Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Інфокомунікаціїі*
(повна назва)

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

другий (магістерський)
(рівень вищої освіти)

(позначення документа)

Аналіз методів реалізації IP-телефонії у корпоративних мережах

(тема)

Виконав: студент 2 курсу, групи *ІМІм-21-1*
Спеціальності *172 Телекомунікації та радіотехніка*
(код і повна назва спеціальності)
Освітньо-професійної програми
Інформаційно-мережна інженерія .
(повна назва освітньо-професійної програми)
Мітраков М. А.
(прізвище, ініціали)
Керівник *доц. Омельченко А.В.*
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ *Безрук В.М.*
(підпис) (прізвище, ініціали)

2022 р.

Не містить відомостей, заборонених до відкритого публікування

Студент _____ *Мітраков М. А.*
(підпис) (прізвище та ініціали)

Керівник _____ *Омельченко А.В.*
(підпис) (прізвище та ініціали)

Харківський національний університет радіоелектроніки
(повна назва вищого навчального закладу)

Факультет *Інфокомунікацій*
Кафедра *Інформаційно-мережної інженерії*
Освітній рівень *другий (магістерський)*
Спеціальність *172 Телекомунікації та радіотехніка*
Освітня програма *Інформаційно-мережна інженерія*
(повна назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри ІМІ
_____ *проф. Безрук В.М.*
"____" _____2022 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Мітракову Микиті Артемовичу

1. Тема роботи *Аналіз методів реалізації IP-телефонії в корпоративних мережах*

керівник роботи *Омельченко Анатолій Васильович, к.т.н., доц.*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом ВНЗ від «21» *жовтня* 2022 року № *1376 Ст*

2. Строк подання студентом роботи *15 грудня 2022 р.*

3. Вихідні дані до роботи *Об'єкт дослідження – методи реалізації IP-телефонії в корпоративних мережах.*

Виконати огляд принципів IP-телефонії. Розглянути архітектуру і основні протоколи IP-телефонії. Проаналізувати фактори, що визначають QoS і інформаційну безпеку в мережі IP-телефонії. Проналізувати методи реалізації серверів (IP-АТС) і шлюзів IP-телефонії.

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Вступ
1. Огляд принципів IP-телефонії
2. Архітектура і протоколи IP-телефонії
3. Аналіз методів реалізації серверів (IP-АТС) і шлюзів IP-телефонії
4. Методи забезпечення інформаційної безпеки IP-телефонії в корпоративних мережах
5. Впровадження IP-телефонії у корпоративній мережі
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Слайди у форматі Power Point (назва, мета і актуальність атестаційної роботи, архітектура VoIP мережі, основні протоколи VoIP, IP-телефонія на платформі Asterisk, застосування віртуальної АТС, типи загроз в мережах IP-телефонії, використання технології VoIP через VPN, схема локальної мережі підприємства, основні результати розрахунків, висновки)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ*	*01.11-4.11*	*Виконано*
2	*Підбір літератури за темою роботи*	*05.11-10.11*	*Виконано*
3	*Виконання розділу 1*	*05.11-10.11*	*Виконано*
4	*Виконання розділу 2*	*11.11-15.11*	*Виконано*
5	*Виконання розділу 3*	*16.11-20.11*	*Виконано*
6	*Виконання розділу 4*	*21.11-25.11*	*Виконано*
7	*Виконання розділу 5*	*26.11-30.11*	*Виконано*
8	*Оформлення пояснювальної записки*	*01.12-10.12*	*Виконано*
9	*Оформлення презентаційного матеріалу,*		
	підготовка до захисту у ЕК	*11.12-15.12*	*Виконано*

Дата видачі завдання *01.11.2022 р.*

Студент _____ *(Мітраков М.А.)*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *(Омельченко А.В.)*
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 77 с., 13 рис., 1 табл., 14 джерел, 1 додатки.

Об'єкт дослідження – методи реалізації IP-телефонії в корпоративних мережах.

Мета роботи – провести порівняльний аналіз реалізації різних методів IP-телефонії у корпоративних мережах.

Досліджено види IP-телефонії у корпоративних мережах.

Розглянуто види IP-телефонії в корпоративних мережах та основні методи їх реалізації.

КОРПОРАТИВНА МЕРЕЖА, ІНФОРМАЦІЙНА БЕЗПЕКА, IP-АТС, IP-ТЕЛЕФОНІЯ, ПРОТОКОЛ, ШЛЮЗИ

THE ABSTRACT

Explanatory note: 77 pp., 13 figures, 1 table, 14 sources, 1 app.

The object of research is methods of implementing IP telephony in corporate networks.

The purpose of the work is to conduct a comparative analysis of the implementation of various methods of IP telephony in corporate networks.

Types of IP telephony in corporate networks have been studied.

The types of IP telephony in corporate networks and the main methods of their implementation are considered.

CORPORATE NETWORK, INFORMATION SECURITY, IP PBX, IP-TELEPHONY, PROTOCOL, GATEWAYS

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АТС – Автоматична телефонна станція
CDMA (Code Division Multiple Access) – Множинний доступ з кодовим розділенням
CHAP (Challenge Handshake Protocol) – Протокол рукостискання виклику
DoS (Denial of Service) – Відмова в обслуговуванні
EDGE (Enhanced Data rates for Global Evolution) – Підвищені швидкості передачі даних для Global Evolution
EV-DO (Evolution -Data Optimized) – Еволюція - Оптимізація даних
EAP (Extensible Authentication Protocol) – Розширюваний протокол
GSM – Глобальна система мобільного зв'язку
GPRS (General Packet Radio Service) – Загальна служба пакетної
ISDN – Цифрова Мережа з Інтегрованими Послугами
LCP (Link Control Protocol) – Протокол керування з’єднанням
MGCP – Протокол керування медіашлюзом
MNP (Mobile number portability) – Перенесення мобільного номера
NCP (Network Control Protocols) – Протоколи керування мережею
PAP (Password Authentication Protocol) – Протокол автентифікації пароля
PPP (Point-to-Point Protocol) – Протокол «точка-точка».
автентифікації
QoS (Quality of Service) – Якість обслуговування
RTP (Real-time Transport Protocol) – Транспортний протокол реального часу
SDP (Session Description Protocol) – Протокол опису сесії
SHA (Secure Hash Algorithm) – Алгоритм безпечного хеша
TLS (Transport Layer Security) – Безпека транспортного рівня
UDP – протокол користувальницьких дейтаграм
VoIP (voice over IP) – голос через IP
радіопередачі
WAP – Бездротова точка доступу
SIP – Протокол початку сеансу

ВСТУП

В наші дні неможливо уявити роботу різного роду фірм та підприємств без використання телефонного зв'язку. Це обов’язковий іструмент для організації роботи колективу та виконання корпоративних завдань. Традиційний телефонний зв'язок практично повністю поступається своїм місцем IP телефонії, що базується на передачі по інтернет-протоколу. Найбільше це торкнулося корпоративного сегмента – компанії які масово відмовляються від аналогової телефонії і замінюють її сучасними VoIP системами. Перехід з традиційної телефонії на IP телефонію обумовлена необхідністю компаній скорочувати витрати на зв'язок і підвищувати ефективність комунікації.

IP-телефонія – це телефонний зв'язок через інтернет, по протоколу IP. Під IP-телефонією мається на увазі набір комунікаційних протоколів, VoIP обладнання, програмного забезпечення, технологій і методів, що забезпечують традиційні для телефонного зв'язку функції: набір номера, двостороннє голосове спілкування, та відеоспілкування через мережу Інтернет або будь-якою іншою IP-мережею. Сигнал по каналу зв'язку передається в цифровому вигляді та, як правило, перед передачею перетворюється з тим, щоб видалити надлишок інформації та знизити навантаження на мережу передачі даних. Основна перевага IP-телефонії в зниженні витрат на зв'язок. У багатьох випадках VoIP-зв'язок – безкоштовний.

До основних переваг, відносять простоту використання таких мереж, відносно невелику вартість побудови та обслуговування таких мереж в порівнянні з аналоговими системами передачі голосового зв’язку, можливість підключення великої кількості абонентів до однієї локальної мережі, а також відносна надійність таких систем зв’язку. Всі вищесказані переваги IP-телефонії дають можливість стверджувати, що VoIP підвищує ефективність ведення бізнесу завдяки можливості організації зв’язку між усіма робітниками компанії, створення центрів технічної підтримки користувачів, інтеграція з

різними додатками, тощо. В наслідок цього розвиток досліджень в даному напрямку представляэться своєчасним і доречним.

Для того щоб максимально знизити витрати на організацію корпоративного телефонного зв'язку, рекомендується використовувати програмне забезпечення з відкритим вихідним кодом для розгортання сервера телефонії набазі дистрибутива Asterisk. Asterisk – вільне рішення комп'ютерної телефонії з відкритим вихідним кодом. У даній роботі приведений детальний опис цього програмного забезпечення, а також приклад налаштування локальної мережі IP-телефонії.

1 ОГЛЯД ПРИНЦИПІВ IP-ТЕЛЕФОНІЇ

1.1 Обробка сигналів у пристроях VoIP

VoIP – технологія передачі медіа-даних у реальному часі за допомогою сімейства протоколів TCP/IP. IP-телефонія – система зв'язку, в якій аналоговий звуковий сигнал абонента дискретизується (кодується в цифрову форму), компресується й пересилається цифровими каналами зв'язку до іншого абонента, де проводиться зворотня операція – декомпресія, декодування й відтворення аналогового сигналу.

IP-телефонія – технологія, яка дозволяє використовувати будь-яку мережу з пакетною комутацією на базі протоколу IP як засіб організації та ведення міжнародних, міжміських та місцевих телефонних розмов та передачі факсів у режимі реального часу. Іншими словами, використовуючи доступні канали Інтернет, можна здійснювати дзвінки в будь-яку точку світу, де є телефон або існує доступ до Інтернету. Під IP-телефонією мається на увазі набір комунікаційних протоколів, технологій та методів, що забезпечують традиційні для телефонії набір номера, додзвон і двостороннє голосове спілкування, а також відеоспілкування через Інтернет або будь-які інші IP-мережі. Сигнал по каналу зв'язку передається в цифровому вигляді і, як правило, перед передачею перетворюється (стискається) для того, щоб видалити надлишок інформації і знизити навантаження на мережу передачі даних.

VoIP – це технологія, яка полягає в тому, що телефонні дзвінки обробляються IP-мережею передачі даних; їй може бути Інтернет чи власна внутрішня мережа організації. Однією з головних переваг VoIP є можливість зниження витрат, оскільки виклики обробляються мережею передачі даних швидше, ніж телефонною мережею компанії. На рис. 1 представлено схематичне представлення архітектури мережі VoIP [1].

