Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Засоби розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі»

Виконав: студент 2-го курсу, групи 2КІ-24м спеціальності 123 «Комп'ютерна інженерія»
_____Мельник Я. І.

Керівник: д.ф., доц. каф. ОТ
_____Обертюх М.Р.
«12» 12 2025 р.

Опонент: к.т.н., доц. каф. МБІС
_____ Грицак А.В.
«12» 12 2025 р.

Допущено до захисту
Завідувач кафедри ОТ
д.т.н., проф. Азаров О.Д.

«16» 12 2025 р.

Вінниця ВНТУ - 2025 рік

Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки
Освітньо—кваліфікаційний рівень магістр
Галузь знань — 12 Інформаційні технології
Спеціальність — 123 Комп'ютерна інженерія
Освітня програма — Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедри ОТ
д.т.н., проф. Азаров О.Д.
_____
"25" 09 2025 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ
Студенту Мельник Ярославу Івановичу

1 Тема роботи: «Засоби розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі», керівник роботи: Обертюх Максим Романович, д.ф., доц. каф. ОТ, затверджені наказом вищого навчального закладу від 24.09.2025 року №313.

2 Строк подання студентом роботи 4.12.2025р.

3 Вихідні дані до роботи: кількість вузлів з IPv4 – не менше 20од; кількість вузлів з IPv6 – не менше 20од; інтернет підключення – від 500 kb/s; мова програмування – об'єктно-орієнтована.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити): вступ, аналіз технологій розгортання інфраструктури IPv6 в існуючій корпоративній мережі, аналіз використання протоколів IPv4 і IPv6, аналіз засобів взаємодії мереж IPv4 і IPv6, тестування та аналіз результатів, економічнй розділ, висновки, перелік використаних джерел, додатки.

5 Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): схема алгоритму функціонування технології розгортання інфраструктури IPv6 в комп'ютерній коорпоративній мережі, схема мережі з інфраструктурою IPv6.

6 Консультанти розділів роботи наведені в таблиці 1

Таблиця 1 — Консультанти роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1-3	Обертюх М.Р., д.ф., доц. каф. ОТ		
4	Адлер О.О., к.т.н., доц. каф. ЕПВМ		
Нормоконтроль	Швець С.І., асист. каф. ОТ		

7 Дата видачі завдання 25.09.2025р.

8 Календарний план виконання МКР приведений в таблиці 2.

Таблиця 2 — Календарний план

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз технологій розгортання інфраструктури IPv6 в існуючій корпоративній мережі	01.10.2025	виконано
2	Аналіз використання протоколів IPv4 і IPv6	14.10.2025	виконано
3	Аналіз засобів взаємодії мереж IPv4 і IPv6	16.11.2025	виконано
4	Підготовка економічної частини	26.11.2025	виконано
5	Апробація результатів дослідження	01.12.2025	виконано
6	Оформлення матеріалів до захисту МКР	03.12.2025	виконано

Студент _____ Мельник Я.І.

Керівник роботи _____ Обертюх М.Р.

АНОТАЦІЯ

УДК 621.374.411

Мельник Я.І. Засоби розгортання інфраструктури IPv6 в комп’ютерній корпоративній мережі. Магістерська кваліфікаційна робота зі спеціальності 123 – Комп’ютерна інженерія, Вінниця: ВНТУ, 2025. 107с.

Укр. мовою. Бібліогр.: 26 назв; рис.: 12; табл. 14.

У магістерській кваліфікаційній роботі виконано аналіз засобів розгортання інфраструктури IPv6 в існуючу комп’ютерну корпоративну мережу.

В ході роботи проведено аналіз предметної області розгортання інфраструктури IPv6. Обґрунтовано вибір технологій, проведено проектування архітектури та розроблено її впровадження в корпоративну мережу компанії.

Ключові слова: протокол IPv6, протокол IPv4, корпоративна мережа, хмарні технології, платформа .Net.

ABSTRACT

Melnyk Y.I. Means of deployment of IPv6 infrastructure in a computer corporate network. Master's thesis on specialty 123 - Computer engineering, Vinnytsia: VNTU, 2025. 107p.

In Ukrainian speech Bibliography: 26 titles; Fig.: 12; table 14.

This master's thesis is devoted to the analysis of means of deployment of IPv6 infrastructure in the existing computer corporate network.

In the course of the work, an analysis of the subject area of IPv6 infrastructure deployment was carried out. The choice of technologies was substantiated, the architecture was designed and its introduction into the company's corporate network was developed.

Keywords: IPv6 protocol, IPv4 protocol, corporate network, cloud technologies, .Net platform.

ЗМІСТ

ВСТУП

Відомо, що протокол Інтернету версії 6 (IPv6) — це набір стандартних протоколів для мережного рівня Інтернету. IPv6 призначений для вирішення багатьох проблем поточної версії набору протоколів Інтернету (відомого як IPv4) про виснаження адрес, безпеки, автоматичної конфігурації, розширюваності тощо. д. IPv6 розширює можливості Інтернету для активації нових видів програм, включаючи програми для однорангової мережі та мобільних пристроїв.

В стандарті IPv6 довжина адреси складає 128 біт. Однією з причин такого великого адресного простору є можливість розділити доступні адреси на ієрархію доменів маршрутизації, що відображають топологію Інтернету. Інша причина полягає в тому, щоб сумістити адреси мережевих адаптерів (або інтерфейсів), які підключають пристрої до мережі. IPv6 має вбудовану можливість дозволяти адреси на їх найнижчому рівні, який знаходиться на рівні мережного інтерфейсу, а також дозволяє виконувати автоматичне налаштування.

Нещодавно організація Internet Society офіційно повідомила інформацію, що з початку всесвітнього запуску IPv6 (World IPv6 Launch) розгортання нової версії протоколу IP збільшилося на 3000%. Ці дані були опубліковані у звіті The State of IPv6 Deployment 2020р. А от в 2019 році компанія Google представила інформацію про те, що лише 1% користувачів отримують доступ до необхідних сервісів за допомогою нових IPv6. На сьогоднішній день ця цифра збільшилась до 20%. Що помітно показує прогрес нової технології, яка поступово входить у життя інтернет-спільноти. На даний момент IPv6 охоплює понад 9 млн. доменних імен та 23% мереж. The IPv4 Market Group заявили, що у 2019 році очікується перевищення кількості користувачів IPv6 понад 50%.

Причиною створення нового Інтернет-протоколу, такого як IPv6, головним чином є збільшення обсягу простору IP-адрес. IPv6 може створювати понад $3{,}4 \times 10^{38}$ унікальних адрес у порівнянні з IPv4, який створює $4{,}3 \times 10^{9}$ унікальних адрес (IPv6 має схему адреси 128 біт/16 байт, тоді як IPv4 має лише 32 біт/4 байти) [2]. Це означає, що IPv6 вирішує проблему, усуваючи вимогу щодо мережевої адреси. Він легко надає всім пристроям, таким як телефон, мобільний

телефон або автомобілі, власні IP-адреси, а також підтримує передачу медіа-контенту, безпеку та масштабованість. Це доводить, що IPv6 розроблено з урахуванням майбутніх додатків.

Отже, виходячи із розглянутого, задачі подальшого розроблення та вдосконалення засобів розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі на теперішній час **є актуальними**.

Метою дослідження магістерської кваліфікаційної роботи є вдосконалення засобів провадження протоколів стандарту IPv6 в існуючу комп'ютерну корпоративну мережу.

Для досягнення поставленої мети слід розв'язати такі завдання:

— проаналізувати існуючі рішення по розгортанню інфраструктури IPv6 в існуючій корпоративній мережі;

— розробити структуру корпоративної мережі компанії для впровадження стандарту IPv6;

— виконати моделювання запропонованої технології розгортання інфраструктури IPv6 в існуючій корпоративній мережі;

— провести тестування нової розробки та виконати аналіз отриманих результатів;

— здійснити економічні розрахунки доцільності впровадження нової розробки.

Об'єкт дослідження — процес розгортання інфраструктури IPv6 в існуючій корпоративній мережі.

Предмет дослідження — інформаційна технологія розгортання інфраструктури IPv6 в існуючій корпоративній мережі.

У роботі використані такі **методи** для наукових досліджень: методи та моделі подання знань, методи математичного моделювання, методи автоматизованого тестування програмних засобів, методи та техніки тест-дизайну, методи об'єктно-орієнтованого програмування.

Наукова новизна одержаних результатів полягає у тому, що удосконалено засоби розгортання інфраструктури IPv6 в комп'ютерну

корпоративну мережу, які відрізняються від існуючих використанням методу тунелювання за технологією 6to4, що дозволяє збільшити швидкість передачі даних в мережі, не погіршуючи при цьому безпеку передачі інформації в мережі.

Практичне значення одержаних результатів:

— створено алгоритм передачі інформаційних пакетів між сегментами інфраструктур IPv6 і IPv4 в корпоративній комп'ютерній мережі;

— розроблено програму обробки інформаційних пакетів між сегментами інфраструктур IPv6 і IPv4 в корпоративній комп'ютерній мережі.

Апробація результатів роботи здійснена шляхом підготовки тез на міжнародну науково-практичну інтернет-конференцію «Молодь в науці: дослідження, проблеми, перспективи (МН-2026)» (м. Вінниця, Україна, 2025 р.).

За результатами досліджень **опубліковано** тези доповіді на науково-практичній конференції [1].

1 АНАЛІЗ ЗАСОБІВ РОЗГОРТАННЯ ІНФРАСТРУКТУРИ IPV6 В ІСНУЮЧІЙ КОРПОРАТИВНІЙ МЕРЕЖІ

1.1 Особливості розгортання програмної інфраструктури

За оцінками компанії IBM біля 70% IT-бюджету витрачається на підтримку існуючої інфраструктури і тільки 30% на її розширення. І чим далі, тим гостріше бізнес потребує раціоналізації використання IT-ресурсів і автоматизації їх управління. Отож, будь-яка автоматизації в області IT, а особливо процесів розробки ПЗ є явищем необхідним.

IT-інфраструктура — це сукупність сервісів та різного роду систем компанії, осередків програмного забезпечення підприємства, обчислювальних програм, які забезпечують все необхідне задля вирішення бізнес-завдань підприємства.

Іншими словами IT-інфрастурктура включає в себе пристрої з виходом в Інтернет, бази даних, програмне забезпечення, корпоративну пошту і багато іншого. Всі ці елементи об’єднуються через інтернет і працюють у зв’язці, що дозволяє ефективно виконувати різні завдання і створити бізнес-середовище для скоординованої роботи всієї компанії і кожного її підрозділу. Коректна робота IT-інфраструктури забезпечує зв’язок між відділами або департаментами, які можуть бути фізично віддалені один від одного, передачу і отримання файлів та інформації, а також правильну роботу всіх сервісів компанії [1].

Грамотно спроектована і побудована IT-інфраструктура створює для бізнесу ряд переваг, серед яких: підвищення прибутковості, оптимізація витрат, поліпшення продуктивності і результативності бізнес-процесів і технологічних процесів.

Попри грамотне проектування внутрішньої взаємодії бізнес елементів, інфраструктура передбачає врахування зовнішніх чинників, чи факторів які можуть вплинути на кінцевий результат роботи та буде, чи не основною, характеристикою що впливатиме на безпосередню відказостійкість основних процесів.

Погано розпланована інфраструктура може містити велику кількість обмежень, які в свою чергу створюватимуть залежності, яким повинні будуть відповідати усі як існуючі, так і майбутні процеси компанії. В гіршому випадку, можливість появи небажанних результатів, некорректного функціювання та взаємодія певних частин інфраструктури, можливо навіть повна відмова працездатності, буде тільки збільшуватись.

На данний момент, існує ряд рішень які можуть бути використаними з цілью розміщення інфраструктури. Наприклад:

— традиційні (On-Premise) фізичні сервери;
— colocation;
— hosting;
— IAAS (infrastructure as a service);
— PAAS (platform as a service);
— SAAS (software as a service).

Серед вище перелічених варіантів, розміщення інфраструктури, можливо виділити рішення що досі є актуальними але мають тенденцію відступати на другорядний план, за наявності більш простіших в опануванні та підтримці рішень, які постійно розвиваються за підтримки певної общини.

Цими варіантами є: традиційне розміщення інфраструктури на фізичних серверах, colocation та hosting. Кожний з цих варіантів передбачає необхідність висококваліфікованого спеціаліста, навички якого, будуть вирішувати подільшу працездатність проекту. Причиною вибору одного з вищеописаних варіантів розміщення інфраструктури, може виступати лише певна специфіка проекту, яка створює неординарні вимоги до платформи, при чому, ці вимоги можуть бути задовільненими лише при виборі конкретної платформи.

Вибір платформи для розміщення інфраструктури повинний бути доцільним. Саме тому, в будь-якому іншому випадку ліпшим рішенням буде обрати більш простішу платформу, наприклад IAAS, PAAS, SAAS, цим самим не створюючи перед собою додаткових вимог, яких потрібно буде дотримуватись для підтримки життєвого циклу продукту, та подальшої розробки.

Згідно статистики, що була зібрана ресурсом Statista, щорічно спостерігається тенденція до зросту кількості компаній, які розміщують інфраструктуру на певній платформі хмарних обчислень. На початок 2021 року 67% компаній використовують хмарні платформи, що добре спостерігається на фоні обігу коштів, які було витрачено лише на ресурси хмарних обчислень [2]. Ця тенденція продовжує свій зріст та з кожним роком все більша кількість компаній відмовляється від розміщення інфраструктури в певному датацентрі, при цьому надаючи перевагу хмарним обчисленням.

1.2 Аналіз існуючих можливостей протоколів TCP/IP

Протокол мережевої взаємодії TCP/IPv4 використовується для передачі зашифрованих даних у мережі інтернет і локальних підмережах вже понад тридцять років. На його підставі створюється та підтримується унікальна адресація мережного обладнання (вузлів). Ще на початку 90-х років минулого століття було визначено основний недолік даного протоколу – обмеження за кількістю можливих ip-адрес, яка не може перевищити 4,23 мільярда. У результаті було розроблено нову систему протоколювання мережевої взаємодії — інтернет-протокол IPv6 (Internet Protocol version 6). Проте масовий перехід на більш прогресивну технологію обумовлений деякими труднощами. Хоча, наприклад, у Сполучених Штатах вже більше половини користувачів застосовують саме протокол IPv6.

Як відомо, ключовим недоліком протоколу четвертої версії TCP/IPv4 є обмежена масштабованість унікальних адрес, що присвоюються для ідентифікації в мережах взаємодії. Для створення ip-адрес на рівні програмних записів використовується 32-бітна система у форматі 0.0.0.0 — 255.255.255.255. При побудові локальних підмереж вводиться додатковий атрибут "маска підмережі", що записується після символу "/". У результаті навіть великі ЛОМ, об'єднані в Ethernet, найчастіше мають одну публічну ip-адресу, що видається провайдером і закріплена на рівні шлюзу (маршрутизатора). Самостійний обмін даними на рівні окремих пристроїв приватної підмережі з виходом у паблік-інтернет потребує

складного адміністрування. Для вирішення завдань маршрутизації, які вимагають отримання статичних IP-адрес, знадобляться додаткові фінансові витрати.

В інтернет-протоколі нового покоління IPv6 для створення адресної маршрутизації використовується 128-бітна система запису. В IPv6-адресі записами є вісім 16-бітних блоків, розділених двокрапками: 2dfc:0:0:0:0217:cbff:fe8c:0. Загальна кількість ip-адрес, можливих для розподілу, може становити загалом 2128 (приблизно 340 282 366 920 938 000 000 000 000 000 000 000 000). Загальне використання даного стандарту дозволить повністю вирішити проблему нестачі мережевих адрес в найближчому майбутньому (рис. 1.1).

About IPv4 and IPv6

IP version	IPv4	IPv6
Deployed	1981	1999
Address Size	32-bit number	128-bit number
Address Format	Dotted Decimal Notation: 192.0.2.76	Hexadecimal Notation: 2001:0DB8:0234:AB00: 0123:4567:8901:ABCD
Number of Addresses	2^{32} = 4,294,967,296	2^{128} = 340,282,366,920,938,463, 463,374,607,431,768,211,456
Examples of Prefix Notation	192.0.2.0/24 10/8 (a "/8" block = 1/256th of total IPv4 address space = 2^{24} = 16,777,216 addresses)	2001:0DB8:0234::/48 2600:0000::/12

Рисунок 1.1 — Відмінності між протоколами IP 4 та 6 версії

Для спрощення запису адреси в протоколі IPv6 використовується варіант стиснення коду, коли суміжні послідовності нульових блоків замінюються парами символів двокрапки. Наприклад, адреса групової розсилки FFEA:0:0:0:0:CA28:1012:4254 у стислій формі буде представлена у скороченому вигляді FFEA::CA28:1012:4254. Цей механізм спрощує процес запису, зберігання та обробки коду.

За правилами протоколу IPv6 призначення мережевих адрес відбувається автоматично і унікалізується за рахунок ідентифікації на рівні MAC-адреси конкретної одиниці обладнання, для якої необхідний вихід в публічну мережу. Іншими словами, кожен домашній комп'ютер, смартфон, холодильник або пральна машина з функцією підключення до зовнішніх пристроїв отримує власну «білу» IP-адресу для коннекту з іншими хостами через інтернет. Доступна також довільна генерація кодів адміністрування з використанням маршрутизаторів.

Вражає мінімальний діапазон адрес підмережі, які користувач отримує при підключенні за протоколом IPv6. Наприклад, під час використання маски підмережі «/128» отримуємо понад 256 адрес.

Спірним є питання відмінності швидкості передачі трафіку по кожному з протоколів. За замовчуванням технологія IPv6 забезпечує велику швидкість обробки трафіку на рівні окремого обладнання мережі в цілому. Використання NAT у протоколі IPv4, який забезпечує трансляцію адрес абонентів та зберігання в пам'яті інформації про встановлені з'єднання, призводить до великого завантаження обладнання. Тому в моменти пікового навантаження кожен користувач відзначає різке зниження швидкості з'єднання.

У протоколі IPv6 не застосовується обов'язкова обробка пакетів та відстеження вже відкритих з'єднань під час маршрутизації доступу до хостів. Відсутність трансляції значно знижує ресурсне навантаження на мережні пристрої. Для користувача це означає вирівнювання швидкості інтернет-з'єднання. Провайдери в такій ситуації можуть використовувати менш ресурсомістке, а отже, дешевше обладнання (рис. 1.2).

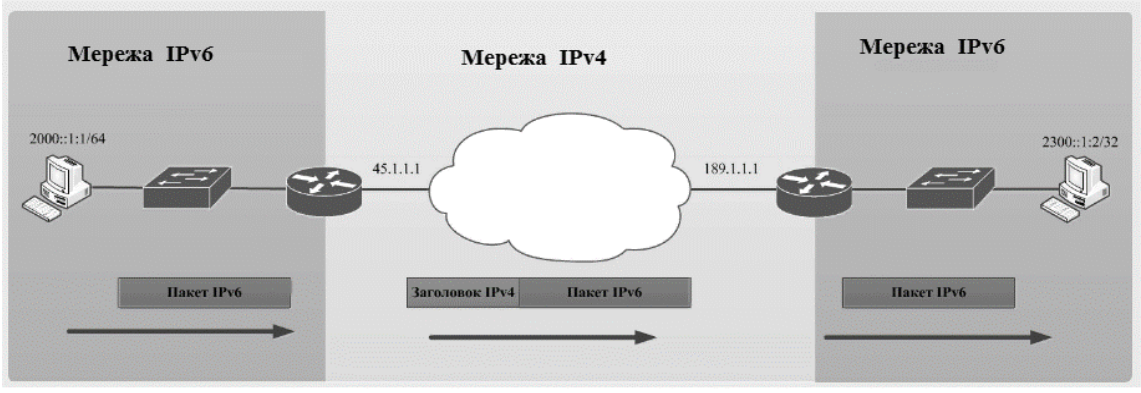

Рисунок 1.2 — Навантаження на обладнання мережі з протоколами IP 4 та 6 версії

Порівняно з четвертою версією, у протоколі TCP/IPv6 реалізовано низку додаткових функціональних можливостей:

— використовується більш простий заголовок, з нього виключені несуттєві параметри, що знижує навантаження маршрутизатори при обробці мережевих запитів;

— більш високий рівень забезпечення безпеки, автентифікації та конфіденційності, які є основою даної технології;

— у протоколі реалізовано функцію Quality of Service (QoS), що дозволяє визначати чутливі до затримки пакети;

— під час передачі широкомовних пакетів використовуються багатоадресні групи;

— для реалізації технології мультимовлення IPv6 задіяно вбудований адресний простір FF00::/8;

— для підвищення безпеки використовується підтримка стандарту шифрування IPsec, який дозволяє шифрувати дані без необхідності підтримки прикладного ПЗ.

Наразі експерти ведуть дискусії щодо забезпечення безпеки даних у разі гібридного застосування двох протоколів. Провайдери вибудовують IPv6-тунелі для надання користувачам IPv4 доступу до високорівневого контенту. Застосування цієї технології збільшує ризики атак хакерів. Функція автоконфігурації, коли пристрої самостійно генерують IP-адресу на основі MAC-адреси обладнання, може бути використана для незаконного відстеження конфіденційних даних користувачів.

1.3 Особливості впровадження протоколу TCP/IPv6

Незважаючи на довгу історію розробки, яка бере початок у 1992 році, тестування нового протоколу відбулося 8 червня 2011 року у Міжнародний день IPv6.

Першою компанією, що впровадила в 2008 році стандарт протоколу IPv6 на постійній основі, стала GOOGLE. Тестування протягом чотирьох років, було визнано успішним. 6 червня 2012 року відбувся Всесвітній запуск IPv6. Сьогодні світові лідери у виробництві мережевого обладнання Cisco та D-Link застосовують

цей мережевий стандарт у своїх маршрутизаторах на базовому рівні.

У мобільних мережах стандарту LTE підтримка протоколу IPv6 є обов'язковою. IT-компанії Google, Facebook, Microsoft та Yahoo використовують IPv6 на своїх основних web-ресурсах (рис. 1.3). Протокол набуває все більшого поширення в корпоративних мережах та при домашньому використанні.

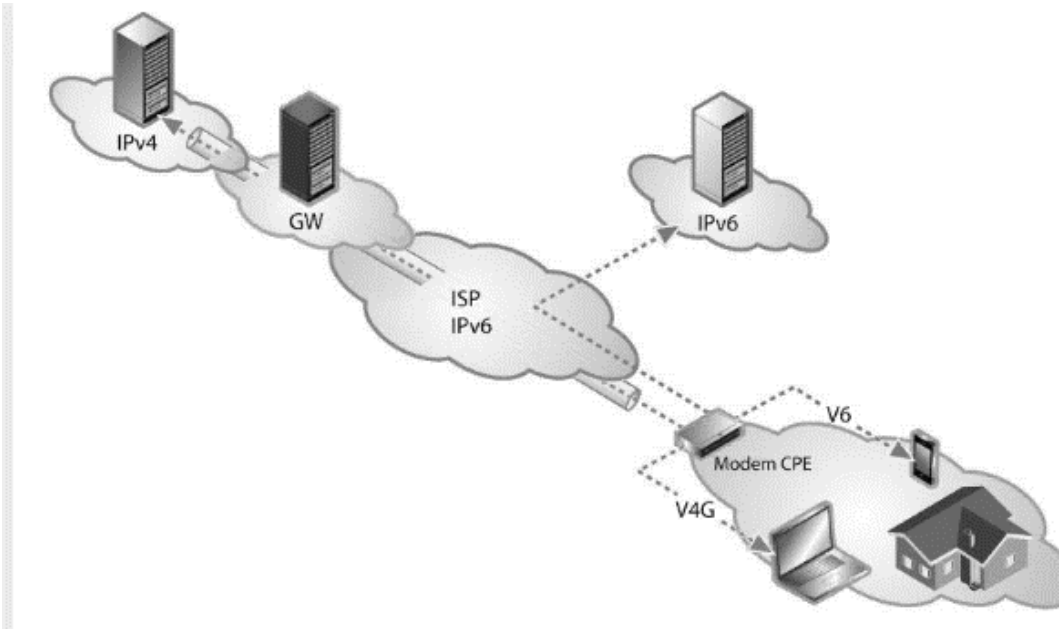

Рисунок 1.3 — Використання протоколів IP 4 та 6 версії

Згідно з дослідженнями Google, на початок 2023 року частка IPv6 у загальносвітовому мережевому трафіку становила близько 30%. В Україні цей показник значно нижчий, він становить приблизно 4,5% всього трафіку. У той же час дедалі більше вітчизняних реєстраторів доменів і хостинг-провайдерів переводять свої DNS-сервери на протокол IPv6.

Виникає резонне питання: якщо протокол TCP/IPv6 має таку кількість переваг у порівнянні з попередником, чому б просто не перейти на нього всім

світом? Основна перешкода лежить у сфері фінансів та тимчасових параметрів. Для повномасштабного використання нової технології потрібні серйозні інвестиції у програмно-технічну модернізацію комп'ютерного парку всіх провайдерів.

