**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ**
**КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ**

# КВАЛІФІКАЦІЙНА РОБОТА

на тему: **«ПОБУДОВА МЕРЕЖ МОБІЛЬНОГО ЗВ'ЯЗКУ НА ОСНОВІ ЗАСТОСУВАННЯ ПРОГРАМНО- КОНФІГУРОВАНИХ МЕРЕЖ»**

на здобуття освітнього ступеня магістра
зі спеціальності 172 Електронні комунікації та радіотехніка
*(код, найменування спеціальності)*
освітньо-професійної програми Телекомунікаційні системи та мережі
*(назва)*

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

Антон ШЕВЧУК

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

Виконав: здобувач вищої освіти гр.ТСДМ-63
Антон ШЕВЧУК

Керівник:
КТН, доцент Костянтин ЛАВРІНЕЦЬ
*Ім'я, ПРІЗВИЩЕ*

Рецензент:

**Київ 2025**

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**Навчально-науковий інститут телекомунікацій**

Кафедра Телекомунікаційних систем та мереж
Ступінь вищої освіти Магістр
Спеціальність 172 Електронні комунікації та радіотехніка
Освітньо-професійна програма Телекомунікаційні системи та мережі

**ЗАТВЕРДЖУЮ**
Завідувач кафедрою Телекомунікаційних систем та мереж
_____Віктор ЗАЇКА
«____» _____ 2025 р.

# ЗАВДАННЯ
# НА КВАЛІФІКАЦІЙНУ РОБОТУ

Шевчуку Антону Юрійовичу
*(прізвище, ім'я, по батькові здобувача)*

1. Тема кваліфікаційної роботи: **:** «Побудова мереж мобільного зв'язку на основі застосування програмно-конфігурованих мереж»
керівник кваліфікаційної роботи Костянтин ЛАВРІНЕЦЬ, КТН, доцент
*(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)*
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «__» _____ 2025 р. № ___.

2. Строк подання кваліфікаційної роботи «___» _____ 2025 р.
3. Вихідні дані до кваліфікаційної роботи:

1. Архітектура та принципи побудови мережі 5G.
2. Переваги та перспективи технології 5G.
3. Міжнародні стандарти з питань побудови мереж п'ятого покоління;
4. Науково-технічна література.

4.Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1.Дослідження сучасних та перспективних технологій для побудови мережевої інфраструктури 5G.
2.Аналіз принципів функціонування програмно-конфігурованих мереж.
3.Дослідження підвищення показників якості та ефективного розподілу мережевих ресурсів.

5. Перелік ілюстративного матеріалу**:** Презентація на слайдах

6. Дата видачі завдання «___» _____ 2025 р.

# КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Підбір та аналіз науково-технічної літератури | 10.10.2024 | Викон. |
| 2 | Дослідження перспективних рішень реалізації та управління мереж п’ятого покоління | 20.10.2024 | Викон. |
| 3 | Аналіз моделі обслуговування та контролю інформаційних потоків | 31.10.2024 | Викон. |
| 4 | Дослідження підвищення показників якості та ефективного розподілу мережевих ресурсів | 20.11.2024 | Викон. |
| 5 | Висновки, вступ, реферат | 30.11.2024 | Викон. |
| 6 | Розробка презентації | 15.12.2024 | Викон. |

Здобувач вищої освіти Антон ШЕВЧУК

*(підпис)* *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи Костянтин ЛАВРІНЕЦЬ

*(підпис)* *(Ім’я, ПРІЗВИЩЕ)*

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**Навчально-науковий інститут телекомунікацій**
**ПОДАННЯ**
**ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ**
**ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ**
**на здобуття освітнього ступеня магістра**

Направляється здобувач Шевчук А.Ю.до захисту кваліфікаційної роботи
*(прізвище та ініціали)*

за спеціальністю 172 Електронні комунікації та радіотехніка
*(код, найменування спеціальності)*
освітньо-професійної програми Телекомунікаційні системи та мережі
*(назва)*
на тему: «Побудова мереж мобільного зв'язку на основі застосування програмно-конфігурованих мереж».

Кваліфікаційна робота і рецензія додаються.

Директор ННІТ _____ Владислав КРАВЧЕНКО
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

**Висновок керівника кваліфікаційної роботи**

Здобувач Шевчук Антон Юрійович показав гарну теоретичну та інженерну підготовку, уміння володіти новими комп'ютерними технологіями, користуватися навчальною, довідковою і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявив ініціативність, сумлінність та хист до наукової роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача Шевчука Антона Юрійовича на оцінку «**добре**» та присвоїти йому кваліфікацію Магістр з електронних комунікацій та радіотехніки.

Керівник кваліфікаційної роботи Костянтин ЛАВРІНЕЦЬ
*(Ім'я,ПРІЗВИЩЕ)*

_____
(*підпис*)

«____» _____ 2024 року

**Висновок кафедри про кваліфікаційну роботу**

Кваліфікаційна робота розглянута. Здобувач Шевчук А.Ю.допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою Телекомунікаційних систем та мереж Віктор ЗАЇКА
*(назва)* *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

**ВІДГУК РЕЦЕНЗЕНТА**
**на кваліфікаційну роботу**
**на здобуття освітнього ступеня магістра**

здобувача вищої освіти Шевчука Антона Юрійовича
*(прізвище, ім'я, по батькові)*
на тему «Побудова мереж мобільного зв'язку на основі застосування програмно-конфігурованих мереж»

**Актуальність:** Чим вища якість та швидкість передачі данних, тим більшу кількість данних можна передавати за певну одиницю часу. А в 2024 році для користувача дуже важливе питання передачі великих масивів даних за менший проміжок часу.

Саме тому магістерська робота, що присвячена мережам п'ятого покоління, є актуальною і своєчасною.

**Позитивні сторони :** Робота дозволяє досить повно оцінити загальну характеристику, сутність та структуру поставленої проблеми. В магістерській кваліфікаційній роботі розглянуто перспективи поширення мереж 5G. Робота виконувалась самостійно, з додержанням термінів виконання розділів роботи.

В результаті роботи був проведений аналіз та експериментальне дослідження підвищення показників якості мережевих ресурсів із застосуванням програмно-конфігурованих мережах .

**Недоліки:** 1. У роботі слід було більш ширше розглянути питання розвитку технології п'ятого покоління в майбутньму.

2. У магістерській кваліфікаційній роботі можна було б більше уваги приділити питанню технології віртуалізації NFV.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної магістерської роботи.

**Висновок:** *кваліфікаційна робота заслуговує оцінку "***добре***", а здобувач* Шевчук Антон Юрійович *заслуговує присвоєння кваліфікації:* Магістр з електронних комунікацій та радіотехніки.

Рецензент: _____ _____
*науковий ступінь, вчене звання* *підпис*
(Ім'я, ПРІЗВИЩЕ)

# РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: __ стор., __ рис., __ табл., __ джерел.

*Мета роботи* – визначення та дослідження основних можливостей та впровадження технології мережі 5G.

*Об'єкт дослідження* – бездротові мережі п'ятого покоління.

*Предмет дослідження* – принципи, моделі та методи побудови технології 5G.

В роботі приведено основні відомості про безпровідну технологію 5G та виявлено тенденції її сучасного розвитку. Досліджено перспективні рішення реалізації та управління мереж п'ятого покоління. Проаналізовано перспективи та стримуючі фактори поширення мереж 5G. Проаналізовано і використано відомі методи теорії телетрафіка, теорії масового обслуговування, теорії оптимізації, імітаційного моделювання. Представлено моделі обслуговування та контролю інформаційних потоків на базі програмно-конфігурованих мереж. Проаналізовані системи контролю параметрів функціонування програмно-керованої мережі, на основі параметрів якості обслуговування для довільних потоків у програмно- керованих мережах. Здійснено експериментальне дослідження підвищення показників якості та ефективного розподілу мережевих ресурсів із застосуванням програмно конфігурованих мережах.

КЛЮЧОВІ СЛОВА:

5G, LTE, ШЛЮЗ, АУТЕНТИФІКАЦІЯ, UMTS, GSM,ТЕРМІНАЛ, ПРОТОКОЛ, MASSIVE MIMO, СИСТЕМА, МЕРЕЖА, IoT,СТАНДАРТИ, СТЕКИ ПРОТОКОЛІВ., ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА, СИСТЕМА УПРАВЛІННЯ, МІТКА, ІНФОРМАЦІЯ, ПЕРЕХІД, ТЕХНОЛОГІЯ, IP, ФУНКЦІЇ УПРАВЛІННЯ.

ABSTRACT

The text part of the qualification work for obtaining the master's degree: __ page, __ figure, __ table, __ sources.

The purpose of the work is to identify and research the main capabilities and implementation of 5G network technology.

The object of research is wireless networks of the fifth generation.

The subject of the research is the principles, models and methods of building 5G technology.

The work provides basic information about 5G wireless technology and reveals trends in its modern development. Prospective solutions for the implementation and management of fifth generation networks have been studied. The prospects and restraining factors of the spread of 5G networks are analyzed. Well-known methods of teletraffic theory, mass service theory, optimization theory, simulation modeling were analyzed and used. Presented models of service and control of information flows based on software-configured networks. The control systems of software-controlled network functioning parameters, based on quality-of-service parameters for arbitrary flows in software-controlled networks, are analyzed.

An experimental study of the increase was carried out

indicators of quality and effective distribution of network resources using software-configured networks.

KEY WORDS:

5G, LTE, GATEWAY, AUTHENTICATION, UMTS, GSM, TERMINAL, PROTOCOL, MASSIVE MIMO, SYSTEM, NETWORK, IoT, STANDARDS, PROTOCOL STACKS, TELECOMMUNICATION NETWORK, MANAGEMENT SYSTEM, LABEL, INFORMATION, TRANSITION, TECHNOLOGY, IP, MANAGEMENT FUNCTIONS .

ЗМІСТ

ВСТУП ..... **Помилка! Закладку не визначено.**

1 ДОСЛІДЖЕННЯ ПЕРСПЕКТИВНИХ РІШЕНЬ РЕАЛІЗАЦІЇ ТА УПРАВЛІННЯ МЕРЕЖ П'ЯТОГО ПОКОЛІННЯ ..... **Помилка! Закладку не визначено.**

1.1 Аналіз перспектив та стримуючих факторів поширення мереж 5G**Помилка! Закладку не**

1.2 Прогноз кількості користувачів і кількості споживаного трафіку з урахуванням еволюційного розвитку мереж ..... **Помилка! Закладку не визначено.**

1.3 Дослідження сучасних та перспективних технологій для побудови мережевої інфраструктури 5G **Помилка! Закладку не визначено.**

1.3.1 .....Технологія віртуалізації NFV

1.3.2 Програмно-конфігуровані мережі..... **Помилка! Закладку не визначено.**

1.3.3 Хмарна інфраструктура Cloud RAN мережі радіодоступу NG-RAN**Помилка! Закладк**

1.4 Формування варіантів розгортання мереж зв'язку ..... **Помилка! Закладку не визначено.**

1.5 Аналіз складностей реалізації програмно-конфігурованих мереж**Помилка! Закладку не в**

1.6 Аналіз принципів функціонування програмно-конфігурованих мереж**Помилка! Закладку**

2 МОДЕЛІ ОБСЛУГОВУВАННЯ ТА КОНТРОЛЮ ІНФОРМАЦІЙНИХ ПОТОКІВ НА БАЗІ ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖ ..... **Помилка! Закладку не визначено.**

2.1 Аналіз системи контролю параметрів функціонування програмно- керованої мережі..... **Помилка! Закладку не визначено.**

2.2 Параметри якості обслуговування для довільних потоків у програмно-керованих мережах ..... **Помилка! Закладку не визначено.**

2.3 Алгоритм перерозподілу трафіку на основі відносного пріоритету потоку**Помилка! Закла**

2.4 Модель балансування навантаження на основі критерію максимально допустимого завантаження каналу ..... **Помилка! Закладку не визначено.**

3 ЕКСПЕРЕМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ПІДВИЩЕННЯ ПОКАЗНИКІВ ЯКОСТІ ТА ЕФЕКТИВНОГО РОЗПОДІЛУ МЕРЕЖЕВИХ РЕСУРСІВ ІЗ ЗАСТОСУВАННЯМ ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖ**Помилка! Закладку не визна**

3.1 Розробка тестового середовища мережі ..... **Помилка! Закладку не визначено.**

3.2 Експерементальне дослідження ефективності застосування моделі балансування навантаження мультипотокового керування трафіком**Помилка! Закладку не виз**

3.3 Експериментальна оцінка точності вимірювання затримки передачі пакетів у SDN ..... **Помилка! Закладку не визначено.**

3.4 Параметри якості обслуговування потоків та ефективності розподілу навантаження..... **Помилка! Закладку не визначено.**

ВИСНОВКИ ..... **Помилка! Закладку не визначено.**

ПЕРЕЛІК ПОСИЛАНЬ ..... **Помилка! Закладку не визначено.**

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ……98

ЗМІСТ

ВСТУП ..... 9
1 ДОСЛІДЖЕННЯ ПЕРСПЕКТИВНИХ РІШЕНЬ РЕАЛІЗАЦІЇ ТА УПРАВЛІННЯ МЕРЕЖ П’ЯТОГО ПОКОЛІННЯ ..... 11
1.1 Аналіз перспектив та стримуючих факторів поширення мереж 5G ..... 11
1.2 Прогноз кількості користувачів і кількості споживаного трафіку з урахуванням еволюційного розвитку мереж ..... 13
1.3 Дослідження сучасних та перспективних технологій для побудови мережевої інфраструктури 5G 17
1.3.1 Технологія віртуалізації NFV ..... 19
1.3.2 Програмно-конфігуровані мережі ..... 21
1.3.3 Хмарна інфраструктура Cloud RAN мережі радіодоступу NG-RAN ..... 23
1.4 Формування варіантів розгортання мереж зв'язку ..... 26
1.5 Аналіз складностей реалізації програмно-конфігурованих мереж ..... 31
1.6 Аналіз принципів функціонування програмно-конфігурованих мереж ..... 35
2 МОДЕЛІ ОБСЛУГОВУВАННЯ ТА КОНТРОЛЮ ІНФОРМАЦІЙНИХ ПОТОКІВ НА БАЗІ ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖ ..... 43
2.1 Аналіз системи контролю параметрів функціонування програмно- керованої мережі ..... 43
2.2 Параметри якості обслуговування для довільних потоків у програмно- керованих мережах 51
2.3 Алгоритм перерозподілу трафіку на основі відносного пріоритету потоку ..... 56
2.4 Модель балансування навантаження на основі критерію максимально допустимого завантаження каналу ..... 65
3 ЕКСПЕРЕМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ПІДВИЩЕННЯ ПОКАЗНИКІВ ЯКОСТІ ТА ЕФЕКТИВНОГО РОЗПОДІЛУ МЕРЕЖЕВИХ РЕСУРСІВ ІЗ ЗАСТОСУВАННЯМ ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖ ..... 68
3.1 Розробка тестового середовища мережі ..... 68
3.2 Експерементальне дослідження ефективності застосування моделі балансування навантаження мультипотокового керування трафіком ..... 71
3.3 Експериментальна оцінка точності вимірювання затримки передачі пакетів у SDN ..... 74
3.4 Параметри якості обслуговування потоків та ефективності розподілу навантаження ..... 81
ВИСНОВКИ ..... 94
ПЕРЕЛІК ПОСИЛАНЬ ..... 96
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ……98

# ВСТУП

***Актуальність дослідження.*** Принципові зміни в технологіях телекомунікацій вимагають перегляду принципів побудови мереж зв'язку для забезпечення реалізації вимог цих нових технологій. Саме реалізація SDN, яка являє собою нову концепцію побудови мережевої інфраструктури та методики надання сервісів кінцевим користувачам, дозволяє створити умови для прискореного впровадження нових послуг, впровадження нових мережевих протоколів і функціональності та дає можливість інтеграції з інноваційними програмами сторонніх розробників.

Перспективи використання технологій SDN в мережах операторів зв'язку обумовлені наступним чинниками, як : висока масштабованість мережі, гнучке централізоване управління мережею і мережевими ресурсами; зниження капітальних витрат на закупівлю обладнання COTS; зниження операційних витрат завдяки використанню віртуальних мережевих функцій; поліпшення енергетичної ефективності за рахунок використання високопродуктивних серверів центрів обробки даних; зменшення часу запуску нових мережевих сервісів; використання хмарних платформ в центрах обробки даних на периферії оператора для підвищення якості сервісу.

Для досягнення поставленої мети у магістерській кваліфікаційній роботі вирішуються наступні завдання: аналіз концепції розвитку мереж п’ятого покоління і вимог, що пред'являються цією концепцією до мереж зв'язку; дослідження моделі обслуговування та контролю інформаційних потоків із використанням програмно-конфігурованих мереж; експерементальне дослідження підвищення показників якості та розподілу мережевих ресурсів на базі програмно- конфігурованих мережа

***Ступінь наукової розробки.*** У роботі досліджено модель адаптації системи моніторингу безпроводової мережі, конфігурація якої визначається програмно, а саме частоти опитування стану мережних ресурсів, до завантаження вузлів та каналу вдається підвищити точність оцінки статистичних характеристик використання мережевих ресурсів та ймовірності блокування певного елементу мережі.

***Практичне значення одержаних результатів.*** У результаті проведення експериментів доведено, що комплексне застосування розглянутих у роботі наукових та технічних рішень дає змогу зменшити затримку для потоків реального часу на 15% та підвищити рівномірність завантаження мережних ресурсів на 30%.

# 1 ДОСЛІДЖЕННЯ ПЕРСПЕКТИВНИХ РІШЕНЬ РЕАЛІЗАЦІЇ ТА УПРАВЛІННЯ МЕРЕЖ П’ЯТОГО ПОКОЛІННЯ

## 1.1 Аналіз перспектив та стримуючих факторів поширення мереж 5G

Мережі 5G розгортаються по всьому світу. І хоча їх географічна доступність поки що обмежен а, оператори швидко розширюють охоплення. У Gartner прогнозують, що в нинішньому році оборот ринку інфраструктури бездротових мереж 5G досягне $ 4,2 млрд, збільшившись у порівнянні з 2019-м на 89% [1].

Під час обговорення перспектив 5G зазвичай наголос робиться на «призначених для користувача» мережах, наприклад, в рекламних матеріалах виробників обладнання основна увага приділяється тому, наскільки швидше можна буде завантажувати відео за допомогою мереж п'ятого покоління.

Деяку затримку в процес може внести епідемія корона вируса, 3GPP вже скасувала очні заходи першого кварталу, замінивши їх, де це можливо, телеконференції. Зустрічі другого кварталу, які передбачалося провести в Китаї, про всяк випадок вирішено перенести в інші місця.

Проте робота йде і аналітики впевнені, що в довгостроковій перспективі 5G вплине на всі підприємства без винятку, тому краще починати освоювати послуги мереж нового типу як можна раніше, щоб випередити конкурентів і отримати важливі переваги.

У лютому 2020р Accenture опублікувала дослідження, присвячене сприйняттю перспектив мереж п'ятого покоління і проблем, пов'язаних з їх впровадженням в корпоративному секторі.

В ході дослідження було опитано 2623 керівника, що приймають рішення в галузі бізнесу та технологій з 12 секторів економіки 10 країн - США, Великобританії, Іспанії, Німеччини, Франції, Італії, Японії, Сінгапуру, Об'єднаних Арабських Еміраті в та Австралії. Аналогічне дослідження проводилося роком раніше, що дозволило порівняти динаміку очікувань і сприйняття проблем.

Головний підсумок дослідження 2020 року - 90% бачать в мережах 5G нові можливості для свого бізнесу, 79% вважають, що мережі п'ятого покоління нададуть значний вплив на їх бізнес, причому 57% вважають, що зміни будуть «революційними» (про 4G в свій час таке сказали тільки 24%). При цьому досить істотна частина опитаних заявила, що мережі 5G вже працюють на їхніх підприємствах [1,2].




Рис.1.1 Рівень проникнення 5G на підприємствах

Надалі частка компаній, що використовують 5G, буде стрімко рости. Наприклад, 85% респондентів заявили, що вони планують використовувати 5G для взаємодії з віддаленими співробітниками протягом наступних чотирьох років. Рік тому таких відповідей було істотно менше - 68%.

Незважаючи на ажіотаж з приводу 5G, 18% респондентів зізналися, що поки не розуміють, як вони зможуть використовувати цю технологію у себе на підприємстві. А 21% - що бояться бути першопрохідникам і піти «по не вірному шляху».

Багато в чому ці побоювання можуть бути пов'язані з фінансовим аспектом: при переході на 5G компаніям доведеться оновити обладнання та поміняти бізнес-процеси, що виллється в копіку. 80% респонденті в Accenture вважають, що вартість управління IT-інфраструктурою та додатками в їх компанії виросте, причому 31% вважає, що ця сума буде «дуже велика» (в 2019 р такої думки дотримувалися

36%). А 17% не впевнені, що впровадження 5G дасть достатні повернення на інвестиції.

Крім того, в компаніях починають розуміти, що багатьом самостійно проблеми з впровадженням 5G не вирішити, знадобляться зовнішні помічники, таку думку висловили 72% опитаних. Всього 14% сподіваються створити додатки для 5G своїми силами (рік тому такої думки дотримувалися 23%). А зовнішні підрядники можуть бути не готові: 24% опитаних відчувають такі побоювання на адресу розробників програмного забезпечення, а 21% - на адресу телеком- партнерів, які не мають достатнього уявлення про те, як використовувати 5G в конкретній індустрії респондента [3].

Втім, порівняння досліджень 2019 і 2020 рр. показує певний прогрес - практично з усіх питань «побоюються» стало на 3-5 процентних пунктів менше.

Серед не багатьох винятків - проблеми з безпекою, на які як на головне гальмо впровадження 5G вказали 35% опитаних у порівнянні з 32% в опитуванні 2019 р.

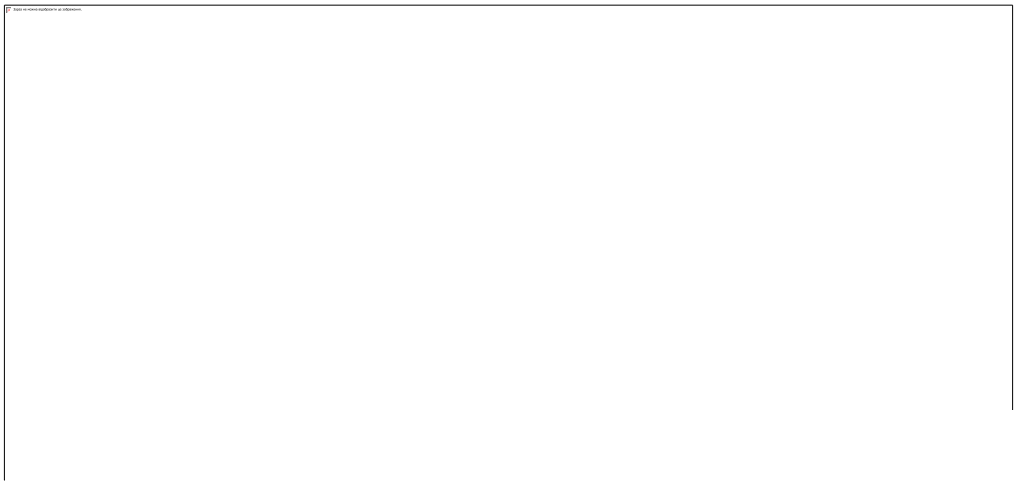


Рис.1.2 Основні перешкоди на шляху впровадження мереж 5G

## 1.2 Прогноз кількості користувачів і кількості споживаного трафіку з урахуванням еволюційного розвитку мереж

В середньому абоненти існуючих мобільних мереж можуть бути готові стати абонентами нової мережі 5G / IMT-2020 через приблизно 2,5 року після запуску

мережі 5G/IMT-2020 в їхній країні. Цей висновок доцільно враховувати операторам для прогнозування зростання їх абонентської бази і передбачуваного обсягу трафіку в їх мережах 5G/IMT-2020 року, а також для оцінок терміну формування критичної маси абонентів мереж 5G / IMT-2020.

Узагальнений аналіз експертних думок і звітних матеріалів підприємств-виробників обладнання для мереж ПРТС показав, що до кінця 2023 р прогнозована кількість абонентів мереж 5G / IMT-2020 в світі досягне 1 млрд., а до 2025 р - 2,6 млрд осіб [3].

Прогноз зростання загального трафіку даних в світі показав, що обсяг трафіку даних збільшиться з 2017 р за 6 років в середньому в 8 разів - в 2023 року обсяг трафіку досягне величини 110 ексабайт на місяць, причому 95% трафіку буде генеруватися користувачами смартфонів. Оцінка обсягу трафіку, що генерується мережами 5G / IMT-2020 в великих містах України в 2025 р склала:

- для Києва: 1,35 ексабайт / рік, що еквівалентно 350 Терабайт / ГНН;
- для Харкова: 0,9 ексабайт / рік, що еквівалентно 230 Терабайт / ГНН.

Прогноз за темпами проникнення пристроїв 5G / IMT-2020 для міст-мільйонників України до 2030 року показаний на рис.1.3.

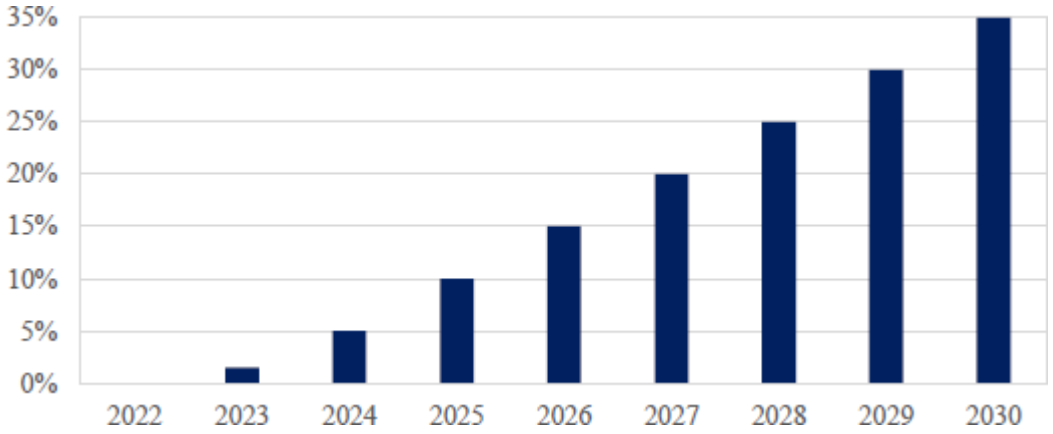



Рис.1.3 Прогноз проникнення пристроїв 5G / IMT-2020 на 15 містах України

Поточний рівень проникнення рухомого зв'язку в містах-мільйонниках - 3 абонентських пристрою на людину. Виходячи з поточної чисельності населення, і

припускаючи, що чисельність населення і рівень проникнення рухомого зв'язку суттєво не зміняться, прогноз кількості користувачі в надширокосмуговому диапазоны мобільного зв'язку eMBB в мережах 5G/IMT-2020 міст-мільйонників представлений на рис.1.4.

