НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий інститут телекомунікаційних систем

Кафедра телекомунікацій

До захисту допущено:

Завідувач кафедри

_____ Сергій КРАВЧУК

«___»_____2024 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Інженерія та програмування інфокомунікацій»

спеціальності 172 «Телекомунікації та радіотехніка»

на тему: «Корпоративна мережа IP телефонії на атомній електростанції (АЕС)»

Виконав:
студент IV курсу, групи ТЗ-02
Молєв Вадим Олександрович _____

Керівник:
Професор кафедри ТК НН ІТС, д.т.н., професор
Романов Олександр Іванович _____

Рецензент:
Доцент кафедри ЕКІР НН ІТС, к.т.н., доцент
Бердников Олег Михайлович _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2024 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий інститут телекомунікаційних систем
Кафедра телекомунікацій

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Інженерія та програмування інфокомунікацій»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Сергій КРАВЧУК
«___»_____2024 р.

ЗАВДАННЯ
на дипломну роботу студенту
Молєву Вадиму Олександровичу

1. Тема роботи «Корпоративна мережа IP телефонії на атомній електростанції (АЕС)», керівник роботи Романов Олександр Іванович, професор, д.т.н., затверджені наказом по університету від «22» травня 2024 р. № 2064-с.

2. Термін подання студентом роботи 10 червня 2024 р.

3. Вихідні дані до роботи: розробити надійну та безпечну корпоративну мережу IP-телефонії на основі протоколу SIP для забезпечення стійкого голосового та мультимедійного зв'язку на атомній електростанції з урахуванням підвищених вимог до безпеки, конфіденційності та відмовостійкості.
4. Зміст роботи: Аналіз сучасного стану корпоративної мережі зв'язку на атомній електростанції; Дослідження технології SIP телефонії, принципи її функціонування, етапи встановлення SIP дзвінків, забезпечення якості обслуговування, інтеграція з іншими системами, а також питання безпеки та надійності; розробка SIP телефонної мережі на атомній електростанції, включаючи вибір обладнання та програмного забезпечення, налаштування та конфігурацію компонентів, а також тестування та безпосереднє впровадження системи.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

Слайд №1 Назва роботи

Слайд№2 Мета роботи

Слайд№3 Актуальність теми

Слайд№4 Розділ дипломної роботи №1

Слайд№5 Розділ дипломної роботи №2

Слайд№6 Розділ дипломної роботи №3

Слайд№7 Висновки

6. Дата видачі завдання 15.04.2024 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Огляд технології IP телефонії та протоколу ініціації сесії (SIP)	21.04-22.04.2024	Виконано
2	Дослідження переваг та вимог до впровадження SIP-базованої IP телефонії на АЕС	23.04-28.04.2024	Виконано
3	Розробка архітектури та компонентів корпоративної SIP-мережі для АЕС	29.04-10.05.2024	Виконано
4	Вивчення питань безпеки, надійності та відмовостійкості SIP-мереж для АЕС	11.05-17.05.2024	Виконано
5	Висновки	18.05-20.05.2024	Виконано
6	Оформлення пояснювальної записки	07.06.2024	Виконано

Студент Вадим МОЛЄВ

Керівник Олександр РОМАНОВ

РЕФЕРАТ

Дипломна робота викладена на 76 сторінках та включає 13 ілюстрацій, та 10 джерел.

Метою роботи є дослідження та аналіз мережі корпоративного зв'язку на АЕС на основі технології SIP (Session Initiation Protocol) для забезпечення ефективної та надійної комунікації.

Об'єкт дослідження: мережі корпоративного зв'язку на АЕС.

Предмет дослідження: технологія SIP та її застосування в мережах корпоративного зв'язку на АЕС.

Актуальність теми: На атомних електростанціях надзвичайно важливо мати надійну та ефективну систему корпоративного зв'язку для забезпечення безперебійної комунікації між різними підрозділами та персоналом. Технологія SIP дозволяє створювати гнучкі та масштабовані рішення для передачі голосу та відео через IP-мережі. Її впровадження в мережах корпоративного зв'язку на АЕС може значно покращити комунікацію, підвищити рівень безпеки та ефективності роботи персоналу.

Методи дослідження: Аналіз існуючих рішень та технологій у сфері корпоративного зв'язку на АЕС, вивчення технології SIP та її можливостей, моделювання та тестування мережі корпоративного зв'язку на основі SIP.

Отримані результати: У результаті дослідження буде проаналізовано переваги та недоліки використання технології SIP в мережах корпоративного зв'язку на АЕС, розроблено рекомендації щодо архітектури та конфігурації такої мережі, а також надано приклади практичної реалізації та тестування. Це дозволить підвищити ефективність та надійність комунікації на АЕС, що є критично важливим для забезпечення безпеки та безперебійної роботи атомної електростанції.

Ключові слова: АТОМНА ЕЛЕКТРОСТАНЦІЯ, МЕРЕЖА КОРПОРАТИВНОГО ЗВ’ЯЗКУ, SIP ТЕЛЕФОНІЯ.

ABSTRACT

The thesis is laid out on 76 pages and contains 13 illustrations and 10 sources.

The purpose of the work is research and analysis of the corporate communication network at the NPP based on SIP (Session Initiation Protocol) technology to ensure effective and reliable communication.

Object of research: corporate communication networks at the NPP.

Research subject: SIP technology and its application in corporate communication networks at NPPs.

Relevance of the topic: At nuclear power plants, it is extremely important to have a reliable and efficient corporate communication system to ensure uninterrupted communication between various departments and personnel. SIP technology allows you to create flexible and scalable solutions for voice and video transmission over IP networks. Its implementation in corporate communication networks at the NPP can significantly improve communication, increase the level of safety and efficiency of personnel.

Research methods: Analysis of existing solutions and technologies in the field of corporate communication at the NPP, study of SIP technology and its capabilities, modeling and testing of a SIP-based corporate communication network.

Results: As a result of the study, the advantages and disadvantages of using SIP technology in corporate communication networks at the NPP will be analyzed, recommendations will be developed regarding the architecture and configuration of such a network, and examples of practical implementation and testing will be provided. This will increase the efficiency and reliability of communication at the NPP, which is critically important for ensuring the safety and uninterrupted operation of the nuclear power plant.

Keywords: NUCLEAR POWER PLANT, CORPORATE COMMUNICATION NETWORK, SIP TELEPHONY.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АЕС	Атомна електростанція
NGFW	New Generation FireWall
ЦОД	Центр Обробки Данних
SIP	Session Initiation Protocol
QoS	Система керування якістю обслуговування
UC	Уніфіковані комунікації

ВСТУП

Атомні електростанції є критично важливими об'єктами інфраструктури, від надійної роботи яких залежить безперебійне енергопостачання цілих регіонів. Ефективні та безпечні комунікації між персоналом різних відділів АЕС мають вирішальне значення для забезпечення злагодженої експлуатації, своєчасного реагування на інциденти та дотримання суворих норм безпеки.

Нинішні мережі корпоративного зв'язку на багатьох атомних електростанціях базуються на застарілих технологіях комутованих телефонних мереж (TDM). Ці традиційні TDM-системи, хоча й мають перевірену надійність, обмежені у своїх можливостях та страждають від низки недоліків, що можуть негативно позначитися на ефективності комунікацій та операційній діяльності АЕС.

Одним з основних недоліків є висока вартість обслуговування TDM-мереж, яка включає необхідність спеціалізованого обладнання, програмного забезпечення та висококваліфікованого персоналу для ремонту та модернізації. Крім того, ці системи мають обмежену масштабованість, що ускладнює розширення мережі для задоволення зростаючих потреб у зв'язку.

Проте, найбільшим недоліком традиційних TDM-мереж є їхня відсутність гнучкості для інтеграції з сучасними технологіями та додатками. Зокрема, відсутня підтримка протоколу ініціації сесії (SIP) - відкритого стандарту для мультимедійних комунікацій через Інтернет, який дозволяє об'єднувати голосові дзвінки, відеоконференції, обмін миттєвими повідомленнями та інші функції уніфікованих комунікацій в одній платформі.

SIP-технологія пропонує численні переваги для корпоративних комунікацій на АЕС, включаючи покращену масштабованість, зниження витрат на зв'язок та більшу гнучкість для інтеграції з різноманітними додатками та пристроями. Впровадження SIP-рішень може значно підвищити ефективність співпраці персоналу АЕС, забезпечити швидкий обмін критично

важливою інформацією та полегшити управління комунікаціями в режимі реального часу.

Отже, модернізація застарілих комунікаційних інфраструктур до сучасних SIP-платформ стає нагальною потребою для атомних електростанцій, щоб забезпечити безпечніші, ефективніші та економічно вигідніші корпоративні комунікації.

РОЗДІЛ 1
СУЧАСНИЙ СТАН МЕРЕЖІ КОРПОРАТИВНОГО ЗВ’ЯЗКУ НА АЕС

1.1 Загальна архітектура мережі корпоративного зв'язку на АЕС

1.1.1 Адміністративний сегмент

Атомні електростанції є критично важливими об'єктами інфраструктури, де надійні та ефективні комунікації відіграють вирішальну роль для забезпечення безпечної та безперебійної роботи. Однак, на багатьох АЕС досі використовуються застарілі мережі корпоративного зв'язку, засновані на традиційних технологіях комутованих телефонних мереж (TDM).

Ці TDM-системи, незважаючи на їхню перевірену надійність, мають ряд серйозних недоліків. По-перше, вони є дорогими в обслуговуванні, оскільки потребують спеціалізованого обладнання, програмного забезпечення та висококваліфікованого персоналу для ремонту та модернізації. По-друге, вони мають обмежену масштабованість, що ускладнює розширення мережі для задоволення зростаючих потреб у зв'язку на АЕС. Крім того, відсутність гнучкості для інтеграції з сучасними додатками, такими як уніфіковані комунікації, мультимедійні конференції та обмін миттєвими повідомленнями, обмежує можливості співробітників ефективно співпрацювати та своєчасно обмінюватися критично важливою інформацією[1].

Загальна архітектура мережі корпоративного зв'язку на АЕС розроблена з урахуванням жорстких вимог до безпеки, надійності та захисту критичних систем. Вона має багаторівневу структуру з чітким розподілом на декілька ізольованих сегментів.

На верхньому рівні знаходиться адміністративний сегмент, який призначений для обслуговування офісних додатків, корпоративних ресурсів та доступу до Інтернету. Цей сегмент фізично відокремлений від виробничої мережі за допомогою окремих комунікаційних каналів та активного мережевого обладнання. Для забезпечення ізоляції та захисту використовуються потужні брандмауери нового покоління (NGFW) та системи виявлення і запобігання вторгнень (IDS/IPS). Вони виконують

глибокий аналіз мережевого трафіку, контролюють додатки та блокують потенційні кіберзагрози. Це дозволяє мінімізувати ризики проникнення шкідливого програмного забезпечення чи несанкціонованого доступу до критичних систем АЕС з адміністративної мережі або Інтернету.

1.1.2 Виробнича мережа

Виробнича мережа відповідає за підтримку основних технологічних процесів АЕС і поділяється на два окремі сегменти: технологічний та інформаційний.

Технологічний сегмент забезпечує зв'язок між системами керування та контролю технологічних процесів АЕС. До нього входять системи управління реакторами, турбінами, електричними підстанціями, системи безпеки та інші критично важливі системи. Цей сегмент має топологію жорсткої зірки, де всі системи безпосередньо підключені до центральних комутаторів. Така топологія мінімізує кількість точок відмови та підвищує надійність мережі. Зв'язок між критичними системами здійснюється через захищені канали передачі даних з використанням технологій віртуальних приватних мереж (VPN) та шифрування трафіку.

Інформаційний сегмент призначений для збору, обробки та зберігання даних про стан обладнання, показники технологічних процесів, параметри експлуатації та інших виробничих даних АЕС. Він має більш гнучку структуру, що поєднує топології "дерево" та "кільце". Це забезпечує високу відмовостійкість, оскільки кільцева топологія дозволяє автоматично перенаправляти трафік в разі пошкодження певної ділянки мережі. Топологія "дерево" використовується для ієрархічної організації мережі та масштабування шляхом додавання нових підмереж та вузлів.

Крім фізичного розділення, для ізоляції різних сегментів використовуються технології віртуальних локальних мереж (VLAN). Кожен сегмент складається з окремих VLAN, що дозволяє логічно розділити трафік та підвищити рівень безпеки.

Всі сегменти мережі захищені комплексом заходів безпеки, включаючи брандмауери, системи виявлення вторгнень (IDS) та запобігання вторгненням (IPS). Ці системи постійно аналізують мережевий трафік на предмет виявлення підозрілої активності чи потенційно шкідливих дій та блокують їх на ранніх стадіях.

Така багаторівнева архітектура з чіткою сегментацією та ізоляцією забезпечує високий рівень безпеки критичних систем АЕС, надійність зв'язку та можливість гнучкого масштабування в майбутньому. Вона відповідає жорстким галузевим стандартам та нормативним вимогам до мереж зв'язку на об'єктах атомної енергетики.

1.2 Активне мережеве обладнання

Активне мережеве обладнання є невід'ємною складовою корпоративної мережі зв'язку на АЕС, забезпечуючи передачу даних, керування трафіком та захист від зовнішніх загроз. Основними елементами є:

Маршрутизатори відіграють ключову роль у забезпеченні зв'язку між різними сегментами мережі АЕС. Вони виконують маршрутизацію трафіку відповідно до визначених правил, керуючи потоками даних між окремими підмережами та сегментами. На АЕС використовуються потужні промислові маршрутизатори, розраховані на роботу в критично важливих середовищах. Вони мають високу продуктивність, надійність та вбудовані функції мережевої безпеки.

Окрім маршрутизації, ці пристрої виконують низку функцій безпеки, таких як фільтрація трафіку на основі списків контролю доступу (ACL), підтримка віртуальних приватних мереж (VPN) та шифрування даних. Це допомагає захистити критичні сегменти мережі АЕС від несанкціонованого доступу та перехоплення конфіденційної інформації.

Комутатори використовуються для об'єднання кінцевих пристроїв та обладнання в межах одного сегмента мережі. Вони забезпечують високошвидкісну передачу даних та керування потоками трафіку на рівні локальної мережі. На АЕС застосовуються промислові комутатори з

підвищеною стійкістю до несприятливих факторів зовнішнього середовища, таких як вібрації, електромагнітні перешкоди та коливання температури.

Сучасні комутатори на АЕС підтримують функції управління трафіком, такі як встановлення пріоритетів для критичних потоків даних, резервування каналів зв'язку та захист від петель у мережі. Вони також можуть виконувати ролі брандмауерів на рівні локальної мережі, фільтруючи та блокуючи небажаний трафік.

Брандмауери відіграють ключову роль у забезпеченні безпеки мережі АЕС, виконуючи функції контролю та фільтрації мережевого трафіку. Вони захищають критичні системи від несанкціонованого доступу, кібератак та проникнення шкідливого програмного забезпечення.

На АЕС застосовуються брандмауери нового покоління (NGFW), які поєднують традиційні функції фільтрації пакетів з додатковими можливостями, такими як:

- Виявлення та запобігання вторгненням (IDS/IPS)
- Контроль додатків та захист від шкідливих програм
- Глибокий аналіз трафіку на різних рівнях (пакетів, протоколів, додатків)
- Підтримка шифрування даних та технологій VPN

Такі розширені функціональності NGFW дозволяють ефективно протидіяти сучасним кіберзагрозам та забезпечувати надійний захист критичних сегментів мережі АЕС.

Усе активне мережеве обладнання на АЕС підлягає ретельному контролю та регулярному оновленню програмного забезпечення для усунення виявлених вразливостей та підтримки актуального рівня безпеки.

1.3 Середовища передачі даних

Корпоративна мережа АЕС використовує різноманітні середовища передачі даних для забезпечення надійного зв'язку між ключовими вузлами та системами. Основними середовищами є:

Волоконно-оптичні лінії зв'язку є основою корпоративної мережі АЕС і використовуються для магістральних каналів зв'язку між критично важливими об'єктами та мережевими вузлами. Вони забезпечують високу швидкість передачі даних, що сягає десятків і сотень гігабіт в секунду, а також великі відстані покриття.

Оптоволоконні кабелі прокладені між ключовими вузлами мережі, такими як центри обробки даних, серверні приміщення, комунікаційні вузли та розподільні пункти. Вони також під'єднують критичні об'єкти АЕС, такі як реактори, турбіни, електричні підстанції та системи безпеки.