Використання динамічних IP-адрес за протоколом IPv4 дозволяє тимчасово стримувати проблему нестачі унікальних мережевих ідентифікаторів. Іншими словами, проблеми адміністрування локальних мереж перекладаються на кінцевих користувачів, які змушені налаштовувати складні схеми маршрутизації підмереж та купувати додаткові IP-адреси. У той же час зростання кількості кінцевих мережевих пристроїв відбувається дуже швидко. Впровадження технологій прямої комунікації навіть із звичайними побутовими приладами через інтернет потребує нових підходів у побудові архітектури їхньої взаємодії. У зв'язку з цим повсюдний перехід використання стека протоколу TCP/IPv6 неминучий.

1.4 Аналіз можливостей налаштування інфрастуктури IPv6

Гнучкий механізм маршрутизації є перевагою IPv6. Через те, як було виділено ідентифікатори мережі IPv4, великі таблиці маршрутизації повинні підтримуватися маршрутизаторами, які знаходяться в магістралі Інтернету. Ці маршрутизатори повинні знати всі маршрути для пересилання пакетів, які потенційно спрямовані будь-який вузол в Інтернеті. Завдяки можливості об'єднання адрес IPv6 забезпечує гнучку адресацію і істотно скорочує розмір таблиць маршрутизації. У цій новій архітектурі адресації проміжні маршрутизатори повинні відстежувати локальну частину мережі, щоб перенаправити повідомлення відповідним чином.

Опишемо функції, які надаються виявленням сусідів:

— виявлення маршрутизатора дозволяє вузлам визначати локальні маршрутизатори;

— дозвіл адрес дозволяє вузлам дозволяти адресу рівня посилань для відповідної адреси наступного стрибка (заміна протоколу дозволу адрес [ARP]);

— автоматичне налаштування адреси дозволяє сайтам автоматично налаштовувати локальні та глобальні адреси сайту.

Виявлення сусідів використовує протокол повідомлень керування Інтернетом для повідомлень IPv6 (ICMPv6), які включають:

— оголошення маршрутизатора, тобто надсилання маршрутизатором на псевдо-періодичній основі або у відповідь на запит маршрутизатора. Маршрутизатори IPv6 використовують оголошення маршрутизаторів для повідомлення про доступність, для вказівки префіксів адрес та інших параметрів;

— запит маршрутизатора надсилається вузлом, щоб запитати, що маршрутизатори за посиланням негайно надсилають оголошення маршрутизатора;

— запит сусіда надсилається вузлами для дозволу адрес, виявлення повторюваних адрес або перевірки того, що сусід, як і раніше, доступний;

— оголошення сусіда надсилається вузлами, щоб відповідати на запит сусідів або повідомляти сусідів про зміну адреси шару посилань;

— перенаправлення надсилається маршрутизаторами, щоб вказати найкращу адресу наступного стрибка у певне місце призначення для вузла відправки.

Одна з найважливіших цілей IPv6 полягає в підтримці вузла, що самоналаштовується. Тобто можна підключити вузол до мережі IPv6 і автоматично налаштувати його без втручання людини.

Протокол IPv6 підтримує різні типи автоматичного налаштування.

Автоматичне налаштування з відстеженням стану , для цього типу налаштування необхідний певний рівень втручання людини, оскільки для встановлення та адміністрування вузлів потрібний DHCPv6-сервер. Сервер DHCPv6 зберігає список вузлів, для яких він надає інформацію про конфігурацію. Він також зберігає інформацію про стан, тому серверу відома тривалість використання кожної адреси та її доступність для перепризначення;

Автоматичне налаштування без відстеження стану — таке налаштування підходить для невеликих організацій та приватних осіб. У цьому випадку кожен

вузол визначає свої адреси на основі вмісту отриманих об'яв маршрутизатора. Використовуючи стандарт IEEE EUI-64 визначення частини мережного ідентифікатора в адресі, розумно припустити унікальність адреси вузла в каналі.

Незалежно від способу визначення адреси вузол повинен перевірити, що його потенційна адреса є унікальною для локального каналу. Для цього на потенційну адресу надсилається запит пошуку сусідів. Якщо вузол отримує відповідь, він знає, що адреса вже використовується, і йому слід визначити іншу адресу.

У зв'язку з розповсюдженням мобільних пристроїв з'явилася нова вимога - пристрій повинен мати можливість довільним чином змінювати розташування на базі IPv6 протоколу і при цьому зберігати наявні підключення. Для підтримки цієї функції мобільному вузлу надається домашня адреса, за якою його завжди можна знайти. Якщо мобільний вузол знаходиться вдома, він підключається до домашнього каналу та використовує свою домашню адресу. Коли мобільний вузол далеко від дому, домашній агент, який зазвичай є маршрутизатором, передає повідомлення між мобільним вузлом та вузлами, з якими він взаємодіє.

Щоб використовувати протокол IPv6, треба переконатися, що він підтримується наявною версією операційної системи, а також, що операційна система та мережні класи налаштовані належним чином.

1.5 Аналіз переваг та недоліків використання інфрастуктури IPv6

Інтернет став невід'ємною частиною нашого життя, а IP-адресація – це основа, яка робить все це можливим. Однак із зростанням числа пристроїв, підключених до Інтернету, виникає потреба у більшій кількості IP-адрес. Саме тут на допомогу приходить протокол IPv6.

Технологія протоколу IPv6 пропонує значно більш надійний і функціонально розширений набір характеристик порівняно з протоколом IPv4, насамперед завдяки суттєвому збільшенню адресного простору. Використання 128-бітних IP-адрес дозволяє практично усунути проблему дефіциту глобальних адрес, що є критично важливим в умовах стрімкого зростання кількості

мережевих пристроїв, зокрема мобільних систем, сенсорних мереж та рішень Інтернету речей (IoT). Окрім цього, IPv6 забезпечує більш ефективну ієрархічну адресацію, що позитивно впливає на маршрутизацію та масштабованість мереж.

Впровадження IPv6 також сприяє спрощенню адміністрування мережевої інфраструктури за рахунок автоматичної конфігурації вузлів, зменшення залежності від технологій трансляції мережевих адрес (NAT) та покращеної підтримки мобільності. Протокол передбачає вбудовані механізми безпеки, зокрема обов'язкову підтримку IPsec, що підвищує рівень захищеності передаваних даних. Крім того, IPv6 має розширені можливості щодо забезпечення якості обслуговування (Quality of Service, QoS), що дозволяє ефективніше керувати мережевим трафіком і забезпечувати стабільну роботу сервісів, чутливих до затримок і втрат пакетів.

Важливою перевагою IPv6 є наявність механізмів сумісної роботи з IPv4, зокрема технологій трансляції та тунелювання IPv4–IPv6. Реалізація таких механізмів дозволяє поступово впроваджувати IPv6 без необхідності дорогої та тривалої повної заміни існуючої інфраструктури, що вже функціонує на базі IPv4. Метою розробки та застосування цих технологій є забезпечення плавного переходу між протоколами з мінімальними витратами та ризиками для замовників.

Завдяки цьому організації отримують можливість підключати до наявної IPv4-інфраструктури пристрої та системи, які підтримують виключно протокол IPv6, а також забезпечувати взаємодію між різними поколіннями мережевих технологій. У результаті впровадження IPv6 компанії та провайдери здатні обслуговувати нове покоління клієнтських систем, підвищувати гнучкість мережі та створювати основу для подальшого розвитку сучасних і перспективних мережевих сервісів.

Переваги використання інфрастуктури IPv6 : велика кількість унікальних адрес, підтримка сучасних технологій, підвищений рівень безпеки, підвищена продуктивність.

Однією з ключових переваг IPv6 є величезна кількість унікальних IP-адрес, що вирішує проблему нестачі адрес IPv4. Це особливо важливо для проектів, які вимагають великої кількості унікальних ідентифікаторів;

Протокол IPv6 розроблений з урахуванням останніх тенденцій, таких як Internet of Things (IoT), де велика кількість пристроїв вимагає унікальних IP-адрес. Використання IPv6 проксі забезпечує сумісність із сучасними технологіями;

IPv6 надають додаткові механізми безпеки, такі як вбудована підтримка IPsec. Це підвищує рівень захисту даних, що передаються, що важливо для проектів, де безпека відіграє вирішальну роль;

IPv6 має більш ефективну структуру заголовків і механізми маршрутизації, що може підвищити продуктивність у порівнянні з IPv4. Це актуально для проектів, де висока продуктивність є ключовою вимогою.

Недоліки використання інфрастуктури IPv6: необхідність оновлення обладнання, проблеми сумісності, складнощі в налаштуванні сервісів, обмежена підтримка з боку провайдерів.

Для повноцінної підтримки IPv6 часто потрібне оновлення мережного обладнання. Це може стати додатковим фінансовим навантаженням для компаній, особливо для тих, у кого вже налагоджено роботу на IPv4;

Деякі старі пристрої та програми можуть не підтримувати IPv6, що створює проблеми з впровадженням нового протоколу. Це важливо враховувати при переході на проксі IPv6;

Впровадження та налаштування IPv6 може вимагати додаткових зусиль та кваліфікації, особливо у технічних фахівців, які не мають досвіду роботи з цим протоколом;

Деякі інтернет-провайдери можуть надавати обмежену підтримку IPv6, що може ускладнити роботу проекту, який повністю перейшов на новий протокол.

IPv4 та IPv6 — це інтернет-протоколи, що забезпечують зв'язок між пристроями в Інтернеті. Хоча протокол IPv4 є найпоширенішим, протокол IPv6 має ряд переваг, таких як ширший адресний простір, покращені засоби безпеки та ефективніша обробка пакетів.

2 АНАЛІЗ ВИКОРИСТАННЯ ПРОТОКОЛІВ IPV6 та IPV4

2.1 Характеристика протоколу IPv4

Протокол розроблено для використання в комп’ютерних мережах з комутацією пакетів. Цей протокол забезпечує передавання блоків даних від джерел до отримувачів. Джерела та отримувачі — це вузли, які ідентифікуються адресами фіксованої довжини.

Дві основні функції протоколу IPv4: адресація та фрагментація. Щоб забезпечити доставку датаграм до пункту призначення, використовуються адреси, які містяться в заголовках IP-датаграм. Відповідні поля заголовків дозволяють реалізувати механізм фрагментації та повторного збирання датаграм. Фрагментація і повторне збирання потрібні, коли потрібно передавати датаграми через мережі, що підтримують невеликий розмір пакета. У протоколі IPv4 немає функцій, які б гарантували надійну наскрізну доставку даних, керування потоком чи впорядкування пакетів.

Internet Protocol використовує чотири ключові механізми:

— Type of Service (Тип сервісу);

— Time to Live (Час життя);

— Options (Опції);

— Header Checksum (Контрольна сума заголовка).

Тип сервісу (Type of Service) потрібен для того, щоб вказати якість сервісу. Він використовується маршрутизаторами для вибору фактичних параметрів передавання через певні мережі.

Час життя (Time to Live) визначає максимальний строк існування датаграми. Він установлюється відправником і зменшується в кожній точці, через яку проходить датаграма на шляху від відправника до отримувача. Якщо час життя датаграми зменшується до нуля до того, як вона досягне отримувача, — датаграма знищується.

Опції (Options) передбачають функції керування, які потрібні лише в окремих ситуаціях, але не використовуються під час більшості звичайних з’єднань.

Контрольна сума заголовка (Header Checksum) дозволяє переконатися, що датаграма була передана правильно. Якщо контрольна сума заголовка не відповідає перевірюваним даним, така датаграма відкидається пристроєм, який виявив помилку.

Протокол IPv4 не гарантує доставку, у нього немає підтверджень "кінець у кінець", контроль здійснюється лише для заголовка. Про виявлені помилки повідомляє протокол ICMP (Internet Control Message Protocol), який реалізований у модулі IP.

Кожен вузол має логічну IP-адресу, яка належить мережевому рівню й не залежить від адреси канального рівня. IP-адресу можна призначити вручну або автоматично за допомогою протоколу DHCP.

Адреса складається з ідентифікатора мережі та ідентифікатора вузла. Усі системи в одній фізичній мережі мають однаковий ідентифікатор мережі, унікальний у межах усієї мережі. Ідентифікатор вузла повинен бути унікальним у межах своєї мережі.

IP-адреса має довжину 32 біти, розділені на чотири октети (по 8 біт). Кожен октет зазвичай подається у десятковому форматі, тому адреса записується як чотири числа від 0 до 255, розділені крапками (табл. 2.1).

Таблиця 2.1 — Приклад IP-адреси в двійковому та десятковому вигляді

Двійковий вигляд	Десятковий вигляд
11000000.10101000.00000001.00000011	192.168.1.3

Існує три основні класи мереж, і залежно від класу мережі для ідентифікації самої мережі та вузла відводиться різна кількість бітів. Клас мережі можна визначити за початковими бітами в адресі (табл. 2.2).

Для мереж класу A значення першого октету лежить у діапазоні від 1 до 126. Номери мереж 0 і 127 зарезервовані.

Адреси мереж у діапазоні 128–191 належать до мереж класу B, а адреси в діапазоні 192–223 – до мереж класу C.

Таблиця 2.2 — Формати адреси

Старші біти	Формат	Клас
0	7 бітів для номера мережі, 24 біта для номера вузла	A
10	14 бітів для номера мережі, 16 біта для номера вузла	B
110	21 біт для номера мережі, 8 біт для номера вузла	C
111	для розширеної адресації	

Існують такі типи адрес IPv4:

— індивідуальна (unicast) адреса (призначається одному інтерфейсу підмережі певної мережі, використовується в з'єднаннях типу «точка — точка»);

— групова (multicast) адреса (може бути призначена одному або кільком інтерфейсам у різних підмережах однієї мережі, використовується в з'єднаннях типу «точка — багато точок»);

— широкомовна (broadcast) адреса (призначається всім інтерфейсам підмережі даної мережі, використовується в з'єднаннях типу «точка — всі точки підмережі»).

Але існують і зарезервовані IP-адреси:

— адреса мережі, у якій всі біти, що відповідають номеру вузла в адресі мережі, заповнюються нулями (наприклад, адреса мережі класу A: «32.0.0.0» («00100000 00000000 00000000 00000000»);

— спрямована широкомовна адреса (Directed Broadcast), яка використовується для передавання даних на всі пристрої певної мережі, у ній усі біти, що відповідають номеру хоста, заповнюються одиницями (наприклад, спрямована широкомовна адреса мережі класу C: «195.55.43.255» («11000011 00110111 00101011 11111111»);

— локальна широкомовна адреса (Local Broadcast), яка використовується для передавання даних на всі пристрої локальної мережі, усі біти адреси призначення пакета встановлюються в одиниці (наприклад, «255.255.255.255»).

Особливе значення має IP-адреса, перший октет якої дорівнює 127. Ця адреса використовується для тестування програм і взаємодії процесів всередині

одного локального комп’ютера.

Коли, як адреса отримувача, використовується IP=127.0.0.1, то утворюється так звана «петля зворотного зв’язку» (loopback).

Дані, надіслані на цю адресу, не передаються мережею, а повертаються до модулів верхнього рівня, ніби вони щойно були отримані.

Таким чином, інформація потрапляє на той самий вузол, з якого була відправлена.

У IP-мережах заборонено присвоювати комп’ютерам адреси, перший октет яких дорівнює «127».

У протоколі IP немає поняття широкомовності в тому сенсі, як воно використовується на канальному рівні локальних мереж, де дані передаються абсолютно всім вузлам. У IP протоколі дані передаються або всім вузлам тієї ж мережі, що й відправник, або всім вузлам тієї мережі, адреса якої вказана як адреса призначення.

Основна мета використання групових адрес — це передавання інформації від одного хоста до багатьох, які можуть знаходитися в різних мережах. Коли один хост хоче передати дані багатьом одержувачам, він за допомогою спеціального протоколу IGMP (Internet Group Management Protocol) повідомляє про створення нової мультикаст-групи з певною адресою.

Маршрутизатори, що підтримують мультикаст, інформують мережі, підключені до їхніх портів, про цю нову групу. Хости, які бажають приєднатися до групи, повідомляють про це свої локальні маршрутизатори. Маршрутизатори, у свою чергу, передають цю інформацію хосту, який ініціював створення групи.

Групові адреси обробляються особливим чином — вони не мають поділу на поля номера мережі та номера вузла.

Структура заголовку IP-пакету представлена на рисунку 2.1.

Проалагізуємо функціональне призначення полів заголовка.

Поле Версія (Version) вказує номер версії даного протоколу міжмережевого рівня. Наразі, поряд із 4-ю версією протоколу (тобто у полі — 0100), починається використання протоколу 6-ї версії (тобто у полі — 0110).

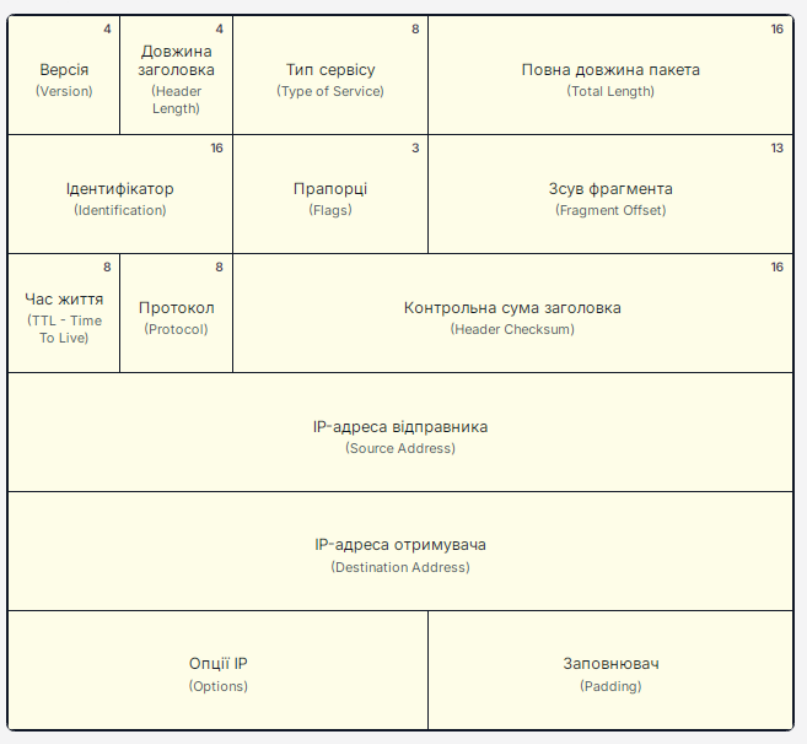

Рисунок 2.1 — Структура заголовоку IP-пакету

Поле Довжина заголовку (Header Length) вказує довжину заголовка міжмережевої датаграми у 32-розрядних словах. Мінімальна довжина — п’ять слів, максимальна — п’ятнадцять 32-розрядних слів (на рисунку заголовок має шість слів).

Поле Тип сервісу (Type of Service) вказує параметри потрібної якості обслуговування. Довжина цього поля становить 8 бітів. Воно визначає набір критеріїв, за допомогою яких задається тип обслуговування IP-пакетів.

Нижче наведено опис окремих бітів:

— біти 0...2 — пріоритет (precedence) даного IP-сегмента;

— біт 3 — вимога до часу затримки (delay) передавання IP-сегмента (0 — нормальна, 1 — низька затримка);

— біт 4 — вимога до пропускної здатності (throughput) маршруту, яким має передаватися IP-пакет (0 — низька, 1 — висока пропускна здатність);

— біт 5 — вимога до надійності (reliability) передавання IP-пакета (0 — нормальна, 1 — висока надійність);

— біти 6...7 – зарезервовані.

Поле Повна довжина пакета (Total Length) визначає загальну довжину датаграми в октетах (байтах), включаючи заголовок і корисне навантаження. Повна довжина пакета може досягати 65535 байт. Рекомендується використовувати датаграму довжиною 576 байт (тобто 4608 біт) — 552 байти даних + 24 байти заголовка.

Поле Загальний ідентифікатор (Identification) призначене для збирання фрагментів міжмережевих датаграм.

Поле Прапорець (Flag) забезпечує можливість фрагментації датаграм і, у разі використання фрагментації, дозволяє ідентифікувати останній фрагмент датаграми.

Поле Зміщення фрагмента (Fragment Offset) вказує місце даного фрагмента в міжмережевій датаграмі. Перший фрагмент має зміщення, що дорівнює нулю.

Щоб усунути з мережі пакети, затримані з будь-яких причин, у заголовку в полі Час життя (TTL — Time To Live) вказується час, протягом якого пакет має існувати в мережі. Значення цього часу зменшується під час проходження пакета через мережу, а після його закінчення пакет знищується з повідомленням відправника відповідним ICMP-повідомленням. Такий механізм захищає мережу від циклічних маршрутів і перевантажень.

Поле Тип протоколу (Protocol) ідентифікує протокол верхнього рівня, який буде використано під час обробки поля даних міжмережевої датаграми (табл. 2.3).

Поле Контрольна сума заголовка (Header Checksum) використовується, щоб зменшити ймовірність спотворення адресної частини пакета і, як наслідок, його відправлення не за призначенням (та втрати), заголовок пакета супроводжується перевірочною послідовністю — контрольною сумою, яка займає 2 байти й обчислюється для всього заголовка. Для обчислення контрольної суми IP-заголовка у вихідній датаграмі значення цього поля спочатку встановлюється в 0. Потім виконується додавання (з циклічним переносом зі старшого розряду в молодший) усіх 16-розрядних слів заголовка, після чого інверсія отриманого результату записується в поле контрольної суми.

Таблиця 2.3 — Типи протоколу

Ідентифікатор	Скорочена назва	Ім’я протоколу
1	ICMP	Міжмережевий протокол керуючих повідомлень
2	IGMP	Міжмережевий протокол групового управління
3	GGP	Протокол «шлюз-шлюз»
6	TCP	Протокол управління передачею
8	EGP	Протокол «зовнішніх» шлюзів
17	UDP	Протокол датаграм користувача
27	RDP	Протокол надійних даних
28	IRTP	Протокол міжмережевої надійної передачі
29	ISO TP4	Транспортний протокол класу ISO 4
80	ISO IP	Міжмережевий протокол ISO
89	OSPF	Протокол «найкоротший шлях першим»

Під час отримання IP-датаграми знову обчислюється сума 16-розрядних слів заголовка. Оскільки в заголовку прийнятої датаграми вже міститься обчислена (та інвертована) відправником контрольна сума, у результаті повинно утворитися слово, що складається лише з одиниць (якщо заголовок не був змінений). Якщо ж отримується інша комбінація (помилка контрольної суми), IP-модуль знищує датаграму.

Жодне повідомлення про помилку не генерується. Виявлення втрати датаграми та її повторна передача вважаються завданнями, що вирішуються на вищих рівнях ієрархії протоколів. Оскільки деякі поля заголовка змінюються під час руху пакета (наприклад, час життя), перевірочні розряди перераховуються в кожній точці обробки міжмережевої датаграми.

IP-адреса відправника (Source Address) і IP-адреса отримувача (Destination Address) є 32-бітними ідентифікаторами об’єктів мережі — кінцевих пристроїв і маршрутизаторів.

Поле Додаткові параметри IP (опції IP) (Options) визначає наявність додаткових сервісів, має змінну довжину і може бути присутнім або відсутнім у міжмережевій датаграмі. За потреби в заголовок можуть включатися деякі додаткові дані.

Поле Заданий маршрут — це список IP-адрес вузлів мережі, через які повинен пройти IP-пакет. Заданий маршрут може бути «м’яким» або «строгим». У першому випадку сегмент не зобов’язаний суворо дотримуватися зазначеного маршруту — можуть бути проміжні вузли, яких немає у списку. У другому випадку сегмент проходить строго через ті вузли, які вказані у списку.

Поле Пройдений маршрут – це список вузлів, які відвідав пакет на шляху до адресата. Кожен транзитний вузол, через який проходить пакет, заносить до цього списку свою адресу.

Поле Часові мітки — це список моментів часу, коли пакет проходив через вузли маршруту до адресата.

Поле Секретність — це вказівка на обробку IP-пакета відповідно до вимог безпеки (RFC 1038).

Поле Прапорець завершення вказує на закінчення додаткових даних заголовка.

Кожен елемент додаткових даних може бути:

— або однобайтовим ідентифікатором додаткових даних (наприклад, «Прапорець завершення»);

— або комбінацією однобайтового ідентифікатора, поля довжини та самих даних (наприклад, «заданий маршрут»).

Для додаткових даних, які можуть доповнюватися під час проходження IP-пакета мережею, відправник має залишити в заголовку вільне місце. Такий підхід спрощує обробку IP-пакета на вузлах.

Поле Заповнювач (Padding) використовується для вирівнювання заголовка за 32-розрядною межею.

