Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Навчально-науковий
інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

здобувача Пащенко Ірини Сергіївни
(ПІБ)

академічної групи 123-22ск-1
(шифр)

спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

за освітньо-професійною програмою Комп'ютерна інженерія
(офіційна назва)

на тему «Кіберфізична система IP-телефонії туристичної компанії з детальним налаштуванням корпоративній мережі»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц. Сергєєва К. Л.			
спеціальної частини	доц. Сергєєва К. Л.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2025

ЗАТВЕРДЖЕНО:

завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)

_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)
« » _____ 2025 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

здобувача Пащенко І.С. **академічної групи** 123-22ск-1
(прізвище та ініціали) (шифр)

спеціальності 123 Комп'ютерна інженерія

за освітньо-професійною програмою Комп'ютерна інженерія
(офіційна назва)

на тему «Кіберфізична система IP-телефонії туристичної компанії з детальним налаштуванням корпоративній мережі»

затверджену наказом ректора НТУ «Дніпровська політехніка» від 05.05.2025 № 336-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел розглянути комп'ютерну систему туристичної компанії	10.05.2025
Формування вимог і розробка апаратної частини	Сформулювати найменування й призначення комп'ютерної системи, висунути технічні вимоги до неї. Виконати розробку апаратної частини комп'ютерної системи.	30.05.2025
Розробка корпоративної мережі	Побудувати в Packet Tracer типову мережну топологію туристичної компанії з VLAN-сегментацією	10.06.2025
Розробка компонента системи	Розробити системи управління IP-телефонією	20.06.2025

Завдання видано _____ доц. Сергєєва К. Л.
(підпис керівника) (прізвище, ініціали)

Дата видачі 25.02.2025

Дата подання до екзаменаційної комісії 20.06.2025

Прийнято до виконання _____ Пащенко І.С.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 76 с., 21 рис., 9 табл., 1 додаток, 22 джерел.

IP-ТЕЛЕФОНІЯ, КОРПОРАТИВНА МЕРЕЖА, БЕЗПЕКА, VLAN, ЯКІСТЬ ОБСЛУГОВУВАННЯ.

Об’єкт розробки – кіберфізична система IP-телефонії для потреб туристичної компанії, яка включає у себе апаратно-програмний комплекс з передачею голосового трафіку через IP-мережу та логічно структуровану корпоративну мережу з підтримкою якості обслуговування (QoS), VLAN-сегментації, DHCP, NAT і захищеного доступу.

Мета роботи – створення надійної, безпечної та масштабованої комунікаційної інфраструктури, яка забезпечує високоякісний голосовий зв’язок і захист даних для туристичної компанії.

Для досягнення мети необхідно провести аналіз сучасних технологій IP-телефонії. Використано програмне забезпечення Cisco Packet Tracer для моделювання та тестування мережі, а також VoIP-обладнання умовного виробника з підтримкою SIP-протоколу.

У ході роботи розроблено структурну модель корпоративної мережі компанії з виділенням віртуальних локальних мереж для голосового і службового трафіку, реалізовано маршрутизацію з дотриманням принципів безпеки, впроваджено сервер IP-телефонії з підтримкою SIP-протоколу, а також засоби керування якістю обслуговування. Новизна полягає в інтеграції IP-телефонії у вже наявну мережеву інфраструктуру із впровадженням кіберфізичних механізмів зворотного зв’язку, моніторингу та автоматичного керування навантаженням.

Виконано розрахунок пропускної здатності мережі для кодека G.711, з урахуванням накладних витрат Ethernet та протоколів IP/UDP/RTP.

Область застосування – туристичні компанії з кількома офісами, високими обсягами дзвінків і потребою в безпечній комунікації.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

КС – комп’ютерна система;

ПК – персональний комп’ютер;

КМ – корпоративна мережа;

КФС – кіберфізична система;

CRM – система управління клієнтськими даними;

VLAN – англ. Virtual Area Network, віртуальна локальна мережа;

FILIAL – англ. Local area network, локальна мережа;

ISP – англ. Internet Service Provider, постачальник Інтернет;

VoIP – англ.Voice over IP, IP-телефонія;

ВСТУП

У сучасному світі ефективна комунікація є ключовим фактором успіху будь-якої компанії, особливо у туристичній галузі, де якість обслуговування клієнтів та швидкість відповіді на запити є критично важливими. Розвиток інформаційних технологій призвів до широкоого використання IP-телефонії, яка пропонує значні переваги порівняно з традиційною телефонією, такі як зниження витрат, масштабованість та інтеграція з іншими корпоративними системами.

На сьогоднішній день IP-телефонія активно використовується у різних галузях, включаючи туризм. Провідні компанії у сфері інформаційних технологій, такі як Cisco, Avaya та Mitel, пропонують рішення, що дозволяють організаціям реалізувати голосові комунікації через IP-мережі. Ці рішення забезпечують не лише базові функції телефонії, але й розширені можливості, такі як відеоконференції, інтеграція з CRM-системами та аналітика дзвінків. Наприклад, Cisco Unified Communications Manager (CUCM) дозволяє автоматизувати обробку дзвінків і інтегрувати їх із бізнес-процесами.

Однак впровадження IP-телефонії у туристичних компаніях має свої особливості. Туристичні компанії часто мають розподілену структуру з кількома офісами, що вимагає надійної та масштабованої мережевої інфраструктури. Крім того, необхідність обробки великих об’ємів даних, включаючи інформацію про клієнтів та бронювання, вимагає високого рівня безпеки та захисту даних [10]. Наприклад, захист від кіберзагроз, таких як підслуховування чи атаки типу відмови в обслуговуванні (DoS), є критично важливим для забезпечення конфіденційності клієнтських даних [14].

Глобально спостерігається тенденція до інтеграції IP-телефонії з іншими корпоративними системами, такими як системи управління відносинами з клієнтами (CRM), наприклад, Salesforce, для підвищення ефективності обслуговування клієнтів. Це дозволяє операторам кол-центру отримувати доступ до історії клієнтів під час дзвінків, що сприяє персоналізації

пропозицій. Також зростає увага до безпеки, оскільки голосові комунікації можуть бути мішенню для кібератак, таких як SIP-флуд чи підслуховування [14].

Іншою важливою тенденцією є використання хмарних технологій для IP-телефонії, таких як Microsoft Teams або Cisco Webex, які дозволяють компаніям зменшити витрати на інфраструктуру та підвищити гнучкість у масштабуванні комунікацій. Хмарні рішення надають доступ до просунутих функцій, таких як відеоконференції, без необхідності значних інвестицій у апаратне забезпечення. Крім того, використання кодеків, таких як G.729, дозволяє економити пропускну здатність, що є важливим для мереж із обмеженими ресурсами.

Актуальність цієї роботи полягає у необхідності створення сучасної, надійної та безпечної системи IP-телефонії для туристичної компанії, яка відповідає специфічним вимогам цієї галузі. Туристичні компанії з розподіленими офісами потребують швидкої обробки клієнтських запитів, особливо в пікові періоди, коли кількість дзвінків може досягати 100–150 на годину. Розробка такої системи дозволить компанії покращити якість обслуговування клієнтів, знизити витрати на комунікації на 30–40% порівняно з традиційною телефонією та забезпечити захист передаваємої інформації [12].

Обґрунтування виконання цієї роботи лежить у зростаючому попиті на рішення IP-телефонії у туристичній галузі, а також у необхідності адаптувати ці рішення до специфічних потреб компаній із розподіленою структурою. Проєкт включає розробку та аналіз мережевої топології, яка складається з п’яти локальних мереж (FILIAL1–FILIAL5), трьох VLAN у FILIAL3 (VLAN10, VLAN20, VLAN30) і серверів (DNS, HTTP, TFTP), що забезпечує відповідність найвищим стандартам продуктивності та безпеки.

Метою цієї кваліфікаційної роботи є розробка корпоративної мережі для кіберфізичної системи IP-телефонії туристичної компанії, яка забезпечує високоякісні голосові комунікації, безпеку та масштабованість. Система повинна підтримувати до 100 одночасних дзвінків із затримкою <150 мс,

джітером <30 мс і втратою пакетів <1%, як рекомендовано стандартом ITU-T G.114 [1].

Результати цієї роботи можуть бути застосовані у туристичних компаніях різного розміру, а також у інших галузях, які вимагають надійних і безпечних голосових комунікацій, таких як роздрібна торгівля, охорона здоров'я та освіта. Наприклад, інтеграція з Salesforce дозволяє автоматизувати обробку клієнтських запитів, що підвищує ефективність роботи кол-центру.

Дипломна робота базується на попередніх дослідженнях у сфері IP-телефонії та корпоративних мереж, використовуючи найкращі практики та сучасні технології, такі як VLAN, VLSM і протоколи безпеки (SRTP, ACL, ISP, SSH) [6, 9, 10]. Вона також враховує вимоги та стандарти інформаційної безпеки у контексті кіберфізичних систем, адаптованих до потреб туристичної галузі [15]. Робота розширює підходи до впровадження IP-телефонії, запропоновані в літературі, шляхом створення комплексного рішення, яке поєднує аналіз, проєктування, тестування та рекомендації для туристичних компаній [12].

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умов застосування системи

Туристична галузь належить до сфери обслуговування, яка активно використовує сучасні інформаційно-комунікаційні технології для підвищення ефективності взаємодії з клієнтами, обробки запитів, здійснення бронювань та надання консультаційних послуг. З огляду на високу динаміку роботи туристичних компаній, оперативний зв’язок між працівниками, менеджерами та клієнтами є критичним чинником у забезпеченні якісного обслуговування та конкурентоспроможності на ринку.

Одним із ключових напрямів цифровізації офісних процесів у туризмі є впровадження IP-телефонії – технології передачі голосового трафіку через мережі на базі протоколу IP. На відміну від традиційної телефонії, IP-телефонія забезпечує зниження витрат, гнучкість масштабування, можливість інтеграції з CRM-системами, а також підтримку мобільності персоналу.

Застосування IP-телефонії у туристичній компанії дозволяє створити єдину централізовану комунікаційну платформу, яка охоплює всі підрозділи, філії та віддалених працівників, включаючи можливість переадресації викликів, запису розмов, автоматичних голосових відповідей (IVR) та організації черг очікування. Це особливо важливо в умовах сезонного навантаження та високого потоку звернень від клієнтів.

Ефективне функціонування IP-телефонії потребує якісної мережевої інфраструктури, яка забезпечує пріоритезацію голосового трафіку, мінімізацію затримок і втрат пакетів, а також гарантовану безпеку передавання даних. У зв’язку з цим, проєктована система повинна бути інтегрована в корпоративну мережу компанії з урахуванням вимог до якості обслуговування (QoS), сегментації (VLAN), централізованого управління (DHCP, NAT), а також із засобами контролю доступу та кіберзахисту.

Таким чином, умови застосування системи визначаються потребами в сучасній цифровій інфраструктурі зв’язку для компаній, що функціонують у сфері туризму, з орієнтацією на масштабованість, надійність та інтегрованість з бізнес-процесами.

Кіберфізичні системи (КФС) – це сучасний напрямок розвитку інформаційних технологій, який уже сьогодні відіграє значну роль у багатьох сферах життя. Вони об'єднують у собі світ цифрових обчислень і фізичних процесів, створюючи складні, але водночас гнучкі й адаптивні системи, які здатні взаємодіяти з навколишнім середовищем в режимі реального часу. В основі КФС лежить поєднання апаратних засобів (датчики, актуатори, мережеве обладнання) з програмним забезпеченням, яке виконує інтелектуальний аналіз даних і автоматичне керування [1].

Такі системи уже довели свою ефективність у сферах енергетики, охорони здоров’я, транспорту, виробництва, а останнім часом і в туристичній галузі. Туризм, як динамічна й сервісно-орієнтована сфера, має особливу потребу в технологіях, які дозволяють швидко реагувати на зміни, покращувати якість обслуговування клієнтів, оптимізовувати витрати та забезпечувати безперервний обмін інформацією.

У сфері туризму КФС відкривають нові горизонти. Наприклад, концепція «розумного готелю» більше не є фантастикою. Системи автоматичного регулювання освітлення, температури, вентиляції та навіть розважального контенту, що налаштовуються під конкретного гостя, стали реальністю завдяки використанню мережі датчиків і підключених пристроїв. Гість може за допомогою смартфона замовити послугу, переглянути карту готелю або проконсультуватися з персоналом – і все це через єдиний зручний цифровий інтерфейс [2]

Окреме місце у таких системах займає IP-телефонія, яка є невід’ємною частиною КФС в організаціях, що активно працюють з клієнтами, партнерами та постачальниками. Вона не тільки дозволяє здійснювати голосовий зв’язок через IP-мережі, але й легко інтегрується з CRM-системами, модулями

бронювання, базами даних. Завдяки цьому співробітники туристичної компанії можуть обробляти вхідні дзвінки, зберігати історію розмов, а також на основі цих даних формувати персоналізовані пропозиції.

КФС не обмежуються лише приміщеннями чи телефонами. Вони також використовуються у транспорті, наприклад, у вигляді систем навігації для туристів, які в реальному часі повідомляють про маршрути, затори, визначні місця поблизу. Це особливо зручно в містах, де багато туристичних маршрутів і важлива кожна хвилина пересування

Ще однією перспективною сферою є використання КФС для реалізації віртуальних турів та елементів доповненої реальності. Наприклад, за допомогою мобільного пристрою турист може "побачити", як виглядала архітектурна пам’ятка у минулому або отримати текстову та аудіоінформацію про експонати в музеї. Це створює нову якість взаємодії з туристичним об’єктом, залучаючи більше клієнтів та відкриваючи нові способи монетизації.

Важливо розуміти, що всі ці технології, від IP-телефонії до інтерактивних карт, не можуть повноцінно працювати без якісної мережевої інфраструктури, яка має бути надійною, масштабованою та безпечною. У випадку з IP-телефонією особливу роль відіграє низька затримка сигналу та стійкість до втрати пакетів, що напряму впливає на якість зв’язку.

Таким чином, КФС виступають не лише як набір окремих технологій, а як цілісна інтелектуальна система, що створює новий рівень зручності, безпеки та автоматизації. Для туристичної компанії це означає не просто інновації, а можливість запропонувати клієнту сучасний, персоналізований сервіс, який відповідає очікуванням цифрової епохи.

1.2 Організаційна структура туристичної компанії

Організаційна структура туристичної компанії є ключовим фактором, що безпосередньо впливає на архітектуру та логіку побудови кіберфізичної системи IP-телефонії. Врахування структури компанії дає змогу розробити не просто технічну мережу, а цілісну, логічно впорядковану інформаційну

систему, яка ефективно задовольняє потреби кожного підрозділу. Особливу роль у цьому процесі відіграє правильна сегментація мережі, безпека даних, розподіл адресного простору, а також відповідність конфігурації обладнання до функціональних завдань, які виконує кожен відділ.

В межах даної роботи розглядається туристична компанія з головним офісом у місті Дніпро та декількома філіями, розташованими в інших регіонах України. Такий географічно розподілений формат вимагає побудови масштабованої, гнучкої та безпечної мережевої інфраструктури, яка дозволяє як централізоване управління ресурсами, так і автономну роботу кожного офісу в разі потреби. Особливо це важливо для реалізації IP-телефонії, яка має функціонувати надійно та безперервно, незалежно від місця розташування користувача.

Організаційна структура туристичної компанії є ієрархічною, із чітким розподілом функцій між підрозділами та посадовими особами (рис. 1.1).

Рисунок 1.1 – Організаціна структура туристичної компанії

На найвищому рівні управління знаходиться генеральний директор, який здійснює загальне керівництво підприємством і координує роботу всіх відділів.

У структурі підприємства виокремлено такі основні підрозділи:

– маркетинговий відділ, який відповідає за просування туристичних продуктів та рекламну діяльність. У складі відділу працює менеджер з реклами, що займається створенням рекламних кампаній та взаємодією із ЗМІ;

– юридична служба, представлена юристом, забезпечує правовий супровід діяльності компанії, контроль договорів та відповідність нормативно-правовим актам;

– кадровий відділ, до складу якого входить HR-менеджер, здійснює управління персоналом, підбір кадрів, навчання та розвиток співробітників;

– бухгалтерія, представлена бухгалтером, забезпечує ведення фінансового обліку, підготовку звітності та контроль фінансових потоків.

Центральним функціональним підрозділом є туристичний відділ, очолюваний начальником туристичного відділу. У його підпорядкуванні працюють:

– менеджер з міжнародного туризму, який організовує подорожі за кордон, співпрацює з іноземними партнерами та туристичними операторами;

– менеджер з внутрішнього туризму, відповідальний за організацію подорожей територією України;

– менеджери з продажів у філіях компанії, що забезпечують реалізацію туристичних послуг у регіональних представництвах;

– менеджери за напрямами, які спеціалізуються на окремих туристичних продуктах чи регіонах, підтримують зв’язок із клієнтами та готують пропозиції відповідно до потреб ринку.

Керівництво виконує управлінські функції, контролює роботу інших відділів та взаємодіє з партнерами. Їхня комунікація повинна бути пріоритетною, захищеною (наприклад, через VPN-канали) та максимально

зручною. Це також включає доступ до внутрішніх звітів, моніторингу мережі, IP-телефонії та систем відеоконференцій.

Туристичний відділ є центральним у діяльності компанії, оскільки він безпосередньо взаємодіє з клієнтами. Співробітники цього відділу активно використовують IP-телефонію, CRM-системи, онлайн-чати, електронну пошту та інші канали зв'язку. Для цього необхідна стабільна телефонна система з підтримкою функцій IVR, автоматичного запису дзвінків, швидкого переадресування та інтеграції з базами даних клієнтів;

– технічна підтримка; надає допомогу як внутрішнім користувачам (співробітникам компанії), так і зовнішнім клієнтам, які можуть мати запитання щодо роботи сайту, бронювання або інших технічних аспектів. Працівники цього відділу повинні мати доступ до внутрішніх серверів, панелей адміністрування IP-телефонії, а також каналів моніторингу мережі;

– бухгалтерія: оперує конфіденційними фінансовими даними, тому потребує окремого ізольованого мережевого сегмента, який би забезпечував як обмеження доступу, так і повну захищеність переданих даних. Крім того, необхідна можливість захищеного зв'язку з банківськими системами, клієнтами та державними службами.

1.3 Стислі відомості про технології збору та передачі інформації в КС туристичної компанії

У сучасних туристичних компаніях інформація є основою для здійснення операційної, комунікаційної та аналітичної діяльності. Ефективне функціонування комп'ютерної системи туристичного агентства неможливе без впровадження технологій, що забезпечують своєчасний збір, обробку, зберігання та передачу даних у реальному часі. До основних технологій, які використовуються в такій системі, належать:

– мережеві технології передачі даних: у корпоративній мережі застосовуються як дротові (Ethernet 100/1000 Мбіт/с), так і бездротові (Wi-Fi 5/6) стандарти зв'язку. Для зовнішньої комунікації використовується доступ до

Інтернету через оптоволоконні канали. Також впроваджуються механізми VLAN для логічного розділення трафіку (офісний, голосовий, гостьовий), що сприяє підвищенню безпеки та ефективності передачі даних;

– IP-телефонія: збір голосових звернень від клієнтів відбувається через IP-телефонію на базі протоколів SIP та RTP. Вся передача викликів і метаданих здійснюється у вигляді IP-пакетів. Сеанси ініціалізуються через SIP-сервери, де також відбувається маршрутизація викликів, збереження логів, автентифікація та контроль якості обслуговування (QoS);

– CRM-системи та бази даних: дані про клієнтів, бронювання, платежі та запити збираються через інтегровану CRM-платформу, яка є центральним вузлом інформаційної взаємодії. Внутрішні сервіси працюють із базами даних (MySQL, PostgreSQL або MS SQL Server), розміщеними локально або в хмарному середовищі.

