is therefore not a direct component of SIP, but is achieved by embedding another protocol in SIP. This separation of session and media negotiation is one of the advantages of SIP, as it allows great flexibility in the supported payload: For example, if a manufacturer wants to use SIP for a specialized application, they can design their own media negotiation if no protocol exists yet.

Internet telephony uses the Real-Time Transport Protocol (RTP, RFC 3550) for media transmission. SIP negotiates the session, the embedded SDP negotiates the media details, and RTP is the protocol that finally transmits the video and audio streams.

Subscriber addresses are written in URI format, which is also used in e-mails and WWW addresses. Such a subscriber address usually follows one of the following three schemes:

- Unencrypted SIP connection: sip:user@domain.
- Encrypted SIP connection: sips:user@domain.
- Telephone number: tel:nummer, for example tel:+49-69-1234567 This scheme is mainly used by devices that provide an interface to the "normal" telephone network and can be converted to a SIP URI, for example sip:+49-69-1234567@domain, if required.

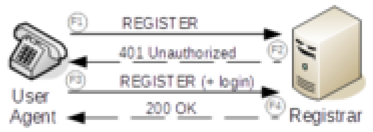
## Encryption and security

By separating session and media, both data streams can also be encrypted independently of each other. SIP can be encrypted using the **TLS protocol** , also called **SIPS** , and the media stream (voice data) can also be encrypted using the SRTP protocol. Any combination of these is possible, but does not make sense in terms of secure encryption.

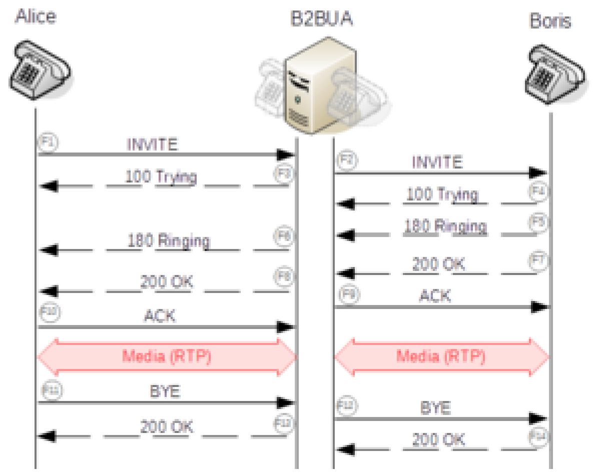
For secure encryption, both data streams (session and media) must be encrypted simultaneously. The symmetric keys of the media stream are exchanged via SDP (i.e. SIP) and could therefore be attacked via an unencrypted SIP. The symmetric keys of  **TLS** are exchanged at the beginning of the session, but the mechanisms of SSL certificates, in which the symmetric keys are encrypted by the asymmetric keys of the SSL certificates, also take effect here.

Since transmission via a connectionless network protocol makes more sense with SIP, a UDP-based counterpart to **TLS** , which is based on TCP, was designed with DTLS. However, it is currently only implemented by a SIP stack (ReSIProcate)

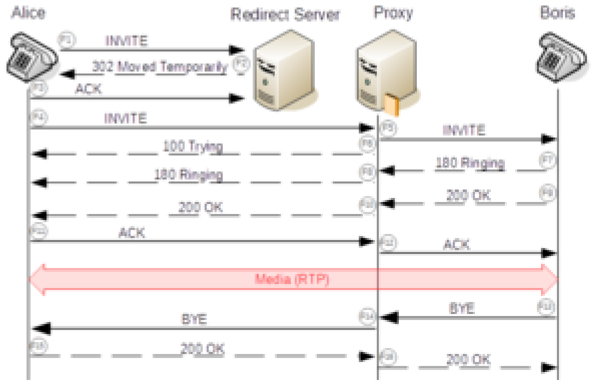
## Network Elements



SIP UA registration on SIP registrar with login authentication



Call flow through redirect server and proxy



Establish a connection with the **B2BUA**

- **User agent**
  The User Agent is an interface to the user that displays content and receives commands. A SIP phone is also a SIP user agent that provides the traditional call functions of a phone, such as dial, answer, reject and hold.

- **Proxy server**
  A proxy server is a communication interface in a network. It works as an intermediary (routing) that receives requests on one side and then establishes a connection to another side via its own address. It is his task to ensure that requests are sent specifically to the user. Proxies are also needed to enforce the hierarchy.

- **Registrar Server**
The registrar server serves as a central switching point in the system architecture of SIP. He takes over the registration of requests for the domain he processes. It processes one or more IP addresses for a specific SIP URI, which are transmitted by the SIP protocol.

- **Redirect server**
The redirect server relieves the proxy server. It transfers the routing information directly to the User Agent Client. It generates redirects to contact incoming requests in an alternative group of URIs. The redirect server allows SIP session invitations to be sent to external domains.

- **Session Border Controller**
A Session Border Controller is a network component for the secure coupling of computer networks with different security requirements. It serves as a middle node between the user agent and the SIP server for various types of functions, including support for Network Address Translation (NAT)

- **Gateway**
A gateway can connect an SIP network to other networks, such as the public telephone network, which uses different protocols or technologies, as an interface.

- **B2BUA**
B2BUA - (back-to-back user agent) is middleware in both SIP and RTP data streams. With SIP clients, a B2BUA behaves like a user agent server on one side of the connection and like a user agent client on the other. The point is to be able to manipulate the data streams.

  B2BUA is specified in RFC 3261.

  Examples for the application:
  - Call management (including billing, call forwarding, automatic disconnection)
  - pairing of different networks (especially to adapt the different dialects of the protocols, depending on the manufacturer)
  - Hiding the network structure (including private addresses, network topology)

  Basically, a B2BUA can be expanded to a proxy with an integrated media gateway.

## SIP-Status-Codes

main article: SIP status codes

The clients and servers involved in a SIP session send requests and answer them using response codes.

- **1xx** – **Provisional**

  Preliminary status information that the server is performing further actions and therefore cannot yet send a final response.

- **2xx** – **Successful**

  The request was successful.

- **3xx** – **Redirection**

  These messages inform about a new contact address of the called party or about other services that enable the connection to be established successfully.

- **4xx** – **Request Failures**

  The previous message could not be processed.

- **5xx** – S**erver Failures**

  A server involved in the transmission could not process a message.

- **6xx** – **Global Failures**

  The server was contacted successfully, but the transaction does not take place.

Source: https://de.wikipedia.org/wiki/Session_Initiation_Protocol

---

**Related Links:**

- ADPCM - Adaptive Differential Pulse Code Modulation
- B2BUA - Back-to-Back-User-Agent

- Basics of VoIP
- Codec
- CSTA - Computer-supported telecommunications applications
- CTI - Computer Telephony Integration
- DHCP - Dynamic Host Configuration-Protokoll
- DNS - Domain Name Service
- ENUM - Telephone Number Mapping
- Hot Desking
- How can I obtain a SIP trace from the phone
- How to obtain a SIP trace from a deskphone
- IP-PBX
- IVR - Interactive Voice Response
- Jitter