УДК 621.391
DOI https://doi.org/10.32782/2663-5941/2025.2.1/19

Приймак С. О.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Кравчук С. О.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

МЕТОД ПІДВИЩЕННЯ ДОСТУПНОСТІ VOIP-СИСТЕМ

У статті розглянуто актуальну проблему підвищення доступності VoIP-систем (Voice over IP), які забезпечують голосовий зв'язок через IP-мережі без використання традиційної телефонної інфраструктури. Автори аналізують основні виклики, пов'язані з експлуатацією VoIP-систем, зокрема необхідність забезпечення безперервності сервісу, відмовостійкості, масштабованості та ефективності використання ресурсів.

Запропонований метод підвищення доступності VoIP-системи базується на використанні безкоштовного програмного забезпечення Kamailio (сервер сигналізації SIP), RTPengine (обробка медіа-трафіку) та Redis (швидка база даних для зберігання RTP-транзакцій). Реалізована архітектура включає механізми автоматичного резервування серверів сигналізації та медіа-шлюзів, балансування навантаги та безшовного перемикання на резервні вузли у разі відмови одного або декількох компонентів.

Це суттєво відрізняється від традиційних підходів, де відмова одного з ключових елементів (сервер сигналізації або медіа-шлюз) призводить до негайного завершення всіх активних з'єднань.

Авторами було виконано експериментальне моделювання роботи системи, яке підтвердило її високу ефективність: навіть у разі відмови 50 % компонентів система зберігає працездатність і не перериває активні голосові виклики. Також проведено аналіз традиційних підходів до побудови VoIP-систем та їхніх недоліків, зокрема залежність від окремих вузлів і неможливість збереження існуючих викликів у разі відмови сервера сигналізації або медіа-шлюзу.

Отримані результати можуть бути корисними для розробників і операторів VoIP-мереж, а також підприємств, які використовують IP-телефонію для критично важливих комунікацій. Запропонована система дозволяє мінімізувати ризики переривання зв'язку, підвищити якість обслуговування користувачів і забезпечити високу надійність роботи VoIP-сервісів.

Ключові слова: *VoIP система, SIP, RTP, висока доступність, надійність.*

Постановка проблеми. Постійна потреба в наявності якісного голосового трафіку через пакетні мережі, зокрема IP-мережі, підтримує високий інтерес розробників до удосконалення технології голос через Інтернет-протокол VoIP (Voice over IP) [1, 2]. Дана технологія не використовує традиційну комутовану телефонну мережу загального користування PSTN (public switched telephone network); натомість виклики здійснюються через мережу передачі даних Інтернет-протоколу.

На даний час, існують певні обмеження в сучасних архітектурах IP-телефонії, що орієнтовані на надання високоякісних телефонних послуг, особливо в умовах великих навантажень, коли необхідно забезпечувати стабільну роботу, як-от в організаціях, де користувачі активно використовують ці послуги [3, 4]. Такі обмеження можуть призвести до того, що організація, аби покращити якість обслуговування і уникнути переривань у роботі, змушена обирати власні рішення, які часто вимагають значних фінансових вкладень. Основні труднощі, з якими стикаються організації, що застосовують програмні рішення з відкритим вихідним кодом для телефонії, полягають у забезпеченні безперервної роботи в умовах високої паралельності при наявності великих обсягів запитів.

Сьогодні багато уваги приділяється наступним дослідженням, пов'язаним із подальшим розвитком VoIP-систем.

1. Висока доступність: VoIP-системи повинні забезпечувати безперервний доступ до зв'язку навіть у випадках відмов або збоїв [5, 6]. Зазвичай, це досягається за допомогою методів резервування, кластеризації серверів та використання кількох маршрутів для передачі даних.

2. Вимоги якості обслуговування (QoS): однією з основних проблем доступності VoIP-

систем є забезпечення стабільної якості передачі голосу, що включає низьку затримку, мінімальні втрати пакетів та відсутність переривань [7]. Це досягається через розподіл ресурсів, планування трафіку та адаптацію до змін у мережі.