– Web-технології: через веб-інтерфейси та мобільні додатки здійснюється онлайн-бронювання турів, перегляд маршрутів, запити зворотного зв'язку. Інформація передається через протоколи HTTPS, REST API та WebSocket для забезпечення інтерактивної взаємодії з клієнтами.

– технології моніторингу та логування: для забезпечення надійності функціонування системи застосовуються сервіси збору телеметрії (наприклад, SNMP, NetFlow, syslog), які дозволяють в реальному часі контролювати стан мережі, серверів, IP-ліній та виявляти аномалії.

– технології інформаційної безпеки: передача даних супроводжується шифруванням (TLS, SRTP), автентифікацією (RADIUS, LDAP), а також фільтрацією доступу через міжмережеві екрани (ACL, ZPF). VPN-технології (ISPec, SSL VPN) забезпечують безпечний віддалений доступ до корпоративних ресурсів.

1.4 IP-телефонія: основні принципи роботи

IP-телефонія (інтернет-телефонія) – це технологія передачі голосу через цифрові мережі, зокрема ті, що функціонують на базі протоколу IP (Internet

Protocol). Сучасна тенденція демонструє поступове витіснення класичної телефонії цією технологією завдяки простоті впровадження, економічності викликів, зручності налаштувань, стабільній якості звуку та достатньому рівню захисту комунікацій. Розгляд функціонування IP-телефонії в цій роботі базується на моделі взаємодії відкритих систем (OSI), з акцентом на поступове вивчення - від нижчих (фізичного і канального) до вищих рівнів [1].

1.4.1 Основи роботи IP-телефонії

Під час ініціації дзвінка голос користувача трансформується у цифровий сигнал, який стискається у пакети даних. Ці пакети надсилаються через мережу з комутацією пакетів, переважно IP-мережу, а після доставки до кінцевого пристрою декодуються назад у звуковий сигнал (рис. 1.2). Такий обмін можливий завдяки використанню цілого ряду мережевих протоколів, які забезпечують правильну обробку, передачу та відтворення аудіоінформації.

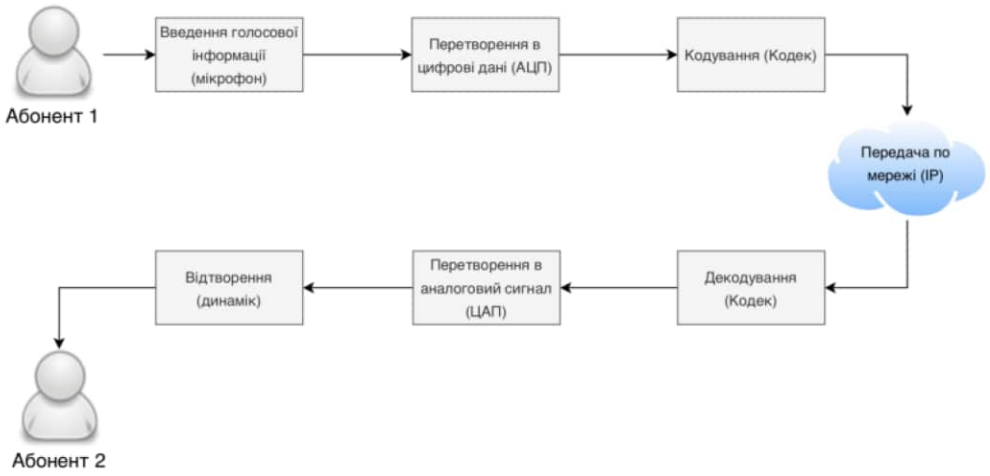


Рисунок 1.2 – Передача годосу через Інтернет

Протокол у цьому контексті можна розглядати як систему правил, що дозволяє обом учасникам зв’язку розуміти одне одного й успішно обмінюватися голосовими даними [2].

1.4.2 Переваги IP-телефонії в порівнянні з традиційною телефонією

У звичайній телефонній мережі встановлення з'єднання здійснюється через комутацію каналів, яка передбачає виділення окремої фізичної лінії для ведення розмови. Голос передається безпосередньо через цю виділену лінію, що є менш гнучким підходом.

Натомість IP-телефонія є більш економним варіантом для обох сторін – провайдерів послуг і кінцевих користувачів. Вона застосовує методи стиснення голосових даних, що дозволяє ефективніше використовувати пропускну здатність мережі. Більше того, поширеність інтернет-доступу дає змогу значно знизити витрати на створення інфраструктури зв'язку або повністю уникнути додаткових витрат.

Таблиця 1.1 – Порівняння IP-телефонії та традиційної телефонії

Показник	IP-телефонія	Традиційна телефонія
Вартість дзвінків	Низька (Інтернет)	Висока (аналогові лінії)
Гнучкість	Висока (легке додавання користувачів)	Низька (фізичні лінії)
Інтеграція з CRM	Підтримується	Не підтримується
Безпека	SRTP, TLS, ISP	Обмежена
Мобільність	Софтфони, віддалений доступ	Обмежена
Пропускна здатність	8–64 кбіт/с (залежить від кодека)	Фіксована, висока

Технологія IP-телефонії пропонує ряд переваг порівняно з традиційною телефонією:

– економія на міжнародних та міжміських дзвінках;

– висока якість звуку завдяки сучасним кодекам;

– можливість інтеграції з іншими корпоративними системами;

– гнучкість налаштувань та масштабування.

IP-телефонія для офісу – це вигідне рішення з точки зору тарифів, особливо для частих міжміських та міжнародних дзвінків. Вона значно

скорочує витрати на зв’язок порівняно з традиційними телефонними системами.

Організація IP-телефонії не потребує свердління стін чи прокладення додаткових кабелів, що робить її встановлення швидким та менш трудомістким. Телефонія працює через інтернет, тому легко інтегрується в існуючу інфраструктуру офісу.

Крім того, функціональні можливості IP-телефонії значно ширші за звичайні телефонні лінії. Можливості включають підключення гарячих ліній, запис дзвінків, переадресацію викликів та ведення докладної статистики. Це сприяє підвищенню якості обслуговування і контролю над процесами комунікації.

Для організації IP-телефонії з нуля потрібно врахувати вибір постачальника послуг, налаштування обладнання та інтеграцію телефонних номерів. Такий підхід дозволить швидко та ефективно перейти на сучасну систему зв’язку, яка оптимізує бізнес-процеси вашого офісу.

Окрім очевидних переваг IP-телефонії, таких як зниження витрат і масштабованість, ця технологія також дозволяє досягти вищої якості голосових комунікацій. Це стало можливим завдяки трьом ключовим чинникам:

– еволюція серверного ПЗ: сучасні телефонні сервери постійно оновлюються, стаючи більш стійкими до типових проблем IP-мереж, таких як затримки чи втрата пакетів;

– контроль у приватних мережах: у власних (корпоративних) мережах адміністратори можуть гнучко керувати параметрами мережі, а саме обмежувати кількість активних з’єднань, резервувати пропускну здатність, що зменшує затримки;

– розвиток мережевих протоколів: впровадження нових рішень, наприклад RSVP (протокол резервування смуги пропускання), дозволяє підвищити стабільність і якість голосового зв’язку.

IP-телефонія також вирішує проблему зайнятої лінії – переадресація викликів або перенаправлення в режим очікування можуть бути налаштовані за допомогою декількох конфігураційних команд на програмній АТС [1].

1.4.3 Якість обслуговування в IP-телефонії (Quality of Service – QoS)

У TCP/IP-мережах забезпечення стабільної якості для трафіку, чутливого до затримок, не є стандартною функцією. Протокол TCP гарантує надійність доставки, але не забезпечує стабільність часу передачі. У свою чергу, UDP зменшує затримки, проте не забезпечує доставку кожного пакета. Оскільки голосовий зв’язок чутливий до затримок і втрат, в IP-телефонії необхідно впроваджувати додаткові методи для покращення якості.

Ключовими параметрами QoS є пропускна здатність і затримка. Остання – це час від моменту відправлення пакета до його прийому. Додатково оцінюється доступність мережі та її надійність, що вимірюються за допомогою статистичних показників або рівнем використання ресурсів.

Щоб підвищити якість голосового зв'язку, застосовуються такі технології:

– зміна маршрутів: при перевантаженні ліній передача може відбуватись через альтернативні шляхи;

– резервування пропускної здатності: виділення ресурсів каналу під час виклику;

– пріоритизація трафіку: маркування пакетів відповідно до важливості й обробка їх за пріоритетом.

Європейський інститут стандартизації телекомунікацій ETSI пропонує розділити мережі IP-телефонії на чотири класи за якістю обслуговування QoS, основним показником якого є затримка пакетів. У Рекомендації ITU-T G.114 для телефонної мережі загального користування наведено близькі до градацій ETSI затримки, які відповідають різним видам зв'язку:

– до 150 мс – вихідна норма;

– до 260 мс – затримка дільниці супутникового зв'язку;

– до 400 мс – допустима затримка з урахуванням ділянки супутникового зв'язку;

– понад 400 мс – неприпустима затримка.

Існує два типи затримок:

– затримки кодування - виникають під час обробки аудіо в шлюзах або телефонах. Зменшуються шляхом оптимізації кодеків.

– мережеві затримки - залежать від інфраструктури й зменшуються завдяки зменшенню кількості проміжних пристроїв і покращенню каналів зв'язку.

1.4.4 Джиттер

Окрім затримок, в IP-телефонії виникає джиттер – варіація в часі надходження пакетів. Причини його виникнення:

– перевантаження або помилки у роботі мережевого обладнання;

– тривалі затримки сигналу;

– електричні шуми (теплові або фонові).

Щоб зменшити ці коливання, використовується джиттер-буфер – тимчасове сховище для пакетів. Його мета – впорядкувати пакети за часовими мітками та передати їх до декодера з правильним інтервалом.

Розмір буфера може визначатись автоматично або налаштовуватись вручну. Занадто великий буфер збільшує загальну затримку, а занадто малий призводить до втрати пакетів при різких змінах часу доставки.

Саме тут виникає конфлікт інтересів: з точки зору інтернет-провайдера пакети доставлені, а для VoIP-пристрою через перевищення допустимого джиттера, частина з них вважається втраченою. Вже при втраті 1% помітно погіршується якість звуку, при 2% ведення розмови стає важким, а втрати понад 4% роблять спілкування практично неможливим [2].

1.5 Типи VoIP-пристроїв та можливі схеми їх підключення

1.5.1 Класифікація VoIP-пристроїв

VoIP-пристрої можна поділити на кілька основних категорій залежно від їх функціонального призначення, форми інтерфейсу та технологічних особливостей.

1) VoIP-телефони (IP-телефони).

IP-телефони – це пристрої, які зовні нагадують традиційні телефони, але для передачі голосу використовують IP-протоколи. Вони поділяються на два основних типи:

– апаратні IP-телефони: мають власний процесор і операційну систему, підтримують роботу з VoIP-протоколами (SIP, H.323). Підключаються безпосередньо до мережі Ethernet або Wi-Fi. Призначені для офісного використання, де потрібне якісне і стабільне голосове сполучення;

– програмні IP-телефони (Softphones): це програмні додатки, які встановлюються на комп'ютери, планшети, смартфони. Вони використовують комп'ютерну периферію – мікрофон, колонки чи гарнітуру. Softphones є гнучким рішенням, доступним за мінімальних витрат, проте залежать від обчислювальних ресурсів і якості підключення до мережі.

2) Аналогово-цифрові адаптери (ATA).

Аналогово-цифрові адаптери дозволяють підключити традиційні аналогові телефони до VoIP-мережі. ATA перетворює аналоговий голосовий сигнал у цифровий пакет, сумісний з IP-протоколами. Ці пристрої економічно вигідні для користувачів, що хочуть зберегти свої старі телефонні апарати, але при цьому перейти на VoIP.

3) VoIP-шлюзи (VoIP Gateways).

Це більш складні пристрої, які забезпечують інтеграцію VoIP-мережі з традиційними телефонними мережами (PSTN), мобільними мережами тощо. VoIP-шлюзи виконують функцію транскодування та маршрутизації дзвінків між різними типами мереж. Вони широко застосовуються у корпоративних мережах для взаємодії з зовнішніми абонентами.

4) Конференц-телефони VoIP.

Спеціалізовані пристрої, призначені для організації багатоточкових аудіоконференцій. Вони обладнані декількома мікрофонами і високоякісними динаміками, що забезпечують чітку передачу голосу навіть у великих залах.

5) VoIP-гарнітури та бездротові пристрої

Для мобільних і офісних користувачів популярні VoIP-гарнітури, які забезпечують зручність і мобільність. Вони можуть працювати по Bluetooth, Wi-Fi або через USB-підключення до ПК та інших пристроїв.

Таблиця 1.2 – Основні типи VoIP-пристроїв

Тип пристрою	Опис	Сфера використання
IP-телефон	Апаратний VoIP-телефон, підключається безпосередньо до мережі Ethernet через RJ-45	Офісні робочі місця
Softphone (софтфон)	Програмне забезпечення (Zoiper, Linphone, MicroSIP), що імітує функції телефону на ПК	Дистанційна робота, ноутбуки
Адаптер VoIP (ATA)	Аналого-цифровий перетворювач для підключення традиційних телефонів до IP-мережі	Модернізація застарілого обладнання
VoIP-шлюз	Пристрій для інтеграції аналогових ліній або GSM/FXO до IP-телефонії	Інтеграція із зовнішніми каналами зв’язку
SIP-сервер (Call Manager)	Центральний керуючий елемент, маршрутизує дзвінки, керує реєстрацією телефонів	Серверна кімната, хмара
PoE-комутатор	Комутатор з підтримкою Power over Ethernet для живлення IP-телефонів	Інфраструктурне рішення для офісів

1.5.2 Схеми підключення VoIP-пристроїв

Підключення VoIP-пристроїв до мережі і забезпечення їх ефективної роботи можуть реалізовуватись за різними схемами. Вибір архітектури залежить від масштабу організації, специфіки використання і наявної інфраструктури.

1) Пряме підключення до IP-мережі (Peer-to-Peer).

Найпростіша схема передбачає пряме з’єднання двох VoIP-пристроїв безпосередньо через інтернет або локальну мережу. В цьому випадку кожний пристрій має IP-адресу і може здійснювати дзвінки напряму. Схема підходить для малого бізнесу або домашніх користувачів, але не має масштабованості і обмежена функціональністю.

Рисунок 1.3 – Пряме підключення до IP-мережі

Ці пристрої можна підключити за двома схемами (рис. 1.4):

– роутер – IP-телефон;

– роутер – IP-телефон – ПК.

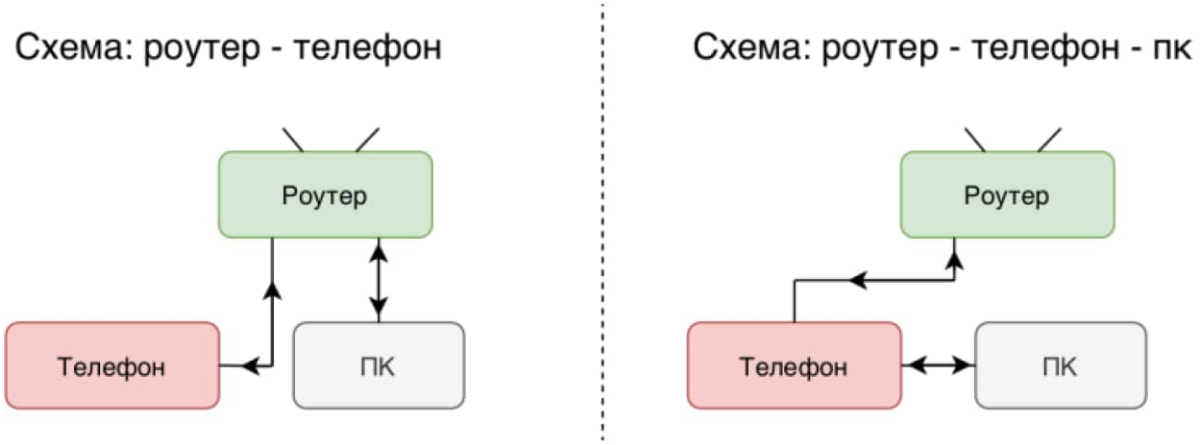


Рисунок 1.4 – Схеми підключення дротових IP-телефлнів

2) Використання SIP-серверів (centralized SIP architecture)

Одним з найпоширеніших підходів є використання SIP-серверів, які виконують функції реєстрації користувачів, маршрутизації дзвінків та управління сесіями. Пристрої реєструються на сервері, отримують своє унікальне ім’я (URI) і взаємодіють через нього. Такі сервіси забезпечують масштабованість, підтримку великої кількості користувачів, а також можуть інтегруватися з внутрішньою телефонною мережею підприємства.

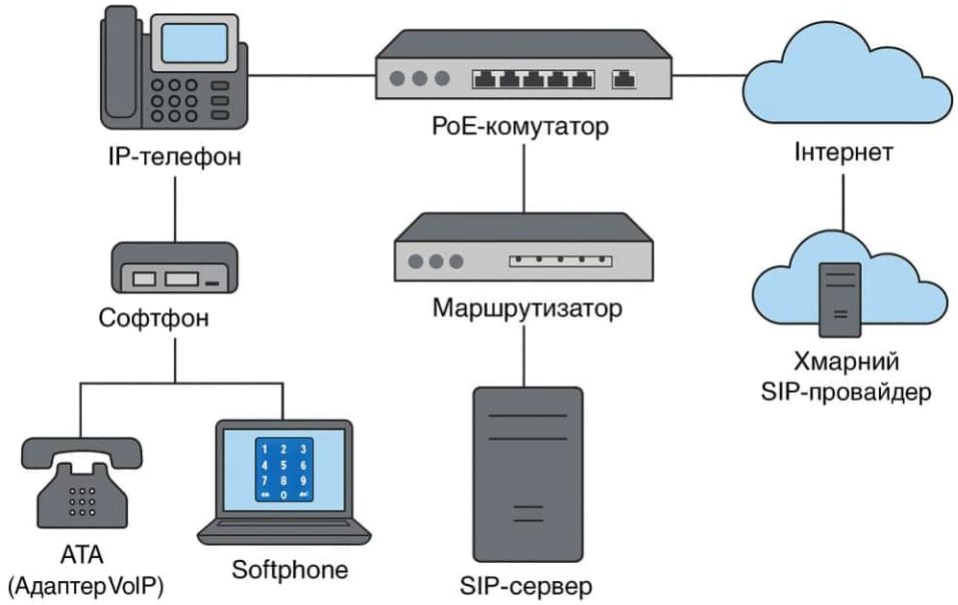


Рисунок 1.5 – Підключення через SIP-сервер

3) Використання VoIP-шлюзів для інтеграції з PSTN.

У великих підприємствах часто виникає потреба сумісності між VoIP і традиційною телефонією. У цьому випадку VoIP-шлюзи з'єднують корпоративну VoIP-мережу з публічною комутаційною мережею. Дзвінки можуть направлятися на звичайні телефони, а вхідні дзвінки з PSTN переадресовуватись у VoIP-систему.

Рисунок 1.6 – Використання VoIP-шлюзів

4) Гібридні схеми з використанням IP-PBX систем.

