МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Роман ОДАРЧЕНКО
“_____”_____2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВР

Тема: «Моделювання мережі на базі протоколу IPv6 з використанням програмного пакету Packet Tracer»

Виконавець: _____ Сергій ПЕЧЕРНИЙ
(підпис)

Керівник: _____ Віталій КУРУШКІН
(підпис)

Нормоконтролер: _____ Денис БАХТІЯРОВ
(підпис)

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

Роман ОДАРЧЕНКО
“_____”_____2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Печерного Сергій Володимировича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Моделювання мережі на базі протоколу IPv6 з використанням програмного пакету Packet Tracer»
затверджена наказом ректора від «29» березня 2023 р. № 421/ст
2. Термін виконання роботи: з 22.05.2023 р. по 25.06.2023 р.
3. Вихідні дані до роботи: аналіз принципів роботи мережі IPv6
4. Зміст пояснювальної записки: принцип моделювання мережі на базі протоколу IPv6 з використанням програмного пакету Packet Tracer; моделювання мережі на базі протоколу IPv6; розрахунок смуги пропускання мережі
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: слайди презентації в програмному пакеті Microsoft Power Point

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	22.05.2023-24.05.2023	Виконано
2	Вступ	25.05.2023	Виконано
3	Основні поняття протоколу IP	26.05.2023-29.05.2023	Виконано
4	Аналіз протоколу IP	30.05.2023-07.06.2023	Виконано
5	Моделювання мережі на базі протоколу IPv6 з використанням програмного пакету Packet Tracer	08.06.2023-14.06.2023	Виконано
6	Усунення недоліків та захист кваліфікаційної роботи	15.06.2023-25.06.2023	Виконано

7. Дата видачі завдання: “19" травня 2023 р.

Керівник кваліфікаційної роботи _____ Віталій КУРУШКІН
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Сергій ПЕЧЕРНИЙ
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Моделювання мережі на базі протоколу IPv6 з використанням програмного пакету Packet Tracer» містить 70 сторінок, 28 рисунків, 3 таблиці, 13 використаних джерел.

МОДЕЛЮВАННЯ МЕРЕЖІ, ПРОТОКОЛ IPv6, PACKET TRACER, ІНФОКОМУНІКАЦІЙНІ ПОСЛУГИ, МУЛЬТИСЕРВІСНІ МЕРЕЖІ, МЕРЕЖЕВІ ПРИСТРОЇ, НАЛАШТУВАННЯ МЕРЕЖІ, ПРОДУКТИВНІСТЬ МЕРЕЖІ, ЕФЕКТИВНІСТЬ ПЕРЕДАЧІ ДАНИХ, ЯКІСТЬ ОБСЛУГОВУВАННЯ (QOS).

Об'єкт дослідження – є протокол IPv6, в рамках дослідження буде проведено моделювання цієї мережі з використанням програмного пакету Packet Tracer та дослідження її функціональних можливостей, продуктивності та ефективності.

Предмет дослідження –є процес моделювання мережі на базі протоколу IPv6 з використанням програмного пакету Packet Tracer. Дослідження зосереджується на вивченні можливостей та ефективності використання IPv6 у мережевому середовищі, а також на розробці та налаштуванні модельної мережі з використанням Packet Tracer.

Мета кваліфікаційної роботи – моделювання мережі на базі протоколу IPv6 з використанням програмного пакету Packet Tracer і дослідження її функціональності та продуктивності. Основна мета полягає в оцінці можливостей та переваг використання IPv6 у сучасних мережевих середовищах.

Метод дослідження – літературний аналіз, експериментальні дослідження, аналіз даних та виведення висновків. Ці методи дозволять дослідити та оцінити можливості моделювання мереж на базі протоколу IPv6 з використанням програмного пакету Packet Tracer та зробити висновки щодо їх ефективності та практичної цінності.

Матеріали кваліфікаційної роботи рекомендується використовувати для підготовки теоретичного обґрунтування дослідження, використання таких матеріалів забезпечить наукову обґрунтованість та додаткову підтримку вашої роботи.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

IP(Internet Protocol) – Інтернет-протокол.

IPv4(Internet protocol version 6) – Інтернет-протокол версії 6.

IPv6(Internet protocol version 4) – Інтернет-протокол версії 4.

CIDR(Classless Inter-Domain Routing) – Безкласова міждоменна маршрутизація.

NAT(Network Address Translation) – Трансляція мережевих адрес.

RFC(Request for Comments) – Запит на коментарі.

TCP(Transmission Control Protocol) – Протокол керування передачею.

DHCP(Dynamic Host Configuration Protocol) – Протокол динамічної конфігурації хоста.

ICMP(Internet Control Message Protocol) – Протокол керуючих повідомлень Інтернету.

ToS(Type of Service) – Тип послуги.

PDU(Power Distribution Unit) – Блок розподілу електроенергії.

UDP(User Datagram Protocol) – Протокол дейтаграм користувача.

IETF(Internet Engineering Task Force) – Інженерна робоча група Інтернету.

IPSec(Internet Protocol Security) – Безпека Інтернет-протоколу.

AH(Authentication Header) – Заголовок автентифікації.

ESP(Encapsulated Security Payload) – Інкапсульоване корисне навантаження безпеки.

ARPANET(Advanced Research Projects Agency Network) – Мережа агентств передових дослідницьких проектів.

IANA(Internet Assigned Numbers Authority) – Орган з присвоєння номерів Інтернету.

SLAAC(Stateless Address Auto-configuration) – Автоматична конфігурація адреси без збереження стану.

ISP(International Standarts Protocol) – Протокол міжнародних стандартів.

ARP(Address Resolution Protocol) – Протокол вирішення адрес.

MAC(Media Access Control) – Контроль доступу до медіа.

IAB(Interactive Advertising Bureau) – Бюро інтерактивної реклами.

DNS(Domain Name System) – Система доменних імен.

API(Application Programming Interface) – Інтерфейс прикладного програмування.

DHCPIBM(Dynamic Host Configuration Protocol) – Протокол динамічної конфігурації хоста.

FTP(File Transfer Protocol) – Протокол передачі файлів.

MLP(Multilink Protocol) – Багатоканальний протокол.

ESP(Electronic stability program) – Електронна програма стабільності.

QoS(Quality of service) – Якість обслуговування.

LAN(Local Area Network) – Локальна мережа.

L2TP(Layer Two Tunneling Protocol) – Протокол тунелювання другого рівня.

PING(Packet Internet or Inter-Network Groper) – Пакетний Інтернет або Inter-Network Groper.

IBM(Business Machines Corporation) – Корпорація Business Machines.

MTU(Maximum Transmission Unit) – Максимальна одиниця передачі.

RIP(Routing Information Protocol) – Протокол інформації про маршрутизацію.

ВСТУП

Сучасний етап розвитку системи електрозв'язку характеризується зростаючим попитом на нові інфокомунікаційні послуги та постійними змінами у технологіях передачі та обробки даних. Для ефективної модернізації мереж електрозв'язку використовуються нові технології, спрямовані на підтримку широкого спектру інфокомунікаційних послуг.

Одним з ключових аспектів цього розвитку є протокол IPv6, який забезпечує масштабованість та дозволяє підключати значно більшу кількість пристроїв до мережі Інтернет. Впровадження IPv6 є важливим кроком у розвитку сучасних телекомунікаційних мереж, оскільки дозволяє подолати обмеження протоколу IPv4 і задовольнити зростаючий попит на адресацію та послуги Інтернету.

Для ефективного вивчення та розгортання IPv6 необхідні засоби, які дозволяють моделювати та аналізувати мережеві структури. Один з таких засобів - програмний пакет Packet Tracer, який є потужним інструментом для моделювання та симуляції мереж на базі протоколу IPv6. Використання Packet Tracer дозволяє інженерам та дослідникам проводити детальний аналіз протоколу IPv6, експериментувати з різними налаштуваннями та оцінювати продуктивність мережі.

Метою даної кваліфікаційної роботи є вивчення протоколу IPv6 та його моделювання на базі програмного пакету Packet Tracer. В рамках роботи планується провести детальний аналіз особливостей IPv6, дослідити його переваги порівняно з IPv4 та визначити оптимальні налаштування для мережі. Застосування Packet Tracer дозволить розробити модель мереж ористанням протоколу IPv6, провести експерименти для оцінки її функціональності та продуктивності.

Результати цієї кваліфікаційної роботи будуть корисними для інженерів та адміністраторів мереж, які планують перехід на IPv6. Робота дозволить їм отримати практичний досвід у моделюванні та розгортанні мереж з використанням IPv6, а також зрозуміти переваги та виклики, пов'язані з цим протоколом.

Актуальність теми. Тема "Моделювання мережі на базі протоколу IPv6 з використанням програмного пакету Packet Tracer" є актуальною у зв'язку з: вичерпанням адресного простору IPv4 і потребою в переході на IPv6. Розвитком нових інфокомунікаційних послуг і підтримкою мультисервісних мереж. Потребою в налаштуванні та оптимізації мережі для ефективної передачі даних. Підвищенням компетенцій фахівців у галузі мережевих технологій. Такі дослідження допоможуть вирішити важливі завдання у сфері мережевого проектування та підготуватися до переходу на IPv6.

Мета і завдання дослідження. ***Мета*** - моделювання мережі на базі протоколу IPv6 з використанням програмного пакету Packet Tracer і дослідження її функціональності та продуктивності. Основна мета полягає в оцінці можливостей та переваг використання IPv6 у сучасних мережевих середовищах.

Для досягнення поставленої мети вирішуються такі наукові завдання.

1. Розробка моделі мережі на базі IPv6 з використанням Packet Tracer, враховуючи вимоги та особливості сучасних мережевих середовищ.
2. Налаштування мережевих пристроїв (маршрутизаторів, комутаторів) та реалізація IPv6-протоколу в модельній мережі.
3. Проведення експериментів та тестування мережі з метою оцінки функціональності та продуктивності IPv6-протоколу.
4. Аналіз отриманих результатів та висновки щодо переваг та викликів використання IPv6 у модельній мережі.

Об'єктом дослідження є протокол IPv6, в рамках дослідження буде проведено моделювання цієї мережі з використанням програмного пакету Packet Tracer та дослідження її функціональних можливостей, продуктивності та ефективності.

Предметом *дослідження* є процес моделювання мережі на базі протоколу IPv6 з використанням програмного пакету Packet Tracer. Дослідження зосереджується на вивченні можливостей та ефективності використання IPv6 у мережевому середовищі, а також на розробці та налаштуванні модельної мережі з використанням Packet Tracer.

Методи досліджень. До методів дослідження можуть належати: літературний аналіз, експериментальні дослідження, аналіз даних та виведення висновків. Ці методи дозволять дослідити та оцінити можливості моделювання мереж на базі протоколу IPv6 з використанням програмного пакету Packet Tracer та зробити висновки щодо їх ефективності та практичної цінності.

Апробація отриманих результатів. Основні положення роботи доповіда лися та обговорювалися на таких конференціях:

- Науково-практична конференція «Проблеми експлуатації та захисту інформа ційно-комунікаційних систем», м. Київ, 2023 р.

РОЗДІЛ 1
ОСНОВНІ ПОНЯТТЯ ПРОТОКОЛУ IP

1.1. Визначення та структура протоколу IP

Інтернет-протокол (IP) є невід'ємною частиною набору інтернет-протоколів (набору з близько 500 мережевих протоколів) і являє собою протокол без з'єднання, що відповідає за адресацію і кешування пакетів даних в цифрових мережах. Разом з транспортним рівнем, протоколом управління передачею (Transmission Control Protocol, TCP), IP є основою Інтернету. Для надсилання пакетів від відправника до одержувача інтернет-протоколи створюють структуру пакетів, яка узагальнює інформацію, що надсилається. Для цього протокол визначає, як описується інформація про джерело і пункт призначення, і відокремлює цю інформацію від інформаційних даних в IP-заголовку. Цей формат пакетів також відомий як IP-дейтаграма.

У 1974 році Інститут інженерів з електротехніки та електроніки опублікував дослідницьку роботу американських вчених-комп'ютерників Роберта Кана та Вінта Серфа, в якій вони описали попередника Інтернету, міжмережеву мережу ARPANET. Вони описали модель протоколу для з'єднання пакетних мереж. Основними елементами цієї моделі були протокол управління передачею TCP і (за винятком спеціального абстрактного рівня) протокол IP, який дозволяв здійснювати зв'язок між різними фізичними мережами. Згодом все більше дослідницьких мереж інтегрувалися на основі комбінації протоколів TCP/IP, які були остаточно встановлені в якості стандартів в RFC 971 в 1981 році.

Інтернет-протокол - це набір правил маршрутизації та адресації, які дозволяють пакетам даних подорожувати мережею і досягати місця призначення. Дані, що надсилаються через Інтернет, розбиваються на менші компоненти, які називаються пакетами. До кожного пакета додається IP-інформація, щоб підготувати маршрутизатор до відправлення пакета в потрібне місце. Кожному пристрою або

домену, підключеному до Інтернету, присвоюється IP-адреса, і пакет надсилається туди, де йому присвоєно IP-адресу, щоб дані були відправлені туди, куди їм потрібно.

Після того, як пакет досягає місця призначення, його обробка відрізняється залежно від транспортного протоколу, що використовується разом з IP-адресою [1].

Протоколи - це способи оперування та форматування даних таким чином, щоб два або більше пристроїв могли спілкуватися і розуміти один одного.

Щоб зрозуміти, навіщо нам потрібні протоколи, давайте розглянемо процес надсилання листа. Адреса на конверті пишеться в такому порядку: ім'я, вулиця, місто та поштовий індекс. Якщо ви покладете конверт у поштову скриньку з індексом та адресою в такому порядку, то пошта не доставить листа. Існує узгоджений протокол для написання адрес, щоб забезпечити роботу поштової системи. Аналогічно, всі IP-пакети даних повинні надавати певну інформацію в певному порядку, а всі IP-адреси повинні відповідати стандартному формату.

Присвоєння IP-адрес хостам здійснюється:

- вручну, налаштовується системним адміністратором під час налаштування обчислювальної мережі;
- автоматично, з використанням спеціальних протоколів (зокрема, за допомогою протоколу DHCP - Dynamic Host Configuration Protocol, протокол динамічного налаштування хостів).

Протокол IP працює міжмережевому (мережевому) рівні стека протоколу TCP/IP. Функції протоколу IP визначено у стандарті RFC-791 так: “Протокол IP забезпечує передачу блоків даних, званих дейтаграммами, від відправника до одержувачам, де відправники і одержувачі є комп'ютерами, ідентифікованими адресами фіксованої довжини (IP-адресами). Протокол IP забезпечує при необхідності також фрагментацію та складання дейтаграм передачі даних через мережі з малим розміром пакетів”.

Протокол IP відправляє та обробляє кожну дейтаграму як незалежну порцію даних, тобто, не маючи жодних інших зв'язків з іншими дейтаграмами у глобальній мережі Інтернет [2].

Після надсилання дейтаграми протоколом IP у мережу, все, що відбувається з дейтаграмою після відправки не піддається контролю з боку протоколу. Виходить так, що якщо дейтаграма з будь-яких причин не може бути передана далі по мережі, вона знищується. Хоча вузол, який знищив дейтаграму, може повідомити причину збою відправнику, за зворотним адресою (зокрема з допомогою протоколу ICMP). Гарантії доставки даних покладено протоколи вищого рівня (транспортний рівень), які використовують цього спеціальні механізми (протокол TCP).

Як відомо, на мережевому рівні моделі OSI працюють маршрутизатори. З цієї причини, одним з найважливіших завдань протоколу IP – це здійснення маршрутизації дейтаграм, іншими словами, визначення оптимального шляху проходження дейтаграм (за допомогою алгоритмів маршрутизації) від вузла-відправника мережі до будь-якого іншого вузла мережі на підставі IP адреси. Алгоритм роботи протоколу ip на якомусь вузлі мережі, що приймає дейтаграму з мережі, представлений на рис 1.1.

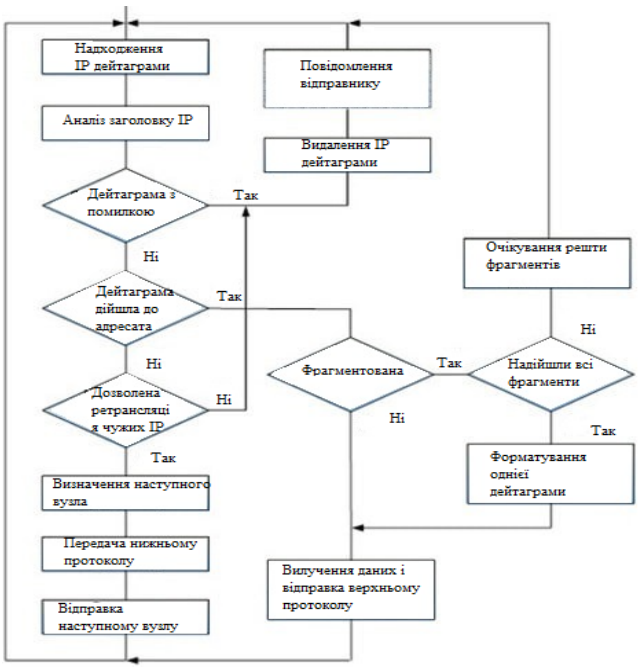

Рис. 1.1. Алгоритм роботи протоколу IP

Структура IP-адреси

IP-адреса відображається у вигляді чотиризначного числа і за замовчуванням має значення 192.158.1.38. Адреса за замовчуванням 192.158.1.38. Кожне число в цьому наборі знаходиться в діапазоні від 0 до 255. Таким чином, загальний діапазон IP-адрес становить 0.0.0.0 до 255.255.255.255.

IP-адреса в основному ділиться на дві частини: X1. X2. X3. X4

1. [X1. X2. X3] — ідентифікатор мережі
2. [X4] – це ідентифікатор хоста

- Ідентифікатор мережі - це ліва частина IP-адреси, яка ідентифікує конкретну мережу, в якій знаходиться пристрій. У типовій домашній мережі, якщо IP-адреса пристрою 192.168.1.32, частина адреси 192.168.1 є ідентифікатором мережі; зазвичай вона заповнюється ненульовим числом, тому можна сказати, що ідентифікатор мережі цього пристрою 192.168.1.0 Ідентифікатор мережі цього пристрою 192.168.1.0.
- Ідентифікатор хоста - це частина IP-адреси, яка не використовується в ідентифікаторі мережі. Він ідентифікує певний пристрій у мережі (у світі TCP/IP пристрої називаються "хостами"). Продовжуючи приклад з IP-адресою 192.168.1.32, ідентифікатор хоста дорівнює 32, що є унікальним ідентифікатором хоста в мережі 192.168.1.0 [3].

