ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Розробка автоматизованої системи багатоадресного аудіосповіщення (Audio-over-IP) для територіально розподілених об'єктів»

на здобуття освітнього ступеня бакалавра
зі спеціальності 123 Комп'ютерної інженерії
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерна інженерія
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ *Тетяна БРОВЧЕНКО*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. КІД-41
Тетяна БРОВЧЕНКО
Ім'я, ПРІЗВИЩЕ
Керівник: Ігор БУЧЕНКО
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ
Рецензент:
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра 123 Комп'ютерної інженерії

Ступінь вищої освіти бакалавр

Спеціальність 123 Комп'ютерної інженерії

Освітньо-професійна програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедри
Комп'ютерної інженерії
_____ Наталія ЛАЩЕВСЬКА
_____
«_____» _____ 2026р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Бровченко Тетяна Яківна
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Розробка автоматизованої системи багатоадресного аудіосповіщення (Audio-over-IP) для територіально розподілених об'єктів
керівник кваліфікаційної роботи Ігор БУЧЕНКО,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «20» лютого 2026р. № 51
2. Строк подання кваліфікаційної роботи «8» травня 2026р.
3. Вихідні дані до кваліфікаційної роботи:передача пакетів, мережева топологія, OSI, AoIP, IGMP, LAN, WAN, NTP, PIM, RTCP, RTP, SIP, TCP, UDP
4. -пояснювальної записки (перелік питань, які потрібно розробити)
1. Принцип побудови та протоколи системи Audio-over-IP
2. Проєктування мережевої інфраструктури
3. Реалізація та аналіз роботи системи
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання «20» лютого 2026р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	20.02-19.03.2026	Виконано
2	Обробка матеріалу	20.03-08.04.2026	Виконано
3	Розробка теоретичної частини	09.04-14.04.2026	Виконано
4	Розробка моделі мережі	14.04-18.04.2026	Виконано
5	Висновки за результатами аналізу	19.04-23.04.2026	Виконано
6	Оформлення пояснювальної записки	24.00-02.05.2026	Виконано
7	Розробка презентації	03.05-05.05.2026	Виконано
8	Передзахист	08.05-11.05.2026	Виконано
9	Здача в деканат	08.06-14.06.2026	Виконано

Здобувач вищої освіти _____ Тетяна БРОВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Ігор БУЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 69 стор., 21 рис., 4 табл., 47 джерел.

Мета роботи – Підвищення надійності, автономності та масштабованості систем масового сповіщення шляхом розробки автоматизованого програмно-апаратного комплексу на базі технологій Audio-over-IP із прив'язкою до сервера точного часу.

Об'єкт дослідження – процес передачі потокових аудіоданих та управління комунікаційними сеансами у територіально розподілених комп'ютерних мережах

Предмет дослідження – Апаратно-програмні засоби та мережеві протоколи (SIP, RTP, Multicast, NTP) для автоматизації систем масового сповіщення

Короткий зміст роботи: У кваліфікаційній роботі розглянуто фундаментальні засади та переваги технології Audio-over-IP порівняно з традиційними аналоговими комплексами. Проведено аналіз ключових мережевих протоколів прикладного та транспортного рівнів, що забезпечують передачу та маршрутизацію медіаданих у режимі реального часу, а також визначено роль протоколів синхронізації часу для уникнення акустичних спотворень. Проаналізовано принципи адресації, сегментації та забезпечення якості обслуговування в архітектурі центро-периферійної взаємодії (Hub-and-Spoke). Проведено практичне моделювання розробленої мережевої інфраструктури в середовищі Cisco Packet Tracer з налаштуванням логічної імітації передачі потокового аудіо. Результати підтверджують доцільність використання обраних інженерних рішень та стека протоколів для створення сучасних, масштабованих і надійних систем масового оповіщення.

КЛЮЧОВІ СЛОВА: AUDIO-OVER-IP, БАГАТОАДРЕСНА РОЗСИЛКА, МУЛЬТИКАСТ, SIP, RTP, МАРШРУТИЗАЦІЯ, CISCO PACKET TRACER/

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ…….. 8
ВСТУП……..... 9
1 ПРИНЦИПИ ПОБУДОВИ ТА ПРОТОКОЛИ СИСТЕМИ AUDIO-OVER-IP……..... 10
1.1 Загальна характеристика систем аудіосповіщення……... 10
1.2 Основна інформація про Audio-over-IP(AoIP)…… 12
1.3 Основні протоколи забезпечення роботи AoIP (RTP, SIP, UDP)…… 16
1.4 Дослідження механізмів багатоадресної розсилки (IP Multicast) та його відмінність від Unicast і Broadcast……... 23
1.5 Використання протоколів синхронізації часу (NTP та PTP) в AoIP…... 31
2 ПРОЄКТУВАННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ…….. 38
2.1 Загальна архітектура типу Hub-and-Spoke та основні компоненти системи…… 38
2.2 Адресація та сегментація мережі…… 39
2.3 Вибір протоколів передачі даних……... 41
2.4 Проєктування логічної структури системи та сценарії роботи……...… 42
2.5 Забезпечення якості обслуговування (QoS)……...… 43
3 РЕАЛІЗАЦІЯ ТА АНАЛІЗ РОБОТИ СИСТЕМИ……...…… 45
3.1 Вибір середовища моделювання…….…… 45
3.2 Побудова моделі мережі…….. 46
3.3 Налаштування багатоадресної передачі……. 51
3.4 Реалізація передачі аудіо та тестування роботи системи……. 52
ВИСНОВКИ…….. 55
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ…….. 57
Додаток А (Демонстраційні матеріали. Презентація)…… 62

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AoIP (Audio-over-IP) – технологія передачі цифрового аудіо через IP-мережі

DHCP (Dynamic Host Configuration Protocol) – протокол динамічного налаштування вузла

IGMP (Internet Group Management Protocol) – протокол управління групами Інтернету

LAN (Local Area Network) – локальна обчислювальна мережа

NTP (Network Time Protocol) – протокол мережевого часу

OSI (Open Systems Interconnection) – еталонна модель взаємодії відкритих систем

PA (Public Address) – система трансляції фонової музики та службових повідомлень

PIM (Protocol Independent Multicast) – незалежна від протоколу багатоадресна розсилка

PTP (Precision Time Protocol) – протокол точного часу

QoS (Quality of Service) – якість обслуговування

RTCP (Real-time Transport Control Protocol) – протокол управління передачею в реальному часі

RTP (Real-time Transport Protocol) – протокол передачі в реальному часі

SIP (Session Initiation Protocol) – протокол ініціювання сеансу

SPL (Sound Pressure Level) – рівень звукового тиску

STI (Speech Transmission Index) – індекс передачі мови

TCP (Transmission Control Protocol) – протокол управління передачею

UDP (User Datagram Protocol) – протокол користувацьких датаграм

VA (Voice Alarm) – система екстреного мовленнєвого сповіщення

VLAN (Virtual Local Area Network) – віртуальна локальна мережа

WAN (Wide Area Network) – глобальна обчислювальна мережа

ВСТУП

Системи аудіосповіщення та керування евакуацією є критично важливими інфраструктурними компонентами будь-якого територіально розподіленого об'єкта. Сучасні вимоги до безпеки, інформування населення та управління технологічними процесами диктують необхідність переходу від традиційних аналогових трансляційних ліній до повністю цифрових автоматизованих комплексів, що функціонують на базі глобальних та локальних комп'ютерних мереж. Використання технології Audio-over-IP дозволяє подолати фундаментальні обмеження класичної централізованої архітектури, забезпечуючи високу масштабованість, відмовостійкість та гнучкість маршрутизації аудіопотоків без необхідності прокладання дороговартісних спеціалізованих мідних трас. Завдяки комутації пакетів сучасні підприємства отримують можливість використовувати вже існуючу IT-інфраструктуру для конвергенції даних, голосу та систем життєзабезпечення.

Актуальність теми кваліфікаційної роботи зумовлена тим, що для ефективної та надійної роботи таких розподілених систем необхідна бездоганна фазова синхронізація аудіосигналів, мінімізація транспортних затримок та жорстка оптимізація мережевого трафіку при одночасній передачі екстрених повідомлень на сотні або тисячі кінцевих пристроїв. Це вимагає від інженерів глибокого розуміння та комплексного впровадження стека мережевих протоколів, зокрема транспортних протоколів у реальному часі, гнучких засобів ініціювання сеансів та алгоритмів багатоадресної маршрутизації. Метою роботи є дослідження принципів побудови та розробка мережевої архітектури автоматизованої системи багатоадресного аудіосповіщення для територіально розподілених об'єктів із подальшим її моделюванням у спеціалізованому програмному середовищі. Для досягнення цієї мети в роботі досліджуються теоретичні засади акустики та цифрової передачі звуку, детально аналізуються механізми одноадресної та багатоадресної розсилки, а також розробляється топологія мережі на базі концепції центро-периферійної взаємодії з відповідним налаштуванням телекомунікаційного обладнання.

1 ПРИНЦИПИ ПОБУДОВИ ТА ПРОТОКОЛИ СИСТЕМИ AUDIO-OVER-IP

1.1 Загальна характеристика систем аудіосповіщення

Системи аудіосповіщення є критично важливими інфраструктурними компонентами будь-якого територіально розподіленого об'єкта. Вони забезпечують виконання широкого спектра завдань: від трансляції фонової музики та службових повідомлень (Public Address, PA) до екстреного мовленнєвого сповіщення про надзвичайні ситуації (Voice Alarm, VA). Такі системи пройшли тривалий шлях еволюції від традиційних аналогових трансляційних ліній до повністю цифрових автоматизованих комплексів, що функціонують на базі локальних (LAN) та глобальних (WAN) комп'ютерних мереж.

Розуміння роботи систем аудіосповіщення неможливе без знання основ акустики. Звук розповсюджується у просторі у вигляді поздовжніх хвиль, що виникають внаслідок коливань тиску повітря (рис. 1.1). Інтенсивність цих коливань визначається рівнем звукового тиску (Sound Pressure Level, SPL), який вимірюється в децибелах (дБ) і відображає різницю між тиском, створюваним звуковою хвилею, та навколишнім атмосферним тиском. Діапазон сприйняття людського вуха зазвичай становить від 0 дБ (поріг чутності) до 120-130 дБ (больовий поріг). Під час проектування систем екстреного оповіщення головною вимогою є забезпечення такого рівня SPL, який перевищував би рівень фонового шуму в приміщенні щонайменше на 10-15 дБ, щоб гарантувати привернення уваги людей.

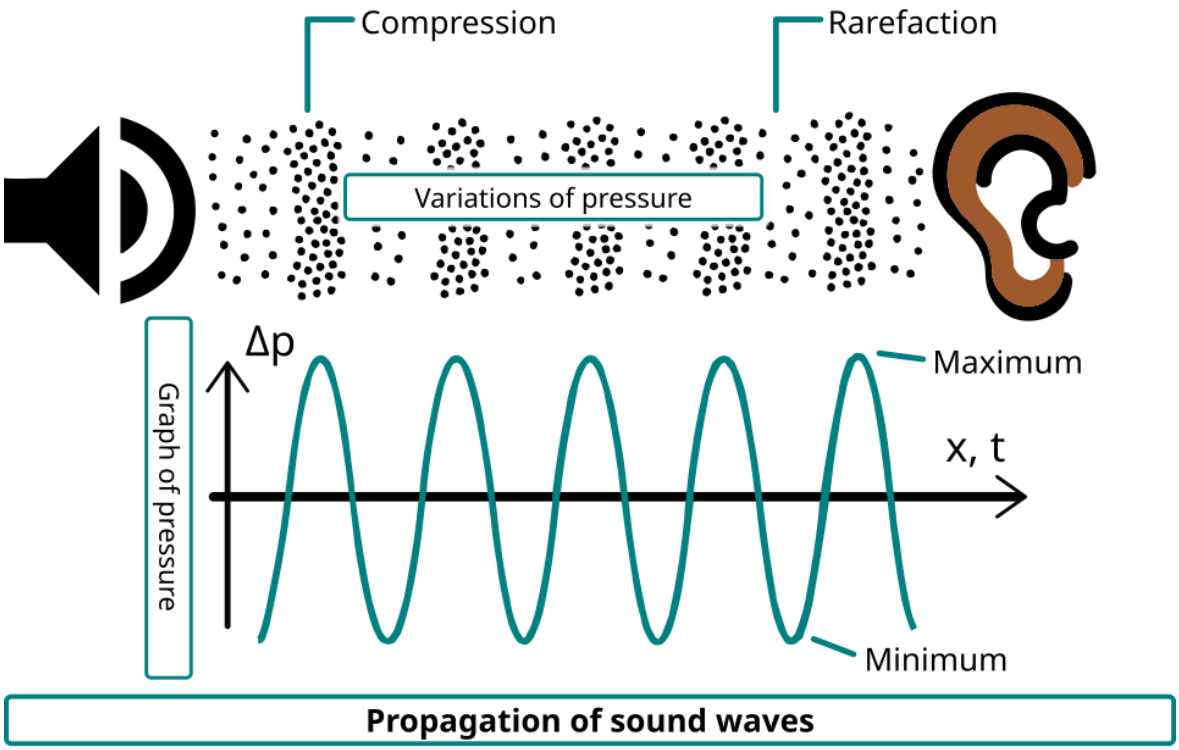


Рисунок 1.1 – Схема розповсюдження звуку у просторі

Але забезпечення високого рівня SPL не є достатньою умовою для ефективного функціонування системи. Надзвичайно важливим параметром є індекс передачі мови (Speech Transmission Index, STI), який характеризує розбірливість трансльованого повідомлення. Під час поширення в середовищі звукові хвилі зазнають впливу таких фізичних явищ, як відбиття, поглинання, рефракція та просторова інтерференція. У закритих приміщеннях зі складними акустичними умовами або на великих відкритих просторах звукові хвилі від різних гучномовців можуть накладатися одна на одну, створюючи реверберацію (ефект, коли звук багаторазово відбивається від поверхонь і поступово згасає) та ефект відлуння, що критично знижує розбірливість мови. Для територіально розподілених об'єктів ця проблема загострюється через необхідність ідеальної фазової синхронізації аудіосигналів між віддаленими кластерами гучномовців.6 Якщо сигнал від одного пристрою досягає слухача навіть з мінімальною затримкою відносно іншого пристрою, виникає так званий ефект гребінчастої фільтрації, що спотворює амплітудно-частотну характеристику звуку.

Територіально розподілені об'єкти, такі як мережі залізничних станцій,

великі промислові підприємства, логістичні хаби, університетські кампуси або системи загальноміського оповіщення, створюють додаткові виклики для розробників. Використання класичної централізованої архітектури для таких об'єктів є технічно складним та економічно неефективним. Тому сучасні інженерні концепції передбачають використання децентралізованих (розподілених) архітектур на основі технологій Audio-over-IP (AoIP).

Розподілена архітектура передбачає, що обробка аудіосигналів та прийняття рішень щодо маршрутизації відбуваються не в єдиному центральному процесорі, а розподіляються між периферійними пристроями (edge computing). У таких мережах кожен кінцевий пристрій, будь то IP-гучномовець, цифровий підсилювач, мікрофонна консоль або датчик фонового шуму, є самостійним мережевим вузлом із власною унікальною IP-адресою. Це дозволяє пристроям обмінюватися даними та керуючими сигналами безпосередньо через існуючу мережеву інфраструктуру, створюючи високонадійні відмовостійкі топології. Завдяки децентралізації, вихід з ладу одного мережевого сегмента або окремого пристрою не призводить до паралічу всієї системи оповіщення, що є критично важливим фактором для систем забезпечення безпеки життєдіяльності.

1.2. Основна інформація про Audio over IP(AoIP)

Audio-over-IP (AoIP) — це передова технологія, що забезпечує передачу високоякісного цифрового (як нестисненого, так і стисненого) звуку через стандартні IP-мережі, включаючи LAN, WAN та мережу Інтернет (рис.1.2). Ця технологія кардинально змінює парадигму розробки інфраструктурних рішень для трансляції медіаданих, переходячи від використання спеціалізованих кабельних систем до універсального мережевого середовища.

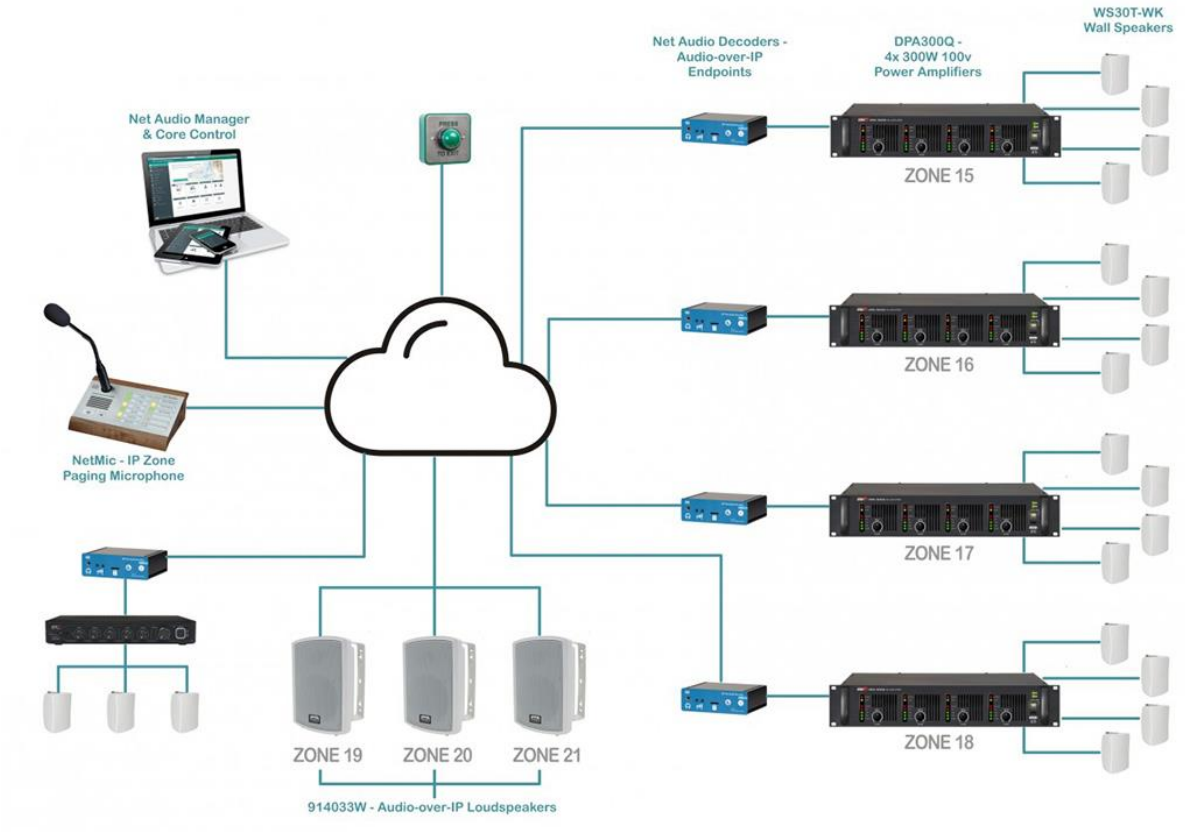


Рисунок 1.2 – Приклад системи AoIP

Історично професійна маршрутизація та передача цифрового звуку спиралися на технології, що використовували принцип комутації каналів (Circuit Switching) та часове мультиплексування (Time Division Multiplexing, TDM). До таких технологій належать, зокрема, стандарти AES3 (відомий також як AES/EBU) та AES10 (відомий як MADI). Протокол AES3 дозволяв передавати два канали нестисненого аудіо через екрановану виту пару або коаксіальний кабель у режимі реального часу з мінімальною затримкою. Протокол MADI став еволюційним прототипом цієї ідеї, дозволивши робити мультиплекс до 64 каналів звуку в одному коаксіальному або оптоволоконному кабелі.