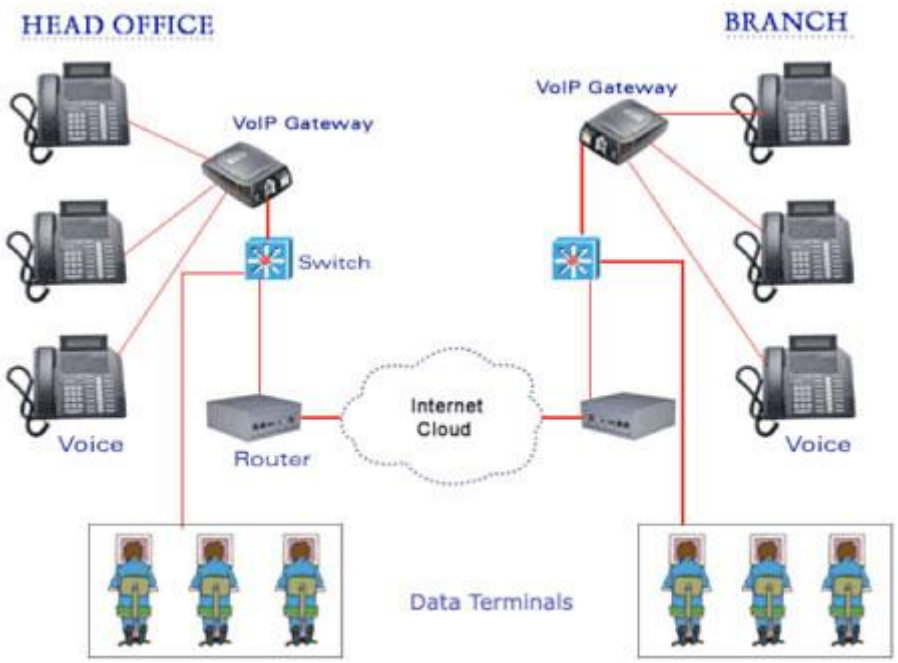

Рисунок 1 – Архітектура VoIP мережі

Принцип роботи полягає в наступному: один із абонентів передає голосові сигнали іншому абоненту, ваш голос проходить обробку за допомогою кодеків та пересилається через Інтернет пакетними даними в режимі реального часу. При цьому максимальна затримка звуку становить приблизно 300-400 мілісекунд залежно від того, скільки часу потрібно апаратному устаткуванню для створення цифрового аудіосигналу. Оскільки в даний час існують технології, що дозволяють звести втрати сигналу в мережі до мінімуму і уникнути пропадання голосу, то ми цього і не помітимо. В результаті за цю розмову ви заплатите набагато менше, ніж якби ви користувалися звичайними телекомунікаціями. Для передачі сигналу необхідні спеціальні пристрої – IP-шлюзи. Це пристрої, за допомогою яких здійснюється трансляція даних з одного типу мережі мережі іншого типу. IP-шлюзи, або як їх ще називають IP-сервери, з одного боку пов'язані з телефонними лініями і можуть встановити з'єднання з будь-яким телефоном світу, а з іншого - з інтернетом, за рахунок чого можуть зв'язуватися з будь-яким комп'ютером, що під'єднаний до інтернету [1].

Телефонний сигнал шлюзом оцифровується, стискається, розбивається на пакети і відправляє через мережу IP за призначенням з використанням

протоколу TCP/IP. Потім сигнал проходить через ще один шлюз, де знову перетворюється на телефонний і абонент отримує виклик. На сьогоднішній день доступ в Інтернет можливий безпосередньо з мобільних телефонів, які підтримують технології: GSM Data, GPRS (General Packet Radio Service), EDGE (Enhanced Data rates for Global Evolution), CDMA (Code Division Multiple Access), EV-DO (Evolution -Data Optimized), які забезпечують широкий спектр послуг "Мобільний Інтернет" та WAP.

З вище згаданого виходить, що голосовий сигнал з каналу VoIP може безпосередньо надходити на IP-телефон, підключений до IP-мережі або на мобільний телефон мобільного оператора, або на аналоговий телефон, підключений до звичайної телефонної мережі [1].

Сумісність мобільних номерів (Mobile number portability, MNP) також впливає на IP-телефонію, або іншими словами, на комерційне застосування VoIP. Голосовий дзвінок, який прийшов каналом, маршрутизується на мобільний телефон традиційного мобільного оператора, також має завдання досягти мети призначення, яка у випадку з мобільним телефоном виражається в тому, що дзвінок (сигнал) повинен досягти порту. Сумісність мобільних номерів – це сервіс, який дозволяє користувачам зберегти існуючий телефонний номер під час переходу від одного мобільного оператора до іншого [1].

Таким чином, IP-телефонія забезпечує передачу голосових сигналів з комп'ютера на комп'ютер, з комп'ютера на телефон та телефону на телефон. Дзвінки здійснюються через постачальника послуг VoIP. Якість передачі голосу залежить від VoIP-провайдера та способу підключення до Інтернету.

1.2 Кодеки і QoS

Аудіокодеком називають програму або алгоритм, який стискає або розтискає цифрові звукові дані, дозволяючи знизити вимоги до пропускної здатності каналу передачі даних. В IP-телефонії на сьогоднішній день найбільш поширене перетворення за допомогою кодека G.729, а також стиснення G.711 за A-законом (alaw) та μ-законом (ulaw) [9].

Кодек G.729

G.729 є кодеком, який стискає вихідний сигнал із втратою даних. Основна ідея, закладена в G.729 - передача не самого оцифрованого сигналу, а його параметрів (спектральної характеристики, кількості переходів через нуль), достатніх для подальшого синтезування на стороні, що приймає. При цьому всі основні характеристики голосу, такі як амплітуда та тембр, зберігаються.

Пропускна здатність каналу, на яку розрахований кодек - 8 кбіт/с. Довжина кадру оброблюваного G.729 - 10 мс, частота дискретизації - 8 кГц. Для кожного з таких кадрів визначаються параметри математичної моделі, які надалі передаються в канал у вигляді кодів [9].

При використанні кодування G.729 затримка становить 15 мс, з яких 5 мс витрачається заповнення попереднього буфера. Зазначимо також, що кодек G.729 висуває досить високі вимоги до ресурсів процесора.

Кодек G.711

G.711 — голосовий кодек, який передбачає ніякого стиснення, крім компандирования — методу зменшення ефектів каналів з обмеженим динамічним діапазоном. У основі цього методу лежить принцип зменшення кількості рівнів квантування сигналу області високої гучності, зберігаючи у своїй якість звуку. Дві схеми компандування, що широко використовуються в телефонії, — alaw і ulaw [9].

Сигнал у цьому кодеку наданий потоком величиною 64 кбіт/с. Частота дискретизації - 8000 кадрів по 8 біт за секунду. Якість голосу суб'єктивно краща, ніж при застосуванні кодеку G.729.

Кодек alaw

alaw або А-закон - алгоритм стиснення звукових даних із втратою інформації. В основному використовується на території Європи

Для сигналу x перетворення за алгоритмом alaw виглядає так:

$$F(x) = \operatorname{sgn}(x) \begin{cases} \frac{A|x|}{1+\ln(A)}, & |x| < \frac{1}{A} \\ \frac{1+\ln(A|x|)}{1+\ln(A)}, & \frac{1}{A} \le |x| \le 1, \end{cases}$$

де A - параметр стиснення (зазвичай приймається рівним 87,7).

Кодек ulaw

Ulaw або μ-закон - алгоритм стиснення звукових даних із втратою інформації. В основному використовується на території Японії та Північної Америки [9].

Для сигналу x перетворення за алгоритмом ulaw виглядає так:

$$F(x) = \operatorname{sgn}(x)\frac{\ln(1+\mu|x|)}{\ln(1+\mu)} \qquad -1 \leqslant x \leqslant 1,$$

де μ приймається рівним 255 (8 біт) у стандартах Північної Америки та Японії.

У мережах на основі стека TCP/IP висока якість обслуговування трафіку, чутливого до затримок передачі, не забезпечується за замовчуванням. При використанні протоколу TCP є гарантія достовірної доставки інформації, але її перенесення може здійснюватись із непередбачуваними затримками. Для UDP характерна мінімізація затримок, але гарантія правильної доставки пакета відсутня [9].

У той же час добротність мовного трафіку залежить від якості передачі, і в мережі, де не реалізовані механізми, що гарантують відповідну якість, реалізація IP-телефонії може бути не задовольняє вимогам користувачів.

Основними показниками якості обслуговування є пропускна спроможність мережі та затримка передачі. Затримка при цьому визначається як проміжок часу, що минув з моменту надсилання пакета, до моменту його прийому [9].

Також існують такі характеристики, як готовність мережі та її надійність (оцінюються за результатами контролю рівня обслуговування протягом тривалого часу або за коефіцієнтом використання).
Для покращення якості зв'язку використовуються такі механізми:

1. Перемаршрутизація. При навантаженні одного з каналів зв'язку дозволяє здійснити доставку за допомогою резервних маршрутів.

2. Резервування ресурсів каналу зв'язку на час з'єднання.

3. Пріоретизація трафіку. Дає можливість помічати пакети відповідно до рівня їх важливості та здійснювати обслуговування на основі міток. Як було сказано раніше, голосовий трафік надзвичайно чутливий до затримок передачі. Максимальний час затримки має перевищувати 400 мс (сюди включається і тривалість обробки інформації на кінцевих станціях). Розрізняють два основні типи затримок:

— Затримка кодування інформації в голосових шлюзах або термінальному обладнанні. Зменшується шляхом покращення алгоритмів обробки та перетворення голосу.

— Затримка мережі мережі передачі. Зменшується шляхом покращення мережевої інфраструктури, зокрема, скороченням кількості маршрутизаторів та використанням високошвидкісних каналів.

Рисунок 1.1 – Джерела затримки в IP-телефонії

Джиттер

Ще одне явище, характерне для IP-телефонії - джиттер, або інакше випадкова затримка розповсюдження пакета.

Обумовлюється джиттер трьома факторами:

• Обмежена смуга пропускання або некоректна робота активних мережевих пристроїв;

• Висока затримка розповсюдження сигналу;

• Тепловий шум.

Метод боротьби з джиттером, що найчастіше застосовується - джиттер-буфер, що зберігає певну кількість пакетів. Обычно предусматривается динамическая подстройка длины буфера в течение всего времени существования соединения. Для выбора наилучшей длины используются эвристические алгоритмы [9].

Джиттер буфер

Для компенсації нерівномірної швидкості надходження пакетів на приймальній стороні створюють тимчасове сховище пакетів або так званий джиттер буфер. Його завдання, зібрати пакети, що надходять у правильному порядку відповідно до тимчасових міток і видати їх кодеку з правильними інтервалами і правильному порядку.

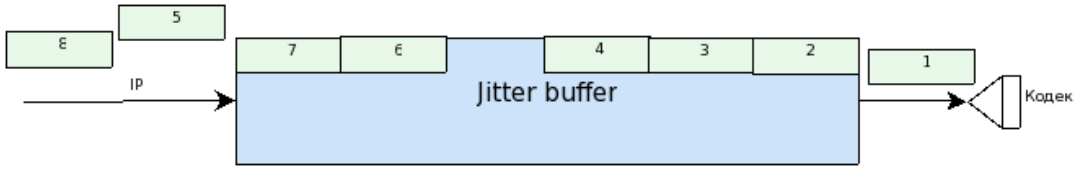

Рисунок 1.3 – Джиттер буфер

Розмір буфера приймальний VOIP пристрій розраховує в процесі роботи, або примусово задається в налаштуваннях. З одного боку, він не може бути занадто великим, щоб не збільшувати транспортну затримку. З іншого боку, невеликий розмір буфера викликає втрати пакетів при зміні часу затримки в IP мережі [9].

Звідси й походить одна з головних протиріч, між інтернет провайдерами та користувачами IP телефонії. З погляду провайдера всі пакети доставлені абоненту, тобто втрат немає. А з погляду VoIP пристрою, різниця у часі між приходом пакетів значно перевищує джиттер буфер. Тож фактично втрати є. Насправді втрата понад 1% викликає певні неприємні відчуття. При 2% розмова виявляється утрудненою. За значень більше 4% розмова вже практично неможлива [9].

Розмір джиттер буфера

Випадкова затримка поширення Ji для і пакету може визначатися за формулою:

$$J_i = J_{i-1} + \frac{|D_{i-1}| - J_{i-1}}{16},$$

де: Di – відхилення від очікуваного часу прибуття і пакету.

Відхилення від очікуваного часу прибуття і пакету Di визначається за формулою:

$$D_i = (R_i - R_{i-1}) - (S_i - S_{i-1}),$$

де:

R – час прибуття пакета у мітках часу RTP,

S – тимчасова мітка RTP, взята з пакета.

Розмір джиттер-буфера повинен бути більшим, ніж флуктуація транзитного часу в мережі (Флуктуація - будь-яке випадкове відхилення будь-якої величини). Наприклад, якщо для 10 пакетів час транзиту коливається від 5 до 10 мс, буфер повинен бути хоча б 8 мс, щоб жоден пакет не був втрачений. Краще якщо буфер ще більше, наприклад 12 мс, тоді зможе працювати механізм перезапиту втрачених пакетів [9].

2 АРХІТЕКТУРА І ПРОТОКОЛИ IP-ТЕЛЕФОНІЇ

2.1 Архітектура VoIP

Архітектура мережі VoIP може бути представлена у вигляді двох площин. Нижня відображає транспортний механізм негарантованої доставки мультимедійного трафіку як ієрархії протоколів RTP/UDP/IP, а верхня - механізм управління обслуговуванням викликів. Її ключовими протоколами є H.323 ITU-T, SIP, MGCP і MEGACO, що є різними реалізаціями обслуговування викликів у мережах IP-телефонії.