3. Надійність і відмовостійкість: VoIP-системи мають бути захищені від різного роду збоїв, включаючи відмову серверів, збої мережі та напади DDoS (distributed denial-of-service). Дослідження в цій сфері спрямовані на розробку механізмів швидкого відновлення після збоїв.

4. Безпека: оскільки VoIP-системи функціонують через Інтернет, вони стають вразливими до атак, таких як підміна IP-адрес, перехоплення викликів, атаки на сервери реєстрації (сервери SIP (Session Initiation Protocol)) та DDoS-атаки. Підвищення доступності часто включає захист від цих ризиків через шифрування даних, автентифікацію користувачів та інші методи захисту.

5. Масштабованість: зі зростанням кількості користувачів та обсягу трафіку VoIP-системи повинні залишатися стабільними та забезпечувати високу якість зв'язку без переривань. Тому дослідження також охоплюють розробку архітектур, які можуть масштабуватися відповідно до потреб.

6. Ефективність використання ресурсів: оптимізація використання мережних і обчислювальних ресурсів є важливою складовою підвищення доступності. Сучасні дослідження охоплюють різні методи компресії голосових даних, управління пропускною здатністю та мінімізації енергоспоживання.

Оскільки все більше компаній переходять на IP-телефонію, зростає потреба у забезпеченні безперебійної роботи VoIP-систем. Тому зростає актуальність досліджень у сфері підвищення доступності VoIP-систем, що обумовлена широким поширенням таких систем як в особистому, так і комерційному середовищі.

Аналіз останніх досліджень і публікацій. В [9] розглянуто приклад побудування VoIP-системи з шифруванням голосового та сигнального трафіку в режимі реальному часі, в [10] приділено увагу побудуванню безпечної комп'ютерної мережі для VoIP-системи та наведені типові показники навантаги серверів VoIP, але в жодній з цих робот не розглянуто аспекти стійкості до збою програмних та апаратних елементів VoIP-системи. В [11] розглянуто декілька методів підвищення доступності VoIP-системи, але жоден з них не виконує резервування існуючих голосових потоків RTP. У випадку реалізації запропонованої нами системи вплив на сервіси відсутній навіть при відмові 50 % її компонентів. Представляє інтерес для поліпшення VoIP-систем підходи на базі безкоштовного програмного забезпечення Kamailio, RTPengine та Redis [17]. Але у відомих роботах їх застосування недостатньо вивчене.

Постановка завдання. Метою даної роботи є розробка методу підвищення доступності VoIP-системи, створеної на базі безкоштовного програмного забезпечення Kamailio, RTPengine та Redis, яка дасть змогу обробляти існуючі та нові голосові виклики без впливу на сервіс в разі відмови 50 % елементів системи.

Виклад основного матеріалу дослідження. На даний час VoIP-системи широко використовуються в мережах мобільного та фіксованого зв'язку для обробки голосового трафіку [13]. Класична схема VoIP-системи наведена на рис. 1 [14].