Незважаючи на високу надійність цих інтерфейсів у межах однієї апаратної або студії, топологія "точка-точка" (point-to-point) робить їх вкрай неефективними для територіально розподілених об'єктів. Створення розгалуженої системи оповіщення на базі MADI вимагало б прокладання окремих фізичних ліній до кожного вузла, а також використання дорогих і складних апаратних маршрутизаторів. Крім того, традиційні з'єднання є неефективними з точки зору

використання смуги пропускання: лінія зв'язку резервується повністю незалежно від того, передається по ній 64 канали чи лише один службовий сигнал.

Технологія AoIP базується на фундаментально іншому принципі – комутації пакетів (Packet Switching). Замість виділення постійного фізичного або логічного каналу, цифровий аудіопотік розбивається на окремі невеликі фрагменти (IP-пакети). Ці пакети передаються мережею спільно з іншими видами трафіку (даними підприємства, відеоспостереженням, керуючими сигналами систем розумного будинку тощо), спільно використовуючи загальну пропускну здатність мережевих ліній. Завдяки цьому досягається можливість використання стандартного мережевого обладнання класу COTS (Commercial Off-The-Shelf) – звичайних Ethernet-комутаторів та IP-маршрутизаторів.

Запровадження концепції AoIP забезпечує кілька ключових технологічних та економічних переваг для систем аудіосповіщення:

– *глобальна масштабованість*. Додавання нового джерела або приймача звуку не вимагає прокладання нових ліній до центральної апаратної. Достатньо підключити новий IP-гучномовець або мікрофонну консоль до найближчого мережевого комутатора та призначити їм IP-адресу;

– *децентралізація та гнучкість маршрутизації*. Будь-який аудіосигнал у мережі може бути програмно перенаправлений на будь-який вихідний пристрій або групу пристроїв майже миттєво. Віртуальна маршрутизація здійснюється через програмні контролери без фізичного перемикання кабелів;

– *гарантована цілісність сигналу*. На відміну від аналогових систем, де якість звуку поступово погіршується через опір кабелю, цифровий аудіосигнал передається ідеально: IP-пакет або доходить абсолютно чистим, або втрачається, але ці втрати миттєво виправляються алгоритмами вищих рівнів;

– *конвергенція інфраструктури*. Можливість передавати аудіодані, сигнали управління та живлення через один кабель витої пари, що суттєво знижує витрати на монтаж та обслуговування системи.

У процесі історичного розвитку мережевих аудіотехнологій сформувалося кілька підходів, які відрізнялися рівнем інтеграції в еталонну модель взаємодії

відкритих систем (OSI). Ранні спроби стандартизації, такі як Audio Video Bridging (AVB, відомий також як набір стандартів IEEE 802.1BA), були зосереджені на удосконаленні канального рівня моделі OSI. Технологія AVB вимагала використання спеціалізованих комутаторів з підтримкою протоколів резервування смуги пропускання та специфічних механізмів формування трафіку. Хоча це гарантувало вкрай низьку затримку та відсутність втрат пакетів завдяки жорсткому контролю на рівні MAC-адрес, прив'язка до канального рівня унеможливлювала маршрутизацію такого трафіку через стандартні IP-мережі. Це робило AVB непридатним для використання в територіально розподілених об'єктах без розгортання складних і дорогих шлюзів.

Розуміючи ці обмеження, індустрія перейшла до протоколів, що працюють на мережевому рівні моделі OSI з використанням IP-маршрутизації. Найбільш відомими рішеннями стали Dante (від Audinate), Ravenna, Livewire (від Telos) та Q-LAN. Проте наявність багатьох несумісних між собою приватних форматів створювала загрозу вендор-локу (залежності від одного виробника). Для забезпечення сумісності Товариство аудіоінженерів (Audio Engineering Society) у 2013 році випустило відкритий стандарт AES67.

AES67 не є окремим комерційним програмним або апаратним продуктом. Цей стандарт є суровим набором технічних вимог до протоколів синхронізації, механізмів якості обслуговування, транспортних рівнів та форматів кодування звуку, які виробники повинні впровадити у своїх пристроях для забезпечення взаємодії. Згідно зі специфікаціями AES67, аудіодані передаються з використанням лінійної імпульсно-кодової модуляції (Linear PCM) з розрядністю 16 або 24 біти та частотами дискретизації 44.1, 48 або 96 кГц. Для мінімізації затримок час пакетування зазвичай встановлюється на рівні 1 мс (або навіть 125 мкс для ультранизьких затримок), що дозволяє досягти наскрізної трансляції аудіо з затримками, які є непомітними для людського сприйняття (від 1 до 4 мс у LAN).

Впровадження стандарту AES67 у системах автоматизованого аудіосповіщення дозволяє інтегрувати в єдину керовану інфраструктуру IP-гучномовці, сервери обробки медіаданих, мікрофонні пейджингові консолі та

системи управління життєзабезпеченням будівлі від абсолютно різних виробників, створюючи відкриту, гнучку та довговічну архітектуру.

1.3. Основні протоколи забезпечення роботи AoIP(RTP, SIP, UDP)

Для безперебійної та якісної передачі потокового аудіо в реальному часі через пакетні IP-мережі, системи AoIP використовують глибоко інтегрований стек стандартних мережевих протоколів. Кожен протокол у цьому стеку виконує свою специфічну, строго визначену функцію на відповідному рівні еталонної моделі взаємодії відкритих систем (OSI). Фундаментальні три протоколи, які забезпечують трансляцію медіаданих та децентралізоване управління комунікаційними сеансами у розподілених системах, є протоколи UDP, RTP та SIP.

User Datagram Protocol (UDP). На транспортному рівні моделі OSI безпосередня передача аудіоданих реалізується практично за допомогою протоколу користувацьких датаграм (UDP). У традиційних комп'ютерних мережах для забезпечення надійності найчастіше використовується протокол управління передачею (TCP). TCP функціонує за принципом встановлення попереднього з'єднання, після чого суворо контролює доставку кожного пакета. Якщо пакет втрачається внаслідок мережевого затору, приймач не надсилає підтвердження, і відправник змушений здійснювати повторну передачу цього фрагмента даних, призупиняючи відправку наступних пакетів до моменту успішного отримання втраченого.

Також, як і всі інші протоколи, UDP має заголовок. Заголовок має фіксований розмір – 8 байтів (64 біти) і складається з чотирьох полів, кожне з яких займає 2 байти(16 бітів)(рис.1.4, табл. 1.1).

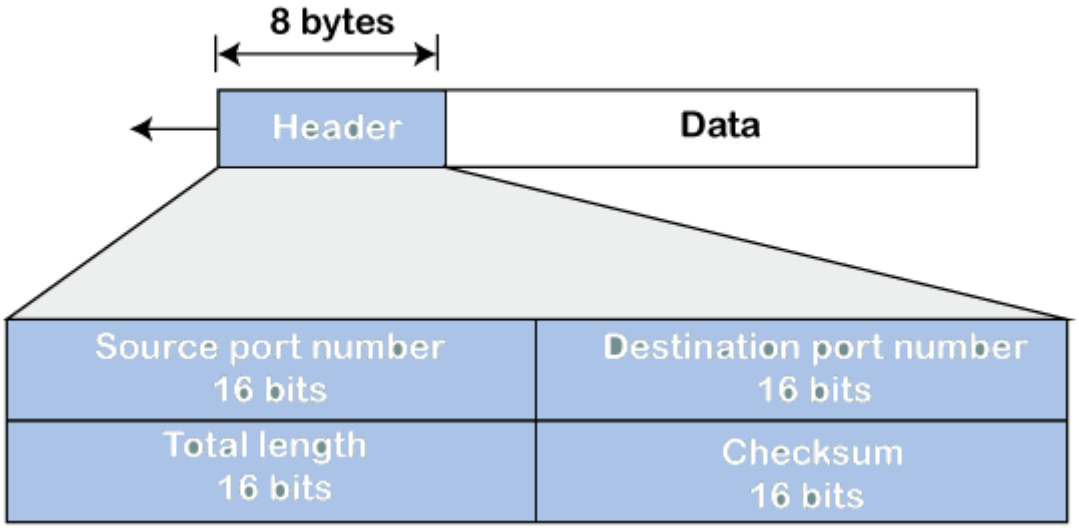


Рисунок 1.3 – Діаграма заголовка UDP

Таблиця 1.1 – Опис полів заголовка UDP

Назва поля	Опис
Порт джерела	Ідентифікує порт відправника. Це поле є необов'язковим; якщо воно не використовується (наприклад, коли клієнт не очікує відповіді), воно заповнюється нулями.
Порт призначення	Ідентифікує порт отримувача, на який спрямовано данограму. Це поле є обов'язковим для доставки даних конкретному процесу на хості.
Довжина	Визначає загальну довжину всієї данограми в байтах (включно із заголовком та даними). Мінімальне значення становить 8 байтів (довжина порожнього заголовка). Теоретичний максимум — 65 535 байтів.
Контрольна сума	Використовується для перевірки цілісності заголовка та даних, а також деяких полів IP-заголовка (псевдозаголовка). В протоколі IPv4 використання контрольної суми є необов'язковим (може бути заповнено нулями), проте в IPv6 вона є обов'язковою.

Для систем аудіосповіщення, які працюють у режимі реального часу, такий механізм є категорично неприйнятним. Очікування на повторну передачу втраченого аудіопакета призведе до непередбачуваних пауз, переривань та значного збільшення наскрізної затримки, що критично спотворить звучання та унеможливить синхронне відтворення. UDP не гарантує доставку пакетів, не контролює їх порядок і не здійснює повторних передач. Ця властивість дозволяє мінімізувати транспортні затримки: датаграми генеруються і негайно надсилаються в мережу. Для людського слуху тимчасова втрата кількох мілісекунд звуку є значно менш помітною (і може бути прихована алгоритмами маскування помилок), ніж тривала зупинка відтворення. Але, оскільки UDP позбавлений будь-яких механізмів відстеження порядку пакетів та синхронізації часу, ці надзвичайно важливі функції виконуються протоколом RTP.

Real-time Transport Protocol (RTP). Протокол передачі в реальному часі (RTP), стандартизований робочою групою IETF у документах RFC 1889 та згодом оновлений у RFC 3550, функціонує на прикладному рівні і інкапсулюється безпосередньо у корисне навантаження UDP-пакетів. Головне інженерне призначення RTP – надання кінцевим пристроям (приймачам) вичерпної інформації, необхідної для точної реконструкції медіапотоку та компенсації мережевих аномалій, таких як джиттер (час, за який пакети проходять нерівномірно) і зміна порядку прибуття пакетів.

Заголовок стандартного RTP-пакета має мінімальний розмір 12 байтів і містить низку оптимізованих структурних полів(рис.1.3):

– PT(Payload Type) являє собою 7-бітне поле, яке чітко ідентифікує формат кодування корисного навантаження (наприклад, нестиснений звук L16, кодеки G.711, Opus, G.722, G.729). Завдяки цьому полю приймаючий гучномовець або декодер розуміє, який саме алгоритм розпакування аудіо потрібно застосувати до отриманих даних;

– sequence number (порядковий номер) – 16-бітне поле, початкове значення яке генерується випадковим чином, після чого збільшується на одиницю для кожного відправленого RTP-пакета. Цей механізм дозволяє приймачу виявляти

втрату пакетів у мережі та відновлювати їхній правильний початковий хронологічний порядок перед тим, як подати дані на цифро-аналоговий перетворювач;

– timestamp (часова мітка) – 32-бітне поле, що відображає точний момент часу генерування першого байта аудіоданих у даному пакеті (вимірюється в одиницях частоти дискретизації, наприклад, кроками по 1/48000 секунди). Часова мітка є критично важливим елементом для роботи буфера джитера на стороні приймача. Буфер накопичує вхідні пакети і випускає їх на відтворення з фіксованою затримкою, спираючись на ці мітки. За допомогою цього можна компенсувати нерівномірність мережевих затримок і забезпечити плавне відтворення звуку без зупинок;

– synchronization source (SSRC) identifier – це 32-бітний унікальний ідентифікатор, що позначає джерело синхронізації потоку. Це поле є незамінним при багатоадресній розсилці (multicast) або під час роботи через RTP-мікшери, оскільки воно дозволяє приймачу безпомилково розрізняти аудіопотоки від різних мікрофонів або серверів, навіть якщо вони надходять на один і той самий UDP-порт.

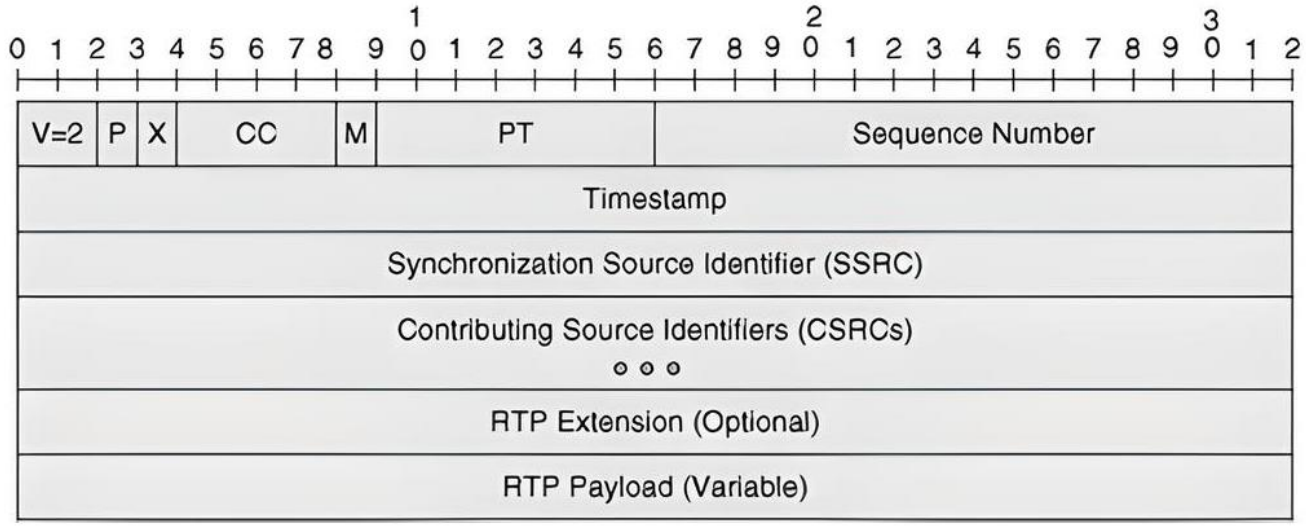


Рисунок 1.4 – Структура заголовка RTP протокола

У нерозривній парі з RTP завжди використовується протокол управління RTCP (Real-time Transport Control Protocol). Якщо RTP відповідає виключно за транспорт самих медіаданих, то функція RTCP полягає у зборі та періодичному розсиланні телеметрії щодо якості обслуговування. Повідомлення RTCP (наприклад, Sender Report або Receiver Report) надають адміністраторам та автоматизованим системам моніторингу інформацію про відсоток втрачених пакетів, рівень джитера, загальну затримку та ідентифікаційні дані учасників сеансу. У територіально розподілених системах своєчасний аналіз RTCP-метрик дозволяє заздалегідь виявляти деградацію окремих ліній зв'язку або перевантаження комутаторів. Крім того, для забезпечення високого рівня інформаційної безпеки та конфіденційності екстреного зв'язку може застосовуватися розширення SRTP (Secure RTP), яке додає надійне криптографічне шифрування до корисного навантаження аудіопакетів та автентифікацію повідомлень.

Session Initiation Protocol (SIP). У той час як тандем RTP/UDP забезпечує безпосередню фізичну передачу аудіоданих, пристроям у мережі потрібен механізм для знаходження одне одного, узгодження параметрів передачі (IP-адрес, номерів портів) та управління логічним станом з'єднання. Цю роль у сучасних системах AoIP та VoIP відіграє протокол ініціювання сеансів (Session Initiation Protocol, SIP).

SIP працює на прикладному рівні і є текстово-орієнтованим протоколом, синтаксис якого свідомо змодельований за зразком протоколів HTTP та SMTP, що робить його гнучким, розширюваним та легким для аналізу. Головне завдання SIP полягає у встановленні , модифікації параметрів у процесі роботи та коректне завершення комунікаційних сеансів між клієнтами.

Архітектура мережі на базі SIP є модульною і включає декілька ключових логічних компонентів:

– *SIP User Agent (UA).* Це кінцеві точки комунікації. У системі аудіосповіщення це можуть бути IP-гучномовці, мікрофонні пейджингові консолі, термінали виклику екстрених служб або центральні сервери автоматизованого оповіщення;

– *SIP Proxy Server.* Сервер-посередник, який приймає запити від клієнтів і ухвалює рішення щодо їх подальшої маршрутизації до кінцевого пункту призначення або до наступного проксі-сервера. Він також може забезпечувати функції авторизації та обліку;

– *SIP Registrar*. Спеціалізований компонент, який приймає запити REGISTER від UA і динамічно оновлює центральну базу даних, пов'язуючи логічне ім'я пристрою з його поточною фізичною IP-адресою. У територіально розподіленій системі цей механізм є безцінним: IP-гучномовець може бути фізично переміщений до іншої підмережі (отримавши нову IP-адресу через DHCP), але завдяки автоматичній реєстрації на Registrar-сервері, система продовжить надсилати на нього виклики за незмінним логічним ім'ям.