Структура пакетів IPv6 багато схожа на структуру пакетів IPv4. Деякі поля були видалені, деякі – додані, але найпомітніші зміни стосуються розмірів адрес. У той час як адреси відправника та одержувача IPv4 мають довжину 32 біти, адреси IPv6 займають 128 біт.

На рис. 1.2. та 1.3. проілюстровані відмінності між заголовками IPv4 та IPv6.

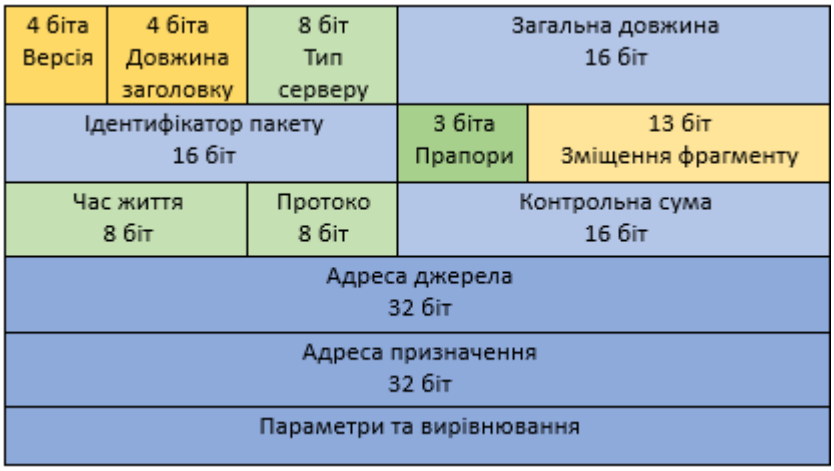

Рис. 1.2. Заголовок IPv4

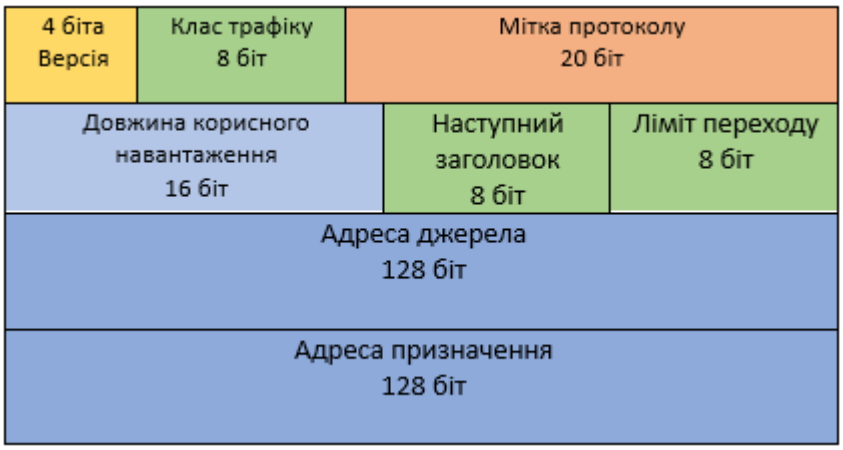

Рис. 1.3. Заголовок IPv6

У цілому IPv6 спрощує структуру основного заголовку, включаючи лише інформацію, яка необхідна передачі пакета. Це виливається в те, що, на відміну від IPv4, заголовок має фіксовану довжину. Заголовки фіксованої довжини сильно полегшують життя розробникам маршрутизаторів та програмістам, тому що вони дозволяють розподіляти пам'ять та реалізовувати алгоритми більш ефективно. Інша інформація, яка традиційно зберігалася в заголовку IPv4, тепер зберігається в ланцюзі за наступними заголовками, що визначаються полем next header . Кінцевими заголовками зазвичай є заголовки TCP, UDP або ICMPv6. Таким чином, завдання просування даних можна вирішити, працюючи лише з першими бітами отриманого пакета.

Багато знайомих полів мають еквіваленти в IPv6: Version (версія), ToS/Traffic

Class (тип обслуговування/клас трафіку), Total Lengt/Payload Length (повна довжина/ефективна довжина), Time to Live/Hop Limit (час життя/граничний та кількість стрибків), Protocol/Next Header (протокол/наступний заголовок), адресу відправника та адресу одержувача. Проте відсутні поля фрагментації (ID, Flags, Offset) та контрольної суми заголовка, Поле Traffic Class замінено досконалішим полем Flow Label (мітка потоку), обидва використовуються для контролю за якістю обслуговування. Протоколи TCP і UDP не змінилися, проте окремо взяті протоколи рівня додатків, у яких жорстко визначено розмір адреси, під час переходу до нового світу можуть піднести неприємні сюрпризи [4].

1.2. Формат пакету

Формат пакету IPv4

IPv4-дейтаграма складається із заголовка та поля даних. Перші 20 байт заголовка є обов'язковими для всіх IPv4-дейтаграм; поля параметрів після цих 20 байт мають різну довжину.

Рис. 1.4. Структура заголовка IP-пакету

Таблиця 1.1

Таб. 1.1. Характеристики структури пакету

Поле	Довжина	Опис
Версія	4 біти	Визначає версію IP-протоколу, IPv4 або IPv6.

Продовження таблиці 1.1

Довжина заголовка	4 біти	Визначає довжину заголовка IPv4.
Тип послуги (ToS)	8 біт	Визначає тип послуги. Це поле діє лише в моделі диференційованого обслуговування.
Загальна довжина	16 біт	Визначає довжину заголовка та даних.
Ідентифікація	16 біт	Програмне забезпечення IPv4 підтримує лічильник у запам'ятовуючому пристрої для запису кількості IP-дейтаграм. Значення лічильника збільшується на 1 кожного разу, коли надсилається дейтаграма, і заповнюється в полі ідентифікації.
Прапори	3 біти	Допустимими є лише два крайні праві біти. Крайній правий біт вказує, чи дейтаграма не є останнім фрагментом даних. Значення 1 вказує на останній фрагмент, а значення 0 вказує на неостанній фрагмент. Середній біт є прапором фрагментації. Значення 1 вказує на те, що датаграму неможливо фрагментувати, а значення 0 вказує на те, що датаграму можна фрагментувати.
Зсув фрагмента	13 біт	Визначає розташування фрагмента в пакеті.
Час життя (TTL)	8 біт	Визначає тривалість життя дейтаграми в мережі. TTL вимірюється кількістю стрибків.
Протокол	8 біт	Визначає тип протоколу, який передається в датаграмі.

Закінчення таблиці 1.1

Контрольна сума заголовка	16 біт	Пристрій обчислює контрольну суму заголовка для кожної отриманої дейтаграми. Якщо контрольна сума дорівнює 0, пристрій знає, що заголовок залишається незмінним, і зберігає датаграму. Це поле перевіряє лише заголовок, але не дані.
Вихідна IP-адреса	32 біти	Визначає адресу IPv4 відправника.
IP-адреса призначення	32 біти	Визначає адресу IPv4 одержувача.
Опції	0-40 байт (змінної довжини)	Дозволяє IPv4 підтримувати різні параметри, такі як обробка помилок, вимірювання та безпека. За потреби додаються байти із значенням 0.
Дані	змінна	Доповнює IP-дейтаграму.

Формат пакету IPv6

Пакет IPv6 складається з трьох частин: базового заголовка IPv6, одного або декількох заголовків розширення IPv6 і блоку даних протоколу (PDU).

PDU верхнього рівня складається із заголовка протоколу верхнього рівня та його корисного навантаження, яким можуть бути пакети ICMPv6, TCP або UDP.

Базовий заголовок IPv6 має фіксовану довжину 40 байт і вісім полів. Кожен IPv6-пакет вимагає наявності базового заголовка IPv6, який містить основну інформацію про пересилання пакета і аналізується всіма пристроями на шляху пересилання [5].

На рис. 1.5. показано базовий заголовок IPv6.

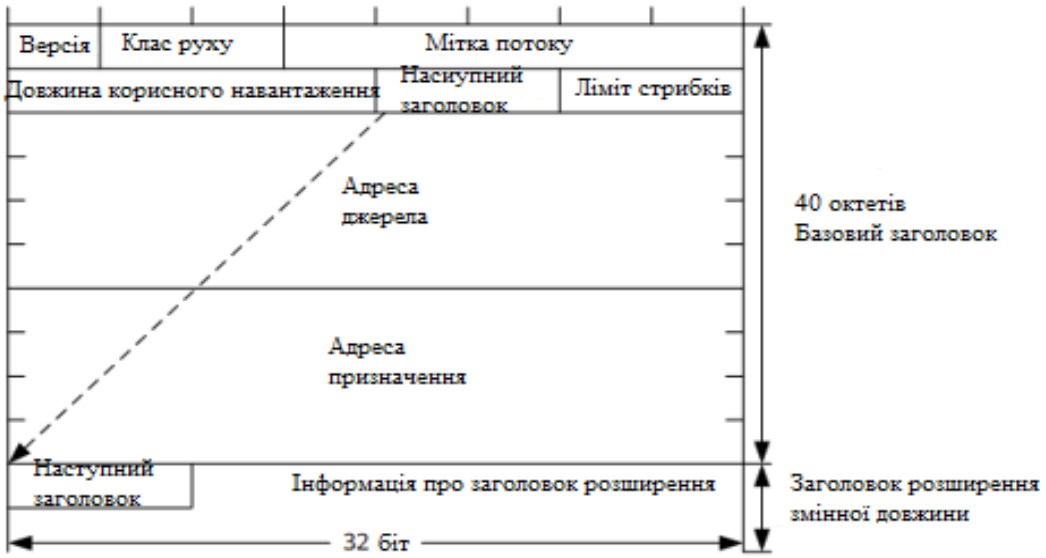

Рис. 1.5. Базовий заголовок IPv6

Базовий заголовок IPv6 містить такі поля:

- Версія: В IPv6 поле Версія має значення 6.
- Клас трафіку: 8 біт. Це поле вказує на клас або пріоритет пакета IPv6. Поле "Клас трафіку" подібне до поля TOS у пакетах IPv4 і в основному використовується для керування якістю обслуговування.
- Тег потоку: 20 біт. Це поле додається до IPv6, щоб розрізняти трафік. Мітка потоку та IP-адреса джерела ідентифікують потік даних. Мережеві посередники можуть ефективно розрізняти потоки даних на основі цього поля.
- Довжина корисного навантаження: 16 біт. У цьому полі вказується довжина корисного навантаження IPv6 в байтах. Корисне навантаження - це частина пакета IPv6, яка знаходиться після основного заголовка IPv6 і включає в себе заголовки розширення і PDU вищого рівня. Максимальне значення цього поля - 65535. Якщо довжина корисного навантаження перевищує 65535 байт, це поле встановлюється в 0, а параметр Jumbo Payload в заголовку Hop-by-Hop Options використовується для вказівки фактичної довжини корисного навантаження.
- Наступний заголовок: 8 біт. У цьому полі вказується тип першого заголовка розширення після основного заголовка IPv6 або тип протоколу PDU вищого рівня.
- Ліміт пропуску: 8 біт. Це поле схоже на поле "Час життя" в пакетах IPv4 і вказує максимальну кількість хопів, які може пропустити IP-пакет. Кожен пристрій,

що пересилає пакет, зменшує значення цього поля на одиницю, і коли значення поля досягає нуля, пакет відкидається.

- Адреса джерела: 128 біт. Це поле містить адресу джерела пакета.
- Адреса призначення: 128 біт. Це поле містить адресу призначення пакета.

На відміну від заголовків пакетів IPv4, заголовки пакетів IPv6 не містять IHL, ID, прапорів, зміщення фрагментів, контрольної суми заголовка, опцій і полів, але містять поля тегів потоку. Це робить обробку пакетів IPv6 простішою та ефективнішою. Для підтримки різних опцій без зміни існуючого формату пакетів до заголовка пакетів IPv6 додаються розширені інформаційні поля заголовка для підвищення гнучкості. У наступних параграфах описано розширений заголовок IPv6 [6].

1.3. Версії протоколу IP

Поточна версія IP-протоколу - фундаментального мережевого протоколу Інтернету - IPv4 була розроблена в 70-х роках минулого століття. Специфікація IPv4 була вперше опублікована як стандарт IETF RFC791 у 1981 році. На той час Інтернет називався ARPANET, налічував лише кілька сотень хостів і перебував під контролем Міністерства Оборони США. З того часу багато що змінилося, і технологія яка була призначена для військових, як і багато інших технологій, прийшла в побутове життя людини та Інтернет досі використовує протокол IP.

У протоколі IP цієї версії кожному вузлу мережі ставиться у відповідність IP-адреса довжиною 4 октету (4 байти), звідси і позначення протоколу цифрою 4. При цьому комп'ютери в підмережах об'єднуються загальними початковими бітами адреси. Кількість цих біт, загальне для даної підмережі, називається маскою підмережі (раніше використовувався розподіл простору адрес за класами - A, B, C; клас мережі визначався діапазоном значень старшого октету і визначав кількість вузлів, що адресуються в даній мережі, зараз використовується безкласова адресація).

У 1999 році було розроблено прокол IP нового покоління під номером 6. В даний час він вводиться в експлуатацію - IPv6, який дозволяє адресувати значно

більше вузлів, ніж IPv4. Ця версія відрізняється підвищеною розрядністю адреси, вбудованими можливостями шифрування та деякими іншими особливостями. Перехід з IPv4 на IPv6 пов'язаний з трудомісткою роботою операторів зв'язку та виробників програмного забезпечення, а також з чималими фінансовими витратами і не може бути виконаний миттєво. На середину 2010 року в Інтернеті було понад 3000 мереж, що працюють за протоколом IPv6. Для порівняння, на той саме час в адресному просторі IPv4 було більше 320 тисяч мереж, але в IPv6 мережі набагато більші, ніж в IPv4 [7].

Протокол IP Security (або як його ще називають IPSec) розроблений з метою реалізації захищеного обміну даними по протоколу IP. При цьому протокол IPSec дозволяє адміністратору вирішити такі завдання безпеки:

- забезпечення конфіденційності переданих даних;

контроль доступу;

- забезпечення цілісності переданих даних;
- захист від повторення;
- підтвердження справжності даних.

Протокол IPSec функціонує на мережевому рівні OSI. Принцип роботи протоколу зводиться до створення захищеного тунелю між двома хостами, які здійснюють обмін даними через відкриті мережі. Оскільки процес шифрування вимагає залучення значних обчислювальних ресурсів, у структурі протоколу IPSec виділяють два рівні забезпечення безпеки даних, що передаються.

Створення захищеного заголовка IP-пакету (Authentication Header, AH). Цей рівень передбачає захист заголовка пакета, що передається. Якщо використано лише цей рівень, дані пакета передаються у відкритому, незахищеному вигляді. Тим не менш, даний рівень найбільш оптимальний у ситуації, коли конфіденційність переданих даних не є критично важливою. Рівень безпеки AH дозволяє гарантувати цілісність даних, підтвердження справжності їх походження, і навіть захист від повторень.

Інкапсуляція вмісту пакету (Encapsulated Security Payload, ESP). На цьому рівні

реалізується захист вмісту пакета шляхом його шифрування.

Інтернет-протокол версії 4 (IPv4) - це протокол для використання в мережах з комутацією пакетів на канальному рівні (наприклад, Ethernet). IPv4 забезпечує можливість обробки приблизно 4,3 мільярда адрес.

Інтернет-протокол версії 6 (IPv6) є більш досконалим і кращим, ніж IPv4. IPv6 має можливість надавати необмежену кількість адрес. IPv6 прийшов на зміну IPv4, щоб обслуговувати зростаючу кількість мереж по всьому світу і вирішити проблему вичерпання IP-адрес [8].

Однією з відмінностей між IPv4 і IPv6 є зовнішній вигляд IP-адрес: в той час як IPv4 використовує чотири однобайтових десяткових числа, розділених крапками (наприклад, 192.168.1.1), IPv6 використовує шістнадцяткові числа, розділені двокрапкою.

Нижче наведено підсумок відмінностей між IPv4 і IPv6:

Таб. 1.6. Відміності між IPv4 і IPv6

	IPv4	IPv6
Кількість бітів в IP-адресі	32	128
Формат	десятковий	шістнадшятковий
Здатний до адрес	4,3 мільярда	нескінченна кількість
Як пінгувати	пінг xxx.xxx.xxx	ping6

Переваги IPv6 над IPv4:

- IPv6 спрощує роботу маршрутизаторів порівняно з IPv4.
- IPv6 більш сумісний з мобільними мережами, ніж IPv4.
- IPv6 дозволяє передавати більше корисного навантаження, ніж IPv4.
- IPv6 використовується менш ніж в 1% мереж, а в решті 99% все ще використовується IPv4.

1.3.1. Мережевий протокол IPv4

Протокол IPv4 був представлений наприкінці 1970-х років, вперше офіційно визначений у документі RFC 760 у січні 1980 року, а згодом замінений документом

RFC 791 у вересні 1981 року. На початку свого існування комп'ютерні мережі в Інтернеті налічували менше кількох тисяч хостів, тому описана кількість у 4,29 мільярда можливих IPv4-адрес здавалася занадто великою і неможливою для використання.

Пізніше, в 1990-х і на початку 2000-х років, з'явилася Всесвітня павутина (WWW), і кількість користувачів Інтернету значно зросла. Однак кількість підключених пристроїв все ще обчислювалася десятками мільйонів, і ємності адрес IPv4 здавалося достатньо на багато років вперед. Потім, на початку 2010-х років, мобільні пристрої почали домінувати в нашому житті, і кількість користувачів Інтернету зросла дуже швидко. На рисунку 1 показано, що в 2012 році було 8,8 мільярдів підключених пристроїв - як 8 мільярдів пристроїв можуть підключатися до глобальної мережі, коли є лише 4,29 мільярда IPv4 адрес?

