

**Міністерство освіти і науки України**

**Луцький національний технічний університет**

(повне найменування закладу вищої освіти)

**Факультет комп'ютерних та інформаційних технологій**

(повне найменування факультету)

**Кафедра комп'ютерної інженерії та кібербезпеки**

(повне найменування кафедри)

**КВАЛІФІКАЦІЙНА РОБОТА  
ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»**

**КОРПОРАТИВНА VOIP МЕРЕЖА НА БАЗІ RINGOSTAT  
CORPORATE VOIP NETWORK BASED ON RINGOSTAT**

спеціальність 123 Комп'ютерна інженерія

(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія

(назва освітньої програми)

Виконав: здобувач вищої освіти

групи КІс-21

Луцьок Арсен Ярославович

(підпис)

Керівник:

к.т.н., доцент

Багнюк Наталія Володимирівна

(підпис)

Кваліфікаційну роботу

допущено до захисту

«    »      червня      2024 р.

Гарант освітньої програми:

к.т.н., доцент

Лавренчук Світлана Василівна

(підпис)

Луцьк – 2024 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет комп'ютерних та інформаційних технологій

Кафедра комп'ютерної інженерії та кібербезпеки

Ступінь вищої освіти: бакалавр

Галузь знань: 12 Інформаційні технології

Спеціальність: 123 Комп'ютерна інженерія

Освітня програма: «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач кафедри

проф. Н.Черняшук

« 10 » 01 2024 р.

ЗАВДАННЯ  
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Луцюку Арсену Ярославовичу

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи Корпоративна VoIP мережа на базі Ringostat

Керівник роботи к.т.н., доцент Багнюк Наталія Володимирівна

затверджені наказом закладу вищої освіти від «30» грудня 2023 року № 459/01-02

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 11.06.2024р.

3. Вихідні дані до роботи Джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області та різні інтернет-ресурси технічного спрямування

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

Вступ

Огляд предметної області

Теоретичні аспекти корпоративних VoIP мереж на базі ringostat

Проектування та реалізація корпоративної VoIP мережі

Висновки

5. Перелік графічного (ілюстративного) матеріалу:

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
<i>Огляд предметної області</i>	<i>Багнюк Н.В., доцент</i>		
<i>Порівняльний аналіз альтернативних варіантів</i>	<i>Багнюк Н.В., доцент</i>		
<i>Реалізація та аналіз роботи корпоративної VoIP мережі</i>	<i>Багнюк Н.В., доцент</i>		
<i>Нормоконтроль</i>	<i>Багнюк Н.В., доцент</i>		
<i>Гарант ОП</i>	<i>Лавренчук С.В., доцент</i>		
<i>Показник запозичень тексту</i>		____%	
<i>Академічна доброчесність</i>	<i>Міскевич О.І., асистент</i>		

7. Дата видачі завдання 10.01.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	<i>Розділ 1. Огляд предметної області</i>	до 15.02.2024 р.	Виконано
2.	<i>Розділ 2. Теоретичні аспекти корпоративних VoIP мереж на базі ringostat</i>	до 15.03.2024 р.	Виконано
3.	<i>Розділ 3. Проектування та реалізація корпоративних VoIP мереж на базі ringostat з використання Ciscj Packet Tracer</i>	до 04.05.2024 р.	Виконано
4.	<i>Висновки та пропозиції</i>	до 07.05.2025 р.	Виконано
5.	<i>Формування списку використаних джерел</i>	до 10.05.2024 р.	Виконано
6.	<i>Формування додатків</i>	до 15.05.2024 р.	Виконано
7.	<i>Оформлення ілюстративного матеріалу</i>	до 20.05.2024 р.	Виконано
8.	<i>Нормоконтроль</i>	до 01.06.2024 р.	Виконано
9.	<i>Інструментальна перевірка на академічний плагіат</i>	до 04.06.2024 р.	Виконано
10.	<i>Представлення кваліфікаційної роботи бакалавра до захисту</i>	до 11.06.2024 р.	Виконано

**Здобувач вищої освіти**

\_\_\_\_\_  
(підпис)

**Луцюк А.Я.**

\_\_\_\_\_  
(прізвище, ініціали)

**Керівник кваліфікаційної роботи**

\_\_\_\_\_  
(підпис)

**Багнюк Н.В.**

\_\_\_\_\_  
(прізвище, ініціали)

## АНОТАЦІЯ

Луцюк А.Я. Корпоративна VoIP мережа на базі Ringostat. Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2024. 55 с.

Кваліфікаційна робота складається з вступу, трьох розділів, висновків, списку використаних джерел, трьох додатків.

Мета роботи: дослідити теоретичні аспекти корпоративних VoIP мереж, проаналізувати можливості системи Ringostat для їх впровадження, розробити та реалізувати проєкт корпоративної VoIP мережі на базі Ringostat з використанням інструменту Cisco Packet Tracer, провести аналіз роботи такої мережі.

В першому розділі визначено актуальність проблеми та поставлено задачі дослідження.

В другому розділі розглядає теоретичні аспекти корпоративних VoIP мереж, включаючи огляд технологій VoIP та аналіз основних характеристик системи Ringostat для корпоративного використання. Також проводиться порівняння Ringostat з іншими системами VoIP для корпоративного сектору.

В третьому розділі описано проєктування та реалізацію корпоративної VoIP мережі на базі Ringostat з використанням інструменту Cisco Packet Tracer.

Об'єкт дослідження – корпоративні VoIP мережі на базі системи Ringostat.

Предмет дослідження – технології VoIP та їх використання у корпоративних мережах.

Ключові слова: VoIP, корпоративні мережі, Ringostat, Cisco Packet Tracer, проєктування мережі, симуляція, аналіз.

## ANNOTATION

Lutsyuk A.Y. Corporate VoIP Network Based on Ringostat. Manuscript.

Qualifying work of a bachelor of EP «Computer Engineering» specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2024. 55 p.

Qualification work consists of an introduction, three chapters, conclusions, a list of references, and three appendix.

The aim of the work: to study the theoretical aspects of corporate VoIP networks, analyze the capabilities of the Ringostat system for their implementation, develop and implement a project of a corporate VoIP network based on Ringostat using the Cisco Packet Tracer tool, and analyze the operation of such a network.

The first chapter defines the relevance of the problem and sets the research tasks.

The second chapter examines the theoretical aspects of corporate VoIP networks, including an overview of VoIP technologies and an analysis of the main features of the Ringostat system for corporate use. A comparison of Ringostat with other VoIP systems for the corporate sector is also conducted.

The third chapter describes the design and implementation of a corporate VoIP network based on Ringostat using the Cisco Packet Tracer tool.

The object of the study is corporate VoIP networks based on the Ringostat system.

The subject of the study is VoIP technologies and their use in corporate networks.

Keywords: VoIP, corporate networks, Ringostat, Cisco Packet Tracer, network design, simulation, analysis.

## ЗМІСТ

ВСТУП .....	7
РОЗДІЛ 1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ .....	9
1.1 Визначення теми та актуальність проблеми .....	9
1.2 Порівняльний аналіз альтернативних варіантів .....	10
1.3 Постановка задачі .....	18
РОЗДІЛ 2 ТЕОРЕТИЧНІ АСПЕКТИ КОРПОРАТИВНИХ VOIP МЕРЕЖ НА БАЗІ RINGOSTAT .....	20
2.1 Огляд технологій VOIP та їх застосування в корпоративних мережах .....	20
2.2 Аналіз основних характеристик системи Ringostat для корпоративного використання .....	23
2.3 Порівняння Ringostat з іншими системами VOIP .....	25
РОЗДІЛ 3 ПРОЕКТУВАННЯ ТА РЕАЛІЗАЦІЯ КОРПОРАТИВНОЇ VOIP МЕРЕЖ НА БАЗІ RINGOSTAT З ВИКОРИСТАННЯМ Cisco Packet Tracer.....	28
3.1 Проектування інфраструктури мережі з використанням Cisco Packet Tracer .....	28
3.2 Симуляція роботи корпоративної VOIP мережі в CiscoPacket Tracer.....	33
3.3 Реалізація та аналіз роботи корпоративної VOIP мережі .....	45
ВИСНОВКИ.....	47
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	49
ДОДАТКИ.....	51

## ВСТУП

У сучасному світі зростає значення технологій голосового передавання через Інтернет (VoIP) у сфері комунікацій та бізнесу. Корпоративні структури все частіше використовують VoIP для забезпечення ефективного обміну інформацією як у межах компанії, так і з клієнтами. У цьому контексті важливо розуміти та досліджувати особливості використання VoIP в корпоративному середовищі, а також розглядати можливості впровадження спеціалізованих систем для управління VoIP трафіком.

Актуальність дослідження полягає у зростанні популярності VoIP технологій серед підприємств та бізнесів, а також у потребі в пошуку оптимальних рішень для побудови та управління корпоративними VoIP мережами. Ефективне використання VoIP може значно підвищити продуктивність бізнесу та зменшити витрати на комунікації, але для цього необхідно детально розібратися у технологічних та організаційних аспектах впровадження VoIP систем.

Метою даної роботи є дослідження, проектування та реалізація корпоративних VoIP мереж на базі системи Ringostat. Зокрема, мета включає аналіз технологій VoIP, вивчення особливостей системи Ringostat для корпоративного сектору, а також проектування та реалізацію корпоративної VoIP мережі з використанням інструменту Cisco Packet Tracer.

Об'єктом дослідження є корпоративні VoIP мережі, які базуються на системі Ringostat та використовуються для організації ефективної комунікації в межах підприємства.

Предметом дослідження є технології VoIP та їх застосування в корпоративних мережах, а також особливості проектування та реалізації корпоративних VoIP мереж на базі системи Ringostat з використанням інструменту Cisco Packet Tracer.

Основними завданнями цієї роботи є:

- розгляд основних технологій VoIP;

- аналіз базових характеристики системи Ringostat та порівняння з іншими системами VOIP;
- розгляд основних переваг Ringostat та можливостей в корпоративному використанні;
- реалізація та аналіз роботи корпоративної VOIP мережі на базі Ringostat.

# РОЗДІЛ 1

## ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

### 1.1 Визначення теми та актуальність проблеми

Корпоративна VoIP мережа на базі Ringostat є надзвичайно актуальною у сучасному діловому середовищі, де ефективно та економічно вигідне спілкування є ключовим фактором успіху. Ця технологія дозволяє компаніям інтегрувати голосові та відеодзвінки, обмін повідомленнями та інші засоби комунікації в єдину уніфіковану систему, забезпечуючи безперервний зв'язок між співробітниками, клієнтами та партнерами.

Ringostat пропонує комплексне рішення для корпоративних комунікацій, яке поєднує в собі гнучкість, масштабованість та зручність використання. Завдяки хмарній архітектурі, компанії можуть легко розгорнути та керувати системою, не витрачаючи значних ресурсів на обслуговування та модернізацію власної телекомунікаційної інфраструктури. Ця технологія забезпечує високу якість зв'язку, надійність та безпеку, гарантуючи захист конфіденційних даних та безперебійну роботу системи [1].

Актуальність корпоративної VoIP мережі на базі Ringostat підкріплюється її численними перевагами та можливостями для підвищення продуктивності та ефективності бізнесу. Вона дозволяє співробітникам спілкуватися з будь-якого місця, використовуючи різноманітні пристрої, такі як комп'ютери, смартфони чи планшети, забезпечуючи мобільність та гнучкість робочого процесу. Інтегрована система управління викликами та автоматичного розподілу дзвінків підвищує якість обслуговування клієнтів, скорочуючи час очікування та підвищуючи задоволеність споживачів [2].

Крім того, Ringostat пропонує корисні інструменти для аналізу та моніторингу комунікацій, такі як запис розмов, статистика дзвінків та звіти про продуктивність. Ці функції дозволяють компаніям виявляти слабкі місця у своїх процесах обслуговування клієнтів, вдосконалювати навички своїх співробітників та оптимізувати операційну діяльність.

Актуальність корпоративної VoIP мережі на базі Ringostat підсилюється її економічною ефективністю. Завдяки використанню Інтернет-протоколу замість традиційних телефонних ліній, компанії можуть значно скоротити витрати на зв'язок, особливо в разі міжнародних дзвінків. Крім того, централізоване управління та масштабованість системи дозволяють легко додавати нових користувачів або розширювати функціональність без значних капітальних вкладень.

