ТЕХНИЧЕСКИЙ ОБЗОР

Общее представление о протоколе SIP

Апрель 2022

AXIS COMMUNICATIONS

Содержание

1 Краткая информация

Протокол инициализации сеанса (SIP) служит дополнительным интерфейсом интеграции систем безопасности. Будучи широко распространенным телекоммуникационным стандартом, протокол SIP расширяет совместимость и повышает гибкость повседневной эксплуатации оборудования. Системные интеграторы, разработчики и конечные пользователи нуждаются в открытых, унифицированных интерфейсах, расширяющих возможности и совместимость устройств в составе разнообразных систем. Устройства Axis с поддержкой протокола SIP применяются в составе как охранных, так и коммуникационных систем.

Установить и настроить SIP-систему несложно. Однако применение сложных сетевых технологий, повышенные требования к безопасности или нужда в дополнительных функциях обработки вызовов требуют установки SIP-сервера и внедрения способов прохождения через NAT, а следовательно, высокой технической квалификации специалистов по монтажу и эксплуатации оборудования.

2 Введение

Протокол инициализации сеанса (SIP) применяется для установления, поддержания и завершения мультимедийной связи между несколькими узлами. Обычно речь идет о звуковой связи, но бывает, что применяется и видеосвязь. Протокол SIP является стандартным для IP-телефонии (VoIP) и объединенных коммуникационных платформ.

Протокол SIP, который поддерживается такими устройствами, как, например, сетевой громкоговоритель AXIS C3003-E Network Horn Speaker или сетевой видеодомофон AXIS I8016-LVE Network Video Intercom, представляет собой принципиально новый способ соединения, интеграции и контроля за работой сетевого оборудования производства компании Axis.

3 Как это работает?

Для связи по протоколу SIP нужны хотя бы два SIP-клиента. SIP-клиентом называется аппаратный или программный телефон, мобильный клиентский узел или устройство Axis с поддержкой протокола SIP.

Каждому SIP-клиенту выделяется отдельный SIP-адрес. SIP-адрес похож на адрес электронной почты, только с префиксом “sip:”

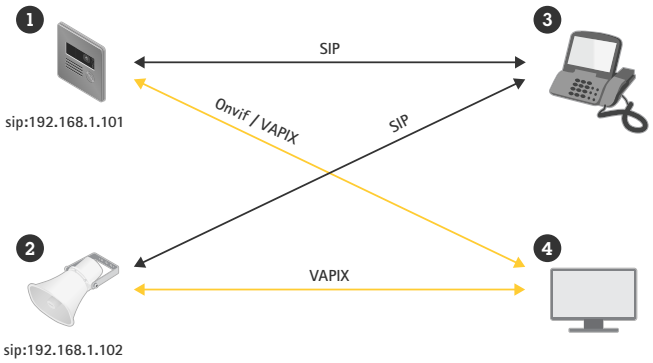
Пример: sip:bob@axis.com [sip:<пользователь@]<провайдер>. Такой идентификатор может работать с несколькими устройствами аналогично телефонному номеру, привязанному к SIM-карте, к которой можно подключить сразу несколько устройств.

3.1 Простейшая одноранговая схема

SIP-системы бывают разными. Простейшая система состоит из нескольких пользовательских SIP-агентов (UA), которые напрямую устанавливают связь друг с другом. Такую систему можно назвать одноранговой, прямой или локальной. В таких случаях типичный SIP-адрес имеет формат sip:<local-ip>, например, sip:192.168.0.90

Пример: По этой простой схеме устройства Axis (1, 2) могут устанавливать звуковую и (или) видеосвязь по протоколу SIP с другими SIP-устройствами (3) в составе этой же сети, не нуждаясь в сервере или УАТС.

При этом их, как и любые другие устройства Axis, можно подключить к системе управления видеонаблюдением (4) через открытый прикладной программный интерфейс VAPIX или ONVIF Profile S.



