ІНСТИТУТ СПЕЦІАЛЬНОГО ЗВ’ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

Cпеціальна кафедра №1

Звіт

З навчальної дисципліни «Засоби і комплекси криптографічного захисту інформації»

Практика №10: "SIP"

**Виконав:**

Курсант С-04 групи

Клячко А.О.

**Перевірив:**

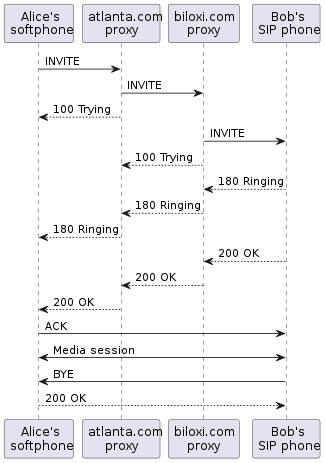
Капітан Володимир Кубрак

**Київ 2023**

**Протоколи встановлення сесії**

SIP — протокол прикладного рівня, розроблений IETF MMUSIC Working Group, і пропонований стандарт на спосіб установки, зміни і завершення користувацького сеансу, що включає мультимедійні елементи, такі як відео або голос, миттєві повідомлення, он-лайн ігри та віртуальну реальність.

Опис



Приклад обміну повідомленнями між двома користувачами за протолом SIP для встоновлення і припинення прямого мультимедійного з'єднання.

Протокол ініціювання сеансів — Session Initiation Protocol — є протоколом прикладного рівня і призначається для організації, модифікації і завершення сеансів зв'язку: мультимедійних конференцій, телефонних з'єднань і розподілу мультимедійної інформації.

Протокол SIP розроблений комітетом IETF, а специфікації протоколу представлені в документі RFC 3261. В основу протоколу закладені наступні принципи:

Персональна мобільність користувачів. Користувачі можуть переміщатися без обмежень в межах мережі, тому послуги зв'язку повинні надаватися їм у будь-якому місці цієї мережі. Користувачеві надається унікальний ідентифікатор, а мережа надає йому послуги зв'язку незалежно від того, де він знаходиться. Для цього користувач за допомогою спеціального повідомлення інформує мережу про свої переміщення.

Масштабованість мережі характеризується, в першу чергу, можливістю збільшення кількості елементів мережі при її розширенні. Серверна структура мережі, побудованої на базі протоколу SIP, повністю відповідає цій вимозі.

Розширюваність протоколу характеризується можливістю доповнення протоколу новими функціями при введенні нових послуг та його адаптації до роботи з різними додатками. Розширення функцій протоколу SIP може бути здійснена за рахунок введення нових заголовків і типів повідомлень.

Інтеграція в стек існуючих протоколів Інтернет, розроблених IETF. Протокол SIP є частиною складної архітектури, розробленої комітетом IETF. Ця архітектура містить у собі також протокол резервування ресурсів (Resource Reservation Protocol, RSVP; RFC 2205), транспортний протокол реального часу (Real-Time Transport Protocol, RTP; RFC 1889), протокол передачі потоків у реальному часі (Real-Time Streaming Protocol, RTSP; RFC 2326), протокол опису параметрів зв'язку (Session Description Protocol, SDP; RFC 2327) та інші. Однак функції протоколу SIP не залежать ні від одного з цих протоколів.

Взаємодія з іншими протоколами сигналізації. Протокол SIP може бути використаний спільно з протоколом Н.323. Можливо також взаємодія протоколу SIP з системами сигналізації ТМЗК — EDSS1 і ОКС № 7. Для спрощення такої взаємодії сигнальні повідомлення протоколу SIP можуть переносити не тільки SIP-адресу, але й телефонний номер формату Е.164 або будь-якого іншого формату. Крім того, протокол SIP, нарівні з протоколами H.323 і ISUP, може застосовуватися для забезпечення функціонування пристроїв управління шлюзами, в цьому випадку він повинен взаємодіяти з протоколом MGCP або MEGACO. Важливою особливістю протоколу SIP є його незалежність від транспортних технологій. Як транспорт можна використовувати протоколи Х.25, Frame Relay, AAL5, IPX і ін Структура повідомлень SIP не залежить від обраної транспортної технології.