Процес логічного ініціювання сеансу (наприклад, ініціювання виклику певної зони оповіщення з диспетчерської консолі) відбувається шляхом обміну стандартизованими запитами (Methods) та відповідями (Responses), що містять тризначні коди стану (рис. 1.5):

1. диспетчерський пульт (джерело) генерує запит INVITE і надсилає його до SIP Proxy сервера або безпосередньо до IP-гучномовця. Життєво важливою складовою цього запиту є вкладене повідомлення у форматі SDP (Session Description Protocol). SDP діє як "технічний паспорт" сеансу: у ньому диспетчерський пульт вказує свою транспортну IP-адресу, UDP-порт, на якому він готовий отримувати зустрічний RTP-потік, та перелік аудіокодеків, які він підтримує, відсортованих за пріоритетом;

2. гучномовець-приймач (через Proxy) отримує запит і відповідає проміжним інформаційним кодом 100 Trying (запит прийнято до обробки), а потім 180 Ringing (відбувається локальне сповіщення/виклик);

3. після того, як гучномовець підтверджує готовність встановити з'єднання і транслювати аудіо, він надсилає код успішного завершення 200 OK. Це повідомлення також містить SDP-відповідь, у якій гучномовець фіксує єдиний обраний кодек (спільний для обох пристроїв) та свої власні мережеві реквізити (IP та порт) для прийому аудіо;

4. диспетчерський пульт надсилає остаточне підтвердження, завершуючи так зване "тристороннє рукостискання" (three-way handshake). Тільки після цього етапу починається фактична передача аудіоданих через протокол RTP/UDP;

5. для завершення трансляції та вивільнення мережевих і апаратних ресурсів будь-яка зі сторін генерує запит BYE, на який інша сторона відповідає кодом 200 OK.

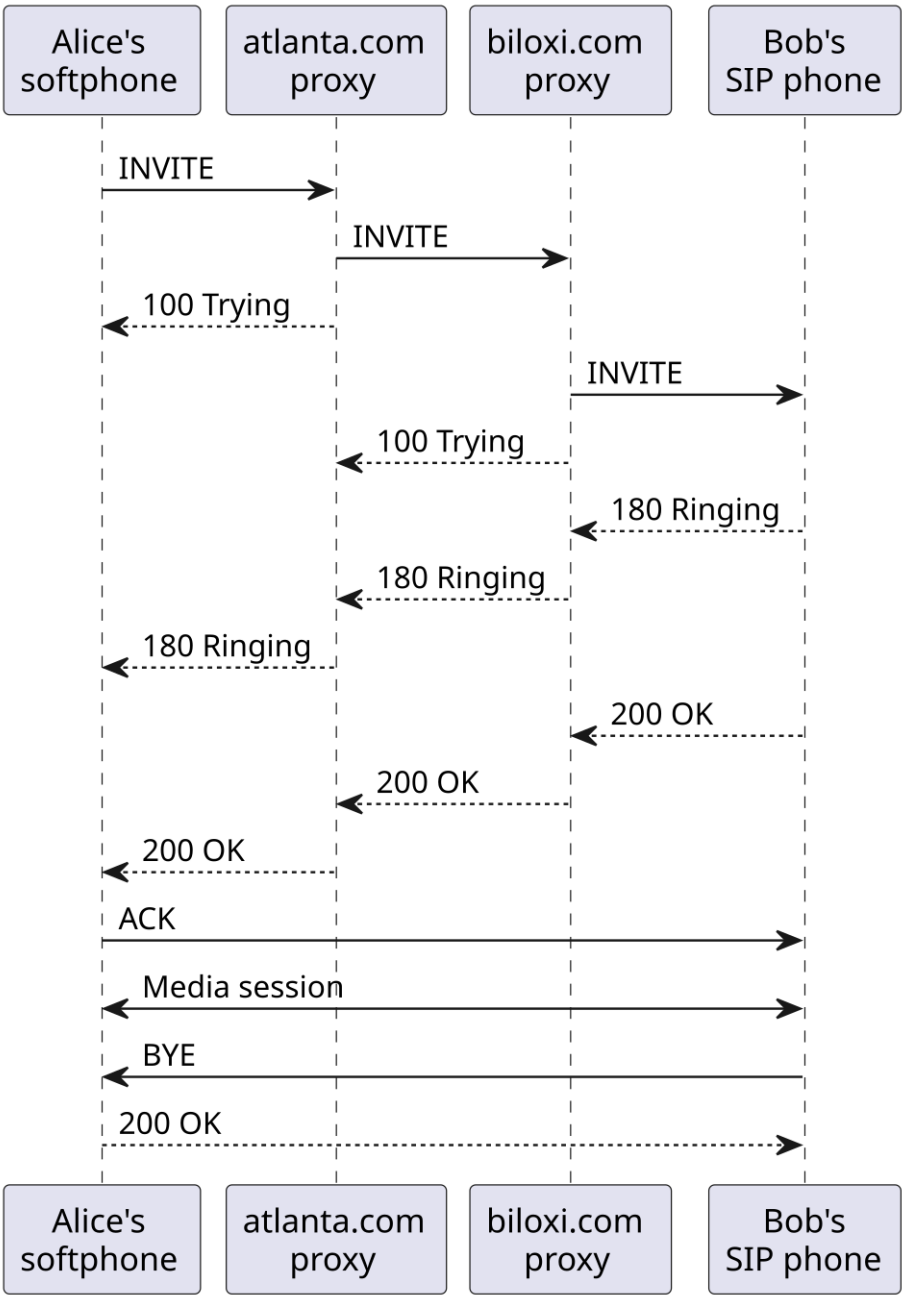


Рисунок 1.5 – Приклад обміну SIP-повідомленнями між двома користувачами

Використання стандартизованого протоколу SIP у розподілених системах аудіосповіщення забезпечує надзвичайно високу гнучкість. Це дозволяє не лише встановлювати прямі з'єднання між IP-мікрофонами та гучномовцями, але й створювати складні сценарії інтеграції: наприклад, підключати систему сповіщення до корпоративної IP-АТС (дозволяючи здійснювати оголошення за допомогою звичайного настільного IP-телефону), інтегрувати з програмними клієнтами на смартфонах керівництва або об'єднувати з глобальними системами диспетчеризації будівель (Building Management Systems, BMS). Завдяки чіткому архітектурному дешифруванню сигнального рівня (SIP) від транспортного (RTP/UDP), система набуває безпрецедентної масштабованості та модульності.

1.4. Дослідження механізмів багатоадресної розсилки (IP Multicast) та його відмінність від Unicast і Broadcast

У системах автоматизованого аудіосповіщення для територіально розподілених об'єктів критично важливим аспектом проектування є оптимізація мережевого трафіку. Ситуація, коли диспетчеру або системі пожежної безпеки необхідно транслювати єдине екстрене повідомлення одночасно на десятки, сотні або навіть тисячі IP-гучномовців по всьому підприємству, є стандартною. Для розуміння архітектурних рішень, що застосовуються в AoIP, необхідно проаналізувати та порівняти три фундаментальні парадигми мережевої маршрутизації IP-пакетів: Unicast, Broadcast та Multicast (рис.1.6, табл. 1.2). Вибір конкретного методу залежить від топології мережі, вимог до пропускної здатності та цільової аудиторії отримувачів контенту.

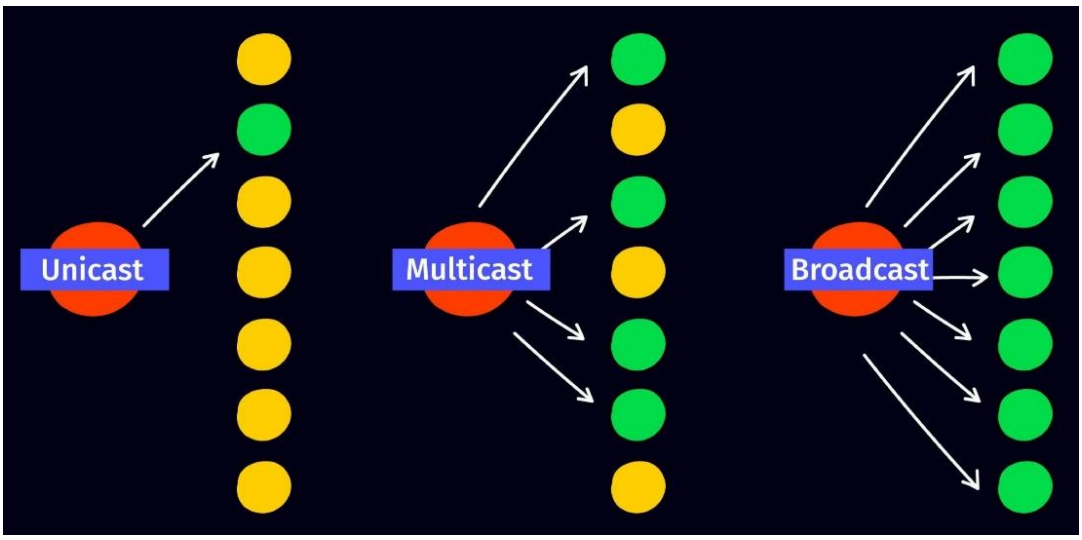


Рисунок 1.6 – Схема передачі даних у Unicast, Multicast та Broadcast

Unicast є домінуючим методом комунікації в мережах IP, що реалізує модель «один-до-одного». При такій передачі пакет даних має чітко визначену адресу відправника та унікальну IP-адресу отримувача. Маршрутизація здійснюється на основі аналізу таблиць відповідності, що забезпечує доставку контенту безпосередньо до цільового інтерфейсу.

Основна перевага даного методу полягає у можливості організації персоналізованих сесій зв'язку з підтримкою контролю цілісності даних (наприклад, протокол TCP). Проте, при одночасній передачі однакового контенту великій кількості вузлів, Unicast створює надмірне навантаження на вихідний канал джерела, оскільки для кожного клієнта генерується окрема копія даних.

Широкомовна передача базується на принципі «один-до-всіх». Пакет, відправлений у режимі Broadcast, доставляється всім активним пристроям у межах одного широкомовного домену (зазвичай сегмента локальної мережі). Адресація на рівні канальному рівні виконується через MAC-адресу FF:FF:FF:FF:FF:FF, а на мережевому рівні – через IP-адресу 255.255.255.255.

Broadcast є незамінним для роботи службових протоколів, таких як ARP (Address Resolution Protocol) або DHCP (Dynamic Host Configuration Protocol). Однак через високий рівень «шуму» та навантаження на процесори всіх вузлів у сегменті, використання бродкасту зазвичай обмежується локальними мережами та

блокується на рівні маршрутизаторів для запобігання глобальним перевантаженням.

Таблиця 1.2 – Порівняльна характеристика механізмів передачі даних

Характеристика	Unicast (Одноадресна розсилка)	Broadcast (Широкомовна розсилка)	IP Multicast (Багатоадресна розсилка)
Принцип адресації	Один відправник надсилає дані одному конкретному одержувачу	Один відправник надсилає дані на спеціальну адресу (наприклад, 255.255.255.255), охоплюючи всі вузли сегмента.	Відправник генерує потік на віртуальну адресу класу D. Мережа доставляє його лише тим, хто "підписався".
Споживання смуги пропускання	Прямо пропорційне кількості одержувачів. Якщо потік має бітрейт 2 Мбіт/с, для 100 гучномовців сервер генерує 200 Мбіт/с.	Мінімальне для відправника, але пакет дублікується на всі порти комутаторів, заповнюючи смугу для всіх пристроїв підмережі.	Максимально ефективне. Сервер генерує 1 потік. Мережа передає лише одну копію пакета по кожному магістральному каналу зв'язку.
Навантаження на кінцеві вузли	Приймачі обробляють лише свої дані. Джерело відчуває колосальне навантаження на CPU.	Усі пристрої в мережі змушені витрачати ресурси CPU на перевірку та відкидання непотрібних їм аудіопакетів.	Мінімальне. Пристрої, що не належать до мультикаст-групи, ігнорують трафік ще на апаратному рівні мережевої карти.

Продовження таблиці 1.2

Характеристика	Unicast (Одноадресна розсилка)	Broadcast (Широкомовна розсилка)	IP Multicast (Багатоадресна розсилка)
Масштабування (WAN / Інтернет)	Легко маршрутизується через будь-які маршрутизатори, але пропускна здатність висхідного каналу сервера швидко вичерпується.	Жорстко обмежене межами локального широкомовного домену. Маршрутизатори відкидають Broadcast-пакети за замовчуванням.	Відмінно масштабується в корпоративних WAN за умови налаштування протоколів багатоадресної маршрутизації (PIM).
Сфера використання в системах AoIP	Двосторонній інтерком, індивідуальні SIP-виклики до конкретного гучномовця, конфігурування обладнання.	Практично не використовується для медіаданих через загрозу "штормів" та перевантаження. Використовується лише для ARP/DHCP.	Абсолютний пріоритет для систем масового сповіщення (PA/VA), розподілу фонової музики, синхронізації часу (PTP).

Як наочно демонструє порівняння, IP Multicast є єдиним архітектурно правильним та ефективним рішенням для дистрибуції аудіо в масштабних системах AoIP. Під час багатоадресної розсилки центральний сервер або мікрофонна консоль не зобов'язані знати точну кількість активних слухачів, їхнє місцезнаходження або індивідуальні IP-адреси. Натомість джерело просто відправляє єдиний екземпляр аудіопакета на спеціально виділену мультикастову IP-адресу класу D (з діапазону від 224.0.0.0 до 239.255.255.255). Пристрої (IP-гучномовці), які відповідно до свого налаштування або команди логічного контролера повинні відтворювати цей потік, "підписуються" на відповідну мультикастову групу.

Однак ця елегантна концепція не працює автоматично. Для того, щоб мультикаст працював ефективно, не перетворювався на хаотичний Broadcast

усередині локальних мереж і успішно долав маршрутизатори у глобальних мережах (WAN), необхідна тісна взаємодія двох спеціалізованих груп протоколів: IGMP на рівні локальної підмережі (між гучномовцем та комутатором/маршрутизатором) та PIM на рівні ядра мережі (між маршрутизаторами).

Також для злагодженої роботи IP Multicast потрібно використовувати багато протоколів, основними з яких є IGMP та PIM.

Internet Group Management Protocol (IGMP) – це керівний протокол мережевого рівня, за допомогою якого кінцеві хости динамічно повідомляють своєму найближчому маршрутизатору про своє бажання приєднатися до певної мультикаст-групи, для того щоб отримувати аудіопотік, чи покинути її(рис.1.7). Маршрутизатор, у свою чергу, використовує IGMP для періодичного опитування підмережі (відправлення повідомлень IGMP Query), щоб перевірити, чи залишилися в підмережі активні слухачі для кожної з існуючих груп.

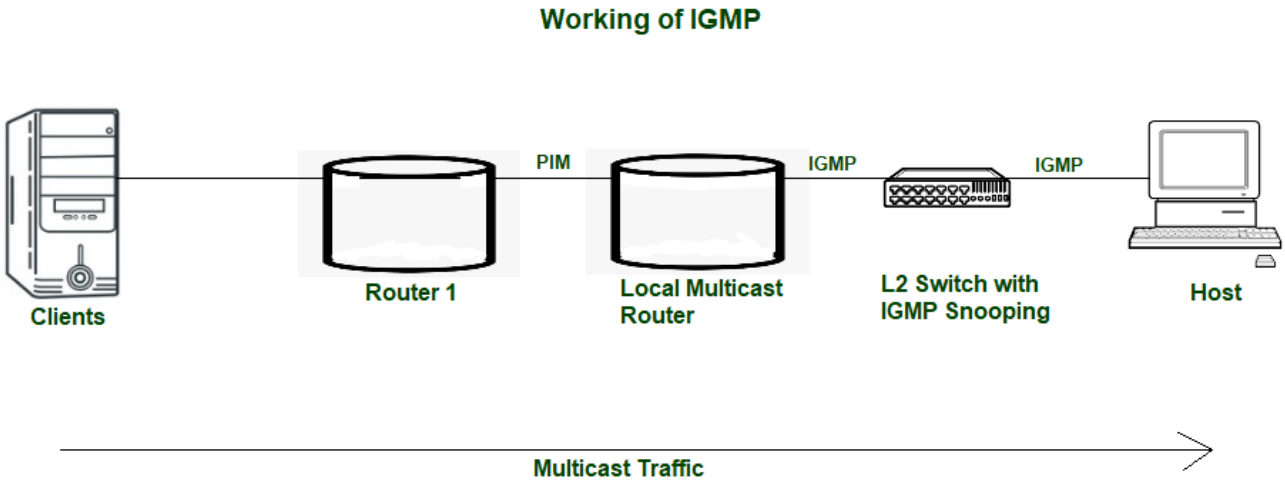


Рисунок 1.7 – Схема роботи протокола IGMP

Протокол пройшов декілька стадій розвитку, з яких для сучасних систем AoIP найважливішими є IGMPv2 та IGMPv3:

– IGMPv2 став індустріальним стандартом завдяки тому, що було впровадженно критично важливе повідомлення "Leave Group". У попередній версії

маршрутизатор дізнавався про те, що гучномовцю більше не потрібен потік, лише після того, як гучномовець переставав відповідати на періодичні запити, що призводило до хвилинних затримок і марнотратства трафіку. IGMPv2 дозволив кінцевим пристроям явно заявляти про відключення від трансляції, що дає змогу маршрутизатору миттєво припинити відправку аудіопакетів у цю підмережу;

– IGMPv3 значно розширив можливості управління, запровадивши парадигму Source-Specific Multicast. Замість того, щоб підписуватися на весь трафік, який надходить на певну мультикаст-адресу групи G, IGMPv3 дозволяє приймачу вказати, що він хоче отримувати дані виключно від конкретного легітимного джерела S (Source). Формується підписка типу (S, G). У системах екстреного аудіосповіщення це кардинально підвищує кібербезпеку: зловмисник або невірно налаштований пристрій не зможе перехопити керування зоною оповіщення, просто почавши транслювати підроблені аудіопакети на мультикастову адресу зони, оскільки маршрутизатори та гучномовці відкинуть трафік від неавторизованого джерела.