Транспортний протокол реального часу (Real-time Transport Protocol, RTP) надає транспортні послуги мультимедійних програм. Він не гарантує доставку та правильний порядок пакетів, але дозволяє програмам виявити втрату або порушення порядку прямування пакетів за рахунок присвоєння кожному з них номера. Протокол призначений для роботи в режимах передачі «крапка-крапка» або «крапка-множина точок» і не залежить від транспортного механізму. Однак як таке зазвичай використовується протокол UDP [1].

RTP працює спільно з протоколом керування реального часу (Real Time Control Protocol, RTCP), що забезпечує керування потоком даних та контроль перевантаження каналу. Учасники сеансу RTP періодично обмінюються пакетами RTCP зі статистичними даними (кількість надісланих пакетів, число втрачених тощо), які можуть бути використані відправником мультимедіа, наприклад, для динамічної корекції швидкості передачі і навіть зміни типу навантаження [1].

Серед мультимедійних стандартів найбільше освоєно стандарт H.323 ITU-T, до того ж він постійно вдосконалюється і має п'ять версій. Рекомендація H.323, історично перший спосіб здійснення дзвінків у мережі IP, передбачає такі види інформаційного обміну:

• «цифровізоване» аудіо;

• «цифровізоване» відео;

• дані (обмін файлами чи зображеннями);

• керування з'єднанням (обмін інформацією про підтримувані функції, керування логічними каналами тощо);

• керування встановленням та роз'єднанням з'єднань та сеансів зв'язку.

Основними елементами мережі стандарту H.323 є термінали (terminal), шлюзи (gateway), воротарі (gatekeeper) та пристрої керування конференціями (Multipoint Control Units, MCU).

Термінал забезпечує двосторонній зв'язок у реальному часі з іншим терміналом H.323, шлюзом або MCU.

Шлюзи встановлюють з'єднання між терміналами мережі H.323 та терміналами, що знаходяться в мережах, де використовуються інші протоколи. Головне завдання шлюзів полягає у взаємному перетворенні інформації між мережами різних протоколів (наприклад, IP та ТФОП).

Брамники беруть участь в управлінні з'єднанням, відповідаючи за взаємне перетворення телефонних номерів та IP-адрес.

Ще один елемент мережі H.323, званий proxy-сервером (тобто посередником), працює на прикладному рівні, він визначає тип програми та виконує потрібне з'єднання [4].

Площина обслуговування викликів стандарту H.323 включає три основні протоколи (див. Рисунок 2.1): протокол взаємодії кінцевого обладнання з воротарем RAS (Registration, Admission and Status), протокол управління з'єднаннями H.225 та протокол управління логічними каналами H.245. Для передачі сигнальних повідомлень RAS використовується протокол UDP, а передачі сигнальних повідомлень H.225 і H.245 - протокол TCP з гарантованою доставкою інформації. UDP не забезпечує гарантованої доставки інформації, тому якщо підтвердження не було отримано у встановлений час, повідомлення передається повторно.

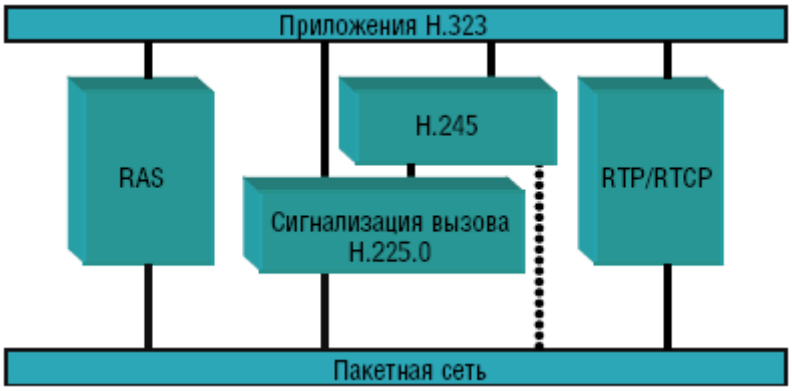

Рисунок 2.1 – Основні протоколи

Процес встановлення з'єднання складається із трьох етапів. У першому вирішуються завдання виявлення воротаря, реєстрації воротарем терміналів, контролю доступу терміналів до мережевих ресурсів, навіщо залучається протокол RAS. На двох наступних етапах виконуються процеси сигналізації H.225 та обмін керуючими повідомленнями H.245 [4].

2.2 Стек протоколів H.323

Стандарт H.323 ґрунтується на чотирьох компонентах для організації відеоконференцій типу точка-точка або багатоточка:

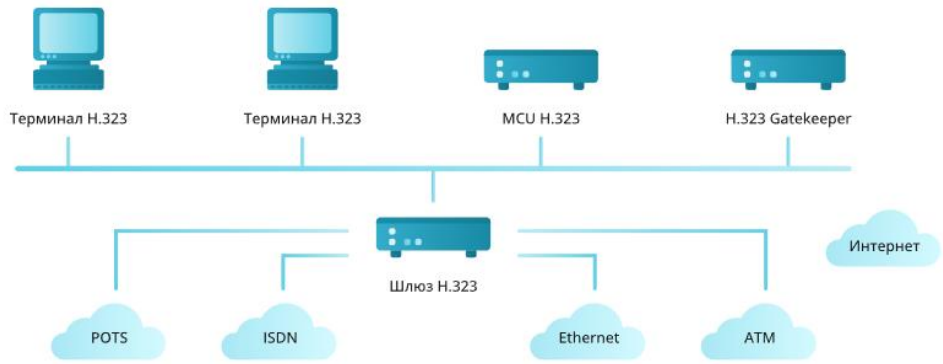

Рисунок 2.2 - Схема шлюзу H.323

- термінали
- шлюзи
- контролери зони (брамник)
- сервер багатоточкових конференцій (MCU)

Термінал - це інструмент для управління H.323-пристроєм, такий собі інтерфейс, кінцева точка. Термінали можуть зв'язуватися один з одним у режимі VoIP-телефонії або відеоконференц-зв'язку. Для зв'язку терміналів із різних мереж — наприклад, H.323 та ISDN, використовуються шлюзи. Вони виконують такі функції:

• встановлення з'єднання між терміналами;

• конвертація звукових форматів;

• обмін інформацією.

• якщо термінали знаходяться в одній мережі H.323, шлюзи не використовуються.

Контролер зони або гейткіпер - це центральна точка H.323-мережі, оскільки саме гейткіпер відповідає за адресацію викликів, керує шириною смуги пропускання та встановлює справжність терміналів та шлюзів під час з'єднання. Хоча рекомендація H.323 не визначає воротар як обов'язковий елемент, все ж таки без нього неможливе використання безлічі сучасних функцій, які впроваджують у свої рішення виробники VoIP-додатків та рішень відеоконференцзв'язку.

Для зв'язку трьох і більше терміналів використовують сервер багатоточкових конференцій MCU (Multipoint Control Unit). Усі термінали, які беруть участь у конференції, спочатку зв'язуються з MCU-сервером, а MCU у свою чергу розподіляє відеопотоки по всіх терміналах. Сам пристрій MCU зазвичай також поєднує в собі ролі гейткіпера та шлюзу.

Кожен H.323-термінал або пристрій, що підтримує протокол H.323, має власну IP-адресу. По ньому здійснюється механізм маршрутизації H.323-пакетів усередині мережі. Для зв'язку терміналів зі шлюзами та гейткіпером, а також для передачі медіатрафіку використовуються протоколи UDP. Транспортні протоколи TCP використовуються лише для встановлення дзвінка між терміналами та обміну додатковими можливостями [1].

Передача медіаданих за рекомендацією H.323 поділена на п'ять основних етапів:

• виявлення гейткіпера та реєстрація на ньому;

• встановлення з'єднання між двома та більше терміналами;

• обмін голосом та відео – передача за допомогою транспортних протоколів;

• обмін мультимедіа – передача різних графічних чи текстових документів, спільна робота над ними;

• завершення дзвінка.

Процес виявлення потрібен для того, щоб кінцеві точки (термінали) могли знайти воротар за мережевою адресою та зареєструватися на ньому. Ця процедура може виконуватися автоматично (багатоадресне розсилання - обмін повідомленнями між кінцевими точками і гейткіпером, якщо гейткіперів кілька, термінал самостійно вибирає, на якому йому реєструватися) або вручну (коли мережна адреса гейткіпера відома заздалегідь при конфігурації пристрою). Переважно перший варіант виявлення гейткіпера, оскільки у разі будь-яких несправностей у роботі термінал (кінцева точка) зможе автоматично переключитися на інший гейткипер, без втручання в конфігурацію.

Процедура реєстрації необхідна для того, щоб кінцеві точки (термінали) могли повідомити свої адреси гейткиперу та увійти до його зони управління.

Для встановлення з'єднання між терміналами та для обміну медіатрафіком використовуються такі протоколи:

Рисунок 2.3 – Протоколи з'єднання для обміну медіа-трафіком

TCP:

• H.225 — встановлення з'єднання між пристроями H.323.

• H.245 — обмін інформацією про можливості (наприклад, кодеки, що підтримуються). Один термінал "повідомляє" іншому терміналу про підтримувані можливості (кодеки), і вибирає кодек для відправлення з можливостей іншого терміналу.

UDP:

• RAS – використовується між терміналами, шлюзами та гейткіпером. Відповідає за реєстрацію, дозвіл на дзвінки та статуси.

• RTP — використовується при передачі медіа-трафіку в реальному часі.

Для завершення з'єднання термінали посилають повідомлення гейткиперу, після чого канал закривається і переривається зв'язок [6].

2.3 Протокол SIP

Застосування сучасних технологій дозволяє покращити якість та зменшити витрати на телефонний зв'язок. Телефонія із застосуванням SIP протоколу стає все більш затребуваною. Використання стандарту значно розширює можливості користувачів телефонної мережі. Ці технології застосовуються в організаціях у багатьох країнах. З їхньою допомогою організують зв'язок між клієнтами та співробітниками компанії, а також оперативну взаємодію між підрозділами.

SIP (Session Initiation Protocol) – протокол ініціації сеансу. Протокол SIP – це технологія, що дозволяє абонентам телефонної мережі розмовляти один з одним, обмінюватися мультимедійною інформацією, здійснювати відеодзвінки, надсилати повідомлення. Передача інформації проводиться за допомогою IP (Internet Protocol).

SIP працює разом із іншими прикладними протоколами.

• SDP (Session Description Protocol) – для обміну даними;

• RTP (Real-time Transport Protocol) – для забезпечення голосового зв'язку;

• TLS (Transport Layer Security) – для шифрування даних, що передаються.

За принципом дії SIP схожий на стандарт HTTP, який використовується для надсилання повідомлень електронною поштою та інтернет-додатків.

Підтримка протоколу SIP дозволяє виконувати такі завдання:

• передача голосової інформації;

• надсилання та прийом мультимедійних даних;

• організація конференц-зв'язку;

• утримання виклику.

Завдяки гнучкості протоколу його можливості можуть бути розширені в залежності від вимог до організації зв'язку. Використання технології SIP дозволяє уникнути обмежень, пов'язаних із застосуванням файрволів.

В основу технології покладено такі принципи:

• Мобільність користувачів. Кожен абонент мережі може безперешкодно переміщатися у зоні її дії. Всі користувачі мають унікальний ідентифікаційний номер, за допомогою якого система визначає їхнє розташування.

• Можливість масштабування. АТС, що використовують SIP протокол, будуються за серверним принципом. Це дозволяє збільшувати кількість елементів мережі за її збільшення.

• Розширюваність. Стандарт можна доповнити новими функціями після появи додаткових послуг. Крім того, система може бути адаптована до різних програм. Розширення можна виконати за допомогою нових заголовків для повідомлень. Сервер обробляє ті повідомлення, дані яких може розпізнати. Іншу інформацію система ігнорує [6].