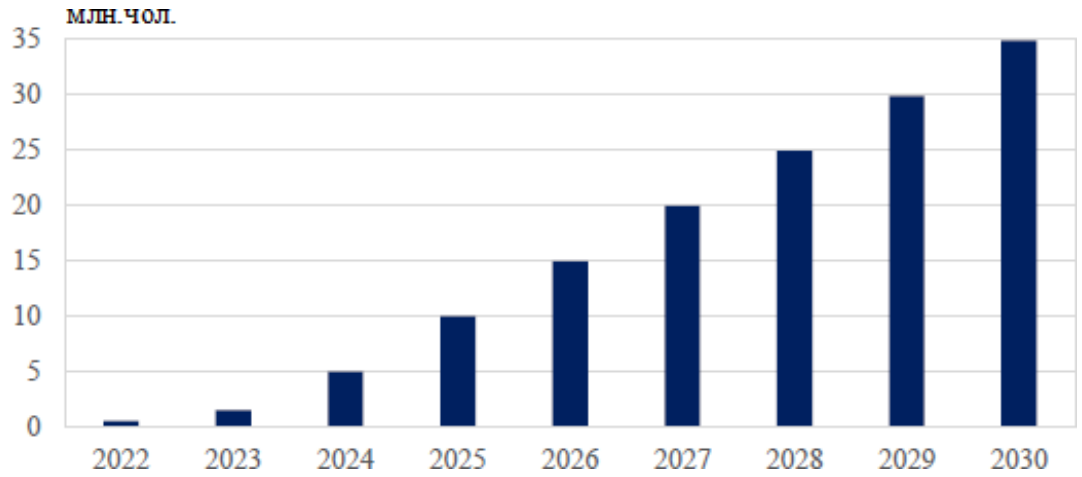



Рис.1.4 Прогноз загальної кількості користувачів послуг eMBB в мережах 5G / IMT-2020 в густонаселених містах України

Кількість IoT / M2M підключень в Україні щорічно зростає в середньому на 30%. Виходячи з існуючих прогнозів по проникненню IoT/M2M пристроїв в мережах 5G/IMT-2020 року, і зіставлення даних за темпами проникнення IoT/M2M пристроїв в мережах LTE [2], складений прогноз по темпах проникнення IoT/M2M пристроїв в мережах 5G/IMT-2020 в Україні до 2030 року рис.1.5.

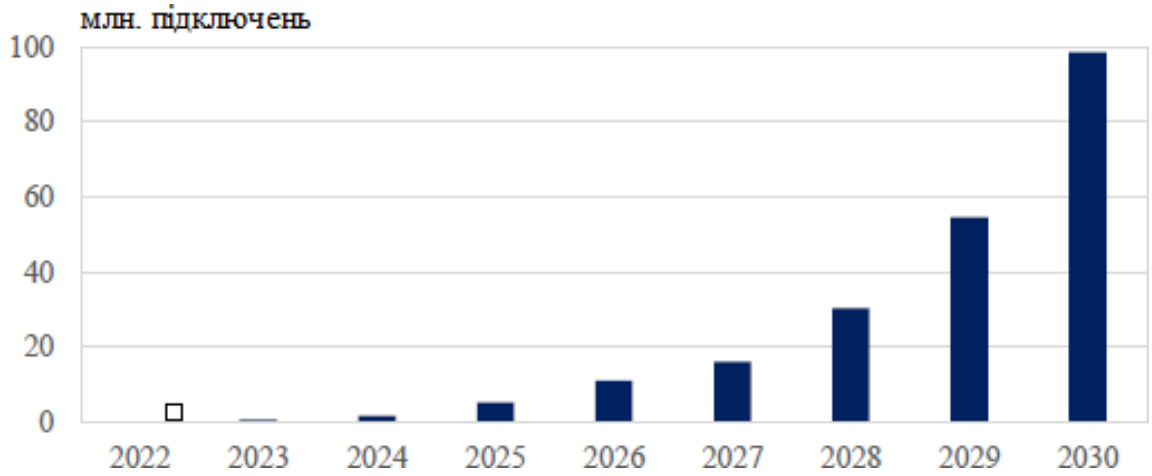



Рис.1.5 Прогноз загальної кількості IoT/M2M підключень в мережах 5G/IMT

На основі аналізу відомостей, наведених в розділі 2 цієї Концепції, виконана оцінка кількості користувачів з урахуванням еволюційного розвитку мереж 4G до мереж 5G / IMT-2020 на різних сферах і галузях економіки України. Результати прогнозу показані в табл. 1.1.

Таблиця 1.1

Прогноз розподілу кількості користувачів мереж 5G по галузям в 2026 р

| Сфера економіки | Прогноз кількості абонентів, млн |
|---|---|
| Промисловість | 3 |
| ЖКХ | 2,55 |
| Медицина | 2,1 |
| Громадська безпека | 1,95 |
| Громадський транспорт | 1,8 |
| Медіа і розваги | 1,5 |
| Автотранспорт | 1,2 |
| Фінансовий сектор | 0,9 |

При розрахунку кількості користувачів були використані наступні вихідні дані і прийняті наступні допущення: домінуюча послуга - eMBB; кількість абонентів eMBB в мережах 5G/IMT-2020 рок у - 15 млн. чоловік в 2026 р. (10% всіх мобільних викликів в 2026 р припадатиме на мережі 5G / IMT-2020); плата за одиницю трафіку однакова для всіх галузей економіки (тобто, розподіл доходів по галузях економіки пропорційно розподілу кількості абонентів);

Також на основі аналізу відомостей, виконано оцінку обсягу переданого трафіку мереж 5G/IMT-2020 на різних сферах і галузях економіки України. Результати аналізу показані в табл.1.2. Наведено прогноз розподілу обсягу трафіку в мережах 5G/IMT-2020 по галузям економіки, як в процентному, так і в абсолютному (Гб / міс.) відношенні [2, 3].

При розрахунку обсягу трафіку були використані наступні вихідні дані і прийняті наступні допущення: - домінуюча послуга: eMBB; - середнє значення обсяг у мобільного трафіку даних за 2-ий квартал 2018 р. бралося за даними операторів

рухомого зв'язку України, рівним 5 Гб/міс на одного абонента; - зростання обсягу мобільного трафіку даних за 2018 - 2026 року: 12 раз; - абонент може споживати послуги 5G/IMT-2020 року, що надаються в одному або декількох з усіх розглянутих галузей економіки України.

Таблиця 1.2

Прогноз розподілу обсягу трафіку в мережах 5G по галузям України в 2026 р.

| Сфера економіки | Розподіл мобільного трафіку даних по галузях економіки,% | Обсяг мобільного трафіку даних на одного абонента, Гб / міс. |
|---|---|---|
| Медіа і розваги | 25 | 15 |
| громадська безпека | 18 | 10,8 |
| промисловість | 15 | 9 |
| Медицина | 15 | 9 |
| Фінансовий сектор | 10 | 6 |
| Громадський транспорт | 7 | 4,2 |
| Автотранспорт | 6 | 3,6 |
| ЖКХ | 4 | 2,4 |

## 1.3 Дослідження сучасних та перспективних технологій для побудови мережевої інфраструктури 5G

Аналіз показав, що з метою підвищення показників якості в мережі має бути якомога менше вузлів включених в процес забезпечення зв'язку. Дані вузли повинні розташовуватися якомога ближче до призначеного для користувача устаткування. Підвищення показників якості можуть бути досягнуті спільним використанням технологій SDN, NFV і MEC в мережах зв'язку п'ятого покоління 5G [2, 4]. SDN, NFV і MEC технології пропонують потужні рішення для вирішення проблем при створенні мережі систем п'ятого покоління 5G. В існуючих стільникових мережах

послуги надаються за допомогою різних мережевих функцій, як правило, статично [5]. Тому не має легкого шляху для додавання нових послуг, що призводить до істотних витрат, витрати енергії і труднощів в інтеграції апаратних рішень при впровадженні нових послуг. Для вирішення цих проблем і були розроблені віртуалізація функцій мережі NFV і програмно- конфігурованої мережі SDN.

Технологія віртуалізації функцій мережі NFV реалізує певні функції мережі за допомогою програмного забезпечення, що розміщується у віртуальному середовищі, що підвищує гнучкість всієї системи. NFV використовує технології віртуалізації на програмованому устаткуванні, такому як пристрої зберігання даних, сервери загального призначення і комутатори, щоб відокремити програмну реалізацію мережевих функцій від виділеного обладнання. Іншими словами, NFV підтримує мережеві функції за допомогою техніки програмної віртуалізації на покупному обладнанні [6]. Кілька проектів були вже реалізовані при розробці відкритого програмного забезпечення, для комерційних рішень і стандартизації NFV. Найбільш відомі з них - Програмування послуг і оркестрації для віртуальних програмних мереж SONATA (Service Programming and Orchestration for Virtualized Software Networks) і Управління та оркестрації MAN (Management and Orchestration). SONATA сконструйована з метою збільшення програмованості і гнучкості мережі систем п'ятого покоління 5G. Це дозволяє як простіше робити сервісні платформи, так і робити їх модульними для забезпечення вимог різних провайдерів. Програмно-конфігуровані мережі SDN є новим підходом до побудови архітектури мережі, що забезпечує динамічне і економічно ефективний розвиток мережевої інфраструктури за допомогою фізичного поділу рівнів передачі даних і управління.

Рівень управління є частиною мережі, яка надає рішення для обробки трафіку [6]. Рівень передачі даних - це інша частина мережі, яка передає трафік відповідно до команд від рівня управління. Управління здійснюється на базі відкритих стандартних протоколів взаємодії, таких як протоколи OpenFlow і ForCES [5]. Технологія SDN дозволяє оператору мережі конфігурувати, керувати і адмініструвати мережу за допомогою спеціалізованого програмного забезпечення, відомого як інтерфейси прикладного програмування (API). SDN в основному

забезпечує спрощення апаратного мережевого обладнання і підвищення гнучкості мережі.

Спільне використання SDN та NFV забезпечує можливість реалізації такої важливої концепції як мережевий слайсінг. Мережевий слайсінг можна розглядати як групу мережевих функцій, які працюють разом з певною технологією радіо доступу (RAT) для досягнення оптимального варіанта використання мережі. Іншими словами, мережевий слайсінг є способом підтримки послуг зв'язку за допомогою спеціального з'єднання. Мережевий слайсінг дозволяє оператору мережі побудувати кілька логічних мереж (кожна для певного варіанту використання) на одній фізичній інфраструктурі [7].

Перспективи використання технологій SDN/NFV в мережах операторів зв'язку обумовлені наступним: висока масштабованість мережі, гнучке централізоване управління мережею і мережевими ресурсами; зниження капітальних витрат на закупівлю обладнання COTS; зниження операційних витрат завдяки використанню віртуальних мережевих функцій; поліпшення енергетичної ефективності за рахунок використання високопродуктивних серверів та центрів обробки даних; зменшення часу запуску нових мережевих сервісів; можливість використання обладнання різних вендорів; підвищення рівня безпеки; використання хмарних платформ в центрах обробки даних на периферії оператора для підвищення якості сервісу.

Віртуальна мережева інфраструктура NFV, яка визначається мережею SDN, дозволяють створити умови для прискореного впровадження нових послуг, впровадження нових мережевих протоколів і функціональності, дають можливість інтеграції з інноваційними програмами сторонніх розробників [7].

### 1.3.1 Технологія віртуалізації NFV

Технологія віртуалізації NFV дозволяє відокремити програмне забезпечення від фізичного обладнання, і, зокрема, реалізувати функції телекомунікаційного обладнання на універсальному обладнанні - IT серверах. На одному фізичному сервері великої продуктивності за допомогою програмного забезпечення

віртуалізації (гіпервізора) може бути організована робота декількох віртуальних серверів (або віртуальних машин VM) зі своїми операційними системами і програмним забезпеченням, що взаємодіють між собою за допомогою віртуального комутатора. При цьому віртуальні сервера спільно використовують ресурси фізичних серверів [8].

Відмінною особливістю опорної мережі 5GC є використання технології віртуалізації - реалізації телекомунікаційних модулів (мережевих функцій 5G Core) з а допомогою віртуальних мережевих функцій VNF рис.1.6.

Віртуальна мережева інфраструктура NFV центрів обробки даних мережі 5G/IMT-2020 повинна відповідати технічним специфікаціям 3GPP і ETSI в частині побудови системи управління і оркестрації MANO.

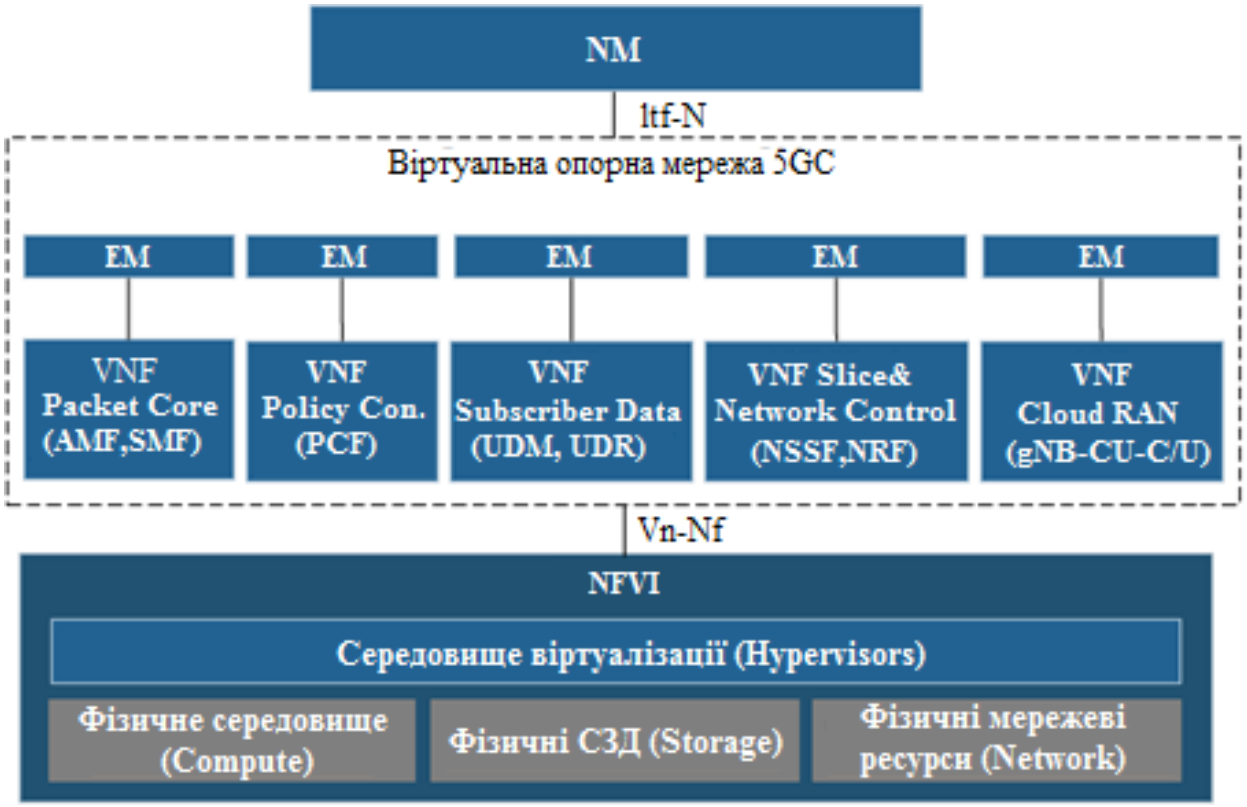



Рис.1.6 Віртуалізація мережевих елементів інфраструктури 5G

Віртуальна інфраструктура NFV дозволяє побудувати гнучку, масштабуючу мережу зв'язку, адаптовану до вимог послуг зв'язку, знизити вартість володіння мережі TCO (Total Cost of Ownership - сукупна вартість володіння) за рахунок

застосування типової високопродуктивної та надійної інфраструктури ЦОД [9].

Недоліком віртуальної інфраструктури є те, що обробка трафіку користувачів (пакетів даних в площині User Plane) виконується на серверному рівні, що вимагає великих ресурсів.

### 1.3.2 Програмно-конфігуровані мережі

Програмно-конфігуровані мережі SDN (Software Defined Network) - це технологія, що дозволяє відокремлювати функції рівня передачі даних від функцій рівня управління комутатором і переданим їм трафіком. Такий підхід передбачає перенесення з мережевого пристрою інтелектуальної складової на виділений сервер і, як наслідок, максимальне спрощення та здешевлення мережевих елементів - комутаторів, маршрутизаторів [10].

Технологія SDN націлена на вирішення таких проблем:

- підвищення ефективності механізмів управління пропускної здатності мережі;
- спрощення управління мережею і підвищенню його рівня автоматизації;
- підвищення масштабованості мережі;
- посилення безпеки мереж;
- підвищення ефективності маршрутизації;
- зниження капітальних витрат і витрат на експлуатацію.

Основна ідея SDN-підходу:

- відокремити управління мережевим обладнанням від управління передачею даних за рахунок створення спеціального програмного забезпечення, яке може працювати на звичайному окремому комп'ютері і яке знаходиться під контр олем адміністратора мережі;
- перейти від управління окремими екземплярами мережевого обладнання до управління мережею в цілому;
- створити інтелектуальний програмно-керований інтерфейс між мережним додатком і транспортним середовищем мережі.

Основними компонентами програмно-визначених мереж SDN на базі протоколу OpenFlow є (рис.1.7):

- OpenFlow комутатор;
- OpenFlow контролер, або мережева операційна система;
- захищений канал, за допомогою якого здійснюється взаємодія контролера і комутатора ( в більшості випадків для захисту переданих повідомлень використовується TLS (transport layer security - протокол захисту транспортного рівня), проте, можлива передача без шифрування) [3].

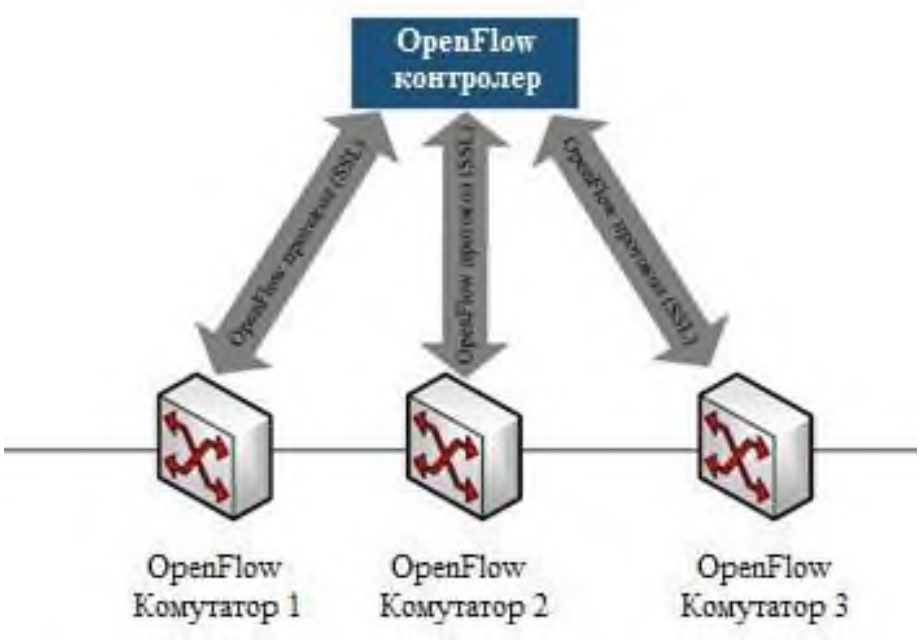



Рис.1.7 Схема взаємодії комутаторів з контролером по протоколу OpenFlow

Мережева інфраструктура програмно-яка визначається мережею SDN повинна будуватися відповідно до відкритих протоколів OpenFlow, бути уніфікованою і забезпечувати можливість реалізації мультивендорних технічних рішень.

Мережева інфраструктура програмно яка визначається мережею SDN дозволяє будувати мережі з високою комутаційної ємністю і швидкістю передач і даних.

До основних переваг SDN відносяться швидке розгортання, гнучке комбінування безлічі мережевих функцій на одній серверній платформі, простота і систематизований характер процедури адміністрування. За статистичними даними

звіту Infonetics Research «SDN and SDN Service Provider Survey», застосування концепції SDN дозволяє значно знизити матеріальні витрати на такі види послуг, як модернізація сервісів, управління, адміністрування, та технічну підтримку ( рис.1.8)

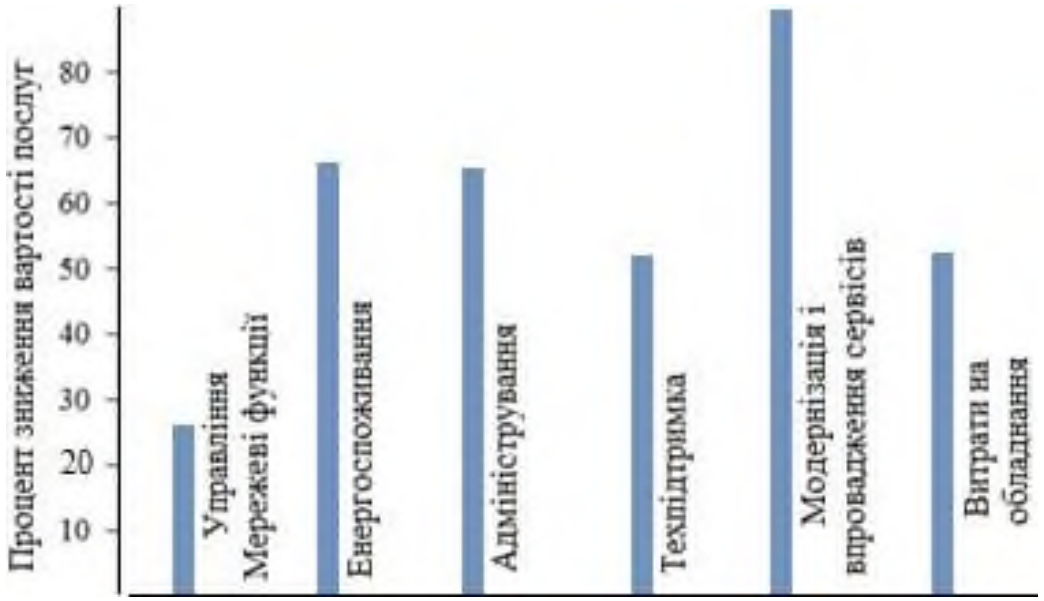



Рис.1.8 Відсоток зниження вартості послуг при впровадженні SDN

### 1.3.3 Хмарна інфраструктура Cloud RAN мережі радіодоступу NG-RAN

Хмарна мережа радіодоступу NG-RAN, представлена на рис.1.9., заснована на реалізації моделей базової станції gNB з використанням технології віртуалізації NVF і має ряд переваг:

- реалізація програмно-визначених мультістандартних базових станцій NR/E-UTRA, гнучкість і масштабованість віртуальних рішень;
- розміщення обладнання базових станцій в центрах обробки даних високого ступеня надійності і безпеки;
- єдина хмарна інфраструктура Cloud RAN управляє великою кількістю радіо модулів і охоплює велику територію радіо покриття, забезпечує більш оптимальне використання частотного ресурсу, більш ефективну роботу алгоритмів компенсації перешкод ICIC і багатоточкової передачі CoMP, Intra- RAT хендоверів.

Класична транспортна мережа мобільної мережі складається з двох основних частин: розподільчої мережі (Backhaul), що зв'язує базові станції з функціональни

ми елементами опорної мережі, і магістральної мережі (Backbone), яка забезпечує високошвидкісні канали зв'язку між функціональними елементами опорної мережі. Перехід на архітектуру C-RAN привів до виділення в мережі Backhaul двох нових сегментів: мережі «Fronthaul», що об'єднує пули радіомодулів gNB-RU і розподілені модулі gNB-DU, і мережі «Midhaul», об'єднуючою пули розподілених модулів gNB-DU і центральні модулі gNBCU [2].

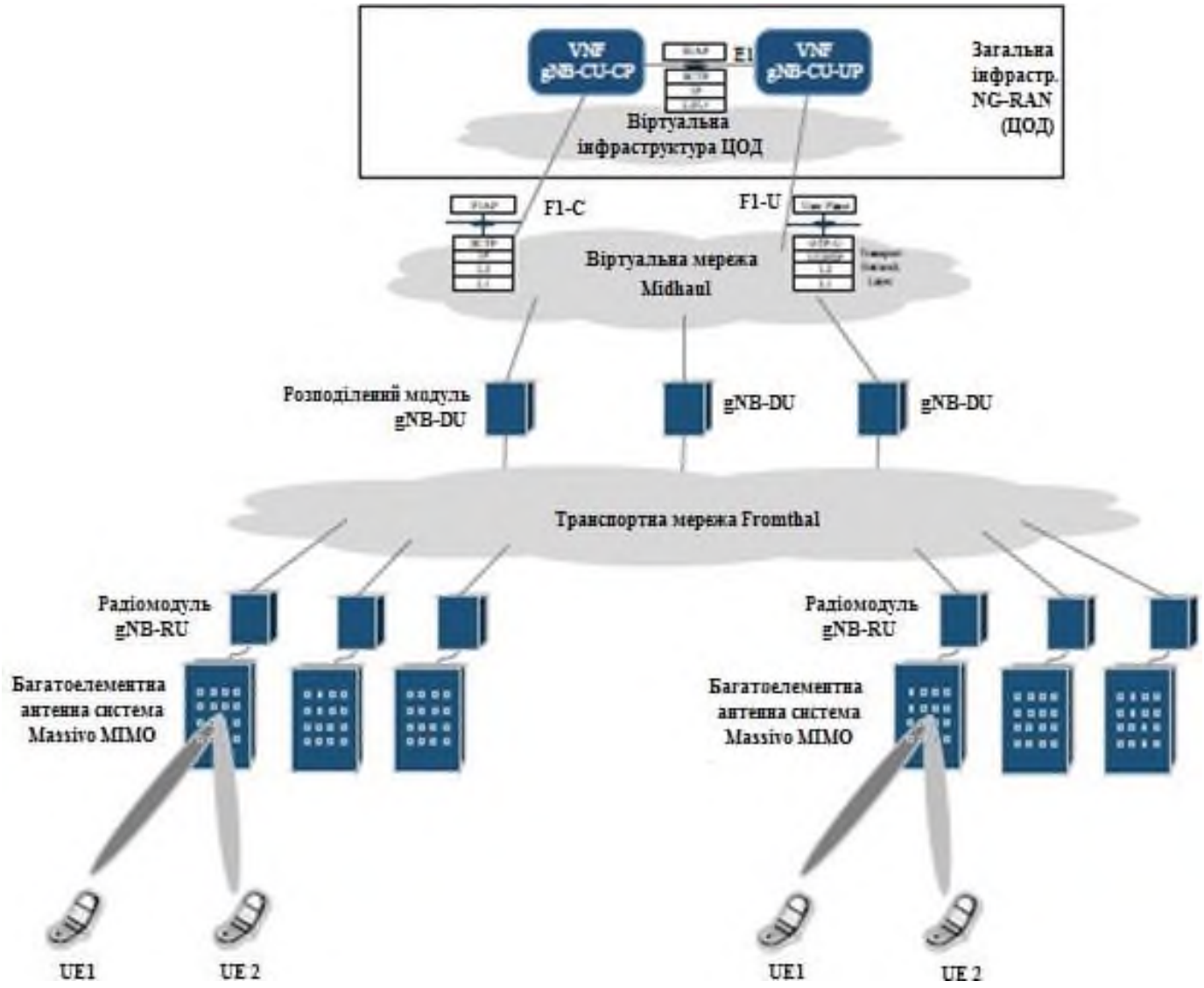



Рис.1.9 Хмарна інфраструктура Cloud RAN мережі радіодоступу NG-RAN

Сукупність мереж «Fronthoul», «Midhaul» і «Backhaul» отримала узагальнене найменування мережі «X-haul» і може бути побудована і з

застосуванням різних технологій, включаючи оптоволоконні лінії зв'язку, радіо релейні лінії, супутникові лінії зв'язку, Carrier Ethernet, IP / MPLS, Segment Routing і ін.

Впровадження технологій SDN / NFV в мережі 5G / IMT-2020 також істотно для модернізації функціональних вузлів транспортних мереж (наприклад, вузлів P, PE, мереж і IP/MPLS). Тому для побудови транспортної мережі можливо, як застосування тільки концепції NFV, тобто впровадження віртуалізованих маршрутизаторів і комутаторів, що працюють на серверах COTS, так і застосування комплексної концепції SDN/NFV, що означає новий підхід до організації мережевої взаємодії (використання контролера і комутаторів SDN, як віртуалізованих, так і ні) [3].