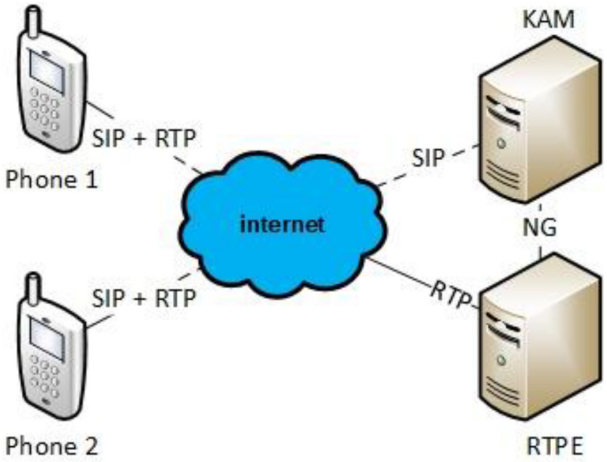

Рис. 1. Класична схема VoIP системи

Система складається з серверу сигналізації «KAM» та медіа-шлюзу «RTPE», які відповідають за опрацювання сигнального (SIP) та голосового (RTP) трафіку, відповідно, та двох абонентських терміналів з підтримкою протоколу SIP – Phone 1, Phone 2. Підвищити доступність системи, структура якої наведена на рис. 1, неможливо, та у разі відмови одного з її компонентів ми отримаємо вплив на сервіс у вигляді відмови обробки голосового або сигнального трафіку. Зазвичай в таких системах використовують програмне забезпечення, яке об'єднує сигнальний та медіа сервери, на кшталт Asterisk, Freeswitch на операційній системі Linux. В окремих випадках використовують віртуальне середовище WMVare, VirtualBox, HyperV, Docker або інше.

Високодоступною VoIP-системою називається система голосового зв'язку, яка використо-

вує IP-пакети для передачі голосу (відео, тощо) та спроектована для забезпечення безперервного функціонування, навіть у випадку збою окремих, як програмних так і апаратних компонентів, або мережних проблем. Основна мета такої системи – мінімізувати час простою, забезпечити стійкість до відмов, балансування навантаження, а також дублювання та резервування ресурсів [14].

Схему високодоступної VoIP-системи можна представити наступним чином, як показано на рис. 2.

Система складається з наступних компонентів:

– сервер сигналізації – KAM1, KAM2, відповідає виключно за обробку сигналізації, в данному випадку SIP;

– медіа шлюз – RTPE1, RTPE2, відповідає виключно за опрацювання голосового RTP трафіку;

– In-memory DB – REDIS, база данних для RTP транзакцій;

– абонентські термінали з підтримкою протоколу SIP – Phone 1, Phone 2.

В якості серверу сигналізації обираємо програмний SIP сервер Kamailio, а медіа шлюзом виступає RTP engine [15] – програмний продукт керування RTP трафіком. База даних REDIS [17] використовується для маніпуляцій (накопичення, видалення) RTP транзакцій.

Між серверами сигналізацій KAM1 та KAM2 присутній логічний канал зв'язку, так званий DMQ interface [15] для обміну ідентифікаторами SIP транзакцій (SIP call id) [1], в той самий час сервера керують медіа шлюзами (RTPE1, RTPE2) за протоколом NG [15]. В той самий час медіашлюзи RTPE1 та RTPE2 обмінюються RTP транзакціями за допомогою БД Redis за протоколом pub/sub [17]. Час перемикання активного вузла сервера на гарячий резерв становить 1 с.

Розглянемо сценарії обробки голосового виклику: як відомо, голосовий виклик в VoIP-мережі складається з декількох компонент:

– сигналізації (в даному випадку SIP);

– голосового потоку даних (RTP).

В схемі, наведений на рис. 2, по замочуванню встановлені такі пріоритети: сервер сигналізації KAM1 керує медіа шлюзами RTPE1 (основний) та RTPE2 (резервний), так само KAM2 керує медіа шлюзами RTPE2 (основний) та RTPE1 (резервний). Обидва медіа шлюзи використовують базу даних REDIS, яка служить для моніторингу активності між екземплярами RTPengine та виконує аварійне перемикання сесій з одного екземпляра на інший.

В даній реалізації лише одна пара KAM+RTPE може бути активною та опрацьовувати голосові виклики, інша пара знаходиться в режимі гарячого резерву.