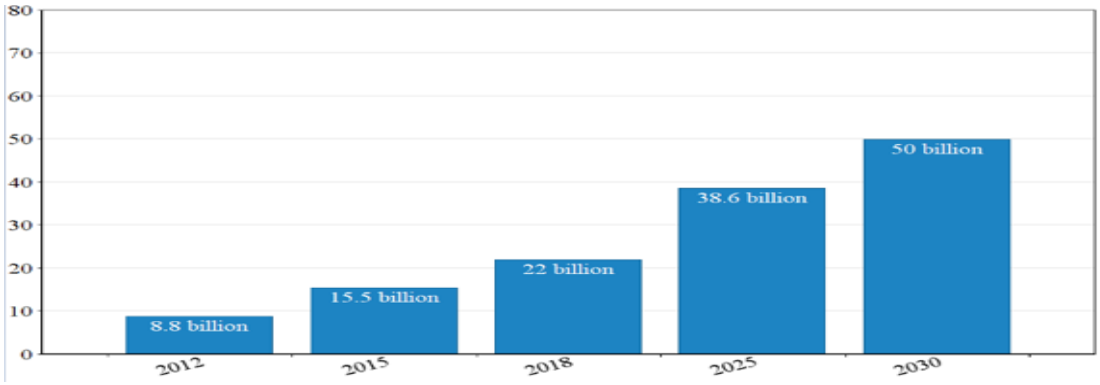

Рис. 1.7. Очікувана кількість підключених пристроїв до Інтернету до 2030

На початку 2000-х років мережеві технології, такі як мережеві проксі-сервери та трансляція мережевих адрес (NAT), були запроваджені як короткострокове рішення проблеми вичерпання публічних IPv4-адрес. Це дозволило внутрішнім мережам використовувати приватні діапазони адрес IPv4 (зазвичай 10.xxx, 172.16.xx і 192.168.xx) і використовувати єдину публічну IPv4-адресу для зв'язку з публічним Інтернетом. Однак кожна приватна мережа потребує принаймні однієї публічної IPv4-адреси.

IPv4-адреси можуть бути виражені в будь-якій системі числення, що представляє 32-бітне ціле число. Найпоширенішим є крапковий запис, де чотири

октети адреси представлені окремо в десятковій системі числення і розділені крапками.

Наприклад, IP-адреса 192.0.2.235 в десятковій системі числення з крапками представляє 32-бітне десяткове число 3221226219, яке в шістнадцятковій системі числення має вигляд 0xC00002EB.

Запис CIDR - це компактна комбінація адреси та префікса маршрутизації, де після адреси ставиться скісна риска (/) і перший біт префікса маршрутизації (маска підмережі).

Інші способи представлення адреси були поширені в часи, коли була реалізована мережа на основі класів. Наприклад, адреса зворотного зв'язку 127.0.0.1 зазвичай представляється як 127.1, тому що ця адреса належить до мережі класу A з 8-бітовою маскою підмережі і 24-бітним номером хоста. Якщо адреса містить чотири цифри або менше в десятковій системі числення, останнє значення розглядається як ціле число, що відповідає кількості байт, необхідних для завершення адреси в чотирьох октетах. Таким чином, адреса 127.65530 еквівалентна 127.0.255.250.

IPv4 використовується в мережах з комутацією пакетів, таких як Ethernet IPv4 забезпечує логічний зв'язок між мережевими пристроями шляхом ідентифікації кожного пристрою IPv4 надає можливість конфігурування всіх типів пристроїв, включаючи ручне та автоматичне конфігурування залежно від типу мережі [9].

IPv4 забезпечує спосіб конфігурації всіх типів пристроїв, включаючи ручну та автоматичну конфігурацію.

IPv4 базується на моделі найкращих зусиль. Ця модель не гарантує доставку або уникнення перевантажень. Ці питання вирішуються транспортом вищого рівня. IPv4 була основною версією в практичному використанні ARPANET в 1983 році. Версія 4 Інтернет-протоколу визначає, як працює адресація, як можна ідентифікувати мережеві хости і визначити їх місцезнаходження в мережі. Адреси IPv4 представлені у вигляді 32-бітових значень, організованих у чотири октети (4x8), зазвичай виражених у вигляді десяткових чисел, включаючи крапки, як показано нижче: 172.140.153.12.

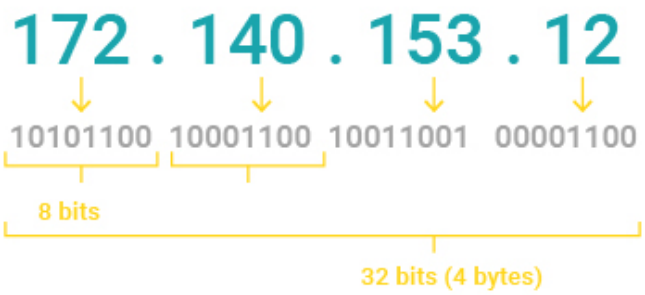

Рис.1.8. Анатомія адреси IPv4

Характеристики IPv4:

- IPv4 може бути 32-бітною IP-адресою.
- IPv4 може бути цифровою адресою з бітами, розділеними крапками.
- Кількість полів заголовка - 12, а довжина полів - 20.
- Існують одноадресні, широкомовні та багатоадресні формати адрес.
- IPv4 підтримує маску підмережі віртуальної довжини (VLSM).
- IPv4 використовує протокол дозволу поштових адрес для відображення MAC-адрес.
- Мережа повинна бути спроектована вручну або використовуватися DHCP.
- Дозволити фрагментацію пакетів маршрутизаторами та хостами, що викликають.

1.3.2. Мережевий протокол IPv6

На початку 1990-х років Робоча група з розробки Інтернету (IETF) почала обговорювати стрімке зростання кількості користувачів Інтернету та збільшення розміру таблиці маршрутизації в Інтернеті. Тоді було вирішено, що настав час розпочати розробку нового протоколу мережевого рівня, який міг би подолати обмеження поточного IPv4 і підтримати майбутні мережеві розробки. Після оцінки низки пропозицій і проектів, у грудні 1998 року набір протоколів, відомий як IPv6, був включений до проекту стандарту IETF. У 1999 році Адміністрація з присвоєння номерів в Інтернеті (IANA) запустила регіональний реєстр Інтернету з першим розподілом публічних блоків адрес IPv6.

IPv6 - це остання версія Інтернет-протоколу, розроблена Робочою групою з розробки Інтернет-технологій (IETF) для ідентифікації та визначення місцезнаходження кінцевих систем у комп'ютерних мережах і маршрутизації Інтернет-трафіку, а також для забезпечення подальшого використання Інтернету в усьому світі. Вона вирішує проблему вичерпання адрес IPv4 через його постійне використання.

Інтернет-протокол версії 6 (IPv6) - це протокол мережевого рівня для обміну даними в мережі. Кожен пристрій в Інтернеті має унікальну IP-адресу, яка використовується для його ідентифікації та визначення місцезнаходження, під час цифрової революції 1990-х років стало зрозуміло, що IP-адреси, які використовувалися Інтернет-протоколом версії 4 (IPv4) для підключення пристроїв, не можуть задовольнити попит.

Тому IETF почала розробляти наступне покоління інтернет-протоколів: IPv6 став проектом стандарту IETF у грудні 1998 року і був затверджений як стандарт Інтернету для глобального впровадження 14 липня 2017 року.

Адреси IPv6 використовують 128 біт, що в чотири рази більше, ніж адреси IPv4, які використовують лише 32 біти. Адреси IPv6 записуються в шістнадцятковій системі числення, а не в десятковій з крапками, як в IPv4 Шістнадцяткова система використовує 4 біти, тому адреса IPv6 складається з 32 шістнадцяткових цифр. Ця адреса складається з 32 шістнадцяткових цифр.

Існує три типи IPv6 адрес

Глобальні одноадресні адреси: Це адреси, що маршрутизуються через Інтернет і починаються з 2001:. Префікс міжнародної одноадресної адреси походить від адреси, яку маршрутизатор публікує в мережевій рекламі. Це те саме, що й глобальна адреса IPv4; SLAAC розшифровується як автоконфігурація адрес без статусу, що вимагає блоку з 64 адрес. Влада Інтернету надає блоки адрес постачальникам послуг Інтернету (ISP), щоб вони могли пропонувати їх своїм клієнтам. В даний час рекомендується, щоб домашні сайти мали більше, ніж одну 64-адресу.

Унікальна локальна адреса: адреса, призначена для використання у внутрішній мережі, наприклад, локальній мережі. Вона маршрутизується у внутрішній мережі, але не в Інтернеті. Простір розподілу адрес розділено на два поля /8: fd00::/8 для глобальних адрес і fd00::/8 для локальних адрес.

Локальна адреса: адреса, призначена для використання у внутрішній мережі. Вони маршрутизуються у внутрішній мережі, але не в Інтернеті. Вона також схожа на IPv4-адресу 169.254.0.0/16, призначену в мережах IPv4 без DHCP-сервера. Локальні адреси починаються з префікса fe80. Навіть без маршрутизації на кожному інтерфейсі IPv6 необхідно налаштувати адресу локального з'єднання.

На перший погляд, багато інженерів вважають, що IPv6 - це просто більший адресний простір, а в іншому він ідентичний IPv4. Однак виявляється, що IPv6 - це більше, ніж просто довші адреси: головною метою при розробці IPv6 було забезпечення наскрізної безпеки, якості обслуговування, більшого адресного простору та простішого й ефективнішого формату заголовків. В результаті в порівнянні з IPv4 були зроблені наступні поліпшення:

- Новий формат заголовка - більшість несуттєвих полів заголовка IPv4 було вилучено з заголовка IPv6, що зробило його більш ефективним для проміжних маршрутизаторів.
- Розширюваність - IPv6 розроблений таким чином, щоб його можна було легко розширити, додавши заголовок розширення після заголовка IPv6.
- Великий адресний простір - IPv6 має 128-бітний адресний простір, що дозволяє створювати кілька рівнів підмережі та ефективніше розподіляти адреси від регіональних провайдерів.
- Покращена безпека - IPSec є вбудованою частиною протоколу IPv6; IPv6 має розширення заголовків для спрощення реалізації шифрування та автентифікації.
- Адресація хостів зі статусом і без нього (SLAAC) - за відсутності DHCP-сервера хости в локальній мережі можуть автоматично отримати IP-адресу і почати користуватися мережею.

- Більш ефективна взаємодія в локальній мережі. Широкомовний протокол ARP замінено на більш ефективний протокол ICMPv4 Neighbour Discovery, який використовує групові широкомовні повідомлення замість широкомовних.
- Кілька IPv6-адрес на пристрій - хости можуть мати кілька IPv6-адрес в одній підмережі. Це забезпечує підвищену безпеку, покращену конфіденційність і додаткову мережеву функціональність.

Нові типи адрес Пакет IPv6 включає нові типи адрес мережевого рівня, такі як не маршрутизовані локальні адреси IPv6.

Важливо зазначити, що багато інших протоколів і функцій у мережі зміняться через різну довжину IPv6-адрес. Наприклад, більшість протоколів маршрутизації покладаються на розуміння IPv4-адрес і включення їх в оновлення та інші повідомлення. Тому для підтримки IPv6 необхідно змінити формат повідомлень, що часто призводить до переписування всього протоколу маршрутизації. Така ж логіка застосовується і до деяких протоколів верхнього рівня. В результаті перехід з IPv4 на IPv6 набагато складніший, ніж зміна однієї IP-адреси з v4 на v6 [10].

РОЗДІЛ 2
АНАЛІЗ ВЕРСІЇ ПРОТОКОЛУ IP

2.1. Аналіз версії протоколу IP

Адреса. IPv4. Довжина 32 біти (4 байти). Адреса складається з мережевої адреси та адреси хоста. Довжина цих компонентів залежить від класу адреси. Адреси поділяються на класи A, B, C, D і E. Клас адреси визначається першими кількома бітами адреси; загальна кількість адрес IPv4 становить 4 294 967 296.

У текстовому форматі IPv4-адреса має вигляд nnn.nnn.nnn.nnn, де 0<=nnn<=255, а кожна літера n означає десяткове число. Маленькі нулі можна опускати. Максимальна довжина адреси - 15 символів, не враховуючи маску.

В IPv6 довжина становить 128 біт (16 байт). Зазвичай перші 64 біти - це номер мережі, а другі 64 біти - номер хоста. У більшості випадків номер хоста або його складові в IPv6 отримують з MAC-адреси або іншого ідентифікатора інтерфейсу.

Для підмереж з декількома префіксами архітектура IPv6 є більш складною, ніж архітектура IPv4.

Кількість адрес IPv6 в 1028 разів (79 228 162 514 264 337 593 543 950 336) перевищує кількість адрес IPv4. IPv6-адреси записуються в текстовому форматі у вигляді xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, де кожна буква x є 4-бітним шістнадцятковим числом. Маленькі нулі можна опускати. У текстовому форматі подвійне двокрапку (::) можна замінити на будь-яку кількість нулів в адресі. Наприклад, ":ff:10.120.78.40" - це IPv6-адреса, перетворена в IPv4.

Розташування адреси. IPv4. Спочатку адреси розподілялися за мережевими класами. Однак, коли кількість вільних адрес почала стрімко зменшуватися, адреси були розділені за допомогою протоколу безкласової міждоменної маршрутизації (CIDR). Адреси були розподілені порівну між різними організаціями та країнами.

IPv6. розподіл адрес все ще перебуває на ранніх стадіях. Робоча група з розробки інтернету (IETF) і Рада з архітектури інтернету (IAB) рекомендують, щоб кожній організації, домашньому комп'ютеру або пристрою було виділено /48-бітовий префікс підмережі. Це залишає 16 біт префікса для ідентифікатора підмережі. Адресний простір достатньо великий, щоб дати кожному на планеті свій власний /48-бітний префікс підмережі.

Термін дії адреси. IPv4. Зазвичай ця властивість визначається лише для IPv4-адрес, виділених службою DHCP.

IPv6. Для IPv6-адрес вказуються дві дати закінчення терміну дії: бажана дата закінчення терміну дії та дата закінчення терміну дії, де бажана дата закінчення терміну дії завжди <= дата закінчення терміну дії.

Після бажаного терміну дії, якщо доступна рівноцінна привілейована адреса, вона більше не відображається як IP-адреса відправника для нових з'єднань. Після дозволеної дати закінчення терміну дії адреса більше не використовується (розпізнається) як IP-адреса отримувача або IP-адреса відправника для отримання пакетів.

Деякі адреси IPv6, такі як адреси канального рівня, за замовчуванням мають необмежений пріоритет і термін дії.

Префікс адреси. IPv4. Іноді використовується для того, щоб відрізнити мережу від адреси хоста. Суфікс /nnn також може використовуватися для вказівки адреси.

IPv6. Використовується для визначення префікса підмережі в адресі, вказаній як суфікс nnn (до 3 знаків після коми, 0 <= nnn <= 128). Приклад: fe80::982:2a5c/10, де перші 10 біт представляють префікс підмережі.

Протокол перетворення адрес (ARP). IPv4: ARP - це протокол IPv4, який використовується для визначення фізичних адрес, таких як MAC-адреси та адреси каналів зв'язку, пов'язаних з IPv4-адресами.

IPv6: IPv6 має ці функції вбудовано. Вони реалізовані в алгоритмах автоматичної конфігурації адрес і виявлення сусідів за допомогою протоколу ICMPv6. У цьому відношенні протокол ARP6 не був розроблений.

Простір адрес. IPv4. Цей термін не застосовується до звичайних адрес. Вважається, що існують спеціальні діапазони адрес і циклічні адреси. Всі інші адреси вважаються глобальними.

IPv6. IPv6 включає поняття адресного простору в свою архітектуру. Існує два звичайних адресних простори: адреси канального рівня і глобальні адреси. Групові адреси належать до 14 різних доменів. Зона, до якої належить адреса, враховується при виборі адрес відправника і одержувача за замовчуванням.

Зона - це екземпляр адресного простору в певній мережі, який в IPv6 може бути вказаний разом з ідентифікатором зони. Цей ідентифікатор вказується у форматі %zid, де zid - це номер (зазвичай короткий номер) або ім'я. Ідентифікатор зони вказується після адреси і перед префіксом: Наприклад,2ba::1:2:14e:9a9b:c%3/48.

Типи адрес. IPv4. IPv4-адреси поділяються на три типи: звичайні адреси, групові адреси та широкомовні адреси.

IPv6. IPv6-адреси зазвичай поділяються на три типи: звичайні адреси, групові адреси та нечіткі адреси.

Трасування з'єднань. В IPv4 трасування з'єднань - це спосіб збору детальної інформації, наприклад, про пакети TCP/IP, надіслані та отримані в системі; подібна підтримка доступна і в IPv6.

Налаштування. IPv4. Перш ніж нова система зможе встановити з'єднання з іншою системою, її потрібно налаштувати. Це означає, що необхідно визначити IP-адреси та маршрути.

IPv6. потрібно налаштувати лише деякі функції: IPv6 може використовуватися з будь-яким адаптером Ethernet і може працювати на будь-якому інтерфейсі зі зворотним зв'язком. інтерфейс IPv6 конфігурується шляхом автоматичного

встановлення IPv6 без збереження його стану. Інтерфейси IPv6 також можна налаштувати вручну. В результаті він може підключатися до інших локальних або віддалених IPv6-систем залежно від типу мережі та наявності IPv6-маршрутизатора.

Система доменів (DNS). Програми можуть використовувати DNS для перетворення імен хостів в IP-адреси за допомогою API сокета gethostbyname(). Програми також можуть використовувати DNS для перетворення IP-адрес в імена хостів. Для цього використовується API gethostbyaddr(); у IPv4 для зворотного перетворення використовується домен in-addr.arpa.

Така ж підтримка доступна і для IPv6: Для підтримки IPv6 використовується тип запису AAAA (4-символьна A) і функція зворотного перетворення (IP-адреса в ім'я). Програма отримує IPv6-адресу з DNS і може вибрати, чи встановлювати з'єднання за цією адресою.

API сокета gethostbyname() підтримує лише IPv4; для IPv6 використовується новий API getaddrinfo(), який дозволяє програмам за бажанням отримувати лише IPv6-адреси або інформацію про IPv4 та IPv6. ipv 6 зворотне перетворення використовує домен ip6.arpa. Якщо перетворення не вдається, використовується домен ip6.int.

Протокол динамічного налаштування хостів (DHCP). IPv4. dhcp використовується для динамічного отримання IP-адрес та іншої інформації про конфігурацію. IBM і підтримує DHCP-сервери для IPv4. IBM і підтримує сервери DHCP для IPv4.

Реалізація DHCP на IBM і не підтримує IPv6. Однак можна використовувати програму ISC DHCP-сервер.

Протокол передачі файлів (FTP). FTP використовується для надсилання та отримання файлів через мережу; аналогічна підтримка доступна і для IPv6.

Фрагменти. Для IPv4. Якщо пакет занадто великий для передачі каналом зв'язку, відправник (хост або маршрутизатор) може розділити його на кілька частин.

В IPv6 В IPv6 пакети можуть бути розділені на частини лише на вузлі-відправнику. Збирати пакети можна лише на вузлі призначення. Використовуються заголовки розширення фрагментів.

Таблиця хостів. IPv4 - конфігурована таблиця, яка пов'язує IP-адреси з іменами хостів (наприклад, 127.0.0.1, циклічні адреси). Ця таблиця використовується програмою Socket Name Resolver. Програма викликається перед зверненням до DNS або після звернення до DNS, якщо перетворення не вдалося (порядок виклику залежить від пріоритету пошуку імен хостів).

Підтримується IPv6; така ж підтримка доступна і для IPv6.