IP-PBX – це програмні або апаратні телефонні станції, які забезпечують повний цикл обробки дзвінків всередині організації. Вони підтримують всі типи VoIP-пристроїв, дозволяють організовувати внутрішні дзвінки, конференції, голосову пошту, інтеграцію з CRM та інші додаткові сервіси. До IP-PBX можуть підключатись як апаратні IP-телефони, так і програмні клієнти через локальну мережу або VPN.

5) Підключення через Wi-Fi та мобільний Інтернет.

Для мобільних користувачів або віддалених співробітників часто застосовуються бездротові схеми підключення. VoIP-гарнітури і мобільні застосунки можуть підключатися до VoIP-сервісу через Wi-Fi або мобільний інтернет, що забезпечує гнучкість і мобільність робочого процесу.

1.6 Огляд існуючих рішень для побудови IP-телефонії

Розглядаючи сучасні інженерні рішення для побудови систем у сфері IP-телефонії, варто звернути увагу на те, що сьогодні існує великий вибір різноманітних технологій, які дозволяють передавати голосовий зв'язок через комп'ютерні мережі та Інтернет. IP-телефонія, також відома як VoIP (Voice over IP), є однією з найперспективніших технологій останніх років. Вона поступово витісняє традиційні аналогові телефонні системи, адже забезпечує більшу гнучкість, зменшує витрати на зв'язок і дозволяє легко інтегруватися з сучасними цифровими платформами.

На відміну від звичайного телефонного зв'язку, де використовується окрема телефонна мережа, IP-телефонія працює поверх вже існуючої комп'ютерної мережі. Це значно спрощує обслуговування, дозволяє легко масштабувати систему та додавати нових користувачів без додаткових витрат на прокладку окремих ліній. Також IP-телефонія відкриває можливості для використання таких зручних функцій, як переадресація дзвінків, голосова пошта, запис розмов, відеодзвінки тощо.

У контексті роботи туристичної компанії IP-телефонія має особливо важливе значення. Така компанія щодня працює з великою кількістю клієнтів, здійснює дзвінки як всередині країни, так і за кордон, часто в умовах високого навантаження - особливо в сезон активних подорожей. У таких ситуаціях швидкий і стабільний зв'язок є критично важливим. Крім того, налагоджена внутрішня комунікація між працівниками різних відділів (наприклад, продажів, підтримки, бухгалтерії) також грає ключову роль у забезпеченні якісного обслуговування.

Саме тому аналіз сучасних технологій та підходів у сфері IP-телефонії дає можливість обрати найкращі рішення для побудови ефективної кіберфізичної системи зв’язку. Така система повинна бути не лише надійною та стабільною, але й зручною в обслуговуванні, легко розширюватися та адаптуватися до змін у структурі компанії або кількості працівників.

Серед ключових інженерних рішень варто виділити використання протоколів, таких як Session Initiation Protocol (SIP), який слугує для ініціалізації, підтримки та завершення сеансів зв’язку, включаючи голосові дзвінки, відеоконференції та обмін повідомленнями. SIP є гнучким і широко застосовуваним протоколом завдяки своїй модульній структурі, що дозволяє інтегрувати його з різними пристроями, такими як IP-телефони, софтфони та шлюзи. Наприклад, туристична компанія може використовувати SIP для створення віртуального кол-центру, де оператори отримують дзвінки від клієнтів із різних регіонів світу. Протокол Real-time Transport Protocol (RTP) забезпечує передачу аудіо- та відеоданих у реальному часі, гарантуючи синхронізацію, що є критично важливим для уникнення затримок під час розмов. Його супутник, Real-time Transport Control Protocol (RTCP), моніторить якість передачі, надаючи статистику про джітер і втрати пакетів, що дозволяє адміністраторам мережі оперативно реагувати на проблеми.

Інший важливий протокол, H.323, є раннім стандартом для VoIP, розробленим ITU-T, який охоплює набір протоколів для мультимедійного зв’язку. Крім того, Media Gateway Control Protocol (MGCP) використовується для централізованого керування медіашлюзами, популярними у 1990-х роках. Його складність і менша гнучкість порівняно з SIP призвели до поступового витіснення цього протоколу. Проте, в деяких застарілих системах він все ще може бути актуальним та корисним для переходу з аналогових систем, а також дозволяє інтегрувати традиційні телефонні мережі з IP-мережами.

Таблиця 1.3 – Параметри протоколів IP-телефонії

Параметр	SIP	H.323	MGCP
Призначення	Ініціація сеансів	Мультимедіа	Керування шлюзами
Гнучкість	Висока	Низька	Середня
Сумісність	Широка	Обмежена	Специфічна
Складність налаштування	Середня	Висока	Низька
Застосування	Кол-центри, VoIP	Стари системи	Перехідні мережі

Щодо кодеків, які визначають якість і стиснення голосу, варто згадати G.711, який забезпечує високу якість звуку з пропускною здатністю 64 кбіт/с без стиснення, ідеально підходячи для мереж із достатньою пропускною здатністю, як-от оптичні з’єднання в нашій топології. Натомість G.729 стискає голос до 8 кбіт/с, що є вигідним для мереж із обмеженими ресурсами, але може призводити до невеликої втрати якості, що потрібно враховувати при тестуванні. Інші кодеки, такі як G.722 (широкосмуговий, 64 кбіт/с) і G.723.1 (5.3–6.3 кбіт/с), також можуть бути розглянуті залежно від потреб компанії, наприклад, для підтримки відеоконференцій чи економії ресурсів у віддалених офісах [10].

Таблиця 1.4 – Порівняльна характеристика кодеків

Кодек	Пропускна здатність	Якість звуку	Стиснення	Застосування
G.711	64 кбіт/с	Висока	Немає	Високошвидкісні мережі
G.729	8 кбіт/с	Середня	Високе	Мережі з обмеженнями
G.722	64 кбіт/с	Висока (широкосмугова)	Немає	Відеоконференції
G.723.1	5.3–6.3 кбіт/с	Низька	Високе	Економія ресурсів

Механізми якості обслуговування (QoS) відіграють вирішальну роль у забезпеченні стабільності IP-телефонії. Наприклад, пріоритезація голосового

трафіку через маркування Differentiated Services Code Point (DSCP) із значенням Expedited Forwarding (EF) дозволяє зменшити затримку до менш ніж 150 мс, як того вимагає стандарт ITU-T G.114. Це особливо актуально для туристичної компанії, де сезонні піки дзвінків можуть досягати сотень на годину. Інші методи, такі як Class of Service (CoS) на рівні комутаторів, також можуть бути інтегровані для локального управління трафіком, що потребує детального налаштування на кожному пристрої, наприклад, Cisco 2950-24 у симуляції.

Безпека IP-телефонії є не менш важливою, враховуючи вразливості, такі як підслуховування чи атаки DoS. Шифрування SRTP (Secure RTP) забезпечує захист голосового трафіку, використовуючи алгоритми, такі як AES-128 або AES-256, що є стандартом для сучасних систем. Протокол Transport Layer Security (TLS) захищає сигнальні повідомлення SIP, а ISPec може бути застосований для шифрування цілих тунелів між офісами, що є корисним для туристичної компанії з розподіленими локаціями. Система запобігання вторгненням (ISP) і списки контролю доступу (ACL) додатково захищають мережу, блокуючи несанкціонований доступ до серверів, таких як DNS у нашій топології [3].

Аналізуючи існуючі рішення, можна виділити комерційні платформи, такі як Cisco Unified Communications Manager (CUCM), Asterisk або Microsoft Teams, які пропонують інтеграцію з CRM-системами, автоматичну маршрутизацію дзвінків і підтримку відеоконференцій. Для туристичної компанії CUCM може бути оптимальним через підтримку великих кол-центрів і сумісність із Cisco-обладнанням, хоча Asterisk є більш економним для малих організацій. Проте кожне рішення має свої обмеження: CUCM вимагає значних інвестицій у ліцензії, а Asterisk потребує складного налаштування, що може бути складним для початківців.

1.7 Обґрунтування обраного напрямку рішення

У процесі аналізу вимог до сучасної туристичної компанії було встановлено, що ефективне функціонування її основних бізнес-процесів безпосередньо залежить від якісної комунікації з клієнтами, оперативної обробки інформації, а також гнучкої та захищеної мережевої інфраструктури. З урахуванням специфіки діяльності підприємства, зокрема великої кількості телефонних звернень, інтеграції CRM-систем, обробки заявок онлайн і координації з філіями, було обрано напрям інженерного рішення, заснованого на побудові кіберфізичної системи IP-телефонії з логічною сегментацією корпоративної мережі.

Основними чинниками, що обумовили вибір цього рішення, є:

– заміна застарілих аналогових телефонних систем IP-телефонією, яка забезпечує масштабованість, мобільність, зниження вартості викликів та інтеграцію з IT-сервісами компанії;

– побудова мережі на основі VLAN, що дає змогу логічно розділити підрозділи компанії, підвищити безпеку, впровадити QoS (Quality of Service) для голосового трафіку та зменшити міжвлановий шум;

– впровадження централізованого керування IP-телефонією через SIP-сервер (наприклад, Asterisk або FreePBX), який забезпечує реєстрацію пристроїв, маршрутизацію викликів, роботу голосових меню (IVR) та ведення журналів;

– застосування політик безпеки (ACL, DHCP Snooping, Port Security) для контролю доступу до внутрішніх сервісів та захисту даних від несанкціонованого доступу;

– оптимальність використання ресурсів завдяки гнучкому плануванню IP-адресації, автоматичному наданню IP-адрес (DHCP), централізованому DNS та можливості інтеграції з зовнішніми службами;

– можливість подальшого масштабування та віддаленого доступу за допомогою VPN або хмарної IP-телефонії, що є актуальним для регіональних філій компанії.

Складність роботи полягає в необхідності створення мережевої інфраструктури, яка б відповідала специфічним потребам туристичної компанії, а саме:

– висока інтенсивність комунікацій (у пікові періоди, такі як літній сезон чи святкові дні, кількість дзвінків значно зростає, що вимагає стійкості мережі до високих навантажень і забезпечення низької затримки для голосового трафіку);

– розподілені офіси (компанія має центральний офіс у Дніпрі та філії в інших містах);

– обмеження ресурсів (мережа повинна бути економічно вигідною, використовуючи оптимальні кодеки, такі як G.729 (8 кбіт/с), для економії пропускної здатності в умовах обмежених ресурсів, або G.711 (64 кбіт/с) для високої якості звуку в мережах із достатньою пропускною здатністю).

Таким чином, вибраний напрямок інженерного рішення відповідає принципам функціональної доцільності, системної безпеки, енергетичної ефективності, а також перспективи інтеграції з цифровими сервісами та мобільними платформами. Впровадження IP-телефонії як елемента кіберфізичної системи дозволяє досягти високого рівня автоматизації комунікаційних процесів та є економічно доцільним для компанії, що працює в конкурентному туристичному середовищі.

1.8 Завдання і мета роботи

На основі проведеного аналізу сучасних технологій IP-телефонії, організаційної структури туристичної компанії та потреб її комунікаційної інфраструктури сформульовано завдання щодо створення кіберфізичної системи IP-телефонії, яка забезпечить надійний, безпечний і масштабований зв’язок для ефективної роботи компанії. Туристична галузь характеризується високою сезонністю, необхідністю обробки великої кількості клієнтських запитів і захисту конфіденційних даних, таких як паспортні дані чи інформація про платежі. Завдання спрямоване на створення мережевої інфраструктури,

яка враховує ці особливості, забезпечує економію витрат порівняно з традиційною телефонією та підтримує інтеграцію з цифровими платформами, такими як системи управління клієнтськими даними (CRM).

Основна мета полягає в розробці корпоративної мережі, яка забезпечить високоякісну голосову комунікацію і можливість розширення для туристичної компанії з розподіленими офісами. Обсяг завдання охоплює повний цикл створення кіберфізичної системи IP-телефонії, включаючи:

– аналіз структури та потреб туристичної компанії щодо зв’язку та обміну даними;

– формування технічних вимог до системи IP-телефонії з урахуванням показників якості (затримка, джиттер, втрата пакетів);

– розробка гібридної топології мережі з використанням оптичного волокна для міжмаршрутизаторних з’єднань, вита пара для локальних сегментів і кросовер-кабель для з’єднання Router-Switch;

– розробка корпоративної мережі з логічною сегментацією (VLAN) та адресацією (VLSM), з побудовою у Cisco Packet Tracer.

– впровадження серверу IP-телефонії з підтримкою SIP-протоколу та засобами моніторингу та управління трафіком;

– налаштування мережевих компонентів, включаючи сегментацію трафіку за допомогою VLAN, розподіл адресного простору за допомогою Variable Length Subnet Masking (VLSM) для 172.25.0.0/16;

– розрахунок пропускної здатності мережі для підтримки навантаження до 100 одночасних дзвінків;

– проведення тестування системи в симуляційному середовищі Cisco Packet Tracer для перевірки функціональності, продуктивності.

2 ФОРМУВАННЯ ВИМОГ І РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМПЮТЕРНОЇ СИСТЕМИ ТУРИСТИЧНОЇ КОМПАНІЇ

2.1 Технічні вимоги до КС туристичної компанії

У зв’язку з високим рівнем конкуренції в сфері туристичних послуг, сучасна туристична компанія потребує надійної комп’ютерної системи, яка забезпечить автоматизацію бізнес-процесів, централізовану обробку клієнтських запитів, безперебійний голосовий зв’язок та захищену мережеву інфраструктуру.

Запропонована комп’ютерна система має відповідати комплексним вимогам щодо функціональності, надійності, масштабованості та інформаційної безпеки. Основними технічними завданнями є підтримка IP-телефонії, логічне розділення підрозділів за допомогою VLAN, надання доступу до ключових інформаційних сервісів (CRM, веб-сервіси, бази даних), організація доступу до Інтернету та захист критичних ресурсів.

2.1.1 Найменування і призначення комп’ютерної системи

Кіберфізична система (КФС) IP-телефонії, впроваджена в роботу туристичної компанії, є не просто інструментом зв’язку, а цілісним і продуманим технічним рішенням, яке поєднує у собі найновіші досягнення цифрових технологій і фізичної інфраструктури. Така система включає в себе великий спектр апаратних компонентів, серед яких: IP-телефони, сервери, мережеві маршрутизатори, комутатори, а також додаткове обладнання, що забезпечує стабільність і безперебійність функціонування мережі. Проте не менш важливою частиною КФС є її програмне наповнення: це спеціалізоване програмне забезпечення, яке відповідає за обробку, маршрутизацію та зберігання дзвінків, управління обліковими записами користувачів, а також за надійний захист даних у процесі передавання.

Комп’ютерна система призначена для організації єдиного інформаційного простору в межах туристичної компанії, що охоплює центральний офіс, філії, персонал та клієнтів, а саме:

– забезпечення внутрішнього й зовнішнього телефонного зв’язку засобами IP-телефонії;

– логічного розділення підрозділів компанії за допомогою VLAN;

– доступу до інформаційних сервісів: CRM, електронна пошта, внутрішній портал, резервне зберігання даних;

– централізованого адміністрування, обліку й безпеки мережевої взаємодії.

Основні функції системи полягають у наступному:

– забезпечення надійного внутрішнього та зовнішнього голосового зв’язку засобами IP-телефонії;

– централізація клієнтських звернень, заявок і бронювань через CRM-систему та веб-сервіси;

– надання працівникам доступу до спільних інформаційних ресурсів у залежності від їхніх повноважень;

– логічне розділення трафіку за допомогою VLAN відповідно до структури компанії;

– підтримка роботи служб DHCP, DNS, FTP, email і контролю доступу через ACL та механізми безпеки;

– підвищення продуктивності за рахунок оптимізації трафіку та впровадження політик QoS для голосових потоків;

– забезпечення віддаленої роботи персоналу філій через захищене VPN-з’єднання.

Завдяки гармонійному поєднанню фізичних засобів і цифрових технологій створюється повноцінне середовище для ефективної внутрішньої і зовнішньої комунікації, яке може бути легко налаштоване відповідно до конкретних потреб організації. Така система має властивості гнучкості, тобто здатності адаптуватися до змін у структурі або обсязі роботи компанії,

масштабованості - можливості розширення з мінімальними витратами, а також стійкості до збоїв і безпеки. Усе це надзвичайно важливо для туристичної сфери, де динаміка обробки клієнтських звернень може суттєво змінюватися впродовж року.

Особливо в періоди активного туристичного сезону, коли кількість звернень, дзвінків, запитів зростає у кілька разів, система повинна демонструвати максимальну стабільність та витривалість. Завдяки впровадженню КФС IP-телефонії туристична компанія отримує не лише зручний інструмент для щоденної роботи, а й стратегічну платформу, яка дозволяє оперативно обслуговувати клієнтів, скорочувати час очікування, надавати консультації без затримок і тим самим значно покращувати якість сервісу.

Більше того, впровадження такої системи є одним з кроків до цифрової трансформації бізнесу в цілому. Адже сучасна IP-телефонія не обмежується виключно голосовим зв’язком, вона інтегрується з CRM-системами, аналітичними платформами, інструментами звітності, що дає змогу аналізувати ефективність роботи співробітників, оптимізувати навантаження та вчасно реагувати на зміни в ринку. Таким чином, КФС IP-телефонії є потужною основою для підвищення конкурентоспроможності компанії, поліпшення клієнтського досвіду та побудови стабільної, довгострокової стратегії розвитку бізнесу.

2.1.2 Вимоги до структури і функціонування системи

Проєктована кіберфізична система IP-телефонії базується на комплексному підході до побудови сучасної телекомунікаційної інфраструктури, що забезпечує високий рівень ефективності, надійності та гнучкості для потреб туристичної компанії. Комп’ютерна система туристичної компанії повинна мати ієрархічну структуру з чітким розподілом функцій між її логічними та фізичними компонентами. Архітектура системи має бути

модульною, із можливістю масштабування, централізованого адміністрування та гнучкого керування доступом до ресурсів.

Структурні вимоги:

– система повинна базуватись на багаторівневій мережевій архітектурі з виділенням рівнів доступу, розподілу та ядра;

– структурна модель має передбачати фізичне і логічне розділення на сектори відповідно до підрозділів компанії (адміністрація, туроператори, бухгалтерія, техпідтримка, маркетинг, гостьова зона);

– в основі мережевої побудови повинна використовуватись VLAN-сегментація, що дозволяє відокремити трафік кожного підрозділу, підвищити рівень безпеки й керованості по таблиці 2.1;

Таблиця 2.1 – Взаємозв'язок VLAN і підрозділів туристичної компанії

VLAN ID	Назва VLAN	Відповідні підрозділи / призначення	Призначення
10	Management VLAN	Генеральний директор, керівники, адміністратор системи	Доступ до мережевого обладнання та серверів
20	HR & Accounting VLAN	Кадровий відділ, HR-менеджер, бухгалтерія	Обробка персональних і фінансових даних
30	Tourism Department VLAN	Начальник туристичного відділу, менеджери з туризму, філії	Робота з CRM, базами клієнтів, бронювання
40	Marketing VLAN	Маркетинговий відділ, менеджер з реклами	Рекламна аналітика, доступ до веб-сервісів
50	Guest VLAN	Клієнти, відвідувачі офісу	Обмежений доступ до Інтернету
70	Voice VLAN	Усі структурні підрозділи	Передача голосового трафіку (IP-телефонія)

– передбачена підтримка централізованих серверів обслуговування (DNS, DHCP, FTP, web, SIP), до яких мають доступ лише авторизовані пристрої з певних VLAN:

- DHCP – автоматичне призначення IP-адрес для робочих станцій у межах відповідного підрозділу;
- DNS – для зручного доступу до внутрішніх та зовнішніх веб-ресурсів;
- FTP/SFTP або TFTP – для внутрішнього обміну службовими файлами, резервного копіювання та оновлення прошивок VoIP-пристроїв;
- Web-сервер – для розміщення внутрішнього порталу, CRM або системи бронювання;
- Email-сервіс – для внутрішньої та зовнішньої комунікації працівників компанії.