Перевагами оптоволоконних ліній є висока пропускна здатність, стійкість до електромагнітних перешкод, що особливо важливо в умовах АЕС, а також велика відстань передачі сигналу без повторювачів. Ці властивості забезпечують надійний та швидкісний обмін даними між ключовими елементами корпоративної мережі[2].

Для підключення окремих пристроїв, обладнання та локальних мереж у межах одного приміщення або будівлі широко використовуються мідні кабельні системи. Найпоширенішими є кабелі вити пари та коаксіальні кабелі.

Кабелі вити пари застосовуються для створення локальних мереж Ethernet та підключення персональних комп'ютерів, принтерів, сканерів та іншого офісного обладнання. Вони забезпечують надійний зв'язок на відстанях до 100 метрів та швидкості передачі даних до 10 Гбіт/с.

Коаксіальні кабелі використовуються для підключення більш віддалених пристроїв та створення бездротових мереж. Вони можуть забезпечувати зв'язок на відстанях до кількох кілометрів та швидкості до 10 Гбіт/с.

У деяких зонах АЕС, де прокладка кабелів є складною або небезпечною, застосовуються бездротові технології передачі даних. Найпоширенішими є технології WiFi та радіорелейні лінії зв'язку.

Технологія WiFi використовується для створення бездротових локальних мереж (WLAN) та забезпечення мобільного доступу користувачів

до корпоративних ресурсів. Вона дозволяє швидко розгортати тимчасові або мобільні мережеві рішення без необхідності прокладання кабелів.

Радіорелейні лінії зв'язку застосовуються для організації магістральних каналів передачі даних між територіально рознесеними об'єктами АЕС. Вони забезпечують високошвидкісний зв'язок на великих відстанях за допомогою ретрансляторів.

Однак бездротові технології вимагають ретельного аналізу безпеки та захисту від перехоплення сигналу. На АЕС використовуються спеціальні заходи, такі як шифрування трафіку, аутентифікація пристроїв та контроль доступу для забезпечення належного рівня конфіденційності та цілісності даних.

1.4 Системи резервування та відмовостійкості

Забезпечення безперервної та надійної роботи є ключовим пріоритетом для корпоративної мережі зв'язку на АЕС. Будь-які збої чи перебої у функціонуванні мережі можуть мати критичні наслідки для безпеки та керованості технологічними процесами станції. Тому на АЕС реалізовано комплексні багаторівневі системи резервування та відмовостійкості, що забезпечують високу стійкість мережі до різноманітних збоїв та аварійних ситуацій.

На фізичному рівні передбачено резервні маршрути передачі даних між ключовими вузлами мережі. Ці резервні канали використовують альтернативні топології прокладання кабелів та різні середовища передачі даних. Наприклад, між двома вузлами може бути прокладено два повністю роздільні волоконно-оптичні кабелі різними маршрутами. У разі пошкодження одного кабелю, трафік автоматично перенаправляється на резервний канал без переривання з'єднання.

Крім того, застосовуються технології радіорелейного та бездротового зв'язку, які можуть виступати в ролі резервних каналів для основних волоконно-оптичних ліній. Ці бездротові канали використовують

альтернативні фізичні шляхи розповсюдження сигналу, що забезпечує їх незалежність від стану кабельної інфраструктури.

Усе критичне активне мережеве обладнання, таке як маршрутизатори, комутатори та брандмауери, має повноцінні резервні дублікати. Ці резервні пристрої підключені до мережі та знаходяться в режимі гарячого резервування, постійно відстежуючи стан основного обладнання. У разі виходу з ладу основного пристрою, його функції автоматично і миттєво переходять на резервний вузол без переривання мережевих з'єднань.

Для забезпечення надійності резервування застосовуються різні технології, такі як кластеризація обладнання, віртуалізація мережевих функцій (NFV) та протоколи резервування, наприклад, VRRP (Virtual Router Redundancy Protocol).

Ключова роль в забезпеченні безперервності роботи мережі належить центрам обробки даних (ЦОД), де розміщуються критичні мережеві сервери, системи зберігання даних та інше обладнання. На АЕС реалізовано високодоступні кластери ЦОД з використанням технологій кластеризації та віртуалізації.

Критичні сервери та системи зберігання даних об'єднані в кластери, де навантаження може динамічно перерозподілятися між активними вузлами. Якщо певний вузол виходить з ладу, його роботу автоматично перебирають на себе інші вузли кластера, забезпечуючи безперервність обслуговування мережевих сервісів.

Для підвищення надійності використовуються технології висококластерних систем зберігання даних, такі як RAID, а також резервні сховища даних для створення резервних копій критичної інформації.

Для забезпечення максимальної відмовостійкості в екстремальних ситуаціях на АЕС передбачено наявність повноцінного резервного центру обробки даних (ЦОД). Він є повною копією основного ЦОД і розташований на значній відстані від нього для запобігання впливу тих самих ризиків.

Резервний ЦОД знаходиться в режимі гарячого резервування та синхронізується з основним ЦОД в режимі реального часу. У разі виходу з ладу основного ЦОД через аварійну ситуацію, пожежу, стихійне лихо чи інші катастрофічні події, резервний ЦОД миттєво бере на себе всі функції та забезпечує безперервність роботи критичних систем АЕС[3].

Загалом, комплексний підхід до резервування на різних рівнях забезпечує надзвичайно високий рівень відмовостійкості корпоративної мережі зв'язку на АЕС. Навіть у випадку виходу з ладу певних компонентів, мережа продовжує функціонувати без переривання критичних зв'язків, керування та моніторингу технологічних процесів. Це гарантує безпечну та безперебійну роботу станції у будь-яких умовах.

Висновки

Застарілі TDM-мережі на атомних електростанціях вже не здатні задовольнити сучасні вимоги до ефективних та безпечних корпоративних комунікацій. Впровадження новітніх технологій, таких як Voice over IP (VoIP) та рішень на основі протоколу ініціації сесії (SIP), є нагальною необхідністю для модернізації комунікаційної інфраструктури АЕС. Це дозволить знизити витрати на зв'язок, підвищити масштабованість, забезпечити безшовну інтеграцію з сучасними додатками та, найголовніше, посилити безпеку та ефективність комунікацій, що є критично важливим для атомних електростанцій.

РОЗДІЛ 2
SIP ТЕЛЕФОНІЯ

2.1. Огляд SIP телефонії

2.1.1 Визначення SIP телефонії

SIP (Session Initiation Protocol) телефонія, також відома як VoIP (Voice over Internet Protocol), є технологією передачі голосового трафіку через IP-мережі, такі як Інтернет або корпоративні мережі. На відміну від традиційних телефонних мереж, які використовують виділені лінії для передачі аналогових або цифрових голосових сигналів, SIP телефонія перетворює голосові дані на цифрові пакети даних і передає їх через існуючу IP-мережу.

Рис.2.1. Session Initiation Protocol

SIP є відкритим стандартом, розробленим Інтернет-інженерним цільовим підрозділом (IETF) для ініціалізації, модифікації та завершення мультимедійних сесій, таких як голосові та відеодзвінки, через IP-мережі. Цей протокол забезпечує встановлення, маршрутизацію та завершення дзвінків, а також управління додатковими функціями, такими як конференц-зв'язок та передача даних.

SIP телефонія базується на клієнт-серверній архітектурі, де клієнтами можуть бути SIP телефони, софтфони (програмні клієнти) або інші SIP-сумісні пристрої, а серверами виступають SIP проксі-сервери та SIP реєстраційні сервери. Під час здійснення дзвінка, клієнт надсилає запит на встановлення з'єднання SIP проксі-серверу, який маршрутизує запит до цільового клієнта,

використовуючи SIP реєстраційний сервер для визначення його поточного місцезнаходження. Якщо цільовий клієнт доступний, він відповідає на запит, і встановлюється мультимедійна сесія між клієнтами для передачі голосового трафіку.

2.1.2 Переваги SIP телефонії

SIP телефонія пропонує низку переваг порівняно з традиційними телефонними мережами:

1. Зниження витрат на комунікації: Оскільки голосовий трафік передається через існуючу IP-мережу, SIP телефонія дозволяє уникнути додаткових витрат на обслуговування та оренду ліній, що є необхідним для традиційних телефонних мереж. Крім того, SIP телефонія часто пропонує більш вигідні тарифи на дзвінки в традиційні телефонні мережі.

2. Масштабованість та гнучкість: SIP телефонна система є більш гнучкою та легко масштабується порівняно з традиційними телефонними мережами. Додавання нових користувачів та функцій не вимагає значних капітальних витрат на оновлення інфраструктури.

3. Інтеграція з додатками уніфікованих комунікацій: SIP телефонія може бути інтегрована з різними додатками уніфікованих комунікацій, такими як відеоконференції, миттєві повідомлення, спільний доступ до екрану та ін. Ця інтеграція дозволяє підвищити продуктивність та ефективність роботи, забезпечуючи зручний спосіб спілкування та співпраці.

4. Підвищена надійність: Завдяки децентралізованій архітектурі SIP телефонії та можливості резервування, забезпечується підвищена надійність та безперервність роботи системи. У разі виходу з ладу одного з компонентів, дзвінки можуть бути автоматично перенаправлені на резервний вузол.

5. Мобільність: SIP телефонія забезпечує можливість перенесення дзвінків між різними пристроями та місцями розташування. Користувачі можуть легко переключатися між SIP телефонами в офісі, софтфонами на персональних комп'ютерах або мобільними додатками, зберігаючи безперервність комунікації.

6. Додаткові функції: SIP телефонія пропонує широкий спектр додаткових функцій, таких як голосова пошта, інтерактивний голосовий відповідач (IVR), конференц-зв'язок, запис розмов та інтеграція з базами даних і CRM-системами.

2.1.3 Компоненти SIP телефонної системи

Типова SIP телефонна система включає такі основні компоненти:

1. SIP телефони або софтфони: Це пристрої або програмні клієнти, що використовуються для здійснення дзвінків через SIP телефонну систему. SIP телефони є спеціалізованими апаратними пристроями, призначеними для голосового зв'язку, тоді як софтфони - це програмні клієнти, що встановлюються на персональних комп'ютерах або мобільних пристроях.

2. SIP проксі-сервер: Це центральний компонент SIP телефонної системи, який відповідає за маршрутизацію викликів між користувачами. SIP проксі-сервер отримує запити на встановлення з'єднання від клієнтів і направляє їх до цільових адресатів, використовуючи інформацію від SIP реєстраційного сервера.

3. SIP реєстраційний сервер: Цей компонент зберігає інформацію про поточне місцезнаходження користувачів та їхні SIP адреси. Коли користувач реєструється в системі, SIP реєстраційний сервер зберігає його поточну IP-адресу та інші дані, необхідні для маршрутизації викликів.

4. Шлюзи: SIP телефонна система часто вимагає взаємодії з традиційними телефонними мережами, такими як аналогові або цифрові мережі. Для забезпечення цієї взаємодії використовуються SIP шлюзи, які перетворюють формати сигналів між SIP та традиційними мережами.

5. Система керування якістю обслуговування (QoS): Оскільки голосовий трафік є чутливим до затримок та втрат пакетів, SIP телефонна система повинна включати механізми забезпечення необхідної якості обслуговування (QoS) в IP-мережі. Це може включати пріоритезацію трафіку, управління черговістю, резервування пропускної здатності та інші методи для гарантування належної швидкості та якості передачі голосових даних.

6. Розглянемо приклади використання додаткових компонентів у SIP телефонній мережі на атомній електростанції:

1. Резервні SIP проксі-сервери та SIP реєстраційні сервери: На атомній електростанції можуть бути розгорнуті резервні екземпляри SIP проксі-серверів та SIP реєстраційних серверів для забезпечення високої доступності та безперервності голосового зв'язку. Наприклад, основний SIP проксі-сервер може розташовуватися в центрі управління станцією, а резервний - в окремому захищеному приміщенні. У разі відмови основного сервера, резервний автоматично перехоплює його функції, гарантуючи безперебійну роботу критично важливої комунікаційної системи.

2. Сервери додатків: Сервери додатків можуть бути інтегровані з SIP телефонною мережею для забезпечення спеціалізованих функцій, необхідних на атомній електростанції. Наприклад, сервер додатків може включати систему екстреного оповіщення, яка дозволяє оперативно розсилати важливі повідомлення та інструкції через SIP телефони в критичних ситуаціях. Також сервер додатків може забезпечувати функції конференц-зв'язку для оперативних нарад під час аварійних ситуацій.

3. Медіа-сервери: Для забезпечення сумісності між різними SIP телефонами та системами, що використовуються на атомній електростанції, можуть бути розгорнуті медіа-сервери для транскодування між різними кодеками аудіо та відео. Це дозволить працівникам ефективно спілкуватися, незалежно від типу пристрою, який вони використовують.

4. Сервери безпеки: Забезпечення безпеки є критично важливим на атомній електростанції. Тому SIP телефонна мережа може бути захищена за допомогою спеціалізованих серверів безпеки, таких як брандмауери SIP, системи виявлення вторгнень (IDS/IPS) та VPN-шлюзи для захищеного віддаленого доступу. Ці компоненти допоможуть запобігти несанкціонованому доступу, атакам та витокам конфіденційної інформації.

5. Системи моніторингу та управління: Системи моніторингу та управління відіграють важливу роль у забезпеченні безперебійної роботи SIP

телефонної мережі на атомній електростанції. Вони дозволяють відстежувати продуктивність системи, виявляти та вирішувати проблеми, а також централізовано управляти конфігураціями та оновленнями програмного забезпечення.

6. Системи балансування навантаження: У разі великої кількості користувачів або критично важливих ситуацій, коли очікується значний пік навантаження на SIP телефонну мережу, можуть бути використані системи балансування навантаження. Вони забезпечать рівномірний розподіл трафіку між декількома SIP проксі-серверами, гарантуючи швидке та надійне обслуговування всіх дзвінків.

7. Шлюзи для інтеграції з іншими мережами та протоколами: На атомній електростанції можуть використовуватися різні типи комунікаційних мереж та протоколів, наприклад, аналогові телефонні лінії, радіозв'язок або спеціалізовані промислові протоколи. Для інтеграції SIP телефонної мережі з цими системами можуть бути використані відповідні шлюзи.

8. Системи зберігання даних: Для зберігання записів розмов, журналів подій та іншої важливої інформації, пов'язаної з експлуатацією атомної електростанції, можуть бути задіяні спеціалізовані системи зберігання даних. Ці дані можуть використовуватися для аналізу, розслідування інцидентів та задоволення вимог регулюючих органів.

Впровадження цих додаткових компонентів у SIP телефонну мережу на атомній електростанції забезпечить підвищену надійність, безпеку, функціональність та ефективність критично важливих комунікаційних систем, що є життєво необхідним для безпечної та безперебійної роботи такого об'єкта.

Перспективи переходу на SIP телефонію:

- Зниження витрат на комунікації за рахунок використання інтернет-протоколу для голосового трафіку.

- Покращена масштабованість та гнучкість для додавання нових користувачів та функцій.
- Інтеграція з додатками уніфікованих комунікацій, такими як відеоконференції, миттєві повідомлення тощо.
- Підвищена надійність завдяки децентралізованій архітектурі та можливості резервування.

Структура мережі SIP телефонії:

- SIP проксі-сервер для маршрутизації викликів
- SIP телефони або софтфони (програмні клієнти)
- Шлюзи для взаємодії з традиційними телефонними мережами
- Система керування якістю обслуговування (QoS)
- Функції та елементи SIP телефонної системи:
- Керування викликами (встановлення, маршрутизація, завершення дзвінків) за протоколом SIP
- Голосова пошта, інтерактивний голосовий відповідач (IVR)
- Конференц-зв'язок
- Мобільність (перенесення дзвінків між пристроями)
- Інтеграція з додатками та базами даних

SIP (Session Initiation Protocol) є відкритим стандартом для встановлення, модифікації та завершення мультимедійних сесій, таких як голосові та відеодзвінки через IP-мережі.

2.2 Принципи побудови мережі SIP телефонії

2.2.1 Архітектура мережі

Архітектура мережі SIP телефонії є ключовим фактором, який визначає її гнучкість, масштабованість, надійність та продуктивність. На відміну від традиційних телефонних мереж, SIP телефонія базується на принципах IP-мереж, що дозволяє використовувати різні архітектурні моделі та підходи. Нижче ми розглянемо детальніше клієнт-серверну модель, розподілену архітектуру та децентралізовану архітектуру SIP телефонної мережі.