Інтерфейс. IPv4: Логічний об'єкт, що використовується для пересилання пакетів у TCP/IP; в IPv4 це поняття завжди тісно пов'язане з адресами, а іноді еквівалентне адресам. Інтерфейси іноді також називають логічними інтерфейсами.

Інтерфейси IPv4 починають і припиняють роботу незалежно один від одного і від TCP/IP. Команди STRTCPIFC і ENDTCPIFC та System і Navigator використовуються для запуску і зупинки інтерфейсу.

Підтримується IPv6; така ж підтримка доступна для IPv6.

Протокол керуючих повідомлень Інтернет (ICMP). IPv4. Використовується в IPv4 для обміну інформацією про мережу.

Використовується в IPv6. Протокол IPv6 використовується з тією ж метою. Однак протокол керуючих повідомлень Інтернету версії 6 (ICMPv6) підтримує ряд нових функцій.

Основні типи повідомлень залишаються незмінними, наприклад, вузол призначення недоступний, ехо-запит, відповідь тощо. Нові типи і коди були додані для підтримки виявлення сусідів та інших пов'язаних функцій.

Протокол Інтернет для керування групами (IGMP). IPv4: IGMP використовується IPv4-маршрутизаторами для пошуку хостів, на які потрібно доставити багатоадресні дані. Він також використовується хостами IPv4 для

сповіщення маршрутизаторів IPv4 про те, що на хості є приймач багатоадресної розсилки.

В IPv6 IGMP замінено протоколом MLD, який виконує ті ж функції, що і протокол IGMP в IPv4. Він використовує протокол ICMPv6 і надає кілька нових типів пошуку, специфічних для MLD.

Заголовок IP. IPv4: довжина від 20 до 60 байт, залежно від кількості додаткових параметрів IP.

IPv6. Довжина - рівно 40 байт, в заголовку IP не вказуються додаткові параметри. Як правило, структура заголовка IPv6 простіша, ніж у IPv4.

Додаткові параметри заголовка IP. IPv4. різні додаткові параметри, які можуть бути вказані в заголовку IP (перед заголовком транспортного рівня).

IPv6. У заголовку IPv6 не вказуються додаткові параметри. Замість цього IPv6 додає додаткові заголовки. Ці заголовки можуть містити інформацію AH і ESP (як в IPv4), а також інформацію про транзитні сегменти, маршрути, фрагменти і транзит одержувача. Наразі IPv6 підтримує кілька розширених заголовків.

Байт протоколу в заголовку IP. IPv4 - код протоколу транспортного рівня. Приклад значення - ICMP.

IPv6 - заголовок, який вказується відразу після заголовка IPv6 і містить ті ж значення, що і поле протоколу заголовка IPv4. Після цього заголовка може бути вказано кілька додаткових заголовків, формат яких можна розширювати. Наступні заголовки можуть бути заголовками транспортного протоколу, одним з додаткових заголовків або заголовками ICMPv6.

Байт Тип сервісу в заголовку IP. IPv4. використовується для визначення класу потоку даних залежно від QoS і диференційованих послуг.

IPv6. Для визначення класу трафіку IPv6 використовуються різні коди.

Наразі IPv6 не підтримує поле TOS.

З'єднання LAN. IPv4: LAN-з'єднання використовують IP-інтерфейс для підключення до фізичної мережі. Існує кілька типів, зокрема маркерне кільце та Ethernet. Іноді його також називають фізичним інтерфейсом, з'єднанням або лінком.

IPv6: IPv6 може використовуватися з будь-яким адаптером Ethernet, а також підтримується у віртуальних мережах Ethernet між логічними розділами.

Протокол L2TP. IPv4. протокол L2TP може використовуватися як віртуальний протокол PPP. Його можна використовувати при роботі з підтримуваними лініями зв'язку.

Підтримка IPv6.IPv6 також підтримується аналогічним чином.

Циклічна адреса. IPv4. Адреса зворотного зв'язку - 127.*. *. * (зазвичай 127.0.0.0.1) - це інтерфейс з адресою у форматі 127.0.0.1, який може використовуватися тільки вузлом для надсилання йому пакетів. Відповідний фізичний інтерфейс (опис лінії) називається *LOOPBACK.

Для IPv6; той самий принцип, що і для IPv4. Доступна єдина циклічна адреса - 0000:0000:0000:0000:0000:0000:0000:0000:0000:0000:0001,

або::1 (скорочена версія). Відповідний віртуальний фізичний інтерфейс називається *LOOPBACK.

Максимальний блок передачі. (MTU) Максимальна одиниця передачі - це максимальна кількість байт, яка може бути передана певним типом каналу зв'язку, наприклад, Ethernet або модемною лінією. Зазвичай максимальна одиниця передачі для IPv4 дорівнює 576.

В IPv6 мінімальний розмір MTU становить 1280 байт. Як наслідок, пакети IPv6, менші за цю межу, не фрагментуються; щоб передавати пакети IPv6 каналами зв'язку з розміром MTU менше 1280 байт, ці пакети потрібно лише розбити і зібрати на рівні каналу зв'язку.

Netstat. IPv4. netstat - це утиліта, яка надає інформацію про стан TCP/IP-з'єднань, інтерфейсів і маршрутів. Доступ до неї можна отримати за допомогою System і Navigator або текстового інтерфейсу. аналогічна підтримка доступна і для IPv6. Вона також доступна для IPv6.

Перетворення мережевих адрес (NAT). IPv4. одна з основних функцій брандмауера, вбудована в стек протоколів TCP/IP; налаштовується за допомогою System і Navigator.

IPv6. Функція NAT наразі не підтримує IPv6. Точніше, функція NAT для IPv6 не є обов'язковою: Адресний простір IPv6 було значно розширено, тому проблеми з нестачею адрес не існує. Протокол також забезпечує простіший спосіб зміни адрес.

Таблиця мереж. IPv4; У System і Navigator це таблиця з інформацією про імена мереж та IP-адреси. Маска мережі не вказується. Наприклад, хостом є мережа 14, а IP-адреса - 1.2.3.4. Ця таблиця залишається незмінною для IPv6.

Запитати інформацію про сайти IPv4. Не підтримується.

Підтримує IPv6, корисна мережева утиліта, подібна до утиліти Ping. Вона дозволяє запитувати імена хостів, звичайні IPv6-адреси або IPv4-адреси від інших IPv6-вузлів. Наразі ця утиліта не підтримується.

Фільтрування пакетів. IPv4. Фільтрація пакетів - це базова функція брандмауера, вбудована в стек протоколів TCP/IP. Для її налаштування використовуйте System і Navigator.

IPv6. фільтрація пакетів не підтримує IPv6. Переадресація пакетів.

Стек протоколів TCP/IP IBM і можна налаштувати на пересилання IP-пакетів, призначених для віддалених мережевих адрес. Зазвичай вхідні та вихідні інтерфейси підключаються до різних локальних мереж.

IPv6. пересилання пакетів підтримує IPv6 з обмеженнями. Стеки i5/OS TCP/IP не підтримують виявлення сусідів як маршрутизатор.

PING. Є основним засобом перевірки доступності хостів TCP/IP; він викликається за допомогою System і Navigator і текстового інтерфейсу; аналогічна підтримка доступна і для IPv6.

Двоточковий протокол. Дозволяє комутовані з'єднання з використанням різних модемів і ліній зв'язку; також підтримується IPv6.

Обмеження використання портів. IPv4. Ці меню IBM і дозволяють користувачеві вибрати номер порту TCP або UDP (User Datagram Protocol) або діапазон номерів портів, які можуть бути використані лише певним профілем.

IPv6. заборона портів IPv6 така сама, як показано нижче.

Порти. IPv4; TCP і UDP використовують різні набори портів, пронумеровані від 1 до 65 535.

IPv6. IPv6 використовує схожі порти. Оскільки протокол надає нове сімейство адрес, кількість наборів портів збільшилася до чотирьох. Наприклад, на 80-х є два TCP-порти, до яких можуть підключатися програми, один на AF_INET і один на AF_INET6.

Внутрішні та зовнішні адреси. IPv4. всі IPv4-адреси є зовнішніми. Єдиним винятком є три діапазони внутрішніх адрес, визначені IETF в RFC 1918, 10.*. *. * (10/8), 172.16.0.0 - 172.31.255.255.255 (172/16/12) і 192.168.*. * (192/168/16).

(192.168/16). Внутрішні адреси широко використовуються багатьма організаціями. Такі адреси не розпізнаються в Інтернеті.

IPv6. IPv6 використовує схожу структуру адрес, але є деякі важливі відмінності. Адреси поділяються на зовнішні та тимчасові (тимчасові адреси раніше називалися анонімними). Додаткову інформацію можна знайти в RFC 3041. На відміну від внутрішніх адрес в IPv4, тимчасові адреси розпізнаються в глобальній мережі. Вони використовуються для різних цілей. Тимчасові адреси приховують ідентифікатор клієнта, який встановлює з'єднання (з міркувань безпеки). Тимчасові адреси мають

обмежений термін дії. Такі адреси не містять ідентифікатора інтерфейсу, тобто адреси контролю доступу до середовища (MAC-адреси). Як правило, тимчасові адреси неможливо відрізнити від звичайних зовнішніх адрес.

IPv6 також має поняття "обмеженого адресного простору", заздалегідь визначеного розподілу адрес.

Таблиця протоколів. IPv4. system і Navigator - таблиця, що містить назви протоколів і відповідні номери портів. Наприклад: UDP, 17. За замовчуванням ця таблиця містить записи для наступних протоколів: IP, TCP, UDP, ICMP.

IPv6. Ця таблиця може бути застосована до IPv6 без змін. Якість обслуговування (QoS).

Для IPv4; Якість обслуговування дозволяє налаштувати пріоритет пакетів і пропускну здатність для TCP/IP додатків.

Для IPv6. Наразі QoS, реалізований на IBM і, не підтримує IPv6 [11].

Зміна адреси. Адреси можна змінювати вручну або за допомогою DHCP.

Зміна адрес комп'ютерів у мережі організації є дуже трудомістким завданням і тому рекомендується лише в разі крайньої необхідності.

IPv6. Розпізнавання адрес є важливою вбудованою функцією IPv6 і відбувається майже автоматично, особливо з префіксом /48.

Маршрут. Одна або більше IP-адрес, пов'язаних з парою значень, що містить ім'я фізичного інтерфейсу та IP-адресу наступного переходу; якщо адреса одержувача IP-пакету знаходиться в межах вказаної групи адрес, пакет пересилається по вказаному каналу до вказаного транзитного вузла Маршрут IPv4 пов'язаний з інтерфейсом IPv4 і, відповідно, з IPv4-адресою.

Маршрут за промовчанням називається *DFTROUTE. IPv6 схожий на IPv4. Але є одна важлива відмінність: Маршрути в IPv6 пов'язані з фізичними інтерфейсами (каналами зв'язку, такими як ETH03), а не з логічними інтерфейсами. Однією з

причин, чому маршрути пов'язані з фізичними інтерфейсами, є те, що IPv6 і IPv4 використовують різні алгоритми для вибору адрес відправників.

Протокол інформації про маршрутизацію (RIP). IPv4. rip - протокол маршрутизації, що підтримується демоном маршрутизації.

IPv6 демон. Наразі протокол RIP не підтримує IPv6. API сокетів.

Ці API доступні для додатків, які працюють з TCP/IP; зміни в сокетах з протоколом IPv6 не впливають на додатки, які не планують використовувати IPv6.

У IPv6 додатки, що використовують сокети в IPv6, можуть використовувати нове сімейство адрес: AF_INET6.

Зміни в IPv6 API не впливають на поведінку існуючих програм, що використовують протокол IPv4: Додатки, які повинні підтримувати потоки даних як IPv4, так і IPv6, або тільки потоки даних IPv6, можуть використовувати IPv4-адреси в форматі IPv6-адрес ::ffff:a.b.c.d для легкої адаптації.

Новий API підтримує перетворення IPv6-адрес з текстового формату в двійковий і навпаки.

Вибір адреси відправника. Програма може призначити IP-адресу відправника (зазвичай для цього використовується API сокета bind()). Якщо bind має значення IN-ADDR_ANY, адреса відправника вибирається з маршруту.

Для IPv6, як і для IPv4, програма може використовувати bind() для призначення адреси відправника у форматі IPv6. Також можна використовувати функцію in6addr_any, щоб дозволити системі вибрати адресу відправника у форматі IPv6. Однак, оскільки в IPv6-з'єднанні може бути більше однієї IPv6-адреси, для вибору IP-адреси відправника використовуються різні внутрішні алгоритми.

Невизначена адреса. IPv4. Такого типу адреси не існує. Для сокетів у програмуванні використовується 0.0.0.0.0 як INADDR_ANY.

IPv6. дорівнює ::/128 (128 нульових бітів). Вказується як IP-адреса відправника у деяких пакетах під час пошуку сусідів, а також використовується при роботі з сокетами. У реалізаціях API сокетів адреса::/128 використовується як in6addr_any.

Запуск та завершення роботи. Команди STRTCP і ENDTCP використовуються для ініціалізації та завершення роботи IPv4. IPv4 зазвичай ініціалізується, коли виконується команда STRTCP для ініціалізації TCP/IP.

IPv6 використовується для запуску або завершення роботи IPv6 за допомогою параметра STRIP6 або команд STRTCP і ENDTCP IPv6 може не запускатися під час запуску TCP/IP IPv6 може бути запущений пізніше.

Встановлення параметра AUTOSTART у значення *YES (за замовчуванням) автоматично запускає всі інтерфейси IPv6; IPv6 не можна використовувати або конфігурувати без IPv4. Інтерфейс зворотного зв'язку IPv6::1 буде автоматично виявлено і ввімкнено під час запуску IPv6 [12].

2.2. Переваги та недоліки

Перерахуємо загальні недоліки протоколу IPv4:

- дефіцит адресного простору - кількість різних пристроїв, що підключаються до мережі Internet, зростає експоненційно, розмір адресного простору на даний час вже вичерпався;
- слабка розширюваність протоколу - недостатній розмір заголовка IPv4, що не дозволяє розмістити необхідну кількість додаткових параметрів у ньому;
- проблема безпеки комунікацій – не передбачає будь-яких засобів для розмежування доступу до інформації, розміщеної в мережі.
- відсутня підтримка якості обслуговування - не підтримує розміщення інформації про пропускну здатність, затримки, необхідні для нормальної роботи деяких мережевих додатків;

- проблеми, пов'язані з механізмом фрагментації - не визначає розмір максимального блоку передачі даних по кожному конкретному шляху;
- відсутня механізм автоматичної конфігурації адрес;
- проблема перенумерації машин.

Крім явної переваги в розширенні адресного простору, можна виділити такі переваги IPv6 над IPv4:

- можливість автоконфігурування IP-адрес.
- спрощення маршрутизації.
- полегшення (спрощення) заголовка пакета.
- підтримка якості обслуговування (QoS).
- наявність можливості криптозахисту дейтограм на рівні протоколу.
- підвищена безпека передачі даних.

Розробники мережного обладнання активно пропагують серед операторів та корпоративних замовників переваги шостої версії протоколу IP, такі як: спрощений заголовок фіксованої довжини, відсутність контрольної суми заголовка, великий адресний простір, класифікація адрес, автоматичне конфігурування та ін.

Інтернет-протокол версії 6 (IPv6) - це інтернет-протокол, який використовується для маршрутизації трафіку в Інтернеті. Він також вирішує проблему закінчення IPv4-адрес.

IPv6 пересилає пакети від комп'ютера-джерела до комп'ютера-одержувача; IPv4 був розроблений у 1980-х роках, коли Інтернет перебував у зародковому стані, а кількість адрес, що надаються Інтернетом, була непередбачуваною.

IPv4 не підтримує достатню кількість адрес для підключення всіх пристроїв по всьому світу.

- Підтримується лише 4,3 мільярда адрес.
- Адресний простір IPv4 недостатньо розподілений, використовується лише 14 відсотків усіх доступних адрес.

IPv6 - це оновлена версія, розроблена Робочою групою з розробки інтернету (IETF) у грудні 1998 року на заміну IPv4, що дозволяє більшій кількості пристроїв підключатися до адресного простору, доступного в IPv4.

Переваги IPv6:

- Більш потужний інтернет
- Розподіл адрес здійснюється самим пристроєм
- Захищає безпеку за допомогою Internet Protocol Security
- Дозволяє легко збирати префікси, призначені для IP-мережі.
- Великі пакети даних можна надсилати одночасно, заощаджуючи пропускну здатність.

Недоліки IPv6:

- Забезпечити плавний перехід з IPv4 на IPv6.
- IPv6 недоступний на машинах, що використовують IPv4.
- Час переходити на IPv6
- IPv4 все ще широко використовується, але світ поступово переходить на IPv6
- Всі витрати, які несуть користувачі при заміні машин з IPv4
- Перехід з IPv4 на IPv6 - трудомісткий і громіздкий процес.
- Розуміння IPv6-повідомлень є складним, не кажучи вже про спроби запам'ятати свою IPv6-адресу
- Пристрої IPv4 та IPv6 не можуть обмінюватися даними безпосередньо один з одним навіть у найекстремальніших випадках.

Оновні плюси

IPv6 дозволяє всім пристроям безперебійно підключатися до мережі IPv6 має багато переваг перед IPv4, окрім більшого адресного простору.

- Ефективна маршрутизація. Це робить таблиці маршрутизації більш ефективними, обмежуючи їх розширення і дозволяючи ієрархічне розподілення адрес. Це полегшує агрегацію маршрутів в Інтернеті.

Для призначення маршруту використовується спеціальний протокол MTU (Maximum Transmission Unit).

- Мультимаршрутизація. IPv6 спрощує процес розгортання завдяки використанню багатоадресної розсилки в Інтернеті та додатковій оптимізації. Він також забезпечує мобільність пристроїв і вирішує конфігураційні аспекти дизайну протоколу. Він також забезпечує наскрізний зв'язок, надаючи більше транспортних рівнів, які дозволяють виявляти несправності.
- Направлена місцева адреса. IPv6 підтримує широкомовну передачу, де він дозволяє глибокі потоки пакетів. Він забезпечує ефективний потік даних між мультимедійними потоками. У ньому також є нове поле під назвою Flow Label , яке розпізнає пакети, що належать одному потоку.
- Збільшена ємність і конфігурація мережі. Ресурси ефективно розподіляються для розміщення інших веб-адрес. Після того, як маршрутизатор надсилає префікс локального з'єднання, хост додає адресу з'єднання, перетворену в 64-бітовий формат, до 64 біт префікса локального з'єднання, щоб сформувати свою власну IP-адресу. Це забезпечує більш швидке середовище зв'язку.
- Більше мобільності. IPv6 запобігає трикутній маршрутизації. Трикутна маршрутизація - це форма маршрутизації, яка надсилає з'єднання на проксі-систему, перш ніж перенаправляти його до місця призначення. Це дозволяє перемістити всі підмережі до нової точки маршрутизації без необхідності перенумерації.