Сигнальні повідомлення SIP можуть переноситися не тільки протоколом транспортного рівня UDP, але і протоколом ТСР. Протокол UDP дозволяє швидше, ніж TCP, доставляти сигнальну інформацію (навіть з урахуванням повторної передачі непідтверджених повідомлень), а також вести паралельний пошук місця розташування користувачів і передавати запрошення до участі в сеансі зв'язку в режимі під LGPL. У свою чергу, протокол ТСР спрощує роботу з міжмережевими екранами, а також гарантує надійну доставку даних. При використанні протоколу ТСР різні повідомлення, що відносяться до одного виклику, або можуть передаватися по одному TCP-з'єднанні, або для кожного запиту і відповіді на нього може відкриватися окреме TCP-з'єднання

SIP є багаторівневим протоколом. Його функціонування описується комплексом слабко пов'язаних незалежних етапів обробки. Якщо елемент мережі SIP містить деякий рівень, це означає, що він підтримує групу правил, визначених для даного рівня. Проте не кожен елемент, що працює по протоколу SIP, містить всі рівні. Крім того, елементи, специфіковані для роботи в SIP, є логічними, а не фізичними. У дійсності фізичний елемент SIP може виконувати функції різних логічних елементів залежно від покладених на нього обов'язків.

Нижній рівень SIP відповідає за синтаксис і кодування. Кодування визначено з використанням розширеної граматики Backus-Naur Form (BNF). Повне BNF-опис для SIP міститься в RFC 3261, структура повідомлень SIP буде розглянута в розділі.

Другий рівень програмної реалізації протоколу є транспортним. Він визначає, як клієнт посилає запити і приймає відповіді і як сервер отримує запити і посилає відповіді по мережі. Транспортний рівень протоколу описаний в розділі.

Третій рівень - це рівень транзакцій. Транзакція - це запит, відісланий клієнтської стороною з використанням транспортного рівня SIP серверній стороні, разом з усіма відповідями на цей запит, відіслані серверної стороною клієнта. Рівень транзакцій здійснює повторну передачу повідомлень прикладного рівня, визначає відповідність відповідей запиту і повідомляє верхній рівень проткокола у разі таймауту. Будь-яка операція, яку виконує клієнт агента користувача (UAC), реалізується за допомогою серії транзакцій. Опис роботи рівня транзакцій наведено в параграфі. Агенти користувача (UA) та проксі-сервери з збереженням станів транзакцій (stateful проксі-сервери) містять рівень транзакцій. На противагу їм проксі-сервер без збереження станів (stateless проксі-сервер) не включає рівня транзакцій. Рівень транзакцій має клієнтську частину, звану клієнтської транзакцією і серверну частину, звану серверної транзакцією. Кожна з них представлена кінцевим автоматом (state machine), пов'язаних з обробкою певного типу запиту.

Рівень, що знаходиться вище рівня транзакцій, називається користувачем транзакцій (transaction user - TU). Кожен із об'єктів SIP, крім stateless проксі-сервера, є користувачем транзакцій. Коли TU бажає відіслати запит, він створює окрему клієнтську транзакцію, і передає їй запит разом з IP-адресою, портом і типом транспортного протоколу для місця призначення, які визначають куди потрібно відіслати запит. TU, який створив клієнтську транзакцію, може також скасувати її. Коли клієнт скасовує транзакцію, він потребує, щоб сервер припинив подальшу обробку запиту, повернувся у вихідний стан і цієї передав транзакції відповідь з певним кодом помилки. Це здійснюється за допомогою запиту CANCEL, який створює свою власну транзакцію, але виконує свої функції щодо скасовуємо транзакції