Все частіше телефонні системи на основі технології SIP використовуються замість традиційної телефонії. Їх переваги:

• Вартість встановлення та підключення обладнання нижча, ніж для реалізації аналогової АТС.

• Користувачі отримують багатоканальний телефонний номер, який ніколи не буває зайнятий (за достатньої чисельності персоналу).

• Кількість абонентів можна збільшити без значних витрат.

• Встановлення та налаштування обладнання виконується швидко та легко.

• Тариф не залежить від локації абонентів. Це робить вигідним використання телефонії в організаціях, які мають філії у різних регіонах. Обмеження щодо географічного розташування абонентів відсутні.

• Можливість відстеження дзвінків та ведення відповідної статистики. Це дає можливість оптимізації роботи персоналу підвищення лояльності клієнтів.

• Широкий функціонал системи дозволяє ставити дзвінки у чергу, записувати розмови, налаштовувати форму зворотного дзвінка тощо.

• На основі СІП може бути створений віддалений кол центр. Це дозволить заощадити на оренді приміщення та наймати на роботу співробітників із різних міст.

• Віртуальна АТС настроюється залежно від графіка роботи організації. Наприклад, у неробочий час можна переадресувати дзвінки на мобільні пристрої співробітників.

2.4 IP-телефонія на платформі Asterisk

IP АТС Asterisk на сьогодні – найкраще рішення для організації офісної телефонії та недорогого call-центру. Це програмний продукт класу Open Source - вільне програмне забезпечення з відкритим кодом. За рахунок унікального поєднання багатьох функцій Asterisk займає лідируючі позиції серед платформ для створення офісної телефонії. Важливу роль грає ціна. Вартість IP-телефонії офісу на платформі Asterisk в рази нижча за вартість рішень на традиційних IP АТС – Panasonic, Samsung та ін.

Апаратна частина

Asterisk підтримує будь-яке обладнання для Voice over IP (VoIP). Пристрої різних виробників VoIP обладнання можна підключати без особливих проблем.

Функціональні можливості

Asterisk має всі можливості класичної АТС, підтримує безліч VoIP протоколів і надає функції голосової пошти, конференцій, інтерактивного голосового меню (IVR), центру обробки викликів (постановка дзвінків у чергу та розподіл їх за агентами використовуючи різні алгоритми), запис CDR та інші функції. Asterisk не має обмежень за кількістю абонентів, каналів та функціональних можливостей.

Для створення власної функціональності можна скористатися мовою Asterisk для написання діалплану. На сьогоднішній день вже написано багато графічних веб-оболонок до Asterisk для зручності використання та легкості сприйняття [10].

Реалізація

1. Почнемо з того, що Asterisk встановлюється на Linux.

Перше питання – який варіант реалізації вибрати. Власне, головний вибір - "плоский" Asterisk, керований через командний інтерфейс (за допомогою командного рядка), або система "Asterisk" з Web-інтерфейсом.

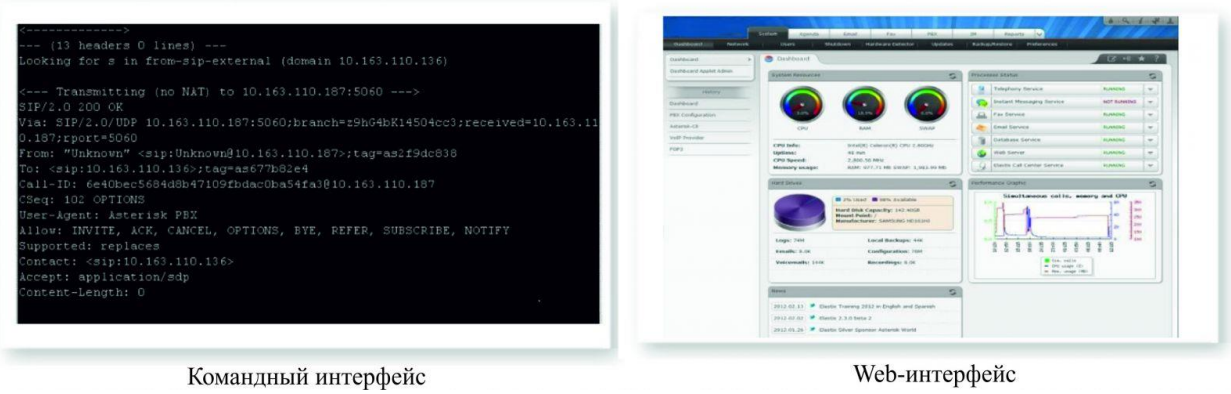

Рисунок 2.4 – Приклад інтерфейсів система Asterisk

Перший варіант передбачає більше гнучкості та ширші можливості, а другий – простішу налаштування та управління.

Для офісних завдань та завдань малого підприємства реалізація складної логіки не є важливою. Тому тут орієнтуємось на побудову простішої системи, призначеної для обслуговування до 100 внутрішніх телефонів при багатоканальних вхідних лініях від одного або кількох телефонних операторів.

Друге питання, яке треба вирішити – яку платформу вибрати для використання Asterisk. Варіантів два: локальний сервер чи «хмара»?

Локальний сервер для IP-АТС в сучасних умовах може обійтися майже безкоштовно: припустимо є старі (або не дуже старі) комп'ютери. Потрібно всього: 2 GB ОЗУ та один процесор (можна навіть якийсь старий і не дуже потужний) [10].

Віртуальна АТС

Рисунок 2.5 – Схема віртуальної АТС

Очевидний плюс хмар – за надійність роботи відповідає хмарний провайдер і не треба витрачати гроші на сервер. Щомісячна плата за віртуальний "сервер" з одного ядра та 2 GB ОЗУ буде не високою. Також

можна використовувати хмарну АТС (експлуатація віртуального сервера та хмарна АТС має незначну різницю) [10].

IP-АТС із використанням сервера

Рисунок 2.6 – Схема организации фелефонии на базе Asterisk

У разі використання "свого" сервера (розташованого всередині мережі) картина буде іншою.

Свій сервер:

- мінімізує «площу атаки» (оскільки скорочує кількість відкритих портів);

- дозволяє унеможливити саму можливість прослухати (перехопити) переговори внутрішніх абонентів або підключитися сторонньому абоненту від імені внутрішнього, навіть якщо є віддалені офіси (оскільки внутрішні абоненти розмовляють між собою, не виходячи у «зовнішню мережу»);

- дозволяє використовувати кількох операторів зв'язку або перемикатися на іншого оператора (який має більш «цікаві» тарифи) у будь-який момент, не налаштовуючи заново АТС.

Якщо вибраний телефонний провайдер з'єднується через SIP, це викликає мінімум витрат і мінімум технічних проблем [10].

3. Далі потрібно підключити IP-телефони або використовувати "софтфони". Використання телефонних апаратів, звичайно, найкращий варіант. У них завжди гарна якість звуку та велика кількість різноманітних функцій. При цьому від марки та моделі залежить зручність використання та ціна, але основні якості з погляду телефонії відрізнятимуться не сильно. «Софтфони» – це програми, які дозволяють використовувати ваш комп'ютер як телефон, потрібні лише навушники та мікрофон.

4. Готове рішення: IP-АТС Asterisk із графічним веб-інтерфейсом на своєму сервері.

Розглянемо варіант організації IP-телефонії в офісі з використанням IP-АТС Asterisk і свого сервера [10].

Рисунок 2.7 – IP-ATC Asterisk з графічним веб-інтерфейсом

Основні можливості IP-ATC Asterisk:

IVR (віртуальний секретар),

• голосова пошта та пересилання на е-мейл,

• запис телефонних розмов,

• можливість працювати з кількома операторами зв'язку,

• підтримка відео дзвінків та конференцій,

• наявність модуля факс-сервера,

Додаткові можливості: реалізація корпоративної пошти та чат.

3 АНАЛІЗ МЕТОДІВ РЕАЛІЗАЦІЇ СЕРВЕРА IP-ТЕЛЕФОНІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ

3.1. Традиційні канальні IP-ATC

IP-ATC (Private Branch Exchange) – це приватний телефонний комутатор, що дозволяє власнику (яким може бути організація або будь-який інший тип) виступати як міні-провайдер послуг для своїх користувачів, водночас зазвичай

надаючи безліч додаткових функцій, таких як виклик переклад, очікування виклику, IVR (інтерактивна голосова відповідь), черги, звіти та багато іншого. Оскільки організація є власником УВАТС, з неї не стягується плата за внутрішні виклики (дзвінки між додатковими номерами, які обидва зареєстровані на УВАТС), хоча, залежно від типу послуги, вона може стягувати плату за такі дзвінки (наприклад, у випадку бізнес-центру , що надає послуги телефонії орендарям) [5].

Телефонні трубки у будь-якому бізнесі чи іншій організації майже ніколи не підключаються безпосередньо до PSTN (телефонної мережі загального користування), а скоріше до місцевої УВАТС, яка забезпечує її гудком та всіма її функціями [5].

Зазвичай, АТС (або IP-АТС) має набір функцій, які дозволяють користувачам максимально ефективно використовувати свої телефонні дзвінки. Ці функції відрізняються в залежності від моделі УВАТС, але деякі з них є загальними:

- Очікування виклику
- Утримання виклику
- Переклад виклику
- Паркування викликів
- Пейджинг
- Запис дзвінків
- Голосова пошта
- IVR (інтерактивна голосова відповідь)
- Підписуйтесь на мене
- Переадресація дзвінка
- Присутність

Переваги систем IP-АТС полягають у тому, що вони ґрунтуються на програмному забезпеченні та використовують звичайні комп'ютерні мережі. Найбезпосереднішою перевагою, яка спадає на думку, є той факт, що при використанні IP-АТС більше не потрібно мати виділену голосову мережу, як це потрібно було б для застарілої АТС, а замість цього використовувати єдину мережу як для голосу, так і для даних. При цьому багато організацій воліють розділяти мережі передачі голосу та даних з міркувань безпеки та забезпечення якості.

Інші переваги включають використання стандартних IP-телефонів (зазвичай SIP-телефонів), можливість створювати та використовувати віддалені та мобільні додаткові номери, підвищену гнучкість за рахунок інтеграції комп'ютерної телефонії, зниження вартості дзвінків, простоту додавання номерів DID (Direct Inbound Dialing), у тому числі кількість різних регіонів та країн та багато іншого [5].

3.2. Програмні IP-АТС

Програмну АТС можна охарактеризувати як програму (або програмний комплекс), яка емулює роботу традиційної АТС. Тут усе переведено в цифру: від комутації каналів до керування викликами.

Програма IP АТС може бути розгорнута на локальному сервері компанії. Для її роботи можуть використовуватися різні платформи. Як правило, розробники пропонують програмні IP АТС для різних дистрибутивів Linux, BSD, Windows. Деякі розробляють програмне забезпечення для розгортання корпоративних автоматичних телефонних станцій для операційної системи OS X. Зв'язок забезпечується при підключенні до будь-якого провайдера IP-телефонії, з використанням його каналів та інфраструктури.

Другий варіант розгортання – на потужностях провайдера, що надає послуги IP-телефонії. Така схема доступна, наприклад, користувачів віртуальної АТС. Доступ до автоматизованої телефонної станції у разі здійснюється через WEB-интерфейс. При використанні такої схеми для компанії-користувача немає потреби у виділенні фахівців для забезпечення працездатності та підтримки системи. Всім займається провайдер. Необхідність у якомусь додатковому апаратному забезпеченні під час використання цієї схеми відсутня. Загалом потрібен лише доступ до інтернету, щоб керувати своєю корпоративною АТС через WEB-інтерфейс [6].

Можливості та переваги програмних АТС для IP телефонії:

• Швидкий запуск. Стосується це переважно варіанта, коли АТС розгортається на потужностях провайдера з доступом через web-інтерфейс.

• Дешевші тарифи на IP-телефонію, ніж на звичний зв'язок. Економії вдається досягти за рахунок безлічі факторів, головний з яких – можливість

забезпечити безкоштовне спілкування між абонентами всередині корпоративної мережі, що обслуговується програмною АТС.

• Величезна кількість функцій та інструментів, доступних для користувачів IP-телефонії та програмних АТС.