Чтобы установить одноранговое соединение двух пользовательских агентов по локальной сети, достаточно SIP-адреса с IP-адресами обоих устройств. Имейте в виду, что одноранговые вызовы поддерживаются не всеми SIP-клиентами.

3.2 Расширение возможностей благодаря SIP-серверу (УАТС)

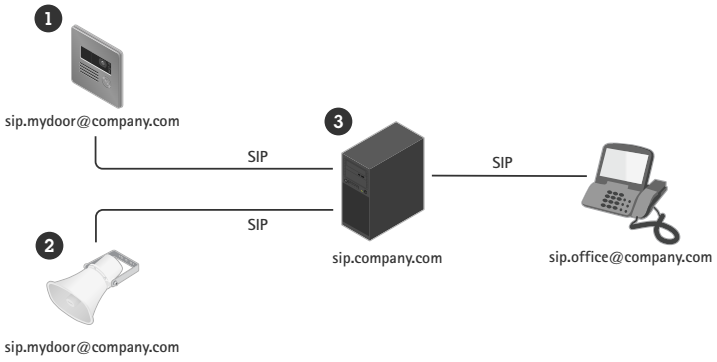
Инфраструктура VoIP на базе протокола SIP превосходно масштабируется. Расширение начинается с установки учрежденческой телефонной станции (УАТС) или SIP-сервера в качестве центрального узла связи. Зарегистрированные на этом узле пользовательские SIP-агенты могут устанавливать связь между собой простым набором добавочного номера УАТС.

В таких случаях типичный SIP-адрес имеет формат sip:<пользователь>@<домен>. Как вариант, можно применять формат sip:<пользователь>@<ip-регистратор>, например, sip:6007@mysipserver.net. УАТС действует как обычный коммутатор, наделенный такими функциями, как индикация текущего статуса клиентов, перенаправление и переадресация вызовов, голосовая почта и множеством других.

Обычно SIP-сервер наделяется такими функциями, как прокси, регистрация и перенаправление. Прокси-функции обеспечивают маршрутизацию вызовов и служат дополнительными логическими элементами входящих вызовов. Регистрационные функции заключаются в приеме запросов на регистрацию и в определении местоположения обслуживаемых доменов. Переадресация заключается в перенаправлении клиента на альтернативный SIP-адрес.

SIP-сервер можно установить как локально, так и за пределами обслуживаемого объекта. Он может находиться в составе внутренней сети компании или предоставляться сторонним поставщиком услуг. Первоначально связь между объектами по протоколу SIP обычно устанавливается через несколько SIP-прокси. Эти прокси запрашивают информацию о местоположении нужных SIP-адресов.

Пример: Устройства Axis (1, 2) можно подключить к SIP-серверу (3) как локально, так и через стороннего провайдера. Сервер устанавливает и прекращает связь между SIP-устройствами по локальной сети или через интернет. По этой схеме SIP-адрес не зависит от IP-адреса абонента, а SIP-сервер обеспечивает доступ к устройству, пока оно зарегистрировано на этом сервере.

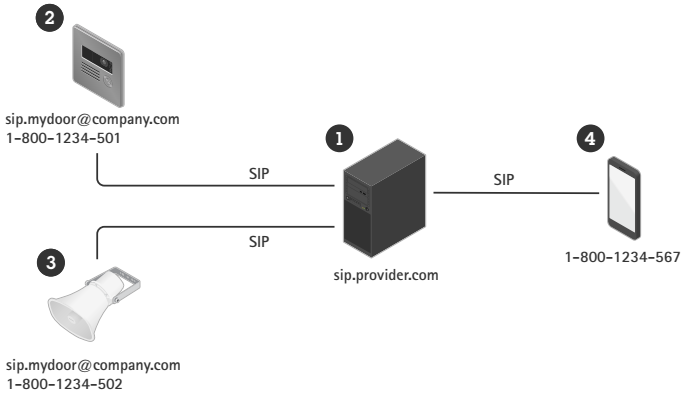


Для установки соединения устройства с SIP-сервером необходимо зарегистрировать на сервере учетную запись с определенным именем пользователя и паролем. Чтобы зарегистрировать устройство на сервере, нужно создать для устройства учетную запись, указав в ней адрес сервера, имя пользователя и пароль.