Функціональні вимоги:

– IP-телефонія: підтримка протоколів SIP та RTP, реалізація внутрішнього нумераційного плану, IVR, переадресації та запису викликів;

– QoS (Quality of Service): надання пріоритету голосовому трафіку над загальним даними в мережі, що є критичним для IP-телефонії;

– ACL (Access Control Lists): обмеження міжвланових з’єднань відповідно до політик безпеки, ізоляція гостьової мережі, захист конфіденційних даних у VLAN бухгалтерії та HR;

– служби безперебійного доступу: впровадження DHCP-серверу для автоматичної адресації пристроїв, DNS – для іменного звернення до ресурсів, а також резервне копіювання налаштувань;

– взаємодія з зовнішніми сервісами: забезпечення виходу в Інтернет через NAT та фаєрвол із контролем трафіку;

– віддалений доступ: підтримка VPN-з'єднання для віддаленої роботи персоналу та філій, з обмеженим доступом до внутрішніх сервісів.

2.1.3 Вимоги до IP-телефонії

Комп’ютерна система повинна підтримувати IP-телефонію на основі протоколів SIP та RTP, що забезпечить:

– внутрішній та зовнішній голосовий зв’язок;

– автоматичну маршрутизацію викликів через SIP-сервер;

– функціонування голосового меню (IVR);

– пріоритизацію трафіку (QoS) для уникнення затримок у передачі голосу;

– шифрування викликів через TLS/SRTP.

Для реалізації системи IP-телефонії сформульовано наступні технічні вимоги:

– кодеки: підтримка G.711 (64 кбіт/с, висока якість звуку без стиснення) для мереж із достатньою пропускною здатністю та G.729 (8 кбіт/с, високе стиснення) для економії ресурсів у мережах із обмеженою пропускною здатністю. Додатково розглядається підтримка G.722 (64 кбіт/с, широкосмуговий звук) для відеоконференцій і G.723.1 (5.3–6.3 кбіт/с) для економії ресурсів у віддалених філіях;

– обладнання для симуляції: використання маршрутизаторів Cisco 2911, комутаторів Cisco 2950-24 і IP-телефонів Cisco IP Phone 7960, які є сумісними з Cisco Packet Tracer і підтримують базові функції VLAN, QoS і SRTP;

– пропускна здатність: локальні з’єднання повинні забезпечувати пропускну здатність не менше 1 Гбіт/с (оптичне волокно, вита пара), зовнішні канали - не менше 100 Мбіт/с для підтримки голосового трафіку та VPN-тунелів;

– масштабованість: резервування адресного простору для додавання нових підрозділів і до 10 IP-телефонів на сегмент.

Пристрої IP-телефонії розміщуються у VLAN 10 з підтримкою PoE на портах комутаторів.

2.1.4 Вимоги до забезпечення високої якості голосового зв’язку

Для того щоб комунікація між співробітниками й клієнтами туристичної компанії була чіткою, безперебійною та приємною на слух, система базується на перевірених і широко застосовуваних протоколах. Зокрема, SIP (Session Initiation Protocol) використовується для ініціалізації, керування та завершення

телефонних дзвінків, а RTP (Real-time Transport Protocol) - для безпосередньої передачі голосових даних у режимі реального часу.

Для забезпечення відповідності стандартам якості зв'язку, прийнятим міжнародною спільнотою (зокрема, ITU-T G.114), особливої уваги надається мінімізації затримки (не більше 150 мс), контролю рівня джітеру (не більше 30 мс) та обмеженню втрат пакетів (до 1%). Досягається це шляхом використання ефективних аудіокодеків. G.711, який використовує 64 кбіт/с, забезпечує високу якість переданого голосу, проте потребує більшої пропускної здатності. Альтернативою виступає кодек G.729, що працює на 8 кбіт/с - менш вимогливий до ресурсу мережі, особливо корисний при великій кількості одночасних дзвінків або при використанні мереж зі зниженими можливостями.

2.2 Вимоги до показників призначення

Для забезпечення ефективної роботи туристичної компанії, комп'ютерна система має відповідати таким основним експлуатаційним та функціональним показникам призначення:

1) Продуктивність системи:

– одночасна підтримка не менше 25 активних SIP-сеансів без втрати якості голосу;

– обробка не менш як 200 запитів/хвилину до CRM та веб-серверів у внутрішній мережі;

– швидкість перемикання VLAN не більше 2 мс при внутрішньомережевих викликах;

– підтримка до 50 одночасних користувачів (робочих станцій, телефонів, мобільних клієнтів).

2) Якість передачі голосу:

– затримка передачі (latency) – не більше 150 мс;

– джитер (Jitter) – не більше 30 мс;

– втрата пакетів – не більше 1%;

– підтримка QoS з пріоритетом DSCP EF (Expedited Forwarding) для VoIP-пакетів.

3) Доступність і надійність:

– рівень доступності системи — не менше 99,5% на рік;

– середній час відновлення після збою (MTTR) — не більше 30 хв;

– реалізація автоматичного резервного копіювання налаштувань і журналів SIP-сервера;

– наявність живлення через UPS або PoE-комутатори з резервуванням.

4) Безпека та контроль доступу:

– шифрування SIP-сесій (TLS) та RTP-потоків (SRTP);

– ізоляція службових VLAN за допомогою ACL;

– підтримка авторизації користувачів за допомогою логінів/паролів або сертифікатів;

– обмеження доступу до адміністративного інтерфейсу лише з VLAN Management.

4) 5) Масштабованість:

– можливість додавання щонайменше 10 нових IP-телефонів без зміни архітектури;

– підтримка розширення кількості VLAN до 10 логічних сегментів;

– готовність до розширення SIP-сервера з локального до хмарного рівня.

2.3 Розробка специфікації апаратних засобів комп’ютерної системи

2.3.1 Розробка загальної архітектури КС

Загальна архітектура комп’ютерної системи (КС) туристичної компанії визначається потребами в автоматизації внутрішніх процесів, уніфікації зв’язку, підтримці IP-телефонії, сегментації мережі для забезпечення безпеки та впровадженням сучасних інформаційних сервісів. Архітектура побудована за принципами модульності, масштабованості та централізованого управління.

Загальна архітектура включає такі основні підсистеми (рис. .2.2):

– мережева інфраструктура – забезпечує передачу даних між користувачами, пристроями та зовнішніми ресурсами;

– IP-телефонія (VoIP) – підтримує внутрішній і зовнішній голосовий зв’язок на основі протоколу SIP;

– серверна підсистема – надає послуги DNS, DHCP, файлового сховища, CRM та SIP;

– безпекова підсистема – включає NAT, ACL, VLAN, QoS і VPN для захисту трафіку;

– користувацька підсистема – охоплює IP-телефони, ПК працівників, мобільні пристрої та Wi-Fi доступ.

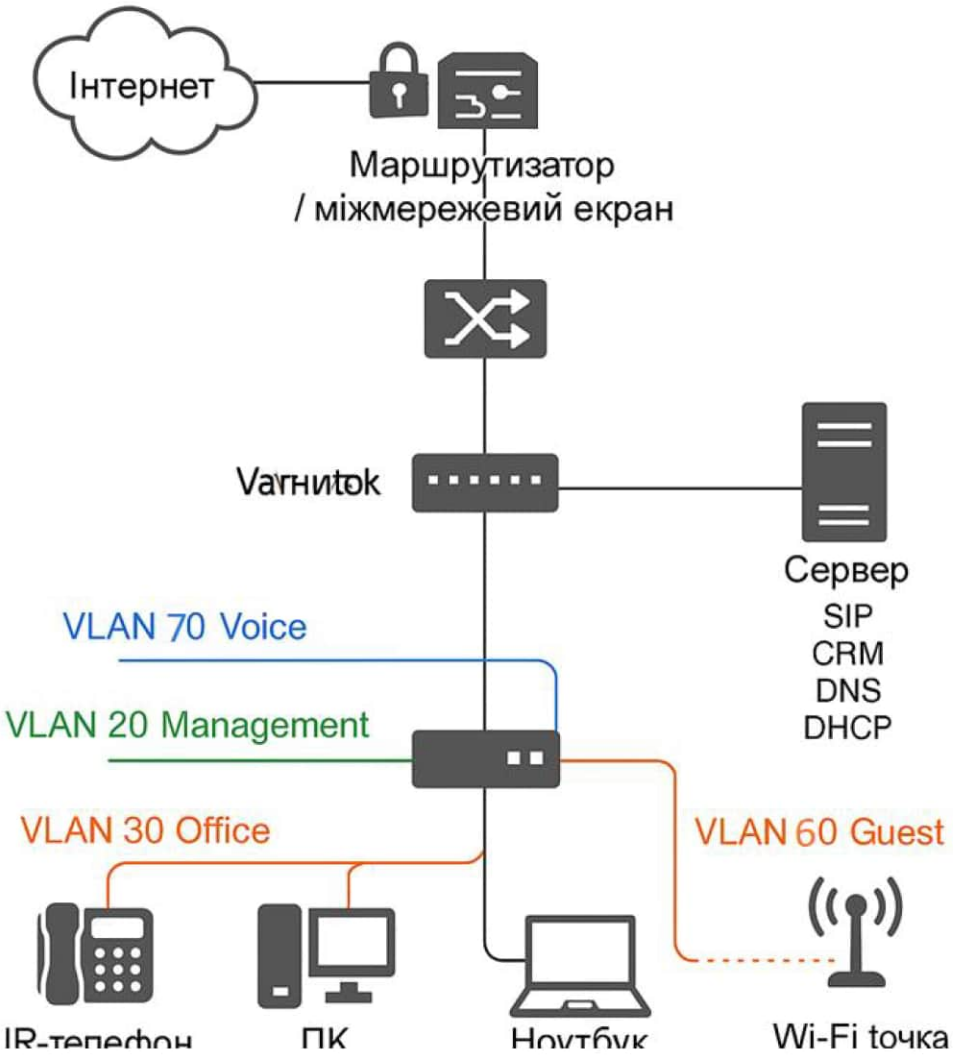


Рисунок 2.1 – Загальна архітектура КС

2.3.2 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи

Архітектура побудована за принципом ієрархічної трирівневої моделі:

1) Рівень доступу (Access layer).

До складу апаратної частини входять IP-телефони, які використовуються співробітниками компанії для здійснення голосових викликів. У середовищі симуляції застосовуються моделі Cisco IP Phone 7960, а в реальних умовах планується використання більш сучасних пристроїв серії Cisco IP Phone 8800, які забезпечують ширший функціонал, включаючи підтримку відеозв'язку та інтеграцію з корпоративними сервісами. Комутатори з підтримкою VLAN та PoE розділяють трафік по сегментах: голосовий (VLAN 10), офісний (VLAN 30), гостьовий (VLAN 40).

Серед іншого обладнання – сервери, що відіграють ключову роль у розподілі функцій у мережі:

2) Рівень розподілу (Distribution layer).

Для розмежування логічних груп усередині мереж застосовується технологія VLAN (Virtual Local Area Network), що дає змогу створити ізольовані середовища для підрозділів або сервісів

Здійснює маршрутизацію між VLAN, фільтрацію трафіку (ACL), реалізацію QoS та політик безпеки. В даній системі представлений одним багатофункціональним маршрутизатором.

Особливої уваги заслуговує використання оптичного волокна між маршрутизаторами, що забезпечує надвисоку пропускну здатність - до 10 Гбіт/с. Така швидкість критично важлива для обробки великого обсягу голосових та службових даних без затримок. У межах локальних сегментів використовується вита пара, яка гарантує швидкість до 1 Гбіт/с, чого цілком достатньо для потреб користувачів в офісному середовищі.

3) Рівень ядра (Core layer)

Представлений зв’язком з провайдером Інтернету через захищене підключення. В майбутньому можливе впровадження резервного каналу або VPN для філій.

Крім того, маршрутизатори типу Cisco 2911 (у симуляції) і Cisco ISR 4451 (у реальному середовищі) з'єднують різні підмережі, а комутатори, зокрема Cisco Catalyst 9300, забезпечують швидкий та надійний обмін трафіком усередині локальних сегментів.

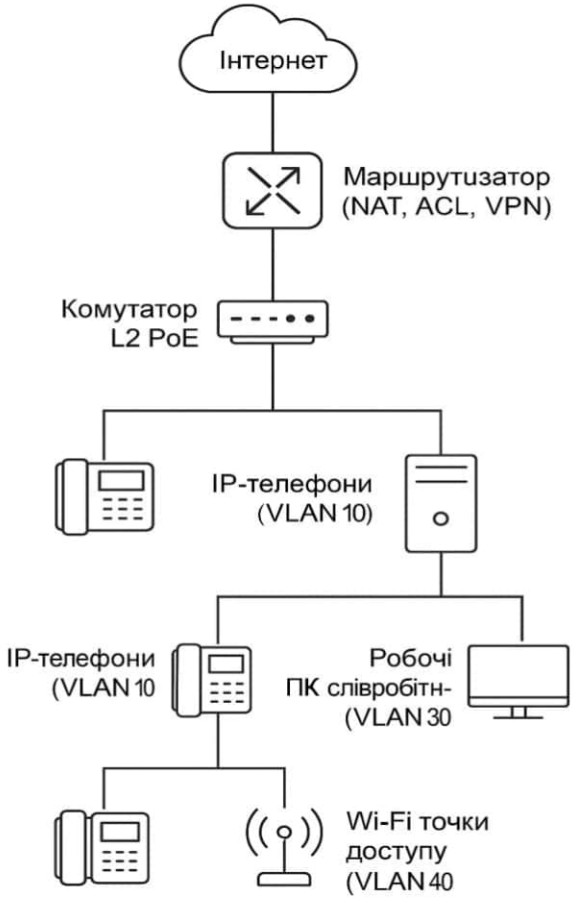


Рисунок 2.2 – Структурна схема

2.3.3 Розробка специфікації апаратних засобів КС

Вимоги до комп’ютерів у корпоративній мережі туристичної компанії формуються залежно від специфіки роботи кожного підрозділу. Співробітники у різних відділах, наприклад, у відділі бронювання, фінансів, маркетингу чи технічної підтримки мають свої унікальні завдання, тому й технічні характеристики комп’ютерів для них можуть значно відрізнятись.

Для офісних працівників, які здебільшого працюють із текстовими документами, електронною поштою або веб-браузером, достатньо базових конфігурацій комп'ютерів. Але якщо мова йде про роботу з графікою, системами бронювання, IP-телефонією чи іншими спеціалізованими програмами, то вимоги до обчислювальної потужності, обсягу оперативної пам'яті та швидкості роботи значно зростають. Так само і з мережею: працівники, які постійно працюють з великою кількістю запитів або дзвінків, потребують стабільного та швидкого з'єднання, тому мережеві адаптери та параметри підключення теж мають враховуватися індивідуально.

Щоб забезпечити ефективну роботу всієї мережі та зменшити ймовірність проблем із сумісністю, рекомендується використовувати однакові або сумісні моделі мережевого обладнання, особливо це стосується роутерів та IP-телефонів. Це значно спрощує процес налаштування, дозволяє легко оновлювати прошивки, дублювати конфігурації, а також полегшує технічну підтримку у разі виникнення несправностей.

Уніфікація обладнання в мережі не тільки знижує витрати часу на технічне обслуговування, але й підвищує стабільність роботи всієї системи, що особливо важливо в умовах великої кількості одночасних дзвінків, бронювань та запитів від клієнтів.

Для успішної реалізації системи рекомендується використовувати сучасне обладнання в реальній мережі, таке як Cisco ISR 4451, Cisco Catalyst 9300 і Cisco IP Phone 8800 Series, для забезпечення високої продуктивності, безпеки та підтримки сучасних функцій, таких як HD Voice і Bluetooth.

Регулярно оновлювати прошивку мережевих пристроїв для усунення вразливостей і підтримки нових протоколів, таких як IPv6, що може бути актуальним для майбутнього розширення.

Проводити періодичні аудити безпеки, включаючи тестування на проникнення за допомогою інструментів, таких як Kali Linux із Metasploit, для виявлення потенційних вразливостей.

Обране обладнання (табл. 2.2) відповідає потребам середньої туристичної компанії з чисельністю до 30 осіб. VoIP-комунікація реалізується на базі SIP-телефонів із живленням через PoE-комутатори. Обладнання Cisco забезпечує сумісність, надійність та підтримку корпоративних стандартів VLAN, QoS, ACL та VPN. Серверна платформа має достатню продуктивність для SIP-сервера, внутрішнього CRM і веб-служб.

Таблиця 2.2 – Специфікація обладнання

№	Найменування	Кількість	Характеристики	Призначення
1	Комутатор Cisco Catalyst 2960 PoE	2	24 порти 10/100/1000 Mbps, PoE, підтримка VLAN	Підключення IP-телефонів та робочих місць
2	Маршрутизатор Cisco ISR 4331	1	3 GE порти, підтримка NAT, ACL, VPN, QoS	Центральний маршрутизатор і захист мережі
3	Безперебійне живлення (UPS)	2	1,5 кВА, автономія 30 хв	Резервне живлення для критичних пристроїв
1	Сервер Dell PowerEdge R250	1	Xeon E-2314, 32 ГБ RAM, 2×SSD 480 ГБ, RAID	SIP-сервер, CRM, DNS, DHCP, Web-сервіси
2	NAS-сервер Synology DS920+	1	4x HDD 2 ТБ, RAID 5, підтримка FTP/WebDAV	Зберігання архівів дзвінків, файлів, резервних копій
1	IP-телефони Cisco 7821	10	Підтримка SIP, PoE, 2 лінії, екран	Голосовий зв’язок працівників
2	ПК працівників (типові робочі станції)	10	Intel i3, 8 ГБ RAM, SSD 256 ГБ, Gigabit LAN	CRM, офісні задачі
3	Wi-Fi точки доступу	2	Dual Band 2.4/5 ГГц, 802.11ac, підтримка VLAN	Бездротовий доступ для співробітників і гостей

3 РОЗРОБКА КОМПЮТЕРНОЇ ІНФРАСТРУКТУРИ ТУРИСТИЧНОЇ КОМПАНІЇ

3.1 Розрахунок адресації

Адресація в локальній мережі організована з використанням приватного діапазону 172.25.0.0/16 IPv4 для внутрішніх сегментів, що дозволяє гнучко масштабувати мережу без ризику колізій та лімітує видимість внутрішньої інфраструктури ззовні.

Voice VLAN має бути окремою VLAN, але логічно пов'язаною з відповідною Data VLAN. Розроблені наступні правила аресації:

– Data VLAN-ам виділяється окрема підмережа з діапазону 172.25.X.0/24, де X = ID VLAN.

– Voice VLAN-ам виділяється окрема підмережа з діапазону 172.25.7X.0/24, де X = ID VLAN (приклад: для VLAN 20 → 172.25.72.0/24).

Маска /24 (тобто 255.255.255.0) дозволяє до 254 хостів у кожній VLAN і цього зазвичай достатньо для типових офісів.