Функціонал та можливості програмних АТС:

Голосове меню (IVR)

Функція дозволяє автоматизувати спілкування з телефонуючими та мінімізувати залучення до цього процесу «живих» фахівців

Конференц зв'язок

Завдяки тому, що при організації зв'язку за допомогою IP-телефонії через програмні АТС використовується інтернет, бізнес отримує можливість організовувати різні типи онлайн-конференцій: аудіоконференції та відеоконференції.

Інтеграція з різними сторонніми сервісами та ПЗ

Програмна АТС може інтегруватися з різними сторонніми рішеннями (чого не можна сказати про «традиційні» автоматизовані телефонні станції). Серед них:

• CRM системи.

• Рішення для автоматизації документообігу.

• Складське ПЗ.

• Програми для роботи з різними типами реклами.

Програмна АТС може обслуговувати різні абонентські пристрої. Це:

• Звичайні, традиційні телефони.

• IP-телефони. Підключаються до програмних АТС без будь-яких пристроїв-«посередників».

• Комп'ютери, планшети та інші пристрої.

• Мобільні телефони.

3.3 IP-АТС базі Asterisk

IP телефонія та системи автоматизації можуть бути пов'язані в одну єдину систему, що дозволяє автоматизувати систему управління відносинами з клієнтами та створити ефективне середовище для телефонного обслуговування клієнтів. Asterisk – платформа IP телефонії з відкритим вихідним кодом, що надає різні функції керування дзвінками. Це дає нам можливість зробити

установку та налаштування Asterisk локально (на сервері клієнта) або у хмарі з подальшою підтримкою.

Головними перевагами програмної АТС Asterisk є гнучкість та безпека. Маючи відкритий вихідний код, Asterisk є модульною комунікаційною платформою, робота якої залежить від телефонних і IP-мереж. На базі рішень Asterisk можна створити гнучку мультифункціональну офісну міні-АТС, вузол зв'язку або call-центр.

Рішення на базі Asterisk дозволяють реалізовувати всі функції традиційної АТС, включаючи при цьому великий набір додаткових сервісних функцій. Asterisk має практично необмежені можливості масштабування і дозволяє побудувати рішення різного рівня для абсолютно різних завдань та адаптувати їх під специфічні вимоги клієнтів. Можливість налаштування та реалізації власних алгоритмів викликів – безперечна перевага IP-АТС Asterisk.

Простота та зручність створення телефонії на базі Asterisk також дозволяють використовувати наявні дроти Ethernet, що дозволяє побудувати корпоративну телефонію на базі існуючої мережі компанії.

До Asterisk можна підключити будь-яку кількість IP-телефонів, а кількість телефонних портів не є обмеженою - тобто. при зміні масштабів мережі не потрібно замінити обладнання (що характерно для традиційних АТС). Підключення нових співробітників до комунікаційної мережі не вимагатиме додаткових витрат, окрім нових апаратів [5].

3.4 Віртуальні IP-А АТС

Віртуальна АТС для офісу дозволяє забезпечити безперебійну комунікацію всередині компанії між філіями, для інформування клієнтів, проведення маркетингових досліджень та аналітики.

Віртуальна або хмарна АТС або VPBX – відмінна альтернатива окремому кол-центру або фізичній офісній міні-АТС. Під час замовлення послуги підприємство отримує в повноцінне користування IP-АТС, яка фактично розміщена у постачальника електронних комунікаційних послуг у захищеному дата-центрі, що забезпечує стабільний сигнал за допомогою Інтернету, мобільної чи локальної мережі. При цьому не потрібно купувати дороге обладнання – офісну АТС, яка потребує спеціального технічного

обслуговування. Клієнту потрібно лише підключити абонентський пристрій для співробітників (IP-телефон, персональний комп'ютер або смартфон із програмним SIP-клієнтом, шлюз для аналогових телефонів, звичайний мобільний телефон для FMC-ліній) [12].

Перевагами віртуальної АТС є:

• багатоканальність - невичерпний обсяг вхідних та вихідних ліній;

• відсутність функції «зайнято» для абонентів, що означає зниження кількості незадоволених клієнтів до нуля;

• функція утримання клієнта на лінії з повідомленням про час очікування;

• розподіл вхідних викликів за пріоритетністю чи специфікацією;

• запис розмов (вибірковий або повний);

• детальна звітність у зручному форматі та онлайн-контроль;

• можливість обмеження трафіку для операторів.

4. ІНФОРМАЦІЙНА БЕЗПЕКА IP-ТЕЛЕФОНІЇ

4.1 Типи загроз в мережах IP-телефонії

Існує кілька основних типів загроз, що становлять найбільшу небезпеку в мережах IP-телефонії:

1. Підміна даних про користувача

Підміна даних користувача означає, що один користувач мережі видає себе за іншого. У зв'язку з цим виникає можливість несанкціонованого доступу до важливих функцій системи. Використання механізмів автентифікації та авторизації в мережі підвищує впевненість у тому, що користувач, з яким встановлюється зв'язок, не є підставною особою та що їй можна надати санкціонований доступ [13].

2. Підслуховування

Під час передачі даних про користувачів (ідентифікаторів користувача та паролів) або приватних конфіденційних даних незахищеними каналами ці дані можна підслухати і згодом зловживати ними. Методи шифрування даних знижують ймовірність цієї загрози.

3. Маніпулювання даними

Дані, що передаються каналами зв'язку, в принципі можна змінити. Багато методах шифрування використовується технологія захисту цілісності даних, що запобігає їх несанкціоноване зміна.

4. Відмова від обслуговування (Denial of Service, DoS)

Відмова від обслуговування (DoS) є різновидом атаки хакерів, в результаті якої важливі системи стають недоступними. Це досягається шляхом переповнення системи непотрібним трафіком, на обробку якого йдуть усі ресурси системної пам'яті та процесора. Система зв'язку повинна мати засоби для розпізнавання подібних атак та обмеження їхнього впливу на мережу [13].

Базовими елементами в галузі безпеки є автентифікація, цілісність та активна перевірка:

• Автентифікація покликана запобігти загрозі знеособлення та несанкціонованого доступу до ресурсів та даних.

• Цілісність забезпечує захист від підслуховування та маніпулювання даними, підтримуючи конфіденційність та незмінність інформації, що передається.

• Активна перевірка означає перевірку правильності реалізації елементів технології безпеки та допомагає виявляти несанкціоноване проникнення в мережу та атаки типу DoS.

4.2 Методи криптографічного захисту інформації

Основою будь-якого захищеного зв'язку є криптографія. Криптографією називається технологія складання та розшифрування закодованих повідомлень. Крім того, криптографія є важливою складовою для механізмів автентифікації, цілісності та конфіденційності. Аутентифікація є засобом підтвердження особи відправника чи одержувача інформації. Цілісність означає, що дані не були змінені, а конфіденційність створює ситуацію, за якої дані не може зрозуміти ніхто, крім їх відправника та одержувача. Зазвичай криптографічні механізми існують як алгоритму (математичної функції) і секретної величини (ключа). Алгоритми широко відомі, у секреті необхідно тримати лише криптографічні ключі. Причому чим більше бітів у такому ключі, тим менш він уразливий [13].

У системах забезпечення безпеки використовуються три основні криптографічні методи:

- симетричне шифрування;
- асиметричне шифрування;
- односторонні хеш-функції.

Усі існуючі технології аутентифікації, цілісності та конфіденційності створені на основі саме цих трьох методів. Наприклад, цифрові підписи можна подати у вигляді поєднання асиметричного шифрування з алгоритмом односторонньої хеш-функції для підтримки автентифікації та цілісності даних [13].

Симетричне шифрування, яке часто називають шифруванням за допомогою секретних ключів, переважно використовується для забезпечення конфіденційності даних. При цьому два користувача повинні спільно вибрати єдиний математичний алгоритм, який використовуватиметься для шифрування та розшифрування даних. Крім того, їм потрібно вибрати спільний ключ (секретний ключ), який використовуватиметься з прийнятим ними алгоритмом шифрування/розшифрування.

Шифрування за допомогою секретного ключа найчастіше використовується для підтримки конфіденційності даних та дуже ефективно реалізується за допомогою незмінних «вшитих» програм (firmware). Цей метод можна використовувати для автентифікації та підтримки цілісності даних, але метод цифрового підпису є більш ефективним [13].

Метод секретних ключів має такі недоліки:

• необхідно часто змінювати секретні ключі, оскільки завжди існує ризик їхнього випадкового розкриття;

• важко забезпечити безпечне генерування та розповсюдження секретних ключів.

Асиметричне шифрування часто називають шифруванням за допомогою загального ключа, при якому використовуються різні, але взаємно доповнюють один одного ключі та алгоритми шифрування та розшифрування. Цей механізм покладається на два взаємопов'язані ключі: загальний ключ і приватний ключ.

Найбільш типові приклади функцій за використання алгоритмів загальних ключів:

• забезпечення конфіденційності даних;

• автентифікація відправника;

• безпечне отримання спільних ключів для спільного використання.

Важливим аспектом асиметричного шифрування є те, що приватний ключ повинен зберігатися в таємниці. Якщо приватний ключ буде розкритий, то людина, яка знає цей ключ, зможе виступати від вашого імені, отримувати ваші повідомлення та надсилати повідомлення так, ніби це зробили ви.

Алгоритми шифрування за допомогою загальних ключів рідко використовуються для підтримки конфіденційності даних через обмеження продуктивності. Натомість їх часто використовують у додатках, де аутентифікація проводиться за допомогою цифрового підпису та керування ключами [13].

Безпечною хеш-функцією називається функція, яку легко розрахувати, але зворотне відновлення якої потребує непропорційно великих зусиль. Вхідне повідомлення пропускається через математичну функцію (хеш-функцію), і в результаті на виході отримують певну послідовність бітів. Ця послідовність називається "хеш" (або "результат обробки повідомлення"). Цей процес неможливо відновити.

Хеш функція приймає повідомлення будь-якої довжини і видає на виході хеш фіксованої довжини. Звичайні хеш-функції включають:

• алгоритм Message Digest 4 (MD4);

• алгоритм Message Digest 5 (MD5);

• Алгоритм безпечного хеша (Secure Hash Algorithm, SHA).

Технологія шифрування часто використовується у програмах, пов'язаних з керуванням ключами та автентифікацією. Аутентифікація в цьому випадку досягається за допомогою цифрового підпису.

Цифровий підпис є зашифрованим хешом, який додається до документа. Вона може використовуватися для автентифікації відправника та цілісності документа. Цифрові підписи можна створювати за допомогою поєднання хеш-функцій та криптографії спільних ключів.

Цифровим сертифікатом називається повідомлення з цифровим підписом, яке нині зазвичай використовується підтвердження дійсності загального ключа. Цифровий сертифікат у стандартному форматі X.509 включає такі елементи:

- номер версії;
- серійний номер сертифіката;
- емітент інформації про алгоритм;
- емітент сертифікату;
- дати початку та закінчення дії сертифіката;
- інформація про алгоритм загального ключа суб'єкта сертифікату;
- підпис емітуючої організації.

4.3 Технології аутентифікації

Під аутентифікацією розуміється визначення користувача або кінцевого пристрою (клієнта, сервера, комутатора, маршрутизатора, міжмережевого екрану і т.д.) та його розташування в мережі з подальшою авторизацією користувачів та кінцевих пристроїв. Найпростішим способом аутентифікації є використання паролів, але для підтримки високого рівня безпеки паролі часто доводиться змінювати. Методи використання одноразових паролів використовуються, як і раніше, широко. Механізм аутентифікації за протоколом "від точки до точки" Point-to-Point Protocol (PPP) часто застосовується в середовищі модемного доступу і включає використання наступних протоколів: аутентифікації пароля (Password Authentication Protocol, PAP), взаємодії викликів (Challenge Handshake Protocol, CHAP) та гнучкої аутентифікації (Extensible Authentication Protocol, EAP) [14].