Програмна - яка визначається транспортна мережа SDN/NFV дозволяє відокремити функціонал управління (площин і Control Plane і Management Plane) від функціоналу прийому, обробки та пересилання пакетів даних (площині Data Plane), а також реалізувати функціонал управління з використанням технології віртуалізації.

Віртуальна транспортна мережа дозволяє підвищити ефективність механізмів управління пропускної здатності мережі; централізувати алгоритми управління мережею, підвищити масштабованість мережі і забезпечити автоматизовану реалізацію нових мережевих сервісів і нових мережевих шарів (network slices) опорної мережі 5GC (5G Core).

Аналіз принципів і вимог забезпечення інформаційної безпеки мереж і 5G / IMT-2020 року, заснованих на застосуванні криптографічних алгоритмів і апаратних засобів, в тому числі вітчизняних USIM-карт з довіреною ПО і ключами, системи забезпечення і управління ключами вітчизняного довіреної абонентського і мережевого устаткування і ПО, що забезпечують стійкість функціонування розроблюваного обладнання та доступність мережі зв'язку.

## 1.4 Формування варіантів розгортання мереж зв'язку

При розробці варіантів розгортання мереж зв'язку 5G/IMT-2020 для задоволення різних сегментів послуг і сервісів враховуються архітектурні особливості поділу мережі на мережеві шари, адаптовані до вимог сегментів послуг.

Для надання Вам послуг певного сегмента задіюється мережевий шар мережі 5G / IMT-2020 року, який включає до свого складу необхідний набір віртуальних мережевих функцій VNF ( рис.1.10). Один абонентський термінал одночасно може використовувати до 8 таких мережевих шарів. Особливістю є те, що модуль управління доступом і мобільністю AMF повинен бути загальним для всіх мережевих шарів, які обслуговують абонентський термінал.

Кожен мережевий шар характеризується інформацією S-NSSAI (Single Network Slice Selection Assistance Information). Інформація декількох мережевих шарів SNSSAI ( до восьми) групується в зведену інформацію про мережеві шари NSSAI [2,3].

Зведена інформація NSSAI формується окремо для різних мереж мобільного зв'язку в залежності від ідентифікатора PLMN-id.

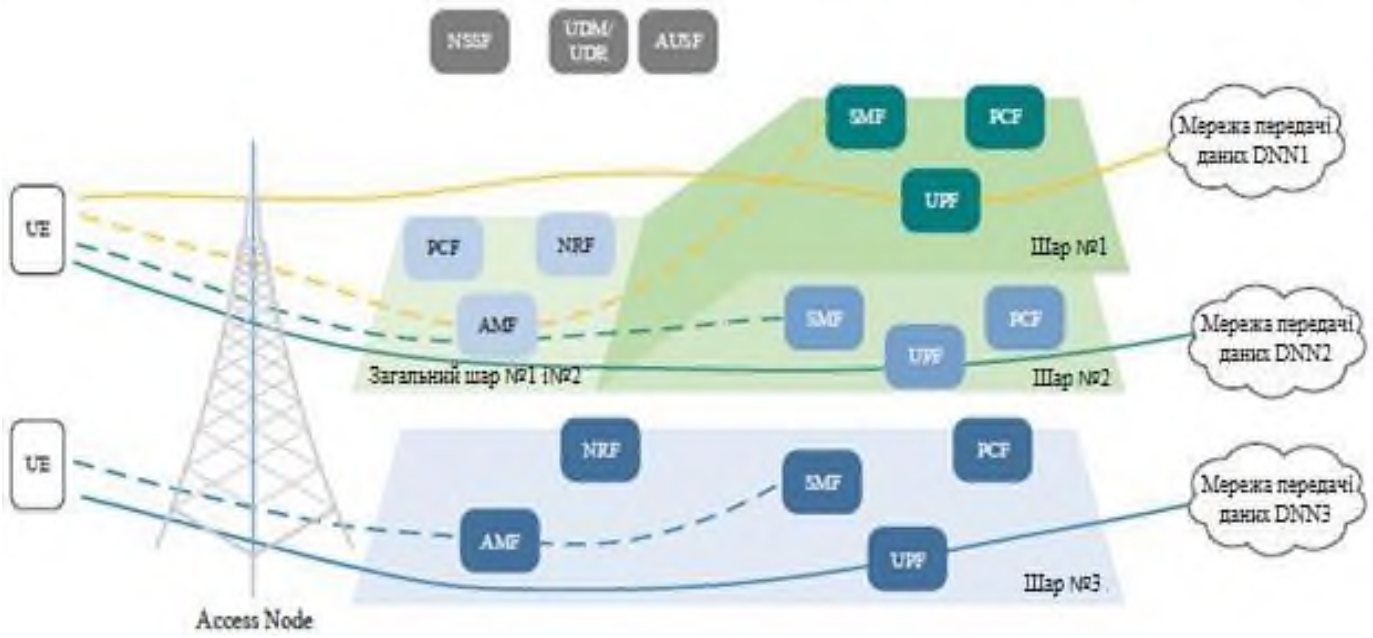



Рис.1.10 Приклад поділу опорної мережі 5GC на мережеві шари

Інформація про мережеві шари (у вертикальній площині) S-NSSAI опорної мережі 5GC містить параметр - тип мережевого шару / сервісу SST (Slice / Service Type). Тип мережевого шару SST приймає як стандартне значення згідно з 3GPP табл.1.3., так і значення, визначені оператором на власний розсуд [4].

Таблиця 1.3

Стандартні значення типів мережевих шарів SST, певні в 3GPP

| Тип мережевого шару | Значення SST | Опис |
|---|---|---|
| eMBB | 1 | Шар для надання послуг передач і даних з високими швидкостями, наприклад, потокова передача високоякісного відео, файлів великих розмірів і ін. |
| URLLC | 2 | Шар для надання послуг з ультра малих затримка ми між кінцеви ми пристроя ми, наприклад, для автоматизації виробництв / індустрій, забезпечення віддаленого управління системами |
| MIoT | 3 | Шар для забезпечення взаємодії величезної кількості пристроїв IoT, розміщених з високою щільністю. |

Реалізація мережевих шарів на базових станціях gNB фактично означає гнучкий розподіл частотно-часових ресурсів між мережевими шарами, з огляду на особливості організації частотно-територіального покриття. Особливості реалізації мережевих шарів eMBB, URLLC і MIoT на опорні й мережі 5GC наведені в табл.1.4.[11].

Варіанти розгортання мереж зв'язку 5G / IMT-2020 повинні також враховувати такі особливості побудови архітектури мережі 5G / IMT-2020:

1. Можливість локалізації трафіку за рахунок децентралізації пакетних

шлюзів UPF і розміщення їх ближче до абонента, в тому числі і в складі обладнання базової станції;

2. Гнучкі режими управління сесіями абонентів, в тому числі забезпечення безперервності сесій абонентів при зміні обслуговуючого пакетного шлюзу UPF в процесі переміщення;

3. Можливість одночасного використання декількох шлюзів UPF і роздільної маршрутизації трафіку;

Таблиця 1.4

Особливості реалізації мережевих шарів на опорній мережі 5GC

| Мережевий шар | | Особливість реалізації мережевих шарів на й мережі 5GC |
|---|---|---|
| Найменування | SST | |
| eMBB | 1 | Абонентський трафік централізований в ЦОД в точці пірінга з Інтернет-провайдера ми ISP. Пакетні шлюзи UPF з великою пропускною здатністю і сесійного ємністю розміщуються в ЦОД макро регіонального рівня. Діапазон допустимих затримок PDB між абонентським терміналом і інтерфейсом N6 - 100- 300 мс. Для обслуговування деяких видів трафіку з затримками PDB в діапазоні 50-75 мс пакетні шлюзи UPF можуть розміщуватися географічно ближче до базових станці й gNB на регіональному рівні. Ступінь резервування - висока. |
| URLLC | 2 | Трафік децентралізується на рівні мережі доступу.<br>Пакетні шлюзи UPF з невисокою пропускною спроможністю і сесійного ємністю розміщуються поблизу, або разом з базовими станціями gNB. Діапазон допустимих затримок PDB між абонентським терміналом і інтерфейсом N6 пакетного шлюзу UPF становить 5-30 мс.<br>Ступінь резервування:<br>- висока для систем автоматизації виробництва і послуг, критичних до доступності та безперервності сервісів;<br>- не висока для масових послуг, не критичних до доступності та |

Продовження таблиці 1.4

| | | |
|---|---|---|
| | | безперервності сервісів. |
| MIoT | 3 | Абонентський трафік централізований в ЦОД макро регіонального рівня в точці розташування сервісної платформи MIoT. Діапазон допустимих затримок PDB між абонентським терміналом і інтерфейсом - до 300 мс. Пакетні шлюзи UPF з не великою пропускною здатністю і великий сесійного ємністю розміщуються в ЦОД макрорегіонального рівня.Ступінь резервування - невисока. |

Схема варіанту розгортання мереж і 5G / IMT-2020 в Україні, розроблена відповідно до вимог до мережевих верств, представлена на рис.1.11.

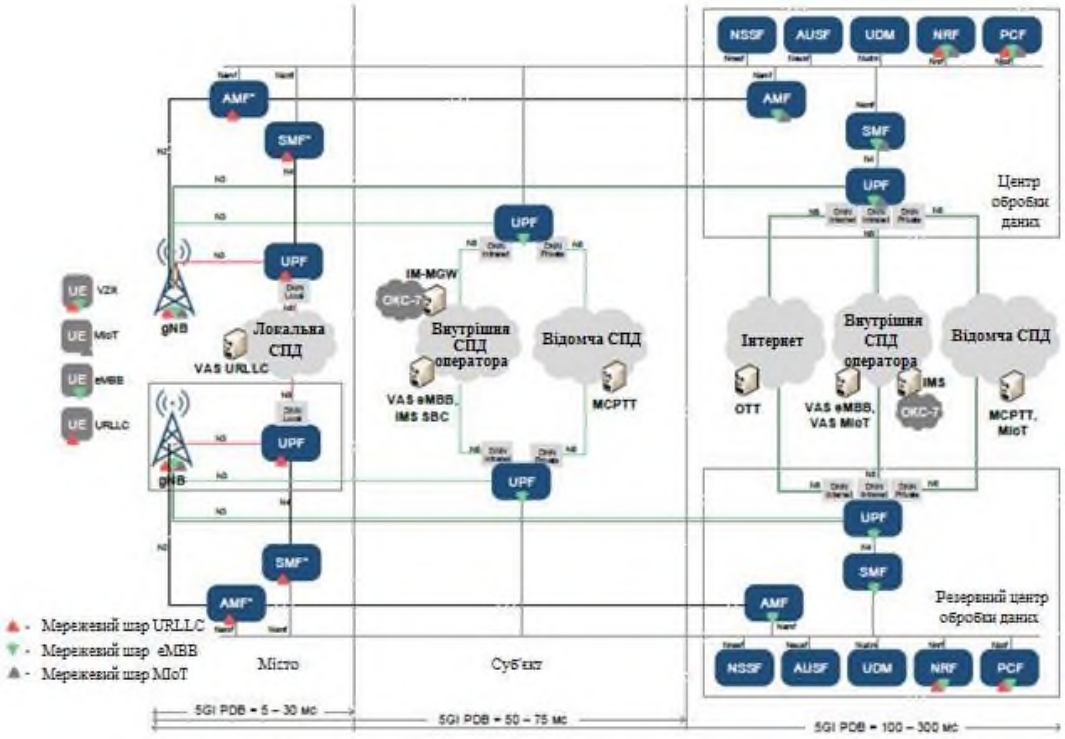



Рис.1.11 Варіант розгортання мережі 5G

Віртуальні мережеві функції AUSF, UDM, NSSF не належать до мережевих верств і є загальними. Віртуальн і мережеві функції NRF, PCF обслуговують всі мережеві шари (або можуть бути розподілен і між мережевими шарами відповідно

до технічної політикою оператора). Віртуальні мережеві функції AMF, SMF, UPF макро регіонального рівня обслуговують сесії і трафік мережевих шарів, не критичних до затримок (eMBB, MIoT).

З метою забезпечення високої надійності (коефіцієнта готовності мережі) можливе використання георезервування - розгортання географічно віддаленого резервного ЦОДа. Резервний ЦОД може мати меншу продуктивність за рахунок відсутності георезервування окремих віртуальних мережевих функцій VNF, наприклад, віртуальних мережевих функцій мережевого шару MIoT. В такому випадку надійність мережевого шару MIoT визначається технічними рішеннями основного ЦОДа.

На рівні суб'єктів країни розміщуються пакетні шлюзи UPF мережевого шару eMBB і платформи додатків VAS, що допускають затримки передачі даних 50-75 мс (наприклад, ігри в реальному часі, деякі платформи V2X, трафік яких не вимагає ультрамалих затримок.

У разі розміщення шлюзів UPF на рівні суб'єктів країни і реалізації голосових послуг за допомогою підсистеми IMS доцільно там же розміщувати обладнання комутації голосового трафіку (IMS SBC, IM-MGW).

На рівні міст муніципальних утворень розміщуються пакетні шлюзи UPF мережевого шару URLLC, що забезпечують ультрамалі затримки передачі даних 5-30 мс. Для послуг URLLC, що вимагають хендовер, наприклад, послуг інтелектуальних транспортних систем V2X, необхідно також на місцевому рівні розміщувати віртуальні мережеві функції AMF, SMF. Наявність віртуальних мережевих функцій AMF, SMF не високою продуктивності на локальному рівні зменшує затримки в процесі хендовер [12].

Розгортання мереж зв'язку 5G/IMT-2020 може здійснюватися за трьома основними сценаріями розвитку та використання мережевої інфраструктури, а також можливі їх комбінації:

- сценарій 1 - «Переважно самостійний розвиток мереж операторами рухомого зв'язку»;
- сценарій 2 - «Інтенсивне спільне використання мережевої інфраструктури

операторами рухомого зв'язку»;

- сценарій 3 - «Розвиток мереж і єдиним інфраструктурним оператором (EIO)».

Відповідно до моделі міграції від мереж попередніх поколінь до мереж 5G / IMT-2020 доцільно розгортання мережі виконувати послідовним кроками (див. табл. 6.3).

Заключний крок, який передбачає демонтаж опорної мережі EPC, виконується, коли всі абонентські термінали LTE підтримують NAS сигналізацію з опорною мережею 5GC, голосовий зв'язок за допомогою підсистеми IMS (мають IMS/SIP/SDP клієнтське програмне забезпечення, підтримують необхідні мережеві процедури управління потоками даних і сигналізацією згідно QoS Flow, забезпечують виявлення на мережі елементів підсистеми IMS (наприклад, P-CSCF), підтримують виклик екстрених оперативних служб за допомогою VoNR [13].

### 1.5 Аналіз складностей реалізації програмно-конфігурованих мереж

SDN розділяє рівень управління і рівень даних, що призводить до значного спрощення модуля управління. Таким чином вся логіка управління мережею зосереджена, наприклад, на одному сервері, а інші пристрої мережі, відповідно до концепції, використовуються тільки для передачі даних. Проте, одним із основних недоліків нової архітектури є складність масштабування рівня управління мережі. З і збільшенням кількості вузлів у мережі, і, відповідно, зі значним збільшенням запитів до рівня управління, навантаження на модуль управління зростає, і його продуктивність може значною мірою знижуватися. Таким чином, обчислення масштабованості рівня управління SDN є критичною проблемою для успішної адаптації SDN до великомасштабних мереж або мереж з великою кількістю потоків.

Оскільки мережі SDN використовують новий принцип побудови мереж, переважна більшість існуючих досліджень не створюють модель, а базуються на експериментах і моделюванні завдяки спеціалізованому програмному забезпеченню. Метою роботи є математичне порівняння різних типів архітектури рівня управління

SDN.

Незважаючи на переваги SDN, технологія досі потребує оптимізації та вирішення багатьох проблем, до яких відносяться наступні:

Динамічно адресувати зміни у реальном у часі. Можливість автоматизації об'єднання нових інфраструктур протягом декількох хвилин з впливом на декілька пристроїв одночасно є складною задачею, особливо з огляду на те, що відносн і статичні середовища сьогодні залежать від ручних конфігурацій. Завдяки SDN, нові обчислювальні пристрої, мережеві пристрої та пристрої для зберігання інформації можуть бути відразу доступні для використання. Щоденні перевірки на наявність нових пристроїв в мережі залишають величезні прогалини у загальні й видимості мережі [2].

Для вирішення цієї проблеми, необхідно розробити інструмент для моніторинг у змін у мережі, спроектований за допомогою відкритих API.

Після цього, адміністратору чи оператору мережі не потрібно буде перевіряти наявність нових пристроїв вручну - кожен новий пристрій буде автоматично додаватися до мережі.

Забезпечення швидкого зростання. Зростаючий попит на нові обчислення, мережі т а сховища в SDN ускладню є моніторинг платформи. Н а рис. 1.12 можн а побачити прогноз по зростанню мереж SDN. Необхідне рішення, що значно збільшить потужності моніторингу для швидкого зростання інфраструктури. Якщо вони не можуть додати додаткову потужність за вимогою, вони почнуть втрачати продуктивність, створюючи пробіли у моніторингу.

На відміну від застарілих інфраструктур у світ і SDN, ми можемо мати декілька накладених топологій, що працюють на вершині фізичної мережі.

Кожного разу, коли запускається новий сервіс, розгортається необхідна віртуальна інфоструктура, і, отже, кількість контрольованих елементів може швидко зростати з підвищеним попитом, перевершуючи традиційний менеджмент потенціал у [3].

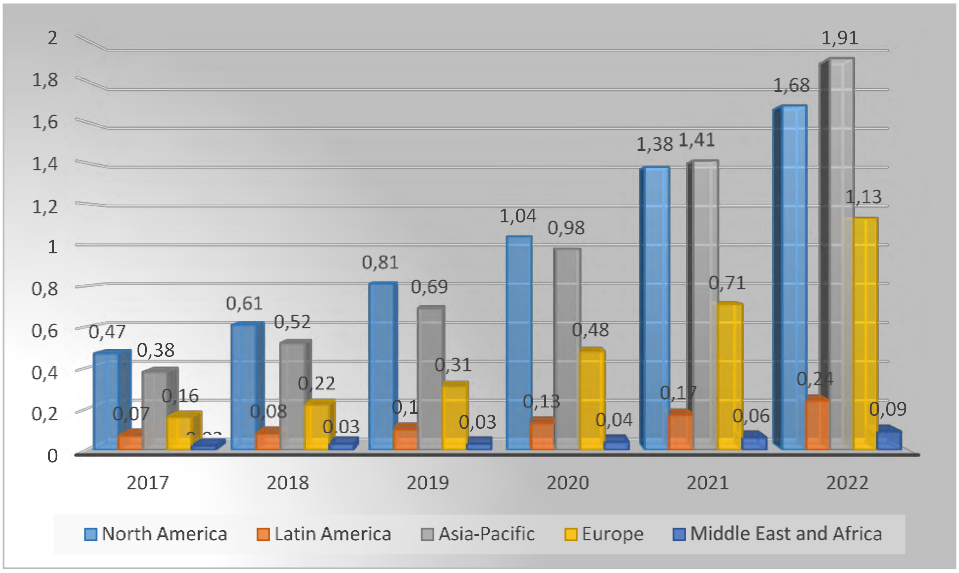



Рис.1.12 Прогноз розвитку мереж SDN

Рішенням є розгортання моніторингу продуктивності як у фізичному, так і у віртуальному вигляді. Коли потрібна додаткова продуктивність управління, необхідне збільшення кількості віртуальних пристроїв з азамовчуванням дозволяє контролювати продуктивність з вимогами SDN та надавати відповіді середовища впродовж декількох секунд.

В результаті моніторинг продуктивності повинен мати можливість зчитувати контекст конкретного клієнта або орендаря мережі. Зрештою, користувачі повинні мати змогу не лише запитати про стан та продуктивність окремих пристроїв або посилань у мережі , а й про те, як саме працює клієнт. Це також поширюється на топологію обслуговування, тобто контролери та рішення для моніторингу продуктивності обмінюються інформацією про фізичні і логічні підключення. SDN все ще дозріває, і в процесі його еволюції важливо подивитися, які динамічні зміни в реальному часі, швидке зростання за вимогою та інтеграція контексту послуг відіграватимуть ключову роль у забезпеченні успішного розгортання та уникненні прогалин у видимості діяльності у вашій інфраструктурі.

Проектування SDN відрізняється від проектування традиційних мережі протоколів, так як мережі SDN за своєю природою є орієнтованими на сервіси і повинні гнучко змінювати значення параметрів і характеристик в реальному часі, а також враховувати асинхронний режим взаємодії елементів і можливість множинного доступу до ресурсі в мережі. В якості моделі життєвого цикл у SDN застосовна спіральна модель. Вона успадковує всі переваги каскадної моделі, її характерною особливістю є можливість внесення змін на ранніх стадіях розробки і завершення кожного етапу перевіркою отриманих результатів, що забезпечує істотне зниження тимчасових і матеріальних витрат. Однак повноцінне функціонування подібної мережі на сьогоднішній день важко організувати. Основні проблеми, що виникають в процесі функціонування мереж, побудованих на основі концепції SDN, пов'язані з відсутністю стандартизованих протоколів взаємодії, наявністю розбіжностей в існуючих версіях специфікацій.

Відсутність єдиних стандартів також істотно впливає і на проектування SDN: організатори повинні враховувати, самостійно формалізувати і впроваджувати в свої рішення всі вимоги, закладені в різних версіях OpenFlow протоколів.

Таким чином, на різних етапах життєвого циклу SDN можливе виникнення ряду помилок, причинами яких є: неповний аналіз предметної області; помилки, що виникають при формалізації специфікації; різна інтерпретація стандартів; логічні помилки проектування; не повна відповідність пропонованим вимога; не правильне урізання функціональності протоколу; надмірність в реалізації протоколу; помилки при реалізації протоколу.

Для усунення помилок, можна сформувати ряд вимог, які можна застосувати на кожному етапі життєвого циклу протоколі в SDN, які дозволять уникнути помилок і підвищують ефективність функціонування мережі:

- формальний опис вимог, що пред'являються до додатків SDN, враховуючи особливості середовища і характеру переданих даних;

- розробка формальних методів перевірки спільного функціонування контролерів різних виробників: перевірка не суперечності команд і правил, закладених в логіку роботи контролера;

- розробка формальних методів перевірки взаємодії між рівнем додатків і передачею даних: перевірка коректності виконання команд і їх несуперечливість;

- формальне уніфіковане представлення специфікацій, які забезпечать єдиний підхід до взаємодії контролерів і додатків, представлених різними розробниками;

- розробка формальних методів перевірки відповідності готового рішення SDN його специфікації. Здійснення всіх перерахованих кроків можливо в процесі верифікації на кожному етапі розробки. При такому підході можливе істотне скорочення вартості розробки і впровадження нових додатків, а також придбання прогностичних знань про взаємодію між рівнями і створення шаблонних підходів.

Ще одною проблемою на шляху до впровадження SDN є трансформація мережі стандартного типу до SDN. Оскільки, як правило, SDN використовує протокол OpenFlow для обміну запитами між рівнем даних, це може ввести деяке обмеження на використання пристроїв. Тому одним з основних факторів при переході на SDN є впровадження в мережу OpenFlow пристроїв, які будуть взаємодіяти з існуючими пристроями. Крім того, не обхідно обміркувати, яким чином буде здійснене повернення до старого типу архітектури, оскільки, після переходу на SDN деякі функції мережі можуть перестати працювати. Також, важливим є перехід з фізичних серверів і пристроїв до віртуальних.

## 1.6 Аналіз принципів функціонування програмно-конфігурованих мереж

Мережеві пристрої, наприклад, комутатор Ethernet в локальній мережі підприємства, або маршрутизатор на мережі оператора зв'язку, складаються з двох основних компонентів: пристрої комутації пакетів (data plane, DP) і програмного забезпечення (ПЗ), яке управляє передачею пакетів з входу на вихід комутатора (control plane, CP). Це ПЗ іноді називають firmware, тому що тільки виробник (вендор) даного мережевого пристрою може його змінювати.

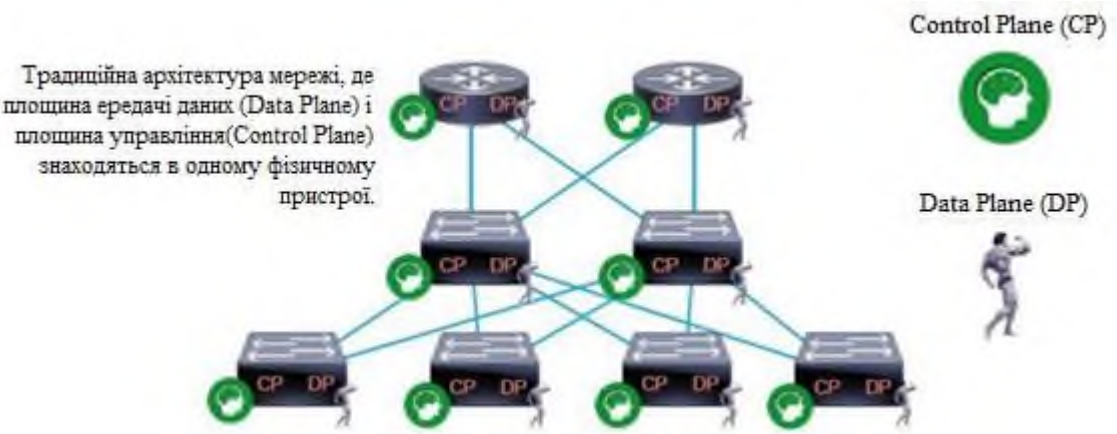



Рис. 1.13 Традиційна архітектура мережі з рівнями передачі даних DP і управління CP в кожному мережевому пристрої

Коли пакет даних прибуває на вхідний порт комутатора, цей порт запитує firmware, що робити з цим пакетом далі. Firmware визначає подальший адрес передачі пакета, по таблиці MAC-адрес сусідніх мережевих пристроїв, які підключені до комутатора, і визначає вихідний порт, куди цей пакет потрібно передати. Це дуже спрощений опис, але для подальшого розуміння принципу роботи SDN його досить.

Склад протоколів firmware є виключною компетенцією вендора, оскільки тільки він має доступ до вихідного коду. Оператор мережі змушений купувати разом з потрібними йому функціями мережевого пристрою і багато непотрібних в даний момент функцій, тільки лише тому, що вони вже «зашиті» в стандартне firmware.

Однак, це не єдиний недолік традиційного проектування мережі (networking). Мережа, у якій кожен мережевий елемент має власні «мізки», працює не кращим чином. Як аналогію, можна привести автомобільний рух в місті без використання хмарного сервісу навігації з пробками, до якого вже звикло більшість водіїв в великих містах.

На мережі кожен маршрутизатор аналогічний перехрестя, який проїжджає водій без навігатора. Щоразу він сам вирішує, куди повертати, орієнтуючись на візуальну завантаженість наступної ділянки.




Рис. 1.14 Порівняння міського водіння з навігацією і без нього

При водінні з навігатором, такої проблеми у нього не виникає. Він не тільки витрачає менше часу на рішення про наступний етап маршруту, а й прибуває в місце призначення набагато швидше, тому що навігатор підказує оптимальний маршрут, з урахуванням пробок, аварій, дорожніх робіт і ін. Проте, такий ефект виникає тільки тоді, коли більшість автомобілів (в ідеалі - всі) використовують хмарну навігацію, наприклад, від Google. Якщо більшість машин використовує оптимізовані маршрути, зменшується завантаженість вулиць і збільшується пропускна здатність всієї міської вуличної мережі.

Саме така ідея лягла у концепцію створення програмно-конфігурованих мереж.

Була запропонована ідея відділення «мізків комутатора» (його ПЗ у вигляді firmware) від обладнання комутатора (hardware). При цьому, традиційна мережа розпадається на дві площини - управління (Control Plane) і передачі даних (Data Plane).