SIP телефонія побудована на класичній клієнт-серверній моделі, де клієнтські пристрої (SIP телефони, софтфони) взаємодіють із серверними компонентами для встановлення, маршрутизації та завершення дзвінків. У цій моделі клієнти ініціюють запити на встановлення з'єднання, а сервери опрацьовують ці запити та надають необхідні послуги.

Основними серверними компонентами в SIP телефонній мережі є SIP проксі-сервер, який відповідає за маршрутизацію викликів між клієнтами, та SIP реєстраційний сервер, який зберігає інформацію про поточне місцезнаходження користувачів та їхні SIP адреси. Також можуть бути задіяні додаткові сервери, такі як сервери додатків (голосова пошта, IVR), медіа-сервери, сервери безпеки та ін[4].

Клієнт-серверна модель забезпечує централізоване управління та контроль над SIP телефонною мережею, а також дозволяє легко масштабувати систему шляхом додавання додаткових серверних компонентів. Однак, ця модель також має певні недоліки, такі як наявність єдиної точки відмови (якщо центральний сервер виходить з ладу, вся система припиняє роботу) та обмежена горизонтальна масштабованість (складність розподілу навантаження між серверами)[5].

SIP телефонна мережа може бути побудована з використанням розподіленої архітектури, де різні компоненти системи розміщуються в різних місцях та взаємодіють між собою через IP-мережу. Це забезпечує гнучкість та масштабованість, дозволяючи легко додавати нові компоненти або розширювати існуючі.

В розподіленій архітектурі SIP телефонної мережі можуть бути задіяні регіональні або локальні SIP проксі-сервери, резервні SIP проксі-сервери та реєстраційні сервери, географічно розподілені медіа-сервери та розподілені сховища даних. Така архітектура дозволяє розподілити навантаження, забезпечити більшу надійність та продуктивність, а також наблизити окремі компоненти системи до користувачів для зменшення затримок.

Розподілена архітектура забезпечує кращу масштабованість, надійність та відмовостійкість SIP телефонної мережі, проте вона також вимагає ретельного планування та координації між різними компонентами системи, а також може бути складнішою в управлінні та налаштуванні.

На відміну від традиційних телефонних мереж, які часто побудовані на основі централізованої архітектури з єдиним центральним вузлом, SIP телефонна мережа може бути децентралізованою. Це означає, що немає єдиного центрального компонента, який контролює всю систему, а замість цього використовується рівноправна модель, де різні компоненти взаємодіють між собою на основі рівноправних відносин.

У децентралізованій архітектурі SIP телефонної мережі кожен SIP проксі-сервер працює як автономний вузол, який може обробляти запити на встановлення з'єднання та маршрутизувати виклики без залежності від інших проксі-серверів. Ця модель забезпечує високу надійність та відмовостійкість, оскільки відмова одного проксі-сервера не призводить до повного виходу системи з ладу.

Децентралізована архітектура також дозволяє легко масштабувати систему шляхом додавання нових SIP проксі-серверів без необхідності вносити зміни в існуючу інфраструктуру. Нові компоненти можуть бути додані в мережу та автоматично інтегруватися в існуючу систему.

Однак, незважаючи на свої переваги, децентралізована архітектура може бути більш складною в управлінні та налаштуванні, оскільки немає єдиного центрального пункту контролю. Це вимагає ретельного планування та координації між різними компонентами системи, а також може ускладнити деякі функції, такі як глобальна маршрутизація викликів або централізоване управління конфігураціями.

У великих та складних SIP телефонних мережах часто використовується гібридний підхід, який поєднує елементи клієнт-серверної моделі, розподіленої та децентралізованої архітектури. Наприклад, можуть бути використані регіональні SIP проксі-сервери, які працюють за клієнт-

серверною моделлю в межах своєї зони обслуговування, але при цьому вони взаємодіють між собою на основі децентралізованої моделі.

Вибір конкретної архітектури для SIP телефонної мережі залежить від розміру організації, вимог до продуктивності, надійності, масштабованості, а також наявних ресурсів та бюджету. Ретельне планування та аналіз потреб організації є ключовими факторами для забезпечення оптимальної архітектури, яка відповідатиме всім вимогам та забезпечить ефективну та безперебійну роботу комунікаційної системи.

2.2.2 Компоненти SIP мережі

SIP телефонна мережа складається з різних компонентів, кожен з яких відіграє важливу роль у забезпеченні ефективної та надійної роботи системи. Нижче ми розглянемо детальніше основні компоненти SIP мережі.

Рис.2.2. SIP мережа

SIP проксі-сервер є центральним компонентом у SIP телефонній мережі та відповідає за маршрутизацію викликів між клієнтами. Коли клієнт (SIP телефон або софтфон) ініціює дзвінок, він надсилає запит на встановлення з'єднання SIP проксі-серверу. Проксі-сервер, в свою чергу, визначає місцезнаходження цільового клієнта, використовуючи інформацію від SIP реєстраційного сервера, і маршрутизує виклик до нього.

SIP проксі-сервери можуть бути налаштовані для виконання різних функцій, таких як:

- Проксіювання (маршрутизація) викликів
- Перенаправлення викликів
- Керування черговістю викликів
- Запис розмов
- Аутентифікація користувачів

У великих SIP телефонних мережах можуть бути задіяні декілька проксі-серверів, розподілених за регіонами або зонами обслуговування, для забезпечення балансування навантаження та відмовостійкості.

SIP реєстраційний сервер є важливим компонентом, який відповідає за зберігання інформації про поточне місцезнаходження користувачів та їхні SIP адреси. Коли клієнт (SIP телефон або софтфон) реєструється в системі, він надсилає реєстраційний запит SIP реєстраційному серверу, який зберігає його поточну IP-адресу та інші дані, необхідні для маршрутизації викликів[6].

SIP реєстраційні сервери тісно взаємодіють з SIP проксі-серверами, надаючи їм інформацію про місцезнаходження користувачів для коректної маршрутизації викликів. Вони також можуть виконувати функції аутентифікації користувачів та управління їхніми обліковими даними.

SIP шлюзи відіграють важливу роль у забезпеченні взаємодії SIP телефонної мережі з традиційними телефонними мережами, такими як аналогові або цифрові мережі загального користування (PSTN). Вони перетворюють формати сигналів між SIP та іншими протоколами, дозволяючи здійснювати виклики між SIP телефонами та звичайними телефонними апаратами.

Архітектура SIP шлюзів:

- SIP шлюзи зазвичай складаються з двох основних компонентів: контролера сигналізації та медіашлюзу.

- Контролер сигналізації обробляє протоколи сигналізації, такі як SIP, H.323, ISDN або SS7, для встановлення, маршрутизації та завершення викликів.

- Медіашлюз займається транскодуванням медіапотоків (голосу, факсу, відео) між різними кодеками та форматами, використовуваними в SIP та традиційних мережах.

Типи інтерфейсів:

- SIP шлюзи підтримують різні типи інтерфейсів для підключення до різних мереж:
- SIP інтерфейси для з'єднання з SIP мережами
- ISDN PRI/BRI інтерфейси
- Аналогові FXO/FXS інтерфейси
- Інтерфейси T1/E1 для цифрових мереж
- Ethernet/IP інтерфейси для передачі мультимедійних даних

Маршрутизація викликів:

- SIP шлюзи використовують складні алгоритми маршрутизації для визначення найкращого шляху для викликів між SIP та традиційними мережами.
- Вони можуть враховувати різні критерії, такі як вартість маршрутів, доступність ресурсів, якість зв'язку та правила маршрутизації, визначені постачальником послуг.
- Деякі шлюзи підтримують гнучку маршрутизацію на основі номера, що дозволяє направляти виклики в SIP мережу або традиційну мережу залежно від набраного номера.

Функції забезпечення надійності:

- SIP шлюзи часто мають функції резервування та відмовостійкості для забезпечення високої доступності:
- Резервування ліній для альтернативних шляхів передачі даних у разі відмови основного з'єднання
- Підтримка резервування SIP проксі-серверів

- Механізми відновлення після збоїв та перезавантаження

Додаткові функції та інтеграція:

- Багато SIP шлюзів мають додаткові функції, такі як:
- Факсимільний шлюз для передачі факсів між SIP та традиційними мережами
- Інтерактивні голосові меню (IVR) та автовідповідачі
- Запис розмов
- Підтримка додаткових протоколів, таких як WebRTC, для інтеграції з веб-додатками

Управління та моніторинг:

- SIP шлюзи зазвичай мають вбудовані інтерфейси керування та моніторингу, такі як веб-інтерфейс, SNMP або спеціалізовані системи управління.
- Це дозволяє адміністраторам налаштовувати, моніторити та керувати шлюзами для забезпечення належної роботи та продуктивності.

Отже, SIP шлюзи є критичними компонентами, які забезпечують сумісність і безперебійну роботу між SIP телефонними мережами та традиційними телекомунікаційними мережами, надаючи гнучкість, надійність і додаткові функції для задоволення різноманітних потреб підприємств та постачальників послуг.

SIP клієнтами є пристрої або програмні додатки, які використовуються для здійснення дзвінків через SIP телефонну мережу. До них належать:

- SIP телефони: спеціалізовані апаратні пристрої, призначені для голосового зв'язку через SIP телефонну мережу. Вони можуть бути настільними, бездротовими або конференц-телефонами.

- Софтфони: програмні клієнти, які встановлюються на персональних комп'ютерах, ноутбуках або мобільних пристроях і дозволяють здійснювати SIP дзвінки за допомогою гарнітури або вбудованого мікрофона та динаміка.

SIP клієнти (телефони, софтфони) є ключовими компонентами в SIP телефонних мережах, що забезпечують користувачам можливість здійснювати голосові дзвінки за допомогою протоколу ініціювання сесії (SIP). Розглянемо їх детальніше:

SIP телефони:

- Це спеціалізовані апаратні пристрої, розроблені спеціально для використання в SIP телефонних мережах.

- Вони мають вбудовану підтримку SIP протоколу та необхідних кодеків для передачі голосового трафіку.

- SIP телефони можуть бути настільними, бездротовими (з підтримкою Wi-Fi або DECT) або конференц-телефонами для групових розмов.

- Вони зазвичай мають LCD-дисплей, клавіатуру та гарнітуру або вбудований гучномовець і мікрофон.

- SIP телефони підключаються до SIP проксі-сервера або безпосередньо до SIP-серверів постачальника послуг для встановлення, маршрутизації та завершення дзвінків.

Софтфони:

- Це програмні додатки, які можна встановити на персональні комп'ютери, ноутбуки, планшети або мобільні пристрої.

- Вони імітують функціональність SIP телефону, використовуючи програмне забезпечення замість спеціалізованого апаратного забезпечення.

- Софтфони підтримують SIP протокол та необхідні кодеки для передачі голосового трафіку.

- Для забезпечення аудіо функціональності софтфони використовують мікрофон, гучномовці або гарнітуру, підключену до пристрою, на якому вони встановлені.

- Софтфони можуть бути настільними або мобільними додатками, що забезпечує зручність використання в різних середовищах.

Як SIP телефони, так і софтфони взаємодіють із SIP проксі-серверами або безпосередньо з SIP-серверами постачальника послуг для встановлення,

маршрутизації та завершення дзвінків у SIP телефонній мережі. Вони можуть підтримувати різні функції, такі як очікування виклику, переадресація, конференц-зв'язок та інші додаткові можливості залежно від реалізації та постачальника послуг.

Клієнти повинні підтримувати SIP протокол та відповідні кодеки для передачі голосового трафіку. Вони взаємодіють із SIP проксі-серверами для встановлення, маршрутизації та завершення дзвінків у SIP телефонній мережі.

Якість обслуговування (Quality of Service, QoS) є критично важливою для забезпечення належної якості голосового зв'язку в SIP телефонній мережі. Оскільки голосовий трафік є чутливим до затримок та втрат пакетів, необхідно вжити заходів для гарантування належної швидкості та стабільності передачі даних.

Система керування якістю обслуговування (QoS) відповідає за управління мережевими ресурсами та пріоритезацію трафіку для забезпечення належної якості голосового зв'язку. Вона може включати такі механізми:

- Пріоритезація трафіку: виділення більшої пропускної здатності та пріоритету для голосового трафіку порівняно з іншими типами даних.

- Управління чергою: забезпечення належного обслуговування пріоритетного трафіку в черзі під час перевантажень мережі.

- Резервування пропускної здатності: виділення певної частини пропускної здатності для голосового трафіку, щоб уникнути затримок та втрат пакетів.

- Механізми контролю затримки та втрат пакетів: використання технологій, таких як буферизація, компенсація втрат пакетів та механізмів корекції помилок для підвищення якості зв'язку.

Система QoS може бути реалізована на різних рівнях мережі, включаючи апаратне забезпечення (комутатори, маршрутизатори) та програмне забезпечення (SIP шлюзи, медіа-сервери).

Ефективна система керування якістю обслуговування є ключовим фактором для забезпечення високої якості голосового зв'язку в SIP телефонній

мережі та задоволення вимог користувачів до безперебійної та чіткої комунікації.

Усі ці компоненти SIP мережі тісно взаємодіють між собою для забезпечення ефективної роботи системи. Їх правильний вибір, налаштування та інтеграція є критично важливими для створення надійної, масштабованої та продуктивної SIP телефонної мережі, яка відповідатиме потребам організації.

2.2.3 Протоколи та стандарти

SIP (Session Initiation Protocol)

Протокол ініціювання сесії (SIP) є основним протоколом сигналізації в IP-телефонії та мультимедійних комунікаціях, визначений в RFC 3261. Він використовується для встановлення, модифікації та завершення мультимедійних сесій, таких як голосові та відеовиклики, а також для передачі даних в Інтернет-телефонії[7].

Основні функції SIP:

1. Встановлення сесій: SIP відповідає за ініціювання та налаштування мультимедійних сесій між учасниками.

2. Маршрутизація викликів: SIP забезпечує механізм маршрутизації викликів через SIP проксі-сервери та перенаправлення між різними мережами.

3. Управління сесіями: SIP дозволяє змінювати параметри сесії під час її перебігу, наприклад, додавати учасників, змінювати кодеки або переключатися на інші медіапотоки.

4. Завершення сесій: SIP також відповідає за коректне завершення сесій після завершення комунікації.

Архітектура SIP включає такі основні компоненти:

1. User Agent (Клієнт): Програмне забезпечення або пристрій, який ініціює або приймає SIP сесії. Наприклад, SIP-телефон або софтфон[8].

2. SIP Proxy Server: Проміжний сервер, який забезпечує маршрутизацію та пересилання SIP повідомлень між клієнтами.

3. Registrar Server: Сервер, який зберігає інформацію про поточне місцезнаходження користувачів для маршрутизації викликів.

4. Redirect Server: Сервер, який надає відповіді з альтернативними адресами, на які клієнт може спробувати з'єднатися.

SIP використовує текстові повідомлення, подібні до HTTP, для ініціювання та керування сесіями. Основні типи SIP-повідомлень:

- INVITE: Ініціює сесію або виклик.
- ACK: Підтверджує успішне встановлення сесії.
- BYE: Завершує сесію.
- CANCEL: Скасовує незавершену спробу встановлення сесії.
- REGISTER: Реєструє поточне місцезнаходження користувача.

SIP широко використовується в IP-телефонії, відеоконференцзв'язку, миттєвому обміні повідомленнями та інших додатках мультимедійних комунікацій. Його перевагами є гнучкість, масштабованість та сумісність з різними мережами і протоколами.

Рис.2.3. SIP-RTP

Протокол передачі даних в режимі реального часу (RTP) є стандартизованим протоколом, визначеним в RFC 3550, який використовується для передачі мультимедійних даних, таких як аудіо та відео, через IP-мережі в режимі реального часу.

Основні функції RTP:

1. Упаковка мультимедійних даних: RTP інкапсулює мультимедійні дані (наприклад, аудіо- або відеопотоки) в пакети для передачі через IP-мережі.

2. Нумерація пакетів: Кожному пакету присвоюється унікальний номер для виявлення втрачених пакетів та відновлення правильного порядку даних.

3. Мітки часу: RTP додає мітки часу до кожного пакета, що дозволяє отримувачу синхронізувати відтворення мультимедійних даних.

4. Ідентифікація джерела: Кожне джерело мультимедійних даних має унікальний ідентифікатор синхронізації джерела (SSRC), що дозволяє розрізняти декілька потоків в одній сесії.

RTP часто використовується разом з протоколом опису сесії (SDP) для обміну інформацією про мультимедійні потоки між учасниками сесії.