2.2 Характеристика протоколу IPv6

Стек протоколів IPv6 підтримує такі можливості:

— послідовна передача даних;

— заголовки фрагментації та маршрутизації;

— параметри призначення;

— незалежне автоналаштування адрес;

— виявлення сусідів;

— середовище передавання даних Ethernet і FDDI;

— IPv6 поверх IPv4;

— обробка основного заголовка IPv6;

— тунелювання IPv6 у IPv4;

— мобільність вузла зв’язку;

— перевірка автентичності IPsec;

— UDP і TCP поверх IPv6;

— функціональність вузла та маршрутизатора;

— протокол ICMPv6;

— автоматичні та сконфігуровані тунелі.

Пакети протоколу IPv6 відрізняються від пакетів IPv4 тим, що деякі поля заголовка відсутні, з’явилися інші опційні поля та додаткові заголовки.

Додаткові заголовки — це окремі заголовки, які не перевіряються вузлами на всьому шляху від відправника до отримувача, що підвищує ефективність маршрутизації. Вони забезпечують більшу гнучкість у виборі способів кодування та дають змогу розширювати набір майбутніх опцій.

Крім того, додаткові заголовки призначені для перевірки цілісності, автентичності пакетів, а також для опційного шифрування даних. У протоколі IPv6 передбачена можливість позначення пакетів. Це дає змогу визначати належність пакетів до певних потоків — наприклад, під час обробки їх службою

QoS або керування пропускною здатністю без необхідності аналізувати заголовки TCP і UDP.

Доцільно подати деякі визначення таких термінів, як вузол, маршрутизатор, хост, інтерфейс — з точки зору IPv6:

— вузол — це будь-який пристрій, що підтримує IPv6;

— маршрутизатор — вузол, який пересилає пакети, призначені для інших вузлів;

— інтерфейс — пристрій для підключення до середовища передавання даних, через який надсилаються IPv6-пакети.

Можлива ситуація, коли пристрій в одних випадках виступає як маршрутизатор, а в інших — як хост. Так, якщо пристрій має кілька інтерфейсів і може пересилати пакети між вузлами, що перебувають у різних підмережах, то для інтерфейсів, які не беруть участі у пересиланні, воно виступатиме як хост, а для інших — як маршрутизатор. Зв’язок — це середовище для передавання пакетів IPv6. Сусіди — це вузли, підключені до одного й того самого каналу. MTU (Maximum Transmission Unit) — це максимальний розмір пакета, який може бути переданий через даний канал, виражений в октетах (байтах). Адреса канального рівня — це фізична адреса інтерфейсу. Наприклад, MAC-адреса для каналів Ethernet .

В IPv6 адресація здійснюється безпосередньо до інтерфейсів, а не до вузлів.

Одноадресна (унікасна) адреса визначає, на який конкретний інтерфейс буде надіслано пакет. Групова (мультикаст) адреса визначає множину інтерфейсів і зазвичай використовується для логічного об’єднання кількох вузлів. Адреса розсилки до першого отримувача (anycast) також визначає множину інтерфейсів, але пакет передається на той інтерфейс, який знаходиться найближче до відправника.

Основна відмінність IPv6 від IPv4 полягає у використанні більшої кількості бітів для адресації.

IPv4 використовує 32-бітне представлення. Адреса в IPv4 зазвичай записується у десятковій формі як послідовність чотирьох чисел, розділених

крапками.

В IPv6 адреса представлена у шістнадцятковій формі і займає 128 біт.

Існує три основні способи текстового представлення адрес IPv6:

— найпоширеніший варіант — представлення адреси у вигляді восьми шістнадцяткових секцій, розділених двокрапками (наприклад: «ABCD:EF12:3456:7890:ABCD:EF12:3456:7890»), якщо секція починається з нулів, їх можна не вказувати, але поле не може бути порожнім;

— скорочене представлення за допомогою “::”. Часто в адресах IPv6 зустрічаються довгі послідовності нульових секцій, для спрощення запису дозволяється один раз у адресі використовувати символи `::`, щоб замінити одну або кілька нульових секцій (наприклад: адреса «1234:0:0:0:ABCD:0:0:123» може бути записана як «1234::ABCD:0:0:123» або «1234:0:0:0:ABCD::123», але не можна писати «1234::ABCD::123»);

— змішане представлення IPv6/IPv4 — використовується у мережах, де одночасно працюють вузли IPv4 і IPv6, у цьому випадку перші шість секцій записуються у шістнадцятковому форматі, а решта — у звичній десятковій формі IPv4 з крапками (наприклад: 0:0:0:0:0:0:131.107.6.100 або ::131.107.6.100 (скорочений формат), 0:0:0:0:0:FFFF:131.107.4.99 або ::FFFF:131.107.4.99 (скорочений формат), ABCD:EF:12:34:0:0:131.107.2.98 або ABCD:EF:12:34::131.107.2.98 (скорочений формат).

Поле змінної довжини, що складається з початкових бітів і називається префіксом формату (FP — Format Prefix) , визначає тип адреси IPv6. Якщо значення цього поля — вісім одиниць (11111111), це означає, що адреса є груповою (multicast). Усі інші значення цього поля вказують, що адреса — одноадресна (unicast). Адреси anycast (адреси розсилки до першого отримувача) належать до простору одноадресних адрес.

Одноадресні адреси належать окремому вузлу в межах мережевого з’єднання. Проте одна одноадресна адреса може бути призначена кількома інтерфейсам, які належать одному вузлу. Такі інтерфейси повинні розглядатися протоколами вищого рівня як єдине ціле. Існує кілька типів одноадресних

(унікасних) адрес, зокрема: глобальні адреси провайдерів, локальні адреси сайтів, локальні адреси каналу та IPv6-адреси з вкладеними IPv4-адресами.

Існують зарезервовані одноадресні (унікасні) адреси. Невизначена адреса 0:0:0:0:0:0:0:0 (або :: у скороченому записі) не може бути призначена жодному вузлу й також не може використовуватися як адреса джерела. Зазвичай ця адреса застосовується під час ініціалізації IPv6 — вона вказує на те, що вузол ще не знає власної адреси. Другою зарезервованою адресою є 0:0:0:0:0:0:0:1 (або ::1 у скороченому записі). Ця адреса є адресою зворотного зв’язку (loopback) і використовується тоді, коли вузол надсилає пакети сам собі.

Глобальні адреси провайдерів мають трирівневу ієрархічну структуру. Верхній рівень ієрархії є частиною адресного простору, яким керують організації, що надають публічні інтернет-послуги. Біти рівня, що йде після верхнього, визначають внутрішні шляхи маршрутизації, а наступний рівень вказує індивідуальні інтерфейси у фізичному з’єднанні організації.

Локальні адреси одноадресної розсилки використовуються для взаємодії в межах однієї мережі (зв’язку), де немає маршрутизаторів. Вони також можуть застосовуватися під час автоконфігурації та виявлення сусідів. Ці адреси еквівалентні приватним адресам IPv4 і використовуються для адресації та обміну даними всередині організації. Маршрутизатори не повинні пересилати пакети з такими адресами за межі сайту, у межах якого вони використовуються.

Щоб полегшити перехід від IPv4 до IPv6, були розроблені два механізми тунелювання пакетів IPv6 у мережеву інфраструктуру IPv4.

Перший механізм передбачає, що перші шість секцій адреси подані у шістнадцятковому форматі, а останні 32 біти — це IPv4-адреса, записана у вигляді чотирьох десяткових чисел, розділених крапками.

Другий механізм відрізняється тим, що перед останніми 32 бітами розташоване значення «FFFF». Цей тип адреси використовується для представлення IPv6-адрес вузлів IPv4 , які не підтримують IPv6. Таким чином, у другому випадку всередині IPv6-адреси міститься IPv4-адреса.

Адреси розсилки до першого отримувача структурно ідентичні одноадресним адресам і призначаються з пулу доступних одноадресних адрес організації. Таку адресу може бути призначено групі вузлів , які найчастіше є маршрутизаторами.

У деяких випадках зручніше використовувати адресу розсилки до першого отримувача, ніж звичайну одноадресну адресу. Якщо адреса розсилки до першого отримувача призначена групі вузлів-маршрутизаторів, тоді взаємодія відбуватиметься між вузлом-відправником і найближчим до нього маршрутизатором.

Водночас існує низка обмежень щодо використання таких адрес.

Групова адреса призначається групі вузлів. На відміну від адреси розсилки до першого отримувача (anycast), у випадку використання групової адреси (multicast) доставка від вузла-джерела відбувається до всіх вузлів, яким призначено цю адресу. Вузол може належати до кількох груп одночасно. Групова адреса не може використовуватися як адреса джерела, а також не застосовується в заголовках маршрутизації.

Механізм виявлення маршрутизаторів використовується для різних цілей. Маршрутизатори застосовують групову розсилку повідомлень «Оголошення маршрутизатора» (Router Advertisement) у відповідь на запити «Запит маршрутизатора» (Router Solicitation). Повідомлення «Оголошення маршрутизатора» містить таку інформацію, необхідну для налаштування вузлів:

— рекомендовану кількість переходів;

— префікс зв’язку (аналог маски підмережі в IPv4);

— адресу маршрутизатора;

— значення MTU зв’язку.

Коли маршрутизатор оголошує свою фізичну адресу, він тим самим дає змогу іншим вузлам у мережі визначити його наявність.

Оголошення маршрутизатором префіксу зв’язку дозволяє вузлам з’ясувати, до яких підмереж вони підключені, і побудувати внутрішню таблицю маршрутизації.

У пакетах IPv6 з кожним переходом зменшується значення, яке зберігається в полі «Обмеження кількості переходів» (Hop Limit) , а не час життя пакета (TTL), як у IPv4.

Маршрутизатор, повідомляючи рекомендовану кількість переходів, дає вузлам зрозуміти, чи доступний пункт призначення за даним маршрутом.

Для коректної роботи багатоадресної (multicast) розсилки усі вузли, що використовують одну й ту саму лінію зв’язку, мають застосовувати однакове значення MTU.

Використовуючи повідомлення «Оголошення маршрутизатора», маршрутизатори також можуть бути налаштовані для розподілу вхідного навантаження. Маршрутизатори можуть мати декілька інтерфейсів, підключених до однієї лінії зв’язку. Такі інтерфейси можуть розглядатися як один інтерфейс із кількома адресами.

Маршрутизатори можуть не включати вихідні адреси у повідомлення «Оголошення маршрутизатора». У цьому випадку вузли, які хочуть надсилати пакети маршрутизатору, надсилають повідомлення «Запит сусіда» (Neighbor Solicitation) , щоб отримати адресу інтерфейсу маршрутизатора.

На різні запити маршрутизатор може надсилати різні адреси , і вузли вважатимуть, що передають пакети на один багатоadресний інтерфейс .Таким чином маршрутизатор може розподіляти вхідне навантаження між своїми інтерфейсами .

Поряд з цим, у IPv6 існують механізми виявлення хоста. Хости використовують цей механізм переважно як засіб для дослідження мережі, але також відповідають на запити , повідомляючи про власну конфігурацію.

Під час ініціалізації хост може надіслати запит маршрутизатору, щоб визначити спосіб налаштування своєї адреси — чи можлива зміна адреси під час роботи, чи така можливість відсутня. Автоконфігурація з можливістю динамічного призначення адреси використовується тоді, коли адреса хосту видається за допомогою служби DHCP.

2.3 Формат заголовка IPv6 та механізми маршрутизації

Інформація про адреси становить лише частину заголовка кожного пакета IPv6. Решта інформації необхідна для ефективної оцінки та обробки пакета.

Окрім основного заголовка, пакет IPv6 може містити один або кілька додаткових заголовків, у яких може зберігатися інформація про маршрутизацію, фрагментацію або наступний перехід. Ця інформація визначається відправником.

Додаткові заголовки не обробляються вузлами на маршруті під час передавання пакета — вони опрацьовуються лише вузлом призначення (це може бути як кінцевий вузол, так і проміжний вузол призначення). Довжина додаткового заголовка кратна 8 октетам, що дозволяє вирівняти довжину пакета й уникнути обробки цих заголовків усіма вузлами під час передачі. Кількість додаткових заголовків може бути різною: можуть бути присутні всі, лише деякі з них або ж вони можуть повністю відсутні (табл. 2.4).

Повна специфікація IPv6 включає такі заголовки (у порядку їх розташування в датаграмі):

— IPv6 Header — заголовок IPv6;

— Hop-by-Hop Options Header — заголовок параметрів «від вузла до вузла»;

— Destination Options Header (Опції одержувача 1);

— Routing Header — заголовок маршрутизації;

— Fragment Header — заголовок фрагментації;

— Authentication Header — заголовок автентифікації;

— Encapsulating Security Payload Header — заголовок інкапсульованих даних безпеки (додаткова автентифікація);

— Destination Options Header (Опції одержувача 2);

— Заголовок верхнього рівня (наприклад, TCP).

Hop-by-Hop Options Header — заголовок параметрів, які обробляються кожним маршрутизатором, через який проходить пакет, тобто «від вузла до вузла» (табл. 2.5).

Next Header (8 біт) — це поле ідентифікує тип наступного заголовка.

Hdr Ext Len (8 біт) — довжина даного заголовка.

Таблиця 2.4 — Призначення полів заголовка пакета IPv6

Поле	Довжина	Характеристика
Версія (Version)	4 біта	Значення «0110» вказує на версію 6.
Клас Трафіку (Traffic Class)	8 біт	Використовується при індентифікації класу чи пріоритету трафіку, для того, чтоб пакети могли бути перенаправлені з іншими пріоритетами для забезпечення QoS.
Мітка потоку (Flow Label)	20 біт	Пакети, які відповідають певному класу потоку, помічаються для визначення належності цьому потоку
Довжина корисного навантаження (Payload Length)	16 біт	Довжина в октетах частини пакету, що залишилась, яка містить додаткові заголовки.
Наступний заголовок (Next Header)	8 біт	Визначає тип заголовку, який слідує зразу після заголовка IPv6. Використовуються ті ж значення, що і в полі протоколу IPv4 (RFC 1700).
Межа переходів (Hop Limit)	8 біт	Число зв’язків, через які пакет може бути переданий, поки не буде відкинутий. Кожна пересилка зменшує значення цього поля на 1.
Адреса відправника (Source Address)	128 біт	Адреса вузла відправника.
Адреса призначення (Destination Address)	128 біт	Адреса вузла призначення, який може бути або кінцевим адресатом, або проміжним вузлом.

Options — це поле додаткових параметрів. Воно містить параметри, які визначають деякі стандартні операції над датаграмою.

Таблиця 2.5 — Приклад Hop-by-Hop Options Header

0 8	16	31
Next Header	Hdr Ext Len	Options

Окрім цих параметрів, поле Options також містить параметр Jumbo Payload (надвеликого розміру).

Цей параметр указує довжину пакета в байтах разом із заголовком Hop-by-Hop і має перевищувати 65535.

Параметр Jumbo Payload використовується в IPv6 для пакетів, розмір яких більший за 65535 байт.

Для таких пакетів значення поля Payload Length в основному заголовку повинно дорівнювати 0.

Опція Jumbo Payload не застосовується, якщо пакет містить заголовок фрагментації.

Routing Header (заголовок маршрутизації) використовується для того, щоб указати пакету список проміжних вузлів (хостів), через які він має пройти на шляху до пункту призначення. Аналогічна функція існує і в IPv4. Такий заголовок ідентифікується значенням 43 у полі Next Header попереднього заголовка (табл. 2.6).

Таблиця 2.6 – Приклад Routing Header

0 8	16	24	31
Next Header	Hdr Ext Len	Routing Type	Segments Left
Type–specific data			

Next Header (8 біт) — це поле ідентифікує тип наступного заголовка.

Hdr Ext Len (8 біт) — довжина даного заголовка.

Routing Type (8 біт) — це поле визначає тип маршрутизації.

Segment Left (8 біт) — це поле містить кількість проміжних вузлів зі списку, які датаграма ще не пройшла перед досягненням одержувача.

Type-specific data — поле даних, структура якого визначається типом маршрутизації. Це поле вирівнюється по 64-бітній межі.

Поле містить список проміжних вузлів, через які проходить пакет на шляху до одержувача.

Fragment Header (заголовок фрагментації) використовується в IPv6, коли розмір пакета перевищує допустимий розмір датаграми, яку можна передати через вузли, розташовані на шляху до пункту призначення. Ідентифікатор цього заголовка — 44 (табл 2.7).

Таблиця 2.7 — Приклад Fragment Header

0 8	16	28	31	
Next Header	Reserved	Fragment Offset	Res	M
Identification				

Next Header (8 біт) — це поле ідентифікує тип наступного заголовка.

Reserved (8 біт) — це поле не використовується.

Fragment Offset (13 біт) — поле зсуву фрагмента, задається у 64-бітних одиницях відносно початку фрагментованої частини пакета.

Res (2 біти) — поле приймає значення 0 під час передавання пакета й ігнорується під час приймання.

M (1 біт) — поле має значення 1, якщо існує наступний фрагмент. Якщо це останній фрагмент, поле приймає значення 0.

Identification (32 біти) — це поле визначає ідентифікатор датаграми.

Коли датаграма є занадто великою, вона розбивається на кілька фрагментів, і кожен фрагмент передається окремо.

Кожен фрагмент групи містить у цьому полі ідентифікатор групи, який має відрізнятися від ідентифікаторів інших груп, надісланих із тими ж адресами відправника й одержувача протягом того самого проміжку часу.

Authentication Header (заголовок автентифікації) забезпечує захист переданих даних шляхом шифрування на основі криптографічного ключа із застосуванням асиметричних методів кодування.

Заголовок автентифікації є механізмом, який дозволяє забезпечити автентифікацію відправника на рівні IP-протоколу як для IPv4, так і для IPv6.

Також цей заголовок сприяє перевірці цілісності даних. Даний механізм безпеки є ефективнішим, ніж той, що використовувався раніше в IPv4. Цей метод застосовується лише для розв'язання конкретних завдань безпеки й не може бути використаний як єдиний засіб захисту. Механізм забезпечує цілісність переданих даних шляхом додавання до IP-датаграми інформації автентифікації. Ця інформація визначається на основі вмісту всіх полів пакета (як заголовків, так і користувацьких даних). Значення полів і опцій, які змінюються під час передавання датаграми, під час обчислення інформації автентифікації приймаються рівними 0. Інформація автентифікації визначається відправником датаграми та перевіряється лише одержувачем даного пакета.

Оскільки проміжні вузли (хости) не контролюють безпеку передавання, наявність такого заголовка не впливає на швидкість обробки пакета.

Також наявність заголовка автентифікації не накладає жодних вимог на вже існуючу інфраструктуру мережі Інтернет.

Дані, необхідні для забезпечення безпеки пакетів, розміщуються в окремому заголовку. І якщо система не працює з пакетами, у яких присутній заголовок автентифікації, вона може просто ігнорувати їх. Для шифрування даних пакета застосовується криптостійкий алгоритм із використанням асиметричного секретного ключа.

Структура пакета побудована таким чином, що алгоритм роботи із секретним ключем не інтегрований у механізм автентифікації IP. Це дозволяє використовувати різні механізми генерації секретного ключа без зміни основних принципів IP-безпеки.

Передавати ключ і набір параметрів алгоритму шифрування для кожного пакета — неефективно. Виходом із цієї ситуації є те, що механізм генерації ключів створює спеціальну логічну таблицю відповідностей SA (Security Association). Ця таблиця зберігає параметри для кожної пари, що шифрується (ключ–алгоритм).

Механізм безпеки IP повинен зчитати запис із цієї таблиці, щоб визначити алгоритм і ключ, які використовуються для автентифікації кожної датаграми. Під час формування відправлюваного IP-пакета насамперед необхідно створити асоціацію в таблиці відповідностей SA (Security Association) для даної датаграми. Вибір асоціації в таблиці здійснюється на основі ідентифікатора відправника та адреси одержувача пакета. Обрана асоціація визначає алгоритм, тип алгоритму, ключ та інші параметри шифрування. Зв'язувальним елементом між механізмом генерації ключа та вибором алгоритму шифрування є індекс відповідності параметрів шифрування SPI (Security Parameters Index). Цей індекс є своєрідним кодом у таблиці асоціацій SA. Індекс SPI передається в заголовку автентифікації пакета.

Одержувач, отримавши пакет, на основі адреси призначення та індексу SPI, який він витягує із заголовка автентифікації пакета, визначає відповідний запис у таблиці SA. Цей запис надає одержувачу інформацію про алгоритм і ключ дешифрування. Після цього одержувач перевіряє цілісність даних і дешифрує їх.

Ідентифікатором заголовка автентифікації у полі Next Header попереднього заголовка є число 51 (табл. 2.8).

Таблиця 2.8 — Приклад Next Header

0 8	16	31
Next Header	Length	Reserved
Security Parameters Index		
Authentication Data		

Next Header (8 біт) — це поле ідентифікує тип наступного заголовка.

Length (8 біт) — додаткова довжина. Це поле містить довжину даних автентифікації у 32-бітних одиницях.

Мінімальне значення цього поля — 0, що означає відсутність шифрування (нульовий алгоритм).

Reserved (8 біт) — це поле не використовується.

Security Parameters Index (SPI) (32 біти) — поле індексу параметра. Воно містить псевдовипадкове число, яке визначає індекс відповідності у таблиці асоціацій SA (ця таблиця задає тип алгоритму, параметри шифрування тощо). Значення 0 використовується за відсутності відповідностей, а значення від 1 до 255 — зарезервовані.

Authentication Data — дані автентифікації, є результатом роботи алгоритму шифрування, що базується на вмісті всієї датаграми. Дані автентифікації зберігають свій формат для певної пари (SPI і адреса одержувача).

3 АНАЛІЗ ЗАСОБІВ ВЗАЄМОДІЇ МЕРЕЖ IPV6 та IPV4

3.1 Аналіз розподілення мереж IPv4 та IPv6 у світі

На сьогоднішній день у глобальному масштабі спостерігається співіснування двох версій протоколу Інтернет — IPv4 та IPv6, що зумовлено історичним розвитком мережі та поступовим переходом до нових технологій. Протокол IPv4, попри свій обмежений адресний простір, досі залишається домінуючим у багатьох регіонах світу, особливо в країнах із застарілою або повільно модернізованою мережевою інфраструктурою. Значна частина IPv4-адрес уже розподілена між регіональними інтернет-реєстрами, що призвело до їх фактичного вичерпання та появи вторинних ринків адрес.

Розподілення IPv4-мереж є нерівномірним: найбільша кількість адрес історично зосереджена у Північній Америці та Західній Європі, що пояснюється раннім розвитком Інтернету саме в цих регіонах. Натомість країни Азії, Африки та Південної Америки відчувають гостріший дефіцит IPv4-адрес, що стимулює активніше впровадження альтернативних рішень, зокрема використання технологій трансляції адрес (NAT) та перехід на IPv6.

Протокол IPv6 демонструє стабільну тенденцію до зростання рівня впровадження у світі. Найвищі показники використання IPv6 спостерігаються в країнах з розвиненою телекомунікаційною інфраструктурою та активною державною або корпоративною підтримкою нових стандартів. Провідну роль у поширенні IPv6 відіграють великі інтернет-провайдери, мобільні оператори та глобальні контент-платформи, які впроваджують IPv6 для забезпечення масштабованості, підвищення якості сервісів і зменшення залежності від IPv4.

Особливо активно IPv6 розвивається в мобільних мережах, де кількість підключених пристроїв постійно зростає. У багатьох країнах мобільні оператори використовують IPv6 як основний протокол доступу, поєднуючи його з механізмами доступу до ресурсів IPv4. У фіксованих мережах впровадження IPv6 відбувається дещо повільніше, однак також має стійку позитивну динаміку.

Аналіз розподілення мереж IPv4 та IPv6 у світі свідчить про поступовий, але незворотний перехід до IPv6. Хоча IPv4 ще тривалий час залишатиметься в

експлуатації, подальший розвиток Інтернету, зростання кількості підключених пристроїв і впровадження нових сервісів неможливі без широкого використання IPv6.

RIR (Regional Internet Registries) — це регіональні некомерційні організації, відповідальні за розподіл та адміністрування інтернет-ресурсів у межах визначених географічних регіонів світу. До таких ресурсів належать IP-адреси (IPv4 та IPv6), номери автономних систем (AS Number, ASN), а також пов’язані з ними реєстраційні дані. Діяльність RIR є ключовою для стабільного функціонування глобальної мережі Інтернет та забезпечення унікальності адресного простору.

Основною функцією регіональних інтернет-реєстраторів є отримання великих блоків адресного простору від IANA (Internet Assigned Numbers Authority) та їх подальший розподіл між локальними інтернет-реєстраторами (LIR), інтернет-провайдерами, великими організаціями та корпоративними мережами. Розподіл ресурсів здійснюється відповідно до затверджених політик, які розробляються та ухвалюються спільнотою користувачів кожного регіону на засадах відкритості та прозорості.

Крім розподілу адрес, RIR виконують важливу роль у веденні реєстрів інтернет-ресурсів, що містять інформацію про власників IP-мереж та автономних систем. Ці дані використовуються для забезпечення коректної маршрутизації, підвищення рівня безпеки мереж, а також для вирішення технічних і адміністративних питань, пов’язаних з експлуатацією Інтернету. Також RIR активно сприяють впровадженню IPv6, організовують навчальні програми, технічні семінари та підтримують розвиток інтернет-спільноти у своєму регіоні.