Перша площина при цьому йде в централізовані сервери, а друга - залишається в обладнанні мережевих елементів, позбавлених надлишкового firmware. При цьому, кожна мережа і кожен мережевий елемент використовують із площини управління тільки ті функції, які в даний момент потрібні. Площина управління (Control Plane) називається SDN-контролером і розташовується на стандартних серверах, які розташовуються в центрах обробки даних (ЦОД), або

дата-центрах.

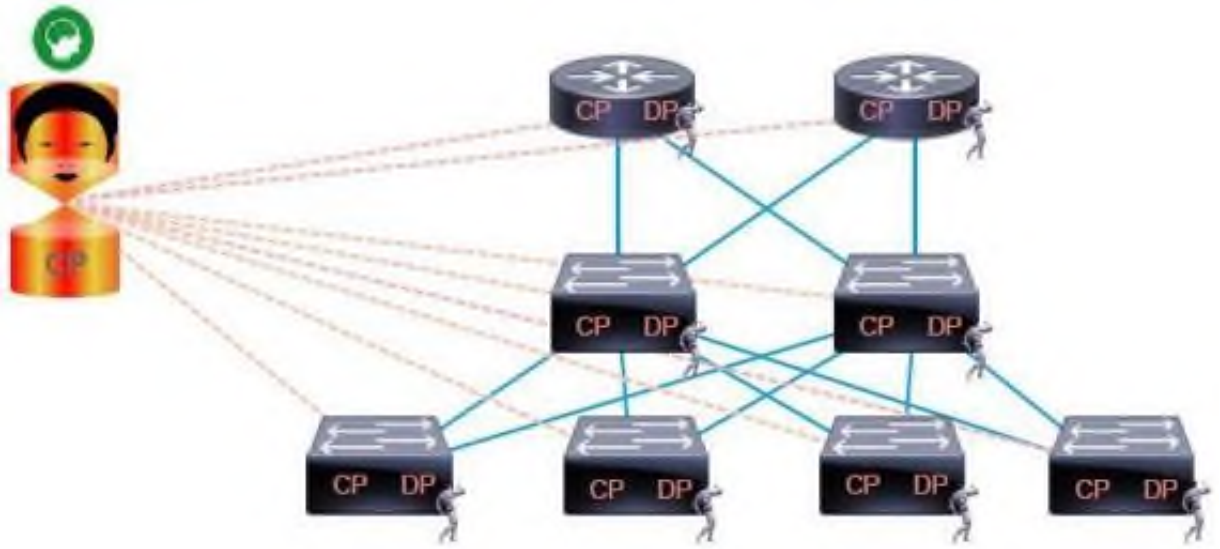



Рис. 1.15 Архітектура SDN-мережі

SDN, Software Defined Network: програмно обумовлена (або конфігурується) мережа. Це означає не тільки те, що мережеві елементи управляються програмно і можуть швидко і ефективно перебудовуватися, але і те, що на одному фізичному пулі мережевих елементів можуть бути розгорнуті багато мереж, які логічно не залежать один від одного. Такі логічні мережі можуть передавати потоки трафіку різних бізнес-додатків, не заважаючи один одному.

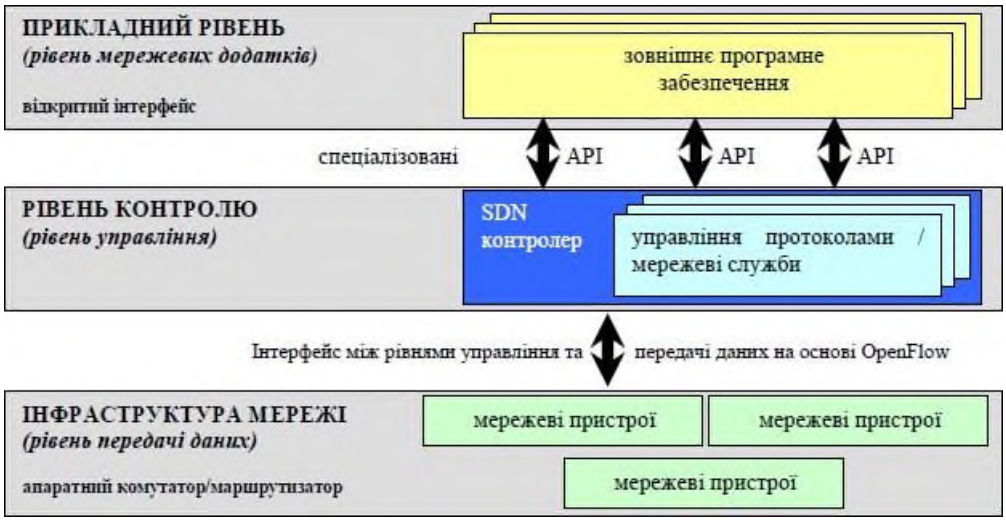



Рис. 1.16 Рівень додатків і протокол OpenFlow в SDN-мережі

Додатки, яким потрібні різні мережеві параметри і конфігурації мережі, адмініструють SDN-контролер за допомогою інтерфейсів програмування додатків API (Application Programming Interface). У такій архітектурі кожне бізнес-додаток може через SDN-контролер конфігурувати для себе логічну мережу із загальних ресурсів мережевої інфраструктури рівня передачі даних. І кожна така мережа буде працювати незалежно від інших логічних мереж в тому ж пулі ресурсів (при їх достатності) [14].

В архітектурі SDN можна виділити три рівні (рис. 1.16):

- інфраструктурний рівень, що надає набір мережних пристроїв (комутаторів і каналів передачі даних);
- рівень управління, що включає мережну операційну систему, яка забезпечує мережні сервіси та програмний інтерфейс для управління мережними пристроями та мережею;
- прикладний рівень – для гнучкого та ефективного управління мережею – прикладні вирішення високорівневого управління мережею (засоби забезпечення безпеки, балансування навантаження програмного міжмережного екрану, адміністрування, виявлення вторгнень, а також функції інжинірингу трафіку, управління мобільністю, управління доступом, організації енергоефективної роботи мережі та ін.).

Виділення функції управління в окремий рівень та її делегування центральному компоненту (рис. 1.17), націлені на оптимізацію мережних конфігурацій для вирішення прикладних завдань і, зокрема, дозволяють отримати наступні переваги:

- формати даних, правила обробки та технології передачі в комутаторі не обмежені певним рівнем взаємодії, типом устаткування або виробником;
- одиниця передачі може бути задана багатовимірним вектором, що включає поля з різних рівнів моделі мережної взаємодії;
- при побудов і правил пересилки пакетів можуть застосовуватися методи автоматизованої корекції потоків залежно від навантаження компонентів та інших

критеріїв;

- контролери мережі можуть об’єднуватися в мережні домени, які дозволяють оптимізувати та резервувати канали передачі.

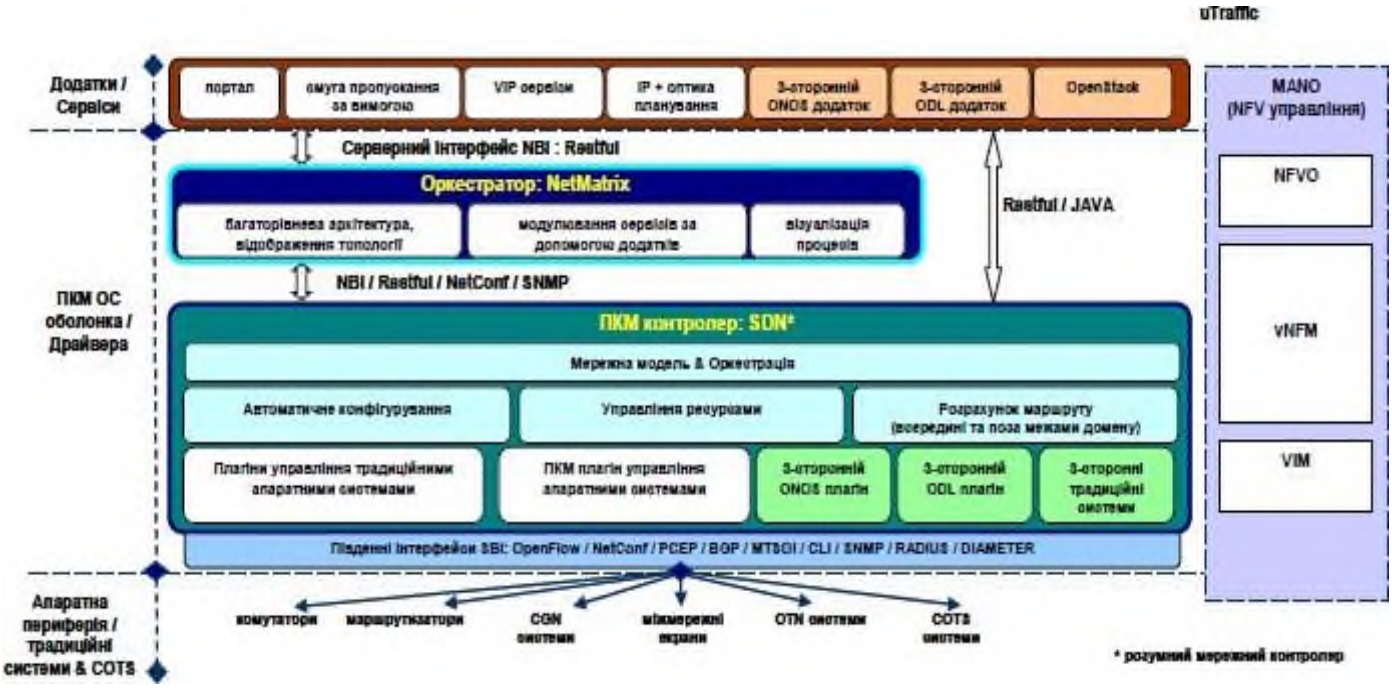



Рис. 1.17 Архітектура програмно-конфігурованих мереж

Інтелектуальні функції мережі зосереджені в централізованому мережному контролері, який відстежує загальний стан мережної інфраструктури і потоків, що протікають по ній. У такій концепції управління всією мережею відбувається в єдиній логічній точці, що значно спрощує завдання конфігурації та управління [15].

Крім того, простіше виглядає і функціонування мережних пристроїв, тому що на відміну від традиційної моделі не потрібно більше підтримувати та обробляти без ліч різних протоколів, а достатньо тільки отримувати та обробляти інструкції від контролерів ПКМ. Для налаштування мережі досить налагодити програмний контролер мережі, замість того, щоб змінювати сотні рядків кодів в безлічі мережних пристроїв мережі. Також поведінку мережі можна змінювати в реальному часі, а нові рішення впроваджувати за набагато коротший час, ніж в традиційній архітектурі. Централізуючи стан мережі в єдиному рівні контролю, ПКМ можуть конфігуруватися за допомогою програмних засобів [16].

Мережні контролери також володіють набором прикладних інтерфейсів, які дозволяють реалізувати типові завдання по маршрутизації, зокрема багатоадресність, безпека, контроль доступу, управління смугою пропускання, якість обслуговування, які дуже вузьконаправлено налаштовані під завдання конкретного споживача.

У комутаторі реалізований тільки рівень передачі даних. Замість контролера використовується набагато простіший пристрій, завдання якого полягає в отриманні даних, які надходять, визначення їх адресів і, якщо адресат є в таблиці комутації, негайної передачі даних комутаційній матриці. Інакше комутатор по захищеному каналу відправляє запит на центральний контролер мережі, і на підставі отриманої від нього інформації, вносить необхідні зміни в таблицю комутації, після чого здійснюється обробка отриманих даних (устаткування не переналаштовується вручну, а налаштовується за допомогою спеціального ПЗ).

Для управління інфраструктурою мережі від SDN-контролера необхідний протокол відкритого управління, а саме протокол OpenFlow. Робота OpenFlow полягає в модифікації змісту таблиці передачі пакетів всередині маршрутизатора або комутатора (Forwarding table). Архітектура мережевих пристроїв часто представляється у вигляді трьох площин: адміністрування (management plane), управління (control plane) і передачі даних (data plane), рис.1.18.

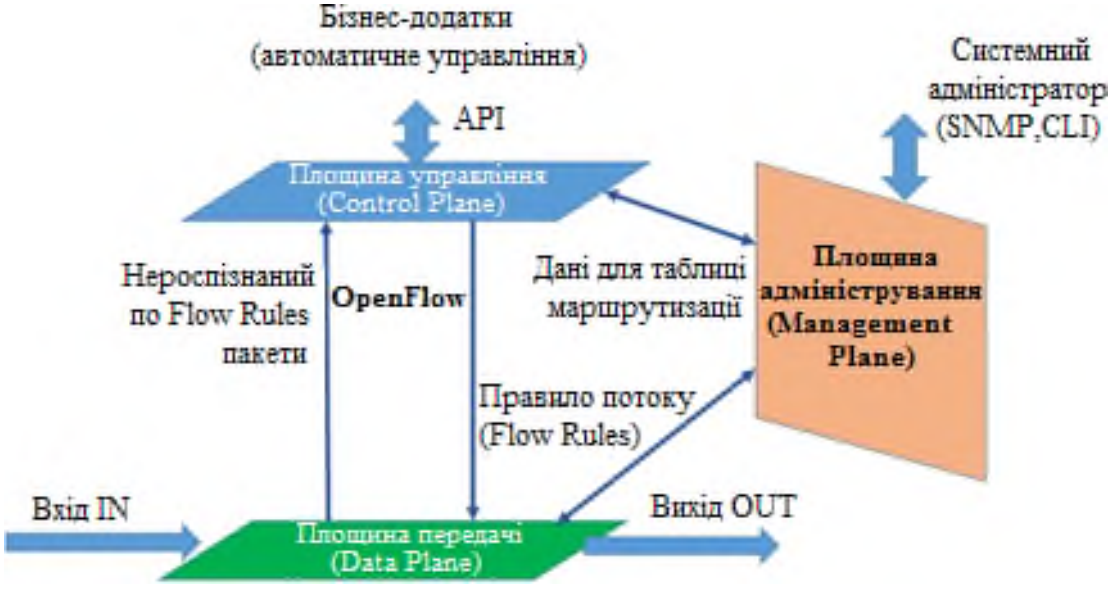



Рис. 1.18 Принцип роботи OpenFlow

Площина адміністрування (Management Plane) встановлює режими роботи пристрою, модифікує версії т.зв. фірмового ПО (firmware), жорстко «зашитого» в мережеве пристрій, виконує команди простого протоколу адміністрування мережі SNMP (Simple Network Management Protocol) від зовнішньої системи адміністрування мережі NMS, а також команди зовнішньої конфігурації пристрою через інтерфейс командного рядка CLI (Command Line Interface) , які вручну може вводити системний адміністратор. Площина передачі даних (Data Plane) передає пакети даних з входу пристрою (IN) на його вихід (OUT) відповідно до таблиці передачі (Forwarding Table). На площині управління (Control Plane) працюють протоколи маршрутизації і комутації.

Площина управління використовує таблицю маршрутизації (routing table) для складання таблиці передач і пакетів (forwarding table), яку використовує площину передачі даних (data plane). Таблиці передачі пакетів доставляється на площину передачі від площини адміністрування. Відповідно до таблиці передачі, пакет, який прибуває на вхідний порт комутатора (IN), передається площиною передачі даних на вихідний порт (OUT)[12].

OpenFlow - це метод управління потоками (flow) в мережі. Справа в тому, що мережеві пристрої (маршрутизатори, комутатори і інші) займаються передачею пакетів і фреймів відповідно до протоколів маршрутизації, проте, бізнес-додатки не використовують певні пакети для надання послуг. Вони обмінюються даними між сервером і клієнтом і створюють потоки пакетів від джерела до одержувача, який називаються «Flow» (потік).

Цінність OpenFlow в тому, що він реалізується автоматично через централізований SDN-контролер. При цьому управління площиною передачі стає набагато більш ефективним і швидким (agile), функціональні можливості пристроїв значно розширюються, і досягається «гранулярність» управління потоками.

# 2 МОДЕЛІ ОБСЛУГОВУВАННЯ ТА КОНТРОЛЮ ІНФОРМАЦІЙНИХ ПОТОКІВ НА БАЗІ ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖ

## 2.1 Аналіз системи контролю параметрів функціонування програмно-керованої мережі

Найважливішим завданням для оперативного управління мережею та перспективного планування її розвитку є облік використання ресурсів мережі на різних часових інтервалах (година, доба, тиждень, місяць) різними групами користувачів. Інше важливе завдання полягає в оперативному відстеженні стану мережі та її компонентів з метою виявлення аномальної поведінки, яка може бути наслідком атак на мережу або порушенням порядку використання мережевих ресурсів абонентами. Беручи до уваги високу цінність мережевих ресурсів (в першу чергу - пропускної здатності каналів), слід, перш за все, забезпечити можливість оперативного аналізу нерегулярностей та аномалій. У зв'язку з цим систему моніторингу слід ще розглядати як важливий компонент системи забезпечення безпеки корпоративної мережі [14].

Системи моніторинг у мережі повинні розроблятися також з урахуванням можливих перешкод різного виду (складність вимірювання, неточність результатів) та безпосередніх атак на ці системи. Через очевидну недостатність традиційної класифікації портів за протоколами/номерами необхідно залучати додаткову інформацію вищих семантичних рівнів. У сучасних мережах практично повсюдно використовується протокол SNMP, який дійсно є простим за своєю суттю, але потребує додаткових ресурсів для забезпечення постійного збору, зберігання, аналіз у даних і візуалізації результатів цього аналізу. У мережах досить великого масштаб у висока складність та поверхневий підхід до побудови системи збору та аналізу статистики призводить до неефективних, немасштабованих рішень.

Завдання дослідження характеристик інтенсивності потоків даних у сучасних корпоративних мережах при завантаженні в сотні і більше Мбіт/с є не тривіальним і вимагає ретельного вивчення.

Спрощені підходи до аналізу трафіку і спроби отримання інформації про мережеві додатки на підставі легкодоступних атрибутів та характеристик потоків даних найчастіше виявляються не продуктивними. Так, в більшості програмах обмін у файлами активно використовуються прийоми, що ускладнюють достовірну ідентифікацію таких додатків (динамічне призначення портів, децентралізовані сховища, використання поширених прикладних протоколів як транспортних, а також криптографічні методи приховування та маскування трафіку). Тому для виявлення мережевих аномалій необхідний ретельний аналіз. Ці обставини вимагають використання додаткових технічних, програмних та алгоритмічних засобів і математичних моделей досліджуваних процесів [15].

Характеристики функціонування програмно-керованої мережі, що складається з різнорідних OpenFlow комутаторів, залежать від апаратних характеристик кожного комутатора. З метою зменшення складності та вартості комутатора постачальники можуть обмежити функціональні можливості OpenFlow, наприклад, розмір апаратної таблиці потоків або можливостей цієї таблиці щодо пошуку за певними полями чи виконання певних дій над пакетами. Додатки, що встановлюються на контролері, повинні явно враховувати ці обмеження, щоб уникнути можливих проблем, пов’язаних з погіршенням продуктивності мережі в процесі її роботи. У цій роботі ми розробляємо систему моніторингу для тестування продуктивності та якості обслуговування потоків у програмно-керованих мережах на етапі їхнього функціонування. Варто також зазначити, що ця система може бути використана як платформа для розробки автоматизованих тестів, специфічних для апаратної реалізації того чи іншого пристрою або топології мережі.

Основна мета полягає в забезпеченні централізованого моніторингу параметрі в мережевих пристроїв і формуванні характеристик функціонування мережі на виході. Результати моніторингу можуть бути додатково використані при плануванні мережі або для динамічної оптимізації мережі, наприклад, встановлення правил з урахуванням апаратних характеристик комутатора й передачі трафіку через різні шляхи для уникнення вузьких місць у мережі.

Специфікація OpenFlow визначає необхідну функціональність, яка повинна

бути реалізована в кожному комутаторі OpenFlow.

Метою цієї специфікації є забезпечення уніфікованих процесів контролю та управління мережею, що складається з пристроїв різних моделей від різних виробників. Проте реалізація необхідної функціональності є індивідуальною та змінюється від виробника до виробника і, таким чином, може привести до змін продуктивності в реальній мережі. Як правило, проблеми виникають уже тоді, коли мережа налаштована й окремі комутатори починають створювати вузькі місця, погіршуючи продуктивність та якість обслуговування. Без сумніву, що такі недоліки можна врахувати на стадії проектування мережі та розробки програмного забезпечення для контролера.

Для цього необхідно, щоб розробники додатків для ПКМ змогли отримати інформацію про обмеження продуктивності конкретного комутатора з метою забезпечення стабільної та надійної роботи мережі. Завдяки запропонованій системі розробники зможуть отримати необхідні дані та можливість охарактеризувати продуктивність конкретного комутатора [15, 16].

Комутатор, залежно від апаратної реалізації, може надавати доступ до окремих параметрів (повідомлення типу ofp_capabilities). Специфікація OpenFlow містить загальний список параметрів доступних для моніторингу:

- статистика потоків (тривалість існування, пріоритет, кількість оброблених пакетів та байт);
- статистика таблиць потоків (кількість правил, кількість оброблених пакетів та байт);
- статистика портів (кількість переданих/відкинутих пакетів/байт, помилок передачі та колізій);
- статистика черг (довжина черги, кількість переданих пакетів/байт, кількість відкинутих пакетів через переповнення);
- інші (STP, збірка сегментів IP пакетів).

Основна мета полягає в тому, щоб створити простий, легкий у використанні інструмент порівняльного аналізу, який може бути основою для написання тестових сценаріїв користувачем. Тому в роботі розроблено систему моніторингу параметрів

функціонування комутатор а OpenFlow з використанням мови програмування *Python* [17].

Розроблена система дозволяє здійснювати моніторинг як OpenFlow параметрів, так і параметрів QoS, пов'язаних з роботою комутатора. До параметрів QoS належать: пропускна здатність, затримка, джиттер і втрати. До параметрів OpenFlow відносять: максимальну кількість правил з конкретною структурою, тривалість встановлення правила, тривалість опитування статистики таблиці потоків, тривалість обробки пакетів з використанням програмних таблиць потоків, тривалість зчитування інформації з лічильників, а також завантаження центрального процесора.

На рис. 2.1 відображено архітектуру програмно-керованої мережі з інтегрованою системою моніторингу.

Основним компонентом розглягутої системи моніторингу є додаток моніторингу, встановлений н а фізичном у сервері. Це й додаток виконує ключову роль збору, форматування та представлення інформації у форматі, зручному як для людини, так і для подальшої обробки цієї інформації іншими додатками, наприклад, контролером. База даних зберігає інформацію, необхідну для роботи центрального додатка, наприклад, налаштування комутаторів, моделі т а технічні особливості того чи іншого комутатора. Ці дані заносить в базу даних адміністратор мережі. У базі даних також зберігаються зібрані дані моніторингу та оброблені статистичні характеристики поведінки мережі в певні періоди.

Для збору даних можуть використовуватися декілька каналів зв’язку як з комутаторами, так і з контролером. Зв’язок з комутаторами може відбуватися через віддалене з’єднання з операційною системою комутатора на основі протоколу SSH або чер з вторинний OpenFlow канал за допомогою додатку OVS- OFCTL, що є частиною пакету OpenVSwitch. Комунікація з контролером може відбуватися без посередньо за рахунок інтеграції його в контролер або ж за допомогою REST API, що на сьогодні надається більшістю існуючих контролерів.




Рис. 2.1 Архітектура програмно-керованої мережі з інтегрованою системою моніторингу

База даних містить дві категорії даних. До першої категорії належать дані для конфігурації системи моніторингу, до другої – дані, зібрані системою моніторингу з мережі. Модель даних для конфігурації системи моніторингу відображено на рис.2.2.

Наведена модель відображає структуру інформації про комутатори та контролери, які є елементами окремої мережевої топології. Ця інформація заноситься адміністратором мережі [18]. У ПКМ кожен комутатор повинен мати власний ідентифікаційний номер довжиною 48 біт. У результаті аналізу структури даних «Конфігурація мережі» система моніторингу отримує на основі зазначених ідентифікаторів всю необхідну інформацію як про комутатори, так і про контролери.

У процесі роботи система моніторингу зберігає всю зібрану інформацію у базі даних. Варто зауважити, що, у разі невеликих обсягів даних, частину даних про попередній стан мережі система моніторингу зберігає в своїй кеш пам’яті.

Це потрібно для того, щоб пришвидшити аналіз динаміки зміни стану мережі протягом невеликих інтервалів часу.

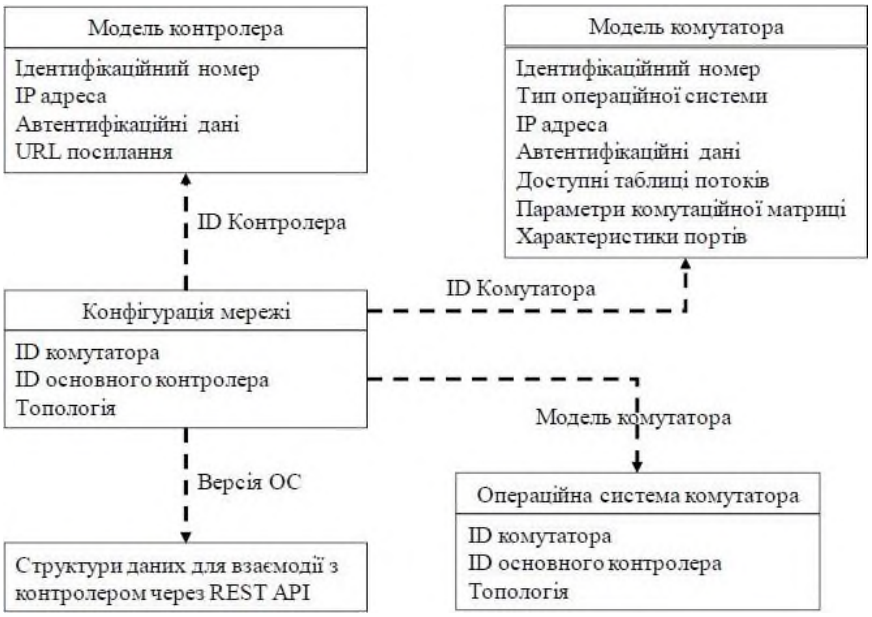



Рис. 2.2 Модель даних для конфігурації системи моніторингу

Приклад структури даних у форматі JSON для контролера та комутатора відображено в табл. 2.1.

Таблиця 2.1

Структури даних для конфігурації комутатора та контролера

```
datapath2 = {
"ip":"10.1.1.15",
"user":"manager",
"password":"",
"openflow_instance_name":"test01",
"cli_name":"sw1#",
"dpid":"00:64:74:46:a0:5f:1e:80",
"model":"3500",
"software_tables":["200"],
"hardware_tables":["100"]}
```

```
controller2 = {
"id":"00:00:00:00:00:01",
"ip":"10.0.1.17",
"user":"sdn",
"password":"skyline",
"URL":"ip:5544/sdn/login",
"OS":"2.5.1",
}
```

Ця інформація також може надаватися контролеру на вимогу, а то й повністю керуватися контролером у випадку інтеграції системи моніторингу та контролера. Модель даних для зберігання поточного стану мережі відображено на рис.2.3.

Розглянемо архітектуру центрального додатку моніторингу, представлену на рис.2.4. Інформація про комутатори (IP-адрес а, SSH ім'я користувача й пароль, ідентифікаційний номер комутатора, модель, ідентифікатори таблиць потоків тощо)

зберігаються в компоненті «Конфігурація мережі». Цей компонент також містить набори моделей потоків, які сумісні з програмно - керованими комутатори конкретної моделі.