RTP не забезпечує механізму управління передачею даних або гарантії доставки пакетів. Замість цього він покладається на нижчі рівні протоколів, такі як UDP або TCP/IP, для транспортування пакетів. RTP забезпечує контроль над якістю обслуговування (QoS) та моніторингом мультимедійних потоків, але не гарантує надійної доставки.

Додаткові функції RTP включають:

1. Ідентифікацію платформ: RTP може передавати інформацію про тип завантаженого вмісту, що дозволяє отримувачу декодувати та відтворювати дані належним чином.

2. Плавне відтворення: RTP забезпечує механізми для забезпечення плавного відтворення мультимедійних даних, компенсуючи варіації затримки та втрати пакетів.

3. Розширюваність: RTP є розширюваним протоколом, що дозволяє додавати нові функції та профілі для різних типів мультимедійних даних.

RTP широко використовується в додатках IP-телефонії, відеоконференцзв'язку, потокового мультимедіа та інших сервісах, що передають мультимедійні дані через IP-мережі в режимі реального часу.

SDP (Session Description Protocol)

Протокол опису сесії (SDP) є стандартом, визначеним в RFC 4566, який використовується для опису мультимедійних сесій та їх параметрів. SDP

забезпечує структурований формат для кодування інформації про потоки мультимедійних даних, такі як аудіо, відео або тексту.

Основні функції SDP:

1. Опис мультимедійних потоків: SDP дозволяє визначати характеристики мультимедійних потоків, такі як тип мультимедіа (аудіо, відео), кодеки, роздільна здатність, частота кадрів тощо.

2. Адресація та транспорт: SDP містить інформацію про IP-адреси та порти, необхідні для встановлення з'єднання та передачі мультимедійних потоків.

3. Управління сесіями: SDP включає дані про час початку та тривалість сесії, а також інформацію про учасників.

4. Додаткові атрибути: SDP дозволяє додавати додаткові атрибути та розширення для задоволення специфічних вимог додатків.

SDP часто використовується разом з протоколами сигналізації, такими як SIP або H.323, для обміну інформацією про мультимедійні потоки між учасниками.

SDP зазвичай включає кілька основних розділів:

1. Інформація про сесію: Містить загальну інформацію про сесію, таку як назва, призначена для користувача інформація, ідентифікатор сесії та інформація про час існування сесії.

2. Інформація про мультимедійні потоки: Визначає характеристики кожного окремого мультимедійного потоку, включаючи тип мультимедіа (аудіо, відео, текст тощо), транспортний протокол (RTP/UDP, RTP/SAVPF тощо), порт, кодек та параметри кодування.

3. Інформація про з'єднання: Вказує IP-адреси та порти, необхідні для встановлення з'єднання та передачі мультимедійних даних.

4. Атрибути: Містить додаткові атрибути або розширення, специфічні для додатків або протоколів, що використовуються.

SDP може бути кодований у текстовому форматі та переданий за допомогою різних протоколів, таких як SIP, RTSP або електронної пошти. Під

час встановлення мультимедійної сесії учасники обмінюються повідомленнями SDP, що містять опис мультимедійних потоків та параметри для успішного з'єднання та передачі даних.

Використання SDP забезпечує стандартизований спосіб опису мультимедійних сесій та сумісність між різними додатками та платформами. Це дозволяє учасникам узгоджувати параметри сесії та підтримувані функції, що є критично важливим для успішної взаємодії в мультимедійних комунікаціях.

Кодеки (скорочення від "кодер-декодер") є програмними або апаратними компонентами, які виконують стиснення та розпакування цифрових аудіо- та відеоданих для ефективної передачі та зберігання. У контексті IP-телефонії та мультимедійних комунікацій кодеки відіграють ключову роль у забезпеченні якісної передачі голосу та відео через IP-мережі.

Існують різні типи кодеків для аудіо та відео, кожен з яких має свої власні алгоритми стиснення, рівень якості та швидкість передачі даних. Деякі поширені кодеки, що використовуються в IP-телефонії, включають:

Аудіокодеки:

1. G.711 (a-law та μ-law): Широко використовуваний кодек для стиснення аудіо з високою якістю, але з відносно низьким ступенем стиснення.

2. G.722: Кодек з більш високим ступенем стиснення та покращеною якістю звуку, ніж G.711, але вимагає більшої пропускної здатності.

3. G.729: Кодек з високим ступенем стиснення, що забезпечує якісний звук при низькій швидкості передачі даних, але з певною втратою якості порівняно з G.711.

4. Opus: Сучасний відкритий кодек з адаптивним битрейтом, який забезпечує високу якість звуку як для мовлення, так і для музики.

5. AMR (Adaptive Multi-Rate): Широко використовується в стільникових мережах та оптимізований для мовлення в умовах шуму та перешкод.

Відеокодеки:

1. H.264 (AVC): Широко використовуваний відеокодек із високим ступенем стиснення та хорошою якістю зображення для різних роздільних здатностей та швидкостей передачі даних.

2. VP8: Високоякісний відкритий відеокодек з гарним балансом між якістю та ступенем стиснення, розроблений Google.

3. H.265 (HEVC): Наступник H.264 з більш високим ступенем стиснення та кращою якістю зображення, але вимагає більших обчислювальних ресурсів для кодування та декодування.

4. VP9: Наступник VP8, який забезпечує кращу якість відео та вищий ступінь стиснення порівняно зі своїм попередником.

Вибір відповідного кодека залежить від вимог до якості, доступної пропускної здатності мережі, обчислювальних ресурсів та підтримки кодеків на кінцевих пристроях. Під час встановлення мультимедійної сесії учасники узгоджують використання підтримуваних кодеків за допомогою протоколів, таких як SDP (Session Description Protocol).

Використання ефективних кодеків є критично важливим для забезпечення високої якості голосових та відеосесій в IP-телефонії та мультимедійних комунікаціях, оптимізуючи використання пропускної здатності мережі та обчислювальних ресурсів.

2.3 Етапи встановлення SIP дзвінка

2.3.1 Процес реєстрації користувача SIP

Ініціювання процесу реєстрації:

Коли користувач вмикає свій SIP клієнт (телефон, софтфон або додаток), клієнт відправляє запит REGISTER на сервер реєстрації (Registrar Server). Цей запит містить наступну інформацію:

- SIP URI користувача (sip:користувач@домен.com)

- IP-адреса та порт клієнта

- Контактна інформація (IP-адреса, порт та транспортний протокол для отримання вхідних викликів)

- Дані автентифікації (ім'я користувача та пароль)

- Заголовки, що описують можливості клієнта (підтримувані кодеки, функції тощо)

Обробка запиту сервером реєстрації:

Після отримання запиту REGISTER, сервер реєстрації виконує наступні дії:

а) Перевірка автентифікації: Сервер перевіряє облікові дані користувача (ім'я користувача та пароль) у базі даних користувачів або в зовнішній системі автентифікації (наприклад, RADIUS або LDAP).

б) Оновлення інформації про місцезнаходження: Якщо автентифікація пройшла успішно, сервер зберігає контактну інформацію користувача (IP-адресу, порт тощо) у базі даних місцезнаходжень. Ця інформація використовується для маршрутизації вхідних викликів до користувача.

в) Відповідь на запит: Сервер реєстрації відправляє відповідь 200 OK на клієнт SIP, підтверджуючи успішну реєстрацію.

Періодичне оновлення реєстрації:

Реєстрація користувача в SIP є тимчасовою і має певний час дії (зазвичай кілька годин). Щоб підтримувати актуальність інформації про місцезнаходження, клієнт SIP повинен періодично оновлювати свою реєстрацію шляхом повторного надсилання запиту REGISTER. Цей процес називається "оновленням реєстрації".

Видалення реєстрації:

Коли користувач вимикає клієнт SIP або клієнт зазнає збою, він повинен відправити запит REGISTER з заголовком "Expires: 0" для вказівки на те, що реєстрація більше не є дійсною. Це дозволяє серверу видалити інформацію про місцезнаходження користувача з бази даних.

Успішна реєстрація користувача є критично важливою для забезпечення правильної маршрутизації вхідних викликів та встановлення мультимедійних сесій у SIP мережах. Вона забезпечує гнучкість та мобільність, дозволяючи користувачам отримувати виклики на різних пристроях та з різних місць.

2.3.2 Ініціалізація SIP дзвінка

Ініціатор відправляє повідомлення INVITE:

- Користувач, що ініціює виклик (User Agent Client, UAC), відправляє повідомлення INVITE на SIP проксі-сервер.

- Повідомлення INVITE містить SIP URI одержувача (sip:користувач@домен.com) та опис сесії SDP (Session Description Protocol), який описує параметри мультимедійної сесії, такі як кодеки, IP-адреси та порти для передачі медіаданих.

Маршрутизація виклику через проксі-сервер:

- SIP проксі-сервер обробляє отримане повідомлення INVITE та визначає, чи зареєстрований одержувач у системі.

- Якщо одержувач зареєстрований, проксі-сервер пересилає повідомлення INVITE на поточну контактну адресу одержувача (User Agent Server, UAS).

- У разі, якщо одержувач не зареєстрований або недоступний, проксі-сервер може відхилити виклик або спробувати знайти альтернативний шлях для доставки повідомлення INVITE.

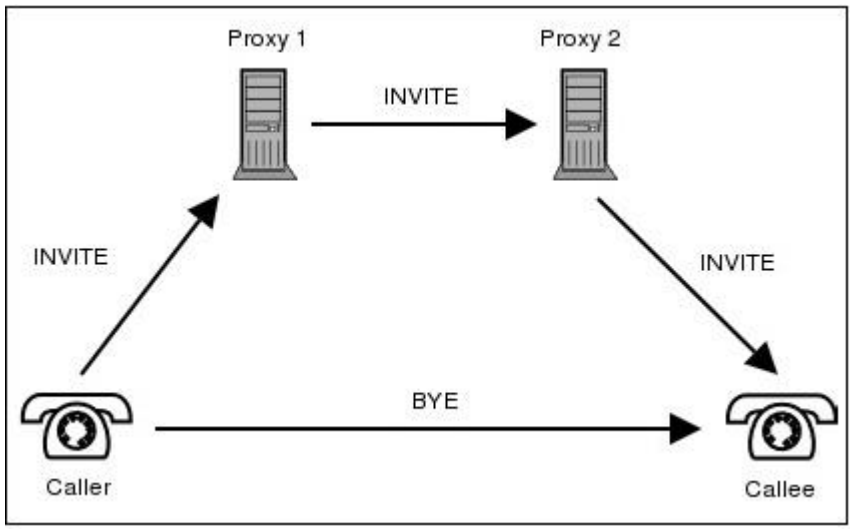

Рис.2.4. Основа SIP викликів

Сповіщення про вхідний виклик:

- Одержувач (UAS) отримує повідомлення INVITE та відповідає тимчасовим повідомленням 180 Ringing назад до ініціатора через проксі-сервер.

- Це повідомлення сигналізує ініціатору, що одержувач отримав виклик і сповіщає його про вхідний дзвінок (наприклад, відтворює рингтон).

Прийняття виклику і встановлення сесії:

- Якщо одержувач бажає прийняти виклик, він відповідає на повідомлення INVITE повідомленням 200 OK, яке також містить опис сесії SDP з підтримуваними параметрами мультимедійної сесії.

- Повідомлення 200 OK проходить через проксі-сервер назад до ініціатора.

Підтвердження встановлення сесії:

- Після отримання повідомлення 200 OK, ініціатор відповідає повідомленням ACK для підтвердження успішного встановлення мультимедійної сесії.

- На цьому етапі ініціатор та одержувач можуть розпочати обмін медіаданими (голосом, відео) через встановлений RTP канал.

Ця послідовність повідомлень забезпечує безпечний та надійний спосіб ініціалізації SIP дзвінка, дозволяючи сторонам узгодити параметри мультимедійної сесії та встановити з'єднання для передачі даних.

Слід зазначити, що SIP є гнучким протоколом, і ця базова послідовність може змінюватися залежно від конфігурації мережі, наявності додаткових серверів (наприклад, серверів переадресації) та специфічних вимог додатків або постачальників послуг.

2.3.3 Процес встановлення мультимедійної сесії в SIP дзвінка

Узгодження параметрів сесії за допомогою SDP:

- Під час обміну повідомленнями INVITE та 200 OK, ініціатор та одержувач включають опис сесії SDP (Session Description Protocol).

- Опис SDP містить інформацію про підтримувані кодеки (аудіо та відео), транспортні протоколи, IP-адреси та порти для передачі мультимедійних даних.

- Сторони аналізують отримані описи SDP та вибирають спільні параметри сесії, які підтримуються обома клієнтами.

Встановлення RTP каналу:

- Після узгодження параметрів сесії, клієнти SIP встановлюють прямий канал передачі RTP (Real-time Transport Protocol) між собою.

- RTP - це протокол, призначений для передачі мультимедійних даних (аудіо, відео) в режимі реального часу через IP-мережі.

- RTP канал встановлюється за допомогою узгоджених IP-адрес та портів, визначених в описі SDP.

3. Передача мультимедійних даних

- Після встановлення RTP каналу, клієнти можуть розпочати передачу мультимедійних даних один одному.

- Аудіо- або відеодані кодуються за допомогою узгоджених кодеків, визначених в описі SDP.

- Закодовані дані упаковуються в RTP пакети та передаються через встановлений RTP канал.

Контроль передачі даних:

- Разом з RTP часто використовується протокол RTCP (Real-time Transport Control Protocol) для контролю та моніторингу передачі даних.

- RTCP забезпечує механізми зворотного зв'язку, статистику, синхронізацію та інформацію про якість сервісу (QoS) для мультимедійних сесій.

Додаткові функції:

- Залежно від реалізації SIP та додатків, під час встановлення мультимедійної сесії можуть бути задіяні додаткові компоненти та функції, такі як:

- Транскодери: для перетворення кодеків між клієнтами з різними можливостями.

- Медіа-релеї: для ретрансляції мультимедійних потоків через посередників (наприклад, через NAT або брандмауери).

- Системи управління якістю сервісу (QoS): для забезпечення належної якості мультимедійної сесії.

Встановлення мультимедійної сесії є критичним етапом, який дозволяє учасникам SIP дзвінка успішно обмінюватися мультимедійними даними після завершення процесу сигналізації. Гнучкість SIP та SDP забезпечує сумісність між різними платформами та пристроями, уможливлюючи ефективну передачу голосу, відео та інших типів мультимедійних даних в IP-мережах.

2.3.4 Процес передачі мультимедійних даних під час SIP дзвінка

Кодування мультимедійних даних:

- На стороні відправника аудіо або відео дані захоплюються з мікрофона, веб-камери або іншого джерела.

- Ці дані кодуються за допомогою узгодженого кодека (наприклад, G.711 для аудіо або H.264 для відео), визначеного в описі SDP під час встановлення сесії.

- Закодовані дані розбиваються на менші фрагменти для упаковки в RTP пакети.

Упаковка даних в RTP пакети:

- Закодовані мультимедійні дані упаковуються у формат RTP (Real-time Transport Protocol).

- Кожен RTP пакет містить заголовок з інформацією про синхронізацію, нумерацію пакетів, тимчасові мітки та ідентифікацію джерела.

- Корисне навантаження RTP пакета містить закодовані аудіо- або відеодані.

Передача RTP пакетів:

- Згенеровані RTP пакети передаються через встановлений RTP канал до одержувача.

- RTP зазвичай використовує UDP як транспортний протокол для забезпечення швидкої доставки пакетів.

- Пакети можуть проходити через різні мережеві компоненти, такі як маршрутизатори, брандмауери та механізми забезпечення якості обслуговування (QoS).

Прийом та декодування RTP пакетів:

- На стороні одержувача RTP пакети приймаються та буферизуються.

- RTP пакети розпаковуються, і закодовані мультимедійні дані витягуються з корисного навантаження.

- Декодер, що відповідає використовуваному кодеку, застосовується для декодування мультимедійних даних.

- Декодовані аудіо- або відеодані відтворюються на динаміках або дисплеї одержувача в режимі реального часу.

Моніторинг та контроль за допомогою RTCP:

- Протокол RTCP (Real-time Transport Control Protocol) часто використовується разом з RTP для контролю та моніторингу якості сесії.

- RTCP забезпечує зворотний зв'язок про втрату пакетів, затримку, джитер та інші метрики якості для обох сторін.

- Ця інформація може використовуватися для адаптації кодеків, регулювання швидкості передачі даних або застосування механізмів відновлення помилок для підвищення якості мультимедійної сесії.