У світі функціонує п’ять основних регіональних інтернет-реєстраторів (рис. 3.1):

— ARIN (American Registry for Internet Numbers) — Північна Америка;

— RIPE NCC (Réseaux IP Européens Network Coordination Centre) — Європа, Близький Схід та частина Центральної Азії;

— APNIC (Asia-Pacific Network Information Centre) — Азійсько-Тихоокеанський регіон;

— LACNIC (Latin America and Caribbean Network Information Centre) — Латинська Америка та Карибський басейн;

— AFRINIC (African Network Information Centre) — Африка.

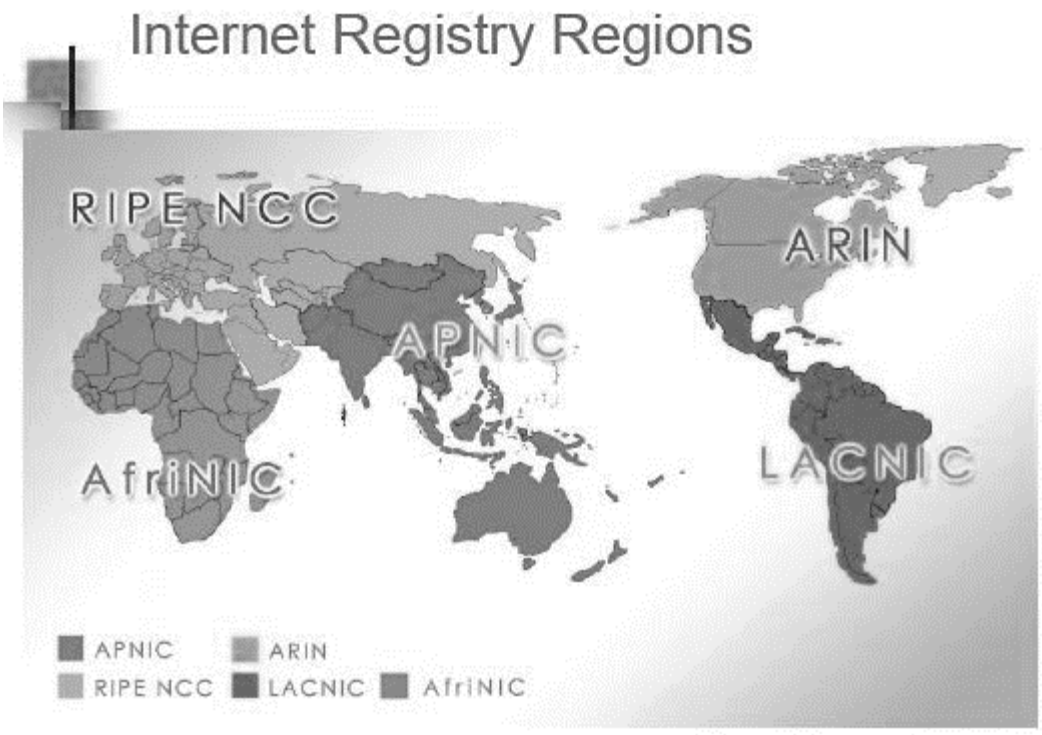

Рисунок 3.1 – Розподіл ресурсів регіональних інтернет-реєстраторів

Україна належить до зони обслуговування регіонального інтернет-реєстратора RIPE NCC (Réseaux IP Européens Network Coordination Centre). Даний реєстратор відповідає за розподіл та адміністрування інтернет-ресурсів у регіоні Європи, Близького Сходу та частини Центральної Азії.

У межах діяльності RIPE NCC для України здійснюється розподіл IP-адрес IPv4 та IPv6, а також номерів автономних систем (ASN) між інтернет-провайдерами, операторами зв’язку, державними установами та комерційними організаціями. Усі ці ресурси виділяються відповідно до політик RIPE, які розробляються спільнотою учасників на принципах відкритості, прозорості та технічної доцільності.

Українські організації зазвичай взаємодіють з RIPE NCC через статус LIR (Local Internet Registry), що дозволяє їм самостійно керувати отриманими адресними ресурсами, реєструвати маршрути, підтримувати актуальність даних у RIPE Database та брати участь у процесах розвитку політик. Також RIPE NCC забезпечує технічну підтримку, навчальні програми та інформаційні ресурси, які сприяють розвитку інтернет-інфраструктури в Україні.

Належність України до RIPE NCC має важливе значення для інтеграції національного сегмента Інтернету у глобальний мережевий простір. Це забезпечує коректну маршрутизацію трафіку, підвищує рівень безпеки мереж, а також сприяє впровадженню сучасних технологій, зокрема IPv6, що є необхідним для подальшого сталого розвитку інтернет-інфраструктури країни.

За даними регіонального інтернет-реєстратора APNIC, у листопаді 2024 року майже 39% світового трафіку передавалося за протоколом IPv6. Якщо ж звернутися до показників великих IT-компаній, то їхня статистика виглядає більш оптимістичною. Так, у травні 2025 року 48% користувачів продуктів Google підключалися до них за протоколом нового покоління.

Загалом експерти позитивно оцінюють перспективи розвитку інфраструктури IPv6. Нік Бурагліо, член робочої групи з розвитку нового протоколу в IETF та відповідальний за просування ініціативи IPv6-only у Міністерстві енергетики США, вважає, що у 2025 році частка IPv6 у глобальному трафіку нарешті досягне бажаної позначки у 50% [5].

Каталізатором росту може стати програма сертифікації IPv6 Ready, розвитком якої займається організація IPv6 Forum. Ініціатива спрямована на перевірку відповідності обладнання та програмного забезпечення стандартам IPv6, тобто на забезпечення сумісності пристроїв і застосунків із протоколом нового покоління. Сертифікацію вже визнано у 35 країнах, зокрема у США, Японії та Південній Кореї, і вона охоплює понад 30 категорій продуктів — від маршрутизаторів і комутаторів до систем кібербезпеки та робототехніки. Згідно зі звітом, опублікованим спільно з китайськими колегами, станом на кінець минулого року у світі було сертифіковано понад 8100 пристроїв, з яких 2971

припадало на Китай, 1100 — на США та 470 — на Японію. При цьому кількість нових сертифікацій зросла на 124% порівняно з попереднім періодом. Як зазначають експерти, ці показники стали рекордними за всю історію програми.

Водночас деякі представники галузі мають більш стриману політику. Так, Уеслі Корреа, фахівець із телекомунікацій з Університету Естасіу-де-Са в Бразилії, виступаючи на конференції LACNIC 42 наприкінці минулого року, наголосив, що не варто очікувати «вибухового» зростання, оскільки впровадження IPv6 потребуватиме певних витрат на обладнання та підготовку кадрів. Багато учасників дискусії з ним погодилися. Якщо поточні тенденції збережуться, повний перехід на IPv6 відбудеться ще нескоро. Наразі частка IPv6-трафіку щороку зростає приблизно на 3%.

У 2025 році характерною тенденцією для України є зростання частки мереж, у яких IPv6 використовується паралельно з IPv4 у режимі dual-stack. Такий підхід дозволяє забезпечити сумісність із наявною інфраструктурою та поступово переводити сервіси й користувачів на IPv6 без порушення доступності ресурсів. Особливо помітним є зростання використання IPv6 у мобільних мережах, де протокол нового покоління часто виступає основним для підключення кінцевих пристроїв.

Водночас розподіл IPv6-адрес в Україні залишається нерівномірним. Найбільша концентрація IPv6-мереж спостерігається у великих містах і регіонах із розвиненою телекомунікаційною інфраструктурою, тоді як у невеликих населених пунктах впровадження IPv6 відбувається повільніше. Основними стримувальними чинниками залишаються потреба в модернізації мережевого обладнання, обмежена кількість фахівців із практичним досвідом роботи з IPv6 та необхідність адаптації прикладних сервісів.

Впровадження протоколу IPv6 в Україні відбувається насамперед завдяки діяльності великих операторів зв’язку, які мають розвинену телекомунікаційну інфраструктуру та значну абонентську базу. Серед них ключову роль відіграють такі компанії, як Укртелеком і Київстар, що використовують IPv6 у різних

сегментах своїх мереж, адаптуючи його до специфіки фіксованого та мобільного доступу відповідно.

Укртелеком, як один із найбільших операторів фіксованого зв’язку в Україні, застосовує IPv6 переважно у магістральних, опорних та корпоративних мережах. Використання IPv6 дозволяє оператору спростити ієрархію адресації, підвищити масштабованість мережі та забезпечити готовність інфраструктури до подальшого зростання кількості підключених вузлів. Для корпоративних клієнтів, державних установ і великих організацій Укртелеком надає IPv6-префікси, що дає можливість будувати власні внутрішні мережі з прямою глобальною адресацією. Крім того, IPv6 використовується для хостингових і серверних сервісів, де відсутність NAT спрощує доступ до ресурсів, підвищує прозорість мережевих з’єднань і рівень безпеки.

Київстар, як провідний оператор мобільного зв’язку, активно впроваджує IPv6 у мережах мобільного доступу, зокрема в 4G/LTE. Для кінцевих користувачів IPv6 часто використовується автоматично, без необхідності додаткового налаштування на стороні абонента. Такий підхід дозволяє значно зменшити навантаження на механізми трансляції IPv4-адрес (CG-NAT) та ефективно обслуговувати мільйони мобільних пристроїв. Доступ до ресурсів IPv4 при цьому забезпечується за допомогою технологій сумісності, що гарантує безперервність роботи сервісів.

Окремим напрямом використання IPv6 у Київстарі є IoT та M2M-рішення, де велика кількість підключених пристроїв потребує унікальної адресації та високої масштабованості. IPv6 у цьому випадку виступає оптимальним рішенням, оскільки дозволяє надавати кожному пристрою унікальну адресу без складних схем трансляції. Крім того, оператор поступово тестує та впроваджує IPv6-only сегменти мережі, що відповідає світовим тенденціям розвитку мобільного Інтернету.

Приклади Укртелекому та Київстару демонструють різні, але взаємодоповнювальні підходи до впровадження IPv6 в Україні. Фіксовані оператори зосереджуються на магістральних і корпоративних рішеннях, тоді як

мобільні оператори активно використовують IPv6 для масового доступу та нових сервісів. Це свідчить про поступовий і системний перехід українського телекомунікаційного ринку до використання протоколу нового покоління та формування основи для подальшого розвитку національної інтернет-інфраструктури.

3.2 Аналіз технологій взаємодії мереж IPv4та IPv6

Фахівці, аналізуючи розвиток мережі Інтернет, доходять висновку, що перехід на мережі IPv6 не буде миттєвим. Протягом тривалого часу співіснуватимуть як мережі IPv4, так і мережі IPv6. Спочатку мережі IPv6 нагадуватимуть «острови» в океані IPv4. На початковому етапі вузли, що реалізують IPv6, не забезпечуватимуть усіх необхідних сервісів.

Тому до вузлів IPv6 висуваються такі основні вимоги:

— можливість взаємодії з вузлами IPv4;

— можливість передавання пакетів IPv6 через наявну інфраструктуру IPv4.

Із цього випливає, що необхідні механізми співіснування мереж IPv4 та IPv6.

Взаємодія систем, які використовують різні стеки протоколів, зазвичай здійснюється за допомогою таких методів:

— трансляція;

— інкапсуляція (тунелювання);

— мультиплексування.

Трансляція забезпечує узгодження стеків протоколів шляхом перетворення форматів повідомлень. Також під час трансляції здійснюється відображення адрес вузлів і мереж, які по-різному інтерпретуються в цих протоколах. Як транслювальний елемент можуть виступати: програмний або апаратний шлюз, міст, комутатор, маршрутизатор тощо. Транслювальний елемент розміщується між взаємодіючими мережами й виконує роль посередника під час передавання повідомлень із мережі, що використовує один протокол, у мережу, яка працює за

іншим протоколом. Такий елемент здійснює перетворення форматів повідомлень і відповідність адрес між різними мережами.

Мультиплексування передбачає, що в мережеве обладнання або в операційні системи серверів і робочих станцій вбудовуються декілька стеків протоколів. На вузлах мережі встановлюється кілька стеків комунікаційних протоколів — за кількістю мереж, які використовують різні мережеві протоколи. Необхідно, щоб запит від прикладного процесу правильно оброблявся та проходив через певний стек протоколів. Для цього застосовується спеціальний програмний елемент — мультиплексор протоколів або менеджер протоколів. Цей програмний елемент визначає, у яку мережу спрямований запит від клієнта.

Інкапсуляція є ще одним методом, який допомагає при взаємодії мереж, що використовують різні мережеві протоколи. Інкапсуляція (тунелювання) застосовується тоді, коли необхідно забезпечити взаємодію двох мереж з однією технологією через транзитну мережу, у якій використовується інша технологія.

У процесі інкапсуляції беруть участь три типи протоколів :

— протокол інкапсуляції;

— транспортований протокол;

— несучий протокол.

Транспортованим є протокол об’єднуваних мереж, а несучим — протокол транзитної мережі. Пакети транспортованого протоколу розміщуються в полі даних несучого протоколу за допомогою протоколу інкапсуляції.

У змішаних мережах IPv4—IPv6 найчастіше використовуються мультиплексування та інкапсуляція (тунелювання).

Ці методи дозволяють вузлам мережі, що використовує протокол IPv6, обмінюватися даними з вузлами іншої IPv6-мережі через мережу, у якій застосовується протокол IPv4.

Для того щоб вузли, які підтримують лише протокол IPv6, могли звертатися до ресурсів мережі IPv4, необхідна наявність додаткових систем: шлюзів транспортного та прикладного рівнів, трансляторів протоколів тощо.

Наразі розробляються такі механізми, які дозволяють протоколу IPv6 безперешкодно працювати поверх мереж, що підтримують лише протокол IPv4.

Однак у майбутньому обов’язково знадобляться механізми, які дадуть змогу передавати IPv4 через мережі, що підтримують лише протокол IPv6, оскільки з часом саме IPv6 стане основним мережевим протоколом.

Механізм мультиплексування передбачає одночасну підтримку вузлами двох стеків протоколів. Для реалізації цього необхідно, щоб кожен вузол мав дві адреси: IPv4 і IPv6. Ці адреси можуть бути ніяк не пов’язані між собою. Адреси IPv4 мають бути унікальними. До моменту вичерпання адресного простору IPv4 процес переходу на IPv6 має просунутися достатньо далеко, щоб нові вузли могли отримувати всі необхідні послуги, використовуючи виключно засоби протоколу IPv6. Для реалізації одночасної підтримки двох стеків протоколів потрібні відповідні інфраструктурні сервіси. Наприклад, служба DNS повинна видавати як записи типу «A» з 32-бітною IP-адресою, так і записи типу «AAAA» зі 128-бітною адресою. Від результату DNS-запиту може залежати, який стек протоколів буде використано.

Підтримка кількох стеків не є серйозною проблемою для маршрутизаторів, які завжди були багатопротокольними. Для хостів це також не становить труднощів, оскільки майже всі операційні системи поряд із IP підтримують і певні успадковані протоколи.

Механізм тунелювання вже давно використовується в IPv4 для транспортування не IP-пакетів. У випадку з IPv6 застосовується механізм інкапсуляції, який зображено на рисунку 3.2.

до інкапсуляції:

Заголовок IPv6	Вміст пакету IPv6

після інкапсуляції

Заголовок IPv4 з полем «Протокол» рівним 41	Заголовок IPv6	Вміст пакету IPv6

Рисунок 3.2 — Механізм інкапсуляції

Пакет IPv6 поміщається в поле даних пакета IPv4, після чого передається звичайною мережею IPv4. На приймальному кінці пакет IPv6 витягується з поля даних пакета IPv4 і обробляється у звичайний спосіб. Він або передається далі (це вже відбувається в IPv6-мережі), або використовується отримувачем.

Несучим протоколом у цьому випадку є IPv4, а транспортованим — IPv6. Протокол IPv4 відіграє роль протоколу канального рівня з точки зору IPv6, тому поле Hop Limit у пакеті IPv6 буде зменшене лише на одиницю (якщо буде потрібне подальше переспрямування пакета).

У загальному випадку повний маршрут пакета IPv6 може включати кілька тунелів через транзитні мережі IPv4. Підтримка механізму тунелювання розширює функціональні можливості вузлів, які є кінцевими точками тунелю. Це накладає на них додаткові обов’язки. Приймальний вузол повинен визначити, що в полі даних отриманого пакета IPv4 міститься пакет IPv6. Для цього перевіряється поле «Протокол» у заголовку пакета IPv4. Значення цього поля в даному випадку повинно дорівнювати десятковому числу 41.

Значення максимального розміру пакета (MTU), який може бути надісланий через інтерфейс IPv6, становить 1280 байт.

Щоб уникнути надмірної фрагментації, інкапсулююча система повинна використовувати таке значення MTU для пакета IPv6, щоб він разом із заголовком помістився в дозволене значення MTU для пакета IPv4.

Якщо розмір передаваного пакета IPv6 не дозволяє розмістити його повністю в полі даних пакета IPv4, інкапсулюючий вузол може надіслати вузлу-джерелу трафіку IPv6 керівне повідомлення ICMPv6.

Під час приймання пакета IPv4, який несе в полі даних пакет IPv6, система повинна застосувати до нього стандартні методи фільтрації трафіку за вихідною адресою — пакет відкидається, якщо це особлива адреса — для широкомовної або багатоадресної розсилки.

Також пакет відкидається, якщо вихідна адреса дорівнює 0.0.0.0 або 127.x.x.x.

Після цього інкапсулюючий заголовок пакета IPv4 відкидається, і методи фільтрації повинні бути застосовані вже до пакета IPv6.

У IPv6 також існують особливі адреси — до них належать адреси багатоадресної розсилки, невизначені адреси, спеціальні адреси, отримані відображенням IPv4 у IPv6, а також адреси зворотного петлевого інтерфейсу.

Далі пакет передається стеку IPv6 і обробляється як звичайний пакет IPv6. Вузол не повинен здійснювати подальшу маршрутизацію пакета IPv6, якщо така можливість не передбачена конфігурацією для IPv4-адреси, з якої цей пакет надійшов. Таким чином, маршрутизація цього пакета IPv6 може виконуватися лише тоді, якщо вузол сконфігурований як кінцева точка тунелю, початковою точкою якого є IPv4-адреса вузла-відправника.

Оскільки початкова точка тунелю, яка здійснює інкапсуляцію пакетів IPv6 у пакети IPv4, є вузлом-відправником стосовно пакета IPv4, то саме ця точка може отримати повідомлення про помилку, що виникла під час передавання пакета IPv4 мережею.

У деяких випадках, залежно від типу ICMP-повідомлення, може виникнути необхідність передати повідомлення про помилку вузлу-відправнику пакета IPv6. Наприклад, якщо ICMP-повідомлення повідомляє про перевищення максимального розміру пакета, то система повинна діяти відповідно до специфікації для визначення максимального розміру блоку даних IPv4, який може бути переданий даним маршрутом без фрагментації.

Таким чином, необхідно зареєструвати допустиме максимальне значення блоку даних IPv4 і ухвалити рішення, чи потрібно надсилати керуюче повідомлення ICMPv6 вузлу-джерелу трафіку IPv6.

Обробка інших типів повідомлень IPv4 залежить від того, яка частина повідомлення, що спричинила помилку, міститься в ICMP-повідомленні. Залежно від реалізації ICMP, повідомлення цього протоколу, окрім зовнішнього заголовка

IPv4, може містити 8 і більше байтів поля даних пакета IPv4, до якого належить це керуюче повідомлення.

Якщо цих даних достатньо для реконструкції заголовка IPv6, то генерується повідомлення ICMPv6, яке надсилається вузлу-джерелу IPv6.

Можна виділити чотири типи тунелів:

— хост — хост;

— маршрутизатор — хост;

— хост — маршрутизатор;

— маршрутизатор — маршрутизатор.

У двох перших випадках кінцева точка тунелю збігається з кінцевою точкою маршруту пакета IPv6 (рис. 3.3, рис. 3.4).

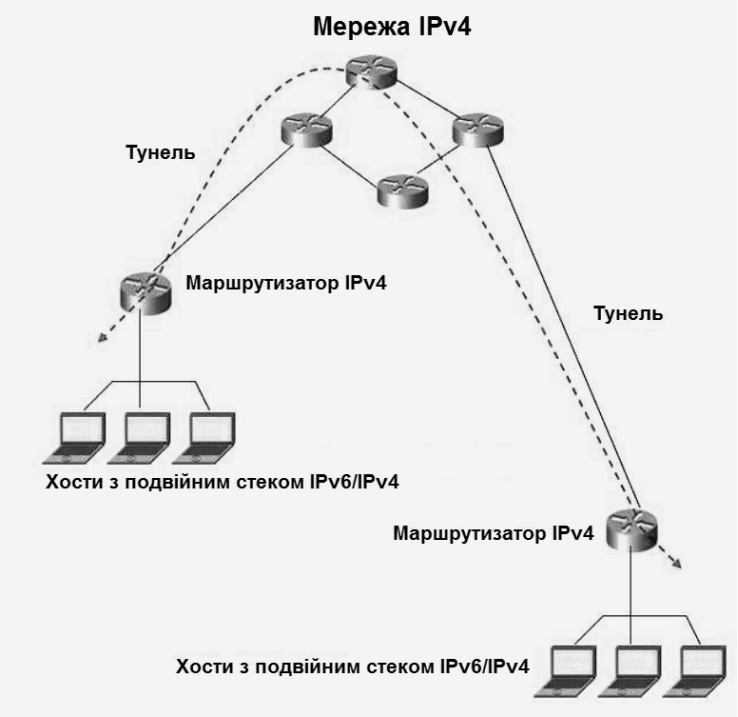

Рисунок 3.3 — Приклад тунелю виду хост — хост

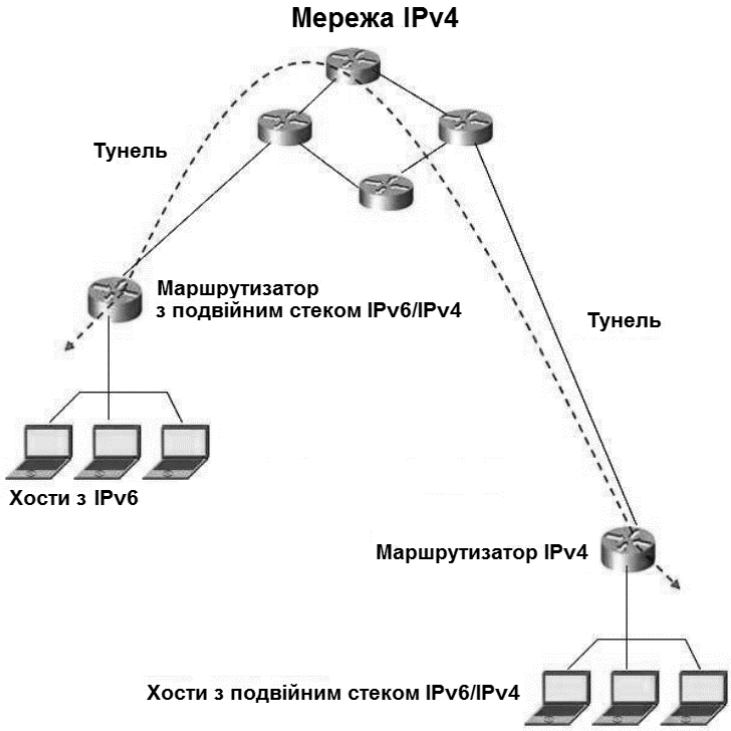

Рисунок 3.4 — Приклад тунелю виду маршрутизатор — хост

Адреса кінця тунелю повинна автоматично обчислюватися як функція адреси цільового вузла. Прийнято говорити, що в цьому випадку здійснюється автоматичне тунелювання (рис. 3.5, рис. 3.6).