3.3 Магистральные линии связи по протоколу SIP: выделение телефонного номера

Через магистральную линию связи по протоколу SIP пользовательские SIP-агенты подключаются даже к обычной телефонной сети общего пользования (ТСОП). Таким образом пользовательскому агенту SIP можно выделить обычный телефонный номер.

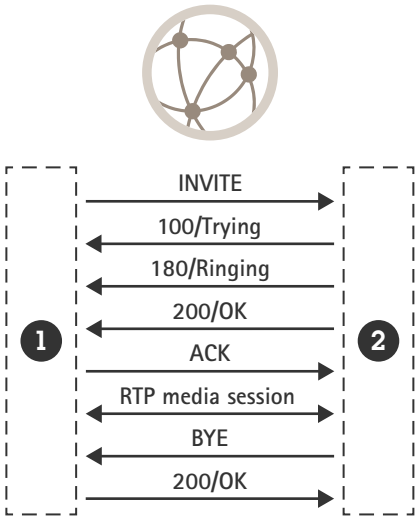
Пример: Через магистральную линию связи по протоколу SIP (1) провайдер может выделить устройствам (2, 3) внешние телефонные номера. Это дает возможность устанавливать связь сетевого громкоговорителя или домофона с обычными телефонами (4).



Таким способом устройство подключается к серверу через магистральную линию связи по протоколу SIP. За подключение внешних номеров провайдер обычно взимает дополнительную плату.

4 «Обычный» вызов по протоколу SIP

При вызове по протоколу SIP выполняется определенная последовательность действий для обмена информацией между пользовательскими агентами, выступающими в роли инициатора и получателя.



Инициатор вызова (1) отправляет запрос INVITE на SIP-адрес вызываемого абонента (2). В запросе INVITE содержится сообщение по протоколу описания сеансов связи (SDP) с информацией о доступных форматах мультимедийных данных и способах связи с инициатором вызова.

По поступлении запроса INVITE получатель немедленно его подтверждает, отправляя в ответ 100 TRYING.

Затем вызываемый пользовательский агент сравнивает предложенные в SDP-сообщении форматы мультимедийных данных с собственными форматами. Если есть доступный общий формат, пользовательский агент уведомляет вызываемого абонента о входящем вызове и отправляет инициатору вызова промежуточный ответ 180 RINGING.

Если вызываемый абонент принимает вызов («снимает трубку»), инициатору отправляется ответ 200 OK в знак подтверждения того, что соединение установлено. В этом ответе содержится SDP-сообщение, указывающее инициатору, какие форматы мультимедийных данных можно использовать и куда направлять мультимедийные потоки.

Затем формируются согласованные потоки мультимедийных данных с использованием протокола передачи данных в реальном времени (RTP) с параметрами, согласованными в SDP-сообщениях. После этого участники сеанса связи могут приступать к обмену мультимедийными данными. На этом этапе инициатор вызова отправляет по протоколу SIP подтверждение (ACK), означающее, что медиа-потоки сформированы согласованным способом. Сеанс связи по протоколу SIP остается активным, но для передачи мультимедийных данных протокол SIP не используется.

Приняв решение завершить вызов, одна из сторон направляет другой новый запрос BYE. Приняв запрос BYE, другая сторона подтверждает его ответом 200 OK, после чего медиа-потоки по протоколу RTP останавливаются.

4.1 Протокол SDP: согласование формата связи

Протокол описания сеансов связи (SDP) предназначен для согласования параметров инициализации потокового обмена мультимедийными данными. В SDP-сообщениях содержится информация о том, какие форматы данных (иначе говоря, кодеки) поддерживаются клиентскими узлами, а также о предпочтительном порядке согласования кодека.