Передача мультимедійних даних в SIP є критично важливою для забезпечення якісної голосової та відеокомунікації. Використання ефективних кодеків, протоколів RTP/RTCP та механізмів контролю якості дозволяє досягти оптимальної продуктивності та користувацького досвіду в IP-телефонії та інших додатках мультимедійних комунікацій.

2.3.5 Завершення SIP дзвінка

Ініціювання процесу завершення дзвінка:

- Коли одна зі сторін (наприклад, ініціатор або одержувач) бажає завершити поточний SIP дзвінок, вона ініціює процес завершення, надсилаючи повідомлення BYE через SIP проксі-сервер на іншу сторону.

- Повідомлення BYE містить ідентифікатор викликаної сесії, щоб чітко вказати, яку саме сесію потрібно завершити.

Маршрутизація повідомлення BYE:

- SIP проксі-сервер отримує повідомлення BYE та маршрутизує його до іншої сторони, використовуючи інформацію про місцезнаходження, отриману під час встановлення дзвінка.

Підтвердження завершення сесії:

- Одержувач повідомлення BYE відповідає повідомленням 200 OK, яке проходить через проксі-сервер назад до ініціатора завершення.

- Це повідомлення 200 OK підтверджує, що інша сторона також готова завершити поточну сесію.

Завершення мультимедійної сесії RTP:

- Після успішного обміну повідомленнями BYE та 200 OK, обидві сторони можуть безпечно завершити мультимедійну сесію RTP.

- Вони припиняють передачу RTP пакетів та закривають RTP канал.

- Будь-які додаткові ресурси, задіяні в мультимедійній сесії (наприклад, транскодери або медіа-релеї), також можуть бути звільнені.

Видалення інформації про сесію з проксі-сервера:

- SIP проксі-сервер, який маршрутизував виклик, видаляє інформацію про завершену сесію зі своїх внутрішніх таблиць маршрутизації та стану.

Запис інформації про дзвінок:

- Залежно від конфігурації системи, інформація про завершений дзвінок (тривалість, учасники, використані ресурси тощо) може бути записана в системи білінгу, моніторингу або журнали подій для подальшого аналізу або облікутарифікаційних цілей.

Завершення SIP дзвінка є важливим етапом у циклі життя сесії, який забезпечує належне звільнення ресурсів, уникнення витоку ресурсів та

підтримку чистоти даних у системах маршрутизації та білінгу. Чітке дотримання протоколу завершення сесії гарантує безперебійну роботу SIP мережі та правильне відображення використаних послуг.

Ці етапи ілюструють детальний процес встановлення, передачі даних та завершення SIP дзвінка з використанням різних протоколів та компонентів SIP телефонії. Ця послідовність подій забезпечує надійну та ефективну взаємодію між SIP клієнтами для здійснення мультимедійних комунікацій.

2.4 QoS

Забезпечення якості обслуговування (QoS) є важливим аспектом в комп'ютерних мережах для гарантування належного рівня продуктивності та задоволення вимог різних типів трафіку. Воно охоплює такі основні механізми:

2.4.1 Пріоритезація трафіку

Перш за все, трафік класифікується на основі певних критеріїв для визначення його пріоритету. Це може здійснюватися за допомогою таких параметрів:

- Типи протоколів (наприклад, TCP, UDP, ICMP тощо)
- Номери портів (наприклад, порт 80 для HTTP, порт 21 для FTP)
- Значення поля DSCP (Диференційовані послуги коду точки, DiffServ Code Point) в заголовку IP-пакету
- Адреси джерела або призначення
- Ідентифікатори віртуальних локальних мереж (VLAN ID)
- Інші мітки або теги, специфічні для конкретної реалізації QoS

Після класифікації трафіку йому присвоюються відповідні пріоритети. Для цього можуть використовуватися різні механізми:

- Strict Priority Queueing (жорстка пріоритетна черга) - пакети з вищим пріоритетом обробляються першими, перш ніж пакети з нижчим пріоритетом
- Weighted Fair Queueing (зважена справедлива черга) - пропускна здатність розподіляється між чергами на основі призначених ваг

- Class-Based Queueing (черговість на основі класів) - створюються окремі черги для різних класів трафіку

Під час обробки та передачі пакетів через мережеві пристрої (комутатори, маршрутизатори тощо), пакети з вищим пріоритетом обробляються та передаються раніше, ніж пакети з нижчим пріоритетом. Це забезпечує меншу затримку та втрати пакетів для високопріоритетного трафіку.

Для ефективного управління чергами в пристроях можуть застосовуватися різні методи, такі як:

- Tail Drop - коли черга заповнена, нові пакети просто відкидаються

- Weighted Random Early Detection (WRED) - пакети відкидаються з певною ймовірністю залежно від середнього розміру черги та ваги класів трафіку

- Class-Based Weighted Fair Queueing (CB-WFQ) - поєднує класифікацію трафіку та зважену справедливу черговість

Резервування пропускної здатності:

Для забезпечення належного рівня обслуговування пріоритетного трафіку може бути виділена певна частина загальної пропускної здатності мережі. Це гарантує, що високопріоритетний трафік матиме достатню пропускну здатність, навіть якщо в мережі присутній великий обсяг низькопріоритетного трафіку.

Важливо зазначити, що пріоритезація трафіку є лише одним з механізмів забезпечення якості обслуговування (QoS) і часто використовується у поєднанні з іншими механізмами, такими як управління черговістю, резервування пропускної здатності та механізмами контролю затримки та втрат пакетів.

2.4.2 Управління черговістю

Управління черговістю (Queueing Management) є важливим механізмом забезпечення якості обслуговування (QoS) в комп'ютерних мережах. Він визначає порядок, в якому пакети обробляються та передаються через

мережеві пристрої, такі як маршрутизатори та комутатори. Давайте розглянемо деякі найпоширеніші алгоритми черговості більш детально:

1. First-In-First-Out (FIFO) - це найпростіший алгоритм черговості, в якому пакети обробляються в тому ж порядку, в якому вони надходять. Пакети, які прибувають першими, передаються першими, без будь-якої диференціації або пріоритизації. Цей алгоритм не забезпечує жодних гарантій QoS, але легко реалізується і забезпечує справедливість для всіх типів трафіку.

2. Priority Queueing (PQ) - при використанні Priority Queueing пакети класифікуються за різними рівнями пріоритету, і для кожного пріоритету створюється окрема черга. Пакети з вищим пріоритетом завжди обробляються та передаються раніше, ніж пакети з нижчим пріоритетом. Однак цей алгоритм може призвести до голодування низькопріоритетних черг, якщо високопріоритетний трафік є постійним.

3. Weighted Fair Queueing (WFQ) - намагається забезпечити справедливий розподіл пропускної здатності між різними потоками трафіку, присвоюючи кожному потоку певну вагу. Чим більша вага потоку, тим більша його частка пропускної здатності. WFQ гарантує, що жодному потоку не буде відмовлено в обслуговуванні, навіть якщо інші потоки мають більш високі пріоритети.

4. Class-Based Weighted Fair Queueing (CBWFQ) - є розширенням WFQ, в якому трафік класифікується за різними класами на основі певних критеріїв (наприклад, типу протоколу, адрес джерела/призначення тощо). Кожному класу присвоюється певна вага, і всередині класу застосовується WFQ для справедливого розподілу пропускної здатності між потоками.

5. Low Latency Queueing (LLQ) - поєднує переваги Priority Queueing та Class-Based Weighted Fair Queueing. У цьому алгоритмі створюється окрема черга для високопріоритетного трафіку (наприклад, голосових або відео потоків), яка обслуговується першою. Решта трафіку класифікується за класами і обробляється з використанням CBWFQ.

Крім вибору відповідного алгоритму черговості, важливо також управляти механізмами відкидання пакетів у чергах, такими як Tail Drop або Weighted Random Early Detection (WRED), для запобігання перевантаженню черг і забезпечення належної продуктивності.

Вибір алгоритму черговості залежить від конкретних вимог мережі, типів трафіку та необхідного балансу між пропускною здатністю, затримкою та справедливістю розподілу ресурсів.

2.4.3 Резервування пропускної здатності

Резервування пропускної здатності (Bandwidth Reservation) є важливим механізмом забезпечення якості обслуговування (QoS) в мережах, який гарантує, що певна частина загальної пропускної здатності буде виділена для критичних або пріоритетних типів трафіку. Давайте розглянемо цей механізм більш докладно:

1. Класифікація трафіку

Перш за все, трафік класифікується на основі певних критеріїв, таких як тип протоколу, номери портів, адреси джерела/призначення, DSCP (Диференційовані послуги коду точки) або інші мітки. Цей крок визначає, який трафік вважається критичним або пріоритетним.

2. Визначення вимог до пропускної здатності

Для кожного класу критичного трафіку визначаються вимоги до пропускної здатності. Це може бути мінімальна гарантована пропускна здатність, середня потрібна пропускна здатність або максимальна пікова пропускна здатність.

3. Резервування ресурсів

На основі визначених вимог до пропускної здатності, частина загальної пропускної здатності мережі резервується для кожного класу критичного трафіку. Це забезпечує, що навіть у разі перевантаження мережі некритичним трафіком, критичний трафік матиме гарантовану пропускну здатність.

4. Механізми розподілу пропускної здатності

Існують різні механізми для розподілу зарезервованої пропускної здатності між потоками трафіку в межах одного класу. Деякі з них:

- Weighted Fair Queueing (WFQ) - розподіляє пропускну здатність пропорційно вагам, присвоєним кожному потоку.

- Class-Based Weighted Fair Queueing (CBWFQ) - поєднує класифікацію трафіку та WFQ для справедливого розподілу пропускної здатності.

- Low Latency Queueing (LLQ) - створює окрему чергу для високопріоритетного трафіку з гарантованою пропускною здатністю.

5. Динамічне налаштування

Механізм резервування пропускної здатності може бути динамічним і адаптуватися до змін в навантаженні на мережу. Наприклад, якщо критичний трафік тимчасово зменшується, невикористана пропускна здатність може бути перерозподілена для інших класів.

6. Комбінація з іншими механізмами QoS

Резервування пропускної здатності часто використовується у поєднанні з іншими механізмами QoS, такими як пріоритезація трафіку та управління черговістю, для досягнення найкращих результатів.

Резервування пропускної здатності є особливо важливим для чутливих до затримки додатків, таких як VoIP, відеоконференції або критичні бізнес-додатки. Воно гарантує, що ці додатки матимуть необхідні мережеві ресурси, незалежно від інших навантажень на мережу.

2.4.4 Механізми контролю затримки та втрат пакетів

Механізми контролю затримки та втрат пакетів (Delay and Packet Loss Control Mechanisms) є ключовою частиною забезпечення якості обслуговування (QoS) в мережах, особливо для чутливих до затримки додатків, таких як голосовий трафік або відеопотоки. Давайте розглянемо ці механізми більш детально:

1. Буферизація (Buffering)

Буферизація використовується для зменшення затримки та джиттеру (варіації затримки) в мережі. Пакети тимчасово зберігаються в буферах на

мережевих пристроях, таких як маршрутизатори або комутатори, перш ніж бути відправленими. Це дозволяє згладжувати коливання в затримці та забезпечити більш плавну передачу даних.

2. Компенсація джиттера (Jitter Buffer)

Компенсація джиттера є специфічним методом буферизації, який використовується для додатків реального часу, таких як VoIP або відеоконференції. Приймаючий бік має спеціальний буфер, який зберігає певну кількість пакетів, щоб згладити варіації затримки перед тим, як відтворювати їх для користувача.

3. Механізми відновлення втрачених пакетів (Packet Loss Recovery Mechanisms)

У разі втрати пакетів під час передачі через мережу, існують різні механізми для відновлення цих пакетів, щоб забезпечити безперервність потоку даних:

- Повторна передача (Retransmission) - втрачені пакети повторно передаються відправником після отримання запиту від одержувача.

- Кодування з виправленням помилок (Forward Error Correction, FEC) - додаткова надлишкова інформація вбудовується в потік даних, що дозволяє одержувачу відновити втрачені пакети без необхідності повторної передачі.

- Інтерполяція (Interpolation) - для відео- та аудіопотоків, втрачені пакети можуть бути замінені наближеними значеннями на основі сусідніх успішно отриманих пакетів.

4. Керування чергами та управління затриманням (Queueing and Delay Management)

Правильне управління чергами та затримкою на мережевих пристроях є важливим для мінімізації затримки та джиттеру. Такі механізми, як Priority Queueing (PQ), Low Latency Queueing (LLQ) та Weighted Fair Queueing (WFQ), дозволяють пріоритезувати чутливий до затримки трафік та забезпечувати йому належну обробку.

5. Механізми керування перевантаженням (Congestion Control Mechanisms)

Перевантаження в мережі може призвести до значних затримок та втрат пакетів. Механізми керування перевантаженням, такі як Random Early Detection (RED) та Weighted Random Early Detection (WRED), використовуються для виявлення та запобігання перевантаженню шляхом контрольованого відкидання пакетів до виникнення критичних ситуацій.

6. Резервування ресурсів (Resource Reservation)

Механізми резервування ресурсів, такі як RSVP (Resource Reservation Protocol) або Інтегроване обслуговування (IntServ), дозволяють додаткам резервувати необхідні мережеві ресурси, такі як пропускна здатність та буфери, для забезпечення гарантованої якості обслуговування та мінімізації затримок та втрат пакетів.

Комбінація цих механізмів допомагає забезпечити належну якість обслуговування для чутливих до затримки додатків, гарантуючи низьку затримку, мінімальний джиттер та низький рівень втрат пакетів, навіть у перевантажених мережевих умовах.

Комбінація цих механізмів QoS дозволяє мережам ефективно розподіляти ресурси та надавати належний рівень обслуговування для різних типів трафіку відповідно до їх вимог та пріоритетів. Це забезпечує кращий користувацький досвід та продуктивність для критичних додатків та послуг, що працюють у мережі.

2.5 Інтеграція з іншими системами

2.5.1 Взаємодія з традиційними телефонними мережами

Для забезпечення інтеграції використовуються спеціальні пристрої - VoIP-шлюзи. Вони можуть бути апаратними (фізичними пристроями) або віртуальними (програмними). Шлюзи виконують декілька важливих функцій:

1. Трансляція сигналізації - перетворення сигнальних протоколів, що використовуються в традиційних мережах (наприклад, SS7, ISDN PRI) у

протоколи VoIP-сигналізації (SIP, H.323 тощо) і навпаки. Це забезпечує взаєморозуміння між системами.

2. Транскодування медіапотоків - конвертація голосових кодеків, що використовуються в IP-мережах (G.711, G.729 тощо) у формати традиційних мереж (G.711) і навпаки. Це необхідно для забезпечення сумісності різних технологій кодування/декодування голосу.

3. Трансляція послуг - перетворення додаткових послуг, таких як переадресація виклику, очікування виклику, конференц-зв'язок, між VoIP та традиційними мережами.

4. Маршрутизація викликів - шлюзи можуть маршрутизувати виклики між VoIP-мережею та PSTN/ISDN, вибираючи найбільш оптимальний маршрут на основі заданих правил.

5. Безпека та якість обслуговування - шлюзи забезпечують захист від атак, фільтрацію трафіку, пріоритезацію голосового трафіку та контроль якості передачі голосу.

Існують різні типи VoIP-шлюзів, які відрізняються за призначенням та можливостями:

- Шлюзи "користувач-мережа" (user-network gateway) - забезпечують підключення окремих користувачів або невеликих офісів до VoIP-мережі через PSTN або ISDN.

- Шлюзи "мережа-мережа" (trunk gateway) - призначені для з'єднання VoIP-мережі з мережами операторів зв'язку на рівні опорних мереж (транків).

- Резидентні шлюзи (residential gateways) - компактні пристрої для підключення звичайних аналогових телефонів до VoIP-мережі в домашніх або малих офісних умовах.

Таким чином, VoIP-шлюзи забезпечують seamless інтеграцію між VoIP та традиційними телефонними мережами, дозволяючи безперешкодне здійснення дзвінків, а також взаємодію додаткових послуг та функцій.

2.5.2 Інтеграція з уніфікованими комунікаціями (UC)

Інтеграція VoIP з уніфікованими комунікаціями (UC) є потужним інструментом для підвищення продуктивності та ефективності робочих процесів[9]. Розглянемо детальніше, як ця інтеграція працює та які переваги вона надає:

1. Єдина платформа комунікацій

Ключовою перевагою інтегрованої UC-системи є консолідація всіх комунікаційних каналів в єдиному інтерфейсі. Користувачі можуть здійснювати голосові дзвінки, відеоконференції, обмінюватися миттєвими повідомленнями, спільно працювати над документами та використовувати інші інструменти з єдиного робочого простору.