Таблиця 3.1 – Підмережі Data VLAN та Voice VLAN

VLAN ID	Назва VLAN	Тип	IP-підмережа
10	Management VLAN	Data	172.25.1.0/24
70	Management Voice VLAN	Voice	172.25.71.0/24
20	HR & Accounting VLAN	Data	172.25.2.0/24
71	HR & Accounting Voice VLAN	Voice	172.25.72.0/24
30	Tourism Department VLAN	Data	172.25.3.0/24
72	Tourism Department Voice VLAN	Voice	172.25.73.0/24
40	Marketing VLAN	Data	172.25.4.0/24
73	Marketing Voice VLAN	Voice	172.25.74.0/24
50	Guest VLAN	Data	172.25.5.0/24
74	Guest Voice VLAN	Voice	172.25.75.0/24

Логіка призначення VLAN та відповідних підмереж:

– Management VLAN (10/70): для управління мережевим обладнанням. Зазвичай відділяється для безпеки;

– HR & Accounting VLAN (20/72): для відділу кадрів та бухгалтерії. Важливо ізолювати через чутливі дані;

– Tourism Department VLAN (30/73): для туристичного відділу;

– Marketing VLAN (40/74): для відділу маркетингу:

– Guest VLAN (50 / 75): для гостьових пристроїв. Це критично важливо для безпеки, щоб гості не мали доступу до внутрішньої мережі компанії.

Використання окремих VLAN ID (10, 20, 30... для Data та 70, 71, 72... для Voice) та окремих діапазонів IP-адрес (172.25.X.0 для Data та 172.25.7X.0 для Voice) дозволяє пріоритезувати голосовий трафік (QoS), забезпечити, щоб голосові дзвінки не переривалися та не мали затримок через завантаження мережі даними; покращити безпеку через ізолювання голосового трафіку від потенційних загроз у мережі даних, та спростити управління, бо легше ідентифікувати та усувати проблеми, що стосуються певного типу трафіку.

Структура мережі проєкту побудована на використанні декількох локальних мереж (FILIAL1–FILIAL5), які з’єднані між собою за допомогою маршрутизаторів, що забезпечують розподіл трафіку між сегментами

Кожна VLAN працює в окремому сегменті з власним маршрутизатором, то кожен з них має свій інтерфейс-шлюз у відповідній підмережі. Нижче таблиці приклад адресації пристроїв: шлюзи, хости (PC, IP-телефони), а також назва VLAN.

Таблиця 3.2 – Схема адресації пристроїв

VLAN ID	Назва VLAN	Тип	IP-підмережа	IP шлюзу (роутер)	Приклад IP ПК	Приклад IP IP-телефона
10	Management VLAN	Data	172.25.1.0/24	172.25.1.1	172.25.1.10	172.25.71.10
70	Management Voice VLAN	Voice	172.25.71.0/24	172.25.71.1	–	172.25.71.11
20	HR & Accounting VLAN	Data	172.25.2.0/24	172.25.2.1	172.25.2.10	172.25.72.10
71	HR & Accounting Voice VLAN	Voice	172.25.72.0/24	172.25.72.1	–	172.25.72.11
30	Tourism Department VLAN	Data	172.25.3.0/24	172.25.3.1	172.25.3.10	172.25.73.10
72	Tourism Department Voice VLAN	Voice	172.25.73.0/24	172.25.73.1	–	172.25.73.11
40	Marketing VLAN	Data	172.25.4.0/24	172.25.4.1	172.25.4.10	172.25.74.10
73	Marketing Voice VLAN	Voice	172.25.74.0/24	172.25.74.1	–	172.25.74.11
50	Guest VLAN	Data	172.25.5.0/24	172.25.5.1	172.25.5.10	172.25.75.10
74	Guest Voice VLAN	Voice	172.25.75.0/24	172.25.75.1	–	172.25.75.11

3.2 Проєктування корпоративної мережі в Cisco Packet Tracer

Проєктування корпоративної телекомунікаційної інфраструктури, призначеної для забезпечення функціонування кіберфізичної системи IP-телефонії, було виконано із використанням інструменту симуляції комп’ютерних мереж Cisco Packet Tracer. Це програмне середовище є потужним засобом для створення, візуалізації та тестування логіки мережевих рішень ще до їх фізичного впровадження. На рисунку 3.1 представлена логічна топологія мережі в Packet Tracer.

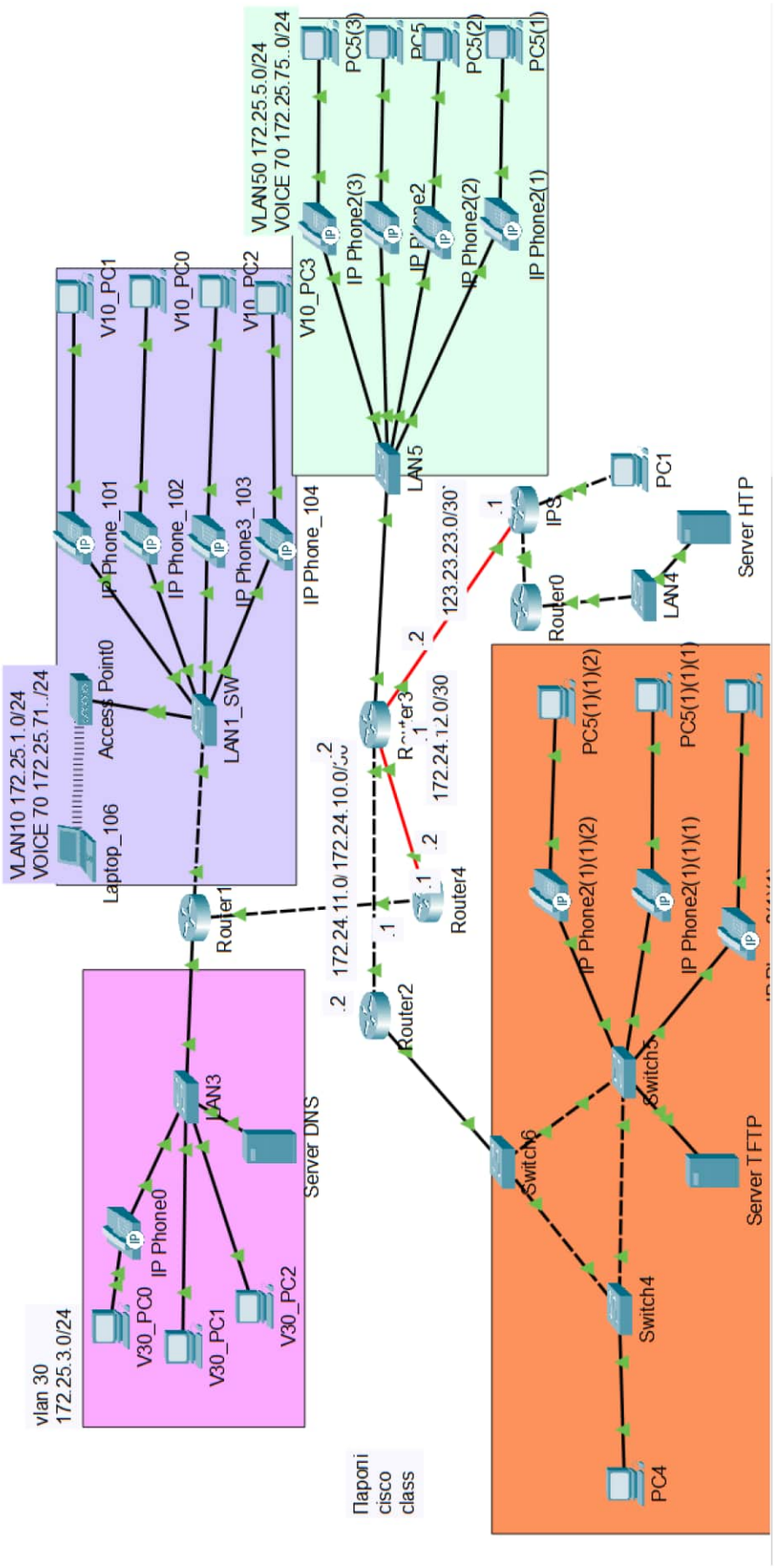


Рисунок 3.1 – Логічна топологія мережі

Зокрема, топологія мережі складається з п’яти окремих локальних сегментів (FILIAL1–FILIAL5), що імітують структурні підрозділи туристичної компанії. Для організації маршрутизації між цими сегментами використовуються п’ять маршрутизаторів (Router0–Router4), кожен з яких відповідає за обробку, переадресацію та аналіз міжмережевого трафіку. Для забезпечення функціонування на канальному рівні використано п’ять комутаторів (Switch1–Switch5), які реалізують фізичне з’єднання між кінцевими пристроями в межах кожної локальної мережі.

У рамках моделі також реалізовано серверну інфраструктуру, яка представлена трьома ключовими серверами: DNS-сервером для розв'язання доменних імен, HTTP-сервером для хостингу внутрішніх вебресурсів та TFTP-сервером, призначеним для зберігання й передачі конфігураційних файлів пристроїв.

Топологія мережі має комбінований характер, що поєднує в собі елементи зіркоподібної структури (для побудови локальних сегментів) та лінійної «магістральної» архітектури (для об’єднання маршрутизаторів у єдину мережу). Центральним вузлом є Router1, який виступає як головний комунікаційний хаб системи, забезпечуючи маршрутизацію між ключовими сегментами FILIAL1 (із 46 активними пристроями), FILIAL2 (122 пристрої), FILIAL5 (6 пристроїв), а також має виходи до зовнішніх систем, зокрема TFTP-серверів.

FILIAL3 та FILIAL4 реалізовані як окремі сегменти з помірним навантаженням (відповідно 36 та 27 активних вузлів), де розміщено серверну інфраструктуру, зокрема TFTP-сервер, підключений до Router0 через оптичне волокно, що забезпечує високу пропускну здатність і стабільність передачі даних. Водночас, Router3 під’єднаний до модуля ISP через серійний інтерфейс, що дозволяє здійснювати глибокий аналіз трафіку на предмет шкідливої активності

Для побудови мережі була обрана гібридна топологія, і це рішення було прийнято не випадково. Такий підхід дозволяє поєднати найкращі властивості

різних типів мережевих структур, щоб створити систему, яка буде одночасно гнучкою, стабільною та зручною в управлінні. Особливо це важливо для сучасної туристичної компанії, де ефективна комунікація та швидкий обмін даними мають вирішальне значення для роботи.

У середині кожного окремого сегменту мережі, таких як FILIAL1, FILIAL2, і аж до FILIAL5, використано зіркоподібну топологію. Це означає, що всі пристрої в мережі: комп'ютери, IP-телефони, принтери, сервери тощо, підключені до одного центрального комутатора. Такий принцип схожий на спиці в колесі, де комутатор – це центр, а всі інші пристрої – це відгалуження. Така модель забезпечує не лише зручне підключення, але й дає змогу швидко знаходити та усувати проблеми. Якщо, наприклад, один комп'ютер виходить з ладу, то вся мережа не страждає, адже решта пристроїв працює незалежно.

Для з'єднання між окремими сегментами мережі, а саме між маршрутизаторами (Router0 до Router4), використана лінійна структура. Це означає, що маршрутизатори з'єднані послідовно, один за одним, що дозволяє ефективно передавати дані з однієї частини мережі в іншу. Такий підхід добре себе зарекомендував у ситуаціях, коли мережа має працювати без перебоїв навіть при великих навантаженнях. А в туристичній компанії, де щогодини може здійснюватися до 100 голосових викликів, стабільна передача трафіку між сегментами критично важлива.

Таким чином, гібридна топологія дає змогу поєднати простоту та централізованість зіркоподібної структури з надійністю та послідовністю лінійного з'єднання. Це ідеальне рішення для компаній, які хочуть мати добре структуровану мережу, здатну витримувати високі навантаження і водночас залишатися зручною в обслуговуванні та масштабуванні.

У симуляції використано маршрутизатори Cisco 2911, комутатори Cisco 2950-24 і IP-телефони Cisco IP Phone 7960, які є сумісними з Cisco Packet Tracer. У реальній мережі рекомендується використовувати Cisco ISR 4451 для маршрутизації, Cisco Catalyst 9300 для комутації та Cisco IP Phone 8800 Series для підтримки HD Voice і Bluetooth [9].

З’єднання між окремими елементами інфраструктури побудовано з використанням різних типів мережевих кабелів, що відповідає реальним практикам побудови фізичного рівня мережі. Так, вита пара (UTP) використовується для з’єднання кінцевих пристроїв із комутаторами, оптичне волокно для високошвидкісного обміну даними між віддаленими маршрутизаторами, серійні з’єднання для конфігурації та взаємодії пристроїв через WAN-інтерфейси, а кросовер-кабелі для прямого з’єднання однотипного обладнання (наприклад, маршрутизатор-комутатор або комутатор-комутатор).

Оптичне волокно між маршрутизаторами (Router0–TFTP, Router1–Router3) забезпечує пропускну здатність до 10 Гбіт/с, вита пара для локальних сегментів – до 1 Гбіт/с, а кросовер-кабель між Router4 і Switch4 – для прямого з’єднання.

Вита пара – це один із найпоширеніших типів кабелів, який активно застосовується для підключення кінцевих пристроїв до комутаторів. Наприклад, з’єднання Switch1–Router2 та Switch2–Server DNS реалізовані саме за допомогою витої пари. Такий кабель підтримує стандарти FastEthernet або GigabitEthernet, що дозволяє досягати швидкості до 1 Гбіт/с. Вита пара є зручною, економічно доступною і легкою в прокладанні, що робить її ідеальним вибором для більшості внутрішніх з’єднань.

Оптичне волокно використовується для з’єднань між основними маршрутизаторами, зокрема Router0–TFTP та Router1–Router3. Цей тип з’єднання забезпечує високу пропускну здатність до 10 Гбіт/с, а також є стійким до електромагнітних завад. Це дозволяє передавати великі обсяги даних на значні відстані без втрат якості сигналу, що особливо важливо для міжмережевих зв’язків у центральній частині інфраструктури.

Serial-з’єднання реалізовано між Router3 та ISP (до провайдера). Воно має нижчу швидкість - до 2 Мбіт/с, але при цьому забезпечує високу стабільність та надійність. Такий тип з’єднання часто використовується для зовнішніх систем безпеки, де головне - не швидкість, а надійність моніторингу та безперебійна передача даних.

Кросовер-кабель застосовується для з’єднання Router4–Switch4 у локальній мережі FILIAL1. Цей тип з’єднання підходить для безпосереднього підключення пристроїв одного рівня без участі проміжних компонентів. Кросовер-кабель також підтримує швидкість до 1 Гбіт/с та є простим і недорогим рішенням для побудови локальних з’єднань у межах одного офісу або технічного приміщення.

Таким чином, використання різних типів кабельних з’єднань дозволяє створити гнучку, ефективну та стабільну мережу, де кожна ділянка виконує свої функції на оптимальному рівні залежно від технічних вимо (табл. 3.2)г.

Таблиця 3.3 – Типи з’єднань

Тип з’єднання	Пристрої	Швидкість	Застосування	Переваги
Вита пара	Switch1–Router2, Switch2–DNS	До 1 Гбіт/с	Локальні сегменти, сервери	Економічність, простота встановлення
Оптичне волокно	Router0–TFTP, Router1–Router3	До 10 Гбіт/с	Міжмаршрутизаторні з’єднання	Висока швидкість, стійкість до перешкод
Serial	Router3– ISP	До 2 Мбіт/с	Моніторинг безпеки	Надійність, низьке енергоспоживання
Кросовер	Router4–Switch4	До 1 Гбіт/с	Пряме з’єднання в FILIAL1	Простота, економія ресурсів

3.2.2 Налаштування та перевірка DHCP

Кожен мамаршрутизатор буде виклнувати роль DHCP-сервера у відповідній підмережі. Наприклад, на рис. 3.2 для налаштування DHCP у мережі, яка включає різні VLAN (зокрема VLAN 30, VLAN 10 Data та VLAN 70 Voice), потрібно буде налаштувати DHCP-сервер на маршрутизаторі Router1.

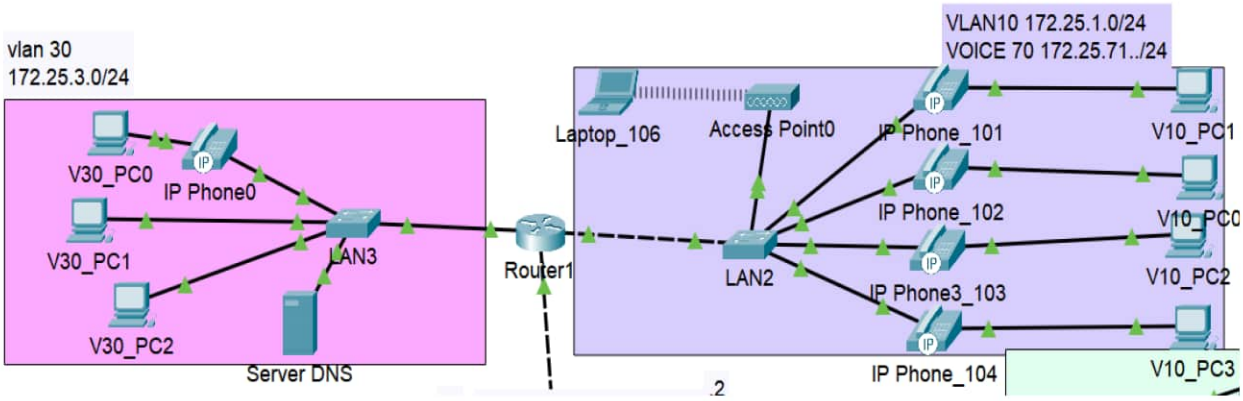


Рисунок 3.2 – Сегмент з VLAN 30 та VLAN 10

Router1 є центральним елементом для VLAN 30 та VLAN 10/70. Тому, саме Router1 буде виконувати роль DHCP-сервера для цих VLAN.

Маршрутизатор Router 1 виконує ключову роль у побудові мережевої взаємодії, оскільки він поєднує між собою дві окремі локальні мережі - FILIAL 2 та FILIAL 3. Завдяки цьому пристрої та користувачі, які знаходяться в різних підмережах, можуть безперешкодно обмінюватися даними, здійснювати голосові дзвінки (у випадку з IP-телефонією) або користуватися спільними ресурсами, такими як принтери чи сервери.

Інакше кажучи, Router 1 виступає "мостом" між двома незалежними мережами, забезпечуючи міжмережеву маршрутизацію. Це особливо важливо для структурованої корпоративної мережі, де окремі відділи чи функціональні зони можуть бути розділені на різні VLAN або IP-сегменти, але при цьому потребують взаємодії.

Припустимо, що на Router1 інтерфейси, підключені до LAN3, LAN2, налаштовані як "router on a stick" або "SVI" для підтримки VLAN.

Налаштування VLAN 30 (Data):

– VLAN ID: 30;

– IP-підмережа: 172.25.3.0/2;

– шлюз за замовчуванням (інтерфейс Router1 для VLAN 30): 172.25.3.1.

```
// Виключаємо шлюз та перші 9 адрес для статичних призначень
Router1(config)# ip dhcp excluded-address 172.25.3.1 172.25.3.10
Router1(config)# ip dhcp pool VLAN30_DATA
Router1(dhcp-config)# network 172.25.3.0 255.255.255.0
```

```
Router1(dhcp-config)# default-router 172.25.3.1
Router1(dhcp-config)# dns-server 172.25.3.5  // Server DNS
```

Налаштування VLAN 10 (Data):

– VLAN ID: 10;

– IP-підмережа: 172.25.1.0/24;

– Шлюз за замовчуванням (інтерфейс Router1 для VLAN 10): 172.25.1.1.

```
Router1(config)# ip dhcp excluded-address 172.25.1.1 172.25.1.10
Router1(config)# ip dhcp pool VLAN10_DATA
Router1(dhcp-config)# network 172.25.1.0 255.255.255.0
Router1(dhcp-config)# default-router 172.25.1.1
Router1(dhcp-config)# dns-server  172.25.3.5
```

Налаштування VLAN 70 (Voice):

– VLAN ID: 70;

– IP-підмережа: 172.25.71.0/24;

– шлюз за замовчуванням (інтерфейс Router1 для VLAN 70): 172.25.71.1;

– TFTP-сервер: 172.25.71.1.

```
Router1(config)# ip dhcp excluded-address 172.25.71.1 172.25.71.9
Router1(config)# ip dhcp pool VLAN70_VOICE
Router1(dhcp-config)# network 172.25.71.0 255.255.255.0
Router1(dhcp-config)# default-router 172.25.71.1
Router1(dhcp-config)# option 150 ip 172.25.71.1
Router1(dhcp-config)# dns-server 172.25.71.1
```

Для перевірки на ПК в налаштуваннях інтерефесй обремено отрмувати динамічно (рис.3.3).