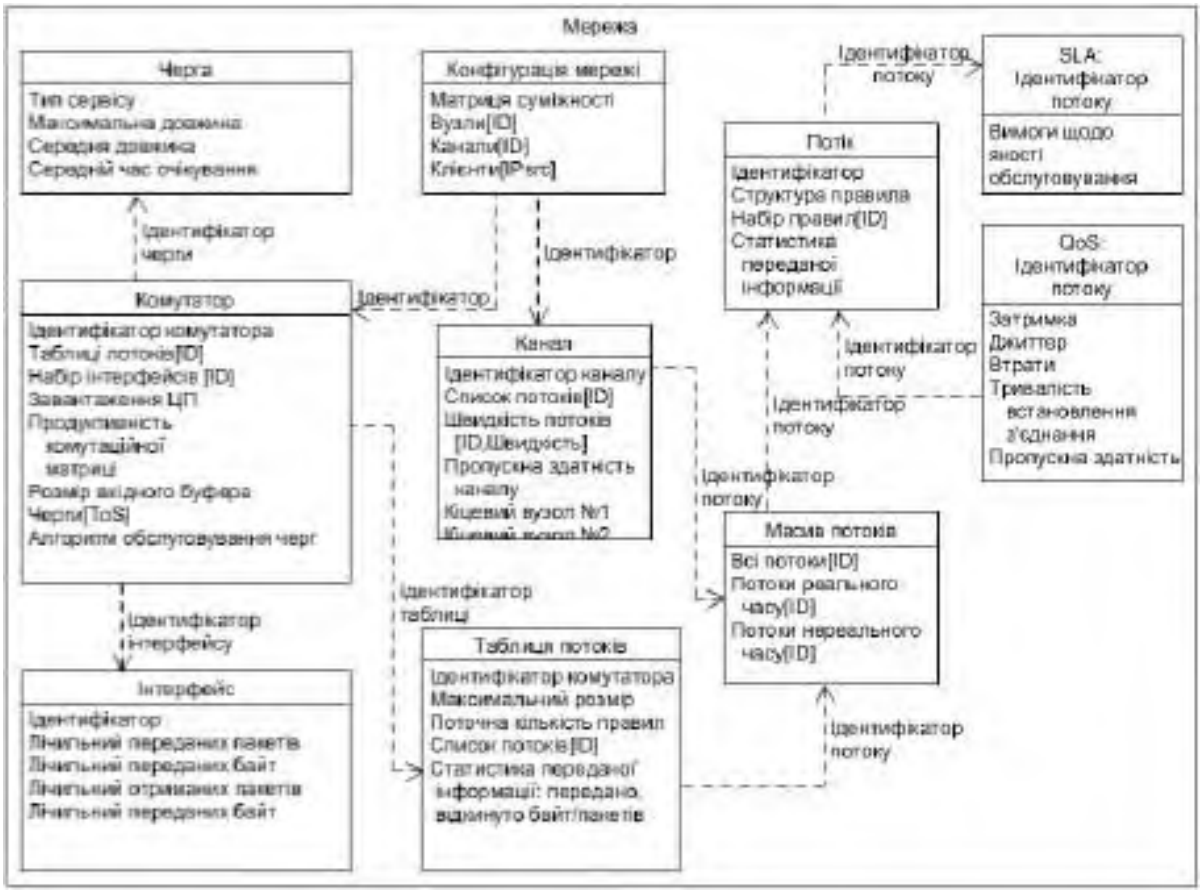



Рис. 2.3 Модель даних для зберігання поточного стану елементів мережі

Для контролю за параметри комутатора використовується один з компонентів «Монітор» залежно від типу параметра. У випадку моніторингу через SSH «Екземпляр мережі» використовує монітор SSH, який на основі ідентифікатора комутатор а отримує дані для формування об’єкта «Віддалений доступ». Цей об’єкт базується на бібліотеці для роботи з терміналом та містить методи для управління й моніторингу комутатора з використанням інструкцій операційної систе ми конкретного комутатора. Таким чином, система моніторингу може бути розширена та доповнена іншими моделями комутаторів [19].

Для маніпуляцій OpenFlow параметрами комутатора додаток може використовувати два способи. Перший забезпечується шляхом інтеграції системи з контролером або ж може використовувати інтерфейс RES T API для комунікації з

контролером. Перевагою використання цього каналу є можливість отримати як не оброблену інформацію про потоки даних та лічильники, так і більш складну інформацію, зокрема: зв'язки між комутаторами, чи найкоротший шлях між двома вузлами в мережі.

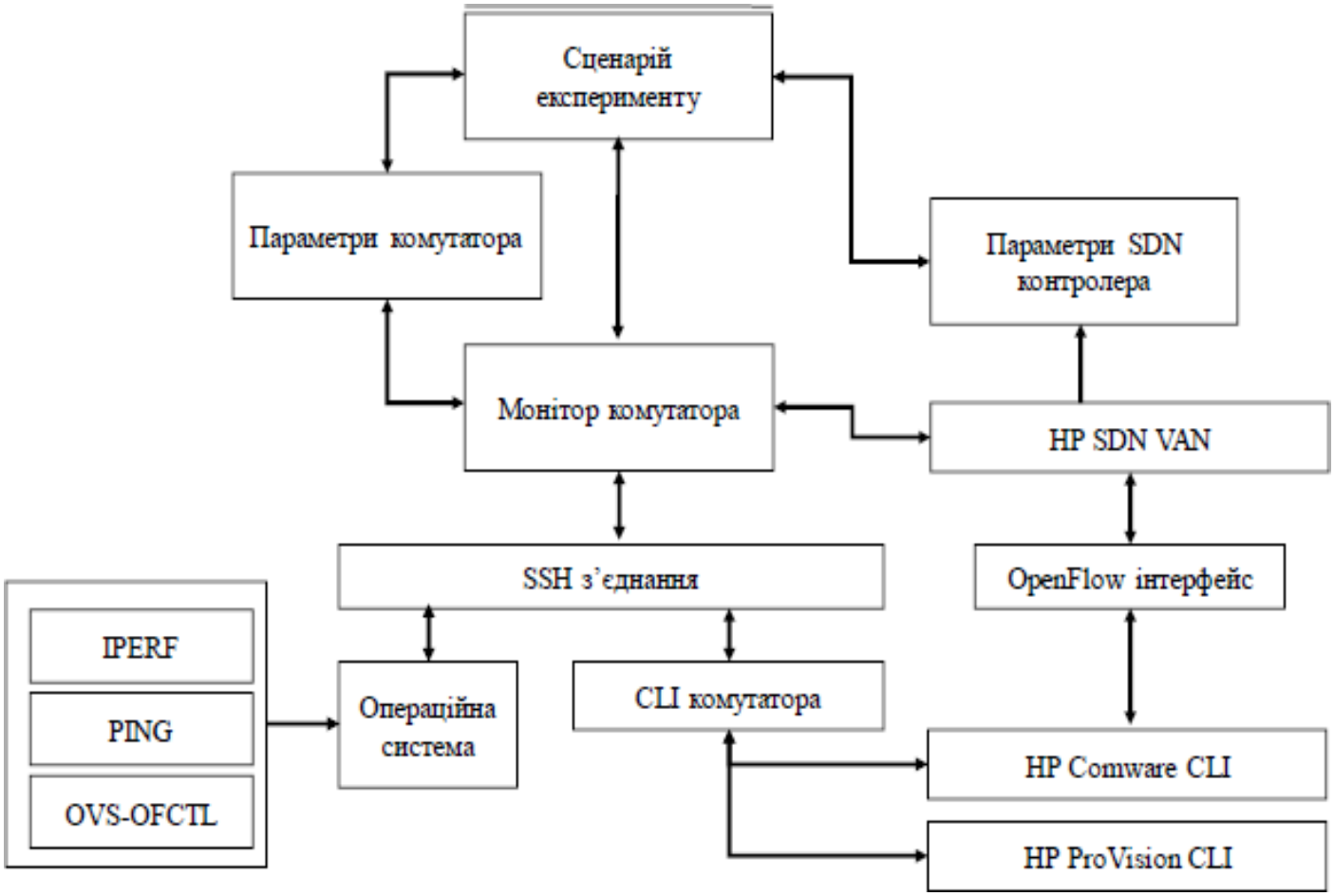



Рис. 2.4 Архітектура центрального додатку моніторингу програмно-керованої мережі

Недоліком використання цього способу є необхідність створення моделей запитів та відповідей у форматі JSON. Відповідно до другого способу, таблицями потоків можна керувати безпосередньо за допомогою додатку *ovs-ofctl*.

У разі, коли система моніторингу вбудована в контролер, він може безпосередньо використовувати методи запущеного додатку SDN для отримання інформації про конкретний комутатор чи маніпулювання таблицею потоків.

## 2.2 Параметри якості обслуговування для довільних потоків у програмно- керованих мережах

Для сервісів потокового характеру втрати пакетів або зміна порядку надходження пакетів спричиняє погіршення якості обслуговування, що проявляється у формі завмирання та спотворення кадру відео чи фрагменту аудіо даних. Для того, щоб забезпечити належний рівень якості обслуговування, а відповідно і сприйняття, моніторинг параметрів якості обслуговування необхідно проводити не окремо на кожному комутаторі, а загалом з моменту входження трафік у в мережу до моменту його виходу з неї.

Методи моніторингу трафіку завжди були актуальними серед науковців у сфері телекомунікацій. Зазвичай, він зводиться до вимірювання обсягів і характеристик трафіку для окремої мережі. На сьогодні велика кількість методів використовується для вимірювання завантаження каналу, затримки передачі пакету з кінця в кінець, а також втрат пакетів. Архітектура ПКМ, завдяки централізованій площині керування, дає змогу управляти багатьма потоками та приймати складні рішення в єдиній логічній точці системи.

Запропонована система моніторингу дає змогу оцінити параметри якості обслуговування для довільних потоків у програмно- керованих мережах. Основна ідея вимірювання – використовувати додаток моніторингу як опорну точку. Для цього в мережу вводиться тестовий пакет, заголовок якого відповідає заголовку пакетів, що належать цьому потоку. Пакет вводиться в мережу на комутаторі, де потік входить у мережу, і виводиться з площини даних на комутатор і, де потік покидає мережу. При цьому корисне навантаження тестового потоку містить дві важливі змінні: перша змінна включає ідентифікатор потоку; друга – момент введення потоку в мережу [20]. Тестовий пакет періодично вводиться у мережу з наперед визначеним інтервалом, що залежить від рівня завантаження каналу та швидкості потоку, для якого вимірюється затримка. Таким чином, пакет передається шляхом проходження всіх пакетів цього потоку і зазнає такої самої затримки. Схему вимірювання затримки потоку відображено на рис.2.5.

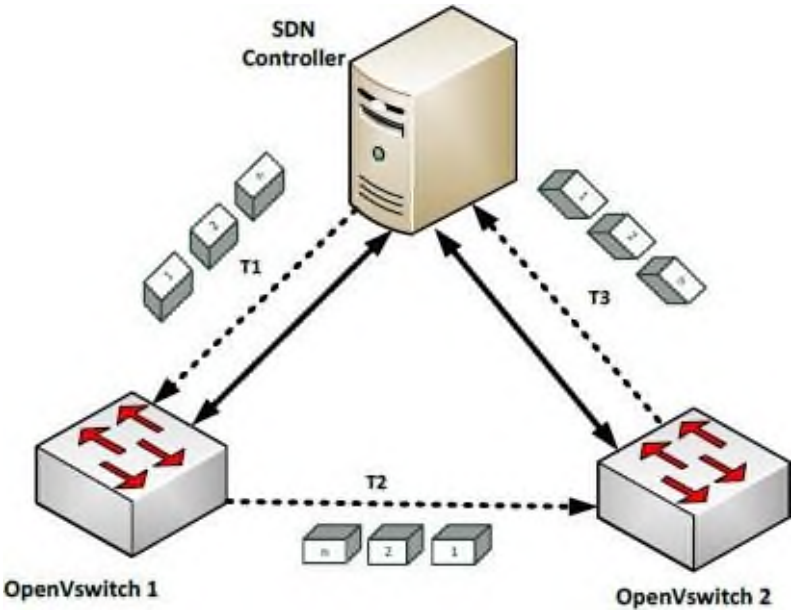



Рис. 2.5 Схема вимірювання затримки окремого потоку в програмно-керованій мережі

На останньому комутаторі тестовий пакет виводиться із площини передачі даних і відправляється в систему моніторингу. Система моніторингу визначає затримку цього пакету як різницю між часом його відправлення, отриманим з корисного навантаження цього пакету, та часом надходження, який фіксується в момент його отримання додатком моніторингу.

Алгоритми моніторингу параметрів якості обслуговування представлено на рис. 2.6. Вся інформація про затримки потоків зберігається в спеціалізованій таблиці. Використовуючи ці дані, інші процеси на контролері мають змогу здійснювати управління трафіком та оптимізацію якості обслуговування для окремих потоків.

Перший алгоритм слідкує за розкладом моніторингу потоків, які були внесені контролером у список таких, що потребують оцінки параметрів якості обслуговування. У випадку, якщо такий список не порожній, алгоритм відправляє тестові пакети в мережу та записує їхні копії в спеціальну чергу. Ці копії використовуються другим алгоритмом для співставлення з отриманими пакетами

з мережі.

Особливістю запропонованого алгоритму є те, яким саме чином тестовий

пакет передається по мережі. Для цього можуть використовуватися додаткові правила, що встановлюються для комутації такого пакету вздовж шляху, для якого вимірюється затримка [19].

Додаткове правило встановлюється на кожному комутаторі. У запропонованому методі додаткове правило встановлюється тільки на комутаторі, де потік покидає мережу. На всіх інших вузлах пакет порівнюється з тим же ж правилом, з яким порівнюються всі інші пакети потоку. Тому, щоб відокремити тестовий пакет на вихідному комутаторі з потоку, пропонується структура правила, подана в табл.2.2.

Відомо, що програмно-керовані комутатори мають змогу порівнювати поля заголовків пакетів з полями правил, використовуючи маску.

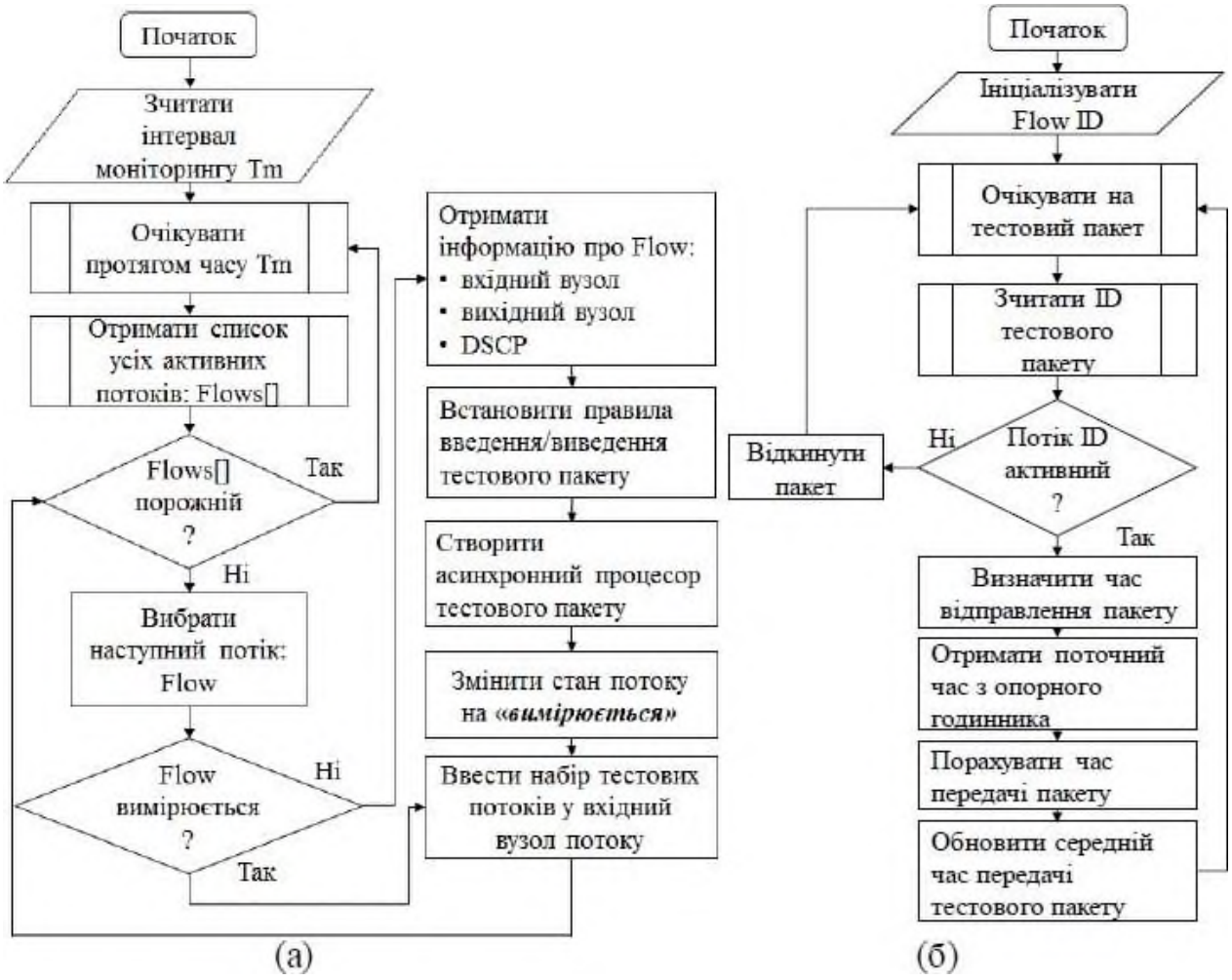



Рис.2.6 Алгоритми відправки (а) та очікування (б) пакету для вимірювання затримки потоку

Таблиця 2.2

Приклад правила в таблиці потоків для вимірювання затримки потоку

| Порт | DST MAC | SRC MAC | ETH TYPE | IP TOS | DST IP | SRC IP | IP PROTO | TCP/UDP SRC | TCP/UDP DST |
|---|---|---|---|---|---|---|---|---|---|
| * | * | * | * | * | * | * | * | * | 40000/4 |

Це, в першу чергу, застосовується для реалізації функцій маршрутизації, коли комутатор порівнює не всю IP адресу, а лише її мережну частину, ігноруючи при цьому біти, що відповідають за адресу станції. Для цього, встановлюючи правило, контролер явно задає комутатору кількість біт адреси, які повинні ігноруватися. Саме ця властивість використовується для вилучення тестових пакетів з потоку. Порівняння на основі TCP чи UDP портів застосовується в мережах вкрай рідко, переважно на крайових вузлах. Такий базовий аналіз протоколів транспортного рівня дає змогу створити найпростіший Firewall на межі мережі та заблокувати проходження окремих потоків, наприклад, заблокувати пакети, які приходять з певної IP адреси та мають встановлені певні порти.

У роботі пропонуємо використовувати діапазон портів від *40000* до *50000,* маскуючи останні чотири цифри порту. Коли проводиться вимірювання затримки для конкретного потоку, система моніторингу вибирає для нього порт із зазначеного діапазону та створює відповідне правило, яке повністю дублює правило для передачі цього потоку і порівнює тестовий пакет з вибраним портом.

Схему вимірювання затримки потоку в мережі відображено на рис.2.8. Усі тестові пакети, введені в мережу з цим портом, будуть виведені з мережі на кінцевому комутаторі шляху і передані на контролер або ж на систему моніторингу, якщо вона фізично відокремлена [20].

Зрозуміло, що виміряна затримка враховує тривалість передачі пакету між контролером та вхідним комутатором, а також тривалість передачі між контролером і вихідним комутатором. Тому з кожним десятим тестовим пакетом

контролер здійснює оцінку сигнального каналу, а саме – відправляє ICMP запит до обох комутаторів та отримує відповідь.

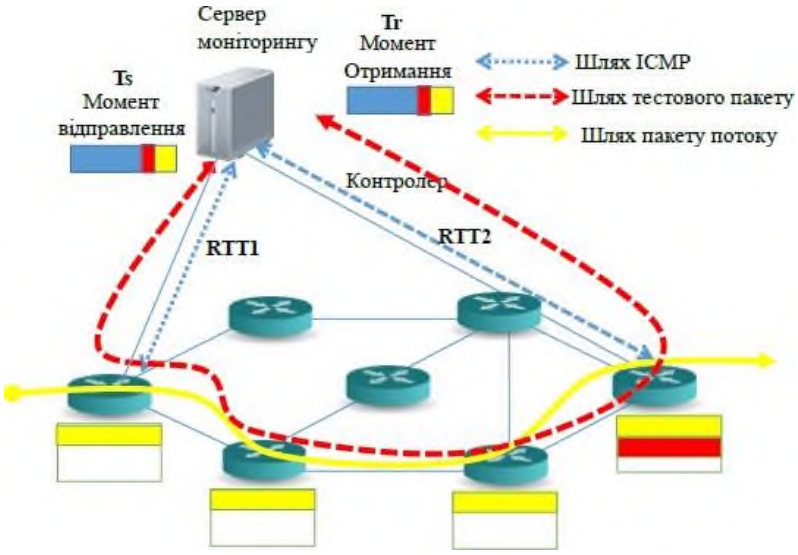



Рис. 2.7 Схема вимірювання затримки передачі окремого потоку в мережі

У результаті отримані значення враховуються при обчисленні затримки шляху таким чином:

$$Delay = t_S - t_r - \left(\frac{RTT_1}{2} + \frac{RTT_2}{2}\right) \quad (2.1)$$

де *Delay* – тривалість передачі тестового пакету між першим та останнім комутатором шляху потоку;

$t_s$ – момент відправлення тестового пакету з контролера; $t_r$ – момент отримання тестового пакету контролером;

$RTT_1$ та $RTT_2$ – тривалості відгуку першого й останнього комутатора шляху на *ICMP* запит від контролера.

Джиттер потоку вимірюється як різниця зазначених затримок.

## 2.3 Алгоритм перерозподілу трафіку на основі відносного пріоритету потоку

Технологія програмно-керованих мереж дає змогу ідентифікувати потік за більшою кількістю ознак, а саме: номером вхідного порту, адресою канального рівня, міткою віртуальної локальної мережі, пріоритетом у віртуальній локальній мережі, типом мережевого протоколу (*ARP, ICMP, IP*), адресою мережевого рівня (*ToS* – типом сервісу у випадку, якщо протокол мережевого рівня IP), типом транспортного протоколу (*UDP, TCP*), значеннями портів транспортного протоколу. Специфікація *OpenFlow* також передбачає ідентифікацію за міткою *MPLS*. Аналіз пакету за перерахованими ознаками дає змогу керувати окремими потоками, що належать окремим користувачам, не впливаючи при цьому на всі інші потоки. У такому разі швидкість потоку не має значення, а важливі тільки параметри, що його ідентифікують у мережі [21].

Для гнучкого управління трафіком важливо врахувати взаємозв'язок між типом трафіку (наприклад, реального часу чи передачі даних з файлового сервера) та мережевих параметрів, зокрема таких: доступна пропускна здатність, втрати пакетів, джиттер та затримка. Аналізуючи типи трафіку, варто зауважити такі моменти:

- VoIP трафік є дуже чутливим до втрат; в ідеалі втрати повинні бути відсутніми, особливо, коли використовується кодек з компресією;
- максимально допустима затримка потокового відео залежить від розміру буфера кінцевих клієнтів, у зв'язку з чим вона може суттєво варіюватися;
- допустимий джиттер не є фундаментальним параметром для передачі потокового відео, а тому до нього немає суворих вимог;
- вимога потокового відео до пропускної здатності залежить від формату кодування та швидкості відеопотоку, а, отже, не є фіксованим значенням.

Більш того, як у мультимедіа, так і в додатках для телефонії, параметри якості обслуговування можуть залежати від типу кодека, механізму виправлення помилок та швидкості складових потоків. Зважаючи на ці зауваження, досить складно точно

виміряти якість обслуговування з точки зору користувача, оскільки необхідно врахувати значну кількість різних змінних.

Вимоги щодо якості обслуговування певних класів трафіку, згідно з рекомендаціями ITU-T Y.1541, зведено в табл.2.3.

Нульове значення параметра означає, що рекомендація не встановлює ніяких обмежень щодо цього параметра. Його значення може бути довільно вибраним самим оператором мережі. Рекомендований інтервал оцінки параметрів у мережі становить одну хвилину, про те оператори самі можуть вибирати цей інтервал [22].

Таблиця 2.3

Класифікація вимог до параметрів якості обслуговування

| Параметри функціонування мережі | Клас трафіку | | | | | |
|---|---|---|---|---|---|---|
| | Клас 1 | Клас 2 | Клас 3 | Клас 4 | Клас 5 | Клас 6 (невизначений) |
| Затримка, мс | 100 | 400 | 100 | 400 | 1000 | 0 |
| Джитер, мс | 50 | 50 | 0 | 0 | 0 | 0 |
| Коофіцієнт витрат, % | 0,001 | 0,001 | 0,001 | 0,001 | 0,001 | 0 |
| Коофіцієнт помилок,% | 0,0001 | | | | | 0 |

З урахуванням рекомендації щодо важливості тих чи інших параметрів для окремих класів трафіку в роботі сформовано таблицю вимог щодо якості обслуговування існуючих сервісів, що функціонують у мережі Інтернет табл.2.4.

Таблиця 2.4

Розподіл найпопулярніших сервісів за класами якості обслуговування

| Клас | Характеристики | Приклад |
|---|---|---|
| 1 | Реального часу, чутливі до джиттеру, інтенсивна взаємодія | VoIP, Skype (аудіо, відео) |
| 2 | Реального часу, чутливі до джиттеру, | VoIP, Інтернет, телебачення |

Продовження таблиці 2.4

| | | |
|---|---|---|
| | інтерактивні | |
| 3 | Транзакції, високоінтерактивні | HTTP, Web-Services |
| 4 | Транзакції, інтерактивні | Сигналізація (OpenFlow) |
| 5 | Тільки з низькою чутливістю до втрат | FTP, Cloud, потокове відео (Youtube) |
| 6 | Тільки з низькою чутливістю до втрат | Будь які інші дані |

У результаті аналізу двох таблиць представлено зведену табл.2.5 вимог що до параметрів якості обслуговування для конкретних додатків. Введемо два додаткових критерії для класифікації потоків: перший критерій – чутливість до неправильного порядку отриманих пакетів; другий критерій – пріоритет окремого користувача.

Для розрахунку відносного пріоритету потоку для конкретного шляху спочатку знайдемо відносні коефіцієнти для кожного потоку. Відносні коефіцієнти розраховують за формулами (2.3-2.9), тобто, як відношення мінімальних значень параметрів якості обслуговування до поточних значень, отриманих у результаті моніторингу мережі [22].

Відносний коефіцієнт втрати пакетів:

$$p = \frac{P_{min}}{P} \tag{2.2}$$

Відносний коефіцієнт затримки пакетів:

$$t = \frac{T_{min}}{T} \tag{2.3}$$

Відносний коефіцієнт джитера:

$$j = \frac{J_{min}}{J} \tag{2.4}$$

Відносний коефіцієнт смуги пропускання:

$$c = \frac{C}{C_{min}} \tag{2.5}$$

Відносний коефіцієнт тривалості встановлення з'єднання:

$$t_c = \frac{Tc_{min}}{T_c} \tag{2.6}$$

Відносний коефіцієнт чутливості до перемішування пакетів:

$$p_m = \frac{Pm_{min}}{P_m} \tag{2.7}$$

Відносний коефіцієнт пріоритетності користувача:

$$c_p = \frac{C_p}{Cp_{max}} \tag{2.8}$$

Таблиця 2.5

Вимоги до QoS окремих додатків

| Тип потоку | Параметри QoS | | | | | | |
|---|---|---|---|---|---|---|---|
| | P, % | T, мс | J, мс | C, кбіт/с | Tc, мс | Pm | Cp |

Продовження таблиці 2.5

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Голосові дані (VoIP, Skype) | <0,25 | 150 | 10 | 64 | 900 | $10^{-2}$ | 2–256 |
| Відеоконференція (Skype) | <2 | 100 | 20 | 2048 | 800 | $10^{-2}$ | 256–512 |
| IPTV | <1 | 100 | 50 | 4096 | 1000 | $10^{-2}$ | 512–768 |
| Інтернет дані (HTTP, Online services) | <0,1 | 100 | 100 | 2048 | 1000 | $10^{-6}$ | 1280–1536 |
| Інтерактивні дані (FTP, Cloud) | <1 | 400 | 500 | 256–10000 | 950 | $10^{-4}$ | 768–1024 |
| Медіа за запитом (Youtube) | <0,1 | 400 | 30 | 2048 | 700 | $10^{-4}$ | 1024–1280 |
| P – втрати пакетів;<br>T – затримка;00<br>J – джитер;<br>C – пропускна здатність;<br>Tc – тривалість встановлення з'єднання;<br>Pm – чутливість перемішування пакетів;<br>Cp – пріоритет клієнта | | | | | | | |

Результати розрахунків заносимо в табл.2.6.