2. Безшовний перехід між каналами

Інтеграція VoIP з UC дозволяє безперервно переходити з одного каналу на інший в рамках однієї сесії спілкування. Наприклад, можна починати з голосового дзвінка, а потім легко перейти до відеоконференції або спільного перегляду екрана без необхідності починати нову сесію[9].

3. Присутність та доступність

UC-системи зазвичай включають функції присутності та індикатори доступності користувачів. Це дозволяє бачити, хто доступний для спілкування в певний момент, а також обирати найбільш зручний канал зв'язку з цією людиною.

4. Інтеграція з бізнес-додатками

UC-платформи можуть інтегруватися з бізнес-додатками, такими як CRM, ERP, системами документообігу та іншими корпоративними системами. Це дозволяє отримувати контекстну інформацію про клієнтів, проекти чи задачі безпосередньо в інтерфейсі комунікацій.

5. Мобільність та BYOD

Завдяки підтримці мобільних пристроїв та концепції "Bring Your Own Device" (BYOD), користувачі UC-систем можуть спілкуватися та

співпрацювати з будь-якого місця та пристрою, забезпечуючи гнучкість та мобільність.

6. Аналітика та звітність

Інтегровані UC-системи забезпечують збір та аналіз даних про використання комунікаційних каналів, продуктивність та ефективність співробітників, що дозволяє виявляти вузькі місця та вдосконалювати процеси.

Загалом, інтеграція VoIP з UC забезпечує безперервність комунікацій, підвищує продуктивність співробітників, покращує співпрацю та надає зручний та гнучкий спосіб спілкування та обміну інформацією в сучасному бізнес-середовищі.

2.6 Безпека та надійність

2.6.1 Захист від несанкціонованого доступу

1. Автентифікація користувачів:

Для захисту VoIP-системи від несанкціонованого доступу важливо впровадити надійні методи автентифікації користувачів. Найпоширенішим методом є використання паролів, які повинні відповідати вимогам складності та регулярно змінюватися. Крім того, можна застосовувати багатофакторну автентифікацію, наприклад, за допомогою апаратних або програмних токенів, біометричних даних (відбитки пальців, розпізнавання обличчя тощо) чи одноразових паролів[10].

Для підвищення безпеки VoIP-системи корисно застосовувати цифрові сертифікати, які забезпечують криптографічну автентифікацію користувачів, пристроїв та сервісів. Ці сертифікати видаються та підтверджуються центром сертифікації (CA) і містять відкритий ключ користувача та інформацію про його ідентифікацію.

2. Контроль доступу на основі ролей та політик безпеки:

Після автентифікації користувачів необхідно впровадити механізми контролю доступу для обмеження їхніх дій та привілеїв у VoIP-системі. Контроль доступу на основі ролей (RBAC) дозволяє визначити різні ролі

користувачів (наприклад, адміністратори, оператори, службовці) та встановити відповідні дозволи на виконання певних операцій. Наприклад, адміністратори матимуть повні права на управління системою, тоді як службовці зможуть лише здійснювати дзвінки.

Політики безпеки визначають правила та обмеження для доступу до ресурсів VoIP-системи, включаючи вимоги до автентифікації, дозволені протоколи та порти, фільтрацію трафіку тощо. Ці політики повинні регулярно переглядатися та оновлюватися відповідно до змін у вимогах безпеки та нових загроз.

3. Брандмауери та системи виявлення вторгнень:

Для захисту VoIP-інфраструктури від зовнішніх загроз необхідно розгорнути брандмауери та системи виявлення вторгнень (IDS/IPS). Брандмауери контролюють вхідний та вихідний мережевий трафік, дозволяючи або блокуючи його на основі заданих правил. Вони можуть застосовувати фільтрацію за IP-адресами, портами, протоколами, а також виконувати більш складні перевірки, такі як аналіз стану з'єднань, перевірка наявності підозрілого вмісту тощо[10].

Системи виявлення вторгнень (IDS) аналізують мережевий трафік та події на предмет підозрілої або шкідливої активності та генерують відповідні сповіщення. Системи запобігання вторгненням (IPS) не лише виявляють загрози, а й активно блокують небажаний трафік або припиняють шкідливі дії.

4. Віртуальні приватні мережі (VPN):

Для забезпечення безпечного доступу до VoIP-системи через загальнодоступні мережі, такі як Інтернет, використовуються віртуальні приватні мережі (VPN). VPN створюють зашифрований тунель зв'язку між клієнтським пристроєм та VoIP-мережею, захищаючи дані від перехоплення та підслуховування. Найпоширенішими протоколами VPN є IPsec та SSL/TLS.

IPsec VPN працює на мережевому рівні та забезпечує шифрування та автентифікацію всього трафіку між клієнтом та VoIP-системою. SSL/TLS VPN

працює на більш високому рівні та зазвичай легше налаштовується та керується, але може бути менш ефективним у деяких середовищах.

Незалежно від використовуваного протоколу, VPN гарантує конфіденційність та цілісність даних під час передачі через незахищені мережі, захищаючи VoIP-систему від несанкціонованого доступу.

2.6.2 Шифрування даних

Для забезпечення конфіденційності та цілісності даних, що передаються під час VoIP-дзвінків, використовуються різні методи шифрування.

1. SRTP (Secure Real-time Transport Protocol):

SRTP (Secure Real-time Transport Protocol) - це стандарт шифрування, що забезпечує захист голосового та відеотрафіку в режимі реального часу. SRTP використовує алгоритми шифрування, такі як AES (Advanced Encryption Standard), для шифрування мультимедійних пакетів даних. Він також застосовує алгоритми цифрових підписів, наприклад, HMAC-SHA1, для перевірки автентичності та цілісності даних.

SRTP забезпечує захист від прослуховування, підробки та відтворення даних, що є критично важливим для забезпечення конфіденційності та безпеки VoIP-комунікацій. Він широко використовується у VoIP-системах і підтримується більшістю VoIP-клієнтів та шлюзів.

2. TLS (Transport Layer Security):

TLS (Transport Layer Security) - це криптографічний протокол безпеки, який забезпечує захист даних під час передачі через мережу. У VoIP-системах TLS застосовується для шифрування сигнального трафіку, наприклад, під час встановлення VoIP-сесій та обміну сигнальними повідомленнями.

TLS використовує асиметричне шифрування для обміну ключами та встановлення захищеного сеансу зв'язку. Після цього симетричне шифрування, таке як AES, застосовується для шифрування даних під час сеансу. TLS також забезпечує автентифікацію сторін та цілісність даних за допомогою цифрових сертифікатів та криптографічних підписів.

TLS є важливим компонентом безпеки у VoIP-системах, оскільки захищає конфіденційність сигнальної інформації та попереджає різні типи атак, такі як прослуховування, підробка та відтворення сигнальних повідомлень.

3. Шифрування на рівні медіашлюзів та проксі-серверів:

Окрім захисту кінцевих точок (клієнтів), також важливо забезпечити шифрування даних на рівні медіашлюзів, проксі-серверів та інших ключових компонентів VoIP-інфраструктури. Це запобігає перехопленню чутливих даних на проміжних вузлах та захищає комунікації всередині VoIP-мережі.

Медіашлюзи та проксі-сервери можуть підтримувати шифрування на різних рівнях, включаючи шифрування на рівні транспортного або додаткового рівня. Наприклад, вони можуть використовувати SRTP або TLS для захисту медіапотоків та сигнального трафіку відповідно.

Крім того, деякі VoIP-системи можуть використовувати спеціалізовані механізми шифрування, такі як пропрієтарні або стандартизовані протоколи шифрування. Це забезпечує додатковий рівень захисту, але може знизити сумісність з іншими системами.

4. Вимоги до довжини ключа шифрування:

Довжина ключа шифрування є важливим фактором, що визначає стійкість шифрування до зламу. Чим довший ключ, тим складніше його зламати за допомогою методів грубої сили або криптоаналізу. Проте, надто довгі ключі можуть спричинити додаткове навантаження на систему та уповільнити шифрування/розшифрування.

Загалом, вважається, що для забезпечення належного рівня безпеки в сучасних VoIP-системах мінімальна довжина ключа симетричного шифрування (наприклад, AES) повинна становити 128 біт. Для асиметричного шифрування (наприклад, RSA) рекомендована мінімальна довжина ключа - 2048 біт.

Однак, ці вимоги можуть змінюватися з часом, оскільки обчислювальна потужність зростає, а методи криптоаналізу вдосконалюються. Тому важливо

регулярно переглядати та оновлювати вимоги до довжини ключа відповідно до сучасних стандартів безпеки та рекомендацій.

Крім того, слід використовувати надійні алгоритми та протоколи шифрування, такі як AES та TLS, які вважаються стійкими до атак та добре протестовані криптографічною спільнотою.

2.6.3 Резервування та відмовостійкість

Для забезпечення високої надійності та безперервності роботи VoIP-системи необхідно впровадити механізми резервування та відмовостійкості, щоб мінімізувати ризик відмов та збоїв.

1. Резервні сервери та шлюзи:

Одним з ключових елементів резервування є використання додаткових серверів та шлюзів, які можуть автоматично перебрати на себе функції основних компонентів у разі їх відмови. Це забезпечує безперервність роботи VoIP-системи та дозволяє уникнути простоїв у наданні послуг.

Резервні сервери можуть бути активними (працюють паралельно з основними) або пасивними (знаходяться в стані очікування). Активні резервні сервери забезпечують максимальну відмовостійкість, але потребують більше ресурсів. Пасивні резервні сервери активуються лише у разі відмови основного компонента.

Резервні шлюзи забезпечують альтернативні маршрути для з'єднання з іншими мережами, такими як PSTN або Інтернет, у випадку відмови основних шлюзів.

2. Кластеризація критичних компонентів:

Для підвищення надійності критичних компонентів VoIP-системи, таких як сервери реєстрації, проксі-сервери та медіашлюзи, можна застосовувати кластеризацію. Кластеризація об'єднує декілька фізичних або віртуальних серверів у єдину логічну систему, яка працює як єдине ціле.

У разі відмови одного з вузлів кластера інші вузли автоматично перебирають на себе його навантаження, забезпечуючи безперервність роботи

системи. Кластеризація також дозволяє рівномірно розподіляти навантаження між вузлами, підвищуючи продуктивність та ефективність системи.

3. Резервні канали зв'язку:

Важливо передбачити альтернативні канали зв'язку для використання у випадку відмови основного каналу передачі даних. Наприклад, якщо основним каналом є мережа Інтернет, можна використовувати резервний канал, такий як ISDN або стільникові мережі.

Резервні канали можуть бути постійно активними або активуватися автоматично у разі виявлення відмови основного каналу. Це забезпечує безперервність зв'язку та мінімізує простої в роботі VoIP-системи.

4. Системи безперебійного живлення (UPS):

Для захисту від збоїв, спричинених перебоями в електропостачанні, необхідно використовувати системи безперебійного живлення (UPS). UPS забезпечують резервне живлення критичних компонентів VoIP-системи, таких як сервери, шлюзи та мережеве обладнання, під час відключення електроенергії.

UPS можуть бути центральними (для захисту всієї інфраструктури) або розподіленими (для захисту окремих компонентів). Важливо правильно розрахувати потужність і час автономної роботи UPS, а також забезпечити їх регулярне технічне обслуговування та тестування.

5. Планування та тестування відновлення після збоїв:

Для забезпечення ефективного відновлення VoIP-системи після збоїв або відмов необхідно розробити детальний план відновлення та регулярно його тестувати. План відновлення повинен містити чіткі інструкції та процедури для різних сценаріїв відмов, визначати відповідальних осіб та вимоги до ресурсів.

Регулярне тестування плану відновлення дозволяє виявити та усунути будь-які недоліки або проблеми до того, як вони можуть вплинути на реальну ситуацію. Під час тестування можна відпрацювати навички та координацію

дій персоналу, а також переконатися в працездатності резервних компонентів та механізмів.

Загалом, впровадження ефективних заходів резервування та відмовостійкості є критично важливим для забезпечення безперервності роботи VoIP-системи та мінімізації ризиків відмов. Це дозволяє підтримувати високий рівень обслуговування клієнтів та уникнути потенційних втрат бізнесу.

2.6.4 Моніторинг та аналітика

Для забезпечення належної якості обслуговування (QoS), виявлення потенційних проблем та оптимізації продуктивності необхідно впровадити ефективні механізми моніторингу та аналітики VoIP-системи.

1. Моніторинг трафіку та аналіз пакетних втрат, затримок і джитеру

Моніторинг мережевого трафіку є критично важливим для виявлення та усунення проблем з продуктивністю VoIP-системи. Необхідно відстежувати та аналізувати такі ключові параметри:

- Пакетні втрати - відсоток втрачених пакетів даних під час передачі, що може призвести до перешкод або переривань звуку.

- Затримки (лаг) - час, необхідний для передачі пакетів від відправника до одержувача, що може спричинити відставання звуку.

- Джитер - коливання затримок пакетів, що може вплинути на якість звуку.

Цю інформацію можна збирати та аналізувати за допомогою спеціалізованих інструментів моніторингу мережі та протоколів, таких як RTCP (Real-time Transport Control Protocol).

2. Аналіз якості звуку (MOS, R-фактор)

Для оцінки суб'єктивного сприйняття якості голосового зв'язку використовуються метрики, такі як MOS (Mean Opinion Score) та R-фактор.

MOS - це стандартизована шкала оцінки якості голосу від 1 (неприйнятна) до 5 (відмінна), яка базується на суб'єктивних оцінках людей.

R-фактор - це об'єктивний показник, який розраховується на основі різних параметрів, таких як затримки, джитер, пакетні втрати та рівень шуму. Він використовується для прогнозування якості передачі голосу в IP-мережах.

Аналізуючи ці метрики, адміністратори VoIP-системи можуть виявляти проблеми з якістю голосу та вживати необхідних заходів для їх вирішення.

3. Збір та аналіз статистики використання

Моніторинг статистики використання VoIP-системи дозволяє відстежувати рівень завантаженості, виявляти пікові періоди та оптимізувати розподіл ресурсів. Серед ключових показників, які потрібно відстежувати, є:

- Кількість дзвінків
- Тривалість дзвінків
- Використання смуги пропускання
- Навантаження на сервери та шлюзи
- Активність користувачів

Аналіз цих даних допомагає виявити тенденції та моделі використання, що дозволяє приймати обґрунтовані рішення щодо масштабування та оптимізації VoIP-системи.

4. Виявлення та реагування на загрози безпеці

Моніторинг безпеки є важливим аспектом для виявлення та запобігання загрозам, таким як злам, DoS-атаки, спам через VoIP тощо. Необхідно постійно відстежувати підозрілу активність, аналізувати логи та використовувати системи виявлення/запобігання вторгнень (IDS/IPS).

У разі виявлення загроз потрібно вжити відповідних заходів, таких як блокування джерела атаки, активація резервних компонентів, оновлення систем безпеки та сповіщення відповідального персоналу.

5. Генерування звітів та повідомлень про стан системи

Для ефективного управління та підтримки VoIP-системи необхідно генерувати звіти та повідомлення про її поточний стан. Ці звіти можуть містити інформацію про продуктивність, безпеку, використання ресурсів, інциденти та попередження.

Звіти допомагають адміністраторам виявляти тенденції, проблеми та вузькі місця, а також приймати обґрунтовані рішення щодо оптимізації, масштабування та вдосконалення VoIP-системи. Крім того, вони можуть використовуватися для звітування керівництву та відстеження дотримання встановлених показників якості обслуговування (SLA).

Загалом, ретельний моніторинг та аналітика VoIP-системи є ключовими елементами для забезпечення її безперебійної та ефективної роботи, високої якості голосового зв'язку, захисту від загроз безпеці та своєчасного виявлення та вирішення потенційних проблем.

Висновки

У цьому розділі було детально розглянуто технологію IP телефонії на базі протоколу ініціації сесії (SIP). SIP являє собою відкритий стандарт для встановлення, модифікації та завершення мультимедійних сесій через IP-мережі. Він забезпечує основу для побудови сучасних корпоративних комунікаційних систем, що інтегрують голосовий зв'язок, відеоконференції, обмін миттєвими повідомленнями та інші функції в єдину платформу.