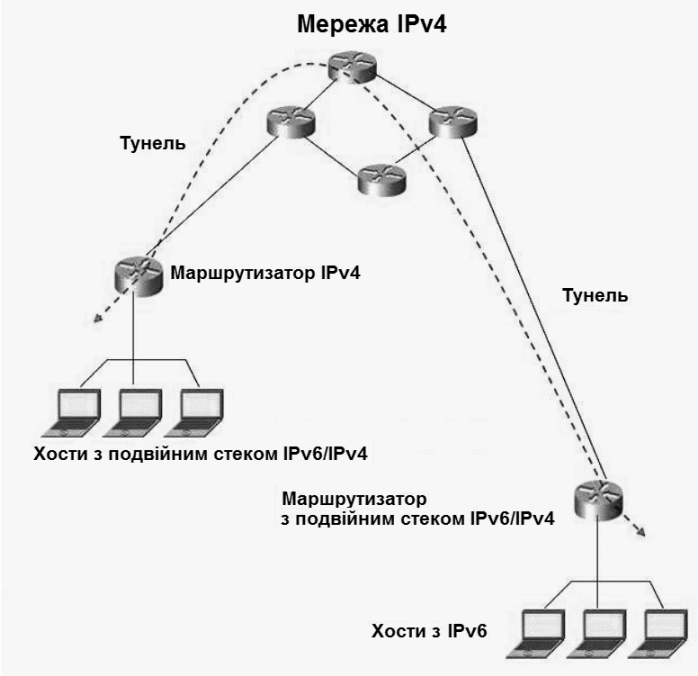

Рисунок 3.5 — Приклад тунелю виду хост — маршрутизатор

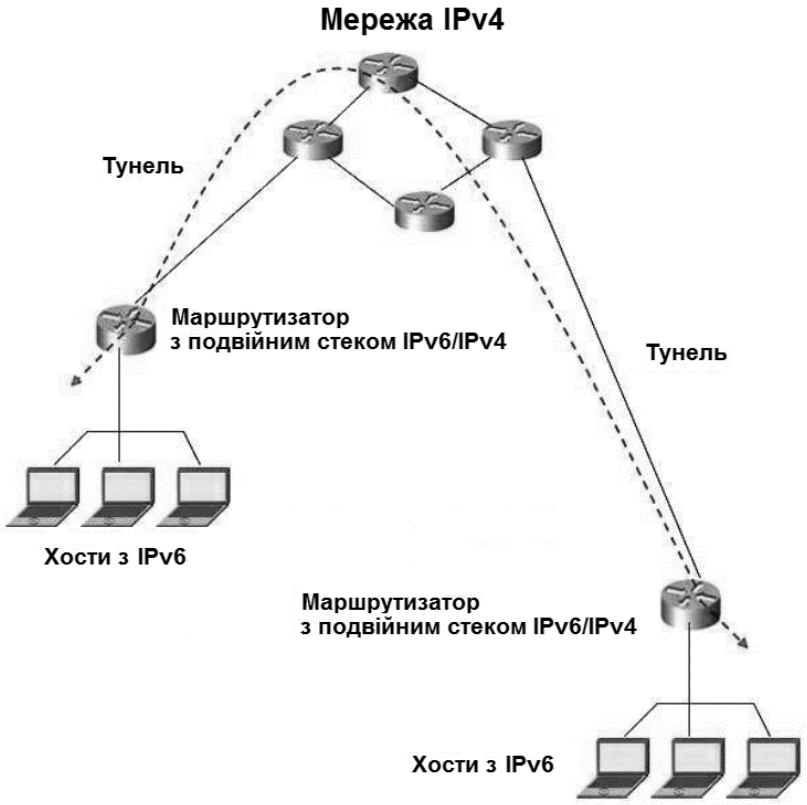

Рисунок 3.6 — Приклад тунелю виду маршрутизатор — маршрутизатор

Для того щоб автоматичне тунелювання було можливим, необхідно, щоб IPv6-адреси були сумісними з IPv4. Фактично вони повинні утворюватися з адрес IPv4 шляхом додавання зліва 96 нульових бітів.

Коли кінцева точка тунелю (маршрутизатор) не визначається за адресою цільового вузла, доводиться використовувати заздалегідь сконфігуроване тунелювання.

У цьому випадку параметри тунелю задаються маршрутною таблицею в інкапсулюючому вузлі.

Такий підхід застосовується, коли цільова адреса не є сумісною з IPv4. У такому разі відправник повинен знати IPv4-адресу маршрутизатора з подвійним стеком, який здатен організувати доставку IPv6-пакета. Обидва кінці тунелю (як автоматичного, так і сконфігурованого) повинні мати IPv4-сумісні адреси.

Можливі три ситуації залежно від того, якою є кінцева адреса:

— кінцева адреса є IPv6-адресою;

— кінцева адреса є IPv4-адресою;

— кінцева адреса є IPv6-адресою, сумісною з IPv4.

Блок-схема IPv6-тунелювання, при якому кінцевою адресою є адреса протоколу IPv6 представлена на (рис. 3.7).

Основними технологіями, які застосовуються для забезпечення взаємодії мереж IPv4 і IPv6, є тунелювання (інкапсуляція) та мультиплексування.

До основних недоліків технології мультиплексування можна віднести:

— складність адміністрування та контролю доступу;

— потребу в додаткових ресурсах через високу надлишковість, особливо якщо потрібно встановити кілька стеків для доступу до різних мереж;

— для реалізації підтримки кількох стеків необхідні відповідні інфраструктурні сервіси.

До переваг мультиплексування належать:

— досить проста процедура перемикання між протоколами;

— надійність, оскільки при відмові стека на одному з комп’ютерів доступ до ресурсів іншої мережі буде можливий за допомогою протоколів, встановлених на інших комп’ютерах.

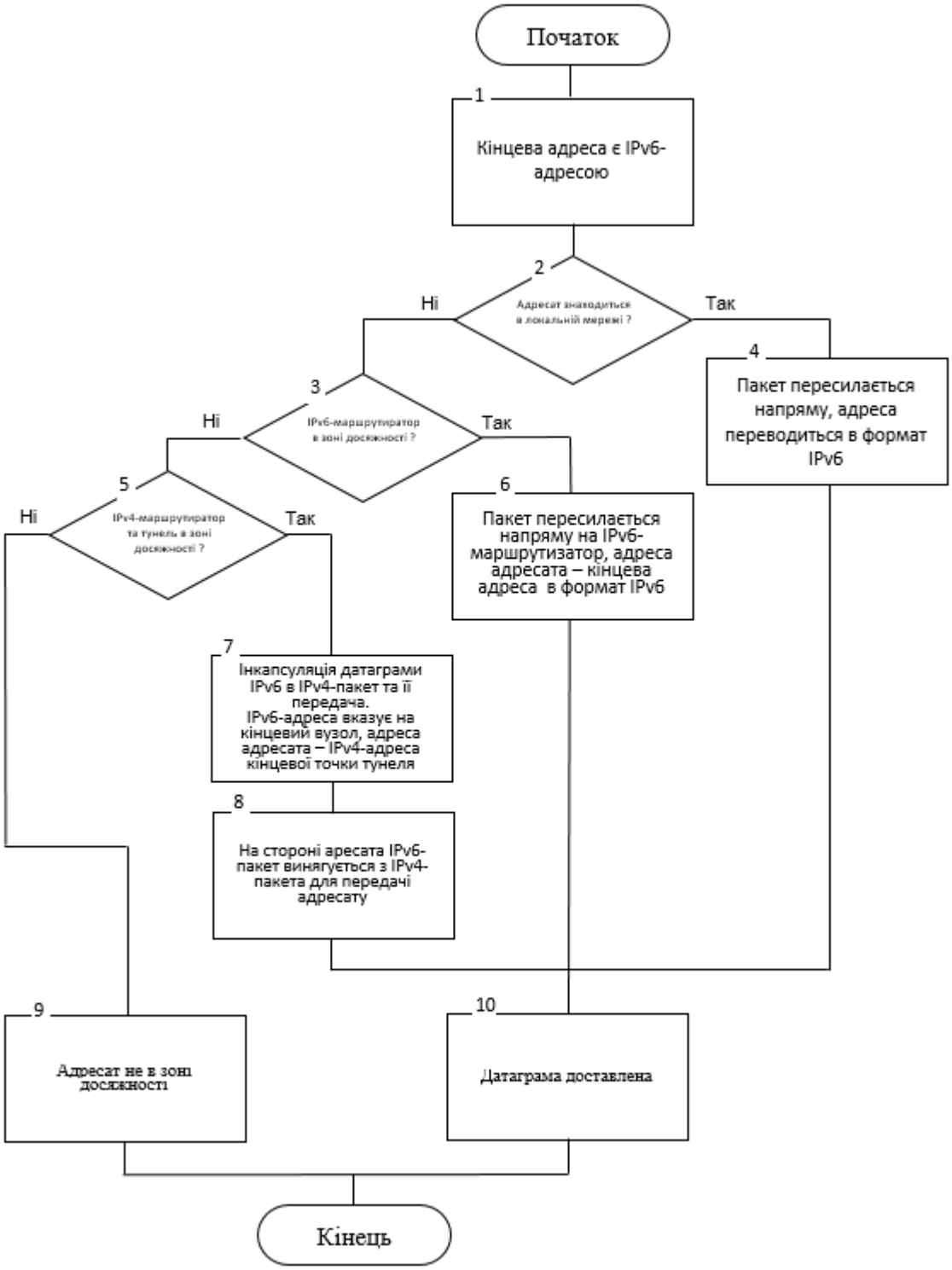

Рисунок 3.7 — Блок-схема IPv6-тунелювання, при якому кінцевою адресою є адреса протоколу IPv6

Блок-схема IPv6-тунелювання, при якому кінцевою адресою є адреса протоколу IPv4 показана на рисунку 3.8

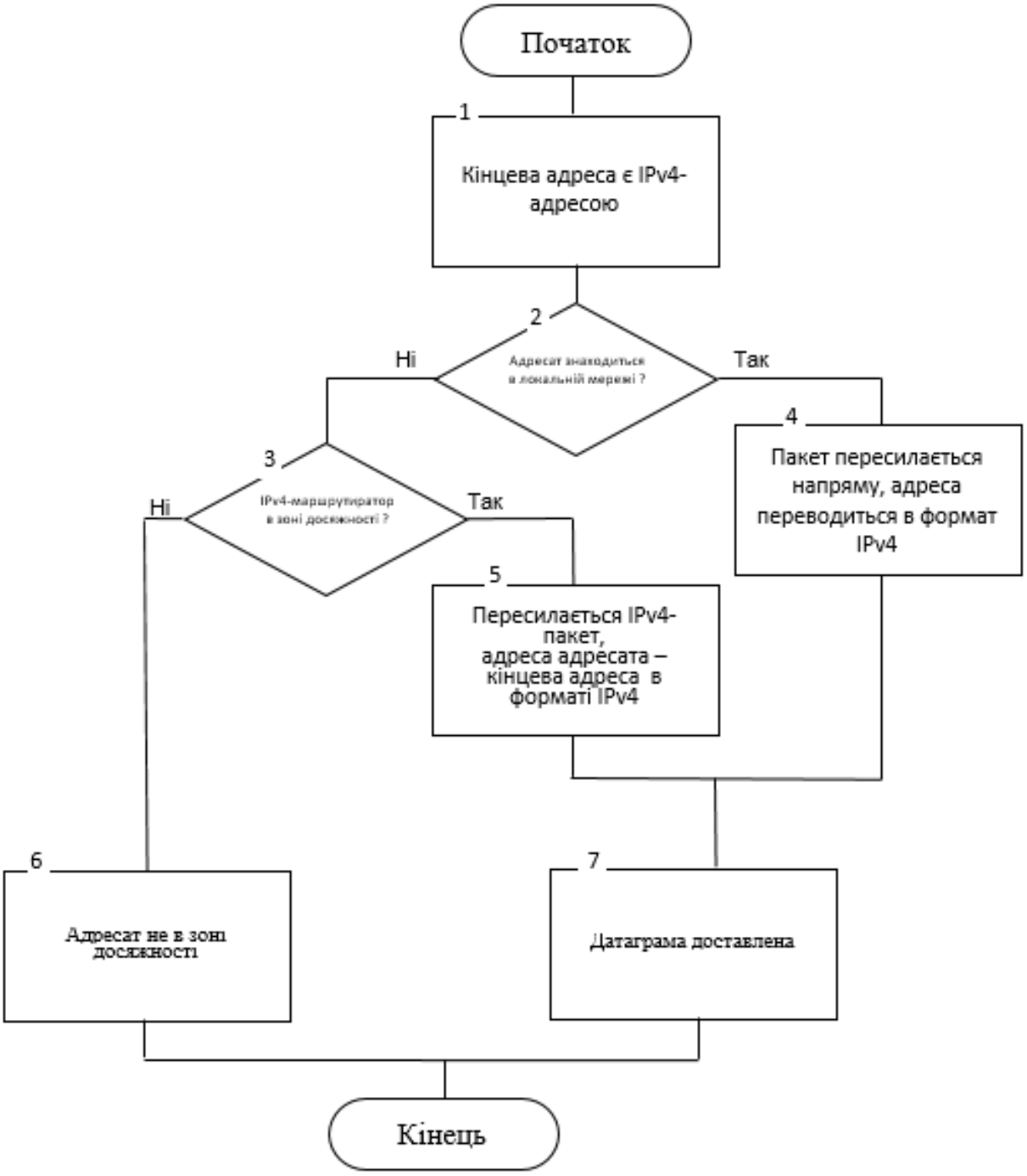

Рисунок 3.8 — Блок-схема IPv6-тунелювання, при якому кінцевою адресою є адреса протоколу IPv4

Блок-схема IPv6-тунелювання, при якому кінцевою адресою є адреса протоколу IPv6, що сумісна з адресою IPv4 показана на (рис. 3.9).

Застосування технології мультиплексування вимагає значних ресурсних витрат, оскільки на всіх вузлах встановлюється відповідне програмне забезпечення, яке дозволяє підтримувати стеки протоколів IPv4 і IPv6.

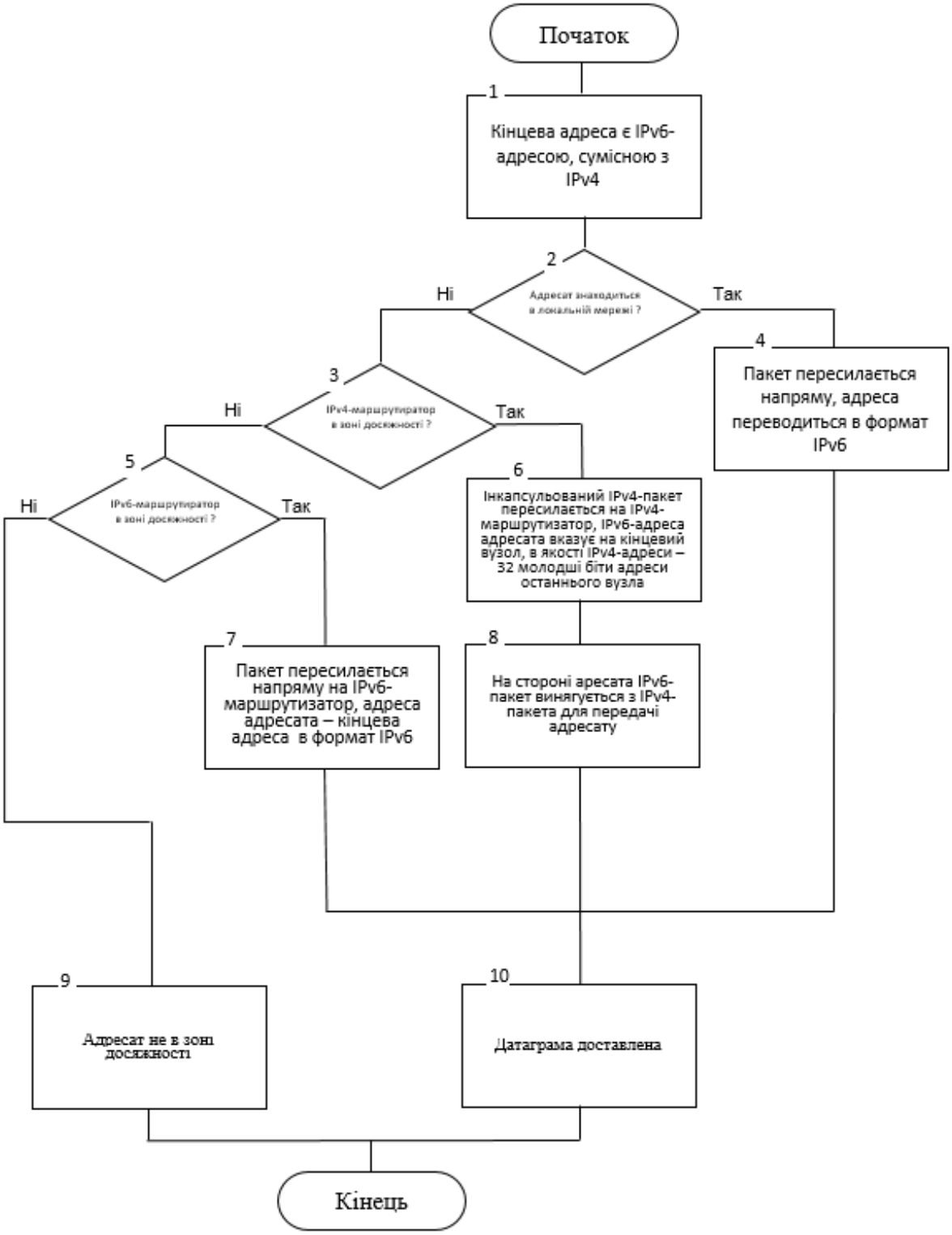

Рисунок 3.9 — Блок-схема IPv6-тунелювання, при якому кінцевою адресою є адреса протоколу IPv6, що сумісна з адресою IPv4

3.3 Оптимізація засобів розгортання інфраструктури IPv6 в комп’ютерній корпоративній мережі

Для того, щоб подвійний стек працював належним чином, необхідно, щоб

майже всі проміжні маршрутизатори глобальної мережі підтримували як протокол IPv4, так і IPv6.

Також мінусом цієї технології є те, що встановлення спеціального програмного забезпечення на вузлах потребує значних часових і матеріальних витрат. Крім того, використання цього механізму збільшує навантаження на системні ресурси вузлів мережі, що може сповільнювати їхню роботу.

Втім, ситуацію можна виправити — необхідно, щоб виробники мережевого апаратного та програмного забезпечення внесли у свої продукти зміни, які дозволять їм працювати з обома версіями протоколу IP. Однак це потребує дуже великих фінансових витрат, тому не факт, що виробники погодяться на такі зміни.

Перевага технології мультиплексування полягає у її відносній простоті та надійності. Якщо на одному з комп'ютерів стек вийде з ладу, все одно залишиться можливість підключення до ресурсів іншої мережі за допомогою протоколів, налаштованих на інших комп'ютерах. Надійність є важливим чинником.

Другою з основних технологій, що застосовуються для організації взаємодії мереж IPv4 і IPv6, є технологія тунелювання.

Основні переваги технології тунелювання:

— пакети IPv6 інкапсулюються в пакети IPv4, які займають менший обсяг (це допомагає вирішити проблему обмеженої пропускної здатності);

— забезпечується можливість взаємодії між мережами IPv6 через мережі IPv4;

— відсутня потреба у придбанні додаткового програмного забезпечення для кожного вузла.

Під час використання технології тунелювання відпадає необхідність витрачати значну кількість часу та ресурсів, як це має місце у випадку мультиплексування, на встановлення й налаштування додаткового програмного забезпечення на кожному окремому мережевому вузлі. Тунелювання передбачає інкапсуляцію пакетів одного протоколу в пакети іншого, що дозволяє передавати трафік IPv6 через існуючу інфраструктуру IPv4 без кардинальних змін у конфігурації всієї мережі.

4 ВПРОВАДЖЕННЯ ІНФРАСТРУКТУРИ IPV6 В КОРПОРАТИВНУ КОМП'ЮТЕРНУ МЕРЕЖУ

4.1 Розробка структури корпоративної мережі компанії для впровадження стандарту IPv6

У мережах з відносно невеликою кількістю комп'ютерів, як правило від 10 до 30 робочих

станцій, найчастіше застосовуються класичні або типові топології побудови мережі, такі як загальна шина, кільце, зірка або повнозв'язна топологія. Кожна з цих топологій має свої особливості організації з'єднань між вузлами, однак усі вони є достатньо простими в реалізації та не потребують складного мережевого обладнання, що робить їх доцільними для використання в невеликих офісах, навчальних лабораторіях або домашніх мережах.

Спільною рисою перелічених топологій є їхня однорідність, тобто всі комп'ютери в такій мережі мають однакові права щодо доступу до мережевих ресурсів і взаємодії з іншими вузлами. Це означає відсутність жорсткої ієрархії між комп'ютерами та рівноправну участь кожного з них у процесі обміну даними. Винятком може бути топологія зірка, у якій центральний комп'ютер або мережевий пристрій (комутатор чи сервер) виконує керівну або розподільчу функцію, однак і в цьому випадку кінцеві вузли залишаються рівноправними щодо доступу до мережі.

Однорідність структури таких мереж значно спрощує їх масштабування, оскільки додавання нових комп'ютерів не потребує суттєвих змін у конфігурації всієї системи. Крім того, це полегшує процес технічного обслуговування та експлуатації мережі, зменшує витрати часу на пошук і усунення несправностей, а також підвищує загальну надійність функціонування. Завдяки цим перевагам прості топології залишаються актуальними та широко використовуються у невеликих комп'ютерних мережах.

Наше підприємство має чітко визначену організаційну структуру та складається з чотирьох основних відділів: керівного підрозділу на чолі з

директором, бухгалтерії, відділу програмного забезпечення та відділу роботи з клієнтами. Кожен із цих відділів виконує власні функції та має специфічні вимоги до використання інформаційних ресурсів і доступу до мережі. Для забезпечення повсякденної діяльності підприємства використовується один ноутбук і сім стаціонарних комп'ютерів, а також периферійне обладнання, зокрема два принтери. Мережева інфраструктура включає два комутатори (свічі) та три маршрутизатори, що забезпечують з'єднання між окремими сегментами мережі та доступ до зовнішніх ресурсів.

У процесі проєктування та експлуатації корпоративної мережі однією з найбільш важливих і складних проблем є перерозподіл мережевого трафіка між різними фізичними сегментами. Ця проблема не може бути повністю розв'язана лише шляхом фізичної структуризації мережі, наприклад, поділом обладнання між різними комутаторами або використанням окремих ліній зв'язку. За відсутності логічного поділу мережі надлишковий трафік може поширюватися на всі сегменти, знижуючи загальну продуктивність і ефективність роботи мережі.

У міру зростання мережі підприємства виникає неоднорідність інформаційних потоків, оскільки мережа починає складатися з кількох підмереж, що відповідають робочим групам, відділам або іншим адміністративним одиницям. Як правило, найбільш інтенсивний обмін даними відбувається між комп'ютерами, що належать до одного відділу або підмережі, наприклад, під час спільної роботи з документами, обміну внутрішньою інформацією чи доступу до локальних сервісів. Водночас лише незначна частина мережевих запитів спрямована до ресурсів, розміщених за межами локальних робочих груп.

Така особливість розподілу трафіка зумовлює необхідність застосування логічної сегментації мережі, наприклад за допомогою віртуальних локальних мереж (VLAN) та маршрутизації між ними. Це дозволяє оптимізувати використання мережевих ресурсів, зменшити навантаження на окремі сегменти, підвищити рівень безпеки та забезпечити стабільну й ефективну роботу мережевої інфраструктури підприємства в цілому.

Для розробки моделі комп’ютерної мережі в межах даного проєкту було використано програмне забезпечення Cisco Packet Tracer, яке є одним із найпоширеніших навчальних та проєктних інструментів у сфері комп’ютерних мереж. Дане програмне середовище широко застосовується для проєктування, моделювання та тестування мережевих рішень різної складності без необхідності використання реального фізичного обладнання, що значно знижує витрати та спрощує процес експериментування.

Програмне рішення Cisco Packet Tracer надає можливість імітувати роботу широкого спектра мережевих пристроїв, зокрема маршрутизаторів, комутаторів, точок бездротового доступу, персональних комп’ютерів, серверів, мережевих принтерів, IP-телефонів та інших елементів мережевої інфраструктури. Це дозволяє створювати як прості локальні мережі, так і складні ієрархічні топології, що складаються з десятків і навіть сотень пристроїв. Робота з інтерактивним симулятором забезпечує максимально наближене до реальних умов відчуття налаштування та адміністрування мережі.

Процес конфігурації мережевих пристроїв у Cisco Packet Tracer залежить від їх типу та функціонального призначення. Частина обладнання налаштовується за допомогою команд операційної системи Cisco IOS, що дозволяє відпрацьовувати практичні навички роботи з командним рядком і вивчати принципи конфігурації реальних пристроїв Cisco. Інші пристрої можуть бути налаштовані за допомогою графічного веб-інтерфейсу або спеціалізованих меню, що робить програму зручною для користувачів з різним рівнем підготовки.

Важливою перевагою Cisco Packet Tracer є наявність режиму візуалізації, який дає змогу в реальному часі відстежувати переміщення даних у мережі. Користувач може спостерігати за проходженням IP-пакетів між вузлами, аналізувати зміну їхніх параметрів при проходженні через маршрутизатори та комутатори, а також оцінювати швидкість передачі даних і маршрути їх поширення. Такий підхід значно полегшує розуміння принципів роботи мережевих протоколів і механізмів маршрутизації.

Аналіз подій, що відбуваються в мережі під час моделювання, дозволяє не лише детально вивчити логіку її функціонування, а й своєчасно виявляти помилки конфігурації, вузькі місця та можливі несправності. Таким чином, використання Cisco Packet Tracer є ефективним інструментом для проєктування, навчання та дослідження комп'ютерних мереж, а також для перевірки коректності прийнятих технічних рішень перед їх реальним впровадженням.