Табл. 2.7 заповнюється числами 1, 2 та 3, які відображають відповідно низьку, середню та високу значимість вимог до показників QoS [23].

Таблиця 2.6

Формування матриці відносних коефіцієнтів

| Тип потоку | Параметри QoS | | | | | |
|---|---|---|---|---|---|---|
| | P | T, мс | J, мс | C, кбіт/с | Tc, мс | Pm |
| Голосові дані | 0,1 | 0,667 | 1 | 0,0063 | 0,556 | $10^{-5}$ |
| Відеоконференція | 0,0125 | 1 | 0,5 | 0,2 | 0,625 | $10^{-5}$ |
| IPTV | 0,067 | 0,1 | 0,2 | 0,4 | 0,5 | $10^{-2}$ |
| Інтернет дані | 0,1 | 0,1 | 0,01 | 0,2 | 0,5 | $10^{-2}$ |
| Інтерактивні дані | 0,1 | 0,25 | 0,02 | 0,025 | 0,526 | $10^{-5}$ |

Продовження таблиці 2.6

| | | | | | | |
|---|---|---|---|---|---|---|
| Медіа за запитом | 0,2 | 0,2 | 0,333 | 1 | 0,714 | $10^{-5}$ |
| Сигналізація | 1 | 1 | 0,01 | 0,0063 | 1 | 1 |

Таблиця 2.7

Формування матриці значимості показників QoS

| Тип потоку | Параметри QoS | | | | | |
|---|---|---|---|---|---|---|
| | P | T, мс | J, мс | C, кбіт/с | Tc, мс | Pm |
| Голосові дані | 2 | 3 | 3 | 1 | 3 | 3 |
| Відеоконференція | 2 | 3 | 3 | 2 | 3 | 3 |
| IPTV | 3 | 2 | 2 | 3 | 3 | 3 |
| Інтернет-дані | 3 | 1 | 1 | 1 | 1 | 2 |
| Інтерактивні дані | 2 | 2 | 1 | 1 | 3 | 2 |
| Медіа за запитом | 2 | 2 | 2 | 3 | 3 | 2 |
| Сигналізація | 3 | 2 | 1 | 1 | 3 | 3 |

Ці параметри може визначати оператор. Більш того, кожному клієнту визначено пріоритет для кожного типу трафіку. Якщо пріоритет не заданий явно в договорі щодо надання сервісу, тоді за замовчуванням клієнтові присвоюють найнижчий пріоритет з усіх можливих.

Відповідно, відносний пріоритет для кожної категорії послуг визначається за формулою (2.9):

$$Pr_i = \frac{\sum_{j=1}^{4} X_{ij} Y_{ij}}{\sum_{i=1}^{7} \sum_{j=1}^{4} X_{ij} Y_{ij}} \qquad (2.9)$$

де Pr – відносний пріоритет і-ої послуги; i – номер типу послуги;

j – номер параметра якості обслуговування;

$X_{ij}$ – відносний пріоритет параметру j для послуги i; $Y_{ij}$ – важливість параметр у j для послуги i.

Кінцевим результатом наведеної формули є дробове число, діапазон значень якого лежить в межах від нуля до одиниці. Чим більше значення, тим вищий пріоритет потоку. Формулу можна застосовувати для будь-якої кількості інформаційних потоків та різних вимог щодо якості обслуговування.

З урахуванням наведеної методики розрахунку відносного пріоритету потоків у роботі запропоновано спосіб підвищення ефективності використання ресурсів таблиці потоків, розмір якої обмежується апаратною реалізацією комутатора. Апаратні комутатори можуть використовувати як апаратну, так і програмну таблиці потоків. Перша характеризується високою продуктивністю та стабільністю, проте має дуже обмежений розмір порівняно з програмною. Зазвичай розмір апаратної таблиці потоків для апаратних комутаторів рівня доступу та агрегації становить від 300 до 3000 потоків. При цьому ресурс таблиці може змінюватися залежно від типів правил, які використовуються. Якщо ж таблиця потоків переповнена, тоді не можливо встановити нове правило, а потік отримує відмову в обслуговуванні.

Зважаючи на зазначене, у роботі запропоновано розділити потоки мультисервісної мережі на три категорії табл.2.8.

Таблиця 2.8

Класифікація типів трафіку мультисервісної мережі

| Тип трафіку | Додатки | Вимоги | Протоколи транспортного рівня |
|---|---|---|---|
| Реального часу | IP-телефонія та відео конференц-зв’язок | чутливість до затримок<br>чутливість до джитеру<br>затримки<br>- мала чутливість до втрат | RTCP, RSVP, UDP, RTP |
| | Процеси управління<br>Ігри on-line | чутливість до затримок<br>чутливість до джитеру<br>затримки<br>- чутливість до втрат | UDP, TCP |
| Потоковий | Аудіо на вимогу<br>Відео на вимогу<br>Інтернет-мовлення | мала чутливість до затримок<br>чутливість до джитеру<br>- чутливість до втрат | RSVP, UDP, TCP, SCTP |

Продовження таблиці 2.8

| | | | |
|---|---|---|---|
| Еластичний | Конференція<br>документів | мала чутливість до затримок<br>мала чутливість до джитеру затримок | TCP |
| | Анімація<br>Передача файлі в E-mail | дуже мала чутливість до затримок<br>мала чутливість до джитеру затримок<br>- висока чутливість до втрат | |

Без сумніву, що у великих мережах з обмеженим розміром таблиці потоків може використовуватися такий самий підхід, як і в IP мережах, де маршрутизація відбувається на основі IP адреси мережі призначення.

Для цього всі інші поля в правилах таблиці потоків повинні мати значення «*». Приклад таблиці потоків та принцип співставлення ідентифікаторів поток у з правилами в таблиці відображено на рис. 2.8.

У роботі пропонуємо поєднати дві схеми обробки пакетів, взявши переваги традиційної таблиці маршрутизації та таблиці потоків в OpenFlow, на основі чого розробити свій спосіб формування таблиці потоків у програмно - керованих мережах [24].

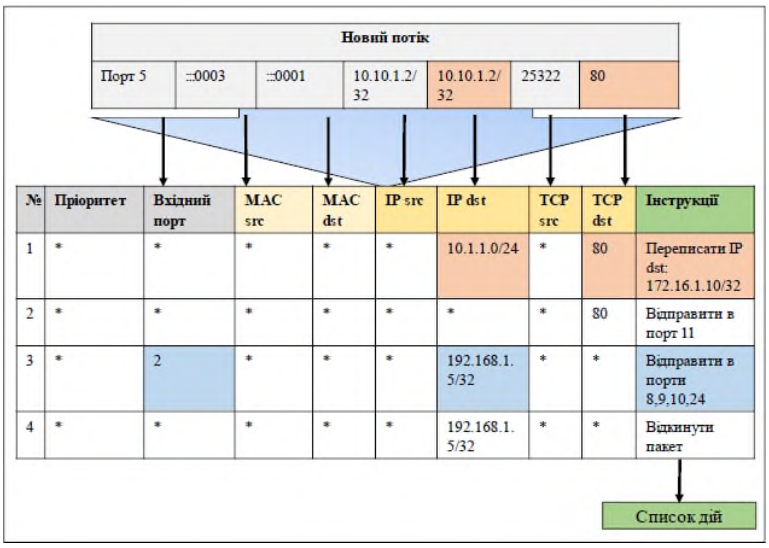



Рис. 2.8 Таблиця потоків у програмно-керованих мережах

Для потоків третьої категорії використовуються правила, які ідентифікують пакет за принципом класичної таблиці маршрутизації, а саме: за адресою мережі

призначення та класом трафіку. Для потоків другої та третьої категорії створюються окремі правила для кожного окремого потоку. Як наслідок, балансування навантаження потоків даних може здійснюватися досить гнучко в довільно визначених пропорціях, при чому досить швидко. У той самий час перерозподіл потоків реального часу є більш тривалим та потребує більше уваги до параметрів якості обслуговування цих потоків.

Кожній сформованій категорії відповідає певна політика керування, згідно якої з потоками конкретної категорії дозволено чи заборонено виконувати певні операції, а також зазначено умови, за яких ці дії можуть бути виконані. Наприклад, у випадку виникнення перевантаження певного шляху в певному комутаторі необхідно здійснити перерозподіл потоків.

Враховуючи те, що потоки першої категорії є чутливими до неправильного порядку пакетів та джиттеру, перенаправлення цих потоків може погіршити якість їхнього обслуговування. Тому розвантаження шляху починається з перерозподілу потоків третьої категорії.

У випадку, коли мережа функціонує в нормальному режимі, без перевантаження чи вузьких місць, система моніторингу опитує мережеві пристрої зі стабільно великим інтервалом часу. Зокрема, система моніторингу опитує завантаження мережевих інтерфейсів, завантаження таблиці потоків комутатора та завантаження центрального вхідного буферу маршрутизатора, на якому ідентифіковано перевантаження інтерфейсів.

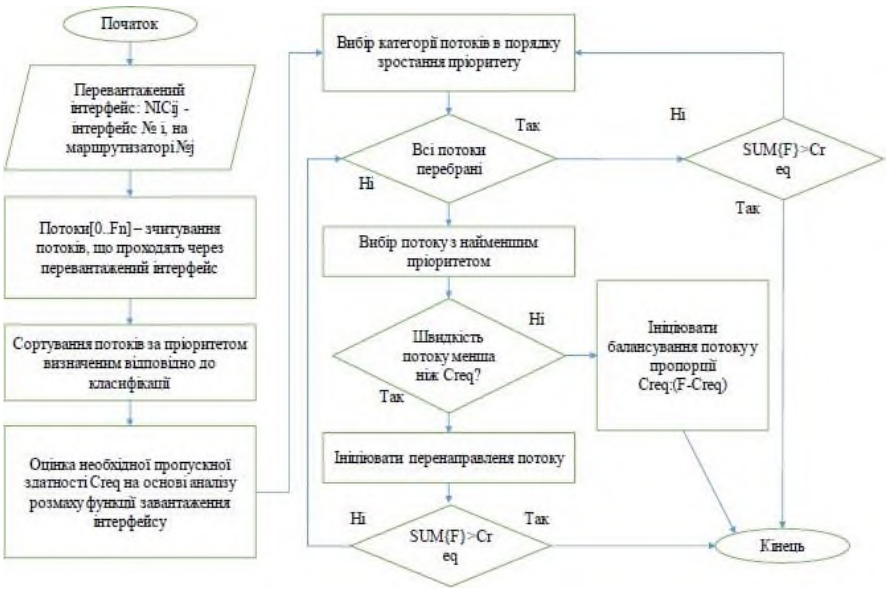



Рис.2.9 Алгоритм перерозподілу потоків у мережі для уникнення перевантаження інтерфейсу

Система моніторингу опитує вузли з певним інтервалом часу та здійснює моніторинг часових параметрів передачі потоків першої категорії. У випадку середньостатистичного зростання завантаження інтерфейсу, затримки передачі та джиттеру система переходить у стан пильного моніторингу зазначеного інтерфейсу та підвищує інтенсивність вимірювання затримки. Крім того, коли рівень завантаження інтерфейсу сягає 0,9, система починає опитувати завантаження буферів пристрою. У тому разі, коли середньостатистичне завантаження буферів потоку реального часу більше від 1, запускається алгоритм розвантаження інтерфейсу, описаний вище.

## 2.4 Модель балансування навантаження на основі критерію максимально допустимого завантаження каналу

Зазвичай використання фізичних каналів протягом дня становить від 30% до 40% від загальної пропускної здатності. Проте існують періоди, коли навантаження зростає і починає стрибкоподібно коливатися в значних межах, що дуже часто призводить до втрати пакетів та погіршення якості обслуговування користувачів.

Оптимальний розподіл трафіку та завантаження каналів здійснюється на

основі методів динамічного балансування навантаження [13,14], які застосовуються під безпосереднім керівництвом контролера. Це означає, що контролер постійно здійснює моніторинг стану каналів та комутаторів та у випадку необхідності відсилає інструкції на комутатор щодо зміни таблиць та процесів обробки потоків.

Ідея методу полягає в розподіленні навантаження одного потоку між декількома незавантаженими каналами, які є елементами шляху, що веде до вузла призначення. Оскільки в груповій таблиці існує множина записів, що відображають різні маршрути передачі даних одного потоку, то можна легко здійснювати управління навантаженням, беручи за основу вагові коефіцієнти кожної гілки. Ваговим коефіцієнтом гілки є числове значення пріоритету відповідної гілки, що вказує на відсоткове співвідношення кількості пакетів потоку, які необхідно передати по даній гілці. Тому в роботі запропоновано вибрати як критерій балансування пакетів потоку в площині передачі даних не відносний пріоритет шляху, а максимально допустиме завантаження наступного каналу, через який проходить шлях. Відповідно до такого критерію, комутатор направляє всі пакети потоку в один канал, якщо завантаження каналу менше, ніж максимально допустиме завантаження. Наприклад, якщо в певний момент часу, сумарна кількість байт, переданих в канал за одну секунду, перевищує 90% пропускної здатності, тоді для передачі наступного пакету вибирається наступний можливий шлях. Перебір шляхів відбувається до тих пір, поки не буде знайдено шляху, доступного для передачі цього пакету. Якщо шлях не знайдено, тобто всі канали перевантажені, тоді пакет відкидається. Контролер постійно здійснює моніторинг завантаження інтерфейсів і, коли він виявляє, що ймовірність блокування певного інтерфейсу наближається до одиниці, тоді розраховує набір можливих шляхів для перерозподілу потоків третьої категорії. Тут же ж він визначає кількість необхідних гілок.

Групова таблиця не підтримує динамічну зміну пріоритетів гілок. Більш того, така зміна не може здійснюватися в дрібному масштабі часу (менше однієї секунди). Навіть, якщо така зміна була б можливою, це б сильно впливало на продуктивність таблиці внаслідок постійної її модифікації та завантаження центрального процесора. Тому в наступному розділі роботи дослідження цього методу проводиться на основі

імітаційного моделювання. Відповідно до запропонованого методу, групова таблиця повинна оперувати обсягом переданих кожним шляхом байт та перенаправляти пакети на основі описаного вище механізму.

Розподіл смуги пропускання мережевих каналів між існуючими потоками з урахуванням прогнозів зміни швидкості кожного потоку дозволяє ефективно використовувати ресурси мережі. Динамічна зміна смуги пропускання дасть можливість завжди забезпечувати ефективність використання ресурсів каналу на високому рівні без втручання контролера. Цей метод особливо важливий у разі виникнення ситуації перевантаження всіх каналів, оскільки дає змогу комутатору локально обрати вільний шлях для передачі пакету, що знижує ймовірність втрати пакетів.

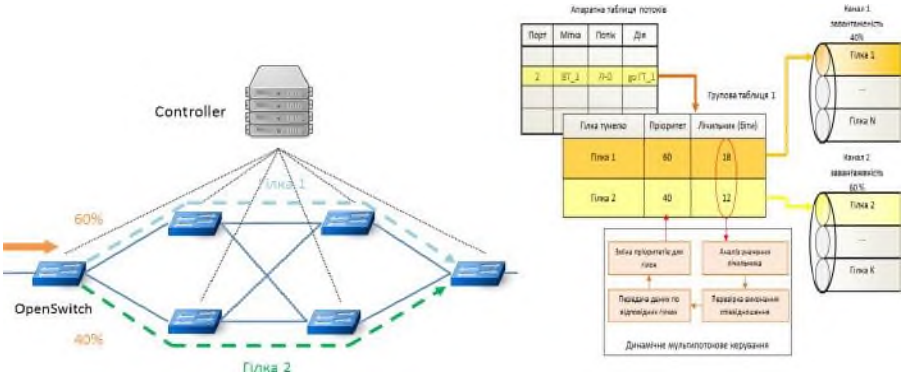



Рис. 2.10 Принцип балансування трафіку між гілками одного віртуального тун

# 3 ЕКСПЕРЕМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ПІДВИЩЕННЯ ПОКАЗНИКІВ ЯКОСТІ ТА ЕФЕКТИВНОГО РОЗПОДІЛУ МЕРЕЖЕВИХ РЕСУРСІВ ІЗ ЗАСТОСУВАННЯМ ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖ

## 3.1 Розробка тестового середовища мережі

Для побудови мережі тестового середовища використано 6 комутаторів модел і HP 3500yl-24G J8692A та 1 комутатор HPE FF 5700-32XGT-8XG-2QSFP+ Всі елементи тестового середовища зведено в табл.3.1.

Таблиця 3.1

Елементи тестового середовища

| Параметр | Конфігурація |
|---|---|
| Пропускна здатність ребра | 1 Гбіт/с |
| Кількість портів комутатора | 24 |
| Кількість серверів | 12 |
| Кількість комутаторів | 7 |
| Кількість ребер | 10 |
| Контролер | HP SDN VAN 2.5 |

Всі з’єднання між комутаторами та комутаторами і серверами мають швидкість 1 Гбіт/с. Схему тестового середовища представлено на рис.3.1.

В основі тестового середовища лежить мережева топологія типу зірки, сформована з 6-ти комутаторі в *HP3500yl*, які розташовані по краях топології. У центрі розташовано комутатор *HP5700*. До крайових комутаторів підключено по два сервери, кожен з яких має такі характеристики:

- центральний процесор: Intel® Xeon® E5-2600 v4 product family;
- кількість процесорів: 1;
- кількість ядер: 16;
- form factor (fully configured): 1U;
- оперативна пам’ять: 128GB;

- кількість слотів оперативної пам’яті: 8 DIMM slots;
- тип оперативної пам’яті: DDR4 SmartMemory;
- опис жорсткого диску: SFF SAS/SATA/SSD;
- мережевий адаптер: 1Gb 361i Ethernet Adapter 0.

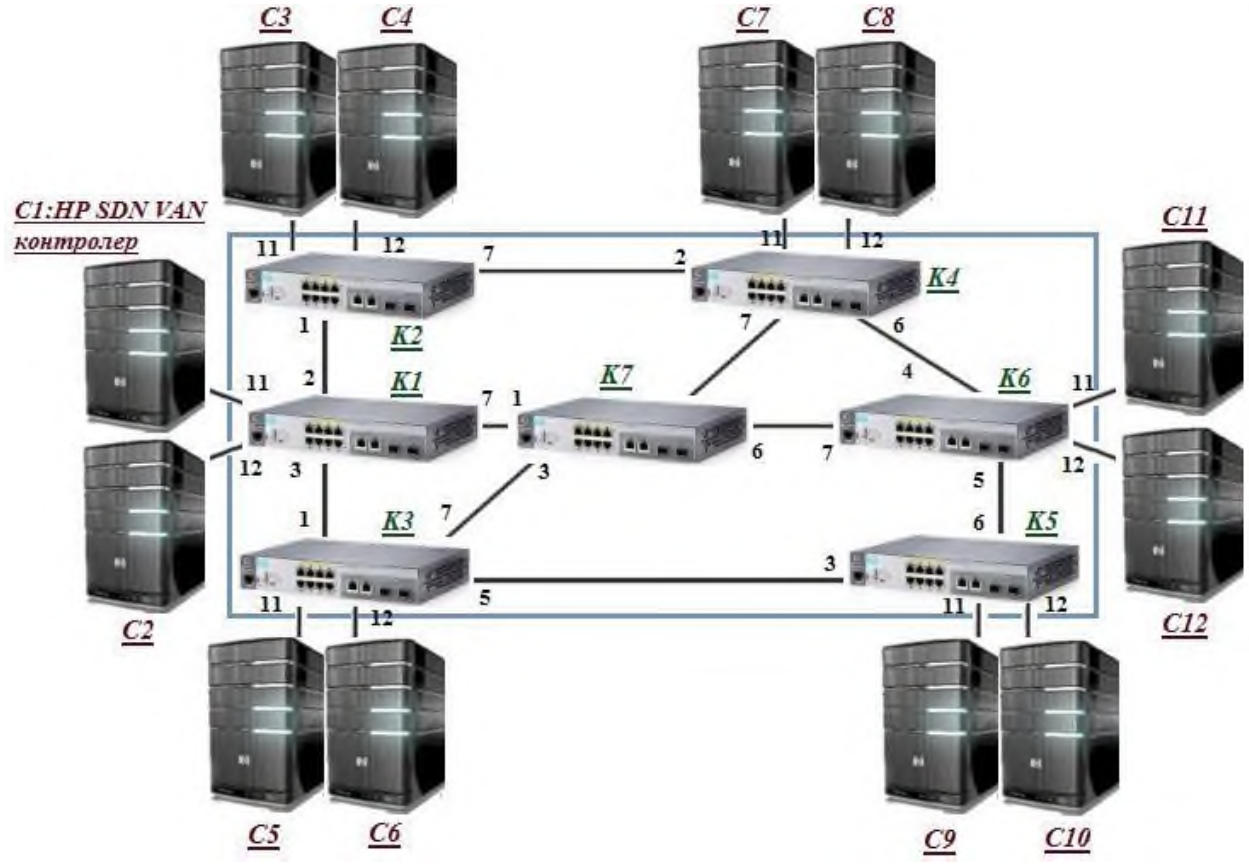



Рис. 3.1 Схема тестового середовища для оцінки ефективності методів підвищення якості обслуговування на основі реальних апаратних пристроїв

Комутатори *HP3500yl* забезпечують високу продуктивність та простоту використання на межі корпоративних мереж. Вони характеризуються низькою затримкою та оптимізованими механізмами буферизації. Стандартна конфігурація комутатора може складатися з 24 або 48 портів, кожен з яких підтримує максимальну пропускну здатність 1 Гбіт/с. Крім того, комутатор має можливість розширення конфігурації за рахунок двох додаткових портів по 10 Гбіт/с кожен. Ці порти можуть використовуватися для агрегації трафіку. Мережевий рівень представлено такою функціональністю: IPv4 BGP, політика маршрутизації, IPv4/IPv6 OSPF, управління якістю обслуговування. Комутатор підтримує функціональність

OpenFlow версії 1.0 та 1.3. Комутатор *HP3500yl* є гібридним, тобто може паралельно працювати в обох режимах: традиційному з використанням децентралізованих протоколів управління та OpenFlow. Для використання порту в режимі OpenFlow його необхідно зробити членом віртуальної локальної мережі, яка контролюється одним з локальних екземплярів OpenFlow. Зведену інформацію про комутатори представлено в табл.3.2.

Таблиця 3.2

Характеристика комутаторів, побудови тестового середовища

| Модель комутатора | Версія операційної системи | Пропускна здатність, мегапакетів/с | Пропускна здатність комутаційної матриці, Гбіт/с | Затримка комутації, мкс |
|---|---|---|---|---|
| HP 3500yl-24G (J8692A) | K.15.17.0007 | 75,7 | 101,8 Gbps | 3,4 |
| HPE FF 5700-32XGT-8XG-2QSFP+ (JG898A) | 2422P01 | 714,2 | 960,0 Gbps | 1,5 |

Комутатор HP FlexFabric 5700 Switch Series призначений для використання в корпоративних мережах та дата центрах. Він забезпечує високу масштабованість за рахунок функцій локальної комутації, що реалізована засобами додаткової апаратної таблиці з високою місткістю та продуктивністю. Комутатор підтримує порти 1, 10 т а 40 Гбіт/с. Комутаційна фабрика забезпечує пропускну здатність 960 Гбіт/с, а відповідно й дуже низьку затримку (1,5 мкс).

Для управління мережею використано контролер HP SDN VAN версії 2.5.2. Його встановлено на сервері №2. На цьому ж сервері встановлено систему моніторингу, розроблену в роботі, а також систему генерації мультисервісного трафіку. Остання використовувала всі інші сервери для генерації трафіку.

## 3.2 Експерементальне дослідження ефективності застосування моделі балансування навантаження мультипотокового керування трафіком

У роботі досліджено модель балансування навантаження, яка за критерій перенаправлення пакетів використовує не відносний пріоритет шляху, а максимально допустиме завантаження наступного каналу. Відповідно до такого критерію комутатор направляє всі пакети потоку в один канал, якщо його завантаження не перевищує максимально допустиме. У випадку, коли сумарна кількість біт, переданих в канал за одну секунду, перевищує 90% пропускної здатності, для передавання наступного пакету вибирається інший доступний шлях. Якщо доступного шляху не знайдено, то пакет відкидається [26].

Для аналізу ефективності роботи розглянутого методу балансування навантаження мультипотокового керування трафіком проведено експеримент , схем у якого відображено на рис.3.2.

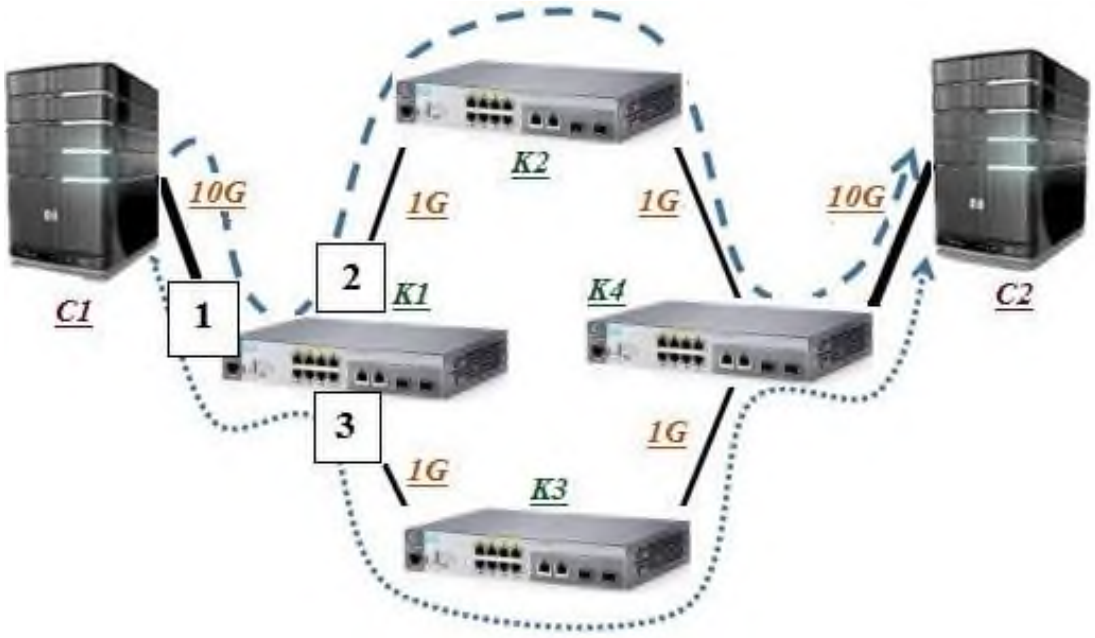



Рис. 3.2 Конфігурація тестового середовища

Для експерименту згенеровано навантаження, яке використовувалося для оцінювання ефективності адаптивної моделі моніторингу (рис. 3.3).