Було детально розглянуто принципи побудови SIP-мереж, включаючи їх основні компоненти, такі як SIP-сервери, шлюзи, термінальні пристрої та сервери додатків. Також було описано процес встановлення SIP-дзвінка з усіма етапами обміну повідомленнями між клієнтами та серверами.

Важливим аспектом є забезпечення належної якості обслуговування (QoS) у SIP-мережах. Для цього використовуються механізми пріоритезації трафіку, резервування пропускної здатності та боротьба з затримками і втратами пакетів.

SIP-телефонія також забезпечує можливості інтеграції з іншими корпоративними системами та додатками, такими як системи уніфікованих комунікацій, центри обробки викликів, CRM-системи тощо. Це досягається завдяки відкритим стандартам та інтерфейсам.

Нарешті, були розглянуті питання забезпечення безпеки та надійності в SIP-мережах, включаючи автентифікацію, шифрування, механізми безпеки на різних рівнях моделі OSI та стратегії відмовостійкості.

Отже, SIP-телефонія являє собою гнучку та масштабовану технологію для побудови сучасних корпоративних комунікаційних систем із широким спектром можливостей та функцій. Вона забезпечує економічну ефективність, інтеграцію з іншими додатками та високі стандарти безпеки і надійності, що робить її привабливим рішенням для впровадження на критично важливих об'єктах, таких як атомні електростанції.

РОЗДІЛ 3
РОЗГОРТАННЯ SIP ТЕЛЕФОННОЇ МЕРЕЖІ НА АЕС

3.1 Вибір обладнання та програмного забезпечення

Розгортання SIP телефонної мережі на АЕС з використанням FreePBX вимагає ретельного планування та виконання декількох ключових кроків. Нижче наведено детальний огляд цього процесу.

Необхідно вибрати потужний сервер, який зможе обробляти очікуваний обсяг викликів та надавати необхідні функції. Вимоги до апаратного забезпечення залежатимуть від кількості користувачів, голосових потоків та додаткових функцій, що потрібні.

Для інтеграції з традиційними телефонними мережами (PSTN/ISDN) потрібно встановити VoIP-шлюзи, які забезпечать перетворення сигналів між IP-мережею та аналоговими/цифровими лініями.

Рис.3.1. Софтфон

Слід вибрати SIP-сумісні IP-телефони або софтфони для кінцевих користувачів. Важливо переконатися, що вони сумісні з FreePBX та відповідають вимогам до якості та функціональності.

Необхідно забезпечити належну мережеву інфраструктуру, включаючи комутатори, маршрутизатори та брандмауери, які підтримують вимоги QoS для VoIP-трафіку.

Рис.3.2. FreePBX

FreePBX - це відкрита платформа для побудови телефонних систем на базі Asterisk. Вона забезпечує функціональність IP-АТС, голосову пошту, інтерактивне голосове меню (IVR) та інші функції.

3.2 Налаштування та конфігурація

Необхідно встановити FreePBX на вибраний сервер та виконати базову конфігурацію, таку як налаштування мережевих параметрів, часового поясу, кодеків та інших основних налаштувань.

Для інтеграції з традиційними телефонними мережами потрібно налаштувати SIP-трунки, які визначають маршрути викликів та параметри з'єднання з VoIP-шлюзами.

Необхідно створити облікові записи користувачів у FreePBX та призначити їм внутрішні номери телефонів. Також слід налаштувати параметри користувачів, такі як голосова пошта та права доступу.

Потрібно налаштувати маршрутизацію викликів у FreePBX, визначаючи правила для внутрішніх, вхідних та вихідних дзвінків, а також налаштувати додаткові функції, такі як черги викликів, IVR та конференц-зв'язок.

За потреби можна інтегрувати FreePBX з іншими системами, такими як CRM, електронна пошта або системи аварійного оповіщення, для автоматизації процесів та покращення комунікацій.

3.3 Тестування та впровадження

Перед впровадженням у виробниче середовище необхідно ретельно протестувати налаштування та функціональність FreePBX у лабораторному

або тестовому середовищі. Це дозволить виявити та вирішити будь-які проблеми або помилки конфігурації.