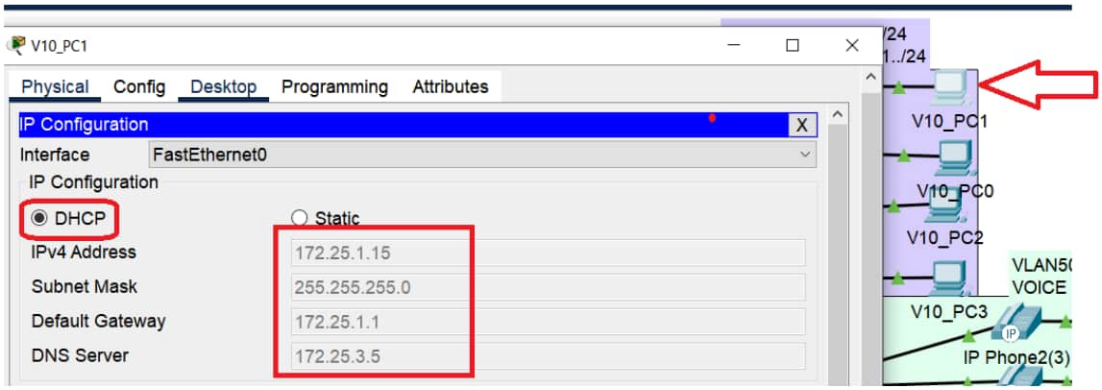


Рисунок 3.3 – V10_PC1 з адресацією по DHCP

Також на рис. 3.4 IP-телефон успішно реєструється а мережі і отримує адресу з VLAN70_VOICE та номер 104.

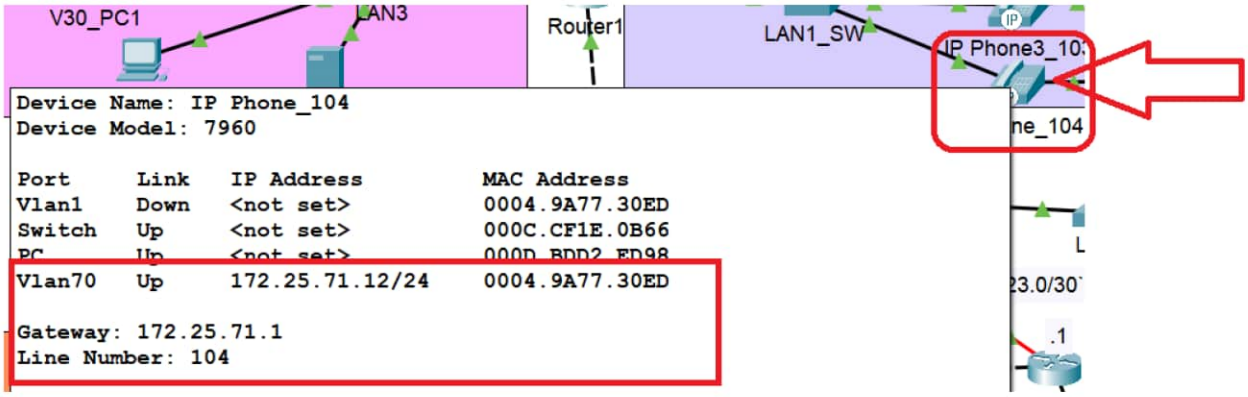


Рисунок 3.4 – IP Налаштування телефону

3.3 Налаштування та перевірка "router on a stick"

Конфігурація інтерфейсів Router1: Переконайтесь, що субінтерфейси Router1 (для "router on a stick" на LAN3 та LAN2) або SVI (Switched Virtual Interfaces) правильно налаштовані для кожного VLAN з відповідними IP-адресами, які будуть служити шлюзами за замовчуванням.

Приклад для Router1:

```
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.25.3.1 255.255.255.0
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.25.1.1 255.255.255.0
interface GigabitEthernet0/0.70
 encapsulation dot1Q 70
 ip address 172.25.71.1 255.255.255.0
```

Порти, до яких підключені ПК та IP-телефони, мають бути налаштовані як access ports для відповідних VLAN (наприклад, switchport access vlan 30).

Порти, до яких підключені IP-телефони з ПК за телефоном (як на LAN2), мають бути налаштовані як voice VLAN ports. Це дозволяє телефону отримувати IP-адресу з голосового VLAN, а комп'ютеру, підключеному до телефону, з VLAN даних.

```
interface FastEthernet0/1
 switchport mode access
 switchport access vlan 10      // Data VLAN
 switchport voice vlan 70       // Voice VLAN
```

Порти, що з'єднують комутатори з маршрутизаторами (trunks), мають бути налаштовані як trunk ports, що дозволяє передавати трафік багатьох VLAN.

```
interface GigabitEthernet0/1
 switchport mode trunk
switchport trunk allowed vlan 10,30,70 // Дозволені VLANи
```

Командою show vlan brief перевіряємо надаштування потрів та VLAN. На рис. 3.3 результат на комутаторі LAN1_SW.

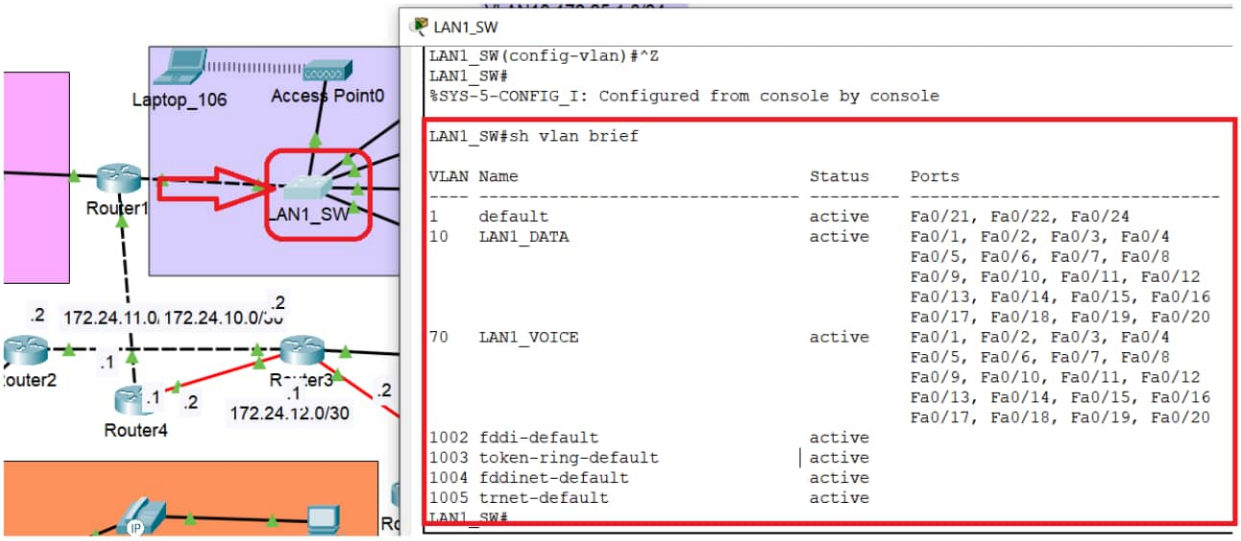


Рисунок 3.5 – Перевірка VLAN та портів на LAN1_SW

3.3.2 Налаштування маршрутизації та доступу в Інтернет

Маршрутизатор ISP виконує функцію своєрідного мережевого шлюзу, через який проходить весь вхідний та вихідний трафік між внутрішньою інфраструктурою компанії та зовнішніми мережами, зокрема глобальною мережею Інтернет. Таким чином, ISP-маршрутизатор не лише забезпечує маршрутизацію пакетів, а й виконує функції контролю, фільтрації та аналізу трафіку з метою виявлення підозрілої активності, що може свідчити про

намагання несанкціонованого доступу до корпоративної мережі або спробу атаки.

У рамках моделювання передбачено, що інтернет-провайдер надав організації статичну IP-адресу - 123.23.23.1, яка разом із маскою підмережі 255.255.255.252 формує дуже обмежений, але цілком функціональний адресний простір. Зокрема, при такій масці підмережі доступні лише дві активні IP-адреси, одна з яких призначається маршрутизатору провайдера, а інша - власному ISP-маршрутизатору організації. Це є типовим рішенням для точкових підключень до провайдера, де немає потреби у великій кількості зовнішніх IP-адрес, але важливо забезпечити стабільність і захищеність каналу.

Незважаючи на простоту такого налаштування, воно повністю відповідає вимогам до реалізації NAT (Network Address Translation). Усі внутрішні пристрої, які використовують приватні IP-адреси, можуть виходити до Інтернету за допомогою трансляції своїх адрес через єдину зовнішню адресу маршрутизатора. Це дозволяє зберігати обмежений публічний адресний простір і водночас забезпечити повноцінний обмін даними з глобальною мережею.

Окрім цього, ISP-маршрутизатор у даній моделі виконує функції фаєрволу першого рівня, який блокує небажані з’єднання ще на етапі їх встановлення. Система ISP постійно оновлюється для виявлення нових типів атак, таких як DoS-атаки, сканування портів, SIP-флуд, спроби підміни SIP-повідомлень тощо, що є особливо важливим у середовищах, де активно використовується IP-телефонія.

Таким чином, включення ISP-маршрутизатора до структури корпоративної мережі забезпечує не лише її функціональність і доступ до зовнішнього середовища, а й створює надійний захисний бар'єр, що є критично важливим для захисту конфіденційної інформації та підтримки стабільної роботи всіх внутрішніх сервісів. Відповідні конфігурації можна знайти у Додатку А.

Застосування OSPF у цій мережі є повністю обґрунтованим і має низку переваг:

– динамічна маршрутизація та адаптивність: OSPF дозволяє маршрутизаторам автоматично дізнаватися про всі мережі в топології без ручного введення статичних маршрутів. У разі змін у мережі (наприклад, вихід з ладу каналу або маршрутизатора, додавання нової підмережі), OSPF швидко адаптується, перераховуючи шляхи та оновлюючи таблиці маршрутизації. Це забезпечує високу доступність та відмовостійкість мережі.

– оптимальна маршрутизація: OSPF використовує алгоритм SPF (Shortest Path First) для визначення найкращих шляхів до кожної мережі на основі вартості (метрики), яка за замовчуванням базується на пропускній здатності каналу. Це забезпечує ефективне використання мережевих ресурсів та швидку доставку трафіку.

– наявність різних метрик (наприклад, [110/3] для 172.24.10.0/30 та [110/2] для 172.24.12.0/30) показує, що OSPF вибирає оптимальний шлях за найменшою вартістю;

– масштабованість: хоча поточна конфігурація використовує одну область (Area 0), OSPF спроектований для роботи у великих і складних мережах. Можливість поділу на багатообласні топології дозволяє зменшити розмір баз даних OSPF на маршрутизаторах, прискорити конвергенцію та локалізувати проблеми. Це робить OSPF чудовим вибором для мережі, яка може зростати в майбутньому.

– ефективне розповсюдження маршруту за замовчуванням: наявність O*E2 0.0.0.0/0 демонструє, що OSPF успішно розповсюджує маршрут за замовчуванням. Це дозволяє всім пристроям у мережі досягати зовнішніх ресурсів (наприклад, Інтернету) через єдину точку виходу (Router2), без необхідності налаштовувати статичний маршрут за замовчуванням на кожному маршрутизаторі вручну. Тип E2 гарантує, що вартість цього маршруту залишається сталою в усьому OSPF-домені.

– підтримка VLSM та CIDR: вивід команди показує використання різних масок підмереж (/24, /30). OSPF повністю підтримує Variable Length Subnet Masking (VLSM) та Classless Inter-Domain Routing (CIDR), що дозволяє ефективно використовувати IP-адресний простір.

– відкритий стандарт: OSPF є відкритим стандартом, що забезпечує сумісність між обладнанням різних виробників (Cisco, Juniper, Huawei тощо).

Таблиця маршрутизації Router1 (рис.3.6) чітко показує, що OSPF успішно функціонує в цій мережі, забезпечуючи динамічну, оптимальну та масштабовану маршрутизацію. Він коректно вивчає як підмережі LAN/VLAN, так і транзитні мережі, а також ефективно розповсюджує маршрут за замовчуванням. Це робить OSPF ідеальним вибором для цієї корпоративної мережі, забезпечуючи її стабільність, ефективність та готовність до подальшого розвитку.

.

```
Router1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.24.11.1 to network 0.0.0.0

     172.24.0.0/16 is variably subnetted, 4 subnets, 2 masks
O       172.24.10.0/30 [110/3] via 172.24.11.1, 00:19:41, FastEthernet0/0
C       172.24.11.0/30 is directly connected, FastEthernet0/0
L       172.24.11.2/32 is directly connected, FastEthernet0/0
O       172.24.12.0/30 [110/2] via 172.24.11.1, 00:19:51, FastEthernet0/0
     172.25.0.0/16 is variably subnetted, 12 subnets, 2 masks
C       172.25.1.0/24 is directly connected, FastEthernet0/1.10
L       172.25.1.1/32 is directly connected, FastEthernet0/1.10
O       172.25.2.0/24 [110/4] via 172.24.11.1, 00:19:41, FastEthernet0/0
C       172.25.3.0/24 is directly connected, Vlan30
L       172.25.3.1/32 is directly connected, Vlan30
O       172.25.5.0/24 [110/3] via 172.24.11.1, 00:19:41, FastEthernet0/0
C       172.25.71.0/24 is directly connected, FastEthernet0/1.70
L       172.25.71.1/32 is directly connected, FastEthernet0/1.70
C       172.25.73.0/24 is directly connected, FastEthernet0/1.73
L       172.25.73.1/32 is directly connected, FastEthernet0/1.73
O       172.25.75.0/24 [110/3] via 172.24.11.1, 00:19:41, FastEthernet0/0
O       172.25.80.0/24 [110/4] via 172.24.11.1, 00:19:41, FastEthernet0/0
O*E2 0.0.0.0/0 [110/1] via 172.24.11.1, 00:19:41, FastEthernet0/0
```

Рисунок 3.6 – Таблиця марштутизації на Router1

На рисунку 3.7 команжою tracert перевіряється доступність між ПК в VLAN 10 та ПК в VLAN50. Як бачимо, пакети на шляху проходять успішно через маршрутизатори Router1, Router4, Router3.

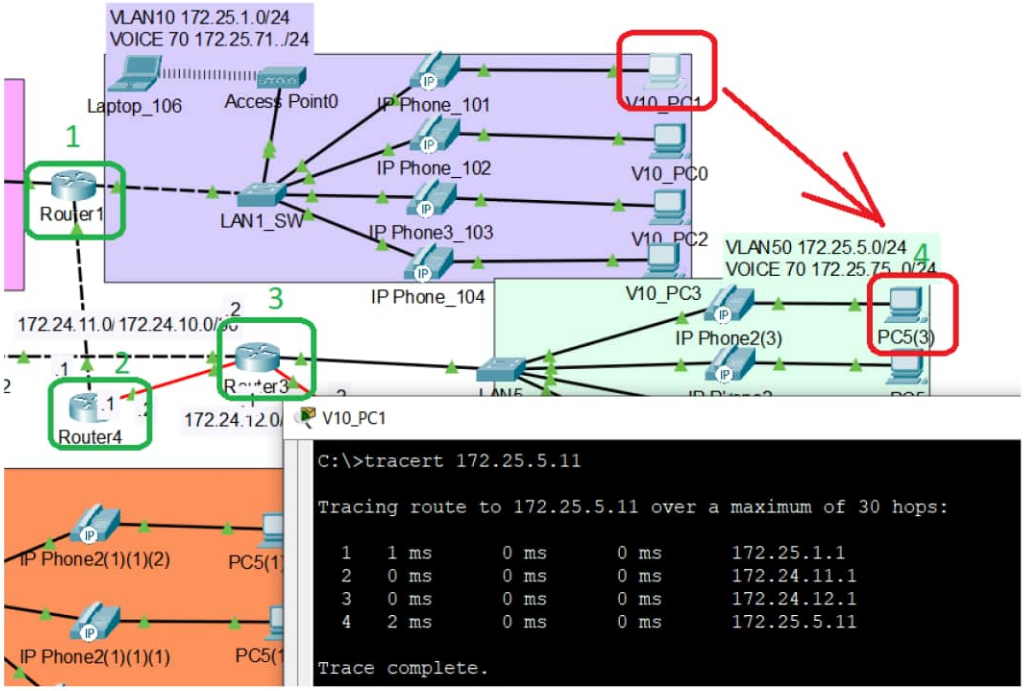


Рисунок 3.7 – Перевірка звязку між VLAN10 та VLAN50

Так успішно працює NAT на граничному маршрутизаторі Router3 при перевірки звязку з провайдеров (рис. 3.8).

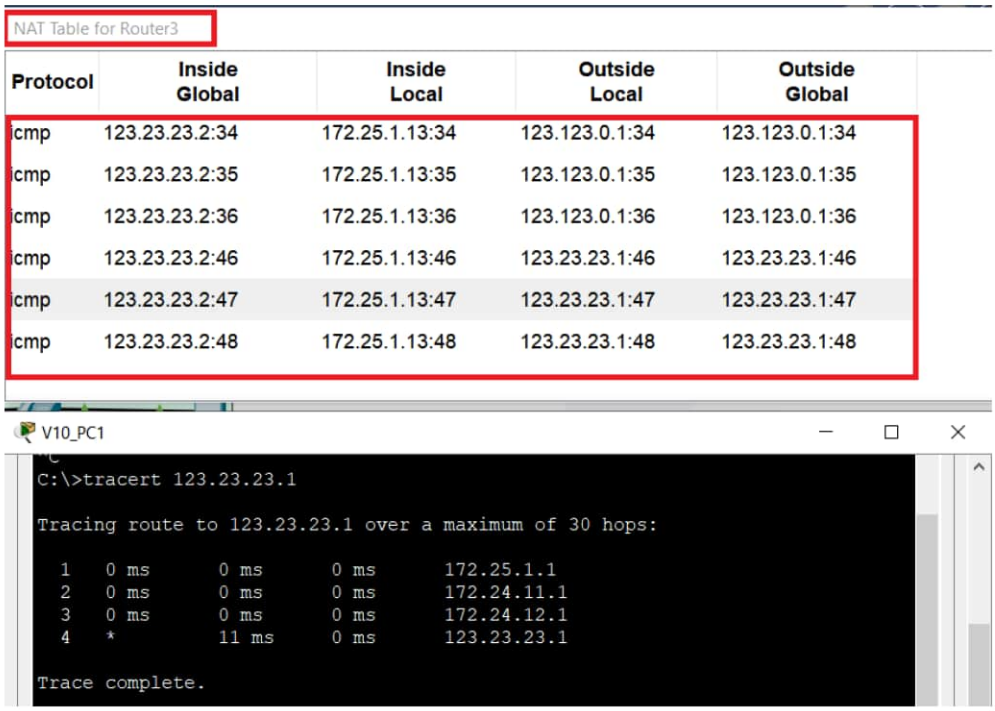


Рисунок 3.8 – Перевірка NAT та звязку між VLAN10 та провайдером

4 РОЗОЛБКА ШЗ-ТЕЛЕФОНІЇ ДЛЯ ТУРИСТИЧНОЇ КОМПАНІЇ

4.1 Підключення VoIP-телефонів

IP-телефони підключаються безпосередньо до комутаторів на модулі комутатора, який є платою, що підключається на маршрутизаторі 2811. Телефон отримує живлення через кабель Ethernet.