Не менш критично важливою є функція IGMP Snooping. Головною проблемою є те, що звичайні Ethernet-комутатори керуються MAC-адресами і не здійснюють IP-маршрутизацію. Коли комутатор отримує кадр з мультикастовою MAC-адресою, він за замовчуванням обробляє його як Broadcast і розсилає на абсолютно всі свої порти. В умовах територіально розподіленого об'єкта це може швидко призвести до деградації пропускної здатності мережі. Технологія IGMP Snooping дозволяє мікропроцесору комутатора "підглядати" (snoop) за обміном IGMP-повідомленнями між гучномовцями та маршрутизатором на канальному рівні. Аналізуючи ці повідомлення, комутатор динамічно будує внутрішню таблицю відповідності мультикаст-груп і конкретних фізичних портів. Завдяки цьому, високоякісний аудіопотік буде фізично пересилатися виключно на ті порти комутатора, до яких підключені гучномовці (рис.1.8).

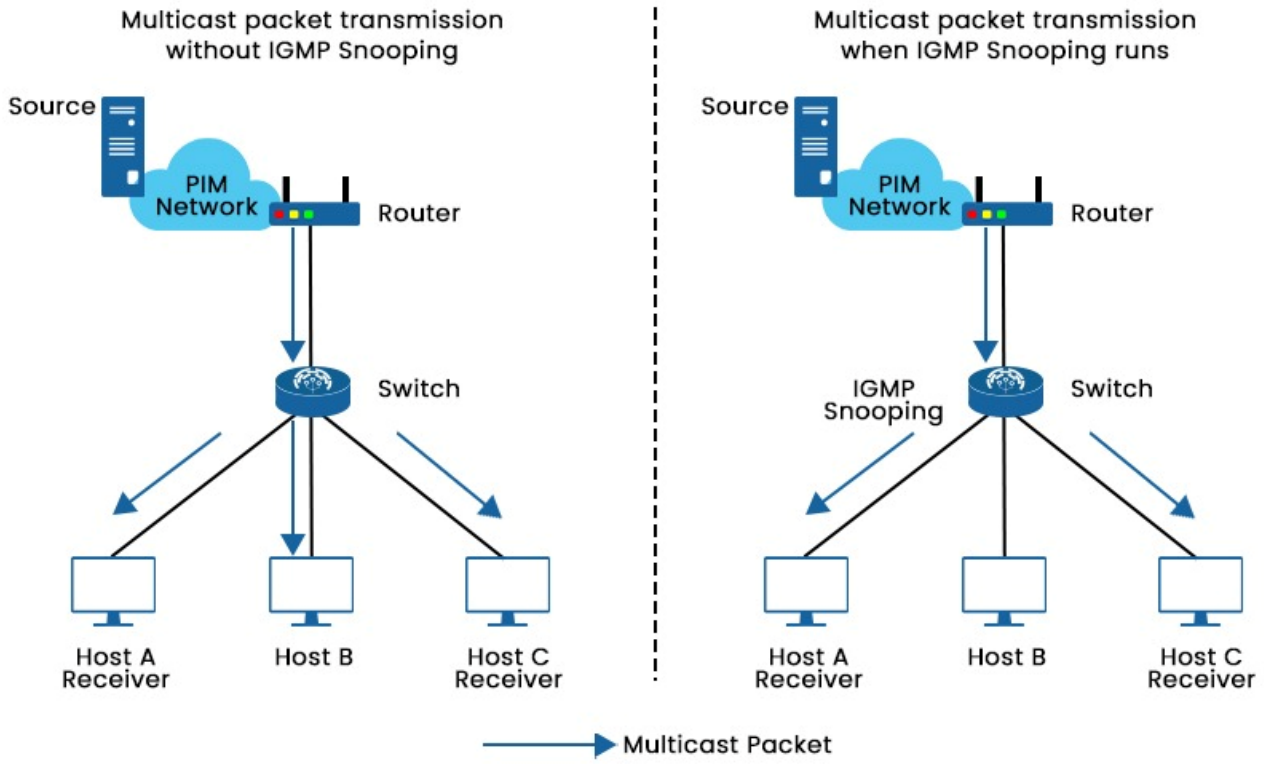


Рисунок 1.8 – Схема передачі багатоадресних пакетів з та без IGMP Snooping

У той час як IGMP вирішує завдання доставки, для того щоб аудіопотік міг перетнути межі LAN і бути доставленим до інших філій чи підприємств WAN, необхідний протокол PIM.

PIM (Protocol Independent Multicast) отримав свою назву через те, що він не створює власної незалежної топологічної карти мережі, а використовує таблицю одноадресної маршрутизації, побудовану будь-яким існуючим протоколом (наприклад, OSPF, EIGRP або BGP) для перевірки зворотного шляху і запобігання появі петель маршрутизації.

Коли групи слухачів можуть бути розподілені нерівномірно по великій інфраструктурі, найчастіше застосовується архітектура PIM Sparse Mode (PIM-SM). PIM-SM використовує модель "pull" (витягування).

Принцип роботи PIM-SM в AoIP-середовищі базується на використанні центрального вузла – точки зустрічі (Rendezvous Point, RP). Логіка побудови дерева маршрутизації виглядає наступним чином (рис.1.9):

1. коли сервер або мікрофонна консоль починає генерувати аудіосповіщення, її локальний маршрутизатор інкапсулює ці перші мультикаст-пакети в спеціальні unicast-повідомлення PIM Register і відправляє їх до RP. Таким чином RP дізнається про наявність активного джерела;

2. з іншого боку мережі, коли IP-гучномовець надсилає запит IGMP Join, його локальний маршрутизатор формує керуюче повідомлення PIM Join і відправляє його від вузла до вузла в напрямку до RP. Цей процес створює в маршрутизаторах стан (S, G), формуючи так зване спільне дерево (Shared Tree), коренем якого є RP;

3. аудіопотік починає рух від джерела до RP, а звідти спускається по Shared Tree до гучномовця;

4. PIM-SM підтримує механізм оптимізації. Після того, як маршрутизатор гучномовця отримує перші пакети від джерела через RP і витягує з них реальну IP-адресу джерела S, він може ініціювати побудову нового дерева безпосередньо до джерела, відправивши PIM Join у напрямку до нього. Це формує Дерево найкоротшого шляху (Shortest Path Tree, стан (S, G)). Після його побудови маршрутизатор відправляє PIM Prune до RP, відсікаючи довший маршрут.48 Цей етап критично важливий для AoIP, оскільки він дозволяє мінімізувати транспортну затримку та кількість транзитних стрибків (hops).

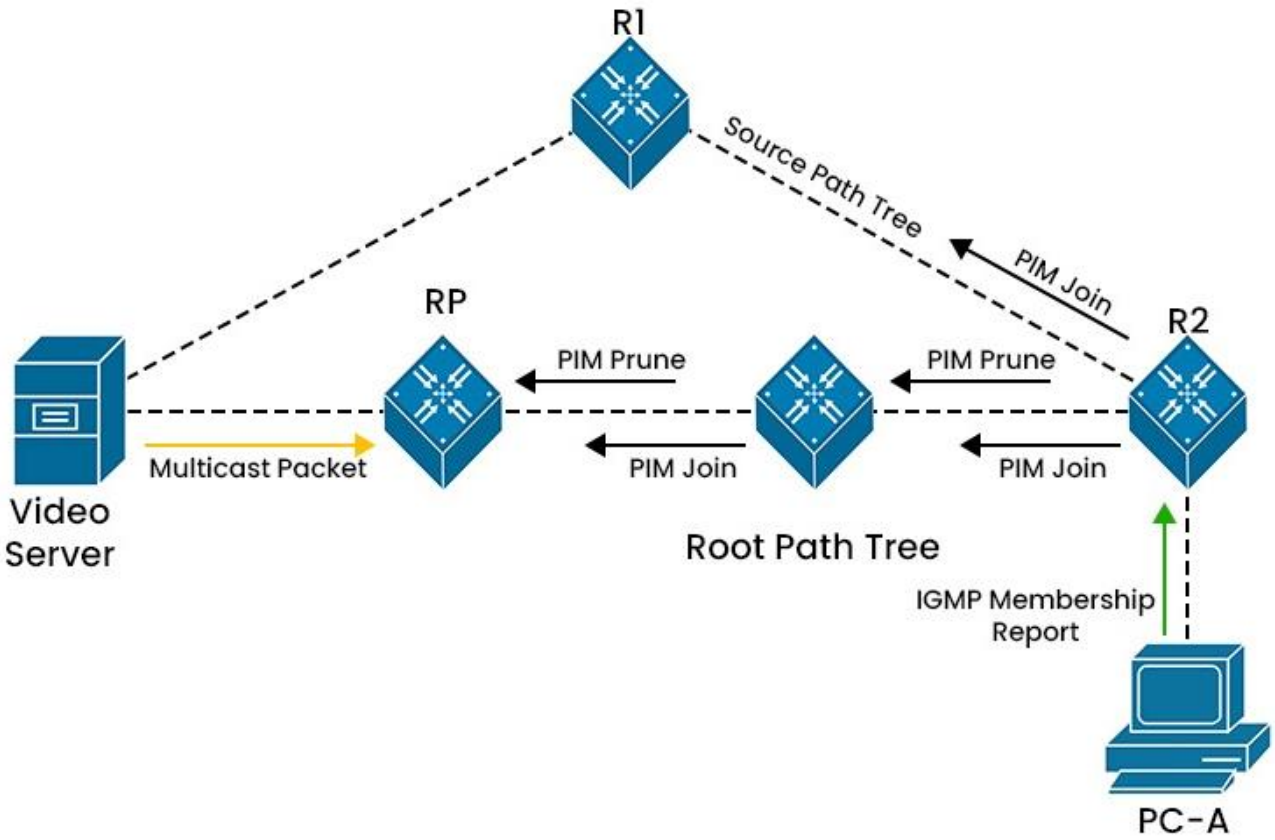


Рисунок 1.9 – Схема роботи протокола PIM

Сукупність протоколів IGMP та PIM дозволяє інженерам будувати високонадійні, повністю автоматизовані системи багатоадресного аудіосповіщення для об'єктів колосального масштабу. Це гарантує безперебійну доставку критичних екстрених повідомлень сотням пристроїв, оптимізуючи навантаження на магістральні канали передачі даних та зберігаючи стабільність решти корпоративної IT-інфраструктури.

1.5. Використання протоколів синхронізації часу (NTP та PTP) в AoIP

Для коректної роботи аудіосистеми необхідно підтримувати синхронізацію часу між усіма вузлами мережі. Це стосується всього ланцюга обладнання: від джерел сигналу (мікрофонів) до кінцевих пристроїв відтворення (IP-гучномовців).

Якщо в аналогових системах звуковий сигнал розповсюджується мідним кабелем зі швидкістю, близькою до швидкості світла, то в IP-мережах ситуація є кардинально іншою. Аудіопотік розбивається на окремі цифрові пакети, які послідовно проходять через буфери маршрутизаторів та комутаторів. Навантаження на мережеве обладнання постійно змінюється, що вносить асиметричні та нестабільні затримки у час доставки кожного пакета.

Для того, щоб перетворити цей нерівномірний потік пакетів назад у високоякісний аналоговий звук без спотворень, приймачі (їхні цифро-аналогові перетворювачі, ЦАП) повинні відтворювати аудіофрагманти з ідеально рівною та узгодженою тактовою частотою (наприклад, рівно 48 000 аудіофрагментів на секунду). Якщо локальний генератор гучномовця працює хоча б на долю відсотка швидше або повільніше за генератор сервера-джерела, це призведе до спустошення або переповнення буфера приймача. Акустично це проявляється у вигляді гучних клацань, спотворень спектра та навіть повного зникнення звуку.

У системах масового оповіщення територіально розподілених об'єктів дуже часто зустрічається ситуація, коли звук від кількох близько розташованих гучномовців покриває одну акустичну площу (наприклад, довгий коридор, ангар або платформу вокзалу). Якщо ці гучномовці не будуть ідеально синхронізовані по фазі, і один з них відтворить сигнал із затримкою лише в 1-2 мілісекунди відносно іншого, звукові хвилі почнуть накладатися в просторі несинфазно. Це явище спричиняє ефект гребінчастої фільтрації, що є періодичним посиленням та послабленням певних частот, що критично погіршує розбірливість мови. Для вирішення цих комплексних завдань застосовуються протоколи NTP та PTP (табл.1.3).

Таблиця 1.3 – Порівняльна характеристика протоколів NTP та PTP

Характеристика	NTP	PTP
Типова точність у LAN	1–10 мілісекунд	100 наносекунд – 1 мікросекунда
Рівень нанесення міток часу	Програмний стек	Апаратний стек
Топологія та архітектура	Клієнт-сервер (гнучка робота через WAN)	Master-Slave з жорсткою локальною ієрархією
Вимоги до мережевого устаткування	Стандартні комутатори без додаткових функцій	Вимагає PTP-сумісних комутаторів для високої точності
Застосування в інфраструктурі AoIP	Синхронізація серверних журналів, графіків планування подій	Відновлення медіа-частоти дискретизації, жорстке фазове вирівнювання гучномовців

Протокол мережевого часу (Network Time Protocol, NTP) є одним із найстаріших і найпоширеніших протоколів в історії розвитку Інтернету. Він розроблений для загальноцільової синхронізації годинників комп'ютерів і серверів. NTP працює за класичною клієнт-серверною архітектурою і використовує ієрархічну систему Stratum для розподілу точності. У цій архітектурі Stratum 0 – це еталонні апаратні джерела часу (наприклад, атомні годинники або приймачі супутникових систем GNSS/GPS). Сервери, підключені безпосередньо до них, стають серверами Stratum 1. Клієнти, що отримують час від Stratum 1 через IP-мережу, отримують статус Stratum 2, і так далі аж до 15 рівнів(рис. 1.10).

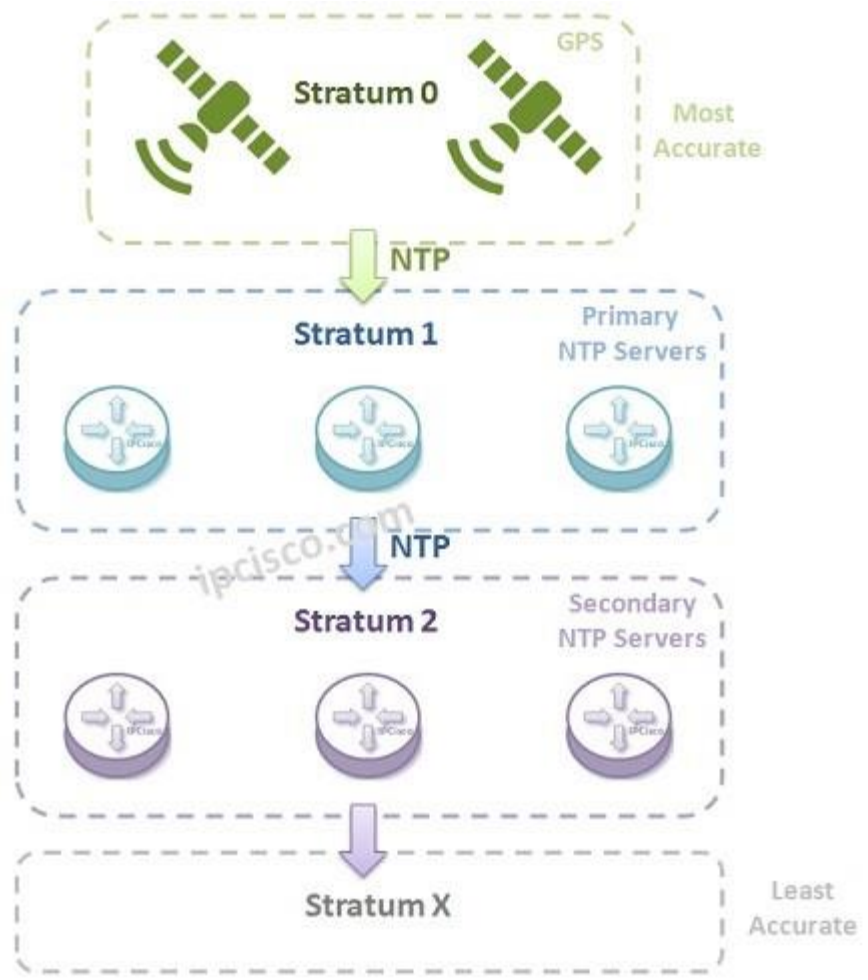


Рисунок 1.10 – Схема ієрархії системи Stratum в NTP

Синхронізація в NTP досягається шляхом обміну запитами між клієнтом і сервером. Клієнт відправляє запит, фіксує час відправлення та час отримання відповіді. Використовуючи ці мітки, алгоритми NTP обчислюють приблизну затримку в мережі та коригують локальний годинник клієнта. Для забезпечення надійності NTP використовує складні алгоритми фільтрації які дозволяють відкидати аномальні або нестабільні відповіді та підтримувати стабільність навіть під час тривалих сесій.

Проте фундаментальна проблема NTP полягає в тому, що всі його алгоритми та механізми проставлення міток часу реалізовані на високому програмному рівні операційної системи. Це означає, що позначка часу накладається на пакет не в момент його фізичної появи на дроті, а до або після того, як пакет пройде через численні програмні черги ОС, буфери ядра та драйвери мережевого інтерфейсу. Ці

процесорні операції вносять значну і непередбачувану затримку в розрахунки.

Як наслідок, максимальна точність, якої можна стабільно досягти за допомогою NTP у добре налаштованій LAN, становить від 1 до 10 мілісекунд, а при передачі через WAN або Інтернет похибка зростає до десятків мілісекунд. Для виконання фонових логічних та адміністративних операцій системи автоматизованого аудіосповіщення (наприклад, точної реєстрації подій у загальному журналі системи безпеки, синхронізації інтерфейсів керування або запуску запланованих розкладів трансляції фонової музики) точності NTP цілком достатньо.

Для радикального подолання меж NTP Інститут інженерів з електротехніки та електроніки (IEEE) розробив стандарт IEEE 1588 – Протокол точного часу (Precision Time Protocol, PTP). Архітектура PTP здатна забезпечити безпрецедентну точність синхронізації в діапазоні субмікросекунд (менше 1 мікросекунди) та наносекунд. У контексті сучасних стандартів Audio-over-IP використання PTP версії 2 (IEEE 1588-2008) є абсолютно обов'язковою вимогою для побудови єдиного глобального годинника.