У випадку 100 % функціональності системи голосовий виклик опрацьовується наступним

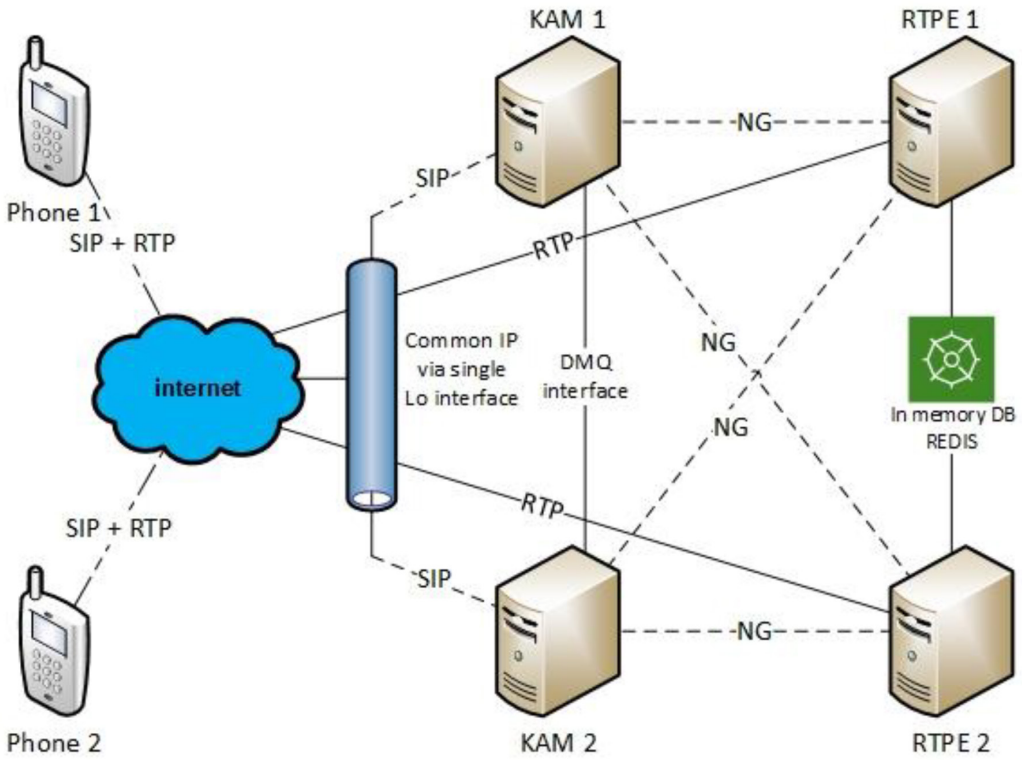

Рис. 2. Схема високодоступої VoIP системи

чином: сигналізацію опрацьовує КАМ1 та в той самий час він керує RTPE1, який в свою чергу відповідає за встановлення голосового RTP потоку між абонентами Phone1 та Phone2. В разі закінчення виклику одним з абонентів, КАМ11 надає команду на припинення RTP потоку RTPE1 та з'єднання розривається.

Загальну доступність системи можна оцінити за допомогою формули [14]:

$$A = \frac{MTBF}{MTBF + MTTR},$$

де MTBF (Mean Time Between Failures) – середній час між відмовами; MTTR (Mean Time to Repair) – середній час відновлення після збою.

Розрахунок доступності в нашому випадку можна виконати, виходячи з наступних даних:

– MTBF для класичної та високодоступної схеми традиційно приймають довжиною два тижні або 336 год. (1209600 с);

– MTTR для класичної системи становить 60 хв., або 3600 с. Саме стільки часу вимагає розгортання серверу з резервної копії;

– MTTR для високодоступної системи становить 1 с, це час перемикання активного вузла сервера на гарячий резерв.

Тоді чисельно доступність класичної системи буде:

$$A = 1\,209\,600/(1\,209\,600 + 3600) = 99{,}7\ \%,$$

а доступність високодоступної системи:

$$A = 1\,209\,600/(1\,209\,600 + 1) = 99{,}9999\ \%.$$

Розглянемо випадки, коли будемо мати відмову одного або декількох елементів системи:

1. З'єднання було успішно встановлено за алгоритмом, описаним вище, але згодом маємо відмову сервера сигналізації КАМ1. Голосовий потік продовжує функціонувати, але такий виклик «ніколи» не завершився б у разі відсутності КАМ2, який контролює SIP транзакції сервера КАМ1 по логічному каналу «DMQ interface». Таким чином КАМ2 «підхоплює» усі активні сигнальні транзакції КАМ1.