SIP елементи, якими є клієнт і сервер агента користувача, stateful і stateless проксі-сервери і сервер реєстрації, містять програмне забезпечення - ядро (core), яка відрізняє їх один від одного. Ядра, за винятком ядра stateless проксі-сервера, є користувачами транзакцій (TU). Попри те, що функціонування ядер UAC і UAS залежить від типу запиту, існують деякі загальні правила для всіх типів запитів. Ці правила описані в розділі для UAC і ці правила стосуються процесу створення запиту, для UAS вони стосуються обробки запиту і створення відповіді. Оскільки реєстрація відіграє важливу роль у протоколі SIP, UAS, який може працювати c запитом REGISTER, має свою назву - сервер реєстрації (registrar). Роботу ядер UAC і UAS для запиту REGISTER. У розділі висвітлюється робота UAC і UAS із запитом OPTIONS, використовуваного для отримання інформації про функціональні можливості UA. Решта запити, визначені в основний RFC для SIP (RFC 3261), надсилаються в режимі діалогу. Діалог являє собою рівноправну взаємодію двох агентів користувача по протоколу SIP, яке триває певний час. Діалог встановлює послідовність повідомлень між UA та забезпечує вірну маршрутизацію запитів. Запит INVITE є єдиним типом запиту, що встановлює діалог, визначеним у рекомендації RFC 3261 (Проте згодом розширення протоколу визначили ще два таких запиту - SUBSCRIBE і REFER). Коли UAC відсилає запит в режимі діалогу, він крім виконання загальних правил UAC, описаних у розділі, дотримується правил для роботи із запитами в ході діалогу. Параграф дає поняття про діалогах і описує процедури їх створення та підтримки на додаток до процедур створення запитів у режимі діалогу.

Найважливіший тип запиту в протоколі SIP - це INVITE, який встановлює сесію між учасниками з'єднання. Сесія - це сукупність учасників з'єднання і медіапотоків між ними, створених з метою обміну інформацією.

Протокол володіє такими характеристиками:

Простота: включає тільки шість методів (функцій).

Незалежність від транспортного рівня, може використовувати UDP, TCP, ATM і т.д.

Економічність: всі запити формуються на основі тексту.

Стандартними елементами в SIP-мережі є:

User Agent (термінал): за протоколом SIP встановлюються з'єднання «клієнт-сервер». Клієнт встановлює з'єднання, а сервер приймає виклики, але так зазвичай телефонний апарат (або програмний телефон) може як встановлювати так і приймати дзвінки, то виходить що він одночасно грає роль і клієнта і сервера (хоча в реалізації протоколу це не є обов'язковим критерієм) — в цьому випадку його називають User Agent (UA) або термінал.

Проксі-сервер: проксі-сервер приймає запити і проводить з ним деякі дії (наприклад визначає місцеположення клієнта, виробляє переадресацію або перенаправлення виклику та ін.) Він також може встановлювати власні з'єднання. Найчастіше проксі-сервер суміщають з сервером визначення місцеположення (Register-сервер), у такому випадку його називають Registrar-сервером.

Сервер визначення місця розташування або сервер реєстрації (Register): даний вид сервера служить для реєстрації користувачів. Реєстрація користувача проводиться для визначення його поточної IP-адреси, для того щоб можна було зробити виклик user @ IP-адреса. У разі якщо користувач переміститься в інше місце і / або не має певної IP-адреси, його поточну адресу можна буде визначити після того, як він зареєструється на сервері реєстрації. Таким чином клієнт залишиться доступний за однією і тією ж SIP-адресою незалежно від того, де насправді знаходиться.

Сервер переадресації: звертається до сервера реєстрації для визначення поточної IP-адреси користувача, але на відміну від проксі-сервера тільки «переадресує» клієнта, а не встановлює власні з'єднання.

Проксі-сервери в SIP-мережі також можуть вносити зміни до повідомлень котрі передаються — це дозволяє без перешкод проходити NAT у випадку якщо проксі-сервер стоїть на NAT-маршрутизаторі (також можлива настройка проксі-сервера, що знаходиться за NAT у випадку якщо на останньому неможливо встановити проксі-сервер — для цього буде потрібно задати параметри переадресації так, щоб отриманий проксі-сервер став «віртуальним сервером»). Крім цього проксі-сервери можна об'єднувати в «ланцюжки», які дозволяють використовувати телефонію, навіть якщо кінцева точка (UA) знаходиться відразу за декількома NAT-шлюзами.

**Схеми проходження пакетів під час дзвінка**