Нарешті, перехід на корпоративну VoIP мережу на базі Ringostat є частиною загальної тенденції цифрової трансформації бізнесу. Інтеграція сучасних комунікаційних технологій у бізнес-процеси дозволяє компаніям залишатися конкурентоспроможними на ринку, покращувати якість обслуговування клієнтів та підвищувати загальну ефективність роботи.

## **1.2 Порівняльний аналіз альтернативних варіантів**

Корпоративні VoIP мережі можуть мати різноманітні конфігурації та особливості, що дозволяють адаптувати їх до специфічних потреб бізнесу. Детальний огляд різних видів корпоративних VoIP мереж охоплює наступні аспекти:

По-перше, корпоративні VoIP мережі можуть бути реалізовані у вигляді локальних або хмарних рішень. Локальні системи розгортаються на власних серверах компанії, забезпечуючи максимальний контроль та безпеку, але вимагають значних початкових інвестицій та обслуговування. Натомість, хмарні VoIP рішення, такі як Ringostat, забезпечують більшу гнучкість, масштабованість та економічну ефективність, оскільки вся інфраструктура та обслуговування керуються постачальником послуг [3].

Важливим аспектом корпоративних VoIP мереж є вибір протоколів передачі голосових даних. Найпоширенішим протоколом є SIP (Session Initiation Protocol), який забезпечує сумісність між різними системами та пристроями.

Проте, деякі компанії можуть використовувати власні пропрієтарні протоколи, що може обмежити їх гнучкість та можливості інтеграції [4].

Корпоративні VoIP мережі також можуть відрізнятися своєю архітектурою та топологією. Централізовані системи мають єдиний вузол управління та маршрутизації викликів, тоді як розподілені системи складаються з кількох вузлів, які можуть бути розташовані в різних географічних місцях. Гібридні топології поєднують переваги обох підходів, забезпечуючи централізоване управління та гнучкість розподілених систем [5].

Ще одним важливим аспектом є функціональність та інструменти, які пропонують корпоративні VoIP мережі. Базові функції зазвичай включають голосові дзвінки, відеоконференції, обмін повідомленнями та спільну роботу. Проте, деякі просунуті системи пропонують додаткові можливості, такі як запис розмов, голосова пошта, конференц-зв'язок, управління чергою вхідних дзвінків, налаштування пріоритетності при обробці дзвінків та аналітика.

Таблиця різновидів корпоративних VoIP представлена в таблиці 1.1.

Наступним фактором є масштабованість корпоративної VoIP мережі. Деякі рішення легко піддаються масштабуванню шляхом додавання нових користувачів або розширення функціональності, тоді як інші можуть мати обмеження щодо максимальної кількості користувачів або одночасних викликів.

Нарешті, важливим аспектом корпоративних VoIP мереж є забезпечення безпеки та надійності. Деякі системи пропонують вбудовані засоби захисту, такі як шифрування даних, аутентифікація користувачів та запобігання втручанню. Крім того, рівень надійності може варіюватися залежно від архітектури системи та резервування критичних компонентів.

Отже, корпоративні VoIP мережі можуть суттєво відрізнятися за своєю реалізацією, протоколами, архітектурою, функціональністю, масштабованістю та рівнем безпеки, що дозволяє компаніям вибрати рішення, яке найкраще відповідає їхнім конкретним вимогам та бюджету [6].

Таблиця 1.1 – Різновиди корпоративних VoIP мереж

Тип мережі	Реалізація	Протоколи	Архітектура	Функціональність	Масштабованість	Безпека
Локальна, власні сервери	Розгортання на власних серверах компанії	SIP, пропрієтарні	Централізована, розподілена, гібридна	Базова (дзвінки, відео, месенджер), розширена (IVR, запис, аналітика)	Обмежена масштабованість, залежить від апаратних ресурсів	Високий рівень контролю безпеки, але потребує налаштування
Хмарна (Ringostat)	Хостинг постачальни ком послуг	SIP	Розподілена, гібридна	Повний набір функцій (дзвінки, відео, IVR, запис, аналітика, CRM)	Висока масштабованість, легке додавання користувачів	Вбудовані засоби безпеки, шифрування, авторизація
Віртуальна приватна хмара	Гібридна модель, поєднує власні та хмарні ресурси	SIP, пропрієтарні	Гібридна	Висока гнучкість у налаштуванні функцій	Масштабованість залежить від конфігурації	Комбінація локальної та хмарної безпеки
Програмно-визначена мережа	Віртуалізована архітектура на базі програмного забезпечення	SIP, WebRTC	Високо розподілена	Широкий спектр функцій, інтеграція з додатками	Висока масштабованість, легке додавання ресурсів	Централізоване управління безпекою
Мережа з відкритим кодом	Вільне програмне забезпечення з відкритим кодом	SIP, часто власні протоколи	Гнучка архітектура	Функціональність залежить від рішення	Масштабованість залежить від конфігурації	Залежить від реалізації безпеки
Спеціалізовані галузеві рішення	Призначені для конкретних галузей (call-центри, медицина тощо)	SIP, галузеві протоколи	Зазвичай централізована	Спеціалізовані функції для галузі	Обмежена масштабованість	Високі вимоги до безпеки та конфіденційності

Корпоративні VoIP мережі можуть використовувати різноманітні протоколи для передачі голосових та відео даних. Детальний опис деяких основних протоколів, які часто використовуються в таких мережах:

а) SIP (Session Initiation Protocol) – це найпоширеніший протокол, який став де-факто стандартом для VoIP систем. SIP визначає правила встановлення, підтримки та завершення мультимедійних сеансів, таких як голосові та відеодзвінки, між двома або більше учасниками. Він забезпечує сумісність між різними платформами та пристроями, дозволяючи безпроблемну взаємодію в рамках корпоративної мережі. SIP є відкритим протоколом, що полегшує його інтеграцію з додатками та системами від різних постачальників. Крім того, він підтримує широкий спектр функцій, включаючи передачу даних, маршрутизацію викликів, управління сеансами та безпеку [7].

б) H.323 – це ще один поширений протокол для мультимедійних комунікацій, розроблений Міжнародним союзом електрозв'язку (ITU). Він забезпечує передачу аудіо, відео та даних в режимі реального часу, дозволяючи здійснювати голосові дзвінки, відеоконференції та обмін файлами. H.323 складається з кількох компонентів, таких як шлюзи, термінали та контролери багатопунктового з'єднання, що забезпечують взаємодію між різними мережами та пристроями. Цей протокол активно використовувався в минулому, але в останні роки SIP став більш популярним через свою відкритість та гнучкість.

в) MGCP (Media Gateway Control Protocol) та Megaco/H.248 – це протоколи управління шлюзами, які використовуються для керування медіа-шлюзами в корпоративних VoIP мережах. Вони визначають способи управління потоками медіаданих, таких як голос та відео, між шлюзами та контролерами викликів. MGCP та Megaco забезпечують централізований контроль над шлюзами, дозволяючи ефективно керувати ресурсами та налаштуваннями в мережі.

г) IAX (Inter-Asterisk eXchange) – це пропрієтарний протокол, розроблений для платформи Asterisk IP PBX. Він забезпечує передачу аудіо та відео даних, а також сигналізацію для встановлення та керування викликами.

IAX відрізняється від інших протоколів своєю спрощеною реалізацією та підтримкою таких функцій, як NAT traversal та шифрування. Проте, він обмежений у використанні переважно в середовищах Asterisk.

д) WebRTC (Web Real-Time Communication) – це відносно новий протокол, який дозволяє здійснювати голосові та відеодзвінки, а також обмін даними безпосередньо у веб-браузері без потреби встановлення додаткових плагінів. WebRTC базується на відкритих стандартах і протоколах, таких як SIP, RTP та SRTP, забезпечуючи безпечну та ефективну комунікацію в режимі реального часу. Він стає все більш популярним у корпоративних VoIP мережах через свою зручність використання та сумісність з веб-додатками.

Ці протоколи відіграють ключову роль у функціонуванні корпоративних VoIP мереж, забезпечуючи передачу голосових та відео даних, встановлення та керування викликами, сумісність та безпеку комунікацій. Вибір відповідного протоколу залежить від конкретних вимог, інфраструктури та обладнання, що використовується в мережі [8].

Основними аналогами корпоративних VoIP мереж є традиційні телефонні системи, які включають:

Аналогові телефонні системи (POTS) – це найстаріші та найпростіші телефонні мережі, які використовують виділені мідні дроти для передачі аналогових голосових сигналів. Ці системи покладаються на класичну комутовану телефонну мережу (PSTN) для здійснення дзвінків. Незважаючи на те, що вони забезпечують надійний та якісний зв'язок, аналогові лінії обмежені в плані масштабованості, функціональності та вартості, особливо для великих корпоративних мереж [9].

Цифрові системи, такі як ISDN (Integrated Services Digital Network), використовують цифрові канали для передачі голосу та даних. ISDN може надавати багаторівневі послуги, такі як передача факсів, відеоконференції та доступ до Інтернету, поряд із звичайними голосовими дзвінками. Однак, незважаючи на свої переваги, ISDN є застарілою технологією, витісненою більш сучасними та економічно вигідними рішеннями, такими як VoIP.

Системи традиційної корпоративної телефонної комутації (PBX та IP-PBX) є спеціалізованими телефонними системами, спочатку призначеними для управління великою кількістю внутрішніх телефонних ліній в організаціях. Традиційні PBX-системи використовують виділені телефонні лінії PSTN або ISDN для зовнішніх викликів, тоді як IP-PBX об'єднує голосовий трафік із даними через IP-мережу.

Бездротові системи мобільного зв'язку, такі як стільникові та стаціонарні радіосистеми, також можуть використовуватися для корпоративних комунікацій. Однак вони переважно призначені для роботи з мобільними пристроями та не завжди забезпечують повноцінну інтеграцію з корпоративними системами [10].

На відміну від цих традиційних аналогів, корпоративні VoIP мережі пропонують низку переваг, таких як економічна ефективність, масштабованість, об'єднання голосу, відео та даних в єдиній мережі, розширена функціональність та гнучка інтеграція із сучасними бізнес-додатками. VoIP дозволяє компаніям скористатися перевагами сучасних технологій та підвищити ефективність комунікацій, забезпечуючи при цьому зручність, безпеку та стійкість до майбутніх змін.

Основними аналогами рішення Ringostat для корпоративних VoIP мереж є інші провідні хмарні VoIP-системи та уніфіковані комунікаційні платформи (UCaaS Unified Communications as a Service):

- RingCentral – одна з найбільших хмарних VoIP платформ, яка пропонує широкий спектр послуг, включаючи голосові дзвінки, відеоконференції, месенджер та інтеграцію з офісними додатками. Підтримує інтеграцію з CRM та іншими корпоративними системами.

- 8x8 – хмарне рішення для уніфікованих комунікацій, що об'єднує VoIP, відеоконференції, чат, контакт-центр та аналітику в єдиній платформі. Забезпечує високий рівень безпеки та надійності.

– Dialpad – хмарна платформа для голосових та відеодзвінків, месенджера та співпраці, з акцентом на штучний інтелект та інтеграцію з Google Workspace і Microsoft Office.

– Zoom Phone – голосовий компонент відомої платформи Zoom для відеоконференцій, який пропонує VoIP-дзвінки, месенджер та інтеграцію з іншими продуктами Zoom.

– Microsoft Teams Phone – голосовий компонент Teams, який інтегрується з рештою функцій уніфікованих комунікацій Microsoft, таких як відео, чат та співпраця.

– Nextiva – хмарна VoIP система з функціями віртуальної АТС, контакт-центру, відеоконференцій та інтеграціями з популярними додатками, такими як Salesforce та Zendesk.

– Grasshopper – економічне хмарне рішення для малого бізнесу, що пропонує віртуальну АТС, VoIP-дзвінки, запис розмов та опцію мобільного додатка.

Детальна таблиця аналогів представлена в таблиці 1.2.

Ці аналоги, подібно до Ringostat, є хмарними VoIP платформами, що пропонують уніфіковані комунікації, включаючи голосові та відео дзвінки, месенджер, інструменти співпраці та різноманітні інтеграції. Хоча вони можуть відрізнятися функціональністю, інтерфейсом та цінами, всі вони прагнуть надати бізнесу гнучке, масштабоване та економічно ефективне рішення для корпоративних комунікацій [11].