Протокол PPP

Аутентифікація на основі протоколу Point-to-Point Protocol (PPP) – це популярний засіб інкапсуляції (упаковки), який часто використовується у глобальних мережах. До його складу входять три основні компоненти:

• метод інкапсуляції дейтаграм у послідовних каналах;

• протокол керування зв'язком (Link Control Protocol, LCP), який використовується для встановлення, конфігурування та тестування зв'язку;

• сімейство протоколів керування мережею (Network Control Protocols, NCP) для встановлення та конфігурування різних протоколів мережного рівня.

Щоб встановити прямий зв'язок між двома точками каналу PPP, кожна з цих точок повинна спочатку відправити пакети LCP для конфігурування зв'язку на етапі її встановлення. Після встановлення зв'язку та перш ніж перейти до етапу роботи на протоколах мережного рівня, протокол PPP надає (за потреби) можливість проведення аутентифікації.

Протокол TACACS

TACACS – це простий протокол керування доступом, що базується на стандартах User Datagram Protocol (UDP) та розроблених компанією Bolt, Beranek and Newman, Inc. (BBN). Компанія Cisco кілька разів удосконалювала та розширювала протокол TACACS, і в результаті з'явилася її власна версія TACACS, відома як TACACS+ [14].

Протокол TACACS+ працює за технологією клієнт-сервер, де клієнтом TACACS+ зазвичай є сервер доступу NetWare (NetWare Access Server, NAS), а сервером TACACS+, як правило, вважається демон (процес, що запускається на машині UNIX або NT). Фундаментальним структурним компонентом протоколу TACACS+ є поділ автентифікації, авторизації та обліку (Authentication, Authorization, Accounting, AAA). Це дозволяє обмінюватися ідентифікаційними повідомленнями будь-якої довжини та змісту, і, отже, використовувати клієнтам TACACS+ будь-який ідентифікаційний механізм, зокрема PPP PAP, PPP CHAP, апаратні карти і Kerberos. Аутентифікація не є обов'язковою. Вона сприймається як опція, яка конфігурується дома. У деяких місцях вона взагалі не потрібна, в інших місцях вона може застосовуватись лише для обмеженого набору послуг [14].

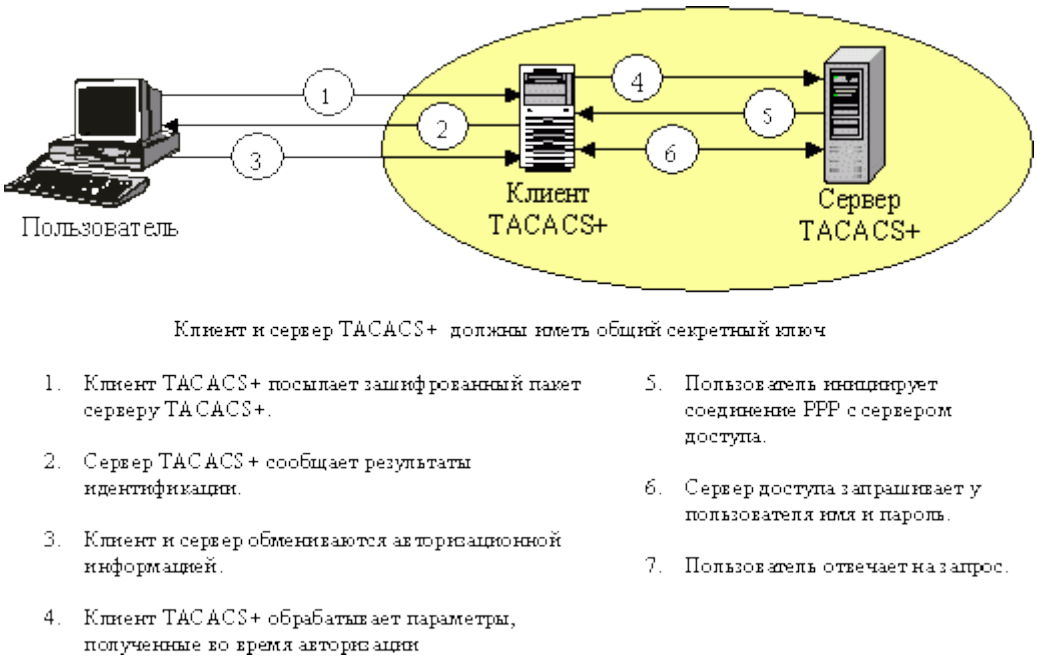

Рисунок 4.1 - Взаємодія між користувачем та системою TACACS+

Авторизація - це процес визначення дій, які дозволені даному користувачеві. Зазвичай автентифікація передує авторизації, проте це необов'язково. Протокол TACACS+ допускає лише позитивну чи негативну авторизацію.

Облік зазвичай слідує за автентифікацією та авторизацією. Облік, є записом дій користувача. У системі TACACS+ облік може виконувати два завдання. По-перше, може використовуватися обліку використаних послуг (наприклад, виставлення рахунків). По-друге, його можна використовувати з метою безпеки. Для цього TACACS+ підтримує три типи облікових записів. Записи «старт» вказують, що послуга має бути запущена. Записи «стоп» свідчать, що послуга щойно закінчилася. Записи "оновлення" (update) є проміжними і вказують на те, що послуга все ще надається. Облікові записи TACACS+ містять всю інформацію, яка використовується під час авторизації, а також інші дані: час початку та закінчення (якщо це необхідно) та дані про використання ресурсів.

Протокол RADIUS

Протокол RADIUS був розроблений Livingston Enterprises, Inc. як протокол аутентифікації серверного доступу та обліку. В даний час

специфікація RADIUS (RFC 2058) та стандарт обліку RADIUS (RFC 2059) запропоновані для затвердження як загальноприйняті стандарти IETF.

Зв'язок між NAS (Network Attached Storage) та сервером RADIUS заснований на протоколі UDP. Загалом вважається, що протокол RADIUS не має відношення до підключення. Всі питання, пов'язані з доступністю сервера, повторною передачею даних та відключеннями після закінчення очікування, контролюються пристроями, що працюють під керуванням протоколу RADIUS, але не самим протоколом передачі. Протокол RADIUS ґрунтується на технології клієнт-сервер (рис. 4.2) [14].

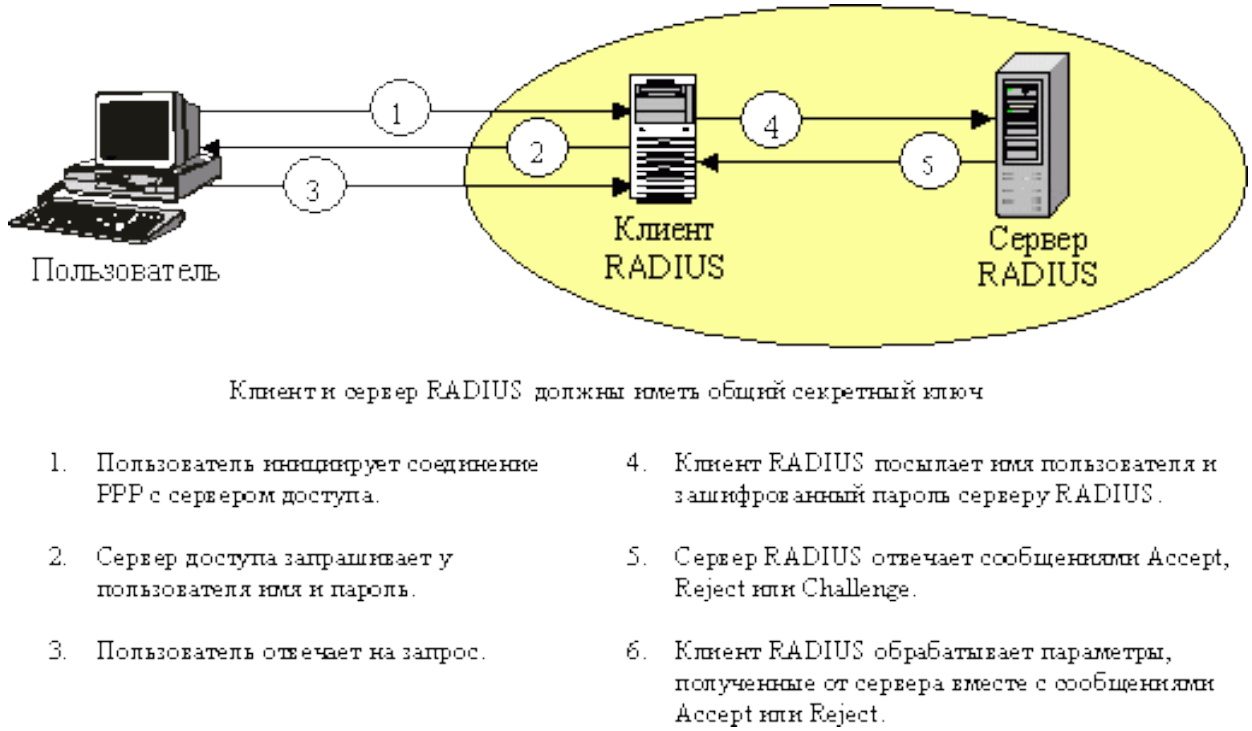

Рисунок 4.2 - Взаємодія між користувачем та системою RADIUS

Клієнтом протоколу RADIUS зазвичай є NAS, а сервером RADIUS вважається демон, що працює на машині UNIX або NT. Клієнт передає інформацію користувача на певні сервери RADIUS, а потім діє відповідно до отриманих від сервера інструкцій. Сервери RADIUS приймають запити користувачів на підключення, проводять ідентифікацію користувачів, а потім надсилають всю конфігураційну інформацію, яка потрібна клієнту для обслуговування користувача. Для інших серверів RADIUS або ідентифікаційних серверів інших типів сервер RADIUS може бути у ролі клієнта-посередника (proxy) [14].

4.4 Використання технології VoIP через VPN

Передача голосу по Інтернет-протоколу (також звана VoIP або передача голосу по IP) - це технологія, що забезпечує голосовий зв'язок через Інтернет шляхом перетворення вашого голосу на цифровий сигнал. Щоб скористатися послугою VoIP, вам знадобиться комп'ютер із підключенням до Інтернету або адаптер, спеціалізований телефон, смартфон або інший сумісний пристрій.

Віртуальна приватна мережа (VPN) — це метод, який забезпечує безпеку, конфіденційність та анонімність у приватній та загальнодоступній мережі, наприклад, в Інтернеті. За допомогою VPN ваші дії в Інтернеті практично неможливо відстежити стороннім, таким як хакери, ваш інтернет-провайдер та уряд [14].

VoIP VPN поєднує в собі передачу голосу по Інтернет-протоколу та технології віртуальної приватної мережі для створення безпечного та зашифрованого тунелю через Інтернет для доставки VOIP-трафіку.

VoIP перетворює аналоговий голосовий зв'язок на потік даних, який потім інкапсулюється і шифрується VPN. Потім голосовий зв'язок надсилається через VPN-тунель на інший кінець, де він декодується і перетворюється на аналоговий сигнал для доставки.

Безпека та анонімність – основні причини, з яких більшість людей прагнуть поєднати послугу VoIP з VPN, але вони не єдині. Багато країн блокують послуги VoIP, такі як Skype, за допомогою брандмауера. VPN розблокує послуги VoIP, щоб ви могли залишатися на зв'язку з колегами, членами сім'ї та друзями, де б ви не знаходилися [14].

Застосування VPN в технології VoIP дозволяє забезпечити:

1. Підвищення безпеки. Хакери можуть стежити за вами та отримувати конфіденційну інформацію, використовуючи відомі вразливості у службах VoIP.

2. Захищає від збереження даних. Шифрування вашого інтернет-з'єднання за допомогою VPN означає, що ваші розмови з VoIP будуть захищені від зловмисників, таких як хакери та інші особи, які відстежують ваші дії в Інтернеті. Шифрування захистить вас від аналізу трафіку та масового спостереження з боку комерційних організацій, урядів та хакерів.

3. Припинення регулювання. Якщо робиться багато викликів VoIP, є велика ймовірність, що інтернет-провайдер може обмежити вашу пропускну здатність через велике використання даних. Якщо ваша пропускна здатність обмежена, ви помітите погіршення якості голосу та зниження швидкості інтернету.