Така детальна точність PTP досягається за рахунок використання апаратного проставлення часових міток. У PTP-сумісному обладнанні мітки часу генеруються спеціалізованим співпроцесором (PHY-чіпом мережевої карти) безпосередньо в ту мікросекунду, коли перший біт IP-кадру фізично покидає або надходить на порт пристрою. Цей підхід повністю виключає вплив непередбачуваних затримок операційної системи та центрального процесора.

Механізм роботи PTP ґрунтується на ієрархії "Master-Slave" і включає безперервний обмін серією з чотирьох ключових повідомлень між головним і підлеглими пристроями для розрахунку точного зміщення годинника та затримки поширення сигналу в кабелі:

– *sync message*. Головний годинник (Master) надсилає повідомлення про синхронізацію підлеглому (Slave). Точний апаратний час відправлення цього пакета фіксується як T1 , а точний час його отримання на Slave — як T2;

– *follow_up message.* У двоетапному режимі роботи Master наступним

пакетом надсилає точне значення T1 підлеглому пристрою;

– *delay_req message.* Для вимірювання затримки зворотного шляху Slave надсилає запит до Master. Фіксується час відправлення T3 та час отримання на Master T4;

– *delay_resp message:* Master повертає виміряне значення T4 підлеглому пристрою.

Зібравши всі чотири значення (T1, T2, T3 та T4), мікропроцесор підлеглого пристрою вирішує систему рівнянь, обчислюючи точну двосторонню мережеву затримку і безпрецедентно точне зміщення свого локального годинника відносно Master, після чого автоматично підлаштовує свій генератор коливань(рис.1.11).

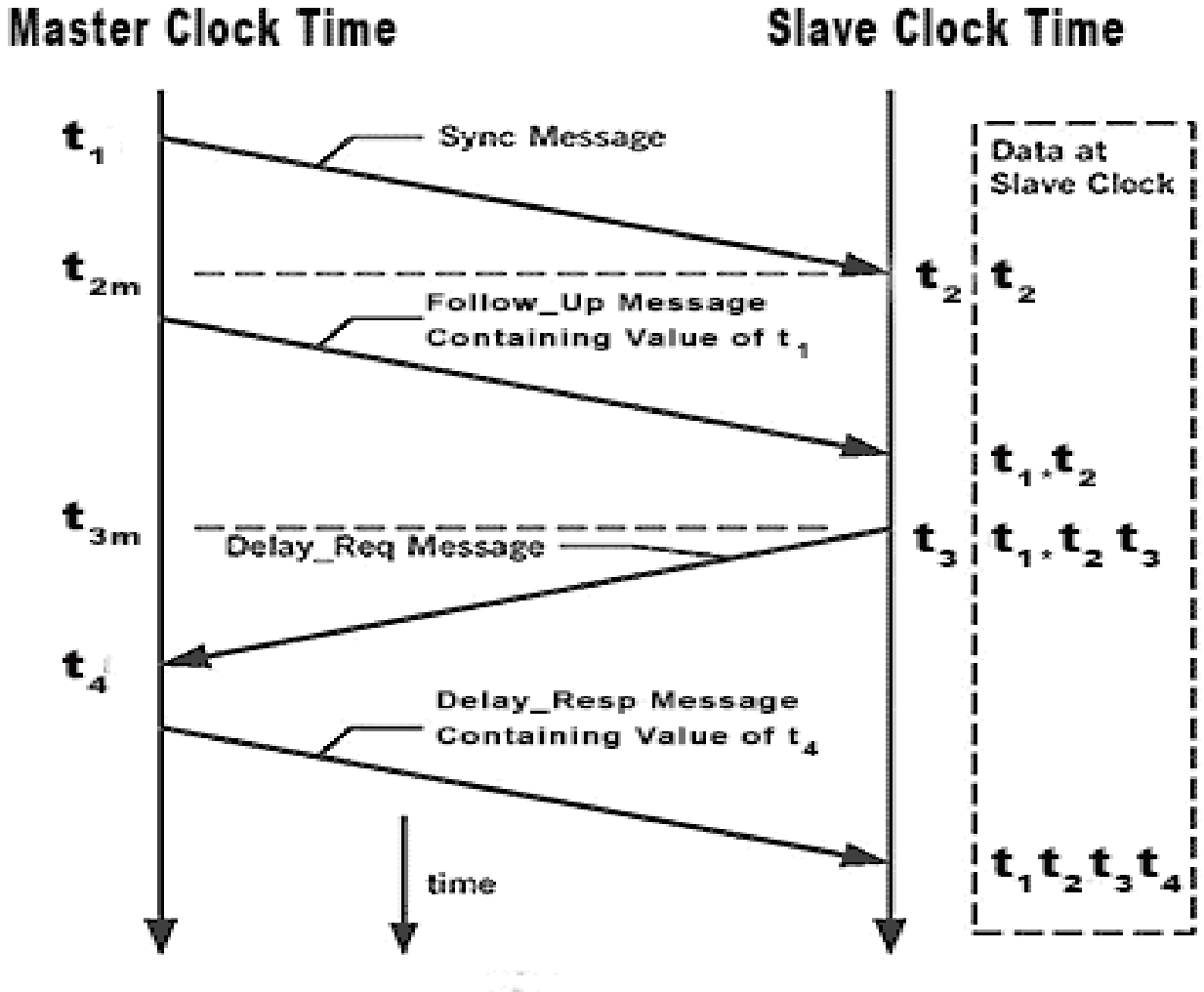


Рисунок 1.11 – Схема процесу синхронізації часу за протоколом PTP

У складній мережі AoIP вибір еталонного джерела часу здійснюється повністю автоматично за допомогою алгоритму Best Master Clock Algorithm (BMCA). Алгоритм аналізує низку показників усіх потенційних майстер-годинників, як пріоритет, клас годинника, стабільність осцилятора, і призначає один найкращий пристрій у ролі Grandmaster Clock.

Варто відзначити ключову проблему масштабування PTP. Формули PTP працюють ідеально лише за умови абсолютної симетрії мережі, коли час передачі туди дорівнює часу назад. Однак у реальних комутаторах пакети можуть затримуватися в чергах на різний час. Для вирішення цієї проблеми у великих територіально розподілених мережах застосовують спеціальні PTP-сумісні комутатори — прозорі годинники (Transparent Clocks, TC), які апаратно вимірюють час перебування пакета всередині комутатора і записують його в поле Correction Field пакета, або межові годинники (Boundary Clocks, BC), що виступають як підлеглий (Slave) для Grandmaster і як Master для локального сегмента гучномовців, зменшуючи багатоадресну передачу і сегментуючи домени синхронізації.

2 ПРОЄКТУВАННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

2.1 Загальна архітектура типу Hub-and-Spoke та основні компоненти системи

Для територіально розподілених об'єктів, таких як великі промислові підприємства, університетські кампуси або розгалужені мережі філій, архітектурна модель Hub-and-Spoke (центр-периферія) визнана найбільш ефективним стандартом побудови мереж. У контексті системи AoIP, центральний вузол (Hub) виступає ядром системи, де зосереджуються сервери обробки аудіо, контролери ініціації сеансів (SIP-сервери) та системи управління базами даних. Периферійні вузли (Spokes) представляють віддалені об’єкти, що містять кінцеві точки відтворення (IP-гучномовці), мікрофонні пейджингові консолі та датчики моніторингу фонового шуму.Централізована природа Hub-and-Spoke забезпечує адміністраторам єдину точку контролю та моніторингу. Це критично важливо для впровадження політик безпеки, оскільки весь трафік між периферійними вузлами обов'язково проходить через центральний вузол, де він може бути підданий інспекції за допомогою міжмережевих екранів (Firewalls) або систем виявлення вторгнень (IDS). Такий підхід дозволяє уникнути дублювання складного та дорогого обладнання на кожному віддаленому об'єкті. З точки зору хмарних технологій, Hub може бути реалізований як приватна хмара (IaaS) або використовувати рішення класу SaaS для управління розкладами сповіщень, тоді як периферія залишається апаратною базою для фізичного виведення звуку.

Однак, модель Hub-and-Spoke має вразливість у вигляді «єдиної точки відмови» (Single Point of Failure). Якщо центральний вузол або магістральний канал зв'язку виходить з ладу, вся система сповіщення може бути паралізована.3 Для вирішення цієї проблеми в проєкті впроваджуються технології резервування першого хопу (First Hop Redundancy Protocols, FHRP). Зокрема, розглядаються

протоколи HSRP (Hot Standby Router Protocol), VRRP (Virtual Router Redundancy Protocol) та GLBP (Gateway Load Balancing Protocol).

Важливим компонентом архітектури є фізичне середовище передачі. Використання модулів SFP (Small Form-factor Pluggable) дозволяє гнучко обирати тип підключення (мідний кабель або оптоволокно) залежно від відстані до віддалених об'єктів. Оптоволоконні лінії в архітектурі Hub-and-Spoke забезпечують гальванічну розв'язку та стійкість до електромагнітних завад, що є вирішальним фактором на промислових об'єктах. Кінцеві пристрої (IP-гучномовці) підключаються за технологією PoE (Power over Ethernet), що дозволяє передавати живлення та дані через один кабель витої пари, спрощуючи монтаж та забезпечуючи можливість централізованого живлення системи від джерел безперебійного живлення (ДБЖ) у серверній шафі.

2.2 Адресація та сегментація мережі

Кожному регіональному об'єкту виділяється окрема підмережа класу C (/24), що дозволяє підключити до 254 IP-пристроїв сповіщення на одну локацію. Для магістральних з'єднань між Hub та Spokes використовуються вузькі підмережі /30, що мінімізує витрати адресного простору та підвищує безпеку за рахунок обмеження кількості вузлів у транзитному сегменті (табл.2.1).

Таблиця 2.1 – Приклад списка адрес IPv4 для AoIP

Призначення підмережі	**Діапазон (приклад)**	**Сервери, контролери**
Центр	$10.0.1.0 - 10.0.1.255$	IP-гучномовці, консолі
Філія №1	$10.1.1.0 - 10.1.1.255$	IP-гучномовці, консолі
Філія №2	$10.2.1.0 - 10.2.1.255$	P2P з'єднання маршрутизаторів
Транзитний канал	$10.255.1.0 - 10.255.1.3$	Адміністративно обмежений мультикаст
Багатоадресна розсилка	$239.1.1.0 - 239.1.1.255$	Сервери, контролери

На фізичному рівні сегментація реалізується за допомогою технології VLAN (Virtual Local Area Network). Це дозволяє логічно розділити пристрої AoIP, офісні комп'ютери, системи відеоспостереження та гостьові мережі Wi-Fi. Головною перевагою такої сегментації є обмеження доменів широкомовних розсилок (Broadcast domains). У великих мережах надмірна кількість широкомовного трафіку може призвести до так званих «штормів», які створюють мікрозатримки у відтворенні аудіо. Винесення аудіопристроїв в окремий Voice VLAN дозволяє пріоритезувати їхній трафік на рівні комутаторів.

Важливим аспектом безпеки є впровадження концепції Zero Trust, який означає «ніколи не довіряй, завжди перевіряй». Кожен порт комутатора, до якого підключений IP-гучномовець, повинен мати налаштовану функцію Port Security для запобігання підміні пристроїв. Списки контролю доступу (ACL) на маршрутизаторах Hub обмежують можливість доступу до серверів сповіщення з будь-яких мереж, крім адміністративних, що мінімізує ризик несанкціонованої трансляції повідомлень.

Перехід на IPv6 розглядається як перспективний етап розвитку системи. IPv6 забезпечує значно більшу кількість адрес та має вбудовану підтримку безпеки (IPsec) та більш ефективні механізми багатоадресної розсилки, оскільки в цьому протоколі відсутній Broadcast як такий, що повністю замінений на спеціалізовані мультикаст-групи.

2.3 Вибір протоколів передачі даних

Для систем масового сповіщення обрано протокол UDP (User Datagram Protocol). На відміну від TCP, UDP працює за принципом «відправив і забув» (fire-and-forget), що забезпечує мінімальні накладні витрати на заголовки та відсутність затримок на підтвердження доставки. Якщо під час передачі даних в UDP було втрачено пакет, система просто передаватиме наступний пакет. Такі незначні втрати сприймаються людським вухом як ледь помітне клацання.

Поверх UDP працює RTP (Real-time Transport Protocol), який додає необхідний контекст для потокових даних. RTP забезпечує:

- порядкова нумерація дозволяє виявити втрати пакетів та відновити правильну послідовність на стороні приймача;
- часові мітки необхідні для синхронізації відтворення та компенсації джитера (тремтіння затримки);
- ідентифікацію джерела дозволяє приймачу розрізняти потоки від різних мікрофонів або серверів.

Допоміжний протокол RTCP (RTP Control Protocol) використовується для збору статистики про якість каналу зв'язку. Якщо рівень втрат пакетів перевищує критичне значення, система може автоматично переключитися на кодек з більшим ступенем стиснення або активувати механізми FEC (Forward Error Correction).

Для керування викликами та логічними з'єднаннями використовується SIP (Session Initiation Protocol). Це текстовий протокол прикладного рівня, що дозволяє пристроям узгоджувати параметри сеансу (вибір кодека, IP-адреси та порти) перед початком трансляції. Використання SIP дозволяє інтегрувати систему AoIP з корпоративною IP-АТС, надаючи можливість здійснювати оголошення зі звичайних офісних телефонів.

2.4 Проєктування логічної структури системи та сценарії роботи

Логічна структура системи базується на моделі клієнт-сервер із використанням механізмів багатоадресної розсилки (IP Multicast). У територіально розподілених об'єктах мультикаст є безальтернативним рішенням для масового сповіщення, оскільки він дозволяє уникнути перевантаження каналів зв'язку.

Для управління групами слухачів у локальних мережах використовується IGMP (Internet Group Management Protocol). При включенні IP-гучномовця він надсилає запит IGMP Join на певну мультикаст-адресу, що відповідає його зоні. Маршрутизатор філії фіксує цей запит і починає транслювати аудіопотік у цей сегмент. Використання IGMPv3 дозволяє реалізувати Source-Specific Multicast (SSM), що підвищує безпеку, оскільки гучномовці прийматимуть звук лише від авторизованого IP-адреса сервера.

Для маршрутизації багатоадресного трафіку між Hub та Spokes використовується PIM (Protocol Independent Multicast). У великих проєктах часто застосовується режим PIM Sparse Mode (PIM-SM). Його особливість полягає в тому, що трафік не розсилається по всій мережі, а передається лише до тих маршрутизаторів, де є активні підписники (модель Pull). Центром координації є Rendezvous Point (RP) – точка зустрічі, яка зазвичай розміщується на комутаторі ядра в Hub.

Для AoIP систем є декілька сценаріїв роботи:

- *загальне екстрене сповіщення.* Диспетчер активує тривожну кнопку. Сервер генерує RTP-потік на мультикаст-адресу групи «Всі зони». Мережа автоматично реплікує цей потік на кожен віддалений об'єкт. Завдяки пріоритезації QoS, повідомлення проходить миттєво, перериваючи інші трансляції;
- *адресний виклик.* Виклик конкретного гучномовця або терміналу допомоги. Використовується Unicast-з'єднання через SIP. Це дозволяє організувати двосторонній зв'язок між Hub та певною точкою на периферії;
- *трансляція фонового контенту.* Сервер відтворює медіа-файли за

розкладом для певних груп зон (наприклад, зони відпочинку). Використовується Multicast з низьким пріоритетом;

- *робота в умовах збою каналу.* При розриві зв'язку з Hub, периферійні контролери Spokes переходять у автономний режим, відтворюючи заздалегідь записані тривожні повідомлення з локальної пам'яті за сигналами від локальних датчиків.

2.5 Забезпечення якості обслуговування (QoS)

Якість обслуговування (Quality of Service) в системах AoIP є критичним фактором, що визначає розбірливість мови та комфорт сприйняття звуку. Мережа повинна гарантувати певні параметри для пакетів реального часу, навіть якщо решта каналу заповнена іншим трафіком.

Ключові параметри QoS для аудіо:

- затримка – це час проходження пакета від джерела до приймача. Для систем сповіщення допустимою є загальна затримка до 150-200 мс. Якщо затримка перевищує ці межі, виникає ефект відлуння, що заважає координації дій у разі надзвичайної ситуації;
- джиттер (jitter) – варіація затримки між послідовними пакетами. Якщо пакети приходять нерівномірно, буфер пристрою відтворення може або спорожніти (пауза), або переповнитися (втрата даних). Для компенсації джиттера використовуються адаптивні буфери (Jitter Buffers);
- втрата пакетів показує скільки відсотків звуку втрачено під час надсилання пакета. Для якісного звуку втрати повинні бути менше 1%. Втрати понад 3% призводять до спотворень голосу, що робить повідомлення незрозумілими.

Система синхронізації часу є окремим важливим аспектом QoS. Для територіально розподілених об'єктів критично важливо, щоб усі гучномовці

відтворювали повідомлення синхронно. Для загальних завдань використовується протокол NTP (Network Time Protocol), що забезпечує точність у межах мілісекунд. Однак для професійних аудіосистем, де важлива фазова синхронізація, впроваджується PTP (Precision Time Protocol, IEEE 1588), що забезпечує точність на рівні мікросекунд, використовуючи апаратні мітки часу в мережевих картах пристроїв.

3 РЕАЛІЗАЦІЯ ТА АНАЛІЗ РОБОТИ СИСТЕМИ

3.1 Вибір середовища моделювання

У процесі розробки автоматизованої системи багатоадресного аудіосповіщення (Audio-over-IP) для територіально розподілених об’єктів виникає необхідність не лише теоретичного проєктування, але й практичної перевірки прийнятих рішень. З цією метою у даній роботі використано програмне середовище моделювання комп’ютерних мереж Cisco Packet Tracer.

Використання Cisco Packet Tracer обумовлене тим, що дана платформа дозволяє створювати повноцінні віртуальні моделі мережевих інфраструктур, максимально наближені до реальних умов функціонування. Це особливо важливо при дослідженні систем, що базуються на технологіях передачі даних у реальному часі, таких як Audio-over-IP, де критичними є параметри затримки, стабільності та ефективності передачі.

Однією з ключових переваг Packet Tracer є можливість моделювання складних топологій, включаючи централізовані структури типу Hub-and-Spoke, які застосовуються у даній роботі. Завдяки цьому можна наочно відобразити взаємодію між центральним вузлом і віддаленими об’єктами, перевірити коректність маршрутизації та оцінити поведінку мережі при передачі multicast-трафіку.