Таблиця 1.2 – Порівняльний аналіз аналогів Ringostat

№ п/п	Платформа	Основні функції	Інтеграції	Масштабованість	Ціноутворення
1	1	2	3	4	5
2	Ringostat	VoIP-дзвінки, відео, месенджер, IVR, запис, аналітика	CRM, офісні додатки	Висока, легке додавання користувачів	За користувача/місяць, безкоштовний тарифний план
3	RingCentral	Голосові дзвінки, відео, месенджер, контакт-центр	CRM, Microsoft 365, Google Workspace	Висока	За користувача/місяць, корпоративні тарифи

## Продовження таблиці 1.2

1	1	2	3	4	5
4	8x8	Уніфіковані комунікації, контакт-центр, аналітика	CRM, офісні додатки	Висока	За користувача/місяць, корпоративні тарифи
5	Dialpad	Голосові та відеодзвінки, чат, штучний інтелект	Google Workspace, Microsoft Office	Висока	За користувача/місяць, безкоштовний тарифний план
6	Zoom Phone	Голосові дзвінки, інтеграція з Zoom	Zoom відеоконференції	Середня	За користувача/місяць, об'єднані тарифи з Zoom
7	Microsoft Teams Phone	Голосові дзвінки, інтеграція з Teams	Microsoft 365	Висока для існуючих клієнтів Microsoft	Включено в корпоративні ліцензії Microsoft 365
8	Nextiva	Віртуальна АТС, контакт-центр, відеоконференції	CRM, Salesforce, Zendesk	Висока	За користувача/місяць, корпоративні тарифи
9	Grasshopper	Віртуальна АТС, VoIP-дзвінки, запис	Інтеграції обмежені	Низька, орієнтована на малий бізнес	Фіксовані місячні тарифи залежно від функцій

Дана таблиця порівнює основні функції, інтеграції з іншими системами, масштабованість та моделі ціноутворення Ringostat та його конкурентів на ринку хмарних VoIP та уніфікованих комунікаційних платформ. Як видно, Ringostat пропонує широкий спектр функцій та високу масштабованість за доступною ціною з безкоштовним тарифним планом, що робить його конкурентоспроможним вибором для корпоративних комунікацій. Але основна перевага даної VoIP платформи це те що вона українська і зроблена в Україні.

### 1.3 Постановка задачі

Мета: розгорнути сучасну, гнучку та економічно ефективну систему корпоративних комунікацій, яка забезпечить безперебійний зв'язок між співробітниками, клієнтами та партнерами, підвищить продуктивність роботи та рівень обслуговування.

Вимоги:

- Забезпечити єдину платформу для голосових дзвінків, відеоконференцій, обміну повідомленнями та спільної роботи над документами.
- Інтегрувати систему з існуючими бізнес-додатками та CRM для ефективного управління взаємодією з клієнтами.
- Впровадити функції інтелектуальної маршрутизації викликів, інтерактивного голосового меню (IVR) та запису розмов для підвищення якості обслуговування клієнтів.
- Забезпечити високий рівень безпеки та надійності комунікацій, включаючи шифрування даних та авторизацію користувачів.
- Реалізувати масштабовану архітектуру, яка дозволить легко додавати нових користувачів та розширювати функціональність за потреби.
- Інтегрувати аналітичні інструменти для моніторингу та звітності про продуктивність системи та якість обслуговування клієнтів.
- Забезпечити безперервність роботи системи та швидке відновлення в разі збоїв або аварій.

Обмеження:

- Впровадження має бути реалізоване в рамках встановленого бюджету та графіку.
- Система повинна забезпечувати сумісність з існуючими телекомунікаційними пристроями та обладнанням.
- Необхідно мінімізувати простой та порушення робочих процесів під час міграції на нову систему.

- Потрібно забезпечити відповідність системи всім нормативним вимогам та стандартам безпеки.

Очікувані результати:

- Повністю функціональна та інтегрована корпоративна VoIP мережа на базі Ringostat.

- Підвищена продуктивність співробітників та ефективність комунікацій.

- Покращене обслуговування клієнтів та рівень задоволеності споживачів.

- Скорочення витрат на телекомунікації та обслуговування застарілих систем.

- Масштабована та гнучка платформа, готова до майбутнього зростання бізнесу.

- Покращений моніторинг та аналітика для ефективного управління системою комунікацій.

## РОЗДІЛ 2

### ТЕОРЕТИЧНІ АСПЕКТИ КОРПОРАТИВНИХ VOIP МЕРЕЖ НА БАЗІ RINGOSTAT

#### **2.1 Огляд технологій VOIP та їх застосування в корпоративних мережах**

Технології VoIP (Voice over Internet Protocol) відіграють ключову роль у сучасних корпоративних мережах, дозволяючи передавати голосовий трафік через IP-мережі замість традиційних телефонних ліній. Ці технології базуються на низці протоколів, серед яких SIP (Session Initiation Protocol) є стандартним для встановлення, модифікації та завершення мультимедійних сесій, широко використовуваним у корпоративних VoIP-системах. RTP (Real-time Transport Protocol) забезпечує передачу аудіо та відео даних в реальному часі, тоді як MGCP (Media Gateway Control Protocol) та Megaco/H.248 виконують функції управління шлюзами в VoIP-мережах.

Для забезпечення належної якості голосу використовуються різні кодеки, такі як G.711, G.729 та iLBC, які стискають голосові дані для ефективної передачі через IP-мережі. Механізми забезпечення якості обслуговування (QoS) гарантують необхідну пропускну здатність та пріоритет для голосового трафіку, щоб уникнути затримок та втрат пакетів. Архітектура VoIP-систем складається з IP-PBX (IP Private Branch Exchange) – програмних або апаратних систем для маршрутизації VoIP-дзвінків у корпоративній мережі, медіа-шлюзів для інтеграції з традиційними телефонними мережами (PSTN) та серверів управління викликами й додатками для надання розширених функцій, таких як інтерактивні голосові меню (IVR) та конференц-зв'язок [12].

Сучасні корпоративні VoIP-системи часто інтегрують концепцію уніфікованих комунікацій (UC), об'єднуючи голосові дзвінки, відео, обмін повідомленнями та інструменти співпраці в єдиній платформі. Вони також забезпечують інтелектуальну маршрутизацію викликів для оптимізації обслуговування клієнтів, функції запису розмов та аналітики для моніторингу й

покращення якості обслуговування, а також інтеграцію з CRM, ERP та іншими бізнес-додатками для підвищення продуктивності.

Застосування VoIP-технологій у корпоративних мережах приносить низку переваг, включаючи скорочення витрат на зв'язок завдяки об'єднанню голосового та даних трафіку, масштабованість та гнучкість, можливість додавання нових користувачів і функцій, а також мобільність співробітників через підтримку віддалених та мобільних пристроїв. Однак, це також вимагає забезпечення достатньої пропускну здатності мережі, механізмів QoS та заходів безпеки [13].

Корпоративні VoIP-рішення можуть бути реалізовані як хмарні послуги або локальні системи. Хмарні VoIP, такі як Ringostat, забезпечують швидке розгортання, масштабованість та економію коштів на інфраструктуру, тоді як локальні системи (on-premise) забезпечують більший контроль та можливість налаштування, але вимагають більших початкових інвестицій та постійного обслуговування. Вибір відповідного рішення залежить від розміру компанії, вимог до функціональності, бюджету та готовності до впровадження хмарних технологій.

Впровадження технологій VoIP у корпоративній мережі відкриває додаткові можливості та тенденції, які варто розглянути. По-перше, мобільність стає все більш важливим аспектом для підприємств, оскільки все більше співробітників працюють віддалено або перебувають у відрядженнях. VoIP забезпечує безшовну інтеграцію мобільних пристроїв, дозволяючи користувачам отримувати доступ до корпоративних комунікаційних сервісів через смартфони та планшети у будь-якому місці та в будь-який час.

Крім того, інтеграція VoIP з платформами уніфікованих комунікацій та співпраці, такими як Microsoft Teams або Slack, стає загальноприйнятою практикою. Ця інтеграція дозволяє співробітникам легко переходити між різними способами спілкування, включаючи голосові дзвінки, відеоконференції, обмін повідомленнями та спільну роботу над документами в єдиному інтерфейсі.

Ще однією важливою тенденцією є використання хмарних VoIP-рішень, які пропонують масштабованість, гнучкість та економію витрат порівняно з традиційними локальними системами. Компанії можуть швидко розгортати та оновлювати хмарні VoIP-сервіси без необхідності інвестицій у власну інфраструктуру. Водночас, постачальники хмарних послуг забезпечують високий рівень безпеки, надійності та відмовостійкості.

Штучний інтелект та машинне навчання також починають відігравати роль у VoIP-технологіях. Наприклад, системи розпізнавання мовлення можуть використовуватися для транскрибування та аналізу записів розмов, що допомагає покращити якість обслуговування клієнтів та виявити можливості для оптимізації бізнес-процесів.

Кібербезпека є критично важливим аспектом при впровадженні та використанні технологій VoIP у корпоративних мережах. Оскільки голосовий трафік передається через відкриті IP-мережі, такі як Інтернет, існує ризик перехоплення, втручання або навіть крадіжки даних зловмисниками. Тому забезпечення належного рівня безпеки корпоративної VoIP-мережі є обов'язковою вимогою для захисту конфіденційної інформації, репутації компанії та безперебійності бізнес-операцій [14].

Одним з ключових заходів безпеки для VoIP є шифрування голосового трафіку. Протоколи, такі як SRTP (Secure Real-time Transport Protocol) та TLS (Transport Layer Security), використовуються для шифрування мультимедійних даних під час їх передачі через мережу. Це перешкоджає несанкціонованому перехопленню та прослуховуванню розмов зловмисниками [15].

Також, важливо забезпечити належну аутентифікацію та авторизацію користувачів у VoIP-системі. Це включає використання сильних паролів, двофакторної автентифікації та систем контролю доступу, щоб запобігти несанкціонованому доступу до системи та її ресурсів.

Фізична безпека також має значення для VoIP-інфраструктури. Серверні приміщення, мережеві комутатори та шлюзи повинні бути належним чином

захищені від несанкціонованого фізичного доступу, щоб запобігти пошкодженню або крадіжці обладнання.

Постійний моніторинг мережевої активності та аналіз журналів подій є важливими для своєчасного виявлення та реагування на потенційні загрози безпеці. Системи виявлення вторгнень (IDS/IPS) та брандмауери можуть допомогти захистити VoIP-мережу від зловмисних атак, таких як DoS-атаки, розповсюдження шкідливого ПЗ або спам через VoIP (SPIT) [16].

До того ж, необхідно регулярно оновлювати програмне забезпечення та операційні системи VoIP-пристроїв, щоб усунути виявлені вразливості та закрити потенційні вектори атак.

Забезпечення належної кібербезпеки у корпоративній VoIP-мережі вимагає комплексного підходу, який включає технічні, процедурні та організаційні заходи. Це може включати розробку політик безпеки, навчання персоналу, регулярне проведення аудитів безпеки та співпрацю з експертами з кібербезпеки. Лише за умови ретельного дотримання всіх цих заходів компанія може максимально знизити ризики та користуватися перевагами VoIP-технологій у безпечному середовищі.

## **2.2 Аналіз основних характеристик системи Ringostat для корпоративного використання**

Розглядаючи Ringostat як повноцінну систему для корпоративного використання VoIP технологій, необхідно ретельно проаналізувати її ключові характеристики. Ringostat є хмарним рішенням, що забезпечує масштабованість та гнучкість для підприємств будь-якого розміру. Завдяки хмарній архітектурі компанії можуть швидко розгортати та легко масштабувати систему відповідно до своїх потреб, без необхідності вкладати значні інвестиції в апаратне та програмне забезпечення. Ringostat пропонує високий рівень надійності та відмовостійкості, гарантуючи безперебійну роботу та доступність системи навіть у разі збоїв або технічних проблем.