Для побудови моделі мережі в середовищі Cisco Packet Tracer необхідно за допомогою миші перетягнути потрібні мережеві пристрої на робоче поле симулятора. До таких пристроїв належать маршрутизатори, комутатори, персональні комп'ютери, сервери, принтери та інші елементи мережевої інфраструктури. Після розміщення обладнання на робочому полі встановлюються необхідні логічні та фізичні зв'язки між пристроями з використанням відповідної піктограми з'єднань. При цьому користувач може обирати тип кабелю або бездротового з'єднання залежно від характеристик пристроїв і вимог до мережі.

Одним із суттєвих недоліків даної системи є обмеження щодо використання обладнання лише фірми Cisco. Це означає, що під час проєктування неможливо безпосередньо моделювати роботу мережевих пристроїв інших виробників, що дещо звужує можливості симулятора з точки зору універсальності. Проте, зважаючи на широке поширення обладнання Cisco в реальних мережах, дана особливість не є критичною для більшості навчальних і проєктних завдань.

Водночас Cisco Packet Tracer успішно дозволяє створювати навіть складні макети мереж, що включають велику кількість пристроїв, різноманітні топології та багаторівневу ієрархію. Симулятор дає змогу перевіряти працездатність спроєктованих топологій, тестувати налаштування мережевих протоколів, маршрутизації, VLAN та інших механізмів до їх впровадження в реальному середовищі.

Згідно з описом, створимо логічну структуру мережі, в якій відділи підприємства розміщені в окремих віртуальних локальних мережах (VLAN) та відповідних підмережах (рис. 4.1).

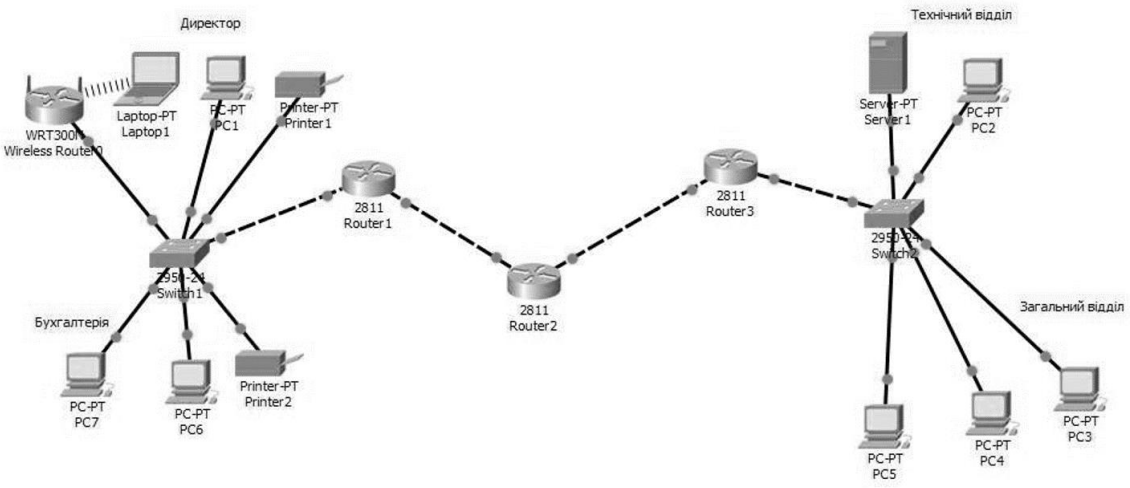

Рисунок 4.1 — Структура мережі в Cisco Packet Tracer

Такий підхід забезпечує логічну сегментацію мережі, підвищує рівень безпеки та оптимізує розподіл мережевого трафіку. Запроєктована локальна структура повністю відповідає логічній організації підприємства: наявні чотири відділи, які з’єднані між собою за допомогою двох комутаторів, а маршрутизація між підмережами здійснюється трьома роутерами. Це рішення дозволяє ефективно керувати потоками даних, зменшувати навантаження на мережу та забезпечувати стабільну роботу всіх структурних підрозділів підприємства.

У відділі директора використовується ноутбук як основний робочий пристрій, що забезпечує мобільність та зручність у повсякденній роботі. Ноутбук підключений до бездротової точки доступу Wi-Fi, яка інтегрована в загальну мережеву інфраструктуру підприємства. Таке рішення дозволяє директору мати постійний доступ до корпоративних ресурсів незалежно від фізичного розташування в межах офісу, а також оперативно підключатися до мережі під час проведення нарад або роботи з документами.

Через точку доступу Wi-Fi ноутбук отримує вихід до локальної мережі підприємства та до глобальної мережі Інтернет. Це забезпечує можливість користування електронною поштою, хмарними сервісами, системами управління підприємством, а також доступ до зовнішніх інформаційних ресурсів. Бездротове підключення спрощує мережеву інфраструктуру відділу директора, оскільки

зменшує потребу у прокладанні додаткових кабельних ліній і підвищує гнучкість організації робочого місця (рис. 4.2).

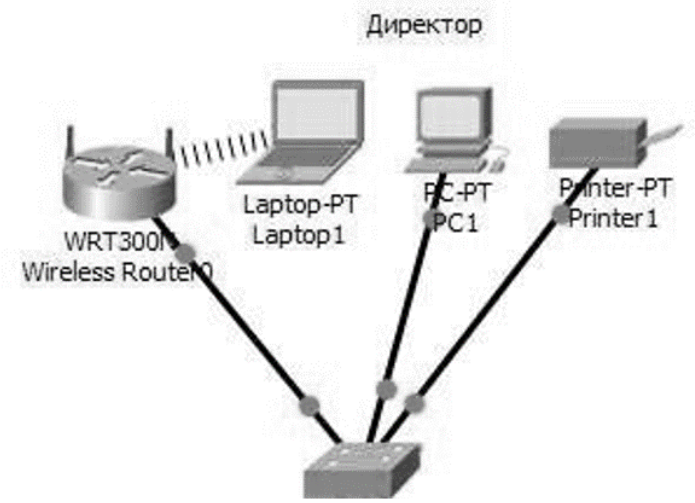

Рисунок 4.2 — Структура мережі кабінету директора з точкою доступу WI-FI

Для правильної роботи мережі в кабінеті директора необхідно налаштувати маршрутизатор Wi-Fi ASUS BRT-AC828 так, як показано рисунку 4.3.

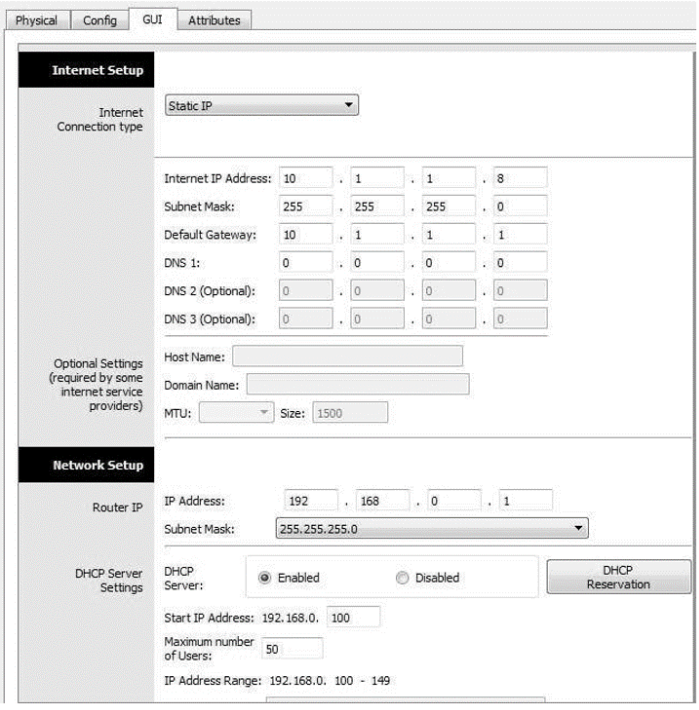

Рисунок 4.3 — Основні налаштування маршрутизатора ASUS BRT-AC828

Всі пристрої, які призначені для користувачів в корпоративній мережі повинні мати обліковий запис з обмеженим функціоналом.

4.2 Вибір технології впровадження інфраструктури IPv6 в корпоративну комп’ютерну мережу

Протокол IP є фундаментальною основою функціонування сучасного Інтернету та корпоративних мереж, тому його надзвичайно широке поширення робить планомірну і повну заміну четвертої версії на шосту складним і багатоетапним процесом. Протокол IPv4 використовується впродовж десятиліть і лежить в основі величезної кількості мережевих пристроїв, програмного забезпечення та сервісів, що унеможливлює його швидке виведення з експлуатації без суттєвих фінансових і технічних витрат. Перехід на IPv6 потребує модернізації обладнання, оновлення програмного забезпечення, а також підготовки кваліфікованих фахівців, здатних працювати з новими мережевими технологіями.

Саме з цієї причини були розроблені спеціальні перехідні технології, які, не будучи безпосередньою частиною базової специфікації IPv6, забезпечують можливість одночасного використання обох версій протоколу IP у глобальних і локальних мережах. Такі технології дозволяють мережам IPv4 та IPv6 співіснувати, взаємодіяти між собою та забезпечувати безперервність доступу до мережевих ресурсів у перехідний період. Серед них можна виділити механізми dual-stack, тунелювання та трансляції адрес, які надають змогу поступово впроваджувати IPv6 без порушення стабільної роботи наявної інфраструктури.

Застосування подібних підходів дозволяє організаціям гнучко планувати перехід на протокол нового покоління, мінімізувати ризики та фінансові витрати, а також забезпечити сумісність між старими і новими мережевими сегментами. У результаті перехід від IPv4 до IPv6 відбувається еволюційно, без різких змін, що є критично важливим для стабільного розвитку глобальної мережі Інтернет і корпоративних інформаційних систем.

У таблиці 4.1 наведено відомості про технології, що застосовуються для переходу з протоколу IPv4 на протокол IPv6, а також їхні різновиди та особливості взаємодії між ними.

Таблиця 3.1 — Взаємодія технологій впровадження протоколу IPv6

Технологія	Вид технології	Опис
1	2	3
Подвійний стек	-	Підтримка обох протоколів одночасно
Тунелювання	MCT	Тунель створюється та конфігурується вручну; передавання IPv6-пакетів через мережу IPv4, як правило, між маршрутизаторами.
Тунелювання	6to4	Автоматичне визначення кінцевих точок тунелю та передавання пакетів IPv6 через мережу IPv4, як правило між маршрутизаторами.
Тунелювання	ISATAP	Автоматичне визначення кінцевих точок тунелю; передавання IPv6-пакетів через мережу IPv4, зазвичай між маршрутизаторами; не функціонує за наявності налаштованого IPv4 NAT.
Тунелювання	Teredo	Тунель, як правило, налаштовується між хостами; при цьому хост формує IPv6-пакет і інкапсулює його в заголовок IPv4; технологія коректно працює навіть за наявності налаштованого IPv4 NAT.
Трансляція	-	Маршрутизатор виконує трансляцію заголовків пакетів з IPv6 у IPv4 і у зворотному напрямку, забезпечуючи взаємодію пристроїв, що працюють за протоколом IPv6, з мережами та вузлами IPv4.

Для впровадження протоколу IPv6 в існуючу корпоративну мережу оберемо технологію 6to4.

На сьогоднішній день у світі сформувалася досить розгалужена та масштабна інфраструктура мереж, що працюють на основі протоколу IPv4. Ці мережі продовжують активно використовуватися й надалі, оскільки більшість існуючих інтернет-провайдерів, сервісів та мережевого обладнання історично були побудовані саме на цій версії протоколу IP. Навіть у випадку, коли підприємство приймає рішення про побудову власної корпоративної мережі з

використанням виключно протоколу IPv6 на мережному рівні, на практиці може виникнути ситуація, коли всі доступні в регіоні провайдери інтернет-послуг підтримують лише IPv4. У такому разі пряме підключення до глобальної мережі IPv6 стає неможливим без використання додаткових технічних рішень.

Таким чином, для забезпечення доступу до ресурсів IPv6 та взаємодії між IPv6-мережами виникає необхідність використання наявної інфраструктури IPv4. Саме з цією метою були розроблені спеціальні механізми переходу, які дозволяють забезпечити сумісну роботу двох версій протоколу IP. Дані механізми дають змогу передавати IPv6-трафік через IPv4-мережі, зберігаючи працездатність існуючих систем і забезпечуючи поступовий, поетапний перехід до протоколу нового покоління без кардинальної перебудови всієї мережевої інфраструктури.

Однією з таких технологій переходу є 6to4, яка дозволяє передавати IPv6-пакети через IPv4-канали без необхідності попереднього налаштування статичних або обопільних тунелів між кінцевими вузлами. Принцип роботи 6to4 ґрунтується на автоматичному створенні тунелів і використанні спеціального формату IPv6-адрес, що містять у собі IPv4-адресу вузла. Завдяки цьому IPv6-пакети можуть інкапсулюватися в IPv4-пакети та передаватися через існуючу IPv4-інфраструктуру.

Технологія 6to4 зазвичай застосовується у випадках, коли кінцевий користувач або організація бажають отримати доступ до IPv6-Інтернету, але не мають прямої підтримки IPv6 з боку свого інтернет-провайдера. Вона дозволяє тимчасово вирішити проблему сумісності та забезпечити доступ до ресурсів IPv6, використовуючи наявні IPv4-канали. Таким чином, 6to4 виступає як проміжне рішення, що полегшує перехід до IPv6 та сприяє поступовому впровадженню протоколу нового покоління в глобальних мережах.

Технологія 6to4 виконує низку ключових функцій, необхідних для забезпечення взаємодії між мережами IPv6 та IPv4. По-перше, вона автоматично виділяє кожному хосту або маршрутизатору, що має глобальну IPv4-адресу, префікс IPv6 розміром /48, який може використовуватися для побудови власної

IPv6-підмережі. По-друге, 6to4 забезпечує інкапсуляцію IPv6-пакетів у IPv4-пакети, що дозволяє передавати трафік IPv6 через існуючу IPv4-інфраструктуру без її модифікації. По-третє, дана технологія надає можливість обміну даними між вузлами, які використовують механізм 6to4, та вузлами з нативною підтримкою IPv6.

У найпростішому сценарії кілька мереж починають використовувати протокол IPv6 паралельно з IPv4, застосовуючи механізм 6to4 для організації IPv6-зв'язку між собою. Для цього на одному з маршрутизаторів кожної такої мережі одночасно налаштовуються протоколи IPv4 та IPv6, після чого активується механізм 6to4. Важливою умовою є наявність у цього маршрутизатора щонайменше однієї глобальної IPv4-адреси, а також доступність його для IPv6-вузлів локальної мережі.

З'єднання між внутрішніми вузлами мережі та маршрутизатором 6to4 може реалізовуватися різними способами: за допомогою внутрішньої IPv6-інфраструктури, через комбіновані маршрутизатори IPv4/IPv6 або з використанням інших механізмів тунелювання. Такий підхід дозволяє організаціям поступово впроваджувати IPv6, зберігаючи сумісність із наявними IPv4-мережами та забезпечуючи безперервність мережевих сервісів.

На рисунку 4.4 наведено реалізації тунелю IPv6-to-IPv4 за технологією 6 to 4, який наочно демонструє механізм взаємодії мереж різних поколінь.

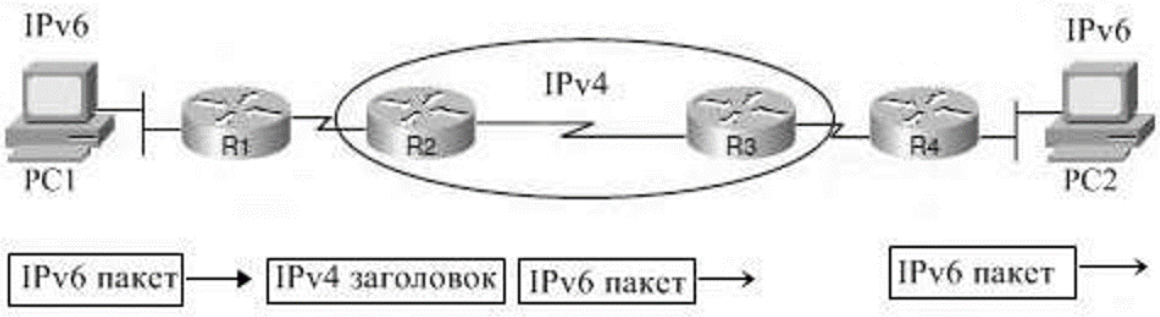

Рисунок 4.4 — Організація тунелю IPv6to IPv4

У даному сценарії хости, що розташовані в окремих підмережах, уже перейшли на використання протоколу IPv6, тоді як транзитна мережа між ними

все ще функціонує на основі протоколу IPv4. Подібна ситуація є доволі поширеною на початкових етапах впровадження IPv6, зокрема під час тестування нового протоколу в межах підприємства або у випадку, коли кінцевий користувач прагне перейти на IPv6, але його інтернет-провайдер підтримує лише IPv4.

У процесі передавання даних IPv6-хост формує та надсилає IPv6-пакет, адресований вузлу в іншій IPv6-підмережі. Оскільки між цими підмережами розташована IPv4-мережа, прикордонний маршрутизатор R1 виконує інкапсуляцію IPv6-пакета в IPv4-заголовок. При цьому як адресу призначення в IPv4-заголовку зазначається глобальна IPv4-адреса маршрутизатора R4, який є кінцевою точкою тунелю.

Далі інкапсульований пакет передається через проміжні маршрутизатори R2 і R3, які обробляють його як звичайний IPv4-трафік, не аналізуючи вкладений IPv6-вміст. Завдяки цьому забезпечується прозоре транспортування IPv6-пакетів через мережу, що не підтримує протокол нового покоління. Після надходження пакета до маршрутизатора R4 відбувається процес декапсуляції: IPv4-заголовок видаляється, а оригінальний IPv6-пакет відновлюється.

На завершальному етапі маршрутизатор R4 пересилає IPv6-пакет безпосередньо до хоста PC2, який працює в IPv6-мережі. Таким чином, механізм тунелювання дозволяє забезпечити повноцінний обмін даними між IPv6-вузлами навіть за умови наявності між ними мережевої інфраструктури, що базується виключно на IPv4. Це робить IPv6-to-IPv4 тунелі ефективним і практичним рішенням для поетапного переходу до IPv6 без необхідності негайної модернізації всієї мережі.

Технологія 6to4 має низку переваг порівняно з іншими механізмами тунелювання IPv6. По-перше, для її використання не потрібна попередня реєстрація, а процес налаштування відзначається високою швидкістю та відносною простотою конфігурування. По-друге, забезпечується безпосередній IPv6-зв’язок між будь-якими двома вузлами без використання проміжних елементів, таких як шлюзи або спеціалізовані тунельні сервери. Крім того, вибір

шлюзу, через який здійснюється передавання пакетів до інших IPv6-користувачів, відбувається автоматично, без участі адміністратора мережі.

Водночас саме автоматичний вибір найближчого шлюзу може розглядатися як недолік даної технології, оскільки він не дозволяє явно контролювати маршрут передавання трафіку та може призводити до використання не завжди оптимальних шляхів.

4.3 Аналіз результатів впровадження інфраструктури IPv6 в корпоративну комп'ютерну мережу

Під час експериментального розгортання мережі встановлено, що технологія 6to4 дозволяє організувати IPv6-з'єднання між віддаленими сегментами мережі через IPv4-канали без необхідності ручного налаштування тунелів між кожною парою вузлів. Інкапсуляція IPv6-пакетів в IPv4 забезпечує прозору передачу даних через існуючу інфраструктуру та не потребує суттєвих змін у конфігурації проміжних маршрутизаторів, що працюють виключно з IPv4.

Аналіз результатів маршрутизації показав, що обмін даними між IPv6-хостами відбувається коректно, а процес інкапсуляції та декапсуляції пакетів на прикордонних маршрутизаторах не призводить до втрати даних. При цьому було зафіксовано незначне збільшення затримки передачі пакетів, що є наслідком додаткової обробки заголовків, однак цей вплив не є критичним для більшості корпоративних сервісів, таких як доступ до внутрішніх ресурсів, вебсервісів і файлових серверів.

Швидкість передавання пакетів є одним із ключових параметрів функціонування будь-якої комп'ютерної мережі. Процес з'єднання комп'ютерів за допомогою каналів зв'язку для обміну даними називається методом комутації. У разі пакетної комутації всі повідомлення, що передаються користувачами мережі, на вихідному вузлі поділяються на відносно невеликі фрагменти — пакети. Довжина повідомлень може бути довільною: від кількох байтів до десятків мегабайт, тоді як розмір пакетів зазвичай обмежений певним діапазоном, наприклад від 46 до 1500 байт.

Кожен пакет містить заголовок, у якому зберігається адресна інформація, необхідна для доставки даних до вузла призначення, а також службові поля, зокрема порядковий номер пакета. Цей номер використовується на приймальному боці для коректного збирання початкового повідомлення з окремих фрагментів. У процесі передавання пакети розглядаються мережею як незалежні інформаційні одиниці.

Комутатори мережі приймають пакети від кінцевих пристроїв і, керуючись адресною інформацією, передають їх далі через проміжні вузли до кінцевого отримувача. Такий підхід забезпечує ефективне використання пропускної здатності мережі та підвищує її надійність.

Для коректної роботи в таких мережах комп’ютер повинен мати IP-адреси обох версій — IPv4 та IPv6, що демонструється на рисунку 4.5. Комп’ютер PC1 налаштований з IPv4-адресою 10.1.1.2 із маскою підмережі 255.255.255.0 та шлюзом 10.1.1.1, а також з IPv6-адресою 2001:1:1:1::2 з довжиною префікса /64 і шлюзом 2001:1:1:1::1. Така конфігурація забезпечує підтримку роботи в мережах обох протоколів і дозволяє використовувати механізми їхньої сумісної взаємодії.

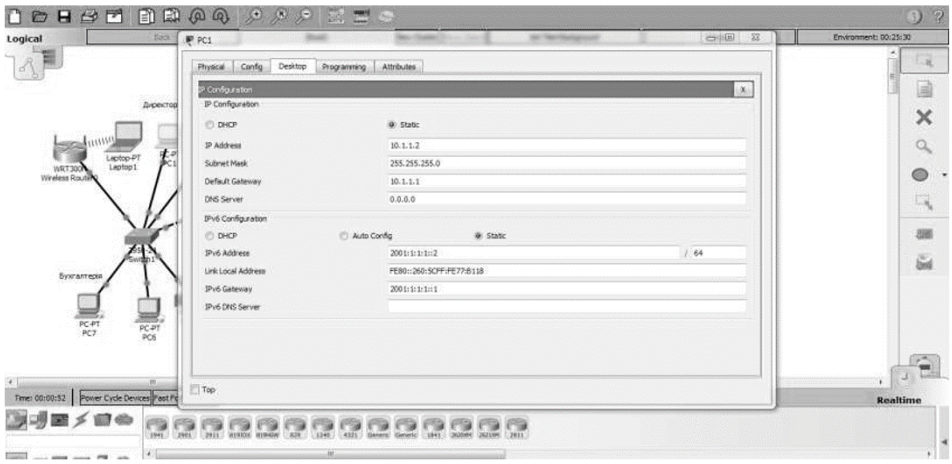

Рисунок 4.5 — Мережеві налаштування комп’ютера в Packet Tracer

Програма Cisco Packet Tracer надає можливість вимірювати та аналізувати швидкість передачі пакетів у змодельованій мережі за допомогою спеціальної панелі симуляції (рис. 4.6). Даний режим роботи дозволяє не лише спостерігати за процесом передавання даних у реальному часі, а й детально відстежувати

проходження окремих пакетів між вузлами мережі, фіксувати затримки, черги обробки та часові характеристики доставки.

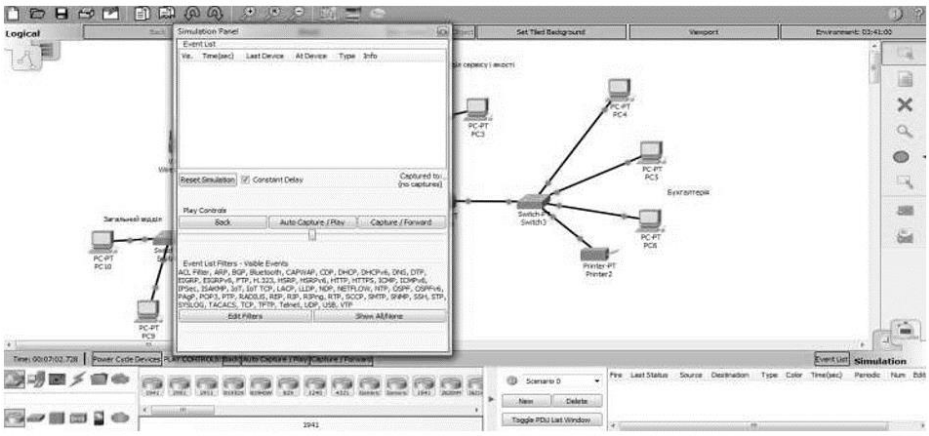

Рисунок 4.6 — Симуляція передачі пакетів в Packet Tracer

Використовуючи інструменти симуляції Packet Tracer, було виконано серію замірів швидкості передачі пакетів у мережі, що функціонує на основі протоколу IPv4, а також у мережі з використанням IPv6. Для отримання об’єктивних результатів вимірювання проводилися за однакових умов: із застосуванням тієї ж топології, однакового мережевого обладнання та аналогічних сценаріїв передавання даних. Це дозволило коректно порівняти показники продуктивності обох протоколів.