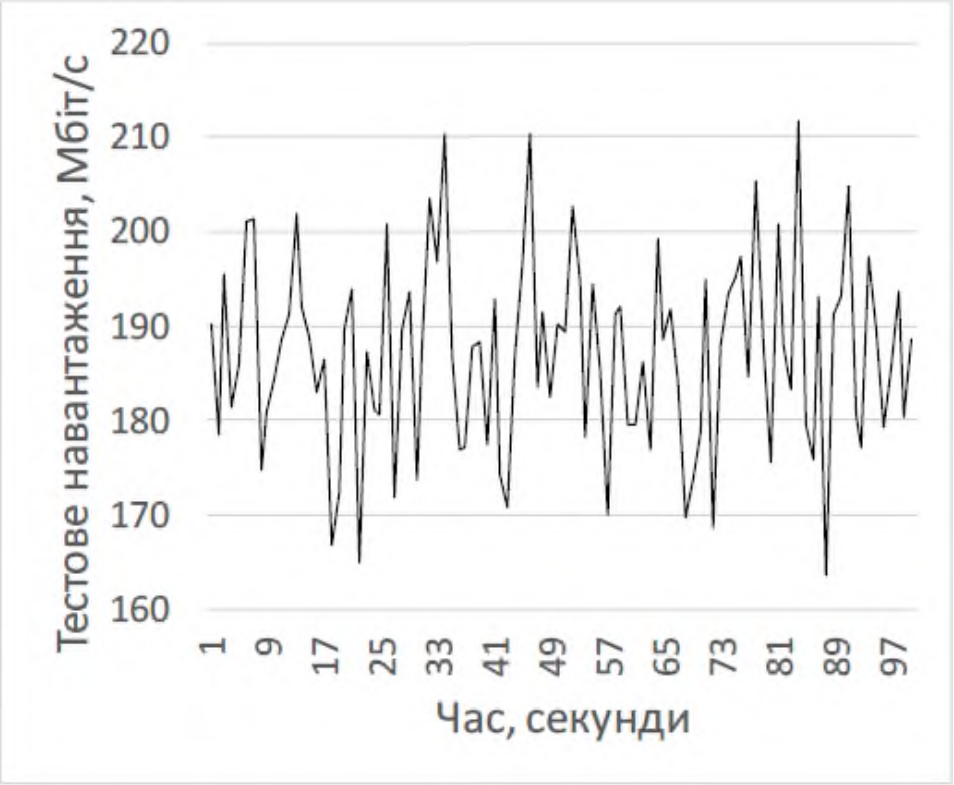



Рис. 3.3 Згенерований мультисервісний агрегований потік на інтерфейс №1 комутатора К1

На першому етапі досліджувався параметр втрати пакетів без балансування навантаження. Для цього на перший інтерфейс комутатора К1 згенеровано мультисервісне навантаження з використанням розробленої системи генерації мультисервісного трафіку, інтенсивність якого відображено на рис.3.3. У зв'язку з тим, що інтенсивність навантаження є більшою від 1 Гбіт/с і не може бути передана до сервера С2 одним каналом, контролер проклав два шляхи в мережі, а саме: С1 – К1-К2-К4 – С2 та С1 – К1-К3-К4 – С2. Маршрутизація реалізована з використанням протоколу EIGRP. Ураховуючи високу інтенсивність навантаження, контролер розділив агрегований трафік з інтерфейсу К1 на два потоки майже однакового розміру. У результаті, в процесі передавання даних проводився моніторинг завантаження всіх портів 1-го комутатора. Завантаження 2-го та 3-го інтерфейсів комутатора К1 відображено на рис. 3.4.

У ході експерименту спостерігаються втрати в каналі К1-К2-К4. В результаті експерименту втрати пакетів у каналі К1-К2-К4 становили 10%. Це означає, що, хоч протокол EIGRP і забезпечив балансування навантаження з пропорційним

розподілом трафіку між допустимими каналами, існуючий механізм балансування навантаження на основі групової таблиці потоків не дав змогу уникнути втрату моменти різких стрибків інтенсивності вхідного навантаження [27].

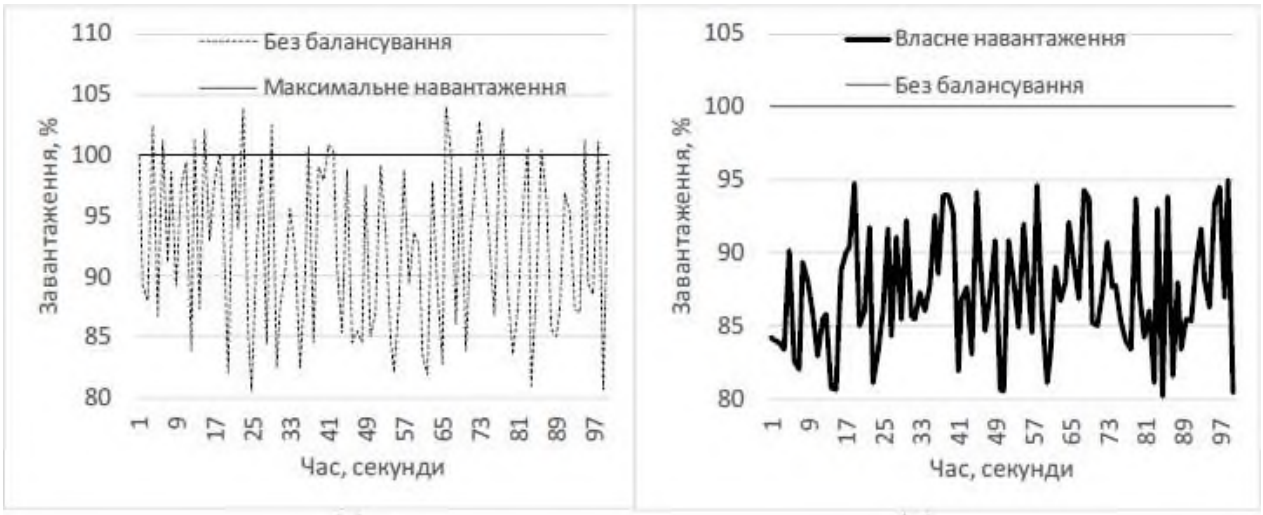



Рис.3.4 Завантаження каналів К1-К2-К4 (а) т а К1-К3-К4 (б) при маршрутизації та балансуванні навантаження на основі протоколу EIGRP

На другому етапі проведено дослідження удосконаленої моделі балансування навантаження. У цьому випадку максимально допустимий рівень завантаження каналу К1-К2-К4 становив 95% від його пропускної здатності. Для канал у К1-К3-К4 ніякого обмеження не встановлено. Для цього дослідження використовувалося навантаження, ідентичне до попереднього експерименту. Результати проведеного експерименту відображено на рис .3.5.

Після застосування запропонованої моделі балансування завантаження каналу К1-К2-К4 не перевищувало 95% без втрат пакетів. Весь надлишковий трафік перенаправлявся в канал К1-К3-К4, завантаження якого в середньому також не перевищувало 95%, проте в деякі моменти досягало 100%, у зв’язку з чим втрати в каналі К1-К3-К4 становили 1,5%. Це пояснюється тим, що трафік не міг бути переданим ні одним шляхом внаслідок перевантаження.

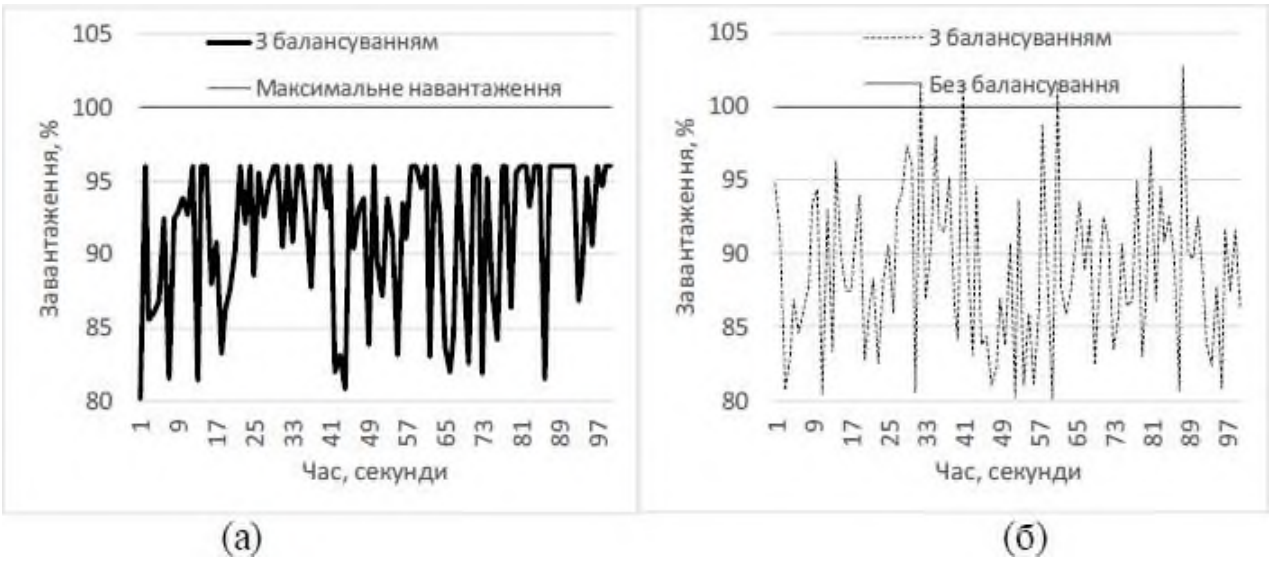



Рис. 3.5 Завантаження каналів К1-К2-К4 (а) та К1-К3-К4 (б) при маршрутизації на основі протоколу EIGRP з використанням удосконаленої моделі балансування навантаження

У результаті експерименту встановлено, що досліджувана модель балансування навантаження, за умов середнього завантаження каналів на рівні 90% та середньоквадратичного відхилення інтенсивності вхідного навантаження 9,981%, дає змогу знизити втрати в середньому в 6 разів [28].

## 3.3 Експериментальна оцінка точності вимірювання затримки передачі пакетів у SDN

Зазвичай двома основними засобами вимірювання затримки між двома вузлами, а також оцінювання тривалості передачі пакету по певному шляху є *Ping* та *Traceroute*. *Ping* дає змогу встановити доступність вузла призначення, а також надає статистичні дані про втрати пакетів та час обходу петлі пакетом. *Traceroute* показує всі вузли на шляху від вузла-відправника до вузла-отримувача, а також тривалість обходу петлі від вузла-ініціатора вимірювання до кожного вузла вздовж шляху. У випадку, коли стоїть задача оцінювання затримки в мережі, дуже важливо враховувати географічну відстань між двома вузлами, оскільки більша відстань

зумовлює довший час передачі. Як тільки проблемні вузли виявлено, використовується додаток *Ping* для більш детального дослідження затримки між двома вузлами. Для прикладу, *Traceroute* дає змогу виявити вузол, на якому саме починається проблемна ділянка. Приклад роботи додатку *Traceroute* представлено на рис. 3.6.

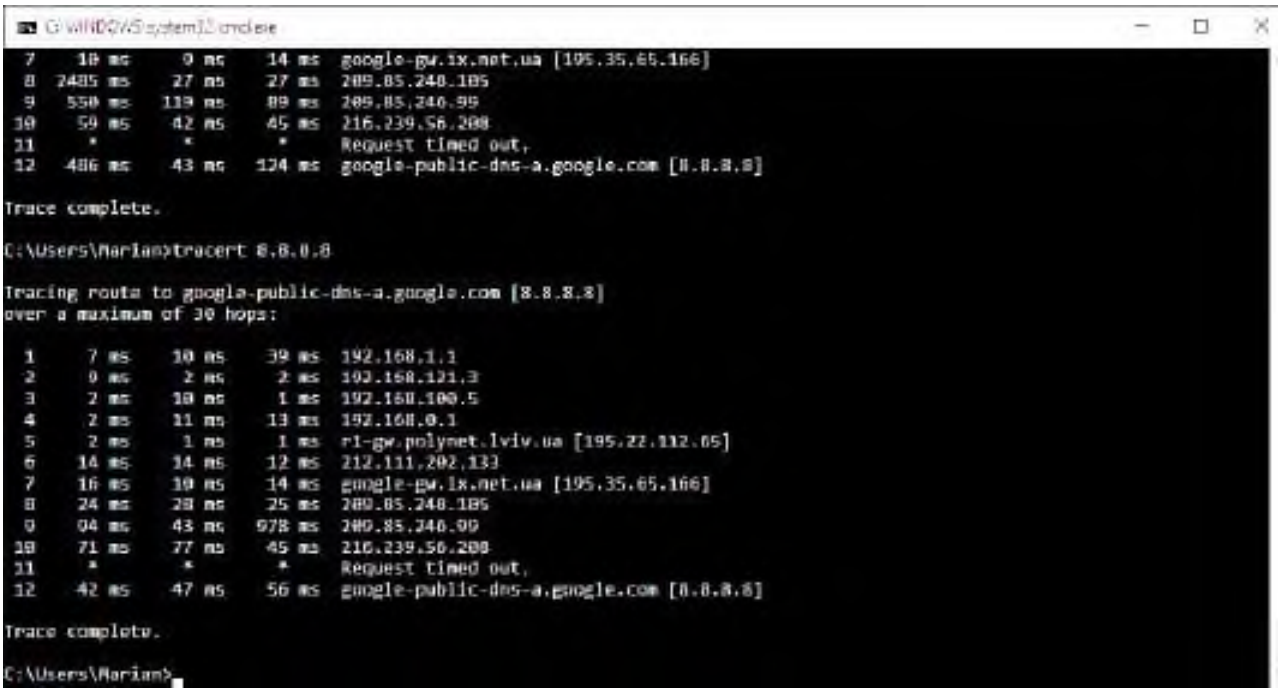



Рис. 3.6 Приклад роботи додатку *Traceroute* для вимірювання затримки та визначення перевантаженої ділянки мережі

Оцінювання затримки передачі пакету між двома комутаторами проводиться на основі розробленого в роботі алгоритму вимірювання затримки з кінця в кінець. Проте в цьому випадку суттєві похибки виміряного значення можуть виникати внаслідок великої кількості процесів, кожен з яких вносить свою затримку. Для точного оцінювання значення затримки між двома вузлами необхідно врахувати такі процеси:

- тривалість обробки комутатором пакету типу “PacketOut” відповідно до специфікації OpenFlow;
- тривалість передачі пакету контролером по мережевому стеку з моменту фіксації часу відправлення пакету;

- тривалість отримання пакету, його розпакування та аналіз вмісту при його отриманні з кінцевого комутатора;
- поточне завантаження комутатора та каналу;
- поточне завантаження центрального процесора комутатора.

Для оцінювання всіх випадкових впливів проведемо експеримент щодо оцінювання затримки передачі пакету. Схему передачі пакету відображено на рис. 3.7.Контролер використовує два типи повідомлень OpenFlow для зчитування пакетів з площини передачі даних та для введення пакетів у цю площину. При чому, обидва повідомлення характеризуються певними особливостями використання.

Повідомлення типу *PacketIn* використовується для упаковування пакетів даних та передачі їх від комутатора до контролера. Є дві причини, що можуть призвести до генерації цього повідомлення. Перша причина – це створення повідомлення на основі явної інструкції конкретного правила. А саме, комутатор передає на контролер всі пакети загорнуті у повідомлення *PacketIn*, що підпадають під правило, яке явно вказує, що наступним вузлом на шляху передавання пакету є контролер. Іншою причиною може бути відсутність правила для пакету в таблиці потоків або ж помилка *TTL*.

Повідомлення *PacketIn* складається з заголовку, після якого наводиться ідентифікатор пакету даних у буфері комутатора. Довжина пакету даних записана в полі *total_len*. Поле *in_port* містить ідентифікатор фізичного порту, через який отримано відповідний пакет. Поле причини описує, чому саме цей пакет було відправлено на контролер. Отже, частина самого пакету передається у цьому повідомленні як масив байт. Контролер також має можливість вводити пакети в площину передачі даних через будь-який комутатор у мережі. Ця процедура здійснюється за допомогою повідомлення типу *PacketOut*. Таке повідомлення може містити як сам пакет даних, так й ідентифікатор місця збереження пакету у вхідному буфері комутатора. Пакет аналізується центральним процесором, який проводить пошук можливих операцій із отриманим пакетом у списку всіх можливих операцій. Якщо знайдена операція вказує, що такий пакет потрібно обробити стандартною апаратною таблицею потоків, тоді поле *port_id*

використовується як вхідний порт пакету даних.

Структура повідомлення *PacketOut* дуже подібна до структури повідомлення *PacketIn*.

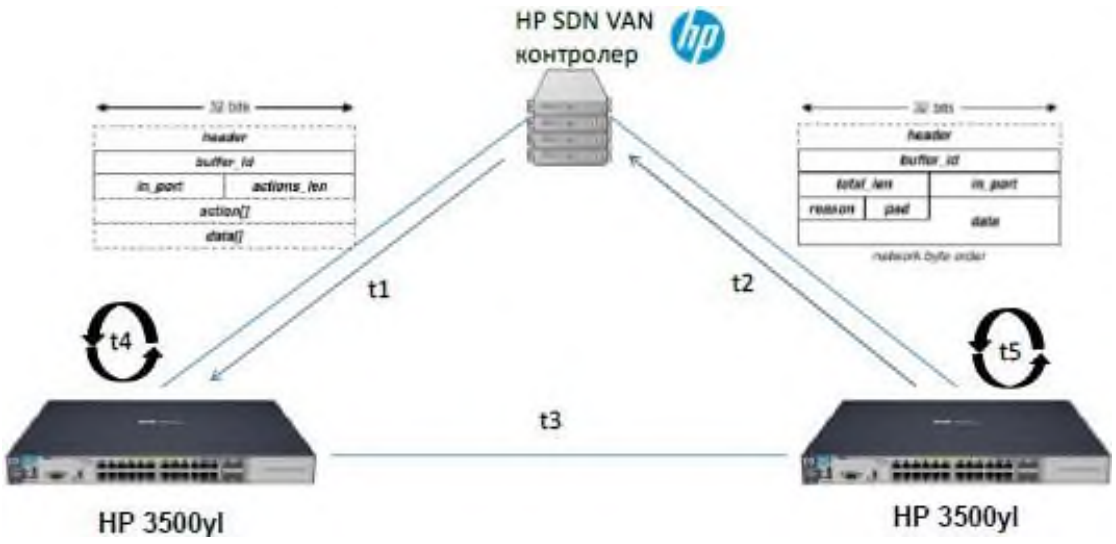



Рис. 3.7 Схема проведення експерименту для вимірювання затримки між двома комутаторами з використанням контролера

Вона також містить ідентифікатор місця збереження пакету у вхідному буфері комутатора. Якщо встановлено значення цього поля *0xffffffff*, це свідчить про те, що пакет зберігається у масиві даних *data*, який передається з цим повідомленням. Список дій, які можуть виконуватися над пакетом, передається у масиві *action*.

Для реалізації такого експерименту в першому комутаторі встановлюється правило, яке відповідає за обробку пакету, введеного контролером у площину даних, і передачу його до наступного комутатора. Наступний комутатор містить правило, відповідно до якого такий пакет видаляється з площини передачі даних, інкапсулюється у повідомлення *PacketOut* та відправляється до контролера.

Структура такого правила може бути довільною, а значення полів повинні бути такими, щоб не перекривалося жодне з уже існуючих правил в таблиці.

В експерименті вибрано правило з максимальною кількістю полів, а кожному полю задано максимально можливе значення. Н а першому комутаторі правило містить інструкцію «відправити пакет через вихідний порт», на другому комутатор

і – інструкцію «відправити пакет на контролер». У разі відсутності інтенсивності навантаження на комутатори, канал звантажений на 0-0,001% за рахунок протоколу *LLDP*, пакети якого пересилалися з інтервалом 2 секунди. Протягом експерименту було переслано 10000 тестових пакетів. Розподіл тривалості передачі пакетів відображено у формі гістограми на рис.3.8.

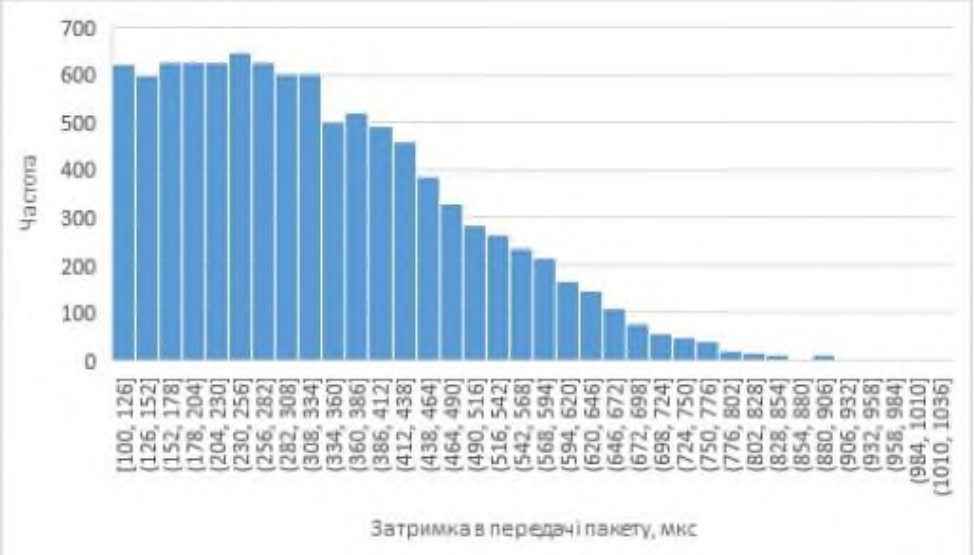



Рис. 3.8 Розподіл тривалості передачі пакету в розглянутому тестовому середовищі

Отримані результати показують, що середнє значення затримки становить 333 мкс, а стандартне відхилення рівне 159,7 мкс. Максимальне та мінімальне значення становлять 1012 та 100 мкс відповідно. Ураховуючи розподіл затримки пакетів залежно від завантаження інтерфейсу, можна стверджувати, що затримка суттєво зростає лише після проходження рівня завантаження інтерфейсу, що становить 800 Мбіт/с, а саме, збільшення завантаження інтерфейсу на 10 Мбіт/с призводить до збільшення затримки 100 мкс. Вже у разі завантаження каналу на рівні 850 Мбіт/с затримка передачі пакету перевищує 400 мкс. Відповідно до отриманих статистичних показників щодо результатів вимірювання на основі розробленого алгоритму можна зробити висновок, що вже на рівні завантаження каналу 850 Мбіт/с можна відфільтрувати затримку передачі пакету з отриманого масиву значень [29]. Отримані результати також використовуються для оцінки затримки всього шляху, оскільки на основі них враховано тривалість обробки OpenFlow

повідомлень та тривалість їх передачі по сигнальному каналу, а також тривалість обробки цих повідомлень комутатором.

Для порівняння ефективності розглянутого алгоритму вимірювання затримки та традиційного методу вимірювання на основі *Traceroute* було прокладено шлях у мережі між комутаторами 3 та 5.

Шляхи проходження тестових пакетів для *Traceroute* (штрихпунктирна крива) та розробленого методу (штрихова крива) відображено на рис.3.8.

Вимірювання проводилося для різних рівнів завантаження шляху. При чому, в каналах циркулював мультисервісний трафік, а основна задача полягала у вимірюванні тривалості передачі даних 1-го класу трафіку, а конкретніше – поток у *VoIP*. Завантаження шляху змінювалося від 10% до 100% з кроком 10. У кожній ітерації вимірювання проводилося 1000 разів окремо з використанням розробленого методу та додатку *Traceroute*.

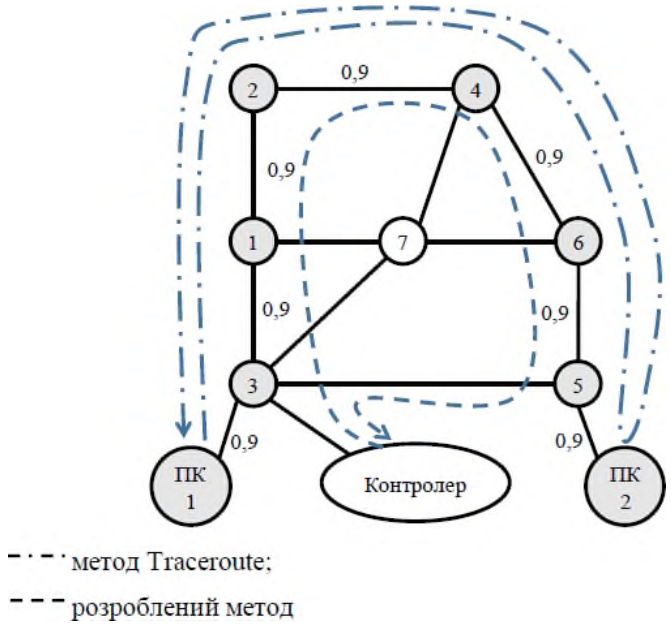



Рис. 3.9 Порівняльна схема вимірювання тривалості проходження пакету вибраним маршрутом в мережі

Порівняти результати моніторингу можна на основі діаграми, представленої на рис.3.10.

На основі розрахунку встановлено, що тривалість передавання пакету

розміром 1500 байт відповідним шляхом, що складається з 7 каналів зі швидкістю 1Гбіт/с та 6 комутаторів зі швидкістю комутації 4 мкс, становить 98 мкс. Аналізуючи отримані результати, можна стверджувати, що у випадку не завантаженого каналу (менше від 50%) затримка, виміряна стандартним методом та алгоритмом, запропонованим у роботі, є однаковою.

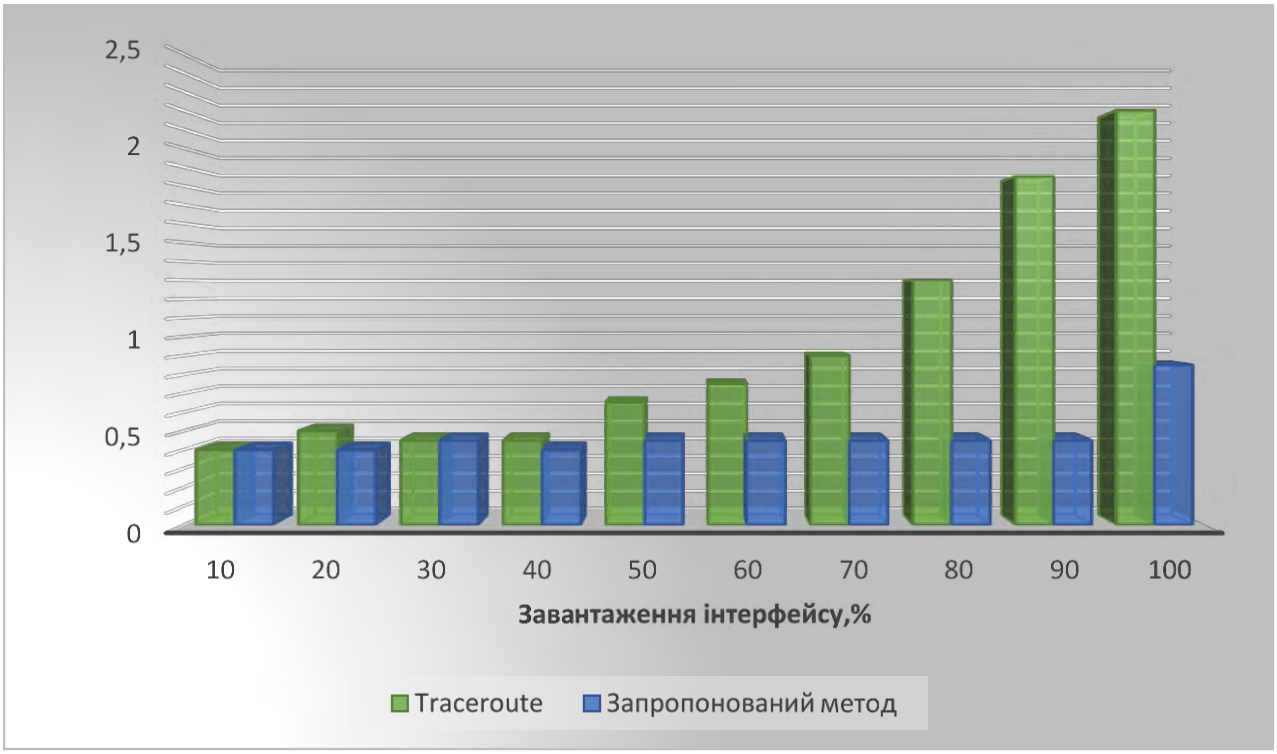



Рис. 3.10 Порівняння результатів оцінки затримки на основі *Traceroute* та розглянутого алгоритму

Коли інтенсивність завантаження перевищує 50%, затримка, виміряна стандартним методом, підвищується, що пов’язано з використання протоколу TCP для реалізації вимірювань. У разі збільшення завантаження шляху тривалість передавання пакетів, а також повернення підтверджень зростає внаслідок виникнення черг [30].