Одним з головних аспектів Ringostat є її функціональність та інтеграційні можливості. Платформа забезпечує комплексне рішення для уніфікованих корпоративних комунікацій, об'єднуючи голосові та відеодзвінки, обмін повідомленнями, конференції та спільну роботу над документами в єдиному інтерфейсі. Вона підтримує широкий спектр функцій, включаючи інтелектуальну маршрутизацію викликів, інтерактивні голосові меню (IVR), запис розмов та аналітику для ефективного управління комунікаціями та покращення якості обслуговування клієнтів. Зручна інтеграція Ringostat з популярними CRM-системами, такими як Salesforce, Microsoft Dynamics та іншими бізнес-додатками, забезпечує безшовну співпрацю та підвищує продуктивність співробітників.

Ключовою перевагою Ringostat є її простота використання та зручний інтерфейс. Система розроблена з акцентом на зручність користувача, що дозволяє швидко опанувати її функціональність та забезпечує плавний перехід від застарілих корпоративних комунікаційних систем. Інтуїтивно зрозумілий веб-інтерфейс та наявність мобільних додатків для різних платформ дозволяють користувачам легко керувати своїми комунікаціями з будь-якого місця та пристрою [17].

Характеристики Ringostat представлені в таблиці 2.1

Питання безпеки та конфіденційності є пріоритетними для Ringostat. Система забезпечує всебічний захист даних, використовуючи передові технології шифрування, такі як TLS та SRTP, для захисту голосового трафіку та конфіденційної інформації. Ringostat також пропонує надійну систему автентифікації користувачів, контроль доступу на основі ролей та регулярні оновлення безпеки, гарантуючи захист від потенційних загроз та відповідність нормативним вимогам [18].

Не менш важливою характеристикою Ringostat є її економічна ефективність. Завдяки хмарній моделі використання, компанії можуть уникнути значних капітальних витрат на придбання та обслуговування апаратного та програмного забезпечення, замінивши їх передбачуваною моделлю оплати за

фактичне використання. Ця модель дозволяє оптимізувати витрати та отримати швидку окупність інвестицій у VoIP-систему.

Таблиця 2.1 – Ключові характеристики системи Ringostat

Характеристика	Параметри
Архітектура	Хмарне рішення
Масштабованість	Легке додавання користувачів, можливість розширення функціоналу
Надійність та відмовостійкість	Висока завдяки хмарній архітектурі, безперебійна робота
Функціональність	Голосові та відео дзвінки, обмін повідомленнями, конференції, спільна робота
	Інтелектуальна маршрутизація викликів, IVR, запис розмов, аналітика
Інтеграції	CRM-системи (Salesforce, Microsoft Dynamics тощо), офісні додатки
Зручність використання	Інтуїтивно зрозумілий веб-інтерфейс, мобільні додатки
Безпека	Шифрування (TLS, SRTP), автентифікація користувачів, контроль доступу
	Регулярні оновлення безпеки
Економічна ефективність	Модель оплати за фактичне використання, відсутність значних капітальних витрат
Користувацькі тарифи	Безкоштовний тарифний план, оплата за користувача/місяць

### 2.3 Порівняння Ringostat з іншими системами VOIP

Порівняння Ringostat з іншими системами VoIP для корпоративного сектору є важливим для визначення її конкурентних переваг та вибору оптимального рішення. На ринку присутні кілька провідних гравців, таких як RingCentral, 8x8, Dialpad та Microsoft Teams Phone, кожен з яких пропонує свій набір функцій та характеристик.

Ringostat вигідно виділяється на тлі конкурентів завдяки своїй хмарній архітектурі, яка забезпечує високу масштабованість, гнучкість та економічну ефективність. Компанії можуть легко розгорнути та масштабувати систему

відповідно до своїх потреб, уникаючи значних капітальних вкладень. На відміну від деяких локальних рішень, Ringostat не вимагає дорогого апаратного забезпечення та обслуговування, пропонуючи зручну модель оплати за фактичне використання.

Порівняльна таблиця провідних VoIP-систем представлена в таблиці 2.2.

Функціональність Ringostat є одною з її головних переваг. Система об'єднує голосові та відео дзвінки, обмін повідомленнями, конференції та спільну роботу в єдиному інтерфейсі, забезпечуючи повноцінні уніфіковані комунікації. Вона також пропонує розширені функції, такі як інтелектуальна маршрутизація викликів, IVR, запис розмов та аналітику, що допомагає оптимізувати обслуговування клієнтів.

Крім того, Ringostat забезпечує безшовну інтеграцію з популярними CRM-системами та офісними додатками, підвищуючи продуктивність співробітників та покращуючи взаємодію з клієнтами. Питання безпеки та конфіденційності даних також є пріоритетними для Ringostat, яка використовує передові технології шифрування та автентифікації користувачів.

Порівняно з конкурентами, Ringostat пропонує більш доступні ціни та навіть має безкоштовний тарифний план, що робить її привабливою для малих та середніх підприємств.

Таблиця 2.2 – Порівняльна таблиця Ringostat та інших провідних VoIP-систем

№ п/п	Система	Масштабованість	Функціональність	Інтеграції	Безпека	Ціноутворення
1	1	2	3	4	5	6
2	Ringostat	Висока (хмарна)	Уніфіковані комунікації, IVR, аналітика	CRM, офісні додатки	Шифрування, автентифікація	Безкоштовний тариф, за користувача/місяць
3	Ring-Central	Висока (хмарна)	Уніфіковані комунікації, контакт-центр	CRM, Microsoft 365, Google Workspace	Шифрування, автентифікація	За користувача/місяць, корпоративні тарифи

## Продовження таблиці 2.2

1	1	2	3	4	5	6
4	8x8	Висока (хмарна)	Уніфіковані комунікації, контакт-центр, аналітика	CRM, офісні додатки	Шифрування, автентифікація	За користувача/місяць, корпоративні тарифи
5	Dialpad	Висока (хмарна)	Голосові та відео дзвінки, чат, штучний інтелект	Google Workspace, Microsoft Office	Шифрування, автентифікація	За користувача/місяць, безкоштовний тариф
6	Microsoft Teams Phone	Висока (для існуючих клієнтів Microsoft)	Інтеграція з Teams (дзвінки, відео, чат)	Microsoft 365	Шифрування, автентифікація	Включено в ліцензії Microsoft 365

Таким чином, Ringostat є однією з систем з уніфікованими комунікаціями, яка пропонує широкий спектр функціональності та можливостей. Вона відрізняється високою масштабованістю, особливо завдяки хмарній архітектурі, що дозволяє легко масштабувати ресурси відповідно до потреб бізнесу. Система підтримує різноманітні функції, такі як уніфіковані комунікації, IVR, аналітика та інші, що дозволяє оптимізувати роботу з клієнтами та внутрішні процеси компанії.

Щодо інтеграцій, Ringostat забезпечує підтримку зв'язку з CRM-системами та офісними додатками, що дозволяє зберігати та обробляти дані з великою ефективністю. При цьому система має вбудовану безпеку, включаючи шифрування та автентифікацію, що забезпечує захист конфіденційної інформації та даних клієнтів.

У ціновій політиці Ringostat пропонує безкоштовний тариф та платні плани за користувача на місяць, що дозволяє бізнесу обрати оптимальний варіант відповідно до своїх потреб та бюджету. Ця система стане ефективним інструментом для компаній, які прагнуть покращити комунікації та оптимізувати внутрішні процеси.

## РОЗДІЛ 3

### ПРОЕКТУВАННЯ ТА РЕАЛІЗАЦІЯ КОРПОРАТИВНОЇ VOIP МЕРЕЖ НА БАЗІ RINGOSTAT З ВИКОРИСТАННЯМ Cisco Packet Tracer

#### 3.1 Проектування інфраструктури мережі з використанням Cisco Packet Tracer

Проектування інфраструктури мережі з використанням Cisco Packet Tracer є ефективним способом моделювання та тестування мережевих топологій та конфігурацій перед їх фізичним впровадженням. Cisco Packet Tracer – це потужний емулятор мережі, який дозволяє створювати віртуальні середовища, що включають маршрутизатори, комутатори, брандмауери та інші мережеві пристрої від різних виробників, таких як Cisco, Juniper, Mikrotik та інші. Цей процес проектування інфраструктури мережі з використанням Cisco Packet Tracer передбачає кілька ключових кроків [19].

Перш за все, налаштовується середовище Cisco Packet Tracer, встановивши відповідне програмне забезпечення та завантаживши необхідні образи операційних систем мережевих пристроїв. Після цього створюються топології мережі, розміщуючи на робочому просторі Cisco Packet Tracer віртуальні маршрутизатори, комутатори та інші компоненти, а також з'єднуючи їх між собою відповідно до бажаної конфігурації. На цьому етапі важливо ретельно спроектувати топологію, враховуючи вимоги до продуктивності, безпеки, масштабованості та надійності мережі.

Під час проектування топології мережі, використано комутатор CISCO WS-C2960-24TT-L серії та маршрутизатор Cisco 2801, які наведені в таблицях 3.1 та 3.2.

Комутатор WS-C2960-24TT-L є лінійкою комутаторів із фіксованою конфігурацією та портами Fast Ethernet і Gigabit Ethernet, що мають розширені LAN сервіси для підприємств початкового рівня та мереж віддаленого офісу. Комутатор Cisco Catalyst 2960 підтримує передачу голосу, даних і відео, а також безпечний доступ.

Таблиця 3.1 – Технічні характеристики комутатора CISCO WS-C2960-24TT-L

Характеристики	Опис
Модель	Cisco WS-C2960-24TT-L
Кількість портів	24 порти 10/100Base-TX Fast Ethernet + 2 порти SFP для гігабітних підключень
Пропускна здатність	8.8 Гбіт/с
Максимальна відстань	До 100 метрів на кожному порту Fast Ethernet
Підтримка VLAN	До 255 активних VLAN
QoS	Підтримка 4 рівнів чергування (CoS) та 4 рівнів поліпшення якості обслуговування (QoS)
Механізми безпеки	IEEE 802.1X, ACL, SSH, SSL, Port Security, DHCP Snooping, IP Source Guard.
Інтерфейси управління	Консольний порт, Telnet, SSH, веб-інтерфейс через HTTP або HTTPS
Енергоспоживання	Максимальне: 30 Вт, В режимі очікування: 12 Вт
Методи монтажу	Може монтуватися в стійку або розміщуватися на столі
Розміри	44.5 x 33.5 x 4.5 см
Вага	Приблизно 3.6 кг

Комутатор Cisco Catalyst 2960 підтримує Intelligent features (створення складних списків управління доступом, розширена безпека), комбіновані гігабітні аплінки (мідний 10/100/1000BASE-T Ethernet або SFP-модуль для переходу в інше середовище - Cisco 1000BASE-SX, 1000BASE-LX, 1000BASE-ZX, 100BASE-FX, 100BASE-LX, CWDM SFP). Також, пристрої Catalyst 2960 підтримують QoS, покроковий Rate Limiting, ACL (на базі MAC або IP-адрес, портів UDP/TCP) і multicast services, можливість регулювати швидкість передавання на кожному порту з кроком 64 кБіт, Link Aggregation для організації швидкісніших з'єднань між комутаторами і серверами, можливість організації транкових з'єднань на кожному порту за допомогою тегів 802.1q, до 255 VLAN на комутатор, до 4000 VLAN ID і управління через Cisco Network Assistant

(підтримує широкий спектр моделей комутаторів від Cisco Catalyst 2960 до Cisco Catalyst 4506).

В таблицях 3.1-3.2 наведено технічні характеристики обладнання Cisco.

Прошивка комутатора Cisco Catalyst 2960 випускається в образах LAN Base і Lan Lite Image. LAN Base має ширший функціонал, включно з поліпшеною безпекою (ACLs), DHCP Snooping і додатковими функціями з контролю доступу – Web authentication і розширення 802.1x, додатковими можливостями установок якості обслуговування QoS, підтримкою надлишкового живлення RPS і великої кількості SFP-портів. Функції Flex Links і Link State Tracking, збільшена кількість підтримуваних VLANs (до 256), IPv6 Host, MLD Snooping, LLDP-MED, RSPAN, MVR, DHCP Option 82, IP SLA (responder) та інше.