На комутаторі, який може живити інший пристрій, наприклад IP-телефон, нанесено трафарет слів INLINE POWER, PoE (Power on Ethernet) або LNK PWR. Підключено шнур живлення до комутатора, який забезпечує вбудоване живлення. Підключено прямий кабель Ethernet від порту 100/10 SW на IP-телефоні до будь-якого порту 100 МБ на вбудованому комутаторі живлення (рис. 4.1 – 4.2).

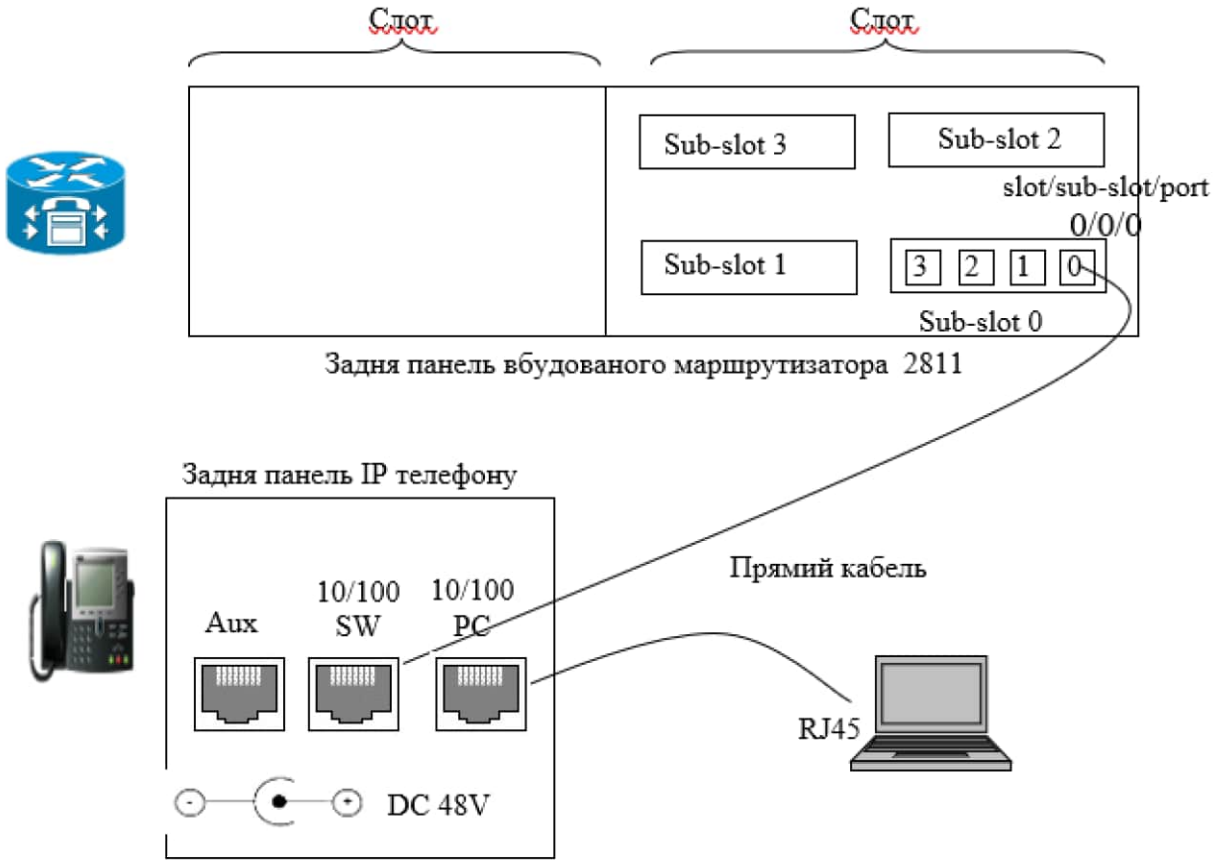
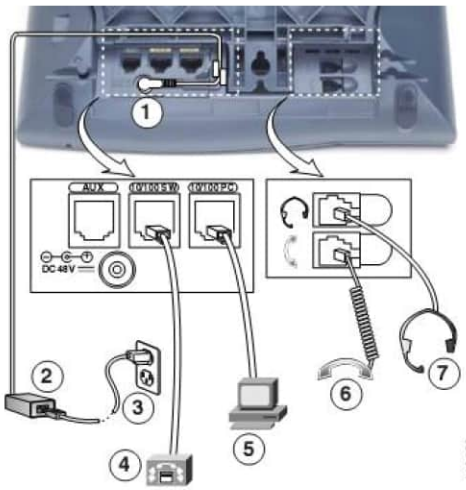


Рисунок 4.1 – Піддючення IP-телефону до комутатора



1	DC adaptor port (DC48V)	5	Access port (10/100 PC)
2	AC-to-DC power supply	6	Handset port
3	AC power cord	7	Headset port
4	Network port (10/100 SW)	8	Footstand button

Рисунок 4.2 – Кабельні підключення до IP-телефону

4.2 Налаштування VoIP

На основі заданої схеми на рис.3.2 Router1 бде виконувати роль Cisco Call Manager Express (CME).

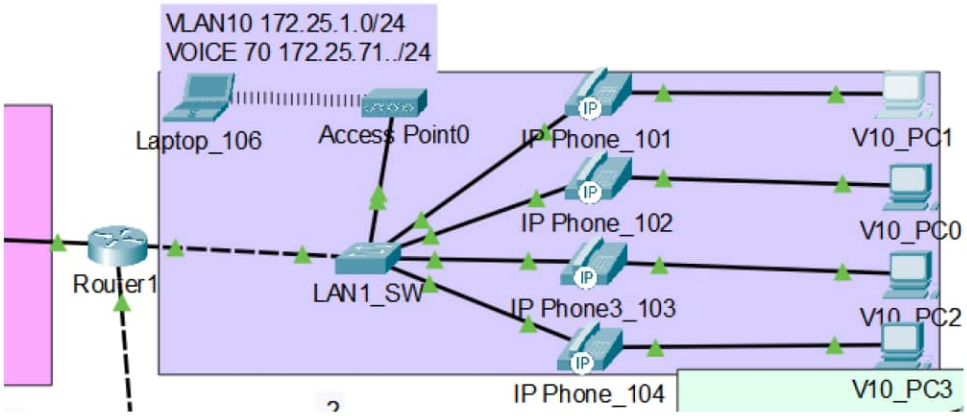


Рисунок 4.3 – Мережа IP-телефонії в VLAN10

Його конфігурація:

– IP-адреса інтерфейсу Router1 для голосового VLAN 70: 172.25.71.1 (це буде IP-адреса CME, яка роздається телефонам через Option 150 DHCP);

– TFTP Server нлаштований і доступний (його IP-адреса потрібна для Option 150 DHCP, але CME також має вбудований TFTP-сервер, який можна використовувати);

– IP-телефони: IP Phone3(1), IP Phone3(2), IP Phone3(3) підключені до LAN1 у VLAN 70.

Кожному телефону в цій системі автоматично присвоюється випадковий номер із заздалегідь визначеного набору вільних номерів. У даній топології для кожного сегменту мережі було зарезервовано по 10 телефонних номерів, але за потреби цю кількість можна легко змінити – збільшити або зменшити.

Цікаво, що кожна мережа (чи відділ компанії) може мати свою унікальну номерну комбінацію. Це дає змогу швидко визначити, з якого саме відділу здійснюється дзвінок або куди він надходить. Такий підхід підвищує організованість та спрощує адміністрування телефонної системи. Наприклад, у мережі FILIAL 2 для цього була обрана комбінація з цифрою 1. Таким чином, номер 101 означає, що дзвінок йде з відділу 1 (перша цифра), а 01 - це конкретний номер телефону в цьому відділі.

Усі деталі налаштування на Router1, що забезпечують підтримку IP-телефонії, можна переглянути у Додатку А.

4.3 Тестування спроєктованої IP телефонії

Щоб переконатися в правильності побудови мережі, її працездатності та здатності підтримувати стабільну роботу IP-телефонії, було проведено тестування за допомогою інструментів симулятора Cisco Packet Tracer. Таке тестування дозволяє перевірити зв’язок між різними мережевими сегментами, оцінити швидкість передачі даних, стабільність з’єднання, а також виявити можливі помилки або недоліки в налаштуваннях.

Особливу увагу було приділено перевірці голосового трафіку, його коректній маршрутизації, відсутності затримок та втрат даних. Завдяки використанню Cisco Packet Tracer стало можливим наочно продемонструвати взаємодію між пристроями в різних VLAN, перевірити доступність основних сервісів і впевнитися, що мережа відповідає заданим вимогам.

На рис. 4.4 скріншот виводу команди «sh ephone» з Cisco маршрутизатора, що виконує роль Call Manager Express (CME). Ця команда

показує стан IP-телефонів, зареєстрованих на цьому CME, а також деякі додаткові деталі зі схеми мережі. Цей вивід надає інформацію про кожен зареєстрований IP-телефон (ephone), наприклад для ephone-4:

– Mac: 0004.9A77.30ED: MAC-адреса телефону;

– REGISTERED in SCCP ver 12: зареєстрований;

– IP: 172.25.71.13: IP-адреса з голосового VLAN 70;

– button 1: dn 4 number 104 CH1 IDLE;

– dn 4: прив'язаний до Directory Number 4;

– number 104: це унікальний телефонний номер;

– IDLE: телефон знаходиться у стані очікування.

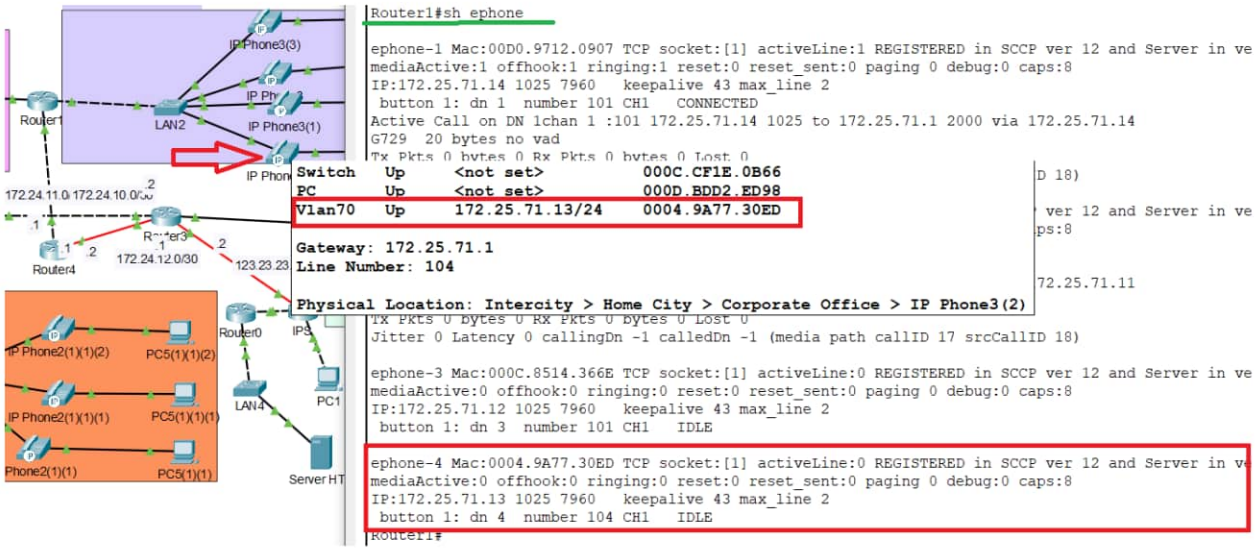


Рисунок 4.4 – Перевірка зв’язку між телефонами в різних мережах

Дані про ephone-4:

– MAC-адреса 0004.9A77.30ED та його IP 172.25.71.13/24 – це той самий телефон, що і ephone-4 у виводі sh ephone;

– VLAN 70 IP: 172.25.71.13/24: підтверджує, що IP-адреса 172.25.71.13 належить до підмережі 172.25.71.0 з маскою /24;

– Gateway: 172.25.71.1: це IP-адреса шлюзу за замовчуванням для голосового VLAN 70 і це IP-адреса інтерфейсу маршрутизатора (Router1) для цього VLAN.

– Line Number: 104: це номер телефону, який асоціюється з IP Phone3(2) на схемі.

Це відповідає ephone-4 у виводі sh ephone. В цілому, система працює, телефони реєструються та можуть здійснювати дзвінки

На рисунку 4.5 здійснено тестування вихідних і вхідних викликів Phone_106→ Phone_104:

– набір номера 104;

– телефон Phone_104 отримує виклик.

– після підняття слухавки встановлено двосторонній голосовий зв'язок.

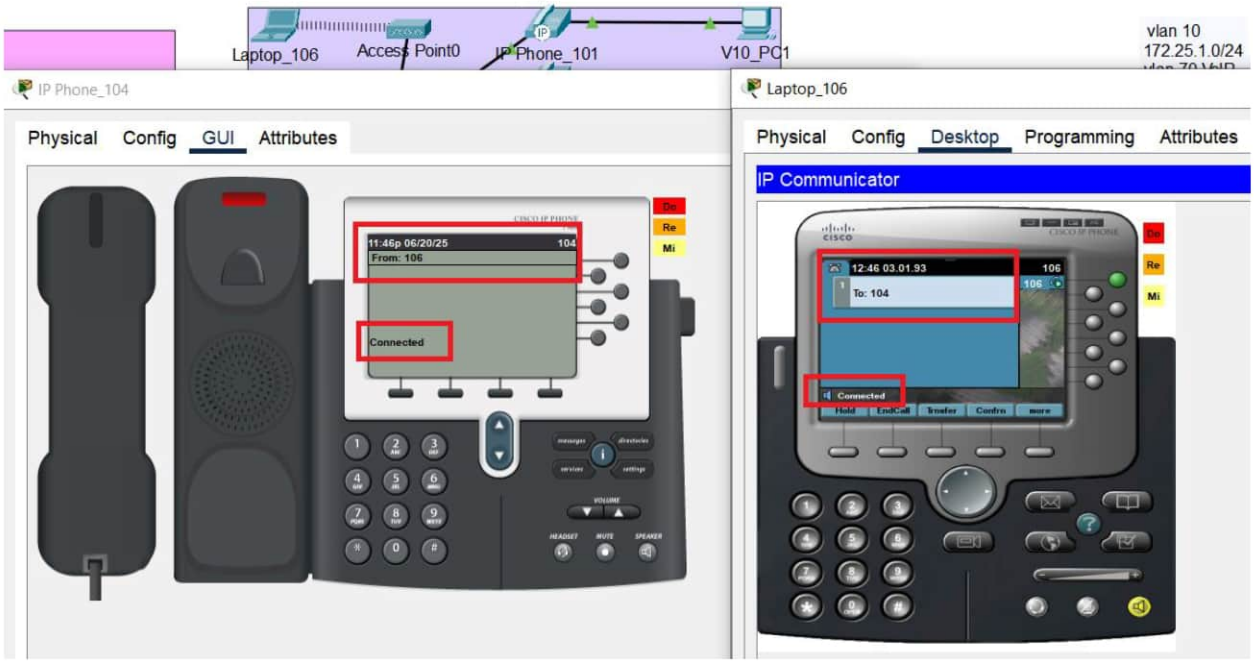


Рисунок 4.5 – Перевірка голосових викликів

4.4 Розрахунок необхідної пропускної здатності: приклад G.711/Ethernet

Пропускна здатність – це максимальний обсяг даних, який може бути переданий через мережеве з'єднання за певний проміжок часу, зазвичай вимірюється в бітах за секунду (bps). У контексті передачі голосу через IP (VoIP), пропускна здатність має вирішальне значення для підтримки якості розмови. Голос, на відміну від багатьох типів даних, є чутливим до затримок (latency) та варіацій затримки (jitter). Будь-яке значне відхилення від ідеальних

умов може спричинити погіршення сприйняття мови, ехо або навіть розриви зв'язку.

Стандарт G.711 є одним з найпоширеніших кодеків для VoIP, який забезпечує якість голосу, порівнянну з якістю телефонної мережі загального користування (PSTN). Він є нестиснутим кодеком, що означає, що він не застосовує значного стиснення до аудіосигналу, що робить його досить "прожерливим" до пропускної здатності порівняно з іншими кодеками, такими як G.729. Однак, його переваги полягають у низькій затримці кодування/декодування та високій вірності відтворення звуку.

Передача голосу по мережах Ethernet передбачає інкапсуляцію голосових пакетів у складну ієрархію протоколів. Кожен рівень цієї ієрархії додає свої власні службові дані (headers), збільшуючи загальний розмір пакету та, як наслідок, вимоги до пропускної здатності. Точний розрахунок цих накладних витрат є ключовим для правильного планування мережі.

4.4.1 Кодек G.711 та його характеристики

G.711 – це стандартний кодек, розроблений ITU-T, який використовується для оцифровки аналогових аудіосигналів з частотою дискретизації 8000 семплів за секунду (8 kHz) і 8 біт на семпл. Це призводить до необробленої бітової швидкості 64 кбіт/с. Існує дві основні версії G.711:

Розмір необроблених даних – 64 кбіт/с. Однак, для передачі цих даних через IP-мережу, вони повинні бути інкапсульовані в пакети. Стандартним розміром голосового фрейму для G.711 є 20 мс аудіо.

Розрахунок бітової швидкості для G.711 (необроблена):

– частота дискретизації: 8000 семплів/секунду;

– глибина дискретизації: 8 біт/семпл;

– бітова швидкість = 8000 семплів/с * 8 біт/семпл = 64000 біт/с = 64 кбіт/с.

Розмір голосового фрейму (для 20 мс):

– кількість семплів у 20 мс = 8000 семплів/с * 0.020 с = 160 семплів;

– розмір фрейму = 160 семплів * 8 біт/семпл = 1280 біт = 160 байт.

Цей 160-байтовий голосовий фрейм є "корисним навантаженням" для подальшої інкапсуляції.

4.4.2 Накладні витрати протоколів

Для передачі голосового фрейму через IP-мережу, він послідовно інкапсулюється кількома протоколами, кожен з яких додає свій заголовок. Ми розглянемо типовий стек протоколів VoIP: RTP/UDP/IP/Ethernet.

1) Заголовок Real-time Transport Protocol (RTP)

RTP – це протокол транспортного рівня, призначений для доставки даних реального часу, таких як аудіо та відео. Він не гарантує доставку, але надає механізми для упорядкування пакетів, тимчасових міток та ідентифікації корисного навантаження.

Розмір заголовка RTP: 12 байт (мінімум). Можуть бути додаткові заголовки, але 12 байт є стандартним для базової функціональності.

2) Заголовок User Datagram Protocol (UDP)

UDP – це простий, беззв'язковий протокол транспортного рівня, який використовується для додатків, що вимагають швидкої, але не гарантованої доставки даних. Він ідеально підходить для VoIP, оскільки втрата декількох голосових пакетів менш критична, ніж затримка, спричинена механізмами повторної передачі TCP.