Важливим аргументом на користь використання даного середовища є підтримка основних мережевих протоколів, які застосовуються в роботі, зокрема UDP, RTP (частково концептуально), IGMP та PIM. Це дозволяє реалізувати модель багатоадресної передачі даних, перевірити механізми підписки на multicast-групи, а також дослідити процес розповсюдження аудіопотоку в мережі.

Крім того, Packet Tracer надає можливість конфігурування мережевого обладнання за допомогою командного рядка, що імітує роботу реальних

маршрутизаторів і комутаторів. Це дає змогу відпрацювати практичні навички налаштування мереж, зокрема:

- адресацію та сегментацію;
- налаштування маршрутизації;
- активацію multicast;
- організацію взаємодії між вузлами.

Ще однією важливою перевагою є можливість візуалізації процесів передачі даних. Packet Tracer дозволяє спостерігати за рухом пакетів у режимі симуляції, що значно спрощує розуміння складних мережевих процесів. Це особливо корисно при аналізі multicast-трафіку, який має специфічну логіку розповсюдження.

Packet Tracer повністю задовольняє вимоги даної роботи, оскільки дозволяє змоделювати логіку функціонування системи, перевірити правильність налаштувань і продемонструвати принципи роботи Audio-over-IP.

3.2 Побудова моделі мережі

Побудова мережі в програмному середовищі Cisco Packet Tracer є ключовою задачею у даній роботі. Реалізація системи AoIP починається з налаштування мережевої інфраструктури, до якої входять маршрутизатори, комутатори, сервер та кінцеві пристрої. На цьому етапі закладається основа для подальшої роботи всієї системи, тому правильність налаштування є критично важливою.

Спочатку було підготовлено всі потрібні пристрої для майбутньої системи(рис.3.1).

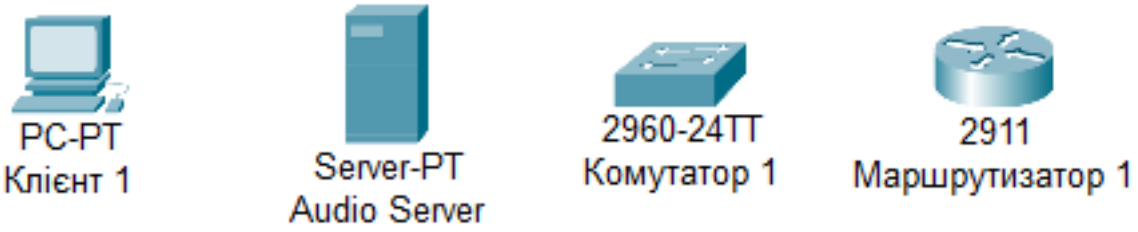


Рисунок 3.1 – Зовнішній вигляд необхідних пристроїв для складання мережевої системи в Cisco Packet Tracer

Після чого було об’єднано пристрої в архітектурну модель Hub-and-Spoke (рис.3.2).

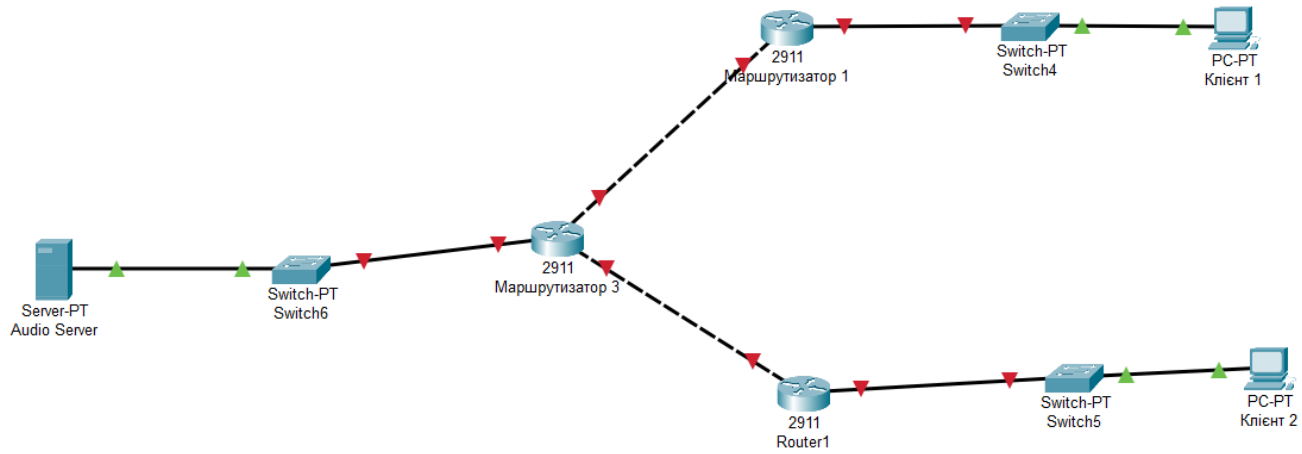


Рисунок 3.2 – Схема архітектурної моделі модель Hub-and-Spoke в Cisco Packet Tracer

Для налагодженого зв’язку між всіма пристроями в кожному LAN потрібно призначити для кожного пристрою свою IP адресу (табл.3.1).

Таблиця 3.1 – Призначення IP адрес для кожного пристрою

Назва пристроя	IP адреса
Audio Server	192.168.1.100
Клієнт 1	192.168.2.10
Клієнт 2	192.168.3.10
Центральний маршрутизатор (зв’язок до сервера)	192.168.1.1
Маршрутизатор 1(зв’язок до Клієнта 1)	192.168.2.1
Маршрутизатор 2(зв’язок до Клієнта 2)	192.168.3.1

Після пропису цих команд було отримано налагоджені зв’язки між пристроями в усіх LAN(рис.3.3).

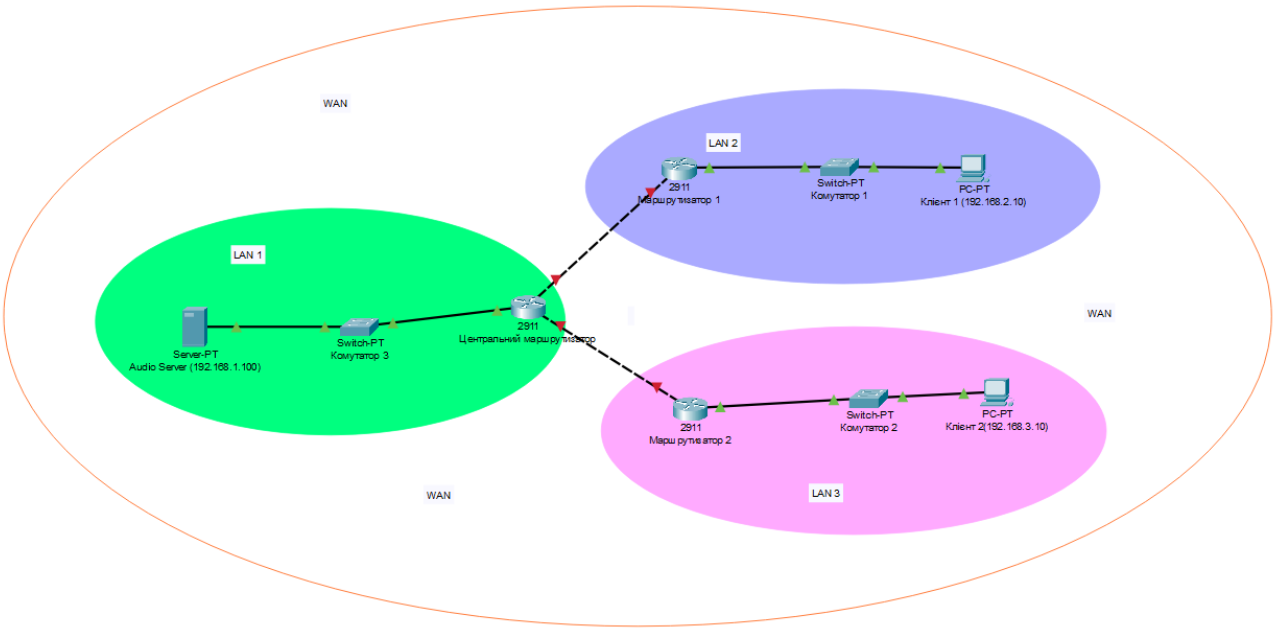


Рисунок 3. 3 – Оновлена схема архітектурної моделі модель Hub-and-Spoke в Cisco Packet Tracer

Але для повної взаємодії між усіма компонентами мережі, потрібно з'єднати 2 клієнтські маршрутизатора з центральним роутером. Для цього, зайшовши в командний інтерфейс центрального маршрутизатора, прописали зв'язки до двох інших роутерів (рис.3. 4).

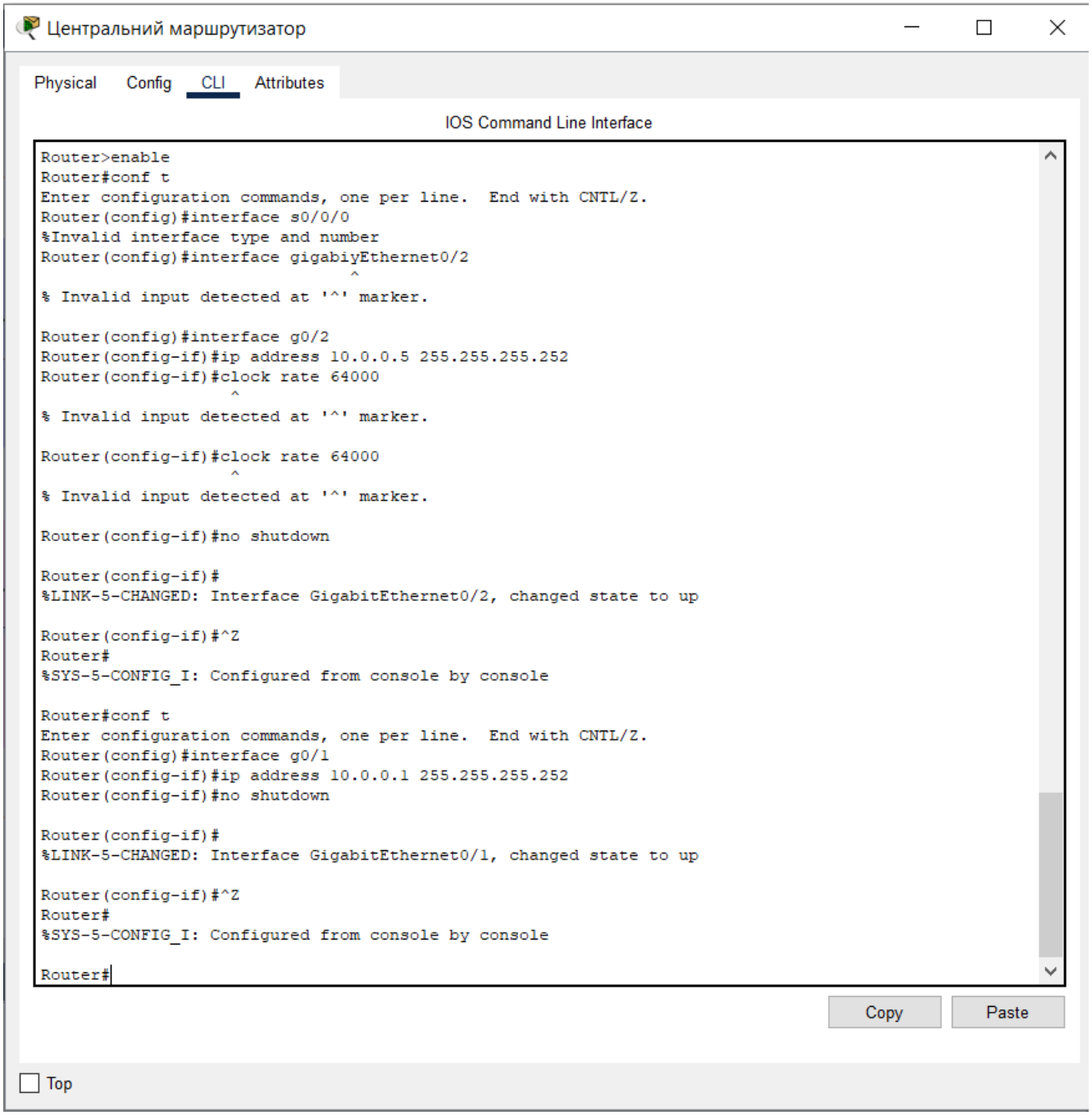


Рисунок 3.4 – Зовнішній вигляд командного інтерфейса центрального маршрутизатора з налаштуванням з’єднання до 1 та 2 маршрутизаторів

Таке саме потрібно прописати і для двох інших маршрутизаторів (рис.3.5).

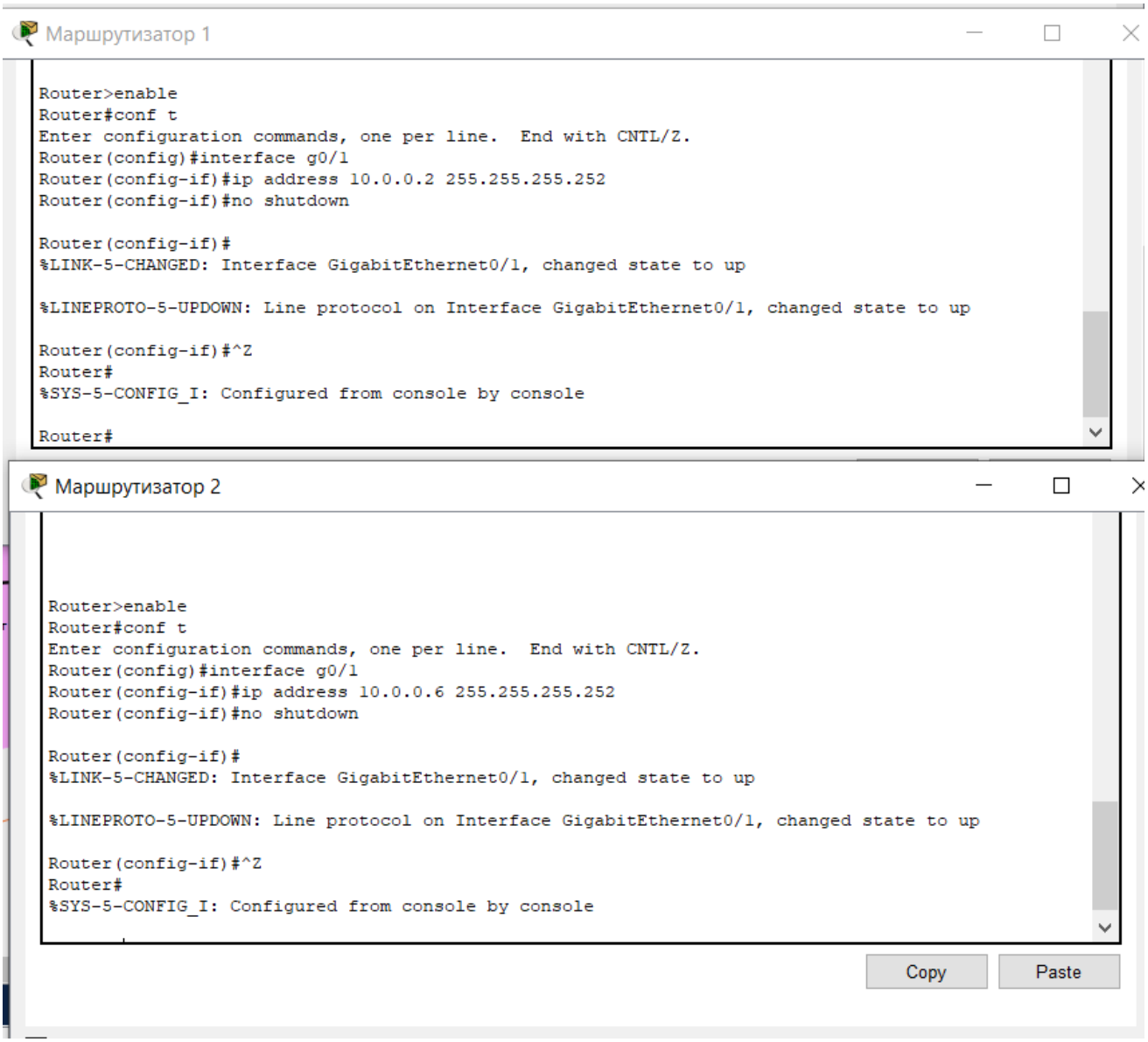


Рисунок 3.5 – Зовнішній вигляд командних інтерфейсів 1 та 2 маршрутизаторів з налаштуваннями з’єднаннями до центрального маршрутизатора

В кінці було отримано повністю налаштовані IP адреси на всих пристроях мережевої системи (рис.3.6).

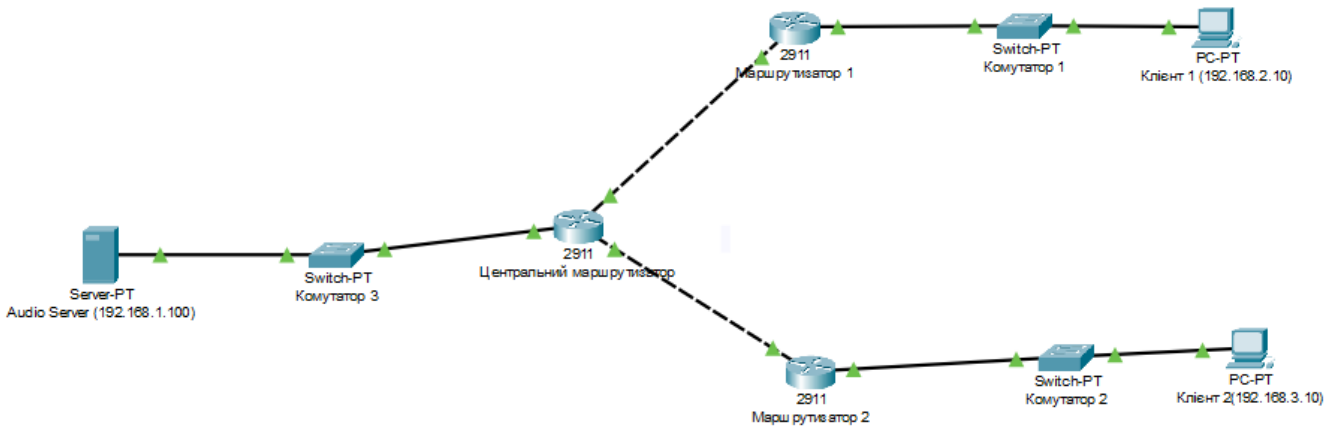


Рисунок 3. 6 – Зовнішній вигляд архітектурної моделі модель Hub-and-Spoke в Cisco Packet Tracer після налаштування IP адрес

3.3 Налаштування багатоадресної передачі

Після налаштування IP адрес, необхідно забезпечити маршрутизацію між різними сегментами мережевої системи. Для цього центральному роутеру потрібно знати, як можна дістатися до інших LAN, а іншим маршрутизаторам потрібно знати шлях, через який буде йти трафік. Для цього було прописано потрібні шляхи в кожному командному інтерфейсі (рис.3.7).