Таблиця 3.2 – Технічні характеристики маршрутизатора

Характеристики	Опис
Модель	Cisco 2801
Процесор	280 МГц
Пам'ять	256 МБ оперативної пам'яті, 64 МБ флеш-пам'яті
Інтерфейси WAN	2 x 10/100 Ethernet
Інтерфейси LAN	2 x 10/100 Ethernet
Підтримка протоколів	IP, IPv6, SNMP, DHCP, NAT, BGP, OSPF
Максимальна швидкість пересилання	75 Мбіт/с
Підтримка VPN	IPsec, SSL
Апаратне шифрування	DES, 3DES, AES 128/192/256
Підтримка голосу	VoIP, SIP, FXO, FXS
Підтримка мережевих служб	Firewall, DHCP, NAT, QoS, VPN
Розширення	Слоти для установки модулів NME, HWIC
Розміри	44.45 x 438.15 x 317.5 мм
Вага	5.2 кг

Після створення топології необхідно налаштувати кожен мережевий пристрій, призначивши їм відповідні IP-адреси, протоколи маршрутизації, правила доступу та інші параметри. Cisco Packet Tracer підтримує командний рядок Cisco IOS та інші операційні системи мережевих пристроїв, що дозволяє

користувачам застосовувати свої навички та знання в реалістичному середовищі. Крім того, Cisco Packet Tracer забезпечує доступ до пакета трасування Cisco, який включає такі функції, як ping, traceroute та інші інструменти для перевірки з'єднання та виявлення проблем у мережі [20].

Пакет трасування Cisco є невід'ємною частиною Cisco Packet Tracer і надає низку корисних функцій для тестування та налагодження мережі. Команда ping дозволяє перевірити зв'язок з іншими пристроями та виявити втрату пакетів. Traceroute показує маршрут, яким проходить пакет до вказаної адреси, допомагаючи ідентифікувати вузькі місця або проблеми з маршрутизацією. Інші інструменти пакета трасування, такі як extended ping, telnet та debug, допомагають детально аналізувати проблеми з мережею та виявляти їхні причини.

Після налаштування та тестування топології в Cisco Packet Tracer, можна переходити до наступного етапу – перевірки роботи мережі шляхом імітації різних сценаріїв трафіку, збоїв та атак. Cisco Packet Tracer дозволяє створювати та запускати скрипти автоматизації для моделювання різних ситуацій, що допомагає виявити вразливі місця та оптимізувати конфігурацію мережі перед її фізичним розгортанням.

У мережевому конфігуруванні вирішено використати п'ять різних мереж, кожна з яких має свої VLAN. В першій мережі VLAN 15 використовує підмережу 192.168.15.0/24, в другій мережі VLAN 15 має підмережу 192.168.25.0/24, а в третій мережі VLAN 15 користується підмережею 192.168.35.0/24 і т.ін.

Для VLAN 16 ситуація аналогічна: в першій мережі використовується підмережа 192.168.16.0/24, в другій – 192.168.26.0/24, а в третій – 192.168.36.0/24 і т.ін

З'єднання між маршрутизаторами:

– Підключення між маршрутизаторами RA і RB використовує підмережу 10.0.0.0/30.

– Підключення між маршрутизаторами RB і RC використовує підмережу 10.0.0.4/30.

Детальна таблиця адресації представлена в таблиці 3.3.

Це означає, що між кожною парою маршрутизаторів будуть використовуватись окремі IP-адреси для забезпечення зв'язку. Кожна з цих підмереж має маску 30, що означає, що вона може містити до чотирьох IP-адрес. Таке налаштування дозволяє ефективно організувати зв'язок між маршрутизаторами та забезпечити безпеку мережі.

Технологія VLAN (Virtual Local Area Network) – це метод розділення фізичної мережі на логічні сегменти на рівні комутатора мережі. За допомогою VLAN можна розділити одну фізичну мережу на логічні сегменти, які можуть функціонувати незалежно один від одного, надаючи більшу гнучкість та безпеку в управлінні мережею. Це дозволяє забезпечити безпеку, ефективність та простоту управління мережею. VLAN може бути корисним в таких аспектах:

- Розділення трафіку: використання VLAN дозволяє розділити трафік мережі на логічні сегменти для користувацьких даних, управлінських повідомлень та даних про статуси на окремі логічні мережі. Це сприяє кращому керуванню та моніторингу трафіку, зменшуючи ймовірність конфліктів та перевантажень. Розділення трафіку допомагає забезпечити, що управлінські дані та дані про статуси мережі не будуть конкурувати з користувацькими даними за ресурси мережі. Такий підхід сприяє збереженню продуктивності та стабільності мережі.

- Підвищення безпеки: використання VLAN дозволяють фізично розділити мережу на логічні сегменти, що забезпечує ізоляцію трафіку між різними групами користувачів. Це дозволяє обмежувати доступ до важливих ресурсів мережі та запобігати несанкціонованому доступу, що забезпечує високий рівень конфіденційності та захисту від несанкціонованого доступу.

- Оптимізація пропускної здатності: використання VLAN дозволяє призначити різним типам трафіку (наприклад, голосовий, відео, даних) відповідні пріоритети та ресурси. Це дозволяє оптимізувати пропускну здатність мережі, надаючи важливому трафіку пріоритет перед менш важливим. Наприклад, можна налаштувати VLAN для голосового трафіку, щоб забезпечити

низьку затримку та безперебійне відтворення аудіо, тоді як інші види трафіку можуть бути обмежені, щоб уникнути перевантажень мережі. Це допомагає забезпечити кращу якість обслуговування для різних типів даних у мережі. Наприклад, важливі дані про місцезнаходження можуть мати вищий пріоритет, що дозволяє їм передаватися з меншою затримкою та високою надійністю.

– Управління мережею: адміністратори можуть легко налаштовувати та керувати доступом до ресурсів мережі, встановлювати політики безпеки та моніторити трафік в межах окремих логічних мереж.

### **3.2 Симуляція роботи корпоративної VOIP мережі в CiscoPacket Tracer**

Симуляція роботи корпоративної VoIP (Voice over Internet Protocol) мережі в Cisco Packet Tracer – це важливий інструмент для тестування, налагодження та вдосконалення мережевих інфраструктур перед їх впровадженням в реальному середовищі. Під час роботи з VoIP у Cisco Packet Tracer можна відтворити усі аспекти роботи реальної мережі, включаючи розгортання IP-телефонів, маршрутизаторів, комутаторів, серверів та інших мережевих пристроїв.

Одним з ключових етапів створення симуляції VoIP є розгортання віртуальних пристроїв в середовищі Cisco Packet Tracer, що відтворює фізичні характеристики та функціональні можливості реальних пристроїв. Це включає встановлення та налаштування IP-телефонів, SIP-серверів, маршрутизаторів з підтримкою VoIP, комутаторів VLAN, DHCP-серверів та інших необхідних компонентів [21].

Після розгортання пристроїв необхідно налаштувати їх відповідно до потреб мережі. Це включає встановлення IP-адрес, конфігурування VLAN для розділення трафіку, налаштування SIP-протоколів для передачі голосу та інші параметри.

У процесі симуляції можна проводити різні тести та аналізувати реакцію мережі на різні сценарії. Наприклад, можна перевірити якість голосового зв'язку, затримки пакетів, пропускну здатність мережі та інші параметри.

Однією з важливих можливостей симуляції VoIP в Cisco Packet Tracer є можливість відтворювати складні топології мережі, що дозволяє тестувати різні сценарії та вирішувати проблеми, які можуть виникнути в реальному середовищі.

Спроектвана топологія мережі представлена на рисунку 3.1. та адресація в таблиці 3.3

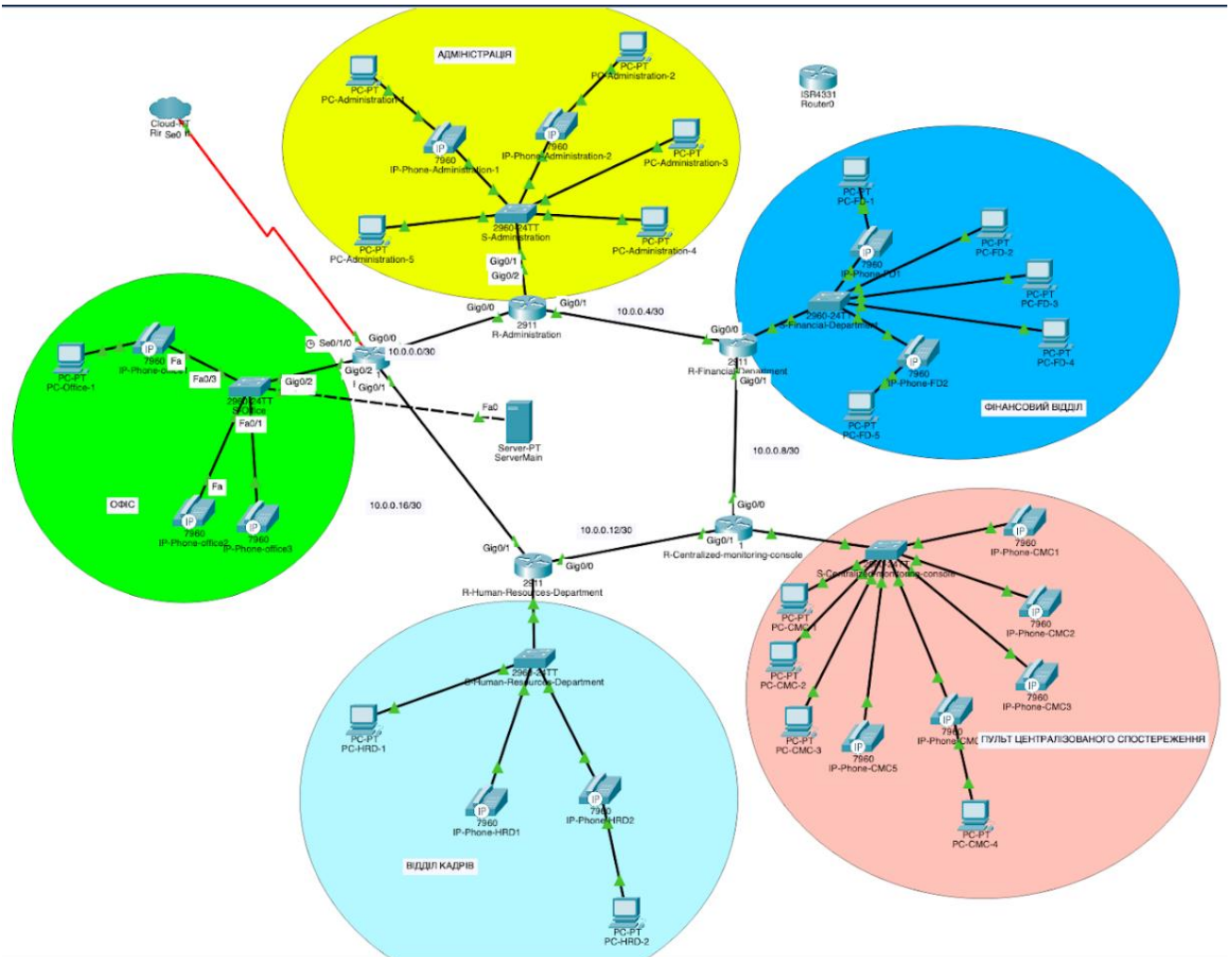


Рисунок 3.1 – Топологія комп'ютерної мережі

Таблиця 3.3 – Таблиця адресації мережі

Мережа	VLAN	Підмережа	Інтерфейс (Router)	Шлюз	Маска підмережі
Мережа між роутерами					
10.0.0.0/30	-	10.0.0.0	-		255.255.255.252
10.0.0.4/30	-	10.0.0.4	-		255.255.255.252
10.0.0.8/30	-	10.0.0.8	-		255.255.255.252
10.0.0.12/30	-	10.0.0.12	-		255.255.255.252
10.0.0.16/30	-	10.0.0.16	-		255.255.255.252
Офіс					
Data VLAN	15	192.168.15.0	GigabitEthernet0/2.15	192.168.15.1	255.255.255.0
VoIP VLAN	16	192.168.16.0	GigabitEthernet0/2.16	192.168.16.1	255.255.255.0
Адміністрація					
Data VLAN	17	192.168.25.0	GigabitEthernet0/2.17	192.168.25.1	255.255.255.0
VoIP VLAN	18	192.168.26.0	GigabitEthernet0/2.18	192.168.26.1	255.255.255.0
Фінансовий відділ					
Data VLAN	19	192.168.35.0	GigabitEthernet0/2.19	192.168.35.1	255.255.255.0
VoIP VLAN	20	192.168.36.0	GigabitEthernet0/2.20	192.168.36.1	255.255.255.0
Пульт централізованого спостереження					
Data VLAN	21	192.168.45.0	GigabitEthernet0/2.21	192.168.45.1	255.255.255.0
VoIP VLAN	22	192.168.46.0	GigabitEthernet0/2.22	192.168.46.1	255.255.255.0
Відділ кадрів					
Data VLAN	25	192.168.55.0	GigabitEthernet0/2.25	192.168.55.1	255.255.255.0
VoIP VLAN	26	192.168.56.0	GigabitEthernet0/2.26	192.168.56.1	255.255.255.0

У таблиці 3.3 вказано IP-адреси та маски підмереж для кожної мережі, а також прив'язку VLAN до відповідних інтерфейсів на маршрутизаторі. Адресація і прив'язка VLAN може залежати від конкретної топології мережі та потреб.