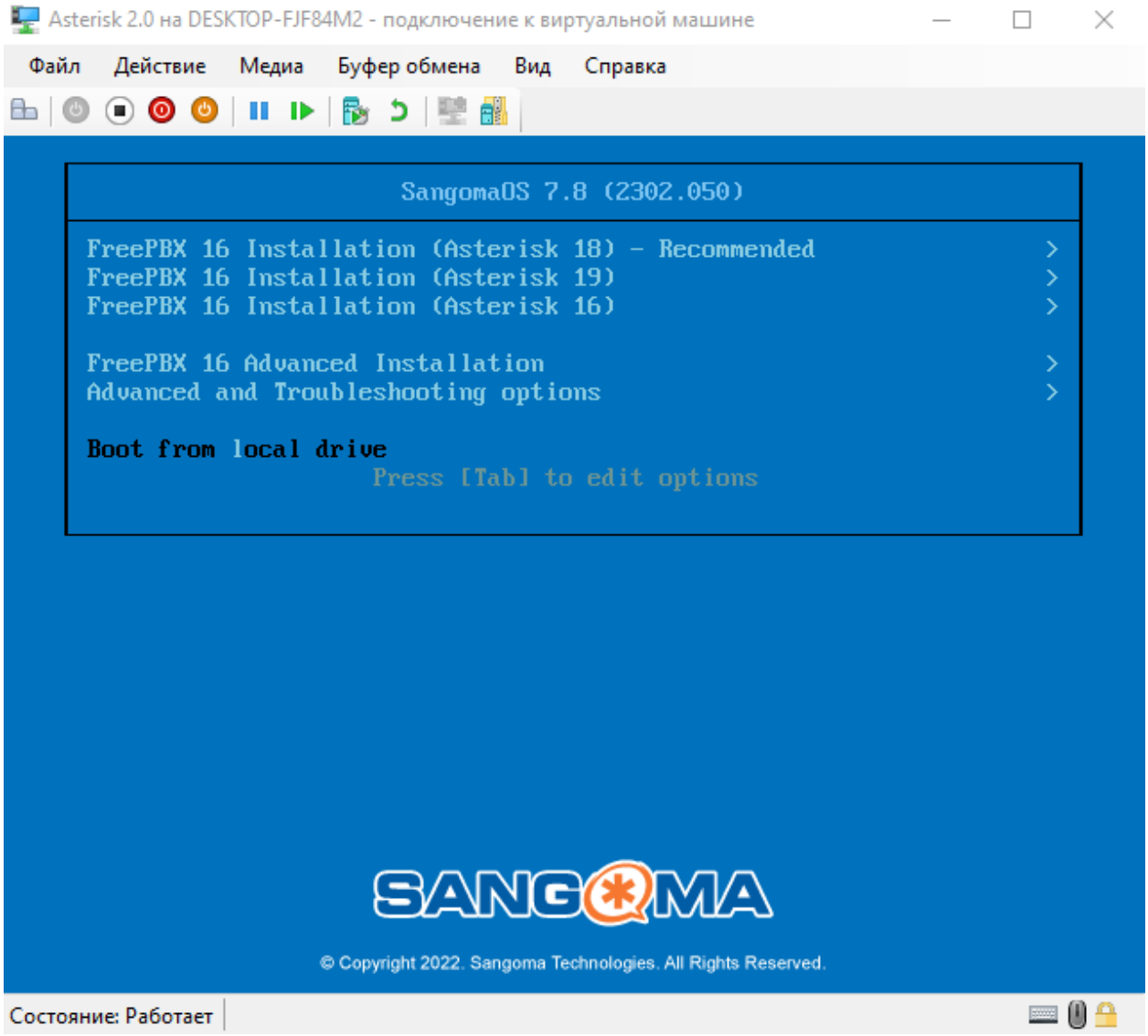

Рис.3.3. Запуск ПЗ на віртуальній машині

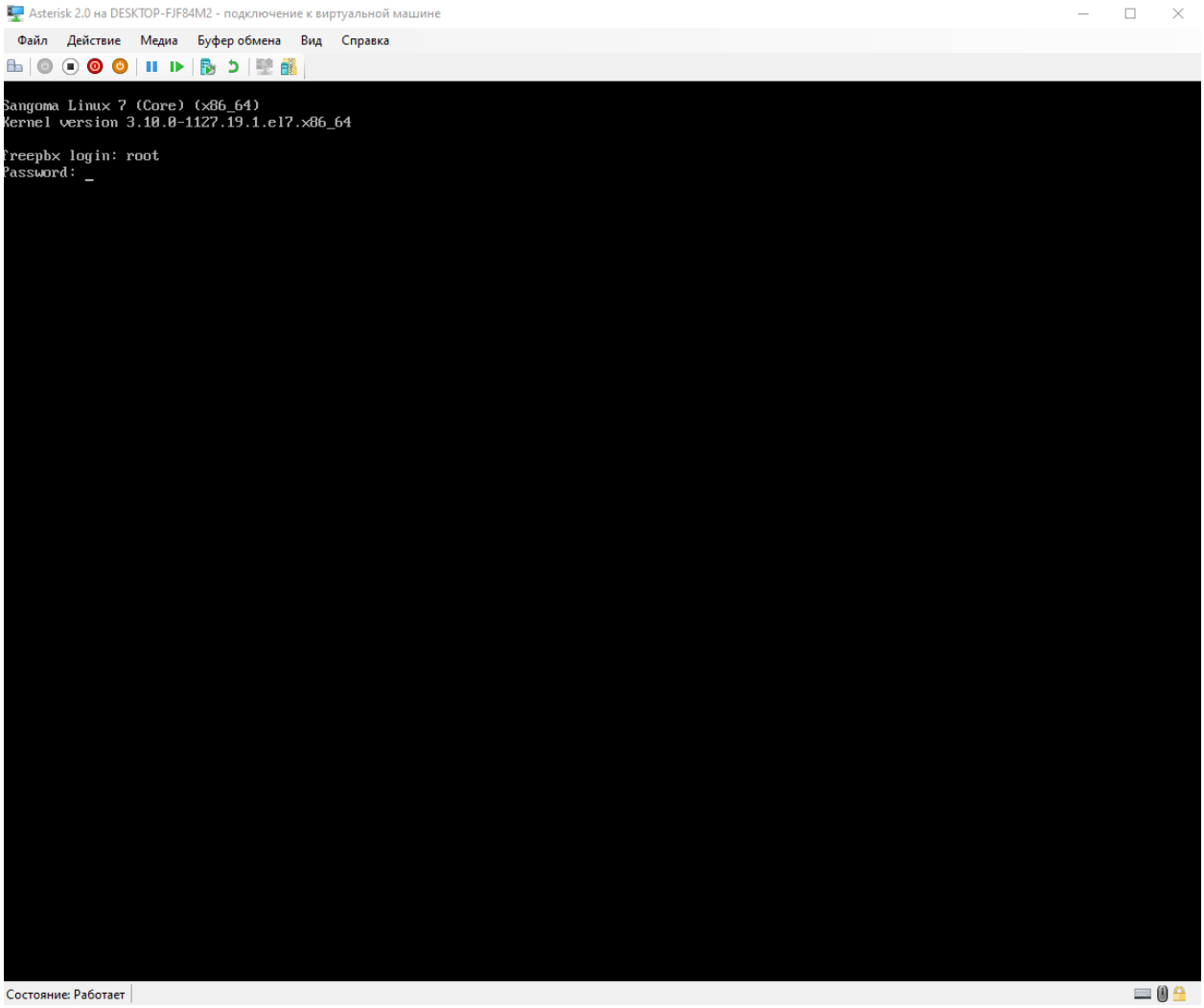

Рис.3.4. Авторизація

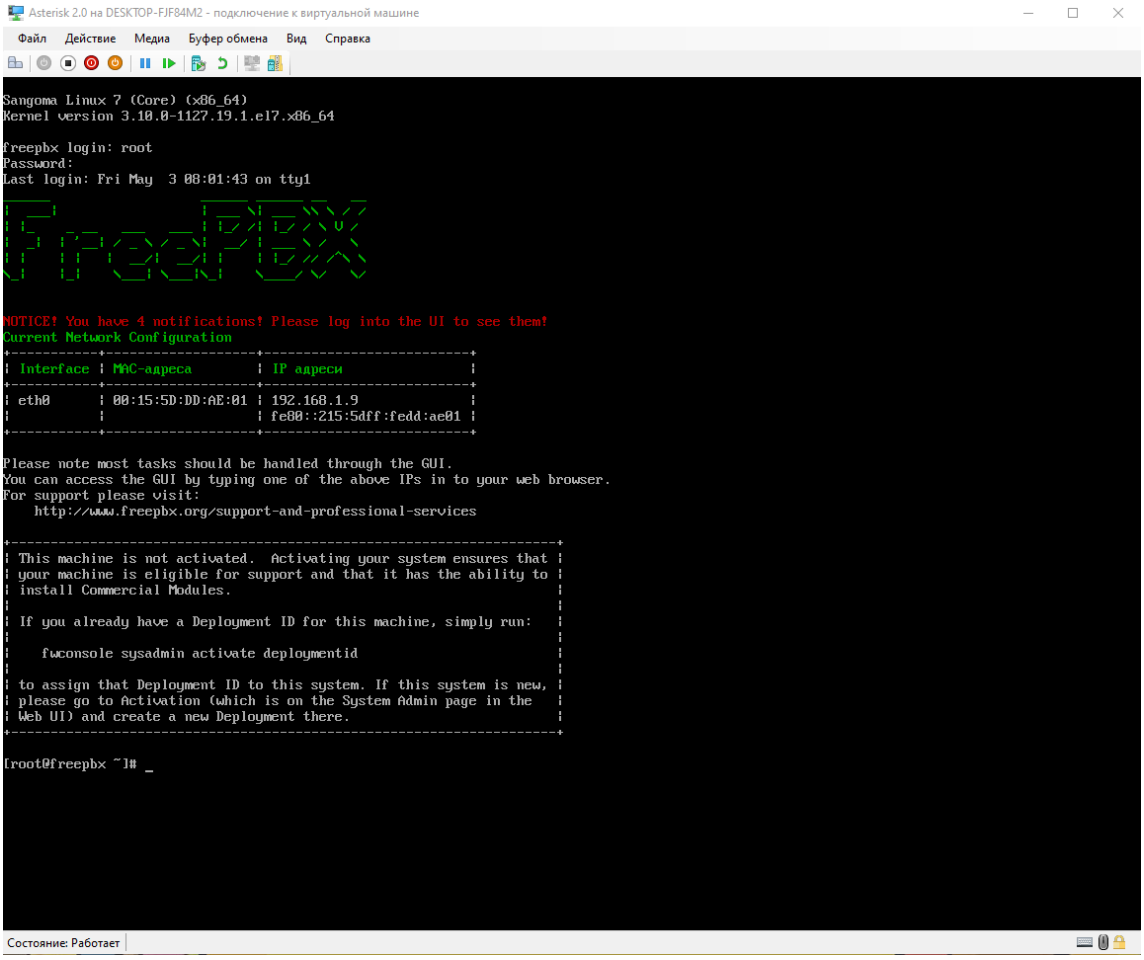

Рис.3.5. Дані FreePBX

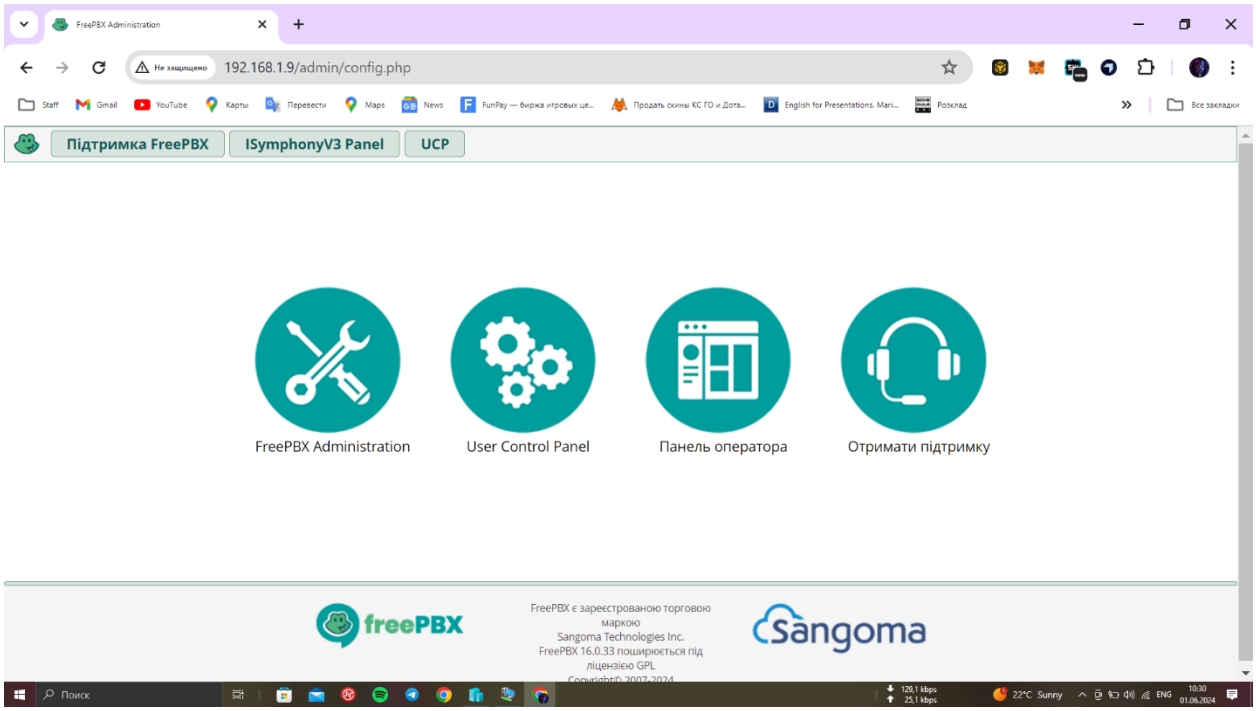

Рис.3.6. Сторінка адміністратора

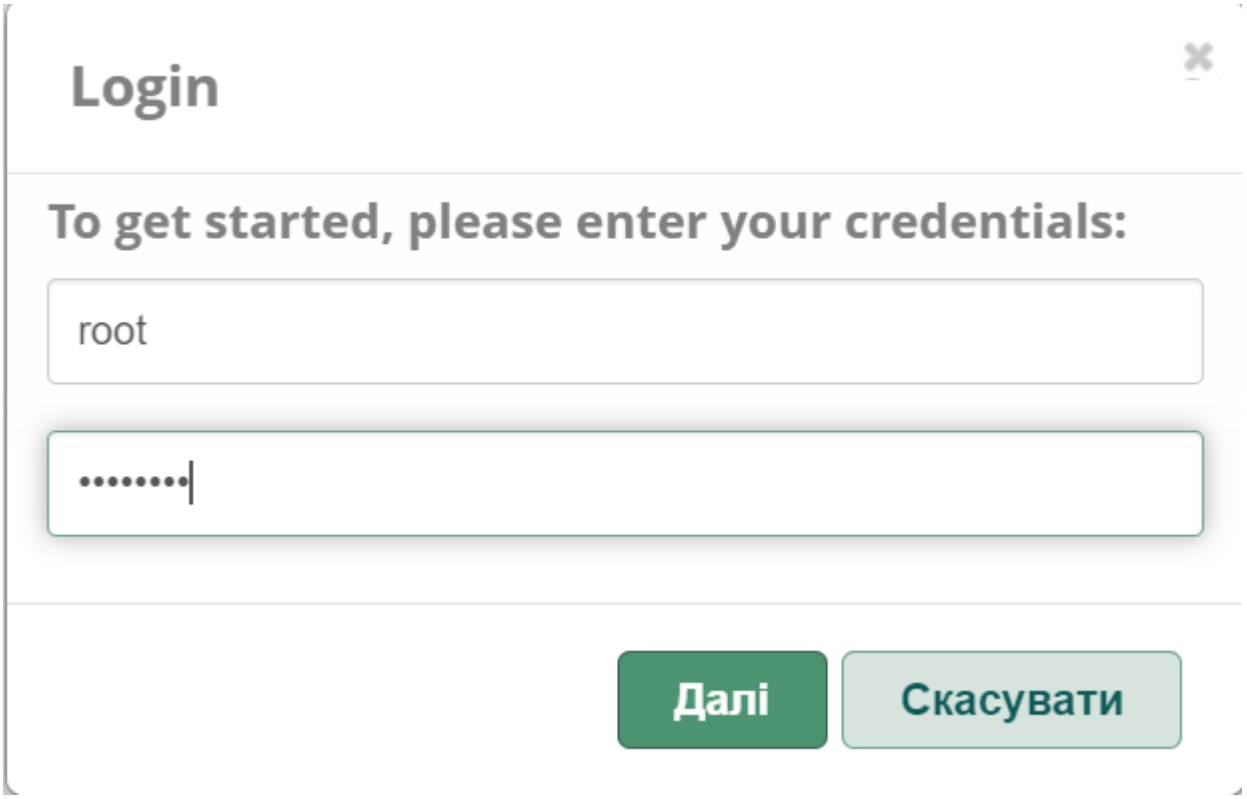

Рис.3.7. Авторизація в графічному середовищі

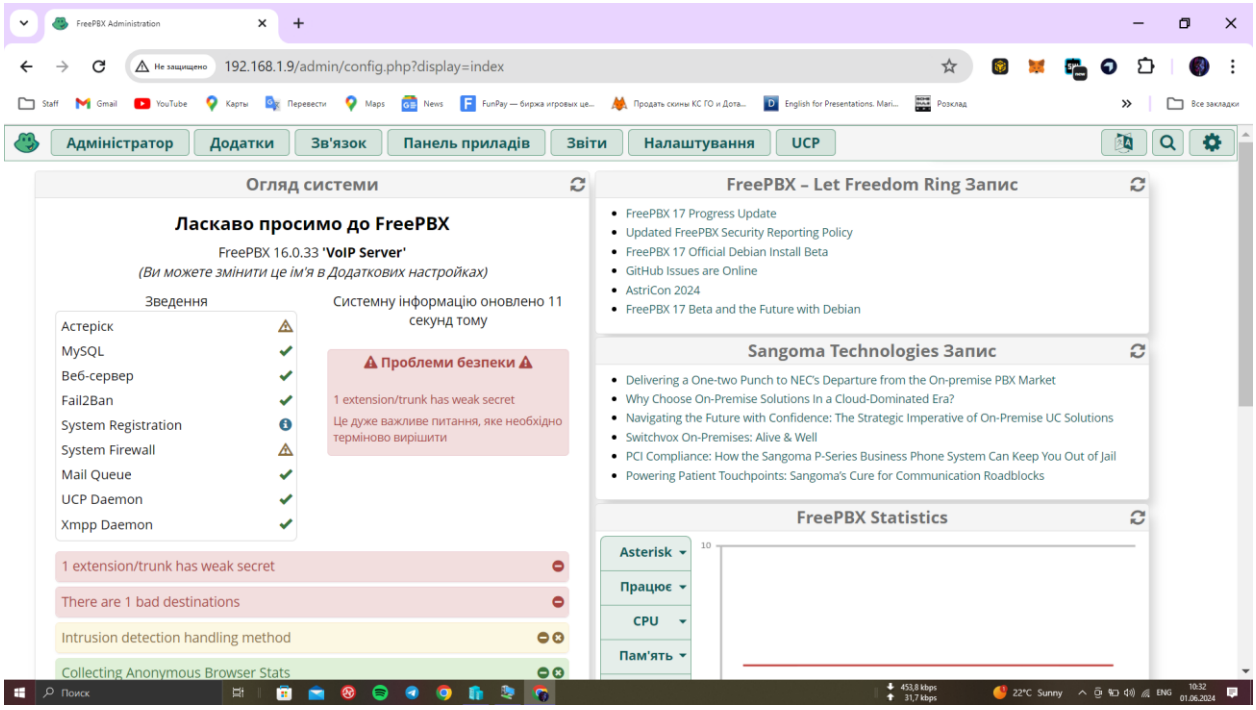

Рис.3.8. Головна панель приладів

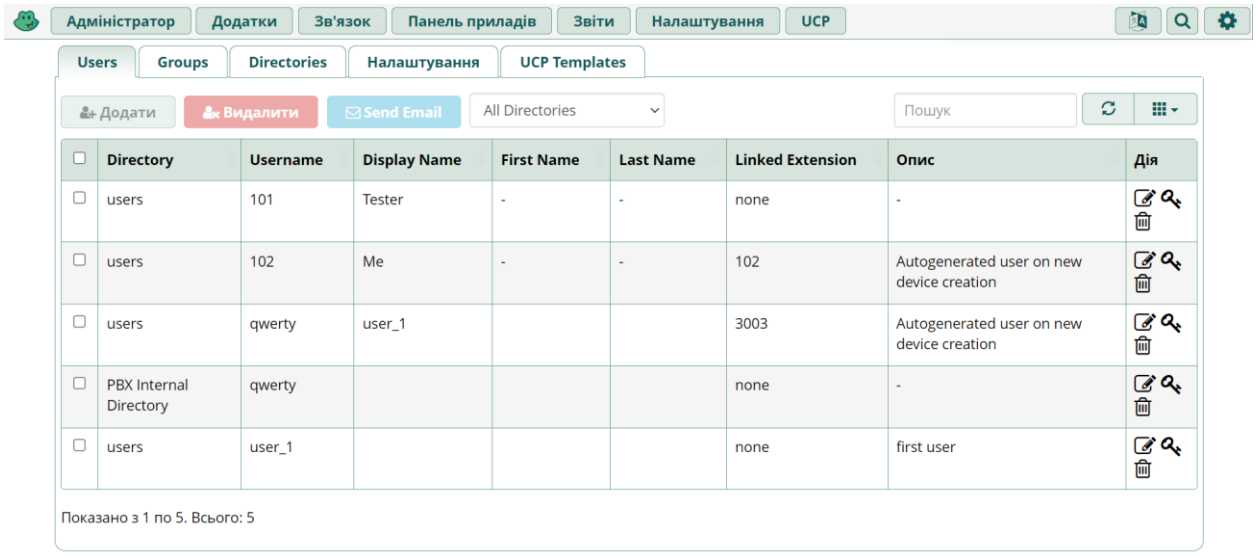

Рис.3.9. Список користувачів

2. Пілотне впровадження

Після успішного тестування можна розпочати пілотне впровадження FreePBX у обмеженому масштабі, наприклад, для однієї групи користувачів або відділу. Це дозволить оцінити роботу системи в реальних умовах та внести необхідні корективи перед повним розгортанням.

3. Навчання користувачів

Перед повним впровадженням необхідно провести навчання для користувачів, щоб вони змогли ефективно використовувати всі функції FreePBX та IP-телефонів.

4. Повне розгортання та міграція

Після успішного пілотного впровадження та навчання користувачів можна розпочати повне розгортання FreePBX у всьому середовищі АЕС. Цей процес може включати поетапну міграцію користувачів з існуючої телефонної системи на нову VoIP-мережу.

5. Моніторинг та підтримка

Після впровадження необхідно постійно моніторити роботу FreePBX, відстежувати показники продуктивності та якості обслуговування, а також забезпечувати своєчасне оновлення системи та усунення будь-яких проблем або інцидентів.

Ретельне планування, належна конфігурація та тестування є ключовими факторами для успішного розгортання надійної та безпечної SIP телефонної мережі на АЕС з використанням FreePBX. Залучення досвідчених фахівців та дотримання найкращих практик допоможе уникнути потенційних проблем та забезпечити безперебійну роботу критично важливої комунікаційної інфраструктури.

Висновки

Для реалізації SIP телефонії на АЕС необхідні такі дії:

- Проведення ретельного аналізу існуючої інфраструктури та потреб
- Визначення вимог до безпеки, надійності та резервування
- Вибір відповідного обладнання та програмного забезпечення
- Розробка детального плану міграції з мінімальним впливом на поточні операції
- Навчання персоналу та забезпечення технічної підтримки
- Поетапне впровадження з ретельним тестуванням на кожному етапі

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

У даній роботі було ретельно досліджено питання модернізації застарілих телекомунікаційних мереж на атомних електростанціях шляхом впровадження IP телефонії на основі протоколу ініціації сесії (SIP). Проведений аналіз показав нагальну необхідність заміни існуючих мереж комутованих телефонних систем (TDM) на сучасніші та більш гнучкі рішення.

Традиційні TDM мережі, не зважаючи на їхню перевірену надійність, мають низку серйозних обмежень, які унеможливлюють їх ефективне використання на критично важливих об'єктах, якими є АЕС. Високі експлуатаційні витрати, обмежена масштабованість, відсутність підтримки сучасних додатків та функцій уніфікованих комунікацій - все це робить TDM мережі застарілими та неприйнятними для АЕС.

Натомість, технологія IP телефонії на базі протоколу SIP пропонує низку істотних переваг, які повністю відповідають сучасним вимогам до корпоративних комунікацій на АЕС. Це включає економічну ефективність, вищу масштабованість, можливість безпроблемної інтеграції з різноманітними додатками, а також підвищену надійність та відмовостійкість за рахунок резервування та розподілених архітектур. Крім того, SIP телефонія дозволяє розгорнути комплексні системи забезпечення якості обслуговування (QoS) та механізми кібербезпеки, які є критично важливими для АЕС.

Однак, успішне впровадження SIP мереж на атомних електростанціях вимагає ретельного планування, вибору відповідного обладнання та програмного забезпечення, налаштування всіх компонентів відповідно до вимог безпеки та продуктивності. Необхідно також розробити стратегію поетапної міграції від існуючої TDM інфраструктури до SIP платформи, забезпечуючи безперервність критичних комунікацій та навчання персоналу роботі з новими технологіями.

Успішне розгортання корпоративної мережі SIP телефонії на АЕС дозволить побудувати надійну, масштабовану, економічно ефективну та захищену платформу для корпоративних комунікацій. Вона забезпечить

вищий рівень безпеки, співпраці, оперативного обміну інформацією та уніфікованих сервісів для персоналу різних відділів АЕС. Це, у свою чергу, сприятиме підвищенню загальної ефективності та безпеки експлуатації атомних електростанцій відповідно до сучасних вимог і технологічних стандартів.

Отже, модернізація телекомунікаційної інфраструктури шляхом впровадження SIP телефонії є не просто бажаною, а життєво необхідною для атомних електростанцій. Це дозволить їм залишатися на передовій забезпечення безпеки та ефективності своєї діяльності в інтересах суспільства та навколишнього середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг (НКРЕКП). (2019). Вимоги до телекомунікаційних мереж операторів, що експлуатують атомні електростанції. [Електронний ресурс] – Режим доступу: https://www.nerc.gov.ua/data/filearch/Proekty/2019/pr_219/pr_219.pdf
2. Міжнародне агентство з атомної енергії (МАГАТЕ). (2015). Комп'ютерна безпека на ядерних установках. Серія норм безпеки МАГАТЕ, № NS-G-1.1. [Електронний ресурс] – Режим доступу: https://www.iaea.org/publications/8741/computer-security-at-nuclear-facilities
3. Парсон, Дж. (2019). Безпечні комунікаційні системи для атомних електростанцій. Журнал "Nuclear Engineering International", 64(787), 14-18. Режим доступу: https://www.neimagazine.com/features/featuresecure-communications-for-nuclear-power-plants-7233819/
4. Кампос, Х., & Ромеро, Е. (2017). Безпека IP-мереж на атомних електростанціях: проблеми та рішення. Журнал "Nuclear Safety and Security", 8(2), 112-127. Режим доступу: https://www.tandfonline.com/doi/abs/10.1080/18811248.2017.1325771
5. Cisco Systems, Inc. (2018). Архітектура безпечної корпоративної мережі для атомних електростанцій. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/secure-network-architecture-for-nuclear-power-plants-white-paper.html
6. Siemens AG. (2022). Розробка інфраструктури IP-телефонії для критично важливих об'єктів. [Електронний ресурс] – Режим доступу: https://new.siemens.com/global/en/products/communications/enterprise-communications/voice-communications.html
7. Бхатія, В., & Бхатія, А. К. (2022). Огляд корпоративних мереж IP-телефонії для атомних електростанцій. Журнал "Nuclear Technology & Radiation Protection", 37(1), 31-42. Режим доступу:

https://www.scholarly.com/journal/2334-7159-Nuclear-Technology-Radiation-Protection

8. Адресація в мережах sip [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Session_Initiation_Protocol
9. VoIP кодеки [Електронний ресурс] – Режим доступу до ресурсу: https://www.terratel.eu/voip-codecs.html
10. Ядерне регулювання Комісії США (NRC). (2020). Кібербезпека у галузі ядерної енергетики. [Електронний ресурс] – Режим доступу: https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/cyber-security-bg.html