2. З'єднання було успішно встановлено за алгоритмом, описаним вище, але згодом маємо відмову RTPE1. В такому випадку, завдяки додатковому алгоритму та наявності бази даних REDIS, RTPE2 бере на себе «доопрацювання» голосового RTP потоку в той самий час як SIP Server 1 продовжує обробляти сигналізацію.

Об'єктом дослідження є проведення двох експериментів:

А. Збереження голосового виклику та його коректне опрацювання після програмного або апаратного збою сигнального сервера КАМ1, який керує цим викликом.

Б. Збереження голосового виклику та його коректне опрацювання після програмного або апаратного збою медіа шлюза RTPE1, який опрацьовує голосовий потік.

Суть проведення експерименту *А* в наступному:

1) абонент Phone1 здійснює виклик абонента Phone2 в системі, наведеній на рис. 2;

2) після успішного встановлення з'єднання між цими абонентами ми штучно вносимо відмову сигнального серверу КАМ1, власне вимикаємо віртуальний комп'ютер;

3) оскільки всі SIP-транзакції «віддзеркалюються» в сигнальному сервері КАМ2, а ПЗ Keepalive впроваджує коректний статус сигнального сервера (в даному випадку КАМ2 змінює свій статус з резервного на основний) та продовжує керувати всіма транзакціями, раніше отриманими від КАМ1;

4) в разі отримання сервером КАМ2 сигнальних повідомлень в рамках SIP-транзакції, яка була створена КАМ1, КАМ2 відшукує цю транзакцію у власній БД та продовжує обробляти цей виклик.

Сигнальний трейс голосового виклику описаного вище, наведено на рис. 3, момент відповіді сигнального серверу КАМ2 позначено міткою [takeover].

Суть проведення експерименту *Б* в наступному:

1) абонент Phone1 здійснює виклик абонента Phone2 в системі, наведеній на рис. 2;

2) SIP транзакція буде опрацьована сигнальним сервером КАМ1, а голосовий потік формується медіа шлюзом RTPE1;

3) після успішного встановлення з'єднання між цими абонентами ми штучно вносимо відмову сигнального серверу RTPE1, власне вимикаємо віртуальний комп'ютер;

4) REDIS відстежує вихід з ладу медіа шлюзу RTPE1 та виконує аварійне перемикання сесій на RTP2;

5) RTPE2 виконує обробку RTP трафіка для існуючих та нових голосових викликів.

На рис. 3 наведено голосовий виклик між абонентами Phone1 та Phone2 через високодоступну VoIP систему, яка складається з абонентських SIP-терміналів Phone1 та Phone2, серверів сигналізації КАМ1 та КАМ2 та SIP proxy, який в данному випадку виконує роль ретранслятора SIP повідомлень та надає можливість зібрати повний трейс сигнального обміну між вищезазначеними еле-