В SIP-вызовах обычно применяются такие аудиокодеки, как PCMU, PCMA, G.722, G.726 и L16. Если инициатор и получатель поддерживают сразу несколько кодеков, обычно согласовывается кодек с наивысшим приоритетом на стороне получателя. Пропускная способность зависит в конечном счете от подбора кодеков, поэтому следует внимательно относиться к вопросам совместимости остальных пользовательских SIP-агентов и поддержания нужной пропускной способности. Так, например, обмен несжатыми аудиоданными эффективен, если все клиентские сети в составе локальной сети поддерживают кодеки L16. Однако для обращения к пользовательскому SIP-агенту с мобильного телефона 3G через интернет лучше выбрать кодек PCMU.

4.2 Вызовы в сложной SIP-инфраструктуре

При сравнительно сложной конфигурации SIP-инфраструктуры процесс инициализации вызова немного отличается: SIP-сеанс устанавливается поочередно для каждого промежуточного узла. Но после того, как связь по протоколу SIP установлена, узлы, как правило, обмениваются данными напрямую без маршрутизации, как в предыдущем примере.

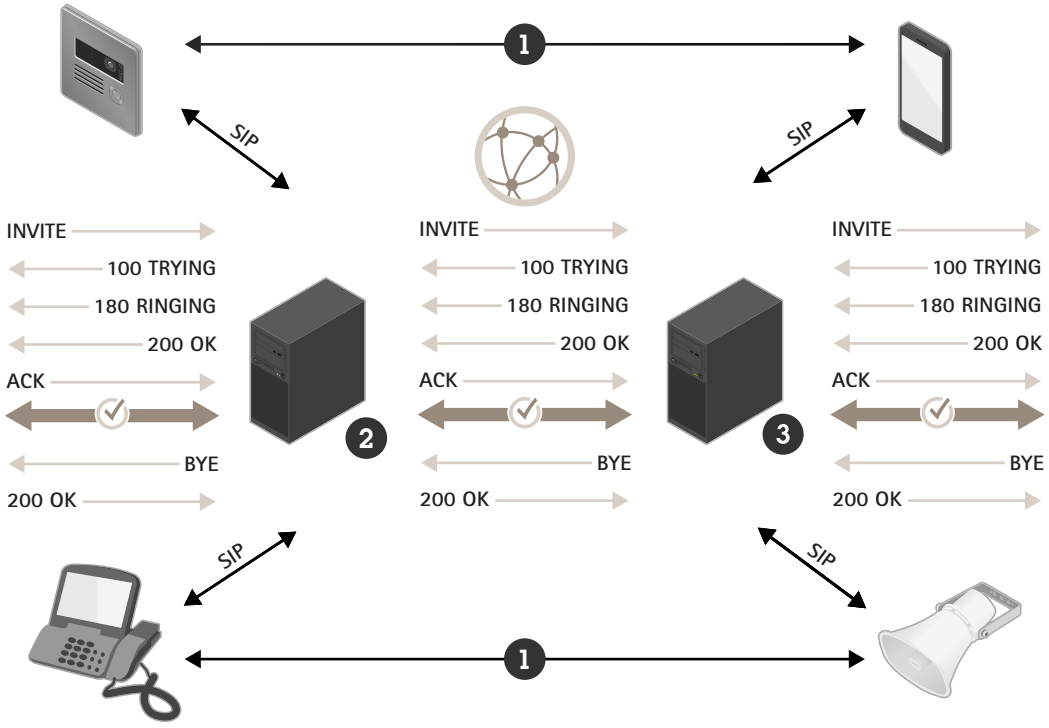


Figure 1. Обработка вызова в сравнительно сложной SIP-инфраструктуре. Медиа-потоки по протоколу RTP (1) перемещаются непосредственно между узлами после установления сеанса SIP между инициатором (2) и получателем (3).

5 Связь по протоколу SIP с применением DTMF-сигналов

Двухтональная многочастотная сигнализация (DTMF-сигналы) – это формат передачи информации по телефону. DTMF-сигналы применяются для передачи команд SIP-устройствам, между которыми устанавливается связь по протоколу SIP. DTMF-сигналы состоят из цифр 0-9, латинских букв A-D, а также символов * и #.