Основні мінуси

- Системні проблеми. Маршрутизація IPv6 має бути ввімкнена залежно від системи, що використовується. Якщо вводити вручну, необхідно ввести довгу IP-адресу. IP-адреси зазвичай дуже довгі і містять літери та цифри, тому їх необхідно запам'ятовувати.
- Складність у кресленнях топології мережі. IPv4-адреси були короткі за довжиною і їх було легко наносити на топологічні схеми; префікси IPv6 ускладнюють завдання; в IPv6 символи майже не читаються.

- Оновлення пристроїв. Комерційним організаціям необхідно модернізувати своє мережеве обладнання, оскільки воно не призначене для впровадження IPv6. Це стосується не лише організацій, які регулярно оновлюють своє обладнання.
- Зміни локальної мережі. В управлінні локальною мережею IP-адреси призначаються певним пристроям, тому вручну призначати нові IP-адреси може бути складним завданням.
- Плутанина в схемах IP. Під час переходу з IPv4 на IPv6 може виникнути плутанина через відсутність зворотної сумісності; провайдерам доведеться нести витрати на підтримку IPv6, щоб обережно перемикатися між різними протоколами [13].

2.2.1. Переваги спільного використання IPv6 та IPv4

Багато організацій хочуть розширити свої мережі на IPv6, але все ще використовують обладнання IPv4 через відсутність зворотної сумісності з IPv4.

Існує три основні варіанти переходу на IPv6 з існуючої мережевої інфраструктури. Ці варіанти збільшують переваги перекладу завдяки аналізу ситуаційних і технічних сценаріїв.

- Мережа з двома стеками. Мережеві пристрої працюють з IPv4 та IPv6. Комп'ютери, маршрутизатори та комутатори працюють з обома протоколами, але перевага надається протоколу IPv6. Обидва протоколи TCP/IP увімкнено на маршрутизаторах глобальної мережі (WAN), потім на брандмауерах, маршрутизаторах центру обробки даних і, нарешті, на маршрутизаторах доступу до робочого столу. Перевага цього підходу полягає в тому, що він підтримується основними мережевими постачальниками.
- Тунелювання. Скорочуючи пакети IPv6 до пакетів IPv4 і навпаки, один протокол тунелює в інший. Це має перевагу в адаптації нових протоколів і забезпеченні підключення користувачів без порушення роботи старих

протоколів. Однак, головним недоліком цих варіантів є те, що нові користувачі протоколу не можуть спілкуватися зі старими користувачами протоколу без двостекового хоста.

2.2.2. Обмеження IPv4 і потреба в IPv6

Адреси IPv4 вичерпувалися через стрімке зростання кількості користувачів Інтернету, інтенсивне використання таких пристроїв, як мобільні телефони, ноутбуки та комп'ютери, неефективне використання адрес і постійно ввімкнені пристрої, такі як кабельні модеми. Щоб пом'якшити проблему виснаження адреси в IPv4, були розроблені такі технології, як класові мережі, безкласова міждоменна маршрутизація та трансляція мережевих адрес. Ці технології зробили внесок у рішення, удосконаливши магістраль систем розподілу веб-адрес і маршрутизації.

Пакет IPv6 складається з 40 розширених октетів, щоб користувачі могли масштабувати протокол у майбутньому, не порушуючи його основну структуру. Пакет має дві частини: заголовок і корисне навантаження. IPv6 представив jumbograms, які дозволили пакету обробляти понад 2^32. Джамбограми підвищують продуктивність у зв'язках з високим максимальним блоком передачі (MTU) і справляються з корисним навантаженням.

Крім того, IPv6 має 128-бітну адресу та більший адресний простір, доступний для майбутнього розподілу. 128-бітна адреса розбита на 8 груп, кожна з яких містить 16 біт. Чотири шістнадцяткові числа представляють кожну групу, а двокрапки використовуються для відокремлення кожної групи від інших. IPv6 надає хосту, підключеному до мережі, унікальний ідентифікатор, специфічний для підмережі.

Структура адресації IPv6, встановлена в RFC 4291, дає змогу здійснювати три різні типи зв'язку — тобто одноадресний, будь-який та багатоадресний методи зв'язку.

РОЗДІЛ 3
МОДЕЛЮВАННЯ МЕРЕЖІ НА БАЗІ ПРОТОКОЛУ IPV6 З ВИКОРИСТАННЯМ ПРОГРАМНОГО ПАКЕТУ PACKET TRACER

3.1. Огляд Packet Tracer

Cisco Packet Tracer - це програмне забезпечення для моделювання від Cisco. Його можна використовувати для створення складних типологій мереж, тестування та моделювання абстрактних мережевих концепцій. Він діє як ігровий майданчик для дослідження мереж і забезпечує досвід, дуже близький до того, що ви бачите в комп'ютерних мережах.

Він також пропонує послуги такими мовами, як німецька, іспанська та французька. Packet Tracer може створювати складні та великі мережі, які зазвичай неможливі за допомогою фізичного обладнання через його вартість, і доступний для Linux, Windows, MacOS, Android та iOS.

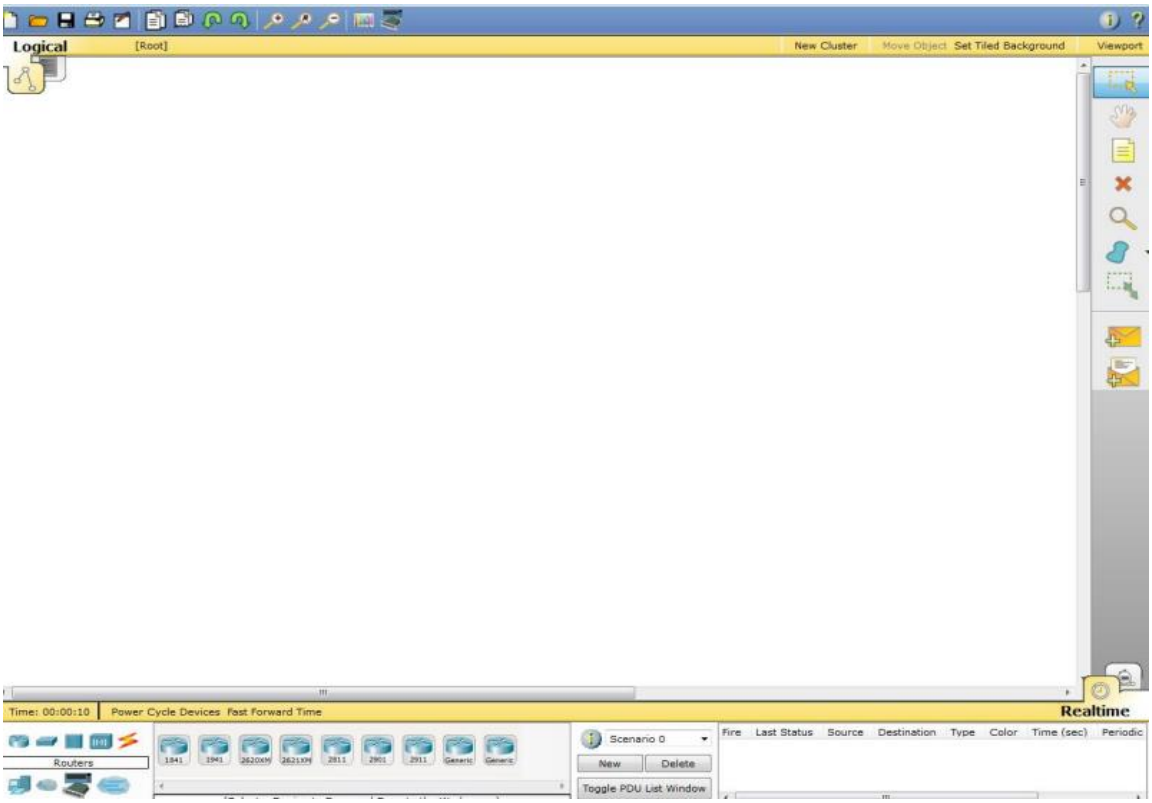

Рис. 3.1. Інтерфейс програмного продукту Packet Tracer

Більшу частину вікна займає робоча область, де різні мережеві пристрої можуть бути розміщені і підключені різними способами, що призводить до різних топологій мережі.

Над робочою областю знаходиться головна панель і меню програми (Рис. 3.2.). Меню дозволяє користувачеві зберігати і завантажувати мережеві топології, налаштовувати симуляції і виконувати багато інших цікавих функцій. Головна панель містить найбільш часто використовувані функції меню.

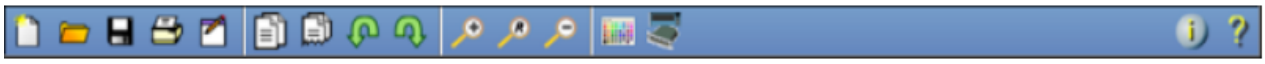

Рис. 3.2. Головне меню Packet Tracer

Праворуч від робочої області знаходиться бічна панель з набором кнопок для переміщення полотна робочої області та видалення об'єктів. Нижче робочої області знаходиться панель обладнання (Рис. 3.3.).

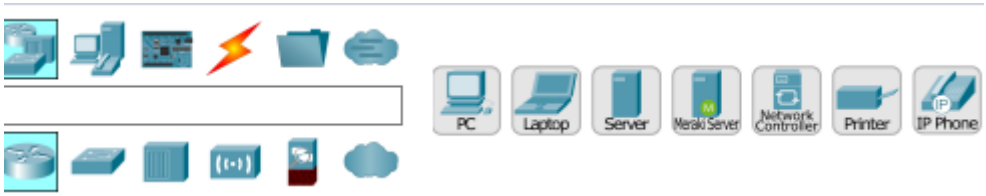

Рис. 3.3. Панель обладнання Packet Tracer

Ця панель показує типи пристроїв, доступних з лівого боку, і моделі, доступні з правого боку. При виконанні різних експериментальних робіт ця панель, швидше за все, буде використовуватися частіше за інші. Розгляньмо її докладніше.

Коли ви наводите вказівник миші на кожен пристрій, його тип відображається у прямокутнику в центрі пристрою. Типи пристроїв, які зазвичай використовуються у Packet Tracer, показано на Рис. 3.4.

Рис. 3.4. Основні типи пристроїв

Не дуже корисно розглядати конкретну модель кожного пристрою. Це пов'язано з тим, що ця модель написана червоно-білим кольором безпосередньо під іконкою кожного пристрою. Окремо слід розглянути тип підключення. Перелічимо найпоширеніші з них (див. Рисунок 3.5, де типи з'єднань описані зліва направо).

Рис. 3.5. Типи з'єднань пристроїв у Packet Tracer

Автоматичний тип - За допомогою цього типу з'єднання PacketTracer автоматично вибирає найкращий тип з'єднання для вибраного пристрою.

Автоматично вибирає найкращий тип з'єднання для вибраного пристрою.

Консоль - підключення до консолі

Copper Straight-through - з'єднання мідного кабелю на основі витої пари, в якому обидва кінці кабелю обтиснуті за однаковою схемою. Підходить для таких з'єднань: комутатор до комутатора, комутатор до роутера, комутатор до комп'ютера тощо.

Мідний крос - з'єднання мідного кабелю витою парою, в якому два кінці кабелю обтиснуті по діагоналі, підходить для з'єднання двох комп'ютерів: комутатор до комутатора, комутатор до роутера, комутатор до комп'ютера і т.д.

Оптичний - з'єднання за допомогою оптичного кабелю, необхідне для підключення обладнання з оптичним інтерфейсом.

Телефонний кабель - звичайний телефонний кабель, який можна використовувати для з'єднання телефонів.

Коаксіальний кабель - коаксіальний кабель використовується для підключення пристроїв.

Програмне рішення Cisco Packet Tracer може імітувати роботу різних мережевих пристроїв, таких як маршрутизатори, комутатори, бездротові точки доступу, ПК, принтери та IP-телефони. Конфігурація залежить від типу обладнання: деякі з них використовують команди Cisco IOS, деякі - графічний веб-інтерфейс, а деякі - командний рядок операційної системи або графічні меню.

Режим візуалізації Cisco Packet Tracer дозволяє переглядати рух даних по мережі, переглядати і змінювати параметри IP-пакетів під час проходження даних через мережеві пристрої, а також контролювати швидкість і шлях проходження IP-пакетів. Аналізуючи події, що відбуваються в мережі, ви можете зрозуміти, як працює мережа, і виявити помилки.

Cisco Packet Tracer можна використовувати не тільки як симулятор, але і як мережевий додаток, що імітує віртуальну мережу поверх реальної мережі, включаючи Інтернет. Користувачі з різних комп'ютерів, незалежно від їх місцезнаходження, можуть налаштовувати і шукати несправності, використовуючи одну і ту ж топологію мережі, і ця особливість багатокористувацького режиму Cisco Packet Tracer широко використовується для організації командної роботи або для ігор і змагань.

Cisco Packet Tracer дозволяє користувачам покращити свої навички проектування, імітуючи створення логічних і фізичних моделей мережі. Мережеві схеми можна накладати на креслення реальних будівель і міст для проектування цілих кабельних систем або розміщення обладнання в конкретних будівлях або приміщеннях з урахуванням фізичних обмежень, таких як довжина і тип кабелю, що прокладається, і радіус зони покриття бездротової мережі.

Моделювання, візуалізація, багатокористувацький режим і функції проектування роблять Cisco Packet Tracer унікальним інструментом для навчання мережевим технологіям.

3.2. Моделювання мережі на основі IP за допомогою Packet Tracer

Для цієї кваліфікаційної роботи побудовано дві ідентичні топології (Рис. 3.6.), одна з яких працює повністю з протоколом IPv4, а інша з IPv6.

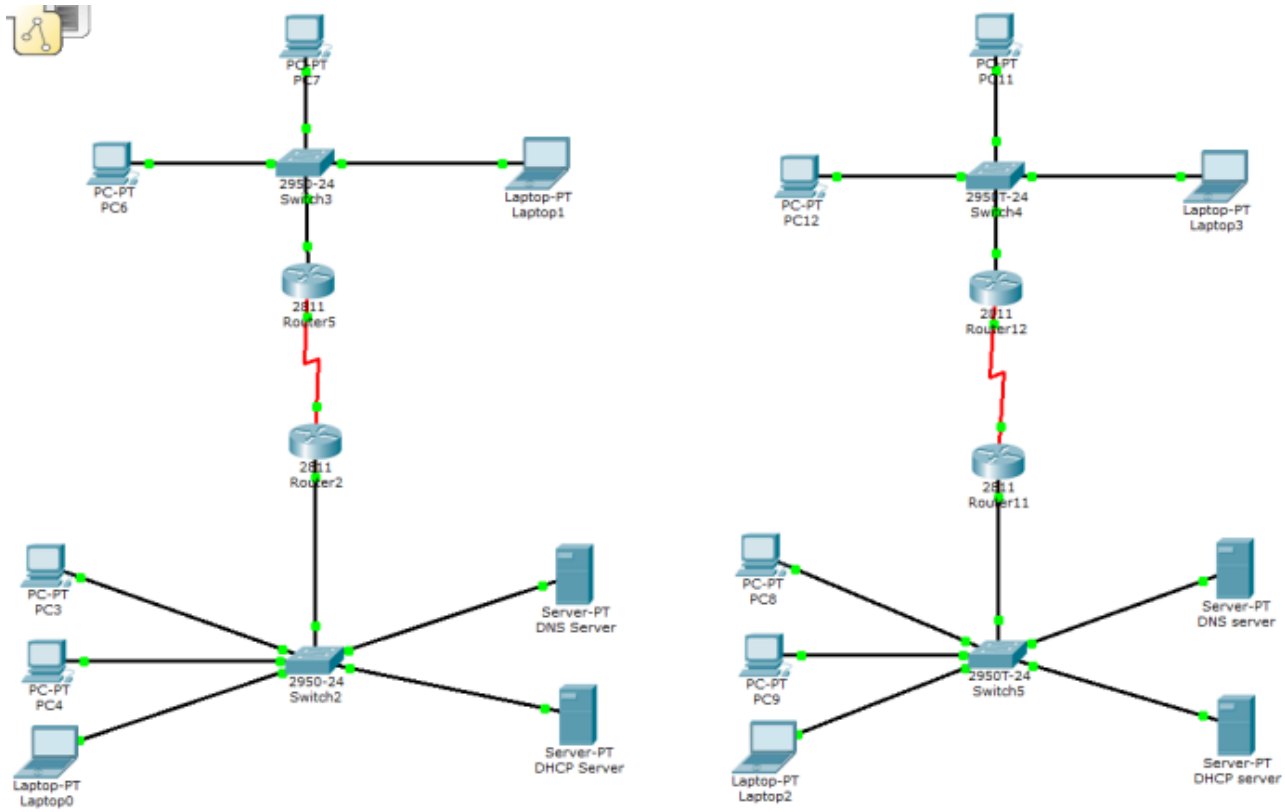

Рис. 3.6. Топологія мережі IPv4 і IPv6

Оскільки це програмне забезпечення працює лише з продуктами CISCO, використовувалися комутатори, маршрутизатори та сервери CISCO. У таблиці 3.1 наведено короткий опис використаного обладнання.

Найменування	Кількість
Маршрутизатор Cisco 2811	4
Комутатор Cisco 2950-24	4
Сервер	3
Персональний комп'ютер	12

Табл. 3.1. Використовувані пристрої

Маршрутизатори Cisco серії 2811 мають гнучку модульну конструкцію. Пристрої мають слоти для встановлення мережевих модулів (NME), інтерфейсних модулів (HWIC) і додаткових голосових інтерфейсів (EVM), а також спеціальні слоти для встановлення модулів обробки та обслуговування голосу (PVDM і AIM) на системній платі маршрутизатора. Інтерфейси NME і HWIC мають зворотну сумісність з модулями NM і WIC відповідно.

Технічні характеристики.

Підтримка модулів WIC/VWIC/NM/AIM/VVIC; комутація L2 (опціонально) і підтримка PoE.

Високопродуктивний захист голосових каналів (T1/E1/xDSL).IOS IOS захищає маршрутизатори Cisco 2811 від вірусів.

Контроль доступу до мережі (NAC).

Організація аналогових і цифрових голосових з'єднань.

Програмне забезпечення для обробки голосових викликів Cisco CallManager Express (Cisco CME - до 36 IP-телефонів).

Catalyst 2950-24 - комутатор серії Cisco Catalyst 2950 - 24-портовий 10/100 BaseTX RJ-45, максимальна кількість мережевих MAC-адрес - 8000, комутаційна шина 8,8 Гбіт/с, максимальна швидкість комутації 4,4 Гбіт/с, споживана потужність 30 Вт.