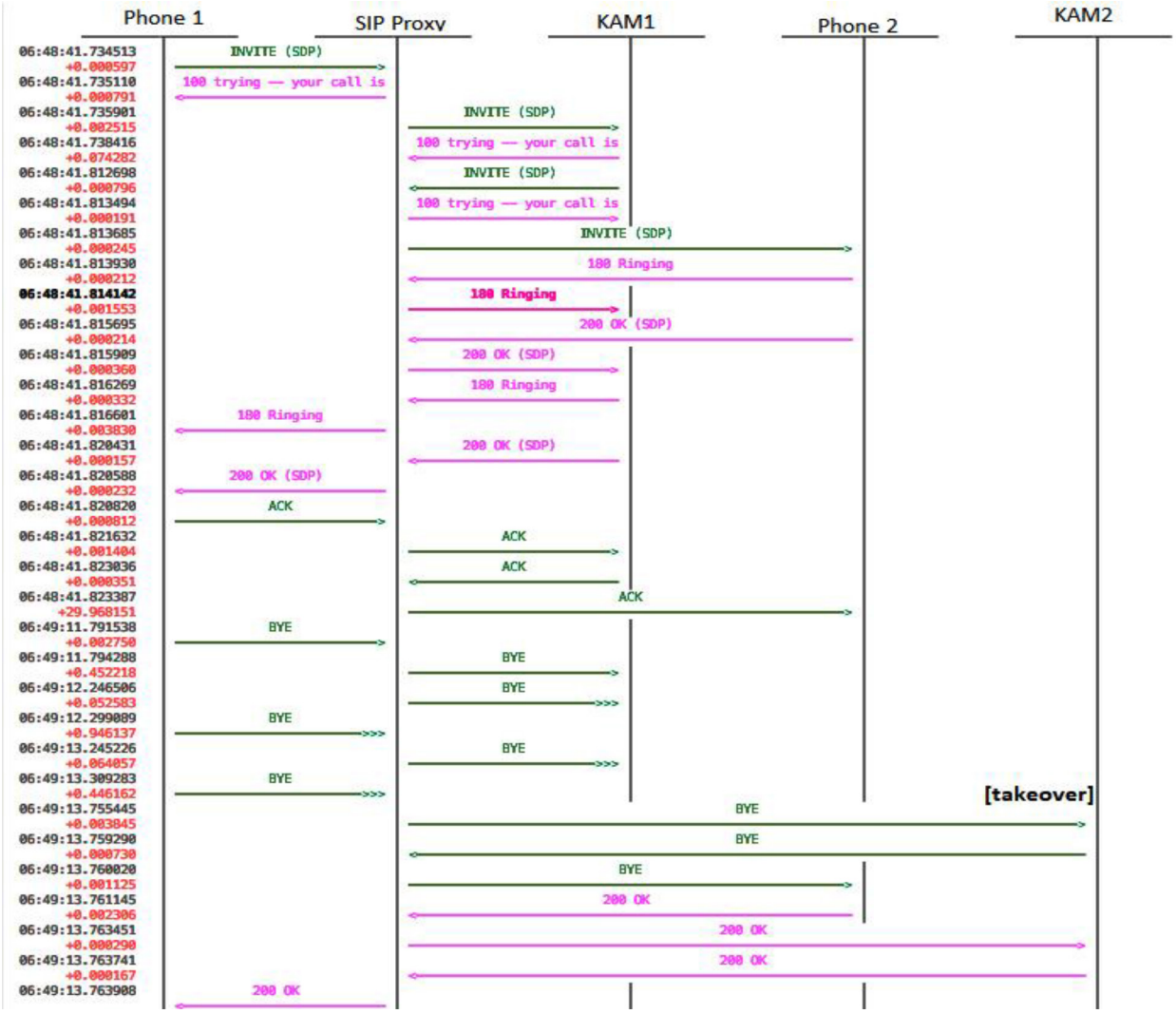

Рис. 3. Сигнальний трейс голосового виклика (Voice call signal trace) з подальшою відмовою сигнального сервера КАМ1

ментами системи. Розглянемо більш детально як саме проходить голосовий виклик.

На момент 06:48:41.734513 від абонента Phone1 надходить SIP-повідомлення **INVITE**, мета якого створити нову сесію голосового зв'язку з унікальним ідентифікатором **call-id** [1]. У відповідь на **INVITE**, абонент Phone1 отримує повідомлення **100 Trying** (запит у обробці) від SIP Proxy, який в свою чергу ретранслює повідомлення **INVITE** до сигнального серверу КАМ1, що є активним за замовченням. КАМ1 у свою чергу перевіряє внутрішню таблицю маршрутизації, знаходить IP адресу абонента Phone2, змінює його в полі «**To:**» повідомлення **INVITE**, та пересилає його до SIP Proxy в момент часу 06:48:41.812698.

Після отримання **INVITE**, SIP Proxy пересилає його кінцевому абоненту Phone2 та у відповідь отримує повідомлення **180 Ringing** (викликаємо абонента), яке в свою чергу транслюється сигнальному серверу КАМ1.