На рисунку 4.7 наведено дані про швидкість передачі інформаціних пакетів для потоколу версії IPv4.

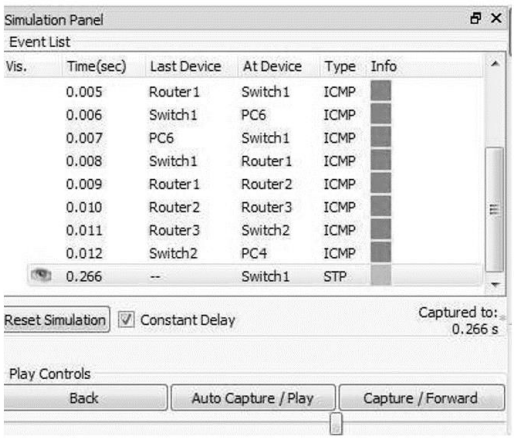

Рисунок 4.7 — Швидкість передачі пакетів для протоколу версії IPv4 в Packet Tracer

Даний сервіс симуляції в програмі Cisco Packet Tracer надає можливість детального аналізу процесу передавання даних у мережі. Зокрема, він дозволяє вимірювати час проходження пакета через кожен мережевий пристрій, визначати тип переданого пакета, а також відстежувати послідовність його маршруту від вузла-джерела до вузла-призначення. Такий підхід є надзвичайно корисним для оцінки продуктивності мережі та виявлення потенційних «вузьких місць» у її роботі.

У ході експерименту було здійснено передавання пакетів з комп'ютера PC4 до комп'ютера PC6. Пакети проходили через низку мережевих пристроїв, а саме: Switch2, Router3, Router2, Router1 та Switch1. Для кожного з цих елементів фіксувався час обробки та пересилання пакета, що дало змогу отримати повну картину затримок у мережі. За результатами вимірювань загальний час передачі пакета склав 0,145 с, що свідчить про стабільну та коректну роботу налаштованої інфраструктури.

Окрему увагу було приділено аналізу швидкості передавання пакетів у мережі з використанням протоколу IPv6. На рисунку 4.8 наведено результати вимірювань, які демонструють характеристики передавання IPv6-пакетів у змодельованій мережі.

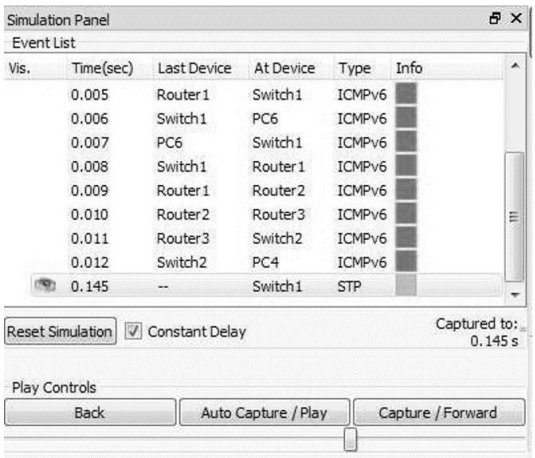

Рисунок 4.8 — Швидкість передачі пакетів для протоколу версії IPv6 в Packet Tracer

5 ЕКОНОМІЧНА ЧАСТИНА

5.1 Проведення комерційного та технологічного аудиту розробки засобів розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі

Актуальність проведення комерційного та технологічного аудиту розробки засобів розгортання інфраструктури IPv6 у корпоративній комп'ютерній мережі зумовлена глобальним переходом від протоколу IPv4 до IPv6. Вичерпання адресного простору IPv4, зростання кількості підключених пристроїв та підвищені вимоги до безпеки роблять перехід на IPv6 стратегічно важливим для будь-якої сучасної організації. Оцінка доцільності та готовності до впровадження IPv6 дозволяє підприємству мінімізувати ризики, пов'язані з сумісністю обладнання, відмовостійкістю мережі та подальшими фінансовими витратами.

Комерційний аудит у цьому контексті покликаний визначити економічну ефективність впровадження IPv6-інфраструктури. Він дозволяє порівняти вартість модернізації з очікуваними вигодами, серед яких — зниження експлуатаційних витрат, підвищення продуктивності мережі, покращення масштабованості та безпеки, а також відповідність міжнародним стандартам. Такий аудит допомагає сформувати обґрунтований бізнес-план переходу, включаючи терміни окупності та потенційні комерційні переваги для підприємства.

Технологічний аудит спрямований на визначення технічного стану існуючої мережевої інфраструктури, її сумісності з IPv6 та оцінки готовності апаратного й програмного забезпечення. Він включає аналіз маршрутизаторів, комутаторів, систем управління, політик безпеки та мережевих сервісів. Результати такого аудиту дозволяють виявити "вузькі місця", спрогнозувати потребу в модернізації обладнання, розробити поетапний план впровадження IPv6 та забезпечити надійний перехід без переривання бізнес-процесів.

Метою проведення комерційного і технологічного аудиту є оцінювання науково-технічного рівня та рівня комерційного потенціалу засобів розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі, створеної в результаті науково-технічної діяльності, тобто під час виконання магістерської кваліфікаційної роботи.

Для проведення комерційного та технологічного аудиту залучаємо 3-х незалежних експертів, якими є провідні викладачі випускової або спорідненої кафедри.

Оцінювання науково-технічного рівня засобів розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі та її комерційного потенціалу здійснюємо із застосуванням п'ятибальної системи оцінювання за 12-ма критеріями, а результати зводимо до таблиці 5.1.

Таблиця 5.1 — Результати оцінювання науково-технічного рівня і комерційного потенціалу засобів розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі

Критерії	Експерти		
	Експерт 1	Експерт 2	Експерт 3
	Бали, виставлені експертами		
Технічна здійсненність концепції	4	3	4
Ринкові переваги (наявність аналогів)	4	3	3
Ринкові переваги (ціна продукту)	4	4	3
Ринкові переваги (технічні властивості)	3	3	4
Ринкові переваги (експлуатаційні витрати)	3	4	3
Ринкові перспективи (розмір ринку)	3	4	4
Ринкові перспективи (конкуренція)	3	4	3
Практична здійсненність (наявність фахівців)	4	3	3
Практична здійсненність (наявність фінансів)	3	4	4
Практична здійсненність (необхідність нових матеріалів)	3	3	4
Практична здійсненність (термін реалізації)	3	3	3
Практична здійсненність (розробка документів)	4	4	4
Сума балів	41	42	42
Середньоарифметична сума балів, СБ	42		

За результатами розрахунків, наведених в таблиці 5.1 робимо висновок про те, що науково-технічний рівень та комерційний потенціал засобів розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі – високий.

5.2 Розрахунок витрат на здійснення розробки засобів розгортання інфраструктури IPv6 в комп’ютерній корпоративній мережі

До витрат на оплату праці належать витрати на виплату основної та додаткової заробітної плати керівникам відділів, лабораторій, секторів і груп, науковим, інженерно-технічним працівникам, конструкторам, технологам, креслярам, копіювальникам, лаборантам, робітникам, студентам, аспірантам та іншим працівникам, безпосередньо зайнятим виконанням конкретної теми, обчисленої за посадовими окладами, відрядними розцінками, тарифними ставками згідно з чинними в організаціях системами оплати праці, також будь-які види грошових і матеріальних доплат, які належать до елемента «Витрати на оплату праці».

Витрати на основну заробітну плату дослідників ($З_о$) розраховують відповідно до посадових окладів працівників, за формулою:

$$З_о = \sum_{i=1}^{к} \frac{М_{ni} \cdot t_i}{Т_р}, \qquad (5.1)$$

де к — кількість посад дослідників, залучених до процесу дослідження;

$М_{ni}$ — місячний посадовий оклад конкретного розробника (інженера, дослідника, науковця тощо), грн.;

$Т_р$ — число робочих днів в місяці; приблизно $Т_р$ = (21…23) дні, приймаємо 22 дні;

t_i — число робочих днів роботи розробника (дослідника).

Зроблені розрахунки зводимо до таблиці 5.2.

Додаткова заробітна плата Зд всіх розробників та робітників, які брали участь у виконанні даного етапу роботи, розраховується як (10…12)% від суми основної заробітної плати всіх розробників та робітників, тобто:

З_д=0,1·(З_о+З_р)=0,1·(34545)=3455 грн. (5.2)

Таблиця 5.2 — Витрати на заробітну плату дослідників

Посада	Місячний посадовий оклад, грн.	Оплата за робочий день, грн.	Число днів роботи	Витрати на заробітну плату, грн.
Керівник	15 000	682	24	16364
Розробник	13 000	591	20	11818
Консультанти	14 000	636	10	6364
Всього:	34545			

Нарахування на заробітну плату $Н_{зп}$ розробників та робітників, які брали участь у виконанні даного етапу роботи, розраховуються за формулою:

$$Н_{зп} = \beta \cdot (З_о + З_р + З_д) = \quad (5.3)$$

$$= 0{,}22 \cdot (34545 + 3455) = 8360 \text{ грн.}$$

де $З_о$ — основна заробітна плата розробників, грн.;

$З_р$ — основна заробітна плата робітників, грн.;

$З_д$ — додаткова заробітна плата всіх розробників та робітників, грн.;

β — ставка єдиного внеску на загальнообов'язкове державне соціальне страхування, % (приймаємо для 1-го класу професійності ризику 22%).

Витрати на матеріали М, що були використані під час виконання даного етапу роботи, розраховуються за формулою:

$$М = \sum_{1}^{n} Н_i \cdot Ц_i \cdot К_i - \sum_{1}^{n} В_i \cdot Ц_i, \quad (5.4)$$

де $Н_i$ — кількість матеріалів і-го виду, шт.;

$Ц_i$ — ціна матеріалів і-го виду, грн.;

$К_i$ — коефіцієнт транспортних витрат, $К_i$ = (1,1…1,15);

n — кількість видів матеріалів.

Зроблені розрахунки зводимо до таблиці 5.3.

Таблиця 5.3 — Матеріали, що використані на розробку

Найменування матеріалів	Ціна за одиницю, грн.	Витрачено	Вартість витрачених матеріалів, грн.
Папір канцелярський офісний (А4)	250	1	250
FLASH-пам'ять (64 ГБ)	200	1	200
Всього, з врахуванням коефіцієнта транспортних витрат			495

Вартість спецустаткування визначається за прейскурантом гуртових цін або за даними базових підприємств за відпускними і договірними цінами.

$$В_{спец} = \sum_{1}^{к} Ц_i \cdot С_{пр.i} \cdot К_i, \quad (5.5)$$

де $Ц_i$ — ціна придбання спецустаткування і-го виду, грн.;

$С_{пр.i}$ — кількість одиниць спецустаткування відповідного виду, шт.;

$К_i$ — коефіцієнт транспортних витрат, $К_i$ = (1,1…1,15);

n — кількість видів спецустаткування.

Зроблені розрахунки зводимо до таблиці 5.3.

Таблиця 5.3 — Витрати на придбання спецустаткування

Найменування спецустаткування	Ціна за одиницю, грн.	Витрачено	Вартість спецустаткування, грн.
Лазерна проекційна система Multi-GRAF1000	46000	1	46000
Router MikroTik hAP ac3	4300	2	8600
Всього, з врахуванням коефіцієнта транспортних витрат			60060

До балансової вартості програмного забезпечення входять витрати на його інсталяцію, тому ці витрати беруться додатково в розмірі 10…12% від вартості

програмного забезпечення. Балансову вартість програмного забезпечення розраховують за формулою:

$$В_{прг} = \sum_{1}^{к} Ц_{іпрг} \cdot С_{прг.і} \cdot К_і,$$

де $Ц_{іпрг}$ — ціна придбання програмного забезпечення і-го виду, грн.;

$С_{прг.і}$ — кількість одиниць програмного забезпечення відповідного виду, шт.;

$К_і$ — коефіцієнт, що враховує інсталяцію, налагодження програмного забезпечення, $К_і = (1{,}1…1{,}12)$;

к — кількість видів програмного забезпечення.

Зроблені розрахунки зводимо до таблиці 5.4.

Таблиця 5.4 — Витрати на придбання програмного забезпечення

Найменування програмного забезпечення	Ціна за одиницю, грн.	Витрачено	Вартість програмного забезпечення, грн.
Прикладний пакет Microsoft Office	7 800	1	7800
Програмний засіб IDE - Visual Studio Code	10 000	1	10000
Всього, з врахуванням коефіцієнта інсталяції та налагодження			19758

Амортизація обладнання, комп’ютерів та приміщень, які використовувались під час (чи для) виконання даного етапу роботи.

У спрощеному вигляді амортизаційні відрахування А в цілому бути розраховані за формулою:

$$А = \frac{Ц_б}{Т_в} \cdot \frac{t}{12}, \quad (5.7)$$

де $Ц_б$ — загальна балансова вартість всього обладнання, комп’ютерів, приміщень тощо, що використовувались для виконання даного етапу роботи, грн.;

t — термін використання основного фонду, місяці;

$Т_в$ — термін корисного використання основного фонду, роки.

Зроблені розрахунки зводимо до таблиці 5.5.

Таблиця 5.5 – Амортизаційні відрахування за видами основних фондів

Найменування	Балансова вартість, грн.	Строк корисного використання, років	Термін використання, місяців	Сума амортизації, грн.
Лазерна проекційна система Multi-GRAF1000	46000	3	2	1533,3
Програмно-аналітичний комплекс	20000	3	2	666,7
Всього	2200			

Витрати на силову електроенергію $В_е$, якщо ця стаття має суттєве значення для виконання даного етапу роботи, розраховуються за формулою:

Зроблені розрахунки зводимо до таблиці 5.6.

Таблиця 5.6 – Витрати на електроенергію

Найменування обладнання	Потужність, кВт	Тривалість годин роботи
Лазерна проекційна система Multi-GRAF1000	0,35	20
Програмно-аналітичний комплекс	0,38	160
Router MikroTik hAP ac3	0,2	100

$$Ве = \sum \frac{W_i \cdot t_i \cdot Ц_е \cdot К_{впі}}{ККД}$$

$$= \frac{0,35 \cdot 20 \cdot 4,32 \cdot 0,75}{0,98} + \frac{0,38 \cdot 160 \cdot 4,32 \cdot 0,75}{0,98} + \frac{0,2 \cdot 100 \cdot 4,32 \cdot 0,}{0,98} \qquad (5.8)$$

$$= 290{,}3 \text{ грн},$$

де W_i — встановлена потужність обладнання, кВт;

t_i — тривалість роботи обладнання на етапі дослідження, год.;

$Ц_е$ — вартість 1 кВт електроенергії, 4,32 грн.;

$К_{впі}$ — коефіцієнт використання потужності;

ККД — коефіцієнт корисної дії обладнання.

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками.

Витрати за статтею «Інші витрати» розраховуються як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$Ів = \left(З_о + З_р\right) \cdot \frac{Н_{ів}}{100\%} = (34545) \cdot \frac{65}{100} = 22454{,}55 \text{ грн.}, \quad (5.9)$$

де $Н_{ів}$ — норма нарахування за статтею «Інші витрати».

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов’язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов’язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов’язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуються як 100…200% від суми основної заробітної плати дослідників та робітників за формулою:

$$Внзв = \left(З_о + З_р\right) \cdot \frac{Н_{нзв}}{100\%} = (34545) \cdot \frac{190}{100} = 65636{,}36 \text{ грн.}, \quad (5.10)$$

де $Н_{нзв}$ — норма нарахування за статтею «Накладні (загальновиробничі) витрати».

Витрати на проведення науково-дослідної роботи розраховуються як сума всіх попередніх статей витрат за формулою:

$$В_{заг} = 34545 + 3455 + 8360 + 495 + 60060 + 19758 + 2200 + 290{,}3 + 22454{,}55 + 65636{,}36 = 217254{,}2 \text{ грн.} \quad (5.11)$$

Загальні витрати ЗВ на завершення науково-дослідної (науково-технічної) роботи з розробки засобів розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі та оформлення її результатів розраховуються за формулою:

$$ЗВ = \frac{В_{заг}}{\eta} = \frac{217254{,}2}{0{,}5} = 434508{,}4 \text{ грн.}, \quad (5.12)$$

де η — коефіцієнт, що характеризує етап виконання науково-дослідної роботи.

Оскільки, якщо науково-технічна розробка знаходиться на стадії розробки дослідного зразка, то η=0,5.

5.3 Розрахунок економічної ефективності науково-технічної розробки засобів розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі за її можливої комерціалізації потенційним інвестором

В ринкових умовах узагальнюючим позитивним результатом, що його може отримати потенційний інвестор від можливого впровадження результатів тієї чи іншої науково-технічної розробки засобів розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі, є збільшення у потенційного інвестора величини чистого прибутку.

В даному випадку відбувається розробка засобу, тому основу майбутнього економічного ефекту буде формувати: ΔN – збільшення кількості споживачів, яким надається відповідна інформаційна послуга в аналізовані періоди часу; N – кількість споживачів, яким надавалась відповідна інформаційна послуга у році до впровадження результатів нової науково-технічної розробки; $Ц_б$ — вартість

послуги у році до впровадження інформаційної системи; $\pm\Delta Ц_о$ — зміна вартості послуги (зростання чи зниження) від впровадження результатів науково-технічної розробки в аналізовані періоди часу.

Можливе збільшення чистого прибутку у потенційного інвестора ΔПі для кожного із років, протягом яких очікується отримання позитивних результатів від можливого впровадження та комерціалізації науково-технічної розробки, розраховується за формулою:

$$\Delta П = (\pm\Delta Ц_о \cdot N + Ц_о \cdot \Delta N_і)_і \cdot \lambda \cdot \rho \cdot \left(1 - \frac{\vartheta}{100}\right), \qquad (5.13)$$

де ±ΔЦ — зміна основного якісного показника від впровадження результатів науково-технічної розробки в аналізованому році. Зазвичай, таким показником може бути зміна ціни реалізації одиниці нової розробки в аналізованому році (відносно року до впровадження цієї розробки);

$\pm\Delta Ц_о$ може мати як додатне, так і від'ємне значення (від'ємне — при зниженні ціни відносно року до впровадження цієї розробки, додатне — при зростанні ціни);

N — основний кількісний показник, який визначає величину попиту на аналогічні чи подібні розробки у році до впровадження результатів нової науково-технічної розробки;

$Ц_о$ — основний якісний показник, який визначає ціну реалізації нової науково-технічної розробки в аналізованому році;

$Ц_б$ — основний якісний показник, який визначає ціну реалізації існуючої (базової) науково-технічної розробки у році до впровадження результатів;

ΔN — зміна основного кількісного показника від впровадження результатів науково-технічної розробки в аналізованому році. Зазвичай таким показником може бути зростання попиту на науково-технічну розробку в аналізованому році (відносно року до впровадження цієї розробки);

λ — коефіцієнт, який враховує сплату потенційним інвестором податку на додану вартість. У 2025 році ставка податку на додану вартість становить 20%, а коефіцієнт λ =0,8333;

ρ — коефіцієнт, який враховує рентабельність інноваційного продукту (послуги). Рекомендується брати ρ =0,2...0,5;

ϑ — ставка податку на прибуток, який має сплачувати потенційний інвестор, у 2025 році ϑ =18%.

Зроблені розрахунки зводимо до таблиць 5.7, 5.8.

Таблиця 5.7 — Очікуваний термін життєвого циклу розробки 3 роки

1-й рік	ΔП1	204918	грн.
2-й рік	ΔП2	204918	грн.
3-й рік	ΔП3	204918	грн.

Таблиця 5.8 — Очікуваний термін життєвого циклу розробки

Рік	Ц0, грн.	N, шт.	ΔЦ0, грн.	ΔN, шт.	Цб, грн.	N0, шт.
1	5000	100	10000	0	15000	100
2	5000	100	10000	0	15000	100
3	5000	100	10000	0	15000	100

Далі розраховують приведену вартість збільшення всіх чистих прибутків ПП, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки засобів розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі:

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t} = \frac{204918}{(1+0{,}1)^1} + \frac{204918}{(1+0{,}1)^2} + \frac{204918}{(1+0{,}1)^3} = 509600{,}7 \text{ грн.}, \quad (5.14)$$

де ΔПі — збільшення чистого прибутку у кожному з років, протягом яких виявляються результати впровадження науково-технічної розробки, грн.;

Т — період часу, протягом якого очікується отримання позитивних результатів від впровадження та комерціалізації науково-технічної розробки, роки (приймаємо Т=3 роки);

τ — ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, τ =0,05…0,15;

t — період часу (в роках) від моменту початку впровадження науково-технічної розробки до моменту отримання потенційним інвестором додаткових чистих прибутків у цьому році.

Далі розраховують величину початкових інвестицій PV, які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки засобів розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі. Для цього можна використати формулу:

$$PV = k_{\text{інв}} \cdot \text{ЗВ} = 1 \cdot 434508{,}4 = 434508{,}4 \text{ грн.} \quad (5.15)$$

де $k_{\text{інв}}$ — коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки засобів розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі та її комерціалізацію, це можуть бути витрати на підготовку приміщень, розробку технологій, навчання персоналу, маркетингові заходи тощо; зазвичай $k_{\text{інв}}$ = 1...5, але може бути і більшим;

ЗВ — загальні витрати на проведення науково-технічної розробки та оформлення її результатів, грн.

Тоді абсолютний економічний ефект $E_{\text{абс}}$ або чистий приведений дохід для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки засобів розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі становитиме:

$$E_{\text{абс}} = \text{ПП} - PV = 509600{,}7 - 434508 = 75092 \text{ грн.}, \quad (5.16)$$

де ПП — приведена вартість зростання всіх чистих прибутків від можливого впровадження та комерціалізації науково-технічної розробки засобів розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі, грн.;

PV — теперішня вартість початкових інвестицій, грн.

Оскільки $E_{абс}>0$, то можемо припустити про потенційну зацікавленість у розробці засобів розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі.

Для остаточного прийняття рішення з цього питання необхідно розрахувати внутрішню економічну дохідність Ев або показник внутрішньої норми дохідності вкладених інвестицій та порівняти її з так званою бар'єрною ставкою дисконтування, яка визначає ту мінімальну внутрішню економічну дохідність, нижче якої інвестиції в будь-яку науково-технічну розробку засобів розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі вкладати буде економічно недоцільно.

Внутрішня економічна дохідність інвестицій Ев, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки засобів розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі, розраховується за формулою:

$$E_в = \sqrt[T_ж]{1 + \frac{Eабс}{PV}} = \sqrt[з]{1 + \frac{75092}{434508}} = 0{,}39, \quad (5.17)$$

де $T_ж$ — життєвий цикл розробки засобів розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі, роки.

Далі розраховуємо період окупності інвестицій $T_о$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки засобів розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі:

$$T_о = \frac{1}{E_в} = \frac{1}{0{,}39} = 2{,}56 \text{ роки} \quad (5.18)$$

Оскільки $T_о<1…3$-х років, то це свідчить про комерційну привабливість науково-технічної розробки засобів розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі і може спонукати потенційного інвестора

профінансувати впровадження цієї розробки засобів розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі та виведення її на ринок.

Проведення комерційного та технологічного аудиту розробки засобів розгортання інфраструктури IPv6 у корпоративній комп'ютерній мережі підтвердило доцільність та перспективність впровадження цієї технології. Оцінювання трьома незалежними експертами за 12 критеріями засвідчило високий науково-технічний рівень і значний комерційний потенціал розробки.

Розрахунок витрат показав, що загальна вартість виконання науково-технічної розробки та оформлення її результатів становить 434,5 тис. грн. Подальші економічні розрахунки засвідчили можливість отримання інвестором додаткового чистого прибутку у розмірі 204,9 тис. грн щороку протягом трьох років, а приведена сума чистого прибутку — 509,6 тис. грн.

Абсолютний економічний ефект становить 75,1 тис. грн, що вказує на доцільність потенційного фінансування. Показник внутрішньої норми дохідності дорівнює 39%, а період окупності — 2,56 року, що є прийнятним і свідчить про інвестиційну привабливість проєкту.

Отже, розробка засобів розгортання інфраструктури IPv6 у корпоративній мережі є технічно обґрунтованою, економічно ефективною та комерційно перспективною, що може зацікавити потенційних інвесторів і сприяти успішному впровадженню технології на практиці.

ВИСНОВКИ

В магістерській кваліфікаційній роботі проведено аналіз предметної області, розглянуто сучасний стан розвитку та використання протоколів для створення інтернет з’єднань. Проведено їх порівняння та виявлено основні переваги та недоліки сучасних протоколів TCP/IP для розгортання інфраструктури корпоративної мережі.