Протокол DHCP (Dynamic Host Configuration Protocol) використовується для автоматичного налаштування мережевих параметрів пристроїв (рисунок 3.2), таких як IP-адреси, мережеві шлюзи та DNS-сервери. Налаштування DHCP мережі може бути виконане через адміністративний інтерфейс роутера.

Для налаштування DHCP в пристроях Cisco необхідно:

- Підключитись до пристрою через консольний кабель або SSH.
- Увійти в привілейований режим за допомогою команди `enable`.
- Перейти в режим глобальної конфігурації за допомогою команди `configure terminal`.
- Створити DHCP пул або пули для IP-адрес.
- Вказати адресацію мережі для кожного DHCP пулу.
- Вказати шлюз за замовчуванням для клієнтів для кожного пулу.
- Налаштувати DNS сервери для DHCP клієнтів.
- Вказати час оренди для IP-адрес.
- Зберегти конфігурацію за допомогою команди `write memory`.

Після правильного налаштування DHCP пристрої, підключені до мережі, автоматично отримають необхідні мережеві налаштування, що спростить управління мережею та забезпечить швидке та ефективне підключення пристроїв до мережі без необхідності ручного налаштування кожного пристрою окремо.

Крім основних налаштувань, важливо також врахувати можливість налаштування додаткових параметрів, таких як резервування IP-адрес для конкретних пристроїв за допомогою команд DHCP binding, а також налаштування опцій DHCP, таких як параметри для VoIP телефонів або інших специфічних пристроїв.

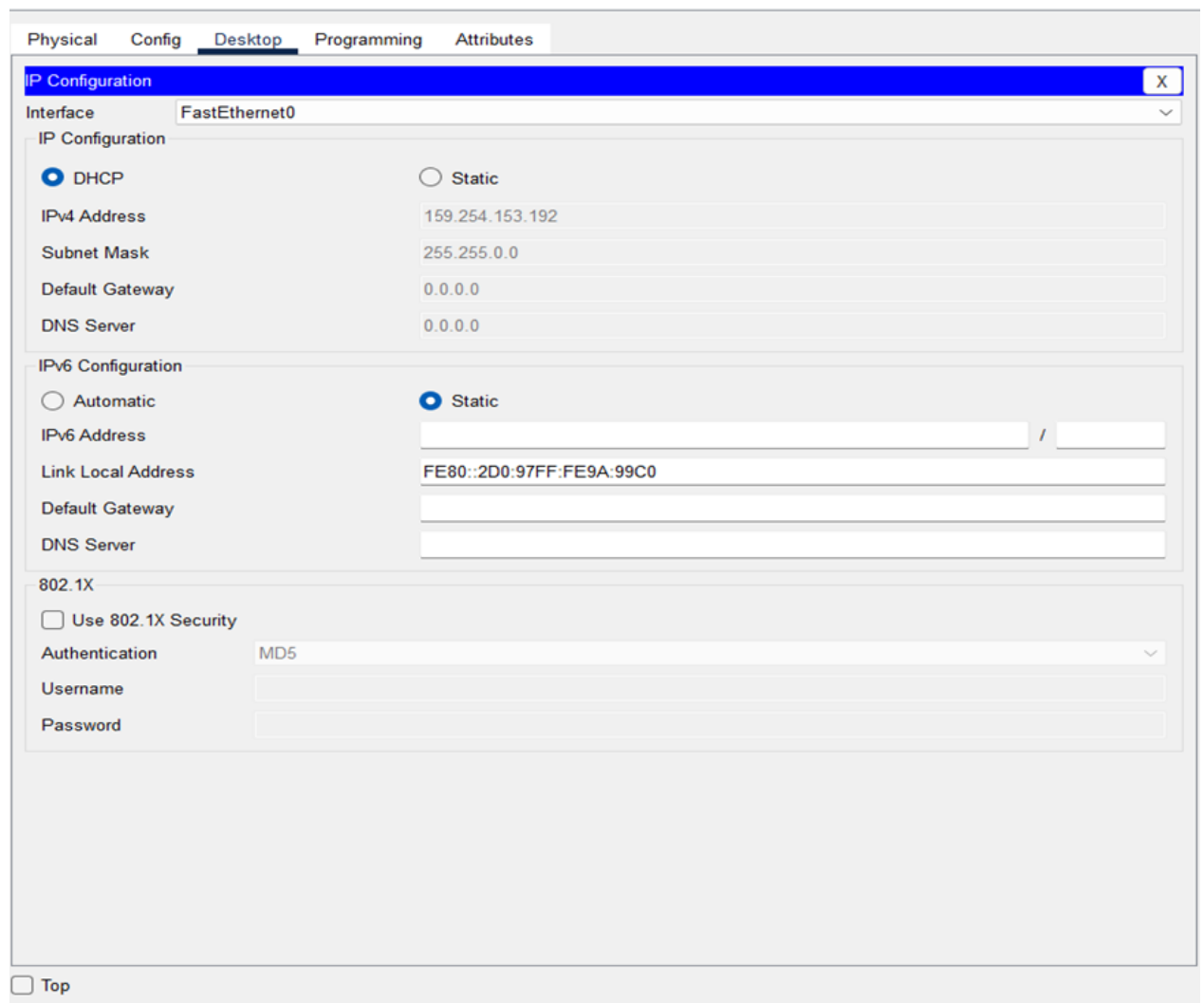


Рисунок 3.2 – Налаштування протоколу DHCP

Технологія IP Phone (IP-телефон) дозволяє здійснювати телефонні дзвінки через Інтернет протокол IP, використовуючи мережу даних замість традиційних телефонних ліній. У контексті даної мережі IP Phone дозволяє співпрацювати з існуючою інфраструктурою мережі, використовуючи IP-адреси для ідентифікації та маршрутизації телефонних дзвінків.

Кожен IP Phone (рисунок 3.3) має свою унікальну IP-адресу, яка ідентифікує його в мережі. Коли користувач намагається здійснити дзвінок, IP Phone взаємодіє з VoIP-сервером (Voice over IP), який використовується для маршрутизації телефонних дзвінків в мережі. Потім дзвінок передається через мережу даних до отримувача, який також може бути IP Phone або традиційний телефон, залежно від конфігурації мережі.

Однією з переваг IP Phone є їх інтеграція з існуючою мережевою інфраструктурою, що дозволяє здійснювати телефонні дзвінки без необхідності встановлення окремих телефонних ліній. Вони також надають більші можливості для функціональності та управління, такі як відеодзвінки, пересилання файлів та інші додаткові функції, які можуть бути важливими для бізнес-спілкування [22].

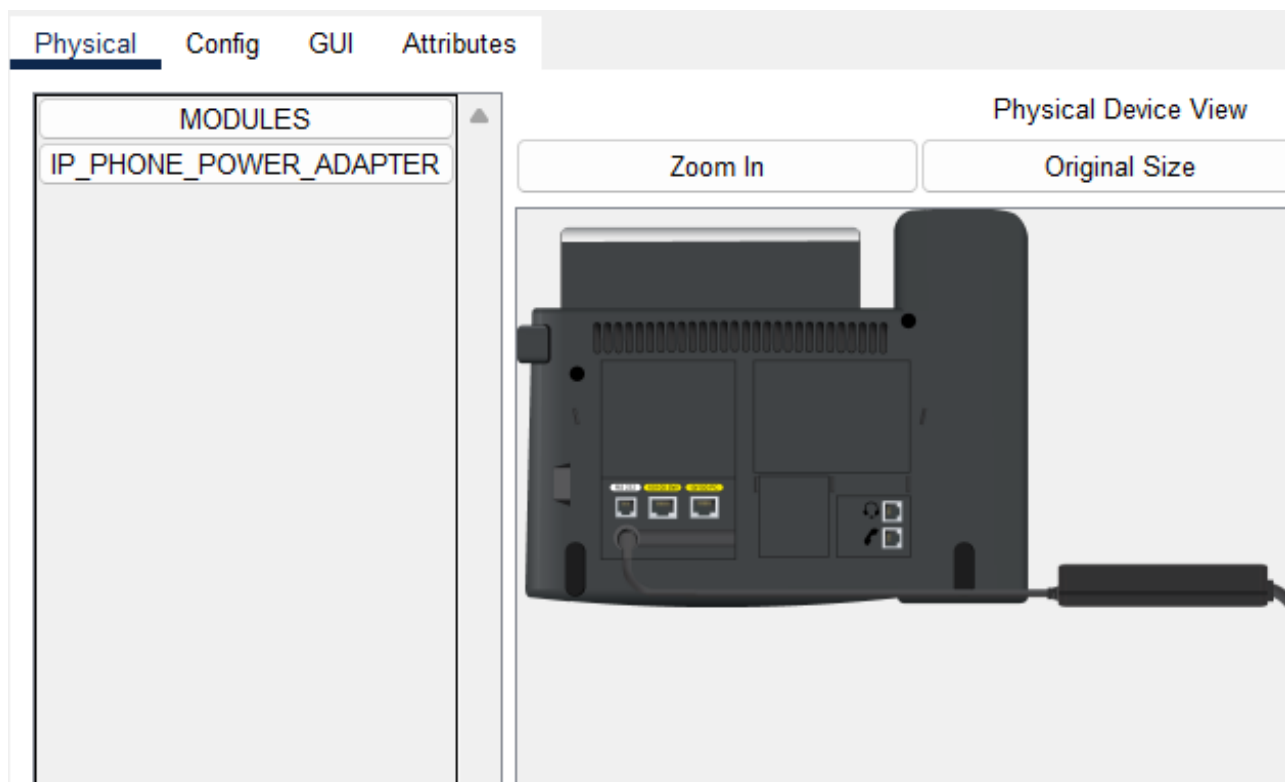


Рисунок 3.3 – Налаштування параметрів IP Phone

Інтеграція системи аналітики дзвінків Ringostat з VoIP шлюзом Cisco є потужним рішенням для підприємств, що бажають оптимізувати свої комунікаційні процеси та покращити якість обслуговування клієнтів. Така інтеграція забезпечує надійний зв'язок і дозволяє використовувати можливості аналітики дзвінків для підвищення ефективності бізнесу [23].

Основними компонентами інтеграції Ringostat є:

- Платформа для аналітики дзвінків і колтрекінгу.

- Моніторинг ефективності маркетингових кампаній і оптимізація роботи кол-центрів.
- Підтримка SIP протоколу для взаємодії з іншими VoIP системами.
- Основними компонентами інтеграції Cisco є VoIP шлюз. Це пристрій, що забезпечує передачу голосових даних через IP мережу Cisco VoIP.
- Підтримує SIP протокол для встановлення і управління VoIP дзвінками.
- Забезпечує надійне підключення і маршрутизацію дзвінків між різними системами.

Процес інтеграції Ringostat до VoIP шлюзу Cisco:

- Створюється SIP-транк між Ringostat і VoIP шлюзом Cisco. SIP (Session Initiation Protocol) використовується для встановлення, управління і завершення дзвінків через IP мережу.
- На VoIP шлюзі Cisco налаштовуються діал-плани для правильного маршрутизації дзвінків до Ringostat.
- Дзвінки, які надходять на VoIP шлюз Cisco, можуть бути спрямовані до Ringostat для аналітики і зворотного зв'язку.
- Ringostat, у свою чергу, може обробляти ці дзвінки, збираючи дані про їх тривалість, якість, джерело тощо.