В 06:48:41.815692 від абонента Phone2 до SIP Proxy надходить повідомлення **200 OK** (абонент відповів на виклик), яке далі транслюється на сигнальний сервер КАМ1 і далі кінцевому абоненту Phone1. Отримавши повідомлення **200 OK** про те, що абонент прийняв голосовий виклик, Phone1 відсилає підтвердження у вигляді повідомлення **ACK**, яке в свою чергу транслюється кінцевому абоненту Phone2 через SIP Proxy та КАМ1 (часовий інтервал 06:48:41.820820 – 06:48:41.823387).

Вносимо штучну відмову сигнального сервера КАМ1 (вимикаємо віртуальну машину).

В 06:49:11.791538 абонент відправляє до SIP Proxy повідомлення про завершення виклику **BYE**, яке транслюється до сигнального серверу КАМ1.

Не отримавши ніякоі відповіді від сигнального серверу КАМ1, SIP Proxy відправляє повідомлення **BYE** до серверу КАМ2, який в свою чергу ідентифікує транзакцію по SIP call-id, раніше отрима-

ного через DMQ інтерфейс від серверу КАМ1 та пересилає його кінцевому абоненту Phone2.

В свою чергу абонент Phone2 відправляє повідомлення про підтвердження завершення виклику **200 ОК** до абонента Phone1 по ланцюгу Phone2 – SIP Proxy – КАМ2 – SIP Proxy – Phone1.

Таким чином ми бачимо, що після відмови сигнального серверу КАМ1 SIP-діалог не обривається, а в 06:49:13.755445 продовжується оброблятися сигнальним сервером КАМ2. Переключення на гарячий резерв виконується в автоматичному режимі, завдяки чому вплив на сервіс з'єднання відсутній.

Висновки. Створена структурна модель високодоступної VoIP-системи, яка зазначена на рис. 2, і шляхом використання програмного забезпечення для віртуалізації комп'ютерних систем виконано її моделювання. Доступність змодельованої системи становить 99,9999 %, і навіть в разі відмови 50 % компонентів системи всі існуючі та нові голосові виклики продовжують опрацьовуватися.

Представлено метод підвищення доступності VoIP-системи у разі відмови одного або декількох її компонентів, який відрізняється від традиційних підходів збереженням всіх існуючих медіа-викликів в разі відмови одного або декількох компонентів та використанню безкоштовного програмного забезпечення. Основна відмінність даного методу полягає в тому, що при відмові одного з двох серверів (КАМх та RTPEx) система не втрачаємо жодного встановленого виклику та має змогу опрацьовувати нові. Схема системи має єдину точку входу (IP адрес для прийому/відправки викликів з/на зовні), яка є незмінною в разі відмови елементів системи.

Представлені типові сценарії відмов компонентів сигнального серверу КАМ1 та медіа шлюзу RTPE1.

Список літератури:

1. Rosenberg J., Schulzrinne H., Camarillo G., Johnston A., Peterson J., Sparks R., Handley M., Schooler E. SIP: Session Initiation Protocol. RFC 3261. Internet Engineering Task Force (IETF) 2002, 269p.

2. Alo U. R., Nweke H. F., Voice over Internet Protocol (VOIP): Overview, Direction And Challenges. Journal of Information Engineering and Applications, Vol.3, No.4, pp.18-28, 2013, URL: https://www.researchgate.net/publication/342_Voice_over_Internet_Protocol_VOIP_Overview_Direction_And_Challenges

3. Vetoshko I. P., Kravchuk S. O. Possibilities of improving the voice services quality in 5G networks. Information and Telecommunication Sciences. 2023. Vol.14, No 2. pp. 9-16, https://doi.org/10.20535/2411-2976.22023.9-16

4. Ahson M. VoIP Handbook: Applications, Technologies, Reliability, and Security. Ilyas, CRC Press, 2009. 472 p.

5. Habraken J. Practical Cisco Routers. QUE USA, 1999. 315 p.

6. Roy O. P., Kumar V. A Survey on Voice over Internet Protocol (VoIP) Reliability Research. IOP Conference Series: Materials Science and Engineering. 6th International Conference on Computers Management & Mathematical Sciences (ICCM 2020) Vol. 1020, 2020. pp. 12–19 Nirjuli, India, DOI 10.1088/1757-899X/1020/1/012015.