Cisco Catalyst 2950-24 - комутатор серії Cisco CAtalyst 2950 - 24 x 10/100 BaseTX RJ-45 порти, максимальна кількість мережевих MAC-адрес - 8000, комутаційна шина 8,8 Гбіт/с і максимальна швидкість комутації 4,4 Гбіт/с, споживана потужність 30 Вт.

Серія Cisco Catalyst 2950 з гігабітною мідною магістраллю 10/100/1000BaseT Серія Cisco Catalyst 2950 надає компаніям середнього бізнесу та багатоофісним підприємствам можливість переходу від Fast Ethernet до більш високопродуктивних мереж з використанням мідного кабелю категорії 5. Це ідеальне рішення для переходу до магістралі Gigabit Ethernet з використанням мідного кабелю категорії 5.

Комутатор Cisco 2950 підтримує технології Fast EtherChannel і Gigabit EtherChannel, забезпечуючи пропускну здатність до 4 Гбіт/с між комутаторами, маршрутизаторами і серверами Catalyst.

У моделюванні мережі IPv4 використовувалися DHCP-сервери, а також DNS-сервери; DHCP - це мережевий протокол. Протокол працює в моделі клієнт-сервер.

Модель "клієнт-сервер". Для автоматичного налаштування клієнтський комп'ютер встановлює з'єднання з так званим DHCP-сервером і отримує від нього необхідні параметри на етапі конфігурації мережевого обладнання. Це робиться для полегшення розподілу IP-адрес в мережі. Конфігурація сервера показана на рис. 3.7.

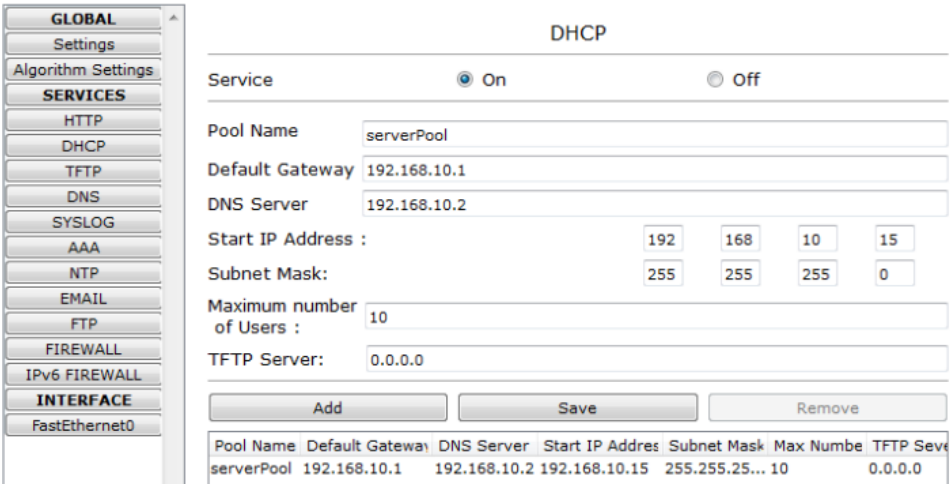

Рис. 3.7. Конфігурація DHCP сервера

На IP конфігурації 4 комп'ютера видно, що IP-адресу було отримано автоматично, завдяки протоколу DHCP (рис. 3.8).

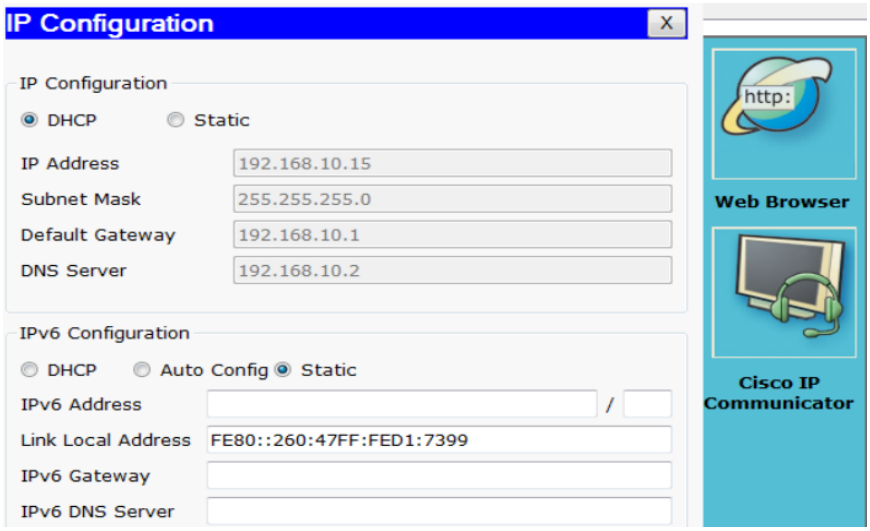

Рис. 3.8. Конфігурація PC4

Статична маршрутизація налаштовується між маршрутизаторами без використання будь-яких протоколів за допомогою безпосередньо пов'язаних між собою команд підмережування ip route, як показано на рисунках 3.9 і 3.10, коли введені команди show run і show ip route. Маршрутизатори мають деякі потужні інструменти, які дозволяють фактично бачити таблицю маршрутизації (напрямок, який використовує маршрутизатор для визначення того, як трафік проходить через мережу). Використовуйте команду show ip route, щоб побачити мережевий рівень. На рисунку 3.10 показано, як перевірити таблицю маршрутизації на наявність запису для потрібної мережі призначення. Команда show run показує поточний стан портів маршрутизатора, а також тип з'єднання і протокол з'єднання.

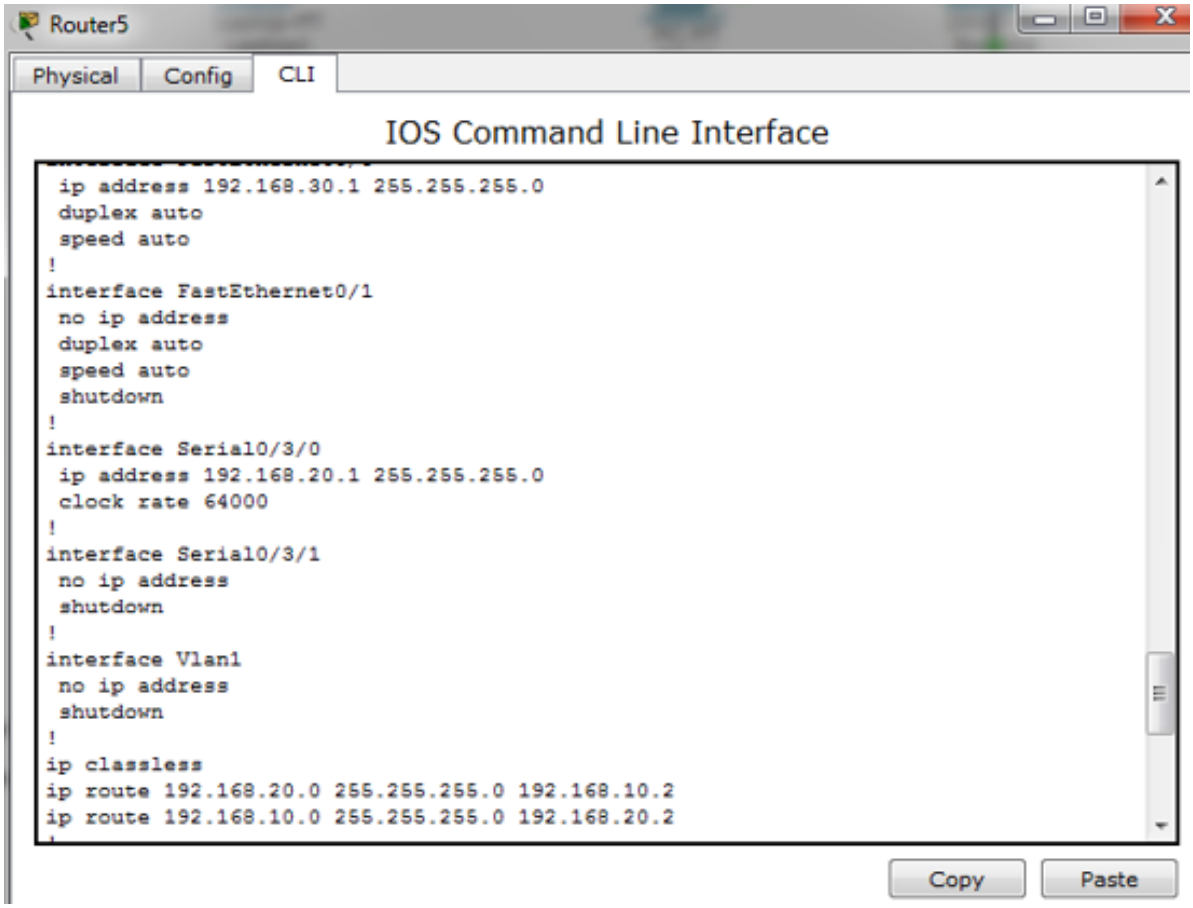

Рис. 3.9. Показання команди show run

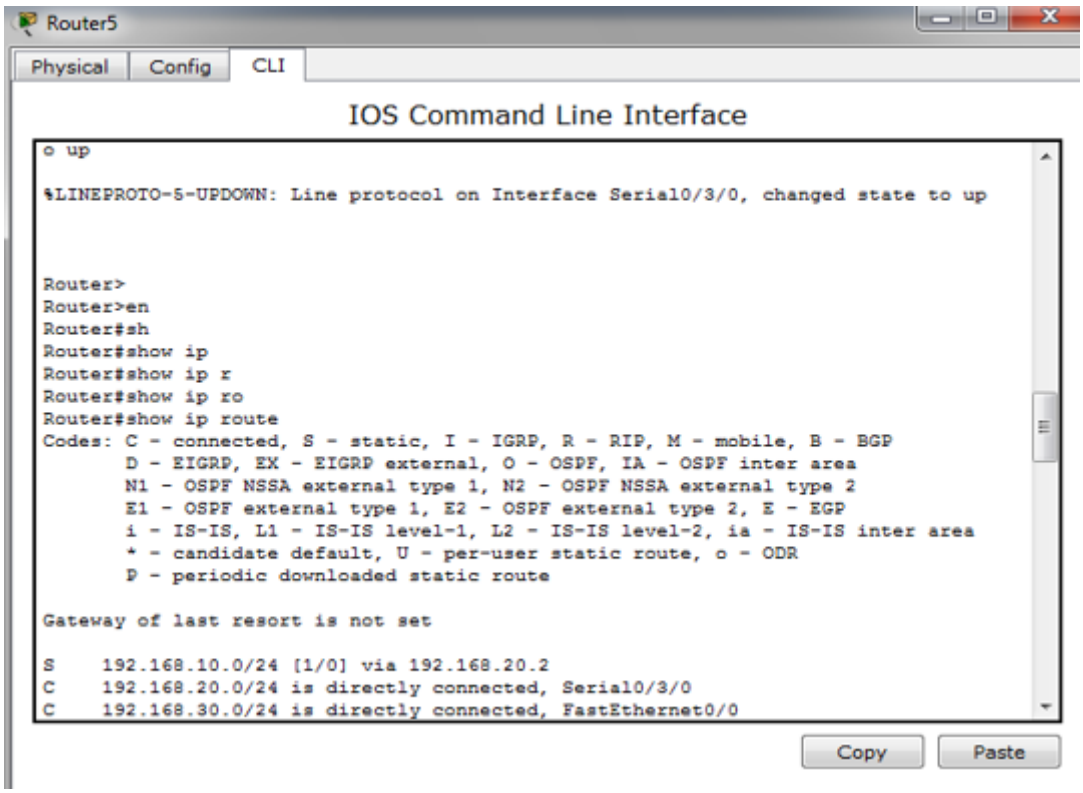

Рис. 3.10. Показання команди show ip route

При моделюванні мережі IPv6, яка ідентична звичайній мережі, використовується те саме обладнання, за винятком DHCP-сервера, який виявився зайвим через функцію автоконфігурації в мережах IPv6. Як показано на Рис. 3.11, комп'ютери автоматично налаштовують свої IP-адреси, просто встановивши маршрут підмережі на маршрутизаторі.

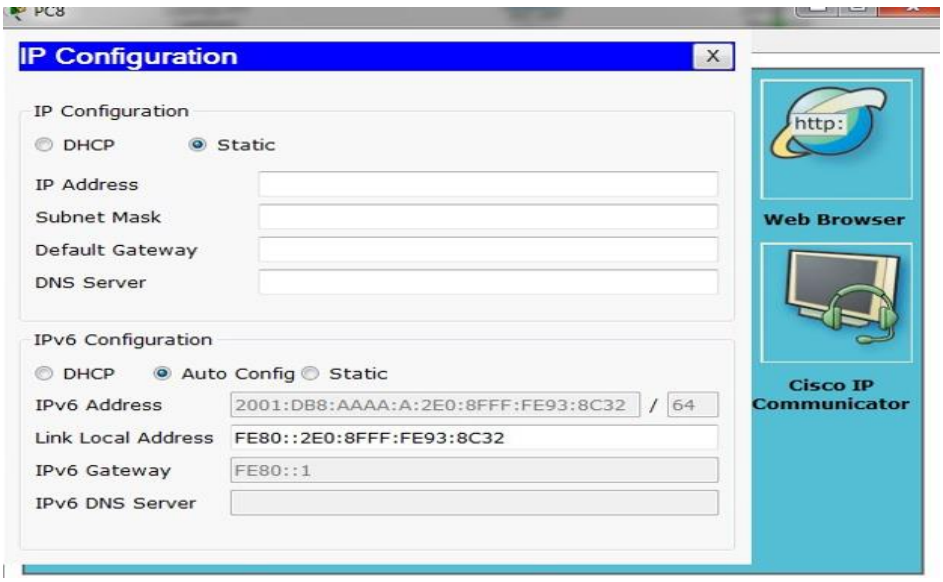

Рис. 3.11. IP конфігурація PC8

Для з'єднання маршрутизаторів використано протокол RIP. RIP - так званий протокол дистанційно-векторної маршрутизації, який оперує транзитними ділянками як метрикою маршрутизації. Максимальна кількість стрибків, дозволена в RIP - 15 (метрика 16 означає "нескінченно велику метрику"). Кожен RIP-маршрутизатор за замовчуванням передає в мережу свою повну таблицю маршрутизації один раз на 30 секунд, дуже сильно навантажуючи низькошвидкісні лінії зв'язку. RIP працює на 3 рівні (мережевий) стека TCP/IP, використовуючи UDP порт 520.

RIP підтримує лише найкращий маршрут до пункту призначення. Якщо нова інформація забезпечує кращий маршрут, вона замінює стару інформацію про маршрут. Якщо топологія мережі змінюється, маршрут може змінитися, наприклад, новий маршрут стає найкращим маршрутом до певного пункту призначення. Коли відбувається зміна топології мережі, це відображається у повідомленнях про координацію маршрутів. Наприклад, якщо якийсь маршрутизатор виявляє збій у каналі або інший маршрутизатор, він перераховує свій маршрут і надсилає повідомлення про оновлення маршрутизації. Кожен маршрутизатор отримує повідомлення про оновлення маршрутизації, що містить зміни, коригує свою таблицю і поширює ці зміни. У сучасному мережевому середовищі RIP не є найкращим оптимальним рішенням в якості протоколу маршрутизації, оскільки його функціональність поступається сучасним протоколам, таким як EIGRP і OSPF. Крім того, обмеження в 15 хопів перешкоджає його використанню у великих мережах. Перевагою цього протоколу є те, що він простий в установці. Цей протокол був обраний через невеликий розмір мережі. На малюнку 3.12 наведено показання команди show IPv6 route. А на малюнку 3.13 показання команди show IPv6 run.