Для даної мережевої інфраструктури було прийнято рішення налаштувати статичну багатоадресну передачу (Multicast) замість використання динамічних протоколів маршрутизації (зокрема OSPF). Такий підхід зумовлений відносною простотою топології системи, де відсутність потреби в автоматичному виявленні сусідів та динамічній перебудові маршрутів дозволяє мінімізувати накладні витрати на службовий трафік та спростити адміністрування.

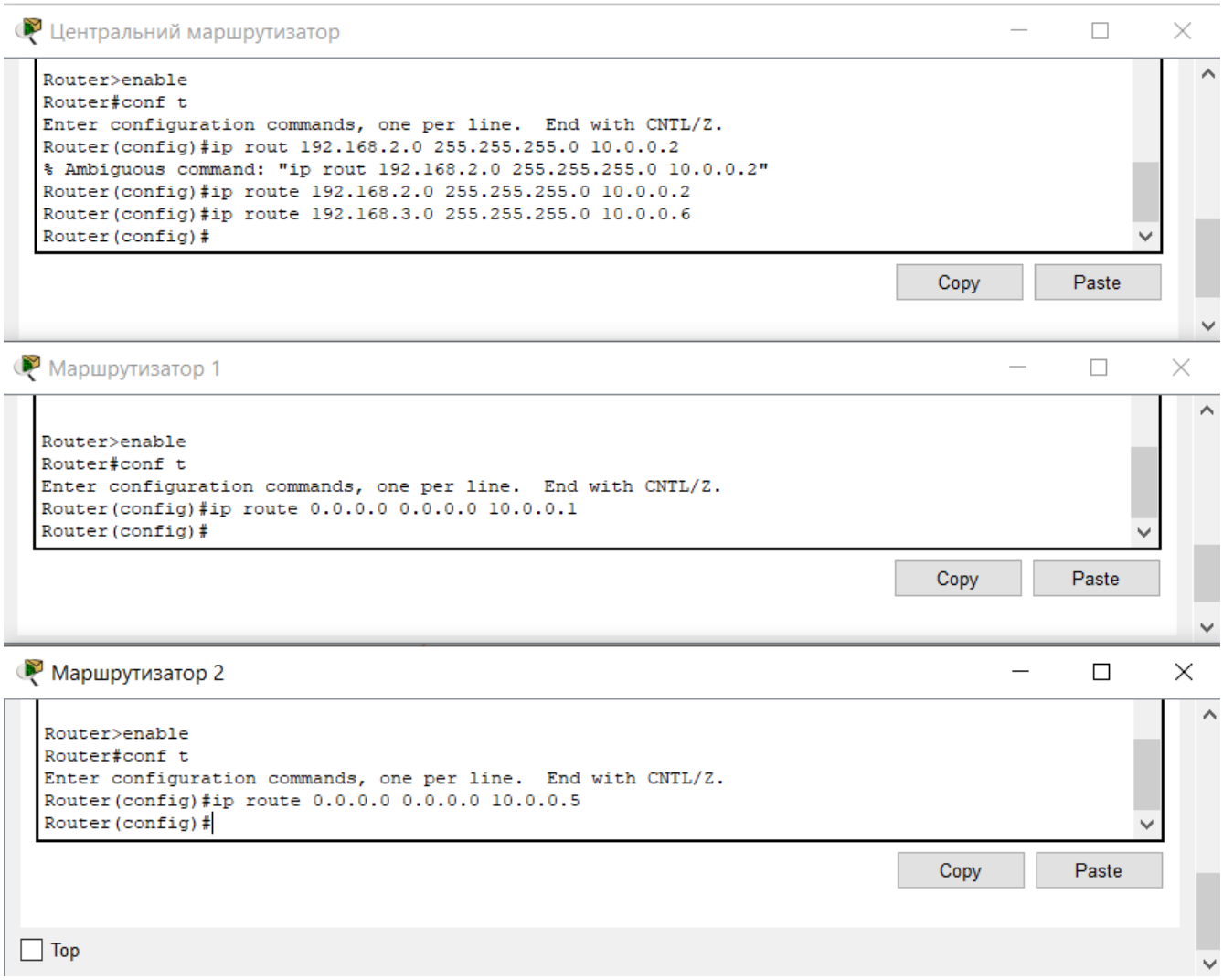


Рисунок 3.7 – Зовнішній вигляд командних інтерфейсів маршрутизаторів з налаштуваннями маршрутизації між ними

3.4 Реалізація передачі аудіо та тестування роботи системи

Одним із ключових етапів реалізації системи є налаштування багатоадресної передачі даних. Multicast дозволяє передавати аудіопотік одночасно великій кількості отримувачів без дублювання трафіку.

Але у зв'язку з архітектурними обмеженнями програмного симулятора мереж Cisco Packet Tracer щодо повноцінної підтримки протоколів багатоадресної маршрутизації (зокрема протоколу PIM та функції ip multicast-routing на

маршрутизаторах доступу серії 2911), фізичне моделювання багатоадресного дерева розсилки у практичній частині було замінено на логічну імітацію.

Для цієї імітації було ввімкнено режим Simulation, залишивши лише ICMP та UDP файли (рис.3.8).

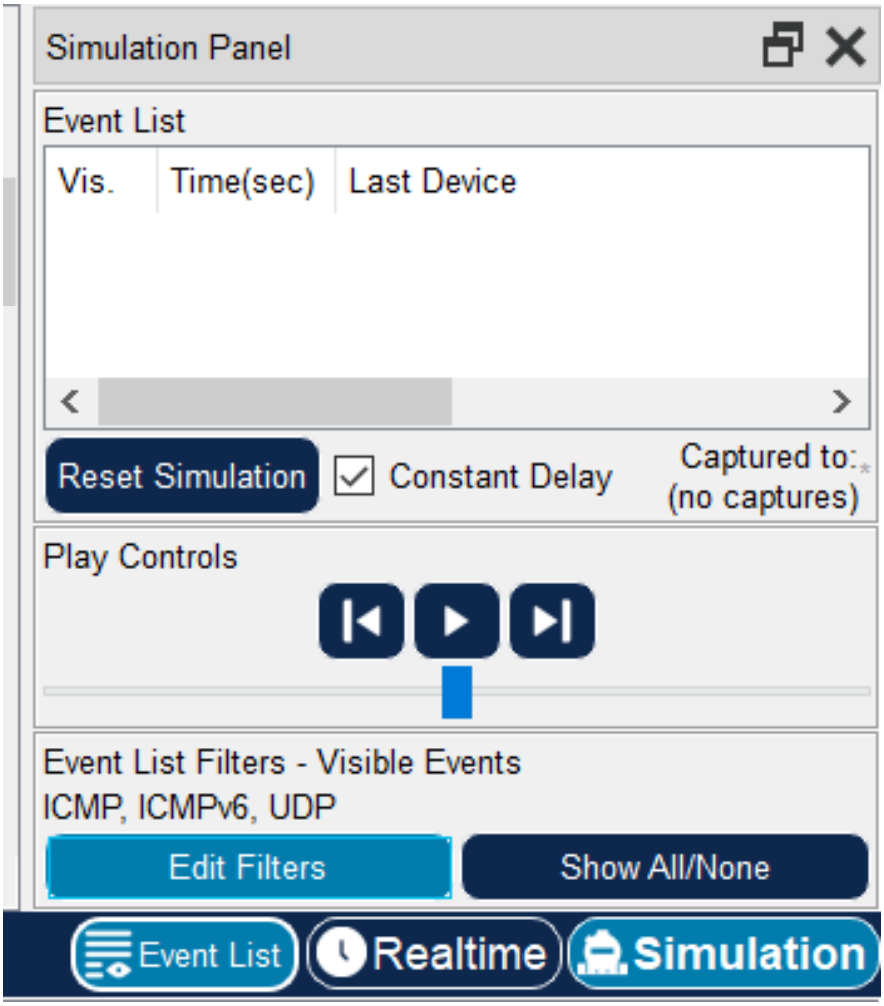


Рисунок 3.8 – Зовнішній вигляд панелі Simulation

Після чого було обрано у верхньому куті Add Simple PDU та відправлено 2 пакета від сервера до клієнтів (рис.3.9).

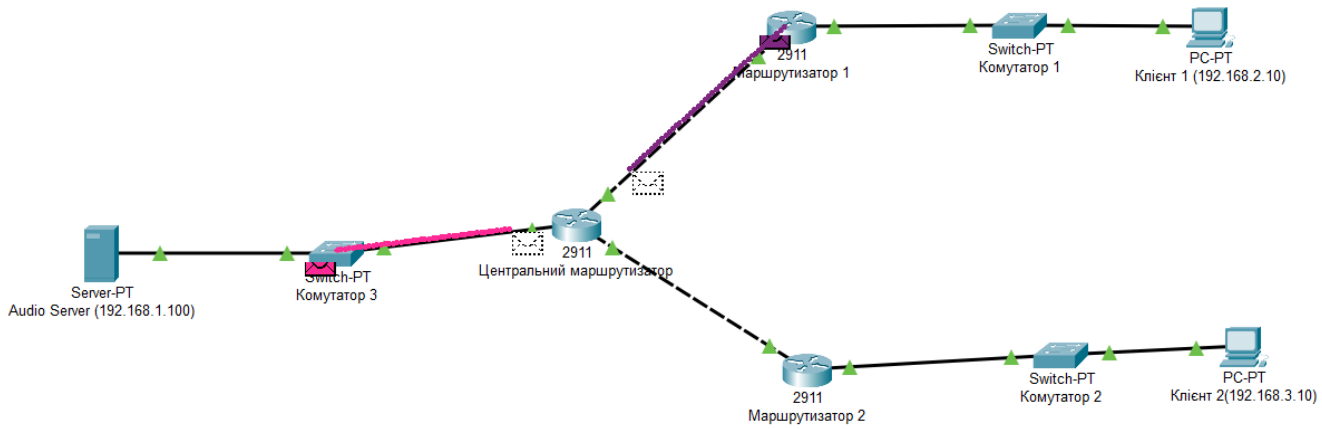


Рисунок 3.9 – Зовнішній вигляд процесу імітації передачі аудіо

Після завершення імітації надсилання аудіо в програмному середовищі моделювання комп'ютерних мереж Cisco Packet Tracer, нижче було вибито ICMP файли, які означають, що система імітації надсилання аудіо в системі Audio-over-IP для територіально розподілених об'єктів була налаштована правильним чином (рис.3.10).

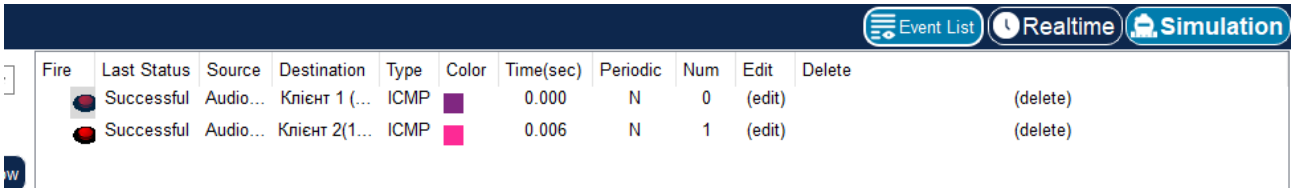


Рисунок 3.10 – Зовнішній вигляд кінцевого тесту на правильність налаштування системи Audio-over-IP

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було успішно вирішено актуальну технічну задачу розробки інфраструктури автоматизованої системи багатоадресного аудіосповіщення для територіально розподілених об'єктів. Дослідження фундаментальних принципів побудови таких систем підтвердило, що технологія передачі аудіо через IP-мережі забезпечує суттєві переваги над застарілими аналоговими рішеннями завдяки децентралізації обчислень, використанню стандартного мережевого обладнання та можливості гнучкої програмної маршрутизації. Аналіз стека протоколів показав, що для безперебійної трансляції медіаданих у реальному часі критично важливою є тісна інтеграція протоколу ініціювання сеансів (SIP) для логічного управління викликами та транспортного протоколу реального часу (RTP) поверх користувацьких датаграм (UDP). Саме такий підхід дозволяє мінімізувати наскрізні затримки та забезпечити стабільно високий індекс розбірливості мови.

Окремо в роботі доведено безальтернативність використання технології багатоадресної розсилки (IP Multicast) для завдань масового сповіщення. Цей метод дозволяє максимально оптимізувати пропускну здатність магістральних каналів зв'язку завдяки використанню протоколів управління групами (IGMP) на рівні доступу та незалежної маршрутизації (PIM) у ядрі мережі. Під час проєктування інфраструктури було обґрунтовано вибір архітектурної моделі Hub-and-Spoke з центральним ядром та периферійними філіями, що забезпечує єдину точку контролю, ефективну логічну сегментацію мережі та високий рівень безпеки. Практична реалізація проєкту була виконана шляхом побудови топологічної моделі у програмному середовищі Cisco Packet Tracer. Також було проведено базове налаштування маршрутизаторів, комутаторів та імітацію передачі потокового трафіку між вузлами. Незважаючи на архітектурні обмеження симулятора щодо підтримки повного стека багатоадресної

маршрутизації, розроблена конфігурація дозволила успішно протестувати логіку взаємодії пристроїв. Отримані результати моделювання повністю підтверджують працездатність запропонованих інженерних рішень, їхню мережеву надійність та доцільність практичного впровадження на реальних об'єктах для організації ефективного екстреного оповіщення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Voice Evacuation Systems Applications Guide - Honeywell | Digital Assets, URL:https://prod-edam.honeywell.com/content/dam/honeywell-edam/hbt/en-us/documents/manuals-and-guides/reference-guides/hbt-fire VoiceEvacuationSystems_AppGuide_AVAG497.pdf (дата звертання:09.04.2026).
2. Understanding VoIP Protocols — SIP, RTP, and More | by RocketMe Up Networking, URL:https://medium.com/@RocketMeUpNetworking/understanding-voip-protocols-sip-rtp-and-more-e1cc54e9f0af (дата звертання: 09.04.2026).
3. What is Audio over IP? - Nevion, URL:https://nevion.com/lexicon/what-is-audio-over-ip/ (дата звертання: 09.04.2026).
4. Distributed Acoustic Sensing of Sounds in Audible Spectrum in Realistic Optical Cable Infrastructure - PMC, URL:https://pmc.ncbi.nlm.nih.gov/articles/PMC12075592/ (дата звертання: 09.04.2026).
5. Wikimedia Commons. URL: https://upload.wikimedia.org/wikipedia/commons/thumb/2/22/Utbredning_av_ljudvågor_--_Onda_sonora_se_propagando_(mul).svg/960px-Utbredning_av_ljudvågor_--_Onda_sonora_se_propagando_(mul).svg.png (дата звернення: 09.04.2026).
6. Audio Over IP | Docs and Guides - NDI, URL:https://docs.ndi.video/all/using-ndi/ndi-for-audio/audio-over-ip (дата звертання: 09.04.2026).
7. Residential Audio over IP (AoIP) is Here - CEPRO, URL: https://www.cepro.com/news/residential-audio-over-ip-aoip/105661/ (дата звертання: 09.04.2026).
8. Contributors to Wikimedia projects. User datagram protocol - wikipedia. Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/User_Datagram_Protocol (дата звертання: 09.04.2026).

9. CIE award winning UK distributor for professional Door Intercom, Access Control and AV equipment. URL: https://cie-group.com/media/upload/images/Infographics/IP-Audio-and-Lockdown-system-diagram.jpg (дата звернення: 10.04.2026).

10. UDP (user datagram protocol) - computer networks - computer science engineering. EDUREV.IN. URL: https://edurev.in/t/97210/udp-user-datagram-protocol- (дата звертання: 10.04.2026).

11. Audio Over IP: Building Pro AoIP Systems with Livewire, URL: http://pws.npru.ac.th/sartthong/data/files/Audio_Over_IP__Building_Pro_AoIP_Systems_with_Livewire.pdf (дата звертання: 10.04.2026).

12. Towards an Architecture for Audio/Video Conferencing in Distributed Brokering Systems - ResearchGate, URL: https://www.researchgate.net/publication/221109749_Towards_an_Architecture_for_AudioVideo_Conferencing_in_Distributed_Brokering_Systems (дата звертання: 10.04.2026).

13. Home page | Webex Blog. URL: https://blog.webex.com/wp-content/uploads/2024/06/rtp-packet-format-shown-in-32-bit.png (дата звернення: 10.04.2026).

14. Understanding IP Production Networks: Part 5 - Audio Over IP Basics, URL:https://www.thebroadcastbridge.com/content/entry/6798/understanding-ip-broadcast-production-networks-audio-over-ip (дата звертання: 10.04.2026).

15. Professional AoIP for Broadcast - The Way Forward - Solid State Logic, URL:https://solidstatelogic.com/assets/uploads/downloads/s300/Professional%20AoIP%20for%20Broadcast%20-%20The%20Way%20Forward.pdf (дата звертання: 10.04.2026).

16. Contributors to Wikimedia projects. Session initiation protocol - wikipedia, 2001. Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Session_Initiation_Protocol#/media/File:SIP_session_setup_example.svg (дата звертання: 10.04.2026).

17. Your practical guide to AES67 - part 1 - RAVENNA Network, URL: https://www.ravenna-network.com/your-practical-guide-to-aes67-part-1-2/ (дата звертання: 11.04.2026).

18. Castr | #1 Live Video Streaming Solution With Video Hosting. URL: https://castr.com/blog/wp-content/uploads/2023/05/Unicast-vs-Multicast-vs-Broadcast-1-2048x1075.jpg (дата звернення: 11.04.2026).