7. Snir Y., Ramberg Y., Strassner J., Cohen R., Policy Quality of Service (QoS) Information Model, RFC 3644. Internet Engineering Task Force (IETF), 2003. 73p.

8. Schulzrinne H., Casner S., Frederick R. RTP: A Transport Protocol for Real-Time Applications. RFC 3550. Internet Engineering Task Force (IETF), 2003. 104 p.

9. Tulemu W., Design of an asterisk-based VoIP system and the implementation of security solution across the VoIP network. World Journal of Advanced Research and Reviews, 2024, Vol.1, № 23(01), P.875–906 DOI: https://doi.org/10.30574/wjarr.2024.23.

10. Tobiloba K. A., Building a Secure Asterisk-Based VoIP System Design and Implementation, Researchgate, 2023. Vol. 4, № 9(82). p. 4–11. URL: https://www.researchgate.net/publication/388707610

11. Martin A., Gamess E., Urribarri D., Gómez J. A Proposal for A High Availability Architecture for VoIP Telephone Systems based on Open Source Software. (IJACSA) International Journal of Advanced Computer Science and Applications, 2021. Vol. 9, No. 9, 20. 2023. URL: https://thesai.org/Downloads/Volume9No9/Paper_1-A_Proposal_for_a_High_Availability_Architecture.pdf

12. The Sipwise C5 CE Handbook mr8.5.10. 400p. URL: https://www.sipwise.com/doc/mr8.5.10/handbook-ce.pdf.

13. Wu W. Packet Forwarding Technologies. Auerb Publications. 2008. 446 p.

14. Ahmed A., Madani H., Siddiqui T., Voip Performance Management and Optimization, Cisco Press. 2010. 448 p.

15. Mierla D. C., Modroiu E. R. "SIP Routing with Kamailio" 2022 356p.

16. Pal S., Gadde R., Latchman H.A. On The Reliability of Voice Over IP Telephony. Computer Science, Engineering. 2011. URL: https://www.iiis.org /CDs2011/CD2011IMC/CCCT_2011/PapersPdf/TA224EV.pdf.
17. Carlson J.L. Redis in action. 2013. 320 p.

Priymak S.O., Kravchuk S.O. METHOD OF INCREASING THE AVAILABILITY OF VOIP SYSTEMS

The article reveals methods of increasing VoIP (Voice over IP) system availability. Authors analyzed main challenges associated with the operation of VoIP systems, in particular the need to ensure service continuity, fault tolerance, scalability and resource efficiency. Method given for increasing the availability of a VoIP system is based on use of free software: Kamailio (SIP signaling server), RTPengine (media traffic processing), Redis (in-memory database for storing RTP transactions) and Linux Ubuntu as a host operating system. Implemented architecture reflects automatic failover of signaling servers and media gateways, load balancing and seamless switching to backup node in case of failure of one or more components. The approach given is drastically differs from others, where failure of one of the key elements (signaling server or media gateway) leads to immediate termination of all active connections. Authors performed experimental simulation of the system by deploying high availability schema depicted on pic.1 into virtual environment and confirmed its high efficiency: even in the event of 50 % components failure, the system remains operational and does not interrupt any active voice call. An analysis of existing traditional approaches in creation of VoIP systems has been conducted and it reveals inability to save existing calls in the event of signaling server or media gateway failure. Obtained results may be useful for developers and operatonal staff of VoIP fixed or mobile telecom networks as well as enterprises which using IP telephony for communications. Given system allows to minimize the risks of communication interruption, improving the quality of user service and ensuring high reliability of VoIP services.

Key words: *VoIP system, SIP, RTP, high availability, reliability.*