Безпека:

- Для захисту голосових даних використовується шифрування за допомогою протоколів TLS (для сигнальних даних) і SRTP (для медіаданих).
- Аутентифікація користувачів і контроль доступу забезпечують безпечне підключення до обох систем.

Коректне налаштування мережевих параметрів у програмі є вкрай важливим для забезпечення надійної IP-телефонії. Одним із ключових налаштувань є визначення адреси SIP-проксі серверу, яка використовується для реєстрації облікового запису та маршрутизації VoIP-трафіку. Ця адреса повинна бути введена у форматі IP або доменного імені відповідно до конфігурації, наданої VoIP-провайдером. Наступним критичним параметром є номер порту

SIP-сервера, найчастіше це порт 5060, проте він може варіюватися залежно від особливостей налаштувань мережі.

Вибір транспортного протоколу для передачі даних також має вирішальне значення.

Користувачі мають можливість вибору транспортного протоколу для передачі даних у системі IP-телефонії. Вони можуть обирати між протоколами UDP, TCP та TLS (Transport Layer Security). UDP забезпечує швидку та ефективну передачу даних, проте не гарантує доставку пакетів. TCP забезпечує надійність доставки, але може спричиняти деякі затримки через механізми підтвердження доставки. TLS є безпечнішим варіантом, оскільки забезпечує шифрування даних, але вимагає більше обчислювальних ресурсів через процес шифрування та розшифрування. Кожен з цих протоколів має свої переваги та обмеження, і вибір залежить від конкретних потреб і вимог користувача (рисунок 3.4).

Ще одним ключовим аспектом є налаштування кодеків голосу та відео. Програма IP Communicator дозволяє встановлювати пріоритетність використання різних кодеків, що оптимізує споживання пропускну здатності та забезпечує сумісність між VoIP-клієнтами. Крім того, належне налаштування параметрів NAT (Network Address Translation) є критичним для коректної трансляції мережевих адрес під час проходження через брандмауери та маршрутизатори, що дозволяє забезпечити безперебійну роботу з'єднання.

По-перше, необхідно правильно ввести IP-адресу або доменне ім'я SIP-проксі сервера, наданого VoIP-провайдером. Це дозволить маршрутизатору Home VoIP успішно зареєструватися в системі для прийому та передачі викликів через Інтернет. Налаштування порту SIP-сервера, як правило, встановлюється на 5060, якщо провайдер не вказав інше.

Окрім цього, слід налаштувати використання відповідних голосових кодеків, які підтримуються VoIP-провайдером та аналоговим телефонним пристроєм для оптимізації якості звуку. Пріоритетність кодеків може бути задана в налаштуваннях.

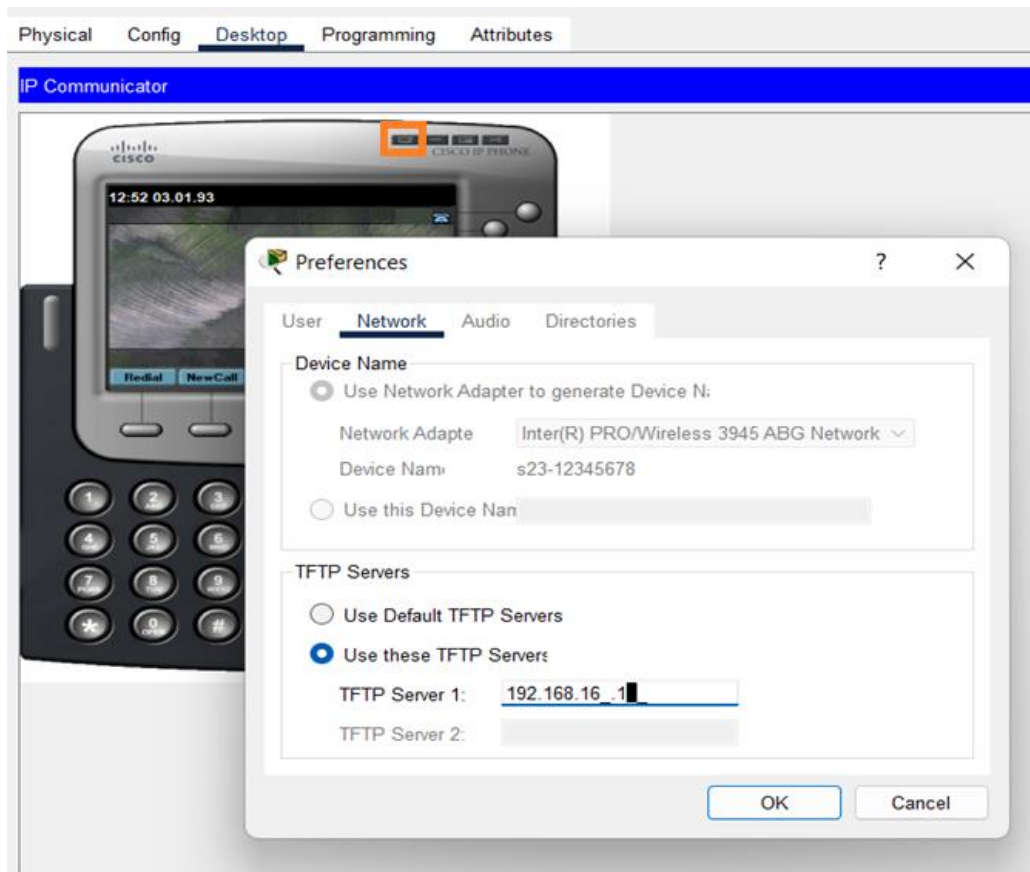


Рисунок 3.4 – Налаштування конфігурації CIPS

Командний рядок CLI (Command Line Interface) є потужним інструментом для конфігурації та управління мережевими пристроями, такими як маршрутизатори, комутатори та системи VoIP. У контексті моніторингу якості VoIP-з'єднання за допомогою RingStatServer, CLI може бути використаний для ряду важливих завдань.

По-перше, CLI дозволяє легко переглядати та змінювати конфігурацію мережевих пристроїв, наприклад, налаштування SIP, маршрутизації та безпеки. Це особливо корисно при інтеграції RingStatServer з мережевою інфраструктурою або при пошуку несправностей у разі виникнення проблем із VoIP.

Крім того, за допомогою CLI можна отримувати детальну статистику та дані про продуктивність у реальному часі. Це включає показники якості сервісу (QoS), такі як затримка, джиттер, втрата пакетів та завантаженість мережі.

Аналізуючи ці метрики, адміністратори можуть виявляти вузькі місця та вживати заходів для оптимізації мережевого середовища для VoIP.

CLI також дозволяє виконувати різноманітні діагностичні команди для виявлення проблем із з'єднанням та маршрутизацією, наприклад, трасування маршруту (traceroute), перевірку доступності (ping) та аналіз протоколів VoIP на рівні пакетів.

Ще одним важливим застосуванням є автоматизація завдань за допомогою скриптів CLI. Це дозволяє легко виконувати повторювані завдання, такі як резервне копіювання конфігурацій, розгортання змін масштабованим способом або автоматичний збір даних для аналізу продуктивності Ringostat.

На рисунках 3.5-3.9 відображено скріншоти налаштування мережі в командному рядку.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 15
Switch(config-vlan)#name data
Switch(config-vlan)#vlan 16
Switch(config-vlan)#name voice
Switch(config-vlan)#vlan 99
Switch(config-vlan)#name native
Switch(config-vlan)#ex
Switch(config)#int fa0/1
Switch(config-if)#sw mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch(config-if)#sw trunk native vlan 99
Switch(config-if)#ex
Switch(config)#int range fa0/2-11
Switch(config-if-range)#sw mode access
Switch(config-if-range)#sw access vlan 15
Switch(config-if-range)#sw voice vlan 16
Switch(config-if-range)#ex
Switch(config)#int range fa0/12-14
Switch(config-if-range)#sw mode access
Switch(config-if-range)#ex
Switch(config)#int range gi0/1-2
Switch(config-if-range)#sw mode access
Switch(config-if-range)#ex
Switch(config)#
```

Рисунок 3.5 – Налаштування світчів

```

Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0.15
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.15, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.15, changed state to up

Router(config-subif)#enc dot1q 15
Router(config-subif)#ip add 192.168.15.1 255.255.255.240
Router(config-subif)#ex
Router(config)#int fa0/0.16
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.16, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.16, changed state to up

Router(config-subif)#enc dot1q 16
Router(config-subif)#ip add 192.168.16.1 255.255.255.240
Router(config-subif)#ex
Router(config)#int fa0/0.99
Router(config-subif)#enc dot1q 99 native
Router(config-subif)#ex
Router(config)#int range fa0/0-1
Router(config-if-range)#no sh
Router(config-if-range)#ex
Router(config)#int fa0/1
Router(config-if)#ip address 192.168.1.1 255.255.255.252
Router(config-if)#ex
Router(config)#

```

Рисунок 3.6 – Налаштування роутерів

```

Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp ex
Router(config)#ip dhcp excluded-address 192.168.15.1
Router(config)#ip dhcp ex
Router(config)#ip dhcp excluded-address 192.168.16.1
Router(config)#ip dhcp pool data
Router(dhcp-config)#network 192.168.15.0 255.255.255.240
Router(dhcp-config)#defa
Router(dhcp-config)#default-router 192.168.15.1
Router(dhcp-config)#dns-se
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#ex
Router(config)#ip dhcp pool voice
Router(dhcp-config)#network 192.168.16.0 255.255.255.240
Router(dhcp-config)#defa
Router(dhcp-config)#default-router 192.168.16.1
Router(dhcp-config)#option 150 ip 192.168.16.1
Router(dhcp-config)#dns-ser
Router(dhcp-config)#dns-server 0.0.0.0
Router(dhcp-config)#ex

```

Рисунок 3.7 – Налаштування параметрів

```

Router(config)#telephony-service
Router(config-telephony)#max-dn 10
Router(config-telephony)#max-ephones 10
Router(config-telephony)#ip source-address 192.168.26.1 port 2000
Router(config-telephony)#ex
Router(config)#do show ephone

ephone-1 Mac:000A.41E7.3712 TCP socket:[1] activeLine:1 UNREGISTERED
mediaActive:0 offhook:1 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:8
IP:0.0.0.0 0 7960    keepalive 43 max_line 2
  button 1: dn 1  number 201 CH1  DOWN

ephone-2 Mac:00E0.A306.4E56 TCP socket:[1] activeLine:1 UNREGISTERED
mediaActive:0 offhook:1 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:8
IP:0.0.0.0 0 ata    keepalive 43 max_line 2
  button 1: dn 2  number 202 CH1  DOWN

ephone-3 Mac:0001.637A.34C7 TCP socket:[1] activeLine:1 UNREGISTERED
mediaActive:0 offhook:1 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:8
IP:0.0.0.0 0 CIPC   keepalive 43 max_line 2
  button 1: dn 3  number 203 CH1  DOWN

```

Рисунок 3.8 – Налаштування телефонії