Так, например, при вызове переговорного устройства, поддерживающего протокол SIP, на клавиатуре телефона можно набрать цифру '5', запрограммированную как DTMF-команда, по которой домофон отпирает дверь.

Существуют три способа отправки DTMF-сигналов при вызове по протоколу SIP:

- Традиционный внутриполосный способ, когда сигнал по сути представляет собой звуковой импульс, чередующийся со звуковым потоком. Однако способ этот ненадежен: он срабатывает только с теми кодеками, которые обрабатывают данные без сжатия.
- Способ SIP INFO, при котором символы DTMF-сигналов встраиваются в SIP-сообщение, которое передается в потоковом режиме. Этот внеполосный отличается высокой надежностью, но ограниченной поддержкой.
- Способ RTP (RFC2833), при котором символы DTMF-сигналов кодируются в виде внеполосного RTP-пакета. Этот способ фактически является стандартным и широко поддерживается.

6 Сложные среды и усиленная защита

В сложной сетевой инфраструктуре, например в корпоративных сетях, могут возникать затруднения с использованием протокола SIP. То же самое относится к применению шифрования.

6.1 Навигация по сложным сетям с прохождением через NAT

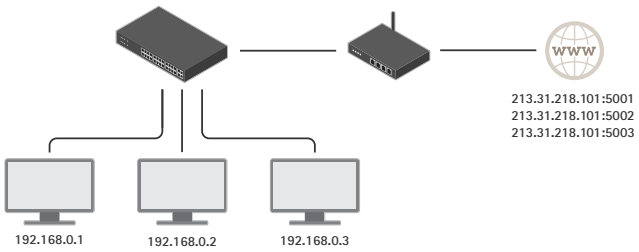
В сравнительно сложной сетевой инфраструктуре возникает необходимость в преобразовании сетевых адресов. Преобразование адресов закрытых локальных сетей в общедоступные IP-адреса называется NAT. Всем узлам в составе закрытой подсети присваивается IP-адрес с общим префиксом, например 192.168.1.XXX. Пользуясь этим адресом, они устанавливают связь друг с другом. А когда они обмениваются данными с другой сетью, этот адрес преобразуется в общедоступный адрес маршрутизатора, к которому добавляется номер порта:

- 192.168.1.24 => 184.13.12.33:44221
- 192.168.1.121 => 184.13.12.33:24325 и т.д.

Поскольку таблица преобразования хранится в маршрутизаторе, пользователи за пределами закрытой сети в большинстве случаев не имеют доступа к адресам устройств по ту сторону NAT. Из-за этого связь по протоколу SIP бывает сопряжена с рядом проблем:

- Отказ в установлении, обновлении или завершении сеанса связи, когда не удается отправить, удерживать или завершить вызов.
- Отказ в потоковом обмене мультимедийными данными.
- Однонаправленный обмен мультимедийными данными.

Прохождение через NAT: адрес отправителя каждого пакета данных NAT меняет на общедоступный IP-адрес с другими исходными портами.



Эти проблемы решаются тремя способами прохождения через NAT с применением протокола SIP:

- STUN: этот способ заключается в направлении запроса общедоступного адреса нужного узла на сервер, местонахождение которого известно. В ответ STUN-сервер сообщает общедоступный IP-адрес с номером порта, через который проходил запрос. Полученные сведения используются для обмена сигналами и мультимедийными данными, что в большинстве случаев срабатывает.
- TURN: протокол TURN перенаправляет весь трафик через известный сервер. Это сопряжено с дополнительными затратами, поскольку машина, на которую устанавливается TURN-сервер, должна быть достаточно мощной, чтобы обеспечивать маршрутизацию потоков мультимедийных данных со всех узлов, подключенных к такому сервису. Так что это достаточно дорогостоящее решение, но оно срабатывает там, где технология STUN зачастую дает отказ.
- ICE: протокол ICE собирает все доступные ему IP-адреса пользовательских SIP-агентов, а затем вычисляет нужный адрес. Когда он используется вместе с технологиями STUN и TURN применительно к пользовательским SIP-агентам, выступающим в роли как отправителей, так и получателей данных, шансы на успешное установление и поддержание связи по протоколу SIP резко повышаются.