5 ВПРОВАДЖЕННЯ IP-ТЕЛЕФОНІЇ У КОРПОРАТИВНІЙ МЕРЕЖІ ПІДПРИЄМСТВА

5.1 Обгрунтування вибору IP-АТС для корпоративної мережі Підприємства

В данному розділі показано впровадження IP-телефонії у мережу підприємства яке починає маштабуватись. Розглянуто особлівості хмарних АТС, вібір шлюзів для IP-телефонії та вибір телефонів для підприємства.

Якщо маленька кампанія починае маштабуватись, то їй буде потрібно номер який не буде залежати від розміщення офісу або від кількості філіалів, які приймають дзвінки. Найкращим вибором для підприємства яке маштабується це віртуальна IP-АТС. У свою чергу вартість впровадження та експлуатації віртуальної АТС нижче. Крім цього, віртуальна АТС підтримує підключення практично необмеженої кількості номерів та абонентів, роботу з багатоканальними лініями та голосовим меню, гнучку переадресацію (у тому числі на мобільні номери телефонів), голосові вітання, інтеграцію з популярними CRM-системами та багато іншого [2].

5.2 Врахування особливостей хмарних АТС

Хмарна або віртуальна АТС на даний момент є одним із найбільш затребуваних рішень у сфері IP-телефонії, у тому числі завдяки можливості налаштовувати функціонал станції під вимоги та потреби конкретного бізнесу. Для передачі даних хмарної АТС використовують протоколи SIP (передача мультимедіа) і VoIP (голосовий зв'язок).

Відсутність необхідності придбання та монтажу громіздкого обладнання, прокладання кабелів та обслуговування апаратури, що власне і забезпечує суттєву економію [12].

Компанія отримує функціональну міні-АТС у свій офіс, причому:

• Вартість міжміського зв'язку знижується на 70%, а міжнародного – на 80%.

• Дзвінки всередині компанії безкоштовні.

• Якість зв'язку суттєво покращується.

Вся інформація АТС зберігається на сервері хмарного провайдера, що надає послугу. Саме він гарантує безпеку та конфіденційність даних.

5.3 Вібір шлюзу IP-телефонії

Мабуть, найважливіший момент – тип обладнання. Усього існує три види шлюзів:

• аналогові FXO/FXS, які підтримують від 2-х до 24-х ліній. Шлюз FXS служить для підключення стандартних дротових телефонів до АТС, а FXO – для приєднання до АТС міської телефонної лінії. Для великих фірм чим більше FXS-роз'ємів, тим краще. Використовувані протоколи – SIP, H.323 та MGCP. Перший вважатимуться універсальним;

• цифрові, що служать для підключення цифрових ліній BRI ISDN, PRI/E1, T1, які широко використовуються в Європі та Америці. Вони використовуються для підключення до АТС або у розрив між основною АТС обсягом від п'ятдесяти клієнтів та міської телефонної мережі без зміни налаштувань. Робота забезпечується за протоколами ISDN, SS7 та QSIG;

• GSM-шлюзи, які мають слоти для SIM, щоб підключити до АТС мобільні телефони.

Другий момент – сумісність. Перед покупкою шлюзу необхідно перевірити набір стандартів, що підтримуються. Для цього слід вивчити специфікації офісної АТС. Буває так, що АТС підтримує переклад виклику за методом RFC 3892, тоді як шлюз – за RFC 3515. Стандарт RFC, начебто, однаковий, але сумісності немає. SIP-телефонія не уніфікована, як багато хто вважає. Кожен виробник розробляє свої унікальні рішення.

Важливе значення має «залізо» устаткування. Якщо ви вирішите придбати бюджетну модель, її DSP-процесор може не справлятися з навантаженнями. Шлюз перетворює аналогові сигнали на цифрові в реальному часі, при піковому навантаженні процесора можливі луна і шум [12].

5.4 Вибір IP-телефонів

Ключовою характеристикою кожного IP-телефону є кількість ліній. Саме на цю характеристику варто звернути увагу перед покупкою оптимальної для Вашого офісу моделі. Ця характеристика відразу вказує на те, скільки буде доступно користувачеві телефонних ліній в той самий момент часу. Середньостатистичний офісний працівник зацікавлений у тому, щоб завжди

були 1 або 2 лінії, а ось співробітники, які використовують телефон, інтенсивніше зацікавлені в 5-ти і більше ліній [7].

Екран IP-телефону та яким він має бути?

Крім самого розміру діагоналі екрана в дисплей IP-телефону мають бути закладені інші функції. Більшість із них будуть дуже корисними для роботи. Сам дисплей може бути монохромним або кольоровим, а також мати підсвічування або взагалі бути сенсорним. На саму роздільну здатність дисплея також варто звернути увагу, адже це впливає на такі параметри, як чіткість зображення та на чіткість відображення тестових даних. Адже чим більше екран, тим простіше зчитувати інформацію з екрану.

IP-телефони Premium часто обладнані саме сенсорним дисплеєм. Такий дисплей суттєво спрощує процес налаштування та саме користування телефоном. Базовому користувачеві буде достатньо IP-телефону, який має маленький екран. А ось співробітникам, які потребують багатьох функцій телефону, потрібен дисплей якомога більшого розміру. Така характеристика підвищує ефективність роботи [7].

Які функції IP-телефонів потрібні користувачам?

Ряд функцій, які перші напрошуються під час вибору телефону, залежить від веб-сервісу та телефонної системи. Серед них переадресація виклику, утримання та очікування виклику та багато інших. Зручність використання вказаного функціоналу залежить від простоти та зрозумілості структурування меню.

Як підключається IP-телефон до мережі?

Наразі найбільш затребуваним способом живлення для IP-телефону є Power over Ethernet (PoE). Якщо ж Ви зупинили вибір на пристрої без PoE, тоді до покупки перевірте, чи входить до комплекту джерело живлення, чи можна купити його окремо.

При виборі телефону з підтримкою Gigabit переконайтеся, що на робочому місці є відповідний Ethernet-порт. В іншому випадку не буде доступу до особливих переваг підключення через Gigabit Ethernet.

5.5 Схема мережі підприємства IP-телефонією

В основі будь-якої схеми (мережі) IP-телефонії лежить мережний комутатор (Switch). Усі пристрої (вузли мережі) ip-телефони, шлюзи, ip-атс, персональні комп'ютери та ін. з'єднуються за допомогою цього комутатора.

Оскільки IP-телефонія накладає певні вимоги (Quality of service) на комп'ютерну (локальну) мережу, виділимо параметри мережного комутатора, на які варто звернути увагу, при проектуванні мережі ай пі телефонії:

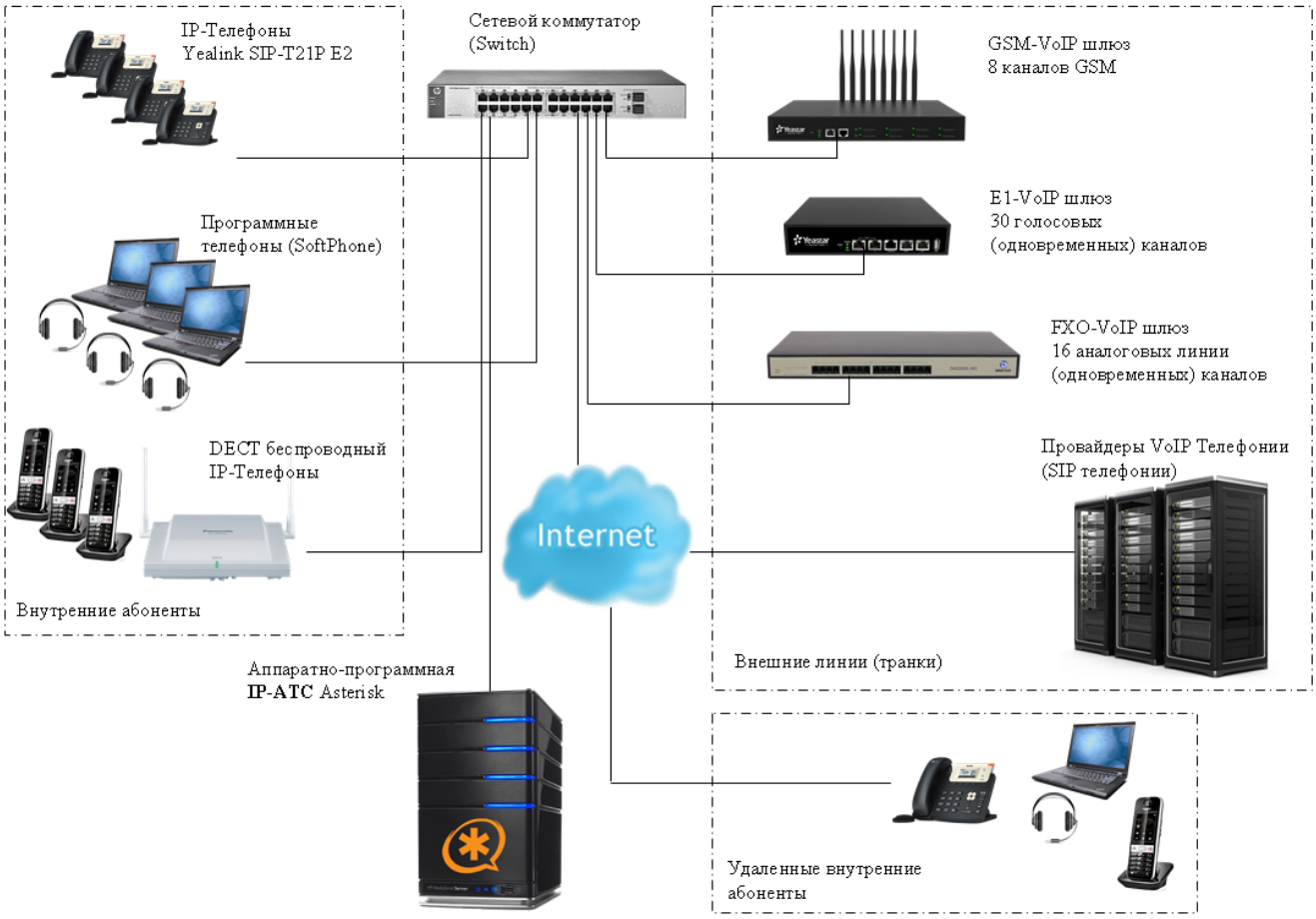

Рисунок 5.1 – Схема сети предприятия IP-телефонии

Один з головних показників продуктивності мережного комутатора, чим вище даний параметр тим кращий за Switch, для нової мережі варто розглядати значення від 52 Гбіт/с.

Кількість портів

Неважко зрозуміти, що кожному VoIP пристрою потрібен свій Ethernet порт, на практиці комутатор підбирається з великою кількістю портів на перспективу розвитку та розширення компанії.

PoE (Power over Ethernet)

Технологія, що дозволяє передавати віддаленому пристрою електричну енергію разом з даними через стандартну кручену пару в мережі Ethernet. За допомогою даної технології вирішується питання централізованого живлення всіх IP-телефонів від єдиного безперебійного джерела живлення. Тим самим реалізується безвідмовність роботи системи IP телефонії [7].

Vlan (Virtual Local Area Network)

Спосіб логічного поділу сегментів мережі між собою на одній фізичній мережі. Подібні установки застосовують для високої безпеки внутрішньокорпоративних відділів однієї чи кількох компаній.

Сервер IP телефонії

Як сервер телефонії може виступати звичайний стаціонарний комп'ютер так і повноцінний Rack-mount (стійковий) сервер, все залежить від бюджету та технічних вимог до системи [7].

Рисунок 5.2 – Сервер Rack-mount

Внутрішні ip телефони

Основна відмінність між аналоговим стаціонарним апаратом, це використання як середовище передачі голосу IP-мережа. Телефон підключається до комп'ютерної мережі як комп'ютер за допомогою конектора RJ-45.

DECT- VoIP телефони

Бездротові телефони DECT база яких використовує для підключення протоколи IP телефонії.

SoftPhone (програмний телефон)

Програма, що реалізує весь функціонал IP-телефону, працює спільно з гарнітурою або USB трубкою.