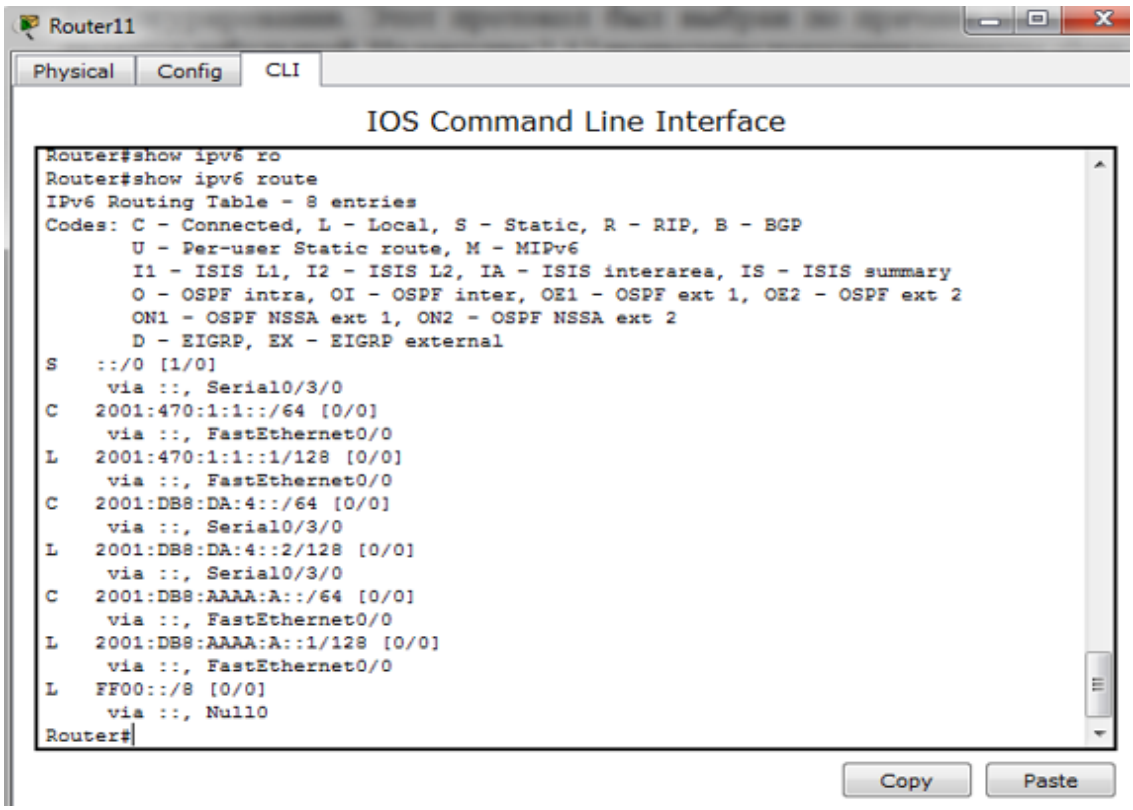

Рис. 3.12. Показання команди show IPv6 route

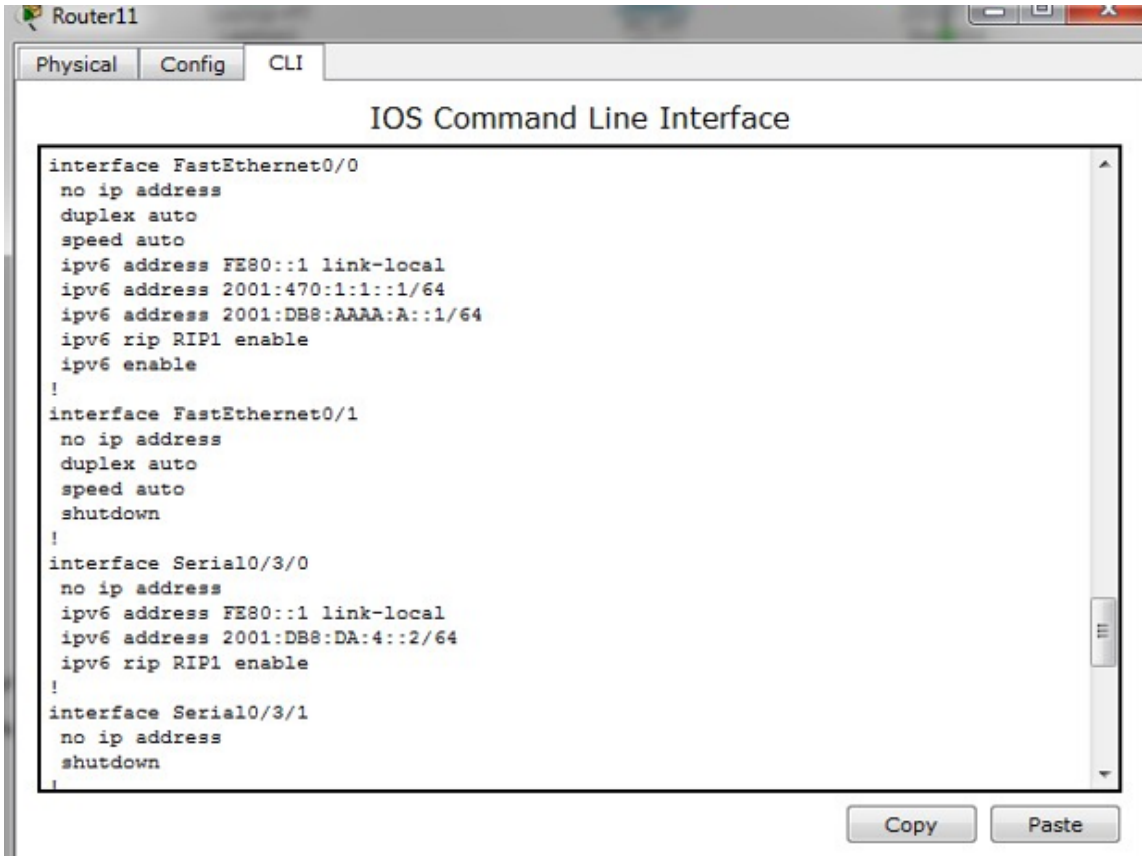

Рис. 3.13. Показання команди show IPv6 run

3.3. Аналіз мережі з урахуванням IP

Одним з найважливіших показників якості мережі є швидкість передачі пакетів; програма Packet Tracer має панель моделювання, яка розраховує швидкість передачі пакетів у мережах IPv4 та IPv6 (Рисунок 3.14). Найдовший шлях передачі був обраний від ПК 7 до DNS-сервера для IPv4 і від ПК 11 до DNS-сервера для IPv6. Для кожного протоколу було виконано по десять турів від відправника до одержувача.

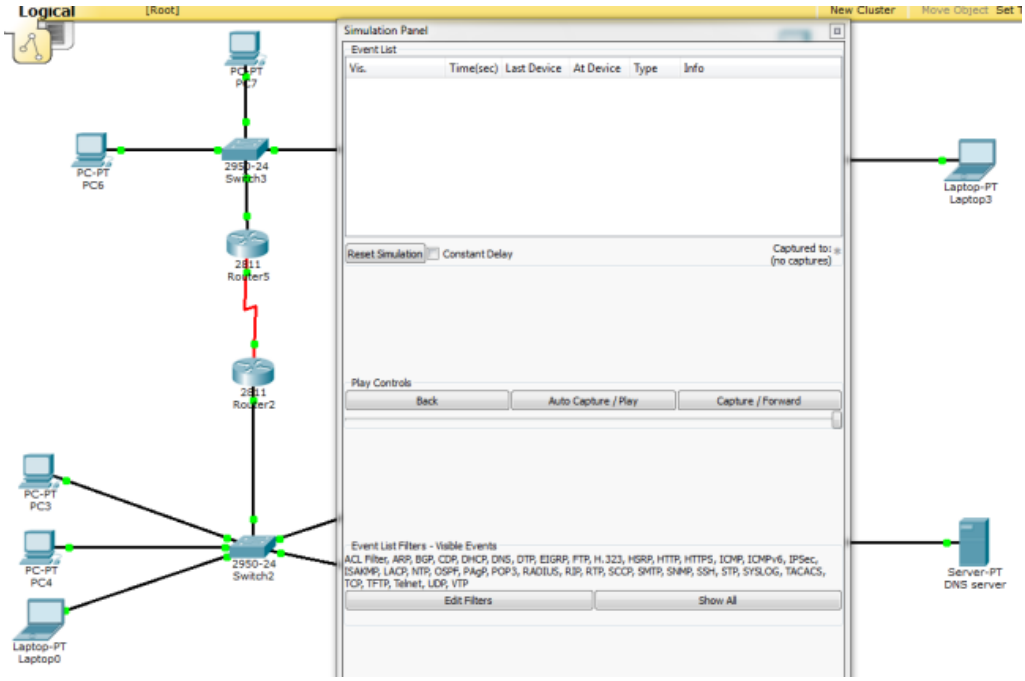

Рис. 3.14. Панель симуляції Packet Tracer

На рис. 3.15. представлено дані про швидкість передавання пакетів для версії IPv4.

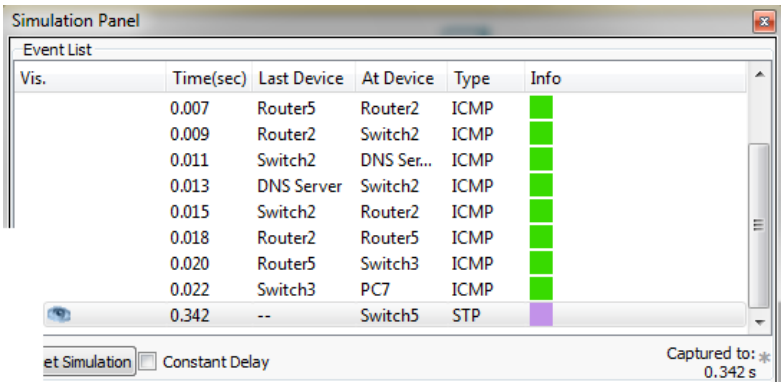

Рис. 3.15. Швидкість передавання пакетів для IPv4

Симуляційна панель надає дані про час передавання пакета, кожен окремо взятий пристрій, через який пройшов пакет, а також тип пакета. На рис. 3.16. представлено швидкість передачі пакета для IPv6.

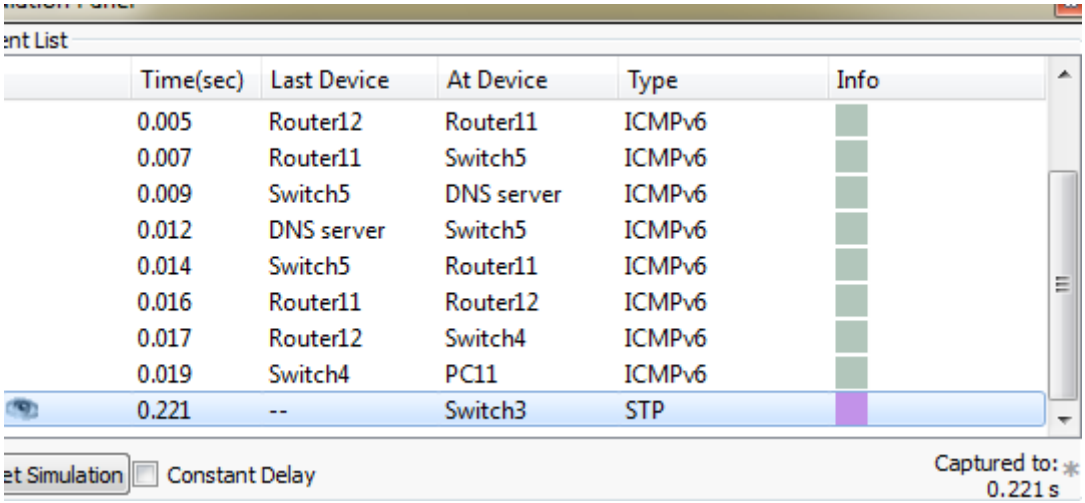

Рис. 3.16. Швидкість передавання пакетів для IPv6

Виходячи з наведених вище даних, середню швидкість передачі пакетів можна розрахувати за такою формулою:

$$C = \frac{C_1 + \ldots + C_{10}}{n}, \quad (3.1)$$

Де C є швидкістю передавання пакета. Розрахунок швидкості передавання пакетів для IPv4

C=0,383+0,438+0,416+0,406+0,455+0,342+0,321+0,401+0,354+0,311/10=0,382

Розрахунок швидкості передавання пакетів для IPv6

C=0,238+0,162+0,35+0,199+0,329+0,228+0,274+0,179+0,26+0,221/10=0,244

3.4. Розрахунок смуги пропускання

Вимоги до пропускної здатності визначаються гарантіями якості обслуговування, які оператори надають користувачам; параметри QoS описані в

Рекомендації ITUY.1541. Зокрема, затримка наскрізного поширення при передачі голосу не повинна перевищувати 100 мс, а ймовірність перевищення порогу затримки в 50 мс не повинна перевищувати 0,001, тобто

$$\begin{matrix} t_P \leq 100, мс, \\ p\{tp > 50\ мс\} \leq 0.001 \end{matrix}, \quad (3.2)$$

Затримка з кінця в кінець складається з таких складових:

$$t_p = t_{пакет} + t_{ад} + t_{core} + t_{ад} + t_{буф;}, \quad (3.3)$$

де t p - час передачі пакета з кінця в кінець;

tпакет - час пакетування (залежить від типу трафіку та кодека);

t ад - час затримки при транспортуванні в мережі доступу;

t core - час затримки при поширенні в транзитній мережі;

t буф - час затримки в приймальному буфері.

Застосування низькошвидкісних кодеків зменшує основну частину бюджету затримки. Затримка в приймальному буфері також велика, тому на мережу доступу і на транспортну мережу має забезпечувати мінімальну затримку.

Припустимо, що затримка мережі доступу не повинна перевищувати 5 мс. Час обробки заголовка IP-пакета близький до постійного. Розподіл інтервалів між надходженнями пакетів відповідає експоненціальному закону. Для цієї моделі відома формула, що визначає середній час виклику в системі (формула Полячека - Хинчина).

$$t_{адi} = \frac{\tau_i(1+C_b^2)}{2(1-h_i\tau_i)}, \quad (3.4)$$

Де τj- середня тривалість обслуговування одного пакета;

Cb2 - квадрат коефіцієнта варіації Cb2 ≈ 0,2;

λj - параметр потоку, N∑ _секj;

tадj - середній час затримки пакета в мережі доступу, t- 0,005 с.

Ненульовий коефіцієнт варіації враховує можливі відхилення при використанні в заголовках IP полів ToS. Крім цього, час обробки IP-пакета сильно залежить від використовуваних на маршрутизаторі правил обробки.

Із формули (3.3) випливає залежність максимальної величини для середньої тривалості обслуговування одного пакета від середнього часу затримки в мережі доступу.

$$j = \frac{1}{\lambda_j + \frac{1+c^2}{2t_{адj}}}$$

$$\tau_1 = \frac{1}{1+\frac{1+c^2}{2t_{адj}}} = 1/(82610 + \frac{1+0,2}{2\times 0,005}) = 12,1\cdot 10^{-6}$$

$$\tau_2 = \frac{1}{2+\frac{1+c^2}{2t_{адj}}} = 1/(129200 + \frac{1+0,2}{2\times 0,005}) = 7,7\cdot 10^{-6}$$

, (3.5)

Побудуємо ці залежності за допомогою прикладної програми MathCad.

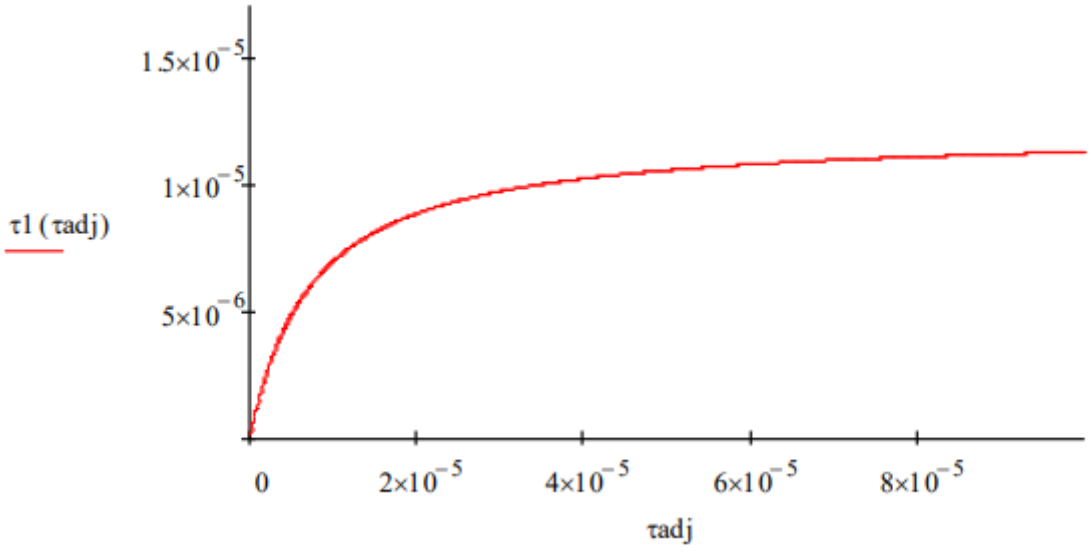

Рис. 3.17. Залежність максимальної величини для середньої тривалості обслуговування одного пакета від середнього часу затримки в мережі доступу для кодека G.711

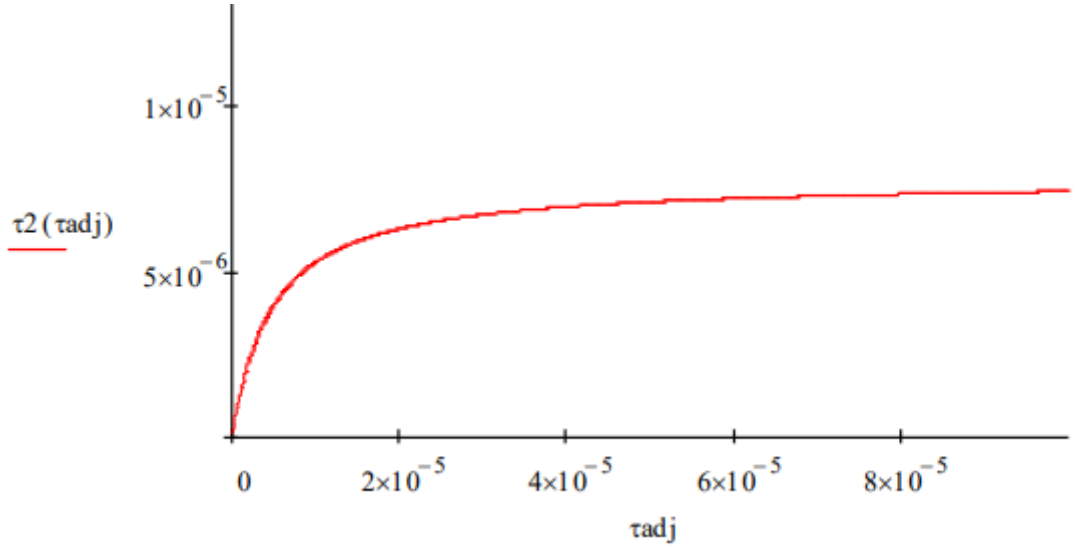

Рис. 3.18. Залежність максимальної величини для середньої тривалості обслуговування одного пакета від середнього часу затримки в мережі доступу для кодека G.726-32

Розрахунок смуги пропускання для IPv4. Інтенсивність обслуговування пов'язана із середнім часом затримки пакета в мережі доступу обернено пропорційно:

$$\beta_j = \frac{1}{c_i}, \tag{3.6}$$

$$\beta_1 = \frac{1}{c_1} = 1/12{,}1 \cdot 10^{-6} = 82640$$
$$\beta_2 = \frac{1}{c_2} = 1/7{,}7 \cdot 10^{-6} = 129900$$

Рівняння 3.2 і 3.3 використовуються для розрахунку середньої затримки в мережі доступу та розрахунку інтенсивності обслуговування при затримці tad = 5 мс для двох кодеків. Для часу tj необхідно вибрати мінімальне з двох можливих значень. Перше значення - це значення, отримане з останнього рівняння; друге значення - це

значення, визначене з умови граничного навантаження системи - ρ. Зазвичай це значення не повинно перевищувати 0,5.

Якщо середня затримка в мережі доступу становить 5 мс, то коефіцієнт використання дорівнює:

$$\rho_j = \lambda_j r_j (0.005)$$

$$\rho_1 = \lambda_1 r_1 = 82610 \cdot 12{,}1 \cdot 10^{-6} = 1$$
$$\rho_2 = \lambda_2 r_2 = 129200 \cdot 7{,}7 \cdot 10^{-6} = 0{,}995 \quad (3.7)$$

Розрахуйте коефіцієнт використання для різних кодеків.