6.2 Применение шифрования с протоколом SIP

Обычно сигнальный трафик SIP идет по протоколу UDP без соединения. Он может идти и по протоколу TCP с шифрованием по протоколу безопасности на транспортном уровне (TLS).

Для надежной защиты соединения при вызове в протоколе SIP применяется схема адресации под названием SIPS (защищенный протокол SIP), которая требует перевода транспортного режима на протокол TLS. При вызове префикс SIP-адреса меняется с “sip:” на “sips:”, например, sips:bob@biloxi.ex.com вместо sip:bob@biloxi.ex.com. Это означает, что каждый переход обязательно защищается протоколом TLS, а получатель обязан установить защиту на таком же уровне. При вызове адреса с префиксом “sip:” по протоколу TLS шифрование ограничивается только первым переходом.

Меры, гарантирующие защиту на наивысшем уровне:

- Обязательный перевод транспортного режима на протокол TLS.
- Обязательное применение префикса “sips:” на всех этапах.
- Обязательное использование SIP INFO при отправке тональных DTMF-сигналов по зашифрованному каналу.

Имейте в виду, что защищенный протокол SIP поддерживается не всеми SIP-клиентами.

7 Терминология, связанная с протоколом SIP

3G	Технология мобильной связи третьего поколения.
API	Прикладной программный интерфейс
Кодек	Кодер-декодер
Аппаратный телефон	Обыкновенный телефонный аппарат
Программный телефон	Программа для звонков по телефону
ICE	Технология Interactive Connectivity Establishment (установление интерактивной связи)
IP	Интернет-протокол
Мобильный клиент	Программа для звонков по мобильному телефону
NAT	Преобразование сетевых адресов
УАТС	Учрежденческая телефонная станция
ТСОП	Телефонная сеть общего пользования, то есть обычная телефонная сеть
RTP	Протокол RTP (передачи данных в реальном времени)
SDP	Протокол SDP (описания сеансов связи)
SIM-карта	Модуль идентификации абонента
SIP	Протокол SIP (инициализации сеанса)
SIP-сервер	Главный элемент IP-УАТС, обеспечивающий инициализацию и завершение вызовов. Иначе называется SIP-прокси или регистратором
SIPS	Защищенный протокол SIP
SIP URI (SIP-адрес)	Унифицированный идентификатор ресурса или уникальный адрес, присвоенный пользовательскому SIP-агенту
STUN	Средства прохождения сеансов связи через серверы NAT
TCP	Протокол TCP (управления передачей данных)
TLS	Протокол безопасности на транспортном уровне
TURN	Протокол Traversal Using Relays around NAT (перенаправления в обход NAT)
UDP	Протокол UDP (передачи пользовательских датаграмм)
UA	Пользовательский агент, то есть одна из двух оконечных точек сеанса связи
VoIP	IP-телефония

T10175991/RU/M2.2/2204

О компании Axis Communications

Компания Axis вносит весомый вклад в формирование более разумного и безопасного мира, разрабатывая решения, которые повышают безопасность и эффективность бизнеса. Занимая в отрасли технологий сетевого видео ведущие позиции, компания Axis поставляет решения для видеонаблюдения, контроля доступа, сетевых домофонов и звукового сопровождения. Эффективность наших решений повышается благодаря приложениям интеллектуальной аналитики и высококачественному обучению.

Около 4000 специалистов компании Axis трудятся более чем в 50 странах мира, вместе с нашими партнерами по технологиям и по системной интеграции разрабатывая и внедряя решения задач, стоящих перед клиентами по всему миру. Компания Axis была основана в 1984 году. Штаб-квартира компании находится в городе Лунд, Швеция