19. AES67 - Wikipedia, URL: https://en.wikipedia.org/wiki/AES67 (дата звертання: 11.04.2026).

20. Synchronization of streamed audio between multiple playback devices over an unmanaged IP network, URL: https://lup.lub.lu.se/student-papers/record/8052964/file/8053165.pdf (дата звертання: 11.04.2026).

21. IGMP-working. Media Geeksforgeeks. URL: https://media.geeksforgeeks.org/wp-content/uploads/20200429202814/IGMP-working-gfg-1024x376.png (дата звертання: 11.04.2026).

22. What is the Real-time Transport Protocol (RTP)? - Sipfront, URL: https://sipfront.com/blog/2026/04/what-is-the-real-time-transport-protocol-rtp/ (дата звертання: 11.04.2026).

23. SIP Protocol: Definition & How it Works [+Video Explainer] (2024) - Yeastar, URL: https://www.yeastar.com/blog/sip-protocol/ (дата звертання: 11.04.2026)

24. AV over IP: How Today's Trends Shape Our Connected Future - NETGEAR Blog, URL: https://www.netgear.com/hub/business/av/av-over-ip-how-todays-trends-shape-our-connected-future/ (дата звертання: 11.04.2026).

25. IP Multicast Technology Overview - Cisco, URL: https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/mcst_ovr.html (дата звертання: 12.04.2026).

26. What is IGMP Snooping? - PyNet Labs. PyNet Labs. URL: https://www.pynetlabs.com/what-is-igmp-snooping/ (date of access: 12.04.2026).

27. Unicast vs. Multicast vs. Broadcast: What's the Difference? - Castr, URL: https://castr.com/blog/unicast-vs-multicast-vs-broadcast/ (дата звертання: 12.04.2026).

28. PyNet Labs: IT, Networking, AI & Automation Training Company. URL: https://www.pynetlabs.com/wp-content/uploads/2024/02/pim-sparse-mode.jpeg (дата звернення: 12.04.2026).

29. Multicast (IGMP and PIM) - NVIDIA Docs, URL: https://docs.nvidia.com/networking/display/nvidiaonyxusermanualv3104408lts/multicast+(igmp+and+pim) (дата звертання: 12.04.2026).

30. What is Multicast Networking and How Does It Work?, URL: https://www.auvik.com/franklyit/blog/multicast-networking/ (дата звертання: 12.04.2026).

31. IPCisco | Cisco Networking Academy | Network Certification | Learn. URL: https://ipcisco.com/wp-content/uploads/2019/02/ntp-stratum.jpg (дата звернення: 12.04.2026).

32. Network Timing Technology: NTP vs. PTP - Masterclock, URL: https://www.masterclock.com/network-timing-technology-ntp-vs-ptp.html (дата звертання: 12.04.2026).

33. PTP vs NTP: Key Differences & Use Cases Explained (2025 Guide) - Syncworks, URL: https://syncworks.com/ptp-vs-ntp-key-diferences-use-cases/ (дата звертання: 13.04.2026).

34. Home - OnTime Networks. URL: https://ontimenet.com/wp-content/uploads/2023/10/PTP-Message-Sequences.gif (дата звернення: 13.04.2026).

35. The Difference between NTP and PTP – We'll show you - mobatime, URL: https://www.mobatime.com/technology/difference-between-ntp-and-ptp/ (дата звертання: 13.04.2026).

36. Immersive Acoustics via Next-Generation Networks: Achieving High-Fidelity Audio in the Metaverse - IEEE Xplore, URL: https://ieeexplore.ieee.org/iel8/8782661/8901158/11160687.pdf (дата звертання: 13.04.2026).

37. Precision Time Protocol - Wikipedia, URL: https://en.wikipedia.org/wiki/Precision_Time_Protocol (дата звертання: 13.04.2026).

38. Disaster Mitigation and Emergency Help with Public Address(PA) System Design Based on Audio Over Ethernet (AoE), IDS, and IOT, URL: https://injoit.org/index.php/j1/article/download/1950/1772 (дата звертання: 13.04.2026).

39. Hub-And-Spoke Office Model – NetComLearning URL: https://www.netcomlearning.com/blog/what-is-hub-and-spoke-model (дата звертання: 13.04.2026).

40. Проєктування мережевої інфраструктури з урахуванням вимог кібербезпеки: підходи та реалізація на базі cisco – Csecurity Kubg, URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/845 (Дата звертання: 13.04.2026)

41. Real-time Transport Protocol - Wikipedia, URL: https://en.wikipedia.org/wiki/Real-time_Transport_Protocol (дата звертання: 14.04.2026).

42. RTP Transmission: coping with real networks - Webex Blog, URL: https://blog.webex.com/engineering/rtp-transmission-coping-with-real-networks/ (дата звертання: 14.04.2026).

43. Real-Time Acoustic Detection of Critical Incidents in Smart Cities Using Artificial Intelligence and Edge Networks - PMC, URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC12030909/ (дата звертання: 14.04.2026).

44. IP Multicast: Tutorial With Examples - Catchpoint, URL: https://www.catchpoint.com/network-admin-guide/ip-multicast (дата звертання: 14.04.2026).

45. IP Multicast in Cable Networks - Cisco, URL: https://www.cisco.com/en/US/technologies/tk648/tk828/technologies_case_study0900aecd802e2ce2.html (дата звертання: 14.04.2026).

46. Quality of service - Wikipedia, URL: https://en.wikipedia.org/wiki/Quality_of_service (дата звертання: 14.04.2026).

47. RFC 4710 - Real-time Application Quality-of-Service Monitoring (RAQMON) Framework, URL: https://datatracker.ietf.org/doc/html/rfc4710 (дата звертання: 14.04.2026).

Додаток А

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ



Навчально-науковий інститут Інформаційних технологій
Кафедра Комп'ютерної інженерії

КВАЛІФІКАЦІЙНА РОБОТА
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА

на тему: «Розробка автоматизованої системи багатоадресного аудіосповіщення (Audio-over-IP) для територіально розподілених об'єктів»

Виконала студенка групи КІД-41
Бровченко Тетяна Яківна

Керівник кваліфікаційної роботи:
Бученко Ігор Анатолійович,
Старший викладач кафедри КІ

Київ – 2026

Мета роботи – Підвищення надійності та масштабованості систем сповіщення шляхом розробки AoIP-комплексу із синхронізацією часу.

Об`єкт дослідження – Процес передачі потокових аудіоданих у територіально розподілених мережах.

Предмет дослідження – Мережеві протоколи та апаратно-програмні засоби автоматизації.

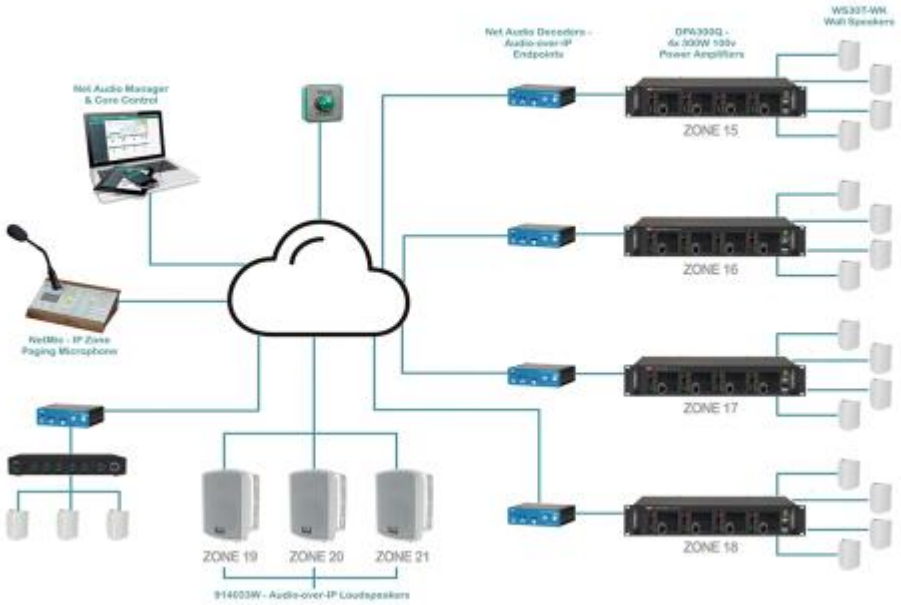
Актуальність обраної теми

Перехід від застарілих аналогових систем оповіщення до цифрових рішень AoIP є критичним для територіально розподілених підприємств. Використання стандартної Ethernet-інфраструктури замість дорогого прокладання кабельних трас дозволяє суттєво знизити капітальні та операційні витрати. Це забезпечує миттєву автоматизацію, централізоване управління та гарантовану якість сигналу, що є базовою вимогою цивільного захисту та промислової безпеки в сучасних умовах.

Характеристика технології Audio-over-IP (AoIP)

Принцип: комутація пакетів замість комутації каналів.
Ключові особливості:
- низька затримка, що забезпечує передачу сигналу в реальному часі (до 10-20 мс);
- можливість додавання необмеженої кількості зон оповіщення без перепроектування мережі;
- легка інтеграція з іншими системами безпеки та IP-телефонією;
- орієнтується на відкриті стандарти (AES67), що забезпечує сумісність обладнання різних виробників;
- технологія гарантує цілісність сигналу;
- конвергенція інфраструктури.

Приклад системи AoIP



Стек протоколів реального часу

UDP (User Datagram Protocol). Транспортний протокол який працює за формою «відправив і забув».
RTP (Real-time Transport Protocol). Додає порядкові номери та часові мітки для відновлення черговості пакетів.
SIP (Session Initiation Protocol). Встановлення, підтримання та завершення мультимедійного зв'язку між декількома вузлами.

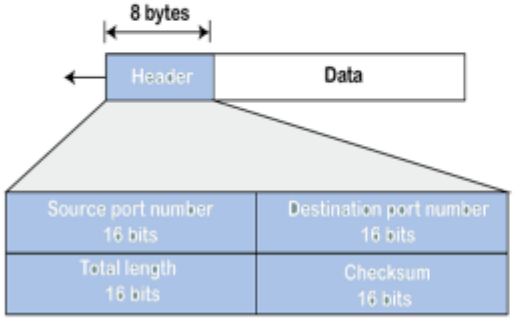


Рисунок 1.1 – Структура заголовка UDP

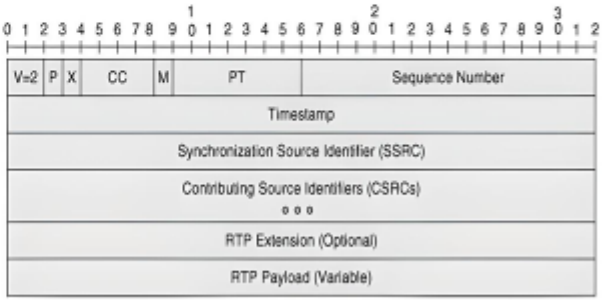


Рисунок 1.2 – Структура заголовка RTP

Механізми передачі: Multicast vs Unicast vs Broadcast

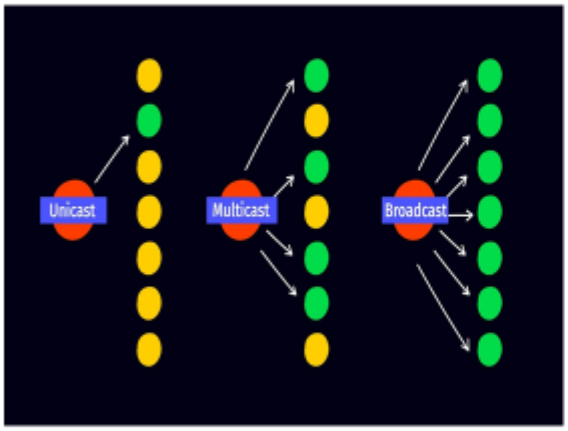


Рисунок 1.3 – Схема передачі даних у Unicast, Multicast та Broadcast

Unicast (Одноадресна): Пряма передача "точка-точка". Велике навантаження на сервер при масовому сповіщенні.

Broadcast (Широкомовна): Передача всім пристроям у сегменті. Створює надлишкове навантаження на пристрої, які не потребують отримання аудіо

Multicast (Багатоадресна) – Оптимальне рішення для AoIP. Сервер генерує лише 1 потік даних. Трафік доставляється лише тим вузлам, які надіслали запит на підписку. Multicast є кращим варіантом для масового сповіщення у великих мережах.

Маршрутизація багатоадресного трафіку

IGMP (v2/v3): Управління підписками клієнтів у локальній мережі та працює на L2 рівні моделі OSI.
IGMP Snooping: Запобігання «штормам» трафіку на комутаторах.
PIM Sparse Mode: Маршрутизація мультикасту між філіями (L3) через «точку зустрічі» (Rendezvous Point).

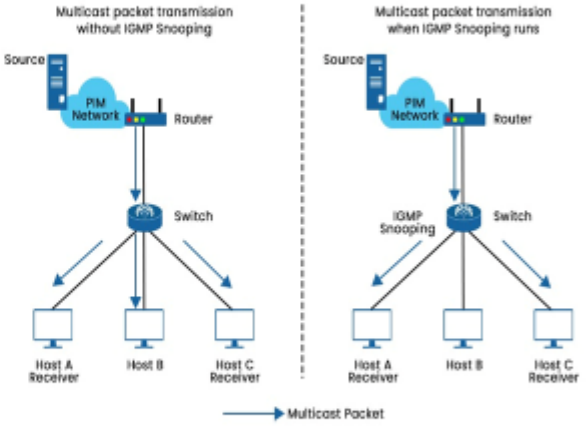


Рисунок 1.4 – Схема передачі багатоадресних пакетів з та без IGMP Snooping

Синхронізація часу

1. NTP (Network Time Protocol) використовується для загальної синхронізації системних логів та розкладу автоматичних оголошень (точність на рівні мілісекунд).
2. PTP (Precision Time Protocol, IEEE 1588) необхідний для фазової синхронізації відтворення звуку на різних IP-гучномовцях.

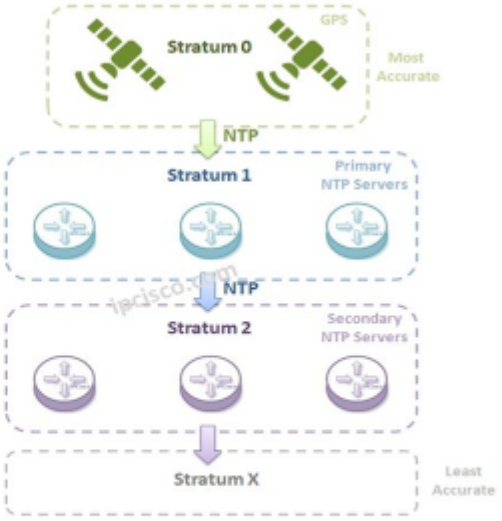


Рисунок 1.5 – Схема ієрархії системи Stratum в NTP

Моделювання мережі в Cisco Packet Tracer

Тип топології: Hub-and-Spoke.

Завдання: перевірка логіки Hub-and-Spoke та маршрутизації між сегментами.

Сценарій: побудова топології, що імітує головний офіс та два віддалених філіали.

Використане обладнання:
- маршрутизатори;
- комутатори;
- кінцеві пристрої (Server та PC).

Аналіз результатів моделювання

Метод. Логічна імітація передачі потокового трафіку в режимі Simulation.

Результати. Тестування успішно підтвердило доставку пакетів (ICMP/UDP) від сервера до територіально віддалених клієнтів.

Висновок. Запропонована структура є працездатною та відмовостійкою.

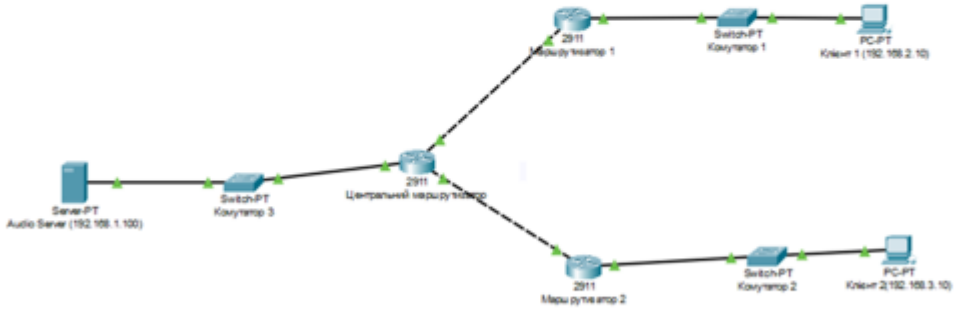


Рисунок 1.6 - Зовнішній вигляд архітектурної моделі модель Hub-and-Spoke в Cisco Packet Tracer

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи розроблено інфраструктуру автоматизованої системи багатоадресного IP-аудіосповіщення для територіально розподілених об'єктів. Дослідження підтвердило ключові переваги таких систем над аналоговими: децентралізацію, використання стандартного мережевого обладнання та гнучку маршрутизацію. Для забезпечення безперебійної трансляції з високою розбірливістю мови та мінімальними затримками обґрунтовано інтеграцію протоколу управління викликами SIP із транспортним стеком RTP/UDP. Визначено, що технологія IP Multicast (із залученням протоколів IGMP та PIM) є безальтернативною для оптимізації магістрального трафіку під час масових трансляцій.

ПРОДОВЖЕННЯ ВИСНОВКІВ

Саму ж мережу спроєктовано за архітектурною моделлю Hub-and-Spoke, що гарантує єдину точку контролю, ефективну логічну сегментацію та високий рівень безпеки. Практичну працездатність та логіку взаємодії пристроїв було успішно протестовано шляхом моделювання топології у середовищі Cisco Packet Tracer. Отримані результати підтверджують мережеву надійність запропонованих інженерних рішень та доцільність їх впровадження на реальних об'єктах для організації екстреного оповіщення.

РЕЗУЛЬТАТИ ВПРОВАДЖЕННЯ

1. Бученко І. А., Бровченко Т. Я. Дослідження Audio-over-IP та стандарта AES67. «Сучасні інтелектуальні інформаційні технології в науці та освіті» : IV науково-практ. конф., м. Київ, 15 трав. 2026 р. Подано до друку.

2. Бученко І. А., Бровченко Т. Я. Огляд сучасних протоколів синхронізації часу в Audio-over-IP: NTP та PTP. «Сучасні інтелектуальні інформаційні технології в науці та освіті» : IV науково-практ. конф., м. Київ, 15 трав. 2026 р. Подано до друку.