При таких високих коефіцієнтах використання невеликі зміни параметрів можуть призвести до нестабільної поведінки системи. Визначимо параметри системи з коефіцієнтом використання 50%. Середній час обслуговування наступний.

$$r_j = \frac{\rho_j}{j}, \quad (3.8)$$

$$r_1 = \frac{\rho 1}{1} = 0{,}5/82610 = 6 \cdot 10^{-6}$$
$$r_2 = \frac{\rho 2}{2} = 0{,}5/129200 = 3{,}87 \cdot 10^{-6}$$

Визначимо інтенсивність обслуговування при цьому

$$\beta_j = \frac{1}{c_i}, \quad (3.9)$$

$$\beta_1 = \frac{1}{c_1} = 1/6 \cdot 10^{-6} = 166700$$
$$\beta_2 = \frac{1}{c_2} = 1/3{,}87 \cdot 10^{-6} = 258400$$

Затримка в мережі доступу розраховується за формулою:

$$\text{ад j} = \frac{c_j(1+C_b^2)}{2(1-{}_jc_j)}, \tag{3.10}$$

$$\text{ад 1} = \frac{c_1(1+C_b^2)}{2(1-{}_1c_1)} \frac{6\times10^{-6}(1+0.2)}{2(1-82610\times6\times10^{-6})} = 7.138\cdot10^{-6} \text{ секунд}$$

$$\text{ад 2} = \frac{c_2(1+C_b^2)}{2(1-{}_2c_2)} \frac{3{,}87\times10^{-6}(1+0.2)}{2(1-129200\times3{,}87\times10^{-6})} = 4{,}644\cdot10^{-6} \text{ секунд}$$

Розраховувати ймовірність s(t)=-(1-)t за відомих λ і τ недоцільно, тому що в Y.1541 ймовірність P{t>50мс} < 0.001 визначено для передавання з кінця в кінець.

За відомого середнього розміру пакета hj визначити необхідну смугу пропускання.

$$\varphi_j = \beta_j h_j \text{ (біт/с)}, \tag{3.11}$$

$$\varphi_1 = \beta_1 h_1 = 166700\cdot200\cdot8 = 266{,}7\cdot10^6$$
$$\varphi_2 = \beta_2 h_2 = 258400\cdot120\cdot8 = 248{,}3\cdot10^6$$

Порівняємо отримані результати (див. Рис. 3.19)

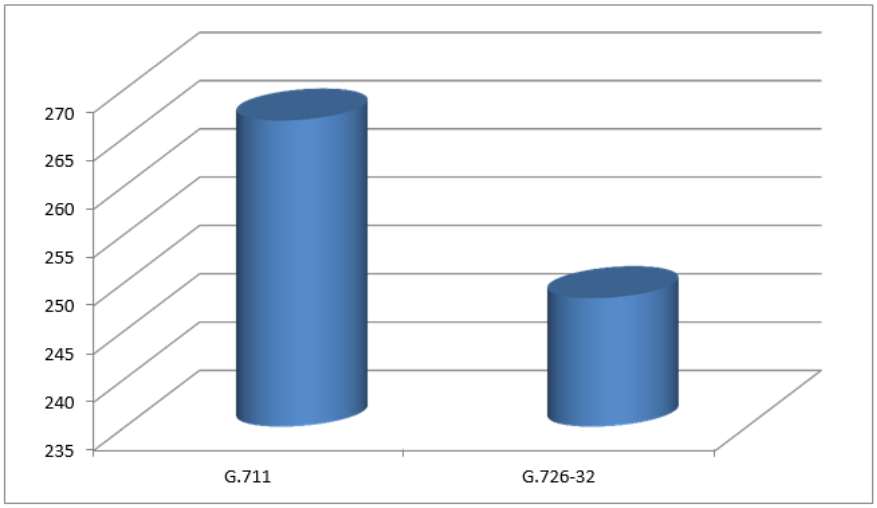

Рис. 3.19. Приклад відображення результатів розрахунку: необхідна смуга пропускання

З цього графіка видно, що для передачі однієї і тієї ж інформації, тобто одного і того ж обсягу даних, потрібна різна пропускна здатність. В даному випадку використання кодека G.711 з довжиною пакету 200 байт вимагає більшої пропускної здатності, ніж використання кодека G.726-32 з довжиною пакету 120 байт, але протокол G.726 є стисненим протоколом.

Розрахунок пропускної здатності для IPv6. Щільність обслуговування обернено пропорційна середній затримці пакетів в мережі доступу:

$$\beta_j = \frac{1}{c_i}$$

$$\beta_1 = \frac{1}{c_1} = 1/12{,}1 \cdot 10^{-6} = 82640$$
$$\beta_2 = \frac{1}{c_2} = 1/7{,}7 \cdot 10^{-6} = 129900$$

Рівняння 3.1 і 3.2 використовуються для розрахунку середньої затримки і щільності обслуговування в мережі доступу для двох кодеків для співвідношення затримок tad = 5 мс. Для часу tj слід вибрати мінімальне з двох можливих значень. Перше значення - це значення, отримане з останнього рівняння; друге значення - це значення, визначене з умови обмеження навантаження системи - ρ. Зазвичай це значення не повинно перевищувати 0,5.

Якщо середня затримка в мережі доступу становить 5 мс, то коефіцієнт використання дорівнює:

$$\rho_j = \lambda_j r_j (0.005)$$

$$\rho_1 = \lambda_1 r_1 = 82610 \cdot 12{,}1 \cdot 10^{-6} = 1$$
$$\rho_2 = \lambda_2 r_2 = 129200 \cdot 7{,}7 \cdot 10^{-6} = 0{,}995$$

Розрахувати коефіцієнт використання для випадків із різними кодеками.

За такого високого використання найменші флуктуації параметрів можуть призвести до нестабільної роботи системи. Визначимо параметри системи за її використання на 50%. Середня тривалість обслуговування дорівнюватиме:

$$r_1 = \frac{\rho 1}{1} = 0{,}5/82610 = 6 \cdot 10^{-6}$$
$$r_2 = \frac{\rho 2}{2} = 0{,}5/129200 = 3{,}87 \cdot 10^{-6}$$

Визначимо інтенсивність обслуговування при цьому

$$\beta_j = \frac{1}{c_i}$$

$$\beta_1 = \frac{1}{c_1} = 1/6 \cdot 10^{-6} = 166700$$
$$\beta_2 = \frac{1}{c_2} = 1/3{,}87 \cdot 10^{-6} = 258400$$

Затримка в мережі доступу розраховується за формулою:

$$_{\text{ад}\,j} = \frac{c_i(1+C_b^2)}{2(1-{}_i c_i)}$$

$$_{\text{ад}\,1} = \frac{c_1(1+C_b^2)}{2(1-{}_1 c_1)} \frac{6\times10^{-6}(1+0.2)}{2(1-82610\times6\times10^{-6})} = 7.138 \cdot 10^{-6} \text{ секунд}$$
$$_{\text{ад}\,2} = \frac{c_2(1+C_b^2)}{2(1-{}_2 c_2)} \frac{3{,}87\times10^{-6}(1+0.2)}{2(1-129200\times3{,}87\times10^{-6})} = 4{,}644 \cdot 10^{-6} \text{ секунд}$$

Розраховувати ймовірність s(t)=-(1-)t за відомих λ і τ недоцільно, тому що в Y.1541 ймовірність P{t>50мс} < 0.001 визначено для передавання з кінця в кінець.

За відомого середнього розміру пакета hj визначити необхідну смугу пропускання

$$\varphi_j = \beta_j h_j \text{ (біт/с)}$$

$$\varphi_1 = \beta_1 h_1 = 166700 \cdot 220 \cdot 8 = 293{,}3 \cdot 10^6$$
$$\varphi_2 = \beta_2 h_2 = 258400 \cdot 140 \cdot 8 = 289{,}4 \cdot 10^6$$

Порівняємо отримані результати

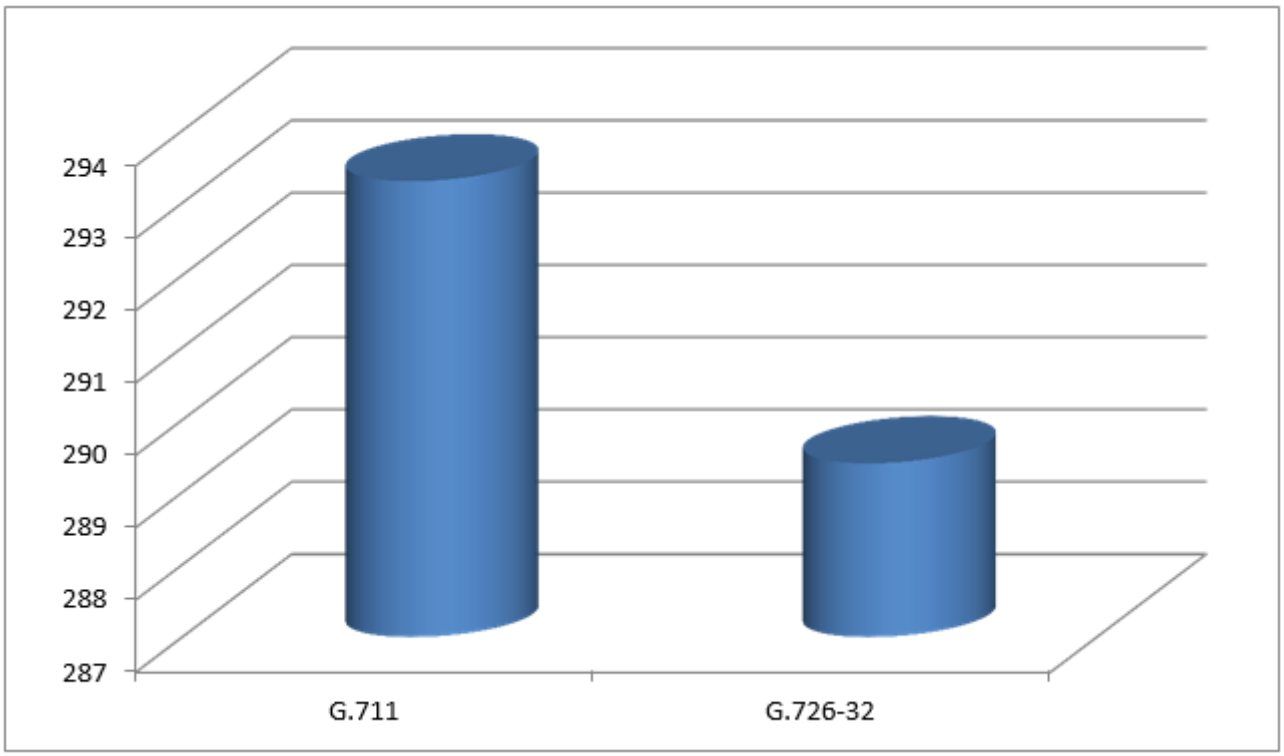

Рис. 3.20. Приклад відображення результатів розрахунку: необхідна смуга пропускання

З графіка видно, що для передавання інформації одного обсягу необхідна різна смуга пропускання, у цьому разі під час використання кодека G.711 з довжиною пакета 220 байт необхідна більша смуга пропускання, ніж під час використання кодека G.726-32 з довжиною пакета 140 байт.

Побудована модель розраховує параметри мережі, а саме час та інтенсивність обслуговування одного IP пакета певної довжини, від часу затримки в мережі доступу.

З вищенаведених даних випливає, що протокол IPv6 має більшу пропускну спроможність, ніж IPv4, як показано на рис. 3.21.

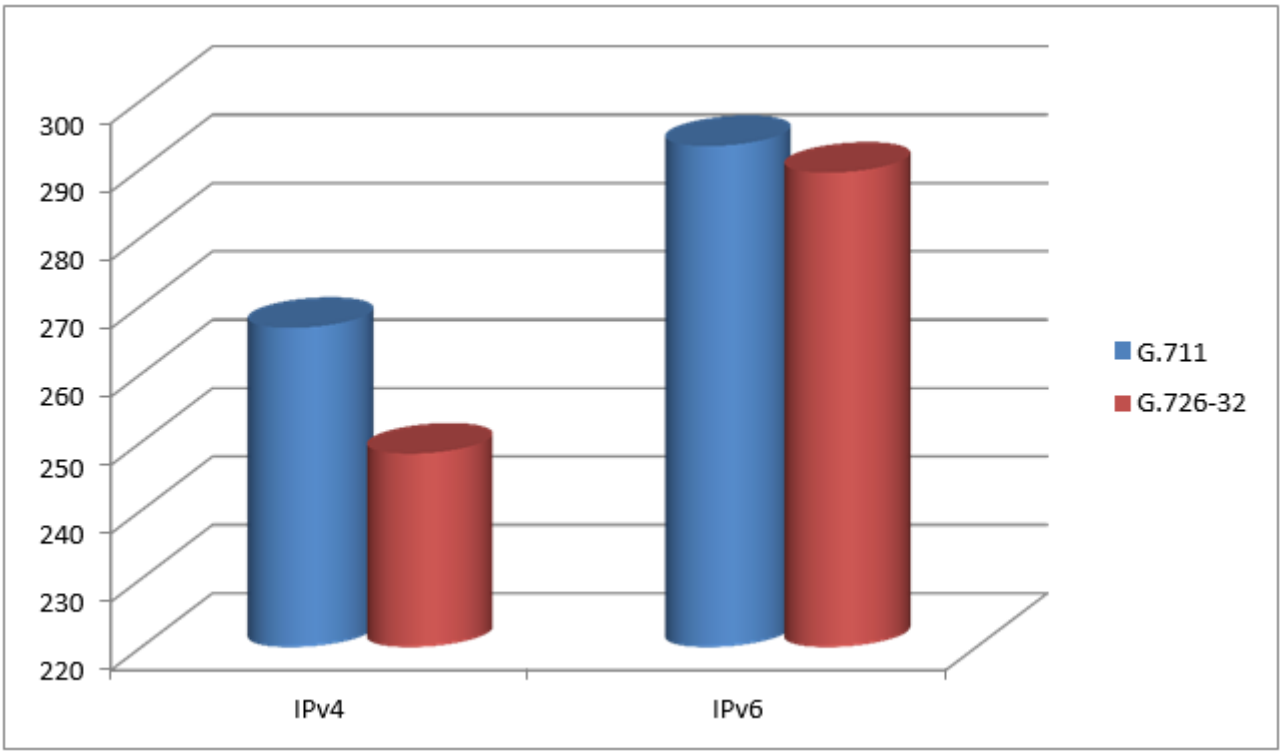

Рис. 2.21. Пропускна спроможність IPv4 та IPv6

ВИСНОВКИ

В даній кваліфікаційній роботі було проведено моделювання мережі IPv6 на базі програмного пакету Packet Tracer. В ході дослідження були використані різні протоколи та технології IPv6, такі як адресація, маршрутизація, інтеграція з IPv4 та безпека мережі.

Моделювання мережі засвідчило ефективність використання IPv6 для передачі даних та забезпечення зв'язності між вузлами. Використання адресації IPv6 дозволяє мати велику кількість унікальних адрес для підключення багатьох пристроїв до мережі, що важливо в сучасному світі Інтернету речей.

Дослідження різних протоколів та технологій IPv6 дозволило зрозуміти їх функціональні можливості та переваги у порівнянні з IPv4. Наприклад, маршрутизація на базі протоколу OSPFv3 дозволяє ефективно керувати мережевим трафіком та забезпечувати оптимальний шлях доставки пакетів.

Також була проведена інтеграція мережі IPv6 з IPv4 за допомогою технології перекладу адрес (NAT64), що дозволяє забезпечити сумісність між двома протоколами та забезпечити безперебійну комунікацію між різними мережами.

Наслідком дослідження є практична реалізація мережі IPv6 на базі програмного пакету Packet Tracer, яка дозволяє ефективно використовувати IPv6-технології та отримувати переваги нового покоління мереж у сфері забезпечення зв'язку та передачі даних.

Загалом, дослідження підтвердило важливість та актуальність використання IPv6 для майбутнього розвитку Інтерн ету та мережевих технологій, а моделювання мережі IPv6 на базі Packet Tracer виявилося ефективним інструментом для вивчення та розуміння принципів роботи мереж на основі цього протоколу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Z. Li and J. Qiu, "Internet Protocol Version 6 Migration", 2021 5th International Conference on Imaging, Signal Processing and Communications (ICISPC), Kumamoto, Japan, 2021, pp. 77-82.

2. A. Alshehri, M. Ben Salem and L. Ding, «Are Smart Home Devices Abandoning IPv Victims?», 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 2020, pp 1368-1375.

3. A. Deng and H. Wang, “Efficient Protocol Conversion Mechanism between Profinet Network and IPv6 Transport Network for Industrial Internet,” 2021 China Automation Congress (CAC), Beijing, China, 2021, p. 4792-4796.

4. "IEEE Approved Draft Standard for Interoperability of Internet Protocol Security (IPsec) Utilized within Utility Control Systems," in IEEE P2030.102.1/D1.13, May 2020 , vol., no., pp.1-21.

5. B. Alqahtani and B. AlNajrani, "A Study of Internet of Things Protocols and Communication," 2020 2nd International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 2020, pp. 1-6.

6. S. Jing, L. Guo, Q. Wang, E. Li, C. Zhao and B. Xiao, "Research and Deployment of IPv4/IPv6 Dual Stack Network in Large-scale Campus Network," 2021 IEEE Conference on Telecommunications, Optics and Computer Science (TOCS), Shenyang, China, 2021, pp. 128-132.

7. D. E. Kurniawan, N. C. Kushardianto and A. H. Thohari, "Simulation and Analysis Network Performance of IPv4, IPv6 and ISATAP Tunneling on Polibatam Network Laboratory," 2019 2nd International Conference on Applied Engineering (ICAE), Batam, Indonesia, 2019, pp. 1-4.

8. M. R. A. Ahmed and S. S. A. Shaikhedris, "Network Migration and Performance Analysis of IPv4 and IPv6," 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE), Khartoum, Sudan, 2021, pp. 1-6.

9. S. Li, Y. Yi and K. Zhu, "Implementation and scheme of IPv4 to IPv6 Transition in enterprise network architecture," 2021 IEEE 2nd International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA), Chongqing, China, 2021, pp. 457-461.

10. R. Fang, G. Han, X. Wang, C. Bao, X. Li and Y. Chen, "Speeding Up IPv4 Connections via IPv6 Infrastructure," 2022 18th International Conference on Mobility, Sensing and Networking (MSN), Guangzhou, China, 2022, pp. 555-562.

11. NN Abdul Aziz, RM Anak Rechie, BB Mohd Bakry, RA Rahman and YM Yussoff, «Analysing Smart Home Security Using Packet Tracer Simulation Software», 2021 IEEE 11th IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE) , Penang, Malaysia, 2021 , стор. 239-244.

12. B. Ratnala, T. Anuradha, V. Maddali and H. V. Chintalapudi, "Designing Smart Room Using Cisco Packet Tracer Simulator," 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2023, pp. 183-188.

13. A. D. Azhari, N. A. Sulaiman and M. Kassim, "Secured Internet Office Network with the Internet of Things Using Packet Tracer Analysis," 2021 IEEE 11th International Conference on System Engineering and Technology (ICSET), Shah Alam, Malaysia, 2021, pp. 200-205.