Розмір заголовка UDP: 8 байт.

3) Заголовок Internet Protocol (IP).

IP – це основний протокол мережевого рівня, який відповідає за маршрутизацію пакетів між мережами. Для VoIP зазвичай використовується IPv4, хоча IPv6 стає все більш поширеним. Розмір заголовка IPv4: 20 байт (мінімум). Можуть бути додаткові опції, але 20 байт є стандартним. Розмір заголовка IPv6: 40 байт. Для цілей нашого прикладу ми використовуватимемо IPv4.

4) Заголовок та трейлер Ethernet.

Ethernet – це найпоширеніший стандарт мережевого інтерфейсу на канальному рівні (рівень 2 моделі OSI). Він відповідає за фізичну передачу даних по дротових або бездротових з'єднаннях.

Заголовок Ethernet (Ethernet Header): 14 байт (включає MAC-адреси джерела та призначення, EtherType).

Трейлер Ethernet (Frame Check Sequence - FCS): 4 байти (використовується для виявлення помилок).

Преамбула та початковий роздільник кадру (Preamble & Start Frame Delimiter - SFD): 8 байт. Ці байти не є частиною кадру Ethernet, але передаються по дроту перед ним для синхронізації. Хоча вони не враховуються в розмірі кадру, вони споживають пропускну здатність на фізичному рівні.

Міжкадровий проміжок (Inter-frame Gap - IFG): 12 байт (96 біт). Це мінімальна пауза між передачею двох послідовних кадрів Ethernet, необхідна для обробки та підготовки мережевим обладнанням.

4.4.3 Повний розрахунок розміру пакета та пропускної здатності

1) Розмір корисного навантаження G.711

Голосовий фрейм G.711 (20 мс) = 160 байт

2) Розмір пакета на мережевому рівні (IP)

Голосовий фрейм G.711 = 160 байт

Заголовок RTP = 12 байт

Заголовок UDP = 8 байт

Заголовок IPv4 = 20 байт

Загальний розмір пакета IP = 160 + 12 + 8 + 20 = 200 байт

3) Розмір кадру на канальному рівні (Ethernet)

Пакет IP = 200 байт

Заголовок Ethernet = 14 байт

Трейлер Ethernet (FCS) = 4 байт

Загальний розмір кадру Ethernet = 200 + 14 + 4 = 218 байт

4) Розрахунок пропускної здатності на "дротовому" рівні

Для розрахунку "дротової" пропускної здатності необхідно врахувати всі байти, що передаються по кабелю, включаючи преамбулу, SFD та IFG.

Розмір кадру Ethernet = 218 байт

Преамбула + SFD = 8 байт

IFG = 12 байт

Загальний обсяг даних, переданих за один пакет = 218 + 8 + 12 = 238 байт

5) Розрахунок кількості пакетів на секунду (PPS)

Оскільки ми використовуємо 20 мс голосові фрейми, це означає, що за одну секунду передається 1000 мс / 20 мс = 50 пакетів.

Кількість пакетів на секунду (PPS) = 50 пакетів/с

6) Розрахунок необхідної пропускної здатності

Тепер ми можемо розрахувати бітову швидкість, множачи загальний обсяг даних на один пакет на кількість пакетів на секунду.

Бітова швидкість = (Загальний обсяг даних за один пакет в байтах) * (PPS) * 8 біт/байт

Бітова швидкість = 238 байт/пакет * 50 пакетів/с * 8 біт/байт

Бітова швидкість = 11900 * 8 біт/с = 95200 біт/с = 95.2 кбіт/с

Таким чином, для одного голосового дзвінка з кодеком G.711 (20 мс фрейми) через Ethernet (з IPv4), необхідна пропускна здатність на "дротовому" рівні становить приблизно 95.2 кбіт/с.

4.4.4 Додаткові фактори

Хоча вищенаведений розрахунок є досить точним для одного потоку, у реальних мережевих середовищах є кілька додаткових факторів, які слід враховувати.

Сигналізація.

Протоколи сигналізації, такі як SIP (Session Initiation Protocol) або H.323, також споживають невелику кількість пропускної здатності. Хоча їхній вплив на загальну пропускну здатність значно менший, ніж голосові потоки, вони є важливими для встановлення, підтримки та завершення дзвінків.

Quality of Service (QoS).

Механізми QoS, такі як Differentiated Services Code Point (DSCP) або 802.1p, використовуються для пріоритизації голосового трафіку над іншими типами даних. Хоча вони не змінюють необхідну пропускну здатність, вони забезпечують, що доступна пропускна здатність буде ефективно використана для голосу.

Стиснення заголовків (Header Compression).

Протоколи, такі як cRTP (compressed RTP), можуть значно зменшити накладні витрати на заголовки RTP/UDP/IP, особливо для невеликих пакетів. cRTP може зменшити розмір заголовка з 40 байт до 2-4 байт, що суттєво економить пропускну здатність, особливо на низькошвидкісних лініях:

– при використанні cRTP, 40 байт (RTP+UDP+IP) може бути зменшено до, наприклад, 4 байт;

– розмір пакета IP = 160 (голос) + 4 (стиснутий заголовок) = 164 байт;

– розмір кадру Ethernet = 164 + 14 + 4 = 182 байт;

– загальний обсяг даних = 182 + 8 + 12 = 202 байт;

– пропускна здатність = 202 * 50 * 8 = 80800 біт/с = 80.8 кбіт/с;

Це показує, що стиснення заголовків може заощадити близько 15% пропускної здатності для G.711.

Загальна кількість дзвінків.

Для розрахунку загальної пропускної здатності, необхідної для N одночасних дзвінків, просто помножте вимогу одного дзвінка на N. Наприклад, для 100 одночасних дзвінків з G.711: 95.2 кбіт/с/дзвінок * 100 дзвінків = 9520 кбіт/с = 9.52 Мбіт/с.

Двосторонній трафік.

Голосові дзвінки є двосторонніми. Тому, якщо розрахунки ведуться для односпрямованого трафіку, необхідно подвоїти результат для повного дуплексного з'єднання. Наведені розрахунки вже враховують односпрямований потік, тому для 100 двосторонніх дзвінків це буде 100 * (95.2

кбіт/с вхідний + 95.2 кбіт/с вихідний) = 19.04 Мбіт/с (загальна пропускна здатність).

Інші кодеки.

Якщо використовуються інші кодеки (наприклад, G.729, G.722), то їхня базова бітова швидкість та розмір фрейму будуть відрізнятися, що вимагатиме перерахунку. Наприклад, G.729 має бітову швидкість 8 кбіт/с та зазвичай використовує 10 мс фрейми, що значно зменшує вимоги до пропускної здатності, але збільшує відносний вплив накладних витрат.

Jitter Buffers.

Для компенсації варіацій затримки (jitter), VoIP-пристрої використовують буфери джиттера. Це додає невелику затримку, але покращує якість голосу. Їхнє використання не впливає на необхідну пропускну здатність, але є важливою частиною дизайну VoIP-системи.

Розмір MTU (Maximum Transmission Unit).

Розмір пакета не повинен перевищувати MTU мережевого шляху, щоб уникнути фрагментації, яка може призвести до додаткових затримок та втрат. Стандартний MTU для Ethernet становить 1500 байт, що значно перевищує розмір голосового пакета.

ВИСНОВКИ

У ході виконання дипломної роботи було розроблено та детально проаналізовано функціональну модель корпоративної мережі, призначеної для кіберфізичної системи IP-телефонії, адаптованої до потреб туристичної компанії. Основною метою створення даної мережі було забезпечення стабільного, масштабованого та якісного каналу зв'язку, що повністю відповідає сучасним технічним вимогам туристичної індустрії - сфери, яка потребує оперативної, безперебійної комунікації з великою кількістю клієнтів, партнерів і внутрішніх структур

Проєктна мережа побудована з урахуванням принципів логічного поділу трафіку між структурними підрозділами організації, шляхом впровадження віртуальних локальних мереж (VLAN). Кожен відділ компанії отримав власну ізольовану підмережу, що дозволяє обмежити доступ до конфіденційних даних і знизити ризик несанкціонованого втручання. Такий підхід сприяє як підвищенню безпеки, так і оптимізації внутрішнього трафіку в межах організації

Особливу увагу в проєкті було приділено голосовому трафіку. Для його обробки й передачі було виділено окрему VLAN з номером 70, яка використовується виключно для IP-телефонії. Завдяки цьому досягається фізична й логічна ізоляція голосових даних від інших типів трафіку. Така сегментація дозволяє суттєво зменшити ймовірність затримок, втрати пакетів і збоїв у комунікації.

Топологічна структура мережі була спроєктована з орієнтацією на майбутнє масштабування. Це означає, що в разі розширення компанії або відкриття нових філій, існуюча інфраструктура дозволяє без суттєвих витрат і труднощів додати нові пристрої. Більше того, автоматизований підхід до налаштування обладнання, завдяки використанню централізованих шаблонів конфігурацій та протоколів дистанційного керування, значно зменшує ризик

людських помилок і пришвидшує процес інтеграції нових елементів у вже існуючу систему.

Створена топологія відповідає вимогам технічного завдання і демонструє не лише технічну реалізованість запропонованої архітектури, але й високий рівень деталізації логічної структури мережі, що є важливим аспектом при впровадженні реального IP-телефонного середовища на базі кіберфізичної інфраструктури.

Розроблена система IP-телефонії має значний потенціал для туристичних компаній, оскільки забезпечує економічно вигідну, безпечну та гнучку платформу для комунікацій. Вона дозволяє оптимізувати взаємодію з клієнтами, підвищити ефективність внутрішніх процесів і адаптуватися до змін у бізнес-потребах. Система може бути використана як у невеликих туристичних агентствах, так і у великих компаніях із розподіленими офісами, що робить її універсальним рішенням.

Точний розрахунок необхідної пропускної здатності є наріжним каменем успішного розгортання VoIP-систем. Як показано, для кодека G.711 з 20 мс фреймами, переданого через Ethernet (IPv4), один голосовий потік споживає приблизно 95.2 кбіт/с пропускної здатності на "дротовому" рівні. Це число значно перевищує базову бітову швидкість 64 кбіт/с G.711, що підкреслює важливість врахування всіх протокольних накладних витрат.

Ігнорування цих накладних витрат при плануванні мережі може призвести до недостатньої пропускної здатності, що виявиться в погіршенні якості голосу, проблемах зі зв'язком та незадоволеністю користувачів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Іванов І. І. IP-телефонія: технології та безпека : навчальний посібник / І. І. Іванов ; Нац. техн. ун-т України «Київ. політехн. ін-т». - Київ : Вид-во НТУУ «КПІ», 2020. - 256 с.

2. Петренко О. М. Безпека мереж IP-телефонії : монографія / О. М. Петренко ; Львів. нац. ун-т ім. Івана Франка. - Львів : Вид-во ЛНУ ім. Івана Франка, 2019. - 320 с.

3. Сидоренко Т. В. Проєктування корпоративних мереж для IP-телефонії : навчальний посібник / Т. В. Сидоренко ; Нац. техн. ун-т «Дніпр. політехніка». - Дніпро : Вид-во НТУ «ДП», 2018. - 280 с.

4. Коваленко М. П. Впровадження систем IP-телефонії в туристичних компаніях : наук. вид. / М. П. Коваленко ; Харків. нац. ун-т ім. В. Н. Каразіна. - Харків : Вид-во ХНУ ім. В. Н. Каразіна, 2017. - 200 с.

5. Бондаренко Л. О. Стандарти безпеки для IP-телефонії : монографія / Л. О. Бондаренко ; Одес. нац. ун-т ім. І. І. Мечникова. - Одеса : Вид-во ОНУ ім. І. І. Мечникова, 2016. - 240 с.

6. Ткаченко В. М. Аналіз загроз для систем IP-телефонії / В. М. Ткаченко // Наук. праці Нац. авіац. ун-ту : зб. наук. праць. - 2015. - № 2 (45). - С. 123–130.

7. Lee E. A. Cyber Physical Systems: Design Challenges / E. A. Lee // University of California, Berkeley Technical Report No. UCB/EECS-2008-8. - Berkeley : University of California, 2008. - 12 p. - [Електронний ресурс]. - Режим доступу: https://www2.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-8.html.

8. Cisco Systems, Inc. Cisco IP Phone 8800 Series Data Sheet [Електронний ресурс]. - San Jose : Cisco Systems, Inc., 2023. - Режим доступу: https://www.cisco.com/c/en/us/products/collaboration-endpoints/ip-phone-8800-series/index.html.

9. Cisco Systems, Inc. Cisco Catalyst 9300 Series Switch Data Sheet [Електронний ресурс]. - San Jose : Cisco Systems, Inc., 2023. - Режим доступу:

https://www.cisco.com/c/en/us/products/switches/catalyst-9300-series-switches/index.html.

10. IP-телефонія «з нуля»: 4 кроки для правильної організації - EServer. Мережеве обладнання. Купити серверне обладнання в Києві, Дніпрі - EServer. URL: https://e-server.com.ua/uk/poradi/ip-telefonija-z-nulja-4-kroki-dlja-pravilnoi-organizacii?srsltid=AfmBOorGrkYWa65xiFg2WwbCFrfuMurzB51ZRCdThgZWNP7gyJytCkrJ (дата звернення: 28.06.2025).

11. ITU-T Recommendation G.114: One-way Transmission Time [Електронний ресурс]. - Geneva : ITU-T, 2003. - Режим доступу: https://www.itu.int/rec/T-REC-G.114-200305-I.

12. ISO/IEC 27001:2013 Information Security Management Systems [Електронний ресурс]. - Geneva : ISO/IEC, 2013. - Режим доступу: https://www.iso.org/standard/54534.html.

13. White J. R&D challenges for mobile cyber-physical applications / J. White, S. Clarke, B. Dougherty // Journal of Internet Services and Applications. - 2010. - Vol. 1, No. 1. - P. 45–56. - [Електронний ресурс]. - Режим доступу: https://link.springer.com/article/10.1007/s13174-010-0004-x.

14. Wan J. Advances in Cyber-Physical Systems Research / J. Wan, M. Chen, F. Xia // KSII Transactions on Internet and Information Systems. - 2011. - Vol. 5, No. 11. - P. 1891–1908. - [Електронний ресурс]. - Режим доступу: https://www.ksii.or.kr/ksii/html/article_view.action?articleId=TIIS.2011.5.11.1891.

15. Чорнобривець О. В. Кіберфізичні системи в туризмі: сучасні тенденції / О. В. Чорнобривець // Вісник Київського національного університету культури і мистецтв. - 2021. - № 4. - С. 78–85.

16. Ковальчук О. П. Інформаційні технології в туристичному бізнесі / О. П. Ковальчук // Економіка та управління туризмом. - 2018. - № 3. - С. 112–120.

17. RFC 3261: SIP: Session Initiation Protocol [Електронний ресурс]. - IETF, 2002. - Режим доступу: https://www.rfc-editor.org/rfc/rfc3261.

18. RFC 3550: RTP: A Transport Protocol for Real-Time Applications [Електронний ресурс]. - IETF, 2003. - Режим доступу: https://www.rfc-editor.org/rfc/rfc3550.

19. Cisco Systems, Inc. Cisco Unified Communications Manager Administration Guide [Електронний ресурс]. - San Jose : Cisco Systems, Inc., 2023. - Режим доступу: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-administration-guides-list.html.

20. Lammle T. CCNA Routing and Switching Study Guide: Exams 100-105, 200-105, and 200-125 / T. Lammle. - Indianapolis : Wiley, 2017. - 1176 p.

21. Cisco Systems, Inc. Cisco Packet Tracer User Guide [Електронний ресурс]. - San Jose : Cisco Systems, Inc., 2023. - Режим доступу: https://www.netacad.com/courses/packet-tracer.

22. Бондар О. В. Цифрова трансформація туристичної галузі / О. В. Бондар // Науковий вісник Ужгородського національного університету. - 2022. - № 1. - С. 45–52.

23. Кравець П. О. Захист інформації в корпоративних мережах / П. О. Кравець // Інформаційні технології та комп’ютерна інженерія. - 2019. - № 2. - С. 67–74.

Додаток А

Текст програми налаштування IP-телефонії на Router 1

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ КОМУТАТОРА SW_R1

Текст програми

804.02070743.25012-01 12 01

Листів 5

2025

АНОТАЦІЯ

Дане налаштування належить маршрутизатору 2811 та включає в себе налаштування для IP-телефонії

ЗМІСТ

1) Активація сервісу "telephony-service" (CME) та базові налаштування.

Це головний крок для ввімкнення функціоналу Call Manager Express на маршрутизаторі.

```
Router1(config)# telephony-service
!
! Максимальна кількість телефонних номерів (Directory Numbers)
! Кількість повинна бути достатньою для телефонів та розширень.
Router1(config-telephony)# max-dn 100
!
! Максимальна кількість фізичних IP-телефонів (ephones)
! Це ліцензійне обмеження для CME, залежить від моделі маршрутизатора.
Router1(config-telephony)# max-ephones 50
!
! IP-адреса та порт, які CME буде використовувати для зв'язку з телефонами.
! Це має бути IP-адреса інтерфейсу маршрутизатора, що належить до голосового VLAN.
! Порт 2000 - стандартний для Skinny (SCCP) протоколу, але може бути SIP-порт.
Router1(config-telephony)# ip source-address 172.25.71.1 port 2000
! Повідомлення, що відображатиметься на екранах телефонів.
Router1(config-telephony)# system message "Welcome to My Office"
!
! Інтервал Keepalive для телефонів (скільки часу CME чекає відповіді від телефону).
Router1(config-telephony)# keepalive 30
!
! Формат часу та дати на дисплеях телефонів.
Router1(config-telephony)# time-format 24
Router1(config-telephony)# date-format dd-mm-yy
!
! Автоматичне призначення телефонних номерів.
! Зазвичай краще робити вручну для контролю, але для тестування можна ввімкнути.
Router1(config-telephony)# auto assign 1 to 50
Router1(config-telephony)# exit
```

2) Створення телефонних номерів (Directory Numbers, DN).

Кожен телефонний номер є логічним об'єктом, який потім буде призначений фізичному телефону. Номери призначатимуться за принципом: №08, де № – номер мережі.

```
Router1(config)# ephone-dn 1
Router1(config-ephone-dn)# number 101
Router1(config-ephone-dn)# description "IP Phone3(1) – VLAN10"
```

```
Router1(config-ephone-dn)# exit

Router1(config)# ephone-dn 2
Router1(config-ephone-dn)# number 102
Router1(config-ephone-dn)# description "IP Phone3(2) - VLAN10"
Router1(config-ephone-dn)# exit

Router1(config)# ephone-dn 3
Router1(config-ephone-dn)# number 103
Router1(config-ephone-dn)# description "IP Phone3(3) - VLAN10"
Router1(config-ephone-dn)# exit
```

3) Реєстрація фізичних телефонів (ephones) та прив'язка до DN

Тут ми вказуємо MAC-адреси фізичних IP-телефонів і призначаємо їм створені раніше телефонні номери.

```
ephone 1
 device-security-mode none
 mac-address 00D0.9712.0907
 type 7960
 button 1:1
!
ephone 2
 device-security-mode none
 mac-address 000C.CF69.DE3E
 type 7960
 button 1:2
!
ephone 3
 device-security-mode none
 mac-address 000C.8514.366E
 type 7960
 button 1:3
!
ephone 4
 device-security-mode none
 mac-address 0004.9A77.30ED
 type 7960
 button 1:4
```