IPv4 та IPv6 — це інтернет-протоколи, що забезпечують зв'язок між пристроями в Інтернеті. Хоча протокол IPv4 є найпоширенішим, протокол IPv6 має ряд переваг, таких як ширший адресний простір, покращені засоби безпеки та ефективніша обробка пакетів. Однак перехід на IPv6 пов'язаний із певними труднощами, зумовленими наявністю застарілих систем та інфраструктури, необхідністю підготовки кадрів, навчання та фінансовими витратами. Для переходу з IPv4 на IPv6 підприємства можуть використовувати двостекову реалізацію, методи тунелювання або механізми трансляції.

Детально проаналізовано основні параметри протоколів IPv4 та IPv6. Визначено основні відмінності між ними а також проаналізовано стуктуру заголовків пакетів даних для пересилки їх мережами.

Проведено аналіз розподілення мереж IPv4 та IPv6 у світі, проаналізовано технологій взаємодії мереж IPv4та IPv6, надано рекомендації з оптимізації засобів розгортання інфраструктури IPv6 в комп’ютерній корпоративній мережі.

Розроблено алгоритми передачі пакетів даних в корпоративній комп’ютерній мережі для різних типів тунелювання.

Здійснено моделювання впровадження інфраструктури IPv6 в корпоративну комп’ютерну мережу в пакеті Cisco Packet Tracer, яке підтвердило доцільність використання нової версії протоколу IPv6 в існуючій корпоративній мережі.

Проведено економічні розрахунки, які показали, що загальна вартість виконання науково-технічної розробки та оформлення її результатів становить 434,5 тис. грн., а приведена сума чистого прибутку — 509,6 тис. грн., період окупності — 2,56 року, що є прийнятним і свідчить про інвестиційну привабливість проєкту. Отже всі поставлені задачі виконано, мету роботи досягнуто.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Обертюх М.Р., Мельник Я.І. Використання протоколу IPv6 в корпоративних комп'ютерних мережах. Матеріали Міжнародної науково-практичної інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи (МН-2026)» − [Електронний ресурс]. – https://conferences.vntu.edu.ua/index.php/mn/ mn2026/paper/viewFile/26758/21967

2. IT-інфраструктура. Чим Вона допомагає в роботі підприємства [Електронний ресурс] – Режим доступу: https://indevlab.com/uk/blog-ua/it-infrastruktura-yak-rozibratisya-v-tsomu-skladnomu-ponyatti-i-chim-vona-dopomagaye-v-roboti-pidpriyemstva

3. Public cloud infrastructure [Електронний ресурс] – Режим доступу: https://www.statista.com/statistics/505251/worldwide-infrastructure-as-a-service-revenue/

4. On-Premises vs Cloud Computing. [Електронний ресурс] – Режим доступу: https://www.intellias.com/cloud-computing-vs-on-premises-comparison-guide/

5. What is Right for Your Business? [Електронний ресурс] – Режим доступу: https://phoenixnap.com/blog/on-premise-vs-cloud.

6. Infrastructure as code. [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/Infrastructure_as_code

7. Джастін Гарісон, Кріс Нова Cloud Native – O'Reilly Media, Inc. 2017. С.195-197.

8. NET Framework [Електронний ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/.NET_Framework#.D0.90.D1.80.D1.85.D0.B8.D1.82.D0.B5.D0.BA.D1.82.D1.83.D1.80.D0.B0_.NET.

9. What are ARM templates? [Електронний ресурс] – Режим доступу: https://docs.microsoft.com/ru-ru/azure/azure-resource-manager/templates/overview

10. Amazon Web Services [Електронний ресурс] – Режим доступу: https://aws.amazon.com/ru/devops/continuous-delivery/

11. CI – wikipedia. [Електронний ресурс] – Режим доступу:

https://uk.wikipedia.org/wiki/Неперервна_інтеграція

12. CD - wikipedia. [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Безперервна_доставка

13. Rafal Leszko Continuous Delivery with Docker and Jenkins: Delivering software at scale: 2018. 140 с.

14. Jenkins-Docker Continuous Integration & Continuous Deployment Pipeline - medium. [Електронний ресурс] – Режим доступу: https://medium.com/prakashkumar0301/docker-jenkins-cicd-pipeline-dd54854125f3

15. OVERVIEW How Ansible Works- medium. [Електронний ресурс] – Режим доступу: https://www.ansible.com/overview/how-ansible-works

16. What is Terraform? [Електронний ресурс] – Режим доступу: https://cloudacademy.com/course/managing-infrastructure-with-terraform/what-terraform/

17. Mono. Mono is a cross platform, open source .NET development framework. [Електронний ресурс] – Режим доступу: http://www.mono-project.com/Main_Page.

18. IPv6 – The History and Timeline [Electronic resource]. – Mode of access: https://www.ipv6.com/general/ipv6-the-history-andtimeline/. – Title from the screen.

19. Goralski W. Learn About: Differences in Addressing between IPv4 and IPv6 [Electronic resource] / W. Goralski. – Juniper Networks, 2014. – Mode of access: https://www.juniper.net/documentation/en_US/learn-about/ipv4-ipv6-differences.pdf. – Title from the screen.

20. Pepelnjak I. IPv6 multihoming without NAT: the problem [Electronic resource] / I. Pepelnjak. – Mode of access: http://blog.ipspace.net/2011/12/ipv6-multihoming-without-nat-problem.html. – Title from the screen.

21. Request for Comments: 1918. Address Allocation for Private Internets [Electronic resource]. – Mode of access: https://tools.ietf.org/html/rfc1918. – Title from the screen.

22. Request for Comments: 3769. Requirements for IPv6 Prefx Delegation [Electronic resource]. – Mode of access: https://tools.ietf.org/html/rfc3769. – Title from

the screen.

23. Request for Comments: 4291. IP Version 6 Addressing Architecture [Electronic resource]. – Mode of access: https://tools.ietf.org/html/rfc4291. – Title from the screen.

24. Troelsen, A., Japikse, P. (2017). Building and Configuring Class Libraries. In: Pro C# 7. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-3018-3_14

25. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. – Вінниця : ВНТУ, 2021. – 42 с.

26. Методичні вказівки до виконання магістерських кваліфікаційних робіт
студентами спеціальності 123 «Комп'ютерна інженерія». / Укладачі О. Д. Азаров, О. В. Дудник, С. І. Швець - Вінниця : ВНТУ, 2023. - 57 с.

ДОДАТОК А Технічне завдання

Міністерство освіти і науки України

Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії

Кафедра обчислювальної техніки

ЗАТВЕРДЖУЮ

Завідувач кафедри ОТ
д.т.н., проф. О. Д. Азаров

"03" 10 2025 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання магістерської кваліфікаційної роботи

«Засоби розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі»

08-54.МКР.006.00.000 ТЗ

Науковий керівник: phd., доц. каф. ОТ

_____ Обертюх М.Р.

Студент групи 2КІ-24м

_____ Мельник Я.І.

ВНТУ 2025

1 Підстава для виконання магістерської кваліфікаційної роботи (МКР)

1.1 Актуальність використання протоколу IPv6 у корпоративному середовищі обумовлена тим, що це суттєво сприяє підвищенню рівня інформаційної безпеки мережевої інфраструктури. Однією з ключових переваг IPv6 є вбудована на рівні стандарту підтримка криптографічних механізмів IPsec, що дозволяє забезпечити автентифікацію, цілісність та конфіденційність переданих даних між мережевими вузлами. Завдяки цьому можливе створення захищених каналів зв’язку як між окремими сегментами корпоративної мережі, так і при організації віддаленого доступу співробітників до внутрішніх ресурсів

1.2 Наказ про затвердження теми МКР.

2 Мета МКР і призначення розробки

2.1 Мета магістерського дослідження — вдосконалення засобів впровадження протоколів стандарту IPv6 в існуючу комп’ютерну корпоративну мережу.

2.2 Призначення розробки — дослідження впливу різних технологій тунелювання на швидкість та достовірність передачі даних в корпоративній комп’ютерній мережі.

3 Вихідні дані для виконання МКР

3.1 Проведення аналізу існуючих засобів розгортання інфраструктури IPv6 в існуючій корпоративній мережі.

3.2 Розробка структури та алгоритмів функціонування тунелів для розгортання інфраструктури IPv6 в існуючій корпоративній мережі.

3.3 На основі алгоритмів та структурних схем здійснення моделювання розгортання інфраструктури IPv6 в існуючій корпоративній мережі.

3.4 Виконання розрахунків для доведення доцільності нової розробки з економічної точки зору.

4 Вимоги до виконання МКР

Використати для моделювання пакет прикладних програм Cisco Packet Tracer.

5 Етапи МКР та очікувані результати

Етапи роботи та очікувані результати приведено в Таблиці А.1.

Таблиця А.1 — Етапи МКР

№ етапу	Назва етапу	Термін виконання		Очікувані результати
		початок	кінець	
1	Аналіз технологій розгортання інфраструктури IPv6 в існуючій корпоративній мережі			Аналітичний огляд джерел, задачі досліджень, Розділ 1
2	Аналіз використання протоколів IPv4 і IPv6			Розділ 2
3	Аналіз засобів взаємодії мереж IPv4 і IPv6			Розділ 3
4	Тестування засобів взаємодії мереж IPv4 і IPv6			Розділ 4
5	Підготовка економічної частини			Розділ 5
6	Апробація результатів дослідження			Тези
7	Оформлення матеріалів до захисту МКР			ПЗ, презентація

6 Матеріали, що подаються до захисту МКР

До захисту подаються: пояснювальна записка МКР, графічні і ілюстративні матеріали, протокол попереднього захисту МКР на кафедрі, відгук наукового керівника, відгук опонента, протоколи складання державних екзаменів, анотації до МКР українською та іноземною мовами..

7 Порядок контролю виконання та захисту МКР

Виконання етапів графічної та розрахункової документації МКР контролюється науковим керівником згідно зі встановленими термінами. Захист МКР відбувається на засіданні Екзаменаційної комісії, затвердженої наказом ректора.

8 Вимоги до оформлювання та порядок виконання МКР

8.1 При оформлюванні МКР використовуються:

— ДСТУ 3008: 2015 «Звіти в сфері науки і техніки. Структура та правила оформлювання»;

— ДСТУ 8302: 2015 «Бібліографічні посилання. Загальні положення та правила складання»;

— ГОСТ 2.104-2006 «Едина система конструкторської документації. Основні написи»;

— методичні вказівки до виконання магістерських кваліфікаційних робіт зі спеціальності 123 — «Комп’ютерна інженерія»;

— документи на які посилаються у вище вказаних.

8.2 Порядок виконання МКР викладено в «Положення про кваліфікаційні роботи на другому (магістерському) рівні вищої освіти СУЯ ВНТУ-03.02.02-П.001.01:21».

ДОДАТОК Б ПРОТОКОЛ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Назва роботи: Засоби розгортання інфраструктури IPv6 в комп'ютерній корпоративній мережі

Тип роботи: магістерська кваліфікаційна робота
(БДР, МКР)

Підрозділ кафедра обчислювальної техніки
(кафедра, факультет)

Коефіцієнт подібності текстових запозичень, виявлених у роботі

системою StrikePlagiarism (КП1) 20,00 %.

Висновок щодо перевірки кваліфікаційної роботи (відмітити потрібне):

✓ Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату , фабрикації, фальсифікації. Роботу прийняти до захисту.

□ У роботі не виявлено ознак плагіату,фабрикації, фальсифікації, але надмірна кількість текстових запозичень та/або наявність типових розрахунків не дозволяють прийняти рішенняпро оригінальність та самостійність її виконання. Роботу направити на доопрацювання.

□ У роботі виявленоознаки академічного плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень. Робота до захисту не приймається.

Експертна комісія:

Завідувач каф. ОТ Азаров О.Д._____ _____
(прізвище, ініціали, посада) (підпис)

Гарант освітнього процесу Мартинюк Т.Б. _____ _____
(прізвище, ініціали, посада) (підпис)

Особа, відповідальна за перевірку_____ Захарченко С.М.
(підпис) (прізвище, ініціали)

З висновком експертної комісії ознайомлений(-на)

Керівник_____Обертюх М.Р., доцент_____
(підпис) (прізвище, ініціали, посада)

Здобувач_____ Мельник Я.І._____
(підпис) (прізвище, ініціали)

ДОДАТОК В Блок-схема IPv6-тунелювання, при якому кінцевою адресою є адреса протоколу IPv4

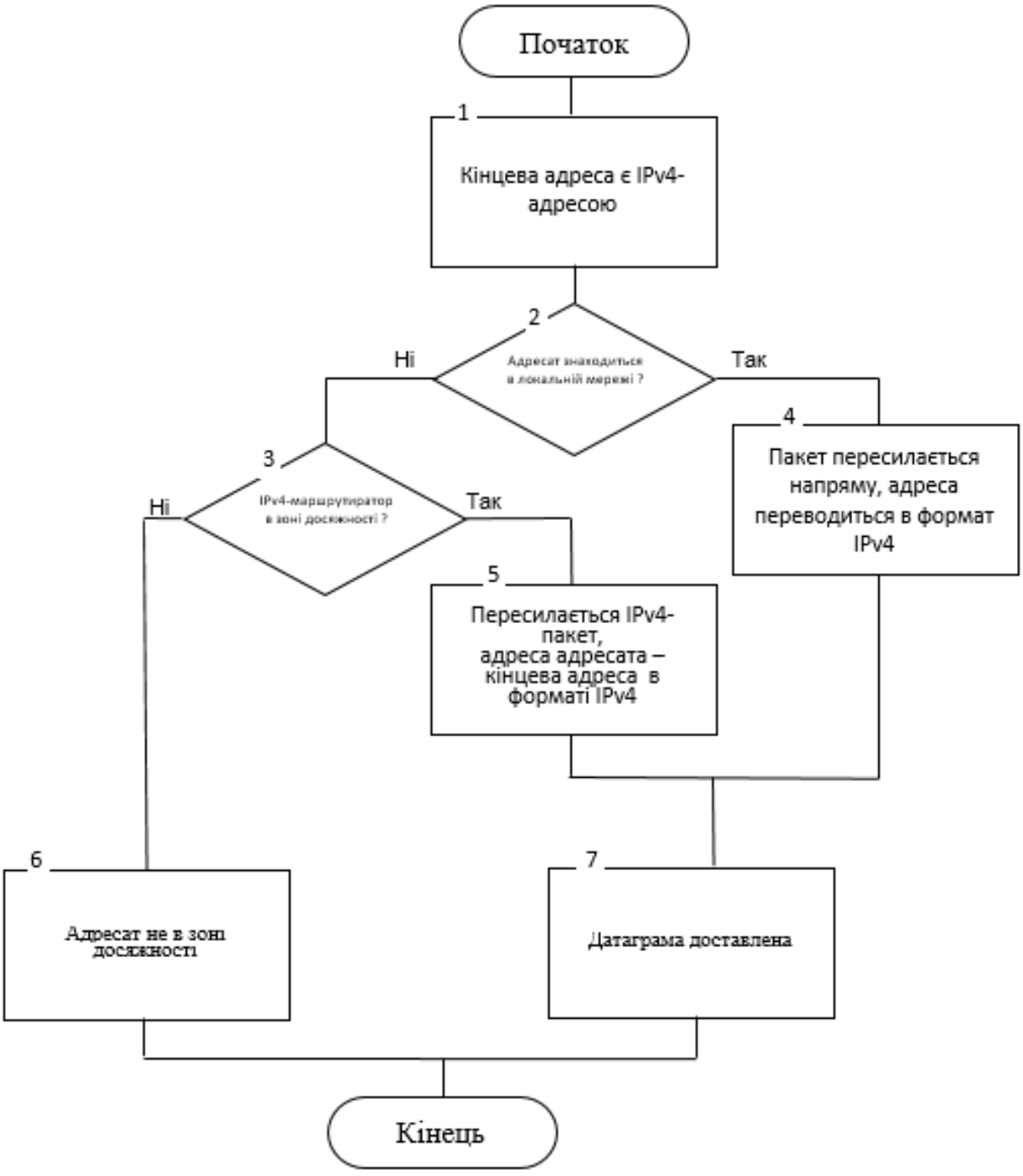

Рисунок В.1 — Блок-схема IPv6-тунелювання, при якому кінцевою адресою є адреса протоколу IPv4

ДОДАТОК Г Структура мережі в Cisco Packet Tracer

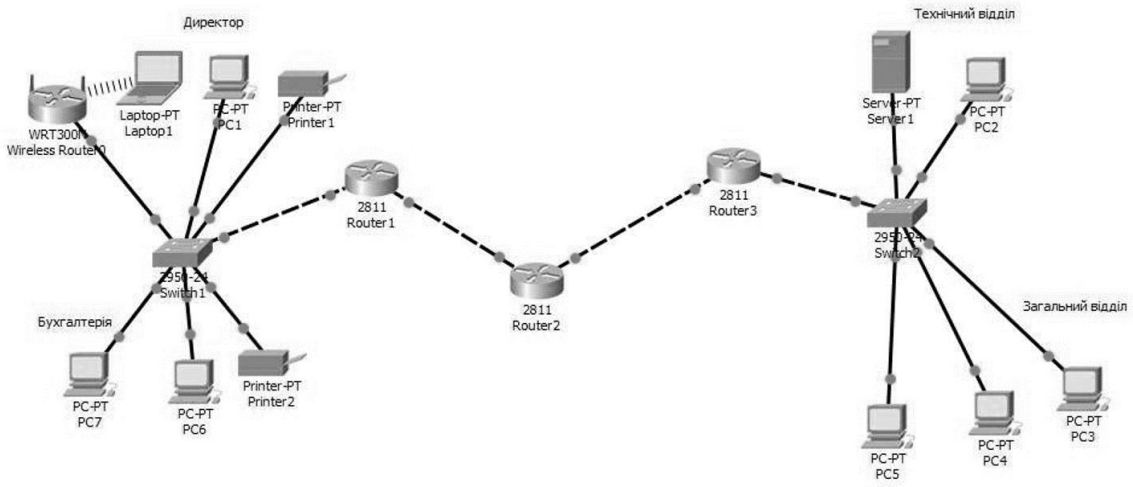

Рисунок Г.1 — Структура мережі в Cisco Packet Tracer

ДОДАТОК Д Лістинг налаштувань маршрутизаторів

NAT64

R1 en conf t
ipv6 unicast-routing
int gi0/0 ipv6 add
2004:def::2/64 no sh
ex
ipv6 route 2003:12::/96
2004:def::1 R2 en conf t ipv6
unicast-routing int gi0/0
ipv6 add
2004:def::3/64 no sh
ipv6 route 2003:12::/96
2004:def::1 R3 en conf t int
gi0/0
ip add 192.168.0.2
255.255.255.0 no sh
ex
ip route 172.16.0.0
255.255.255.0 192.168.0.1 R4 en conf t
int gi0/0 ip add 192.168.0.3
255.255.255.0 no sh
ip route 172.16.0.0
255.255.255.0 162.168.0.1 R5 en conf t
ipv6 unicast-routing int gi0/0 ipv6 add
2004:def::1/64 no sh ipv6 nat ex int
gi0/1 ip add 192.168.0.1 255.255.255.0
no sh ipv6 nat ex ipv6 nat v4v6 source
192.168.0.2 2003:12::2 ipv6 nat v4v6
source 192.168.0.3 2003:12::3 ipv6 nat
v6v4 source 2004:def::2 172.16.0.2 ipv6
nat v6v4 source 2004:def::3 172.16.0.3
ipv6 nat pr ipv6 nat prefix 2003:12::/96

Подвійний стек

R1

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 10.10.1.97 255.255.255.224
Router(config-if)#ipv6 address FE80::1 link-local
Router(config-if)# ipv6 address 2001:DB8:1:1::1/64
Router(config-if)#ex
Router(config)#interface Serial0/0/1
Router(config-if)#ip address 10.10.1.6 255.255.255.252
Router(config-if)# ipv6 address FE80::1 link-local
Router(config-if)# ipv6 address 2001:DB8:1:2::2/64
Router(config-if)#ex
R1(config)#router eigrp 1
R1(config-router)# network 10.10.1.4 0.0.0.3
R1(config-router)# network 10.10.1.96 0.0.0.31
R1(config)#ipv6 unicast-routing
R1(config)#int gi 0/0
R1(config-if)#ipv6 eigrp 1
R1(config-if)#int se 0/0/1
R1(config-if)#ipv6 eigrp 1
```

R2

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host
Router(config)#hostname R2
R2(config)#interface Serial0/0/0
R2(config-if)# ip address 10.10.1.5 255.255.255.252
R2(config-if)# ipv6 address FE80::2 link-local
R2(config-if)# ipv6 address 2001:DB8:1:2::1/64
R2(config-if)#ex
R2(config)#interface Serial0/0/1
R2(config-if)# ip address 10.10.1.9 255.255.255.252
R2(config-if)# ipv6 address FE80::2 link-local
R2(config-if)# ipv6 address 2001:DB8:1:3::1/64
R2(config)#router eigrp 1
R2(config-router)# network 10.10.1.8 0.0.0.3
R2(config-router)# network 10.10.1.4 0.0.0.3
```

R3

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hos
Router(config)#hostname R3
```

```
R3(config)#interface GigabitEthernet0/0
R3(config-if)#ip address 10.10.1.17 255.255.255.240
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)# ipv6 address 2001:DB8:1:4::1/64
R3(config-if)#
R3(config-if)#ex
R3(config)#interface Serial0/0/1
R3(config-if)#ip address 10.10.1.10 255.255.255.252
R3(config-if)# ipv6 address FE80::3 link-local
R3(config-if)# ipv6 address 2001:DB8:1:3::2/64
R3(config)#router eigrp 1
R3(config-router)# network 10.10.1.8 0.0.0.3
R3(config-router)# network 10.10.1.16 0.0.0.15
R3(config)#ipv6 router eigrp 1
R3(config-rtr)#no sh
```

Тунелювання

R1

```
Router#conf t
Router(config)#ipv6 unicast-routing
Router(config)#int fa0/0
Router(config-if)#no shutdown
Router(config-if)#ipv6 add 2000:1:1:1:1:1:1:1112/112
Router(config-if)#ipv6 rip 6bone en
Router(config-if)#ipv6 rip 6bone enable
Router(config-if)#ex
```

R2

```
Router>en
Router#conf t
Router(config)#ipv6 unicast-routing
Router(config)#int serial 0/3/0
Router(config-if)#ip add 192.23.1.2 255.255.255.0
Router(config-if)#no sh
Router(config-if)#int fa0/0
Router(config-if)#ipv6 add 2000:1:1:1:1:1:1:1111/112
Router(config-if)#no sh
Router(config-if)#ipv6 rip 6bone enable
Router(config-if)#ex
Router(config)#int tunnel0
Router(config-if)#ipv6 add 3000::1/112
Router(config-if)#ipv6 rip 6bone enable
Router(config-if)#tunnel source serial 0/3/0
Router(config-if)#tunnel destination 192.34.1.4
Router(config-if)#tunnel mode ipv6ip
Router(config-if)#ex
Router(config)#router ospf 1
Router(config-router)#network 192.23.1.0 0.0.0.255 area 0
Router(config-router)#ex
```

```
R3
Router>en
Router#conf t
Router(config)#int serial 0/3/0
Router(config-if)#ip add 192.23.1.3 255.255.255.0
Router(config-if)#no sh
Router(config-if)#ex
Router(config)#int s
Router(config)#int serial 0/3/1
Router(config-if)#int serial 0/3/1
Router(config-if)#ip add 192.34.1.3 255.255.255.0
Router(config-if)#no sh
Router(config-if)#ex
Router(config)#router ospf 1
Router(config-router)#network 192.23.1.0 0.0.0.255 area 0
Router(config-router)#network 192.34.1.0 0.0.0.255 area 0
Router(config-router)#ex
R4
Router>en
Router#conf t
Router(config)#ipv6 unicast-routing
Router(config)#int serial 0/3/1
Router(config-if)#ip add 192.34.1.4 255.255.255.0
Router(config-if)#no sh
Router(config-if)#ex
Router(config)#int fa0/1
Router(config-if)#ipv6 add 4000:1:1:1:1:1:1:1111/112
Router(config-if)#ipv6 rip 6bone enable
Router(config-if)#no sh
Router(config-if)#ex
Router(config)#int tunnel0
Router(config-if)#ipv6 add 3000::2/122
Router(config-if)#ipv6 rip 6bone enable
Router(config-if)#tunnel source serial 0/3/1
Router(config-if)#tunnel destination 192.23.1.2
Router(config-if)#tunnel mode ipv6ip
Router(config-if)#ex
Router(config)#router ospf 1
Router(config-router)#network 192.34.1.0 0.0.0.255 area 0
Router(config-router)#ex
R5
Router>en
Router#conf t
Router(config)#ipv6 unicast-routing
Router(config)#int fa 0/1
Router(config-if)#no sh
Router(config-if)#ipv6 add 4000:1:1:1:1:1:1:1112/112
Router(config-if)#ipv6 rip
6bone enable  Router(config-if)#ex
```