```

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#dial-pe
Router(config)#dial-peer vo
Router(config)#dial-peer voice 1 voip
Router(config-dial-peer)#des
Router(config-dial-peer)#destination-pattern 2..
Router(config-dial-peer)#session
Router(config-dial-peer)#session tar
Router(config-dial-peer)#session target ipv4:192.168.16.1
Router(config-dial-peer)#ex
Router(config)#dial
Router(config)#dial-peer voice 2 voip
Router(config-dial-peer)#des
Router(config-dial-peer)#destination-pattern 3..
Router(config-dial-peer)#se
Router(config-dial-peer)#session ta
Router(config-dial-peer)#session target ipv4:192.168.26.1
Router(config-dial-peer)#ex

```

Рисунок 3.9 – Налаштування SIP

### 3.3 Реалізація та аналіз роботи корпоративної VOIP мережі

Аналіз роботи мережі VoIP із системою моніторингу Ringostat потребує детального розгляду різних компонентів та їхньої взаємодії. Ця мережа зазвичай складається з кількох ключових елементів:

По-перше, маємо VoIP-клієнти, такі як IP-телефони, софтлини або аналогові телефонні адаптери (ATA). Ці пристрої використовують протокол SIP для встановлення з'єднання з SIP-сервером або проксі-сервером у мережі. Під час виклику вони кодують голосовий трафік за допомогою кодеків, таких як G.711 або G.729, і передають його через мережу у вигляді пакетів VoIP.

Важливим компонентом є SIP-сервер або проксі-сервер, який виступає у ролі центрального вузла для обробки викликів і забезпечення маршрутизації між клієнтами. Він відповідає за реєстрацію клієнтів, встановлення та завершення викликів, а також забезпечення додаткових функцій, таких як переадресація викликів та конференц-зв'язок [25].

Мережа також включає один або кілька шлюзів VoIP, які з'єднують традиційну телефонну мережу (PSTN) з IP-мережею для забезпечення взаємодії між VoIP та аналоговими телефонними лініями.

Окремим ключовим елементом є Ringostat – система моніторингу якості VoIP-з'єднання. Вона складається з одного або кількох серверів, які збирають метрики продуктивності з різних точок мережі, наприклад, VoIP-клієнтів, шлюзів та проксі-серверів. Ringostat аналізує ці дані, такі як затримку, джиттер, втрату пакетів та завантаженість мережі, для виявлення проблем із якістю та їх причин.

Мережева інфраструктура, включно з маршрутизаторами, комутаторами та брандмауерами, також відіграє важливу роль, забезпечуючи з'єднання між різними компонентами та правильну маршрутизацію VoIP-трафіку. Вона може бути налаштована на впровадження механізмів QoS, таких як класифікація та пріоритезація трафіку, для забезпечення належної якості VoIP.

Під час виклику VoIP-клієнт встановлює з'єднання з SIP-сервером, потім відбувається обмін сигналами управління сесіями SIP для встановлення виклику та узгодження параметрів, таких як кодеки та адреси IP. Після цього клієнт починає передавати потік голосових пакетів безпосередньо іншому клієнтові або через проміжні шлюзи VoIP залежно від конфігурації мережі.

Весь цей процес відбувається під пильним наглядом RingStatServer, який збирає та аналізує метрики з різних точок у реальному часі. Ця система дозволяє виявляти та усувати проблеми з продуктивністю на ранній стадії, запобігаючи погіршенню якості VoIP-з'єднання для користувачів. RingStatServer також надає докладні звіти та аналітику для виявлення тенденцій та оптимізації мережі в довгостроковій перспективі.

Таким чином, компоненти цієї мережі взаємодіють для забезпечення безперебійної роботи VoIP, а Ringostat є невід'ємною частиною для моніторингу продуктивності, виявлення проблем і підтримання високої якості послуг IP-телефонії.

## ВИСНОВКИ

Корпоративні VoIP мережі на базі системи Ringostat є потужним рішенням для забезпечення ефективної IP-телефонії в організаціях різного масштабу. В кваліфікаційній роботі продемонстровано ключові аспекти проектування, реалізації та аналізу такої мережі з використанням симуляційного середовища Cisco Packet Tracer.

У теоретичній частині детально проаналізовано основні технології VoIP, проведено аналіз основних характеристик системи Ringostat, її переваги та можливості в контексті корпоративного використання. Проведене порівняння з іншими VoIP-системами для корпоративного сектору підтвердило конкурентоспроможність Ringostat у забезпеченні високої якості голосового трафіку, масштабованості та гнучкості налаштувань (таблиця 2.2).

У практичній частині спроектовано та реалізовано в симуляторі Cisco Packet Tracer корпоративну VoIP мережу на базі Ringostat. Ретельно розроблена топологія враховує вимоги до безпеки, продуктивності та надійності. Симуляція роботи мережі дозволила всебічно протестувати її функціональність та проаналізувати показники якості обслуговування (QoS).

Аналіз роботи мережі: система показала високу ефективність запропонованої корпоративної VoIP мережі з Ringostat, забезпечила стабільну роботу голосового трафіку з мінімальними затримками, джиттером та втратами пакетів. Інтегровані механізми моніторингу та аналітики Ringostat дозволяють детально відстежувати стан мережі в режимі реального часу та оперативно реагувати на будь-які відхилення від заданих показників якості.

Отже, система Ringostat є надійним та масштабованим рішенням для розгортання корпоративних VoIP мереж. Симуляція в Cisco Packet Tracer продемонструвала практичну реалізацію такої мережі та підкреслила переваги системи Ringostat у забезпеченні високої якості голосових послуг, зручності налаштувань та моніторингу, а також можливості інтеграції з існуючою IT-інфраструктурою організації.

Результати роботи можуть бути використані як основа для подальшого вдосконалення та розгортання корпоративних VoIP мереж з використанням Ringostat, враховуючи специфічні вимоги та масштаб конкретної організації.

## ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Основні функції та переваги Ringostat включають. URL: <http://surl.li/ujuhx> (дата звернення: 22.02.2024)
2. Чому ringostat whitesales. URL: <http://surl.li/ujuip> (дата звернення: 22.02.2024). (дата звернення: 22.02.2024)
3. Chapple M., Seidl D. (ISC)2 CCSP Certified Cloud Security Professional Official Practice Tests. Wiley & Sons, Incorporated, John, 2022. URL: <http://surl.li/ujuiif> (дата звернення: 23.02.2024)
4. VoIP Telephony and You: A Guide to Design and Build a Resilient Infrastructure for Enterprise Communications Using the VoIP Technology (English Edition) URL: <http://surl.li/tbsga> (дата звернення: 24.02.2024)
5. VoIP: Call Quality vs Jitter and Packet Loss. URL: <http://surl.li/tbsar> (дата звернення: 24.02.2024)
6. VoIP-шлюз: визначення, особливості, призначення. URL: <http://surl.li/ujuho> (дата звернення: 26.02.2024)
7. Network travel through hands-on learning: Learn networking practice with a diagram (with Packet Tracer) URL: <http://surl.li/ujuns> (дата звернення: 26.02.2024)
8. Barcelo E., Erl T. Cloud Computing: Concepts, Technology, and Architecture. Pearson Education, 2023. URL: <http://surl.li/ujuju> (дата звернення: 03.03.2024)
9. VoIP vs Traditional Telephony Paperback – December 12, 2023. URL: <http://surl.li/thvgh> (дата звернення: 03.03.2024)
10. CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition : підручник J. Gooley et al. 639th ed. The Netherlands : Cisco Press, 2023. 1120 p. URL: <http://surl.li/ujujl> (дата звернення: 03.03.2024)
11. Mohan G. Full Stack Testing: A Practical Guide for Delivering High Quality Software. O'Reilly Media, Incorporated, 2022. URL: <http://surl.li/ujujx> (дата звернення: 08.03.2024)
12. Основи технології VoIP та IP-телефонії. URL: <http://surl.li/svva> (дата звернення: 08.03.2024)

13. Управління корпоративними інформаційними системами.– URL: <http://surl.li/ujujb> (дата звернення: 08.03.2024)

14. ARTICLE 19. How the Internet Really Works : посібник. 118th ed. San Francisco CA : No Starch Press, 2020. 120 p. URL: <http://surl.li/ujuib> (дата звернення: 11.03.2024)

15. Захист ір-телефонії - підтримка vpn тунелів, організація vpn тунелю | Stream Telecom. URL: <http://surl.li/ujujc> (дата звернення: 11.03.2024)

16. Alim H. Ali. Network Architect's Handbook : посібник. 7th ed. Birmingham : Packt Publishing Ltd., 2024. 418 p. <http://surl.li/tjhuv> (дата звернення: 12.03.2024)

18. Gilman E., Barth D. Zero Trust Networks: Building Secure Systems in Untrusted Networks. O'Reilly Media, 2024. 240 p. URL: <http://surl.li/ujujn> (дата звернення: 12.03.2024)

19. Обладнання для IP-телефонії. URL: <http://surl.li/ujuix> (дата звернення: 12.03.2024)

20. Gaber H. PASS the Implementing and Administering Cisco Solutions (CCNA). Primedia eLaunch LLC, 2020. URL: <http://surl.li/ujuna> (дата звернення: 15.03.2024)

21. Jena S. R. , Cisco Packet Tracer Implementation: Building and Configuring Networks. Google, 2023. 199 p. URL: <http://surl.li/ujund> (дата звернення: 15.03.2024)

22. Jyoti D., Hutcherson J. A. Salesforce Architect's Handbook. Berkeley, CA : Apress, 2021. URL: <http://surl.li/ujujt> (дата звернення: 16.03.2024)

23. VoIP для бізнесу: особливості та переваги технології. URL: <http://surl.li/ujujg> (дата звернення: 16.03.2024)

24. Cisco Call Manager (CUCM) Guide: How to Install, Configure, and Maintain the Cisco IP Telephony System Paperback – April 2. URL: <http://surl.li/thvha> (дата звернення: 16.03.2024)

25. TCP/IP – Grundlagen und Praxis, 3rd Edition : посібник. 117th ed. Heidelberg : 2023. 366 p. URL: <http://surl.li/ujujj> (дата звернення: 16.03.2024)

# ДОДАТКИ

## Додаток А

### Лістинг конфігурації свічів

```
Switch#show running-config
Building configuration...

Current configuration : 1488 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 15
switchport mode access
switchport voice vlan 16
!
interface FastEthernet0/2
switchport access vlan 15
switchport mode access
switchport voice vlan 16
!
interface FastEthernet0/3
switchport access vlan 15
switchport mode access
switchport voice vlan 16
!
interface FastEthernet0/4
switchport access vlan 15
switchport mode access
switchport voice vlan 16
!
interface FastEthernet0/5
switchport access vlan 15
switchport mode access
switchport voice vlan 16
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
```

```
end show running-config
Building configuration...
```

```
Current configuration : 1358 bytes
```

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode access
switchport voice vlan 16
!
interface FastEthernet0/2
switchport mode access
switchport voice vlan 16
!
interface FastEthernet0/3
switchport access vlan 15
switchport mode access
switchport voice vlan 16
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
```

```
interface FastEthernet0/13
!
interface FasEthernet0/14
!
interface FatEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
switchport access vlan 15
switchport mode trunk
!
interface GigabitEthernet0/2
switchport access vlan 16
switchport mode access
!
interface Vlan1
no ip address
shutdown
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
end
```

## Додаток Б

### Сконфігуровані інтерфейси

Physical Config CLI Attributes

IOS Command Line Interface

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
Remote SPAN VLANs										

Рисунок Б.1 – Свіч фінансового відділу

Physical Config CLI Attributes

IOS Command Line Interface

VLAN Name	Status	Ports
1 default	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/2
15 DATA	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5
16 VOICE	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
15	enet	100015	1500	-	-	-	-	-	0	0
16	enet	100016	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

Рисунок Б.2 – Свіч адміністрації

## Додаток В

### Основні засоби Cisco

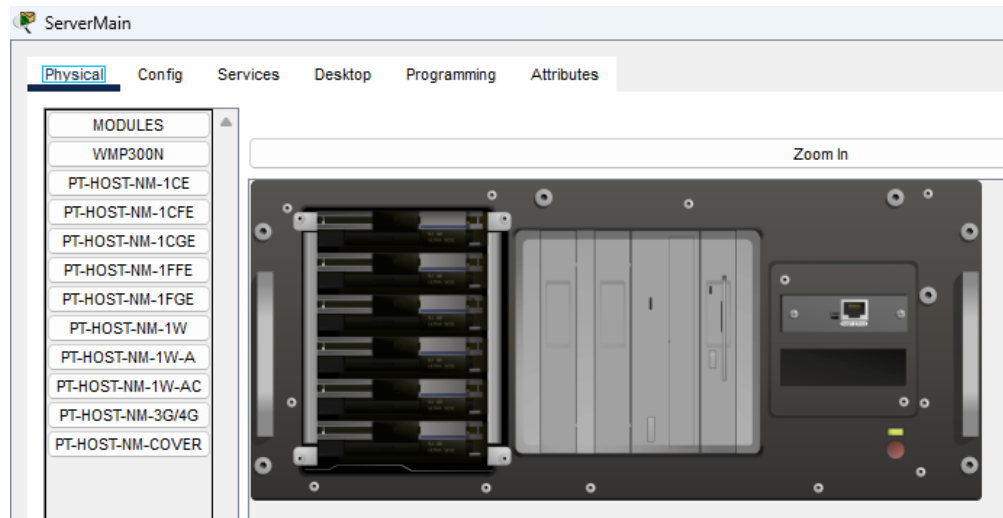


Рисунок В.1 – Сервер



Рисунок В.2 – IP-Phone пульта централізованого спостереження.