У схемі ip телефонії внутрішні абоненти не прив'язані до робочого місця і можуть бути віддаленими операторами так і знаходитися всередині офісу.

З боку станційної частини ip атс підключаються зовнішні лінії за допомогою шлюзів voip, що виконують перетворення аналогових FXO лінії, GSM sim карт і цифрових потоків E1.

5.6 Розрахунок необхідної пропускної здатності каналів IP-телефонії

Одним з найважливіших факторів, який слід враховувати при побудові мереж з пакетною передачею голосу, є правильне планування пропускної спроможності. При плануванні пропускної спроможності розрахунок пропускної спроможності є важливим фактором, який слід враховувати при проектуванні та усуненні несправностей мереж пакетного голосового зв'язку для забезпечення хорошої якості передачі голосу.

VoIP – пропускна здатність на виклик

Ці припущення заголовка протоколу використовуються для обчислень:

• 40 байтів для заголовків IP (20 байтів) / протоколу дейтаграм (UDP) (8 байтів) / транспортного протоколу реального часу (RTP) (12 байтів).

• Стислий протокол реального часу (cRTP) скорочує заголовки IP/UDP/RTP до 2 або 4 байтів (cRTP недоступний через Ethernet).

• 6 байтів для Multilink Point-to-Point Protocol (MP) або Frame Relay Forum (FRF).12 Заголовок рівня 2 (L2).

• 1 байт для прапора кінця кадру у кадрах MP та Frame Relay.

• 18 байт для заголовків Ethernet L2, які включають 4 байти послідовності перевірки кадру (FCS) або перевірки циклічним надлишковим кодом (CRC).

Таблиця 5.1 – Таблиця розмірів голосового корисного навантаження за умовчанням у шлюзах H.323

Информация о кодеке				Расчет пропускной способности					
Кодек и битрейт (кбит/с)	Размер выборки кодека (байты)	Интервал выборки кодека (мс)	Средняя оценка мнений (MOS)	Размер голосовой полезной нагрузки (байты)	Размер голосовой полезной нагрузки (мс)	Пакетов в секунду (PPS)	Пропускная способность MP или FRF.12 (Кбит/с)	Пропускная способность с cRTP MP или FRF.12 (кбит/с)	Пропускная способность Ethernet (кбит/с)
G.711 (64 Кбит/с)	80 байт	10 мс	4.1	160 байт	20 мс	50	82,8 Кбит/с	67,6 Кбит/с	87,2 Кбит/с
G.729 (8 Кбит/с)	10 байт	10 мс	3,92	20 байт	20 мс	50	26,8 Кбит/с	11,6 Кбит/с	31,2 Кбит/с
G.723.1 (6,3 Кбит/с)	24 байта	30 мс	3,9	24 байта	30 мс	33,3	18,9 Кбит/с	8,8 Кбит/с	21,9 Кбит/с
G.723.1 (5,3 Кбит/с)	20 байт	30 мс	3,8	20 байт	30 мс	33,3	17,9 Кбит/с	7,7 Кбит/с	20,8 Кбит/с
G.726 (32 Кбит/с)	20 байт	5 мс	3,85	80 байт	20 мс	50	50,8 Кбит/с	35,6 Кбит/с	55,2 Кбит/с
G.726 (24 Кбит/с)	15 байт	5 мс			20 мс	50	42,8 Кбит/с	27,6 Кбит/с	47,2 Кбит/с
G.728 (16 Кбит/с)	10 байт	5 мс	3,61	60 байт	30 мс	33,3	28,5 Кбит/с	18,4 Кбит/с	31,5 Кбит/с
G722_64k (64 Кбит/с)	80 байт	10 мс	4.13	160 байт	20 мс	50	82,8 Кбит/с	67,6 Кбит/с	87,2 Кбит/с
ilbc_mode_20 (15,2 Кбит/с)	38 байт	20 мс	нет данных	38 байт	20 мс	50	34,0 Кбит/с	18,8 Кбит/с	38,4 Кбит/с
ilbc_mode_30 (13,33 Кбит/с)	50 байт	30 мс	нет данных	50 байт	30 мс	33,3	25,867 Кбит/с	15,73 Кбит/с	28,8 Кбит/с

Формули розрахунку пропускної спроможності

Ці розрахунки використовуються:

• Загальний розмір пакета = (заголовок L2: MP або FRF.12 або Ethernet) + (заголовок IP/UDP/RTP) + (розмір корисного голосового навантаження)

• PPS = (бітрейт кодека) / (розмір корисного голосового навантаження)

• Пропускна спроможність = загальний розмір пакета * PPS

Приклад розрахунку

Наприклад, необхідна пропускна здатність для виклику G.729 (швидкість передачі кодека 8 Кбіт/с) з cRTP, MP та 20 байтами голосового корисного навантаження за замовчуванням становить:

• Загальний розмір пакета (байти) = (заголовок MP з 6 байтів) + (стислий заголовок IP/UDP/RTP з 2 байтів) + (голосове корисне навантаження з 20 байтів) = 28 байтів

• Загальний розмір пакета (біт) = (28 байт) * 8 біт на байт = 224 біти

• PPS = (бітрейт кодека 8 Кбіт/с) / (160 біт) = 50 пакетів за секунду

ВИСНОВКИ

В кваліфікаційної роботі на тему «Аналіз методів реалізації IP-телефонії в корпоративних мережах» завдання виконано в повному обсязі.

У першому розділі проведено "Огляд принципів IP-телефонії".

Розглянуто принцип роботи обробки сигналів у приладах VoIP. Принцип роботи полягає в наступному: один із абонентів передає голосові сигнали іншому абоненту, ваш голос проходить обробку за допомогою кодеків та пересилається через Інтернет пакетними даними в режимі реального часу. При цьому максимальна затримка звуку становить близько 300-400 мілісекунд залежно від того, скільки часу потрібно апаратному устаткуванню для створення цифрового аудіосигналу. Оскільки в даний час існують технології, що дозволяють звести втрати сигналу в мережі до мінімуму і уникнути пропадання голосу, ми цього не помітимо. В результаті за цю розмову ви заплатите набагато менше, ніж якби ви користувалися звичайними телекомунікаціями.

Також у розділі були розглянуті кодеки та QoS які використовуються у приладах VoIP. На даний момент використовують такі кодеки як: G.729 – передача параметрів оцифрованого сигналу, G.711 – голосовий кодек, alaw або A-закон – алгоритм стиснення звукових даних із втратою інформації, Ulaw або μ-закон – алгоритм стиснення звукових даних із втратою інформації.

У другому розділі було розглянуто архітектуру та протоколи IP-телефонії. Архітектура мережі VoIP може бути представлена у вигляді двох площин. Нижня відображає транспортний механізм негарантованої доставки мультимедійного трафіку як ієрархію протоколів RTP/UDP/IP, а верхня – механізм керування обслуговуванням дзвінків. Її ключовими протоколами є H.323 ITU-T, SIP, MGCP та MEGACO, що є різними реалізаціями обслуговування дзвінків у мережах IP-телефонії. Протоколи які реалізуються в IP-телефонії: SIP і стек протококолів H.323. У свою чергу, стандарт H.323 заснований на чотирьох компонентах для організації відеоконференцій типу точка-точка або багатоточка: термінали, шлюзи, контролери зони, сервер багатоточкових конференцій. Для зв'язку терміналів із різних мереж, наприклад H.323 та ISDN, використовуються шлюзи.

Протокол SIP – це технологія, яка дозволяє абонентам телефонної мережі розмовляти один з одним, обмінюватися мультимедійною інформацією,

здійснювати відеодзвінки, надсилати повідомлення. Завдяки гнучкості протоколу його можливості можуть бути розширені в залежності від вимог до організації зв'язку. Використання технології SIP дозволяє уникнути обмежень, пов'язаних із застосуванням файрволів. В основу технології покладено такі принципи: мобільність користувачів, можливість масштабування, розширюваність.

У третьому розділі було розглянуто аналіз методів реальзації сервера IP-телефонії в корпоративних мережах. На даний момент існують такі методи реалізації: традиційні канальні IP-АТС, програмні, IP-АТС на базі Asterisk та Віртуальні. Програмну АТС можна охарактеризувати як програму (або програмний комплекс), що емулює роботу традиційної АТС. Тут усе переведено у цифру: від комутації каналів до керування викликами.

Програма IP АТС можна розгорнути на локальному сервері компанії. Для її роботи можуть використовуватись різні платформи. Як правило, розробники пропонують програмні IP АТС для різних дистрибутивів. IP-АТС базі Asterisk – платформа IP телефонії з відкритим вихідним кодом, що надає різні функції керування дзвінками. Це дає нам можливість зробити установку та налаштування Asterisk локально (на сервері клієнта) або у хмарі з подальшою підтримкою.

Головними перевагами програмної АТС Asterisk є гнучкість та безпека. Маючи відкритий вихідний код, Asterisk є модульною комунікаційною платформою, робота якої залежить від телефонних та IP-мереж. На базі рішень Asterisk можна створити гнучку мультифункціональну офісну міні-АТС. Віртуальна IP-АТС, яка фактично розміщена у постачальника електронних комунікаційних послуг у захищеному дата-центрі, що забезпечує стабільний сигнал за допомогою Інтернету, мобільної чи локальної мережі. При цьому не потрібно купувати дороге обладнання — офісну АТС, яка потребує спеціального технічного обслуговування.

У четвертому розділі було розглянуто інформаційну безпеку IP-телефонії та методи криптографічного захисту інформації. Існує кілька основних типів загроз, що становлять найбільшу небезпеку в мережах IP-телефонії: заміна даних про користувача, підслуховування, маніпулювання даними, відмова від обслуговування. Криптографія це технологія складання та розшифрування закодованих повідомлень. Крім того, криптографія є важливою складовою механізмів автентифікації, цілісності та конфіденційності. Аутентифікація є

засобом підтвердження особи відправника чи одержувача інформації. Цілісність означає, що дані не були змінені, а конфіденційність створює ситуацію, за якої дані не може зрозуміти ніхто, крім відправника та одержувача. Зазвичай криптографічні механізми існують у вигляді алгоритму та секретної величини. У системах забезпечення безпеки використовуються три основні криптографічні методи: симетричне шифрування, асиметричне шифрування, односторонні хеш-функції.

У п'ятому розділі вже було розглянуто впровадження IP-телефонії в корпоративній мережі. Було запропоновано використання віртуальної (хмарної) АТС. Запропоновано шлюзи для підключення стандартних дротових телефонів до АТС та підключення АТС у міській телефонній мережі. Продемонстровано вибір телефонів для потреб користувача. Розраховано необхідну пропускну здатність каналів для виклику G.729, яка склала 50 пакетів в секунду.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Домашняя Cisco VoIP лаборатория на базе эмулятора GNS3 // nabr [2006–2018]. Дата изменения: 18.01.2011.
2. IP-телефония: преимущества использования и сравнительные характеристики операторов услуг // Курсовой проект [2010].
3. Азарова, А. О. Комп’ютерні мережі та телекомунікації: навчальний посібник / Азарова А. О., Лисак Н. В. – Вінниця : ВНТУ, 2012. – 293 с.
4. Гольдштейн Б.С., Пинчук А.В., Суховицкий А.Л. IP+Телефония. – М.: Радио и связь, 2001. –336 с.: ил.
5. Asterisk - Окончательное руководство, 4-е издание –Название с экрана. – Электронный ресурс].
6. IBM System i IP Telephony: Configuring the System i Infrastructure, April 2007.
7. 3Com IP Telephony Suite for System i WLE-based Sizing Guide http://www.developer.ibm.com/graphics/estimator/HTML/IP3Com.html
8. IBM System i IP Telephony http://www.ibm.com/systems/i/solutions/iptelephony/
9. https://habr.com/ru/post/183152/
10. https://www.ascod.ru/solutions/asterisk/
11. https://ic-sts.com/solutions-and-service/articles/asterisk/
12. https://cartli-global.com.ua/uslugi/dopolnitelnye-uslugi/virtualnaya-ip-ats
13. http://rz6hpi.narod.ru/net/ip_phone/system/sub-8.1.htm
14. http://rz6hpi.narod.ru/net/ip_phone/system/sub-8.3.htm