Підсумовуючи зазначене, можна стверджувати, що у випадку вимірювання затримки шляху в каналі з максимальним завантаженням запропонований алгоритм дає змогу підвищити точність вимірювання затримки у середньому в 2,5 рази. Це, у свою чергу, дає змогу точніше оцінити затримку шляху в реальних

умовах перевантаження мережі та провести оптимальний перерозподіл навантаження з врахуванням критеріїв якості обслуговування.

### 3.4 Параметри якості обслуговування потоків та ефективності розподілу навантаження

Для дослідження ефективності моделей маршрутизації використано розроблений метод вимірювання затримки для оцінювання затримки передавання пакетів між всіма парами вузлів у мережі тестового середовища. Результати вимірювань представлено на рис. 3.11.

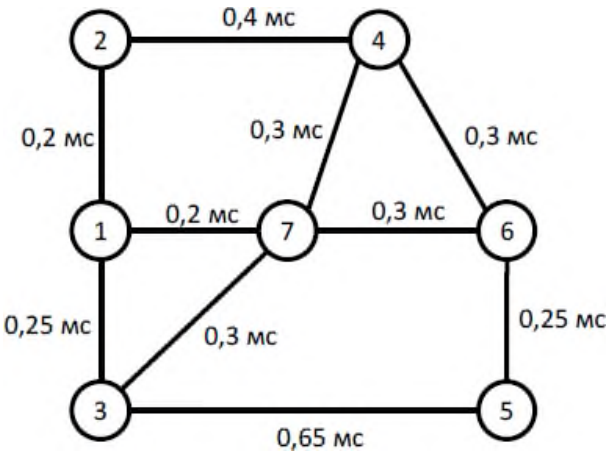



Рис. 3.11 Характеристика затримки в каналах побудованої тестової мережі

Число, що стоїть біля кожного ребра, відповідає затримці, яка враховує тривалість передачі пакету в цьому каналі, а також тривалість обробки пакету обома вузлами.

Пропускну здатність між усіма вузлами для всіх портів встановлено на рівні 100 Мбіт/с. Для проведення експерименту в мережі згенеровано фонове навантаження за допомогою системи генерації мультисервісного трафіку. Матрицю вимог щодо пропускної здатності між вузлами відображено в табл.3.3.

Вузол №7 є проміжним (представляє рівень агрегації), а тому до нього не під’єднано кінцеві пристрої (сервери).

Побудована мережа використовувалася студентами університету м. Вюрцбурга (Німеччина) для доступу до сервісів даних у локальному центрі обробки

даних, тому усереднені вимоги щодо пропускної здатності отримано в результаті моніторингу трафіку в цій мережі впродовж двох днів.

Таблиця 3.3

Вимоги щодо пропускної здатності між вузлами для створення фонового мультисервісного навантаження, Мбіт/с

| | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | ----- | 12,5 | 16,5 | 5 | 9 | 7 |
| 2 | 11 | ----- | 12,5 | 20 | 14 | 13 |
| 3 | 5 | 16,5 | ----- | 21 | 12,6 | 5 |
| 4 | 10 | 14,5 | 12 | ----- | 13 | 11 |
| 5 | 8 | 18 | 6 | 8 | ----- | 15 |
| 6 | 12 | 8 | 9 | 15 | 5 | ----- |

Відповідно до матриці вимог згенеровано список потоків для всіх типів трафіку. Для смуги пропускання 100 Мбіт/с згенеровано набір клієнтів та послуг, які вони використовують. Список потоків для 9-ти клієнтів, агрегована швидкість яких становить 100 Мбіт/с, відображено в табл.3.4. (*C* – пропускна здатність, Мбіт/с; *P* – пріоритет).

З табл. 3.4 видно, що для пропускної здатності 100 Мбіт/с згенеровано 9 клієнтів. Кожен клієнт користується певним набором послуг. У тому разі, коли клітинка на перетині стовпця та рядка є порожньою, цю послугу слід вважати такою, для якої відсутня будь-яке гарантування якості обслуговування у випадку, якщо клієнт нею скористується.

Всі інші послуги мають вимоги щодо пропускної здатності та параметрів обслуговування для конкретного клієнта, і, відповідно до його пріоритету, гарантуються сервісним договором між клієнтом та оператором мережі. Як видно з табл.3.4, кожному клієнту присвоєно пріоритет у відповідному діапазоні пріоритетів для конкретного типу сервісу. Такий метод генерації проведено для кожної пари серверів, що використовуються для генерації клієнтського навантаження [28].

Таблиця 3.4

Список клієнтських потоків, сумарна швидкість яких становить 100 Мбіт/с

| Послуга | | Клієнт | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| VoIP | C | 0,17 | 0,19 | 0,16 | 0,19 | 0,18 | 0,18 | - | - | - |
| | P | 5 | 10 | 15 | 20 | 25 | 30 | - | - | - |
| Skype | C | 1,25 | 1,01 | 1,17 | 1,25 | 1,17 | 1,27 | 1,11 | 1,09 | 1,44 |
| | P | 260 | 265 | 270 | 275 | 280 | 285 | 290 | 295 | 300 |
| IPTV | C | 1,91 | 2,09 | 2,13 | 2,21 | 2,15 | 2,17 | 1,95 | 2,33 | 2,42 |
| | P | 515 | 520 | 525 | 530 | 535 | 540 | 545 | 550 | 555 |
| Interactive | C | 1,59 | 1,60 | 1,54 | 1,80 | 1,68 | 1,53 | 1,90 | 1,46 | 1,81 |
| | P | 770 | 775 | 780 | 785 | 790 | 795 | 800 | 805 | 810 |
| VoD | C | 2,06 | 2,22 | 1,71 | 1,84 | 2,15 | 2,13 | 1,97 | 2,16 | 2,14 |
| | P | 1025 | 1030 | 1035 | 1040 | 1045 | 1050 | 1055 | 1060 | 1065 |
| Дані | C | 5,56 | 5,57 | 3,99 | 5,50 | 5,72 | 5,72 | 5,50 | - | - |
| | P | 1280 | 1285 | 1290 | 1295 | 1300 | 1305 | 1310 | - | - |
| Cloud | C | 9,96 | 9,90 | 9,48 | 10,63 | 10,06 | 10,49 | 8,30 | 12,98 | 9,82 |
| | P | 1540 | 1545 | 1550 | 1555 | 1560 | 1565 | 1570 | 1575 | 1580 |

Наступний крок полягав у розрахунку відносних пріоритетів потоків з урахуванням класифікації сервісів на категорії.

Таблиця 3.5

Відносні пріоритети потоків з урахуванням пріоритету клієнта та його вимог

| Номер клієнта | 1 | 2 | 3,00 | 4,00 | 5,00 | 6,00 | 7,00 | 8,00 | 9,00 |
|---|---|---|---|---|---|---|---|---|---|
| VoIP | 0,25 | 0,22 | 0,22 | 0,21 | 0,21 | 0,21 | ---- | ---- | ---- |
| Відео Skype | 0,188 | 0,187 | 0,186 | 0,185 | 0,184 | 0,183 | 0,182 | 0,181 | 0,18 |
| IPTV | 0,148 | 0,147 | 0,146 | 0,145 | 0,144 | 0,143 | 0,142 | 0,141 | 0,42 |
| Інтерактивні сервіси | 0,128 | 0,127 | 0,126 | 0,125 | 0,124 | 0,123 | 0,122 | 0,121 | 0,12 |
| VoD | 0,108 | 0,107 | 0,106 | 0,105 | 0,104 | 0,103 | 0,102 | 0,101 | 0,1 |
| Дані | 0,088 | 0,087 | 0,086 | 0,085 | 0,084 | 0,083 | 0,082 | ---- | ---- |
| Cloud | 0,048 | 0,047 | 0,046 | 0,045 | 0,044 | 0,043 | 0,042 | 0,041 | 0,04 |

Для першої категорії сервісів, яка визначає потоки реального часу, надзвичайно чутливі до флуктуації часових параметрі в якості обслуговування, належать: голосовий дзвінок, відеодзвінок, IPTV та потокове відео.

Результати розрахунку відносних пріоритетів для всіх клієнтів згідно методики, вдосконаленої у другому розділі роботи, відображено в табл.3.5.

Оцінювання маршрутизації з використанням протоколу EIGRP.

Зазвичай найпоширенішими протоколами маршрутизації в традиційних IP мережах на основі стану каналу є OSPF та IS-IS. Протокол OSPF (*Open Shortest Path First*) — це протокол динамічної маршрутизації, який належить до протоколів, що обирають маршрут на основі стану каналу (завантаження чи параметрів якості обслуговування). OSPF використовує алгоритм Дейкстри для знаходження найкоротшого шляху. IS-IS – протокол також використовує стан каналів для знаходження найкоротших шляхів на основі алгоритму Дейкстри. Протокол EIGRP (Enhanced Interior Gateway Routing Protocol) – один з найбільш поширених протоколів, що визначають маршрути на основі стану каналу, використовуючи алгоритм Diffused Update Algorithm (DUAL) для пошуку найкоротшого шляху на основі інтегральної метрики. Основними параметрами, які EIGRP використовує для обчислення метрики, є мінімальна пропускна здатність та затримка. Проте перевагою протоколу EIGRP є можливість балансування навантаження та знаходження маршруту на основі метрики, яка враховує параметри якості обслуговування і стан каналів. Тому в роботі для дослідження вибрано протокол EIGRP, який реалізований як програмний компонент контролера ПКМ [15].

Для тестування ефективності запропонованих рішень використано сервіс IPTV, що транслює відео з одинадцятого сервера. Мережу заповнено фоновим трафіком відповідно до вимог, наведених у табл.3.3, за допомогою системи генерації мульти сервісного трафіку, яка встановлена на кожному сервері, що під’єднаний до кожного комутатора. Отримано гістограму завантаження мережних каналів з використанням протоколу EIGRP, яку відображено на рис. 3.12.




Рис. 3.12 Гістограма завантаження мережних каналів унаслідок маршрутизації

У результаті роботи протоколу EIGRP мережа була заповнена фоновим трафіком. Всі шляхи для всіх вимог відображено в табл. 3.6.

Таблиця 3.6

Шляхи проходження фонового трафіку відповідно до протоколу EIGRP

| Потік | Шлях | Вимога, Мбіт/с | Потік | Шлях | Вимога, Мбіт/с |
|---|---|---|---|---|---|
| 1-2 | 1-2 | 12,5 | 4-1 | 4-7-1 | 10 |
| 1-3 | 1-3 | 16,5 | 4-2 | 4-2 | 14,5 |
| 1-4 | 1-7-4 | 5 | 4-3 | 4-7-3 | 12 |
| 1-5 | 1-7-6-5 | 9 | 4-5 | 4-6-5 | 13 |
| 1-6 | 1-7-6 | 7 | 4-6 | 4-6 | 11 |
| 2-1 | 2-1 | 11 | 5-1 | 5-3-1 | 8 |
| 2-3 | 2-1-3 | 12,5 | 5-2 | 5-6-4-2 | 18 |
| 2-4 | 2-4 | 20 | 5-3 | 5-3 | 6 |
| 2-5 | 2-4-6-5 | 14 | 5-4 | 5-6-4 | 8 |
| 2-6 | 2-1-7-6 | 13 | 5-6 | 5-6 | 15 |
| 3-1 | 3-1 | 5 | 6-1 | 6-7-1 | 12 |
| 3-2 | 3-1-2 | 16,5 | 6-2тиь | 6-4-2 | 12 |
| 3-4 | 3-7-4 | 21 | 6-3 | 6-7-3 | 9 |
| 3-5 | 3-5 | 12,6 | 6-4 | 6-4 | 15 |
| 3-6 | 3-7-6 | 5 | 6-5 | 6-5 | 5 |




Рис. 3.13 Завантаження каналів мережі після маршрутизації IPTV потоків за допомогою протоколу EIGRP

На наступному етапі було створено навантаження від сервісу IPTV, який встановлено на одинадцятому сервері. У результаті роботи EIGRP протоколу обрано маршрути для IPTV потоків, які подано в табл.3.7.

Таблиця 3.7

Маршрутизація IPTV потоків на основі EIGRP протоколу

| Пара вузлів | Вимога, Мбіт/с | Шлях | Частина навантаження, % |
|---|---|---|---|
| 6-1 | 23 | Немає вільної пропускної здатності | 100 |
| 6-2 | 18 | 6-4-2 | 100 |
| 6-3 | 32 | 6-7-3 | 100 |
| 6-4 | 21 | 6-4 | 100 |
| 6-5 | 14 | 6-5 | 100 |

Діаграму завантаження каналів мережі після запуску сервісу IPTV відображено на рис. 3.13.

У результаті маршрутизації за допомогою протоколу EIGRP у мережі виникло нерівномірне завантаження каналів. Особливу увагу слід звернути на канали 4-6, 3-7 та 6-7. Ці канали перебувають у стані, близькому до перевантаження з високою імовірністю блокування. Крім того, потік між вузлами 6 та 1 не зміг бути

прокладений у зв’язку з тим, що всі канали, які виходять від вузла 6, є перевантаженими. Для детального аналізу якості обслуговування потоків IPTV обрано канал 3-7 як найбільш близький до перевантаження. На основі аналізу мережевих потоків отримано схему основних потоків, що призводять до перевантаження каналу 3 - 7 рис. 3.14.

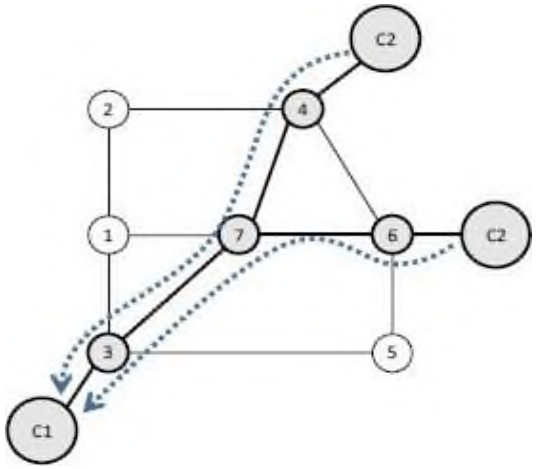



Рис. 3.14 Схема проходження основних потоків, що призводять до перевантаження каналу 3-7

Агреговану інтенсивність навантаження на канал 3-7 (комутатор №7, порт №3) відображено на рис. 3.15.

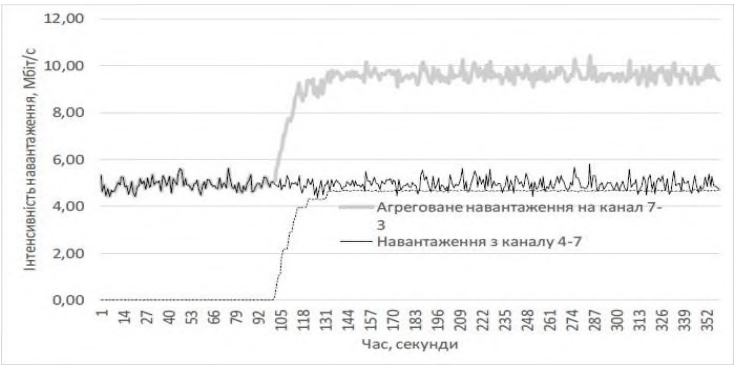



Рис. 3.15 Агрегована інтенсивність навантаження на канал 3- 7 з каналів 6-7 та 4-7

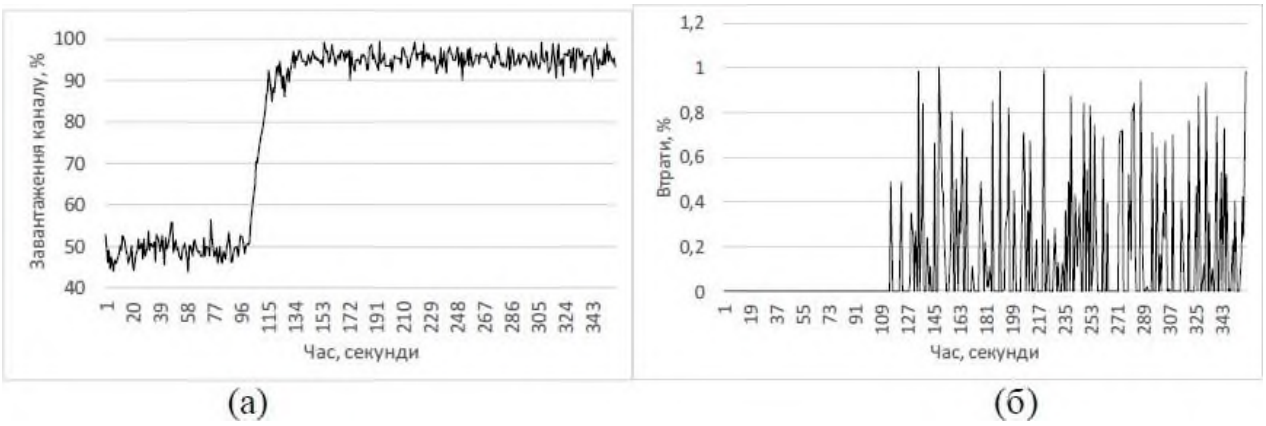



Рис. 3.16 Завантаження (а) каналу 7-3 та втрат(б) у ньому

У результаті використання алгоритму вимірювання затримки потоків побудовано графік середніх затримок всіх потоків, що проходять каналом 3-7. Виміряні затримки відображено на рис.3.17.

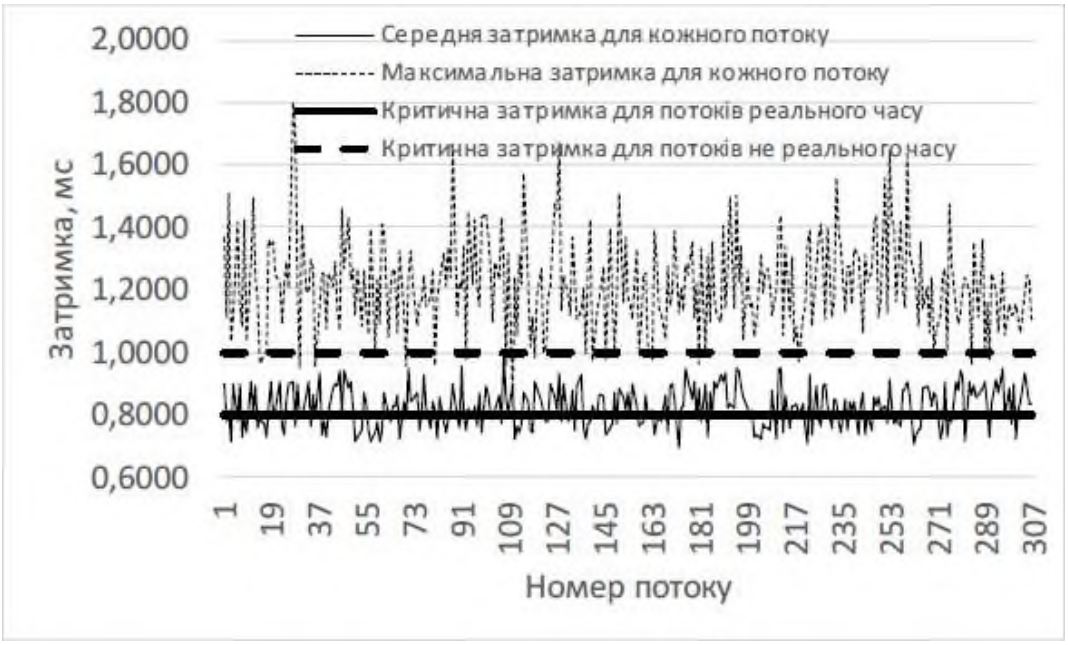



Рис. 3.17 Середні та максимальні значення затримок для всіх потоків, що проходять через канал 3-7

З отриманого графіка на рис. 3.17 можна стверджувати, що всі потоки, які проходять через канал 3-7, зазнають погіршення якості обслуговування. Зокрема, критичний рівень затримки для потоків реального часу становить 0,8 мс, а для

потоків класу нереального часу (друга категорія) – 1 мс. Для детальнішого аналізу затримок проведемо сортування потоків за значенням відносного пріоритет у( рис. 3.18 і рис.3.17).

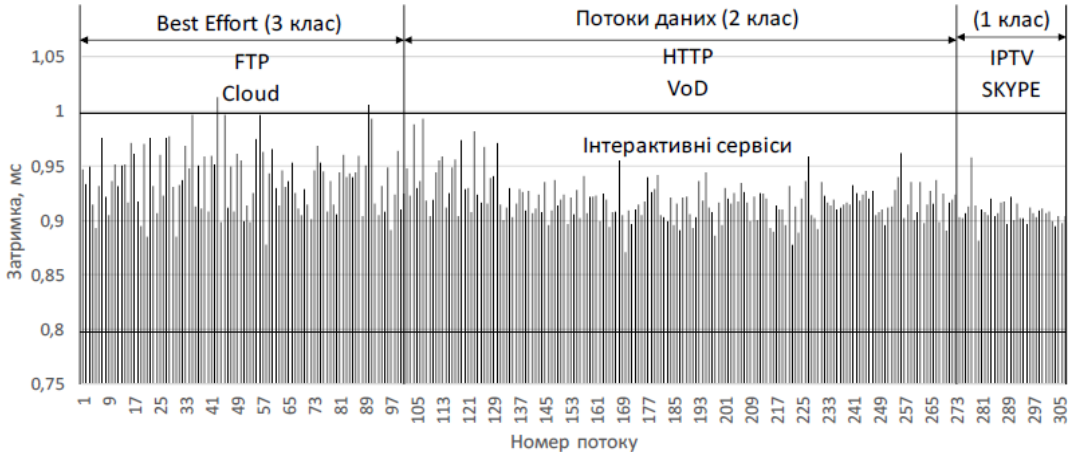



Рис. 3.18 Потоки, що проходять через канал 3-7, відсортовані за значенням відносного пріоритету

Діаграма, наведена на рис.3.19, демонструє те, що середня затримка всіх потоків реального часу (1-ий клас) перевищує критичне значення 0,8 мс.

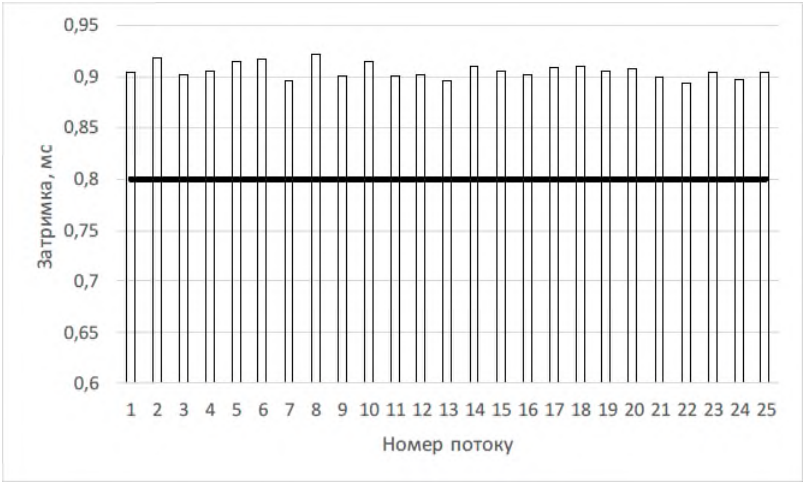



Рис. 3.19 Характеристика середньої затримки для потоків реального часу, що проходять через канал 3-7

Діаграма, відображена на рис.3.20, демонструє затримки для потоків даних, що належать до 2-го та 3-го класу.

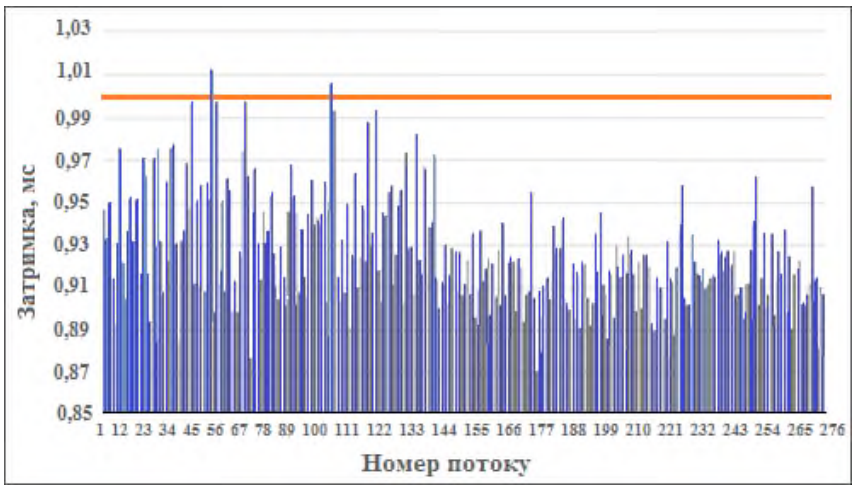



Рис. 3.20 Характеристика середньої затримки для потоків реального часу, що проходять через канал 3-7

Очевидним є те, що середня затримка для 99% потоків не перевищує критичного значення 1мс.

Для підвищення якості обслуговування потоків реального часу та уникнення перевантаження каналів 3-7, 4-7 та 6-7 на контролері увімкнено використання удосконаленої моделі маршрутизації.

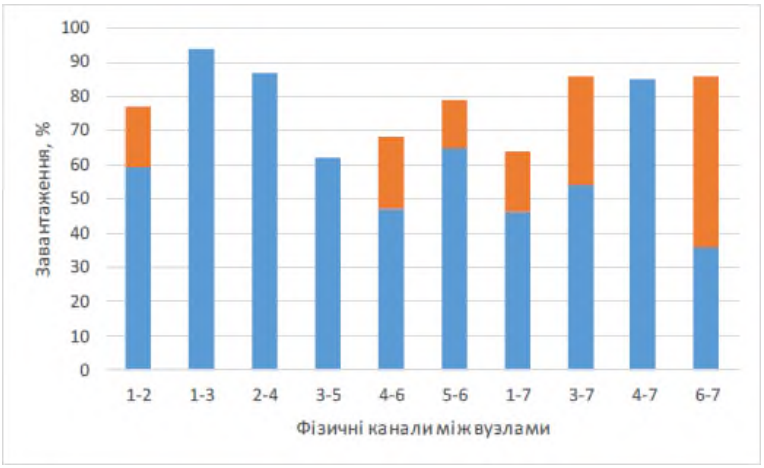



Рис. 3.21. Розподіл завантаження мережевих каналів після використання удосконаленої моделі маршрутизації

Алгоритм розвантаження каналу в кожній ітерації розраховує оптимальний маршрут для потоків з найменшим відносним пріоритетом, а в кожній наступній ітеграції потоки вибираються за зростанням їхнього пріоритету. Розподіл завантаження шляхів у мережі відображено на рис.3.21.

У результаті аналізу потоків встановлено, що основними потоками, за допомогою яких вдалося розвантажити мережу, є потоки, відображені схемою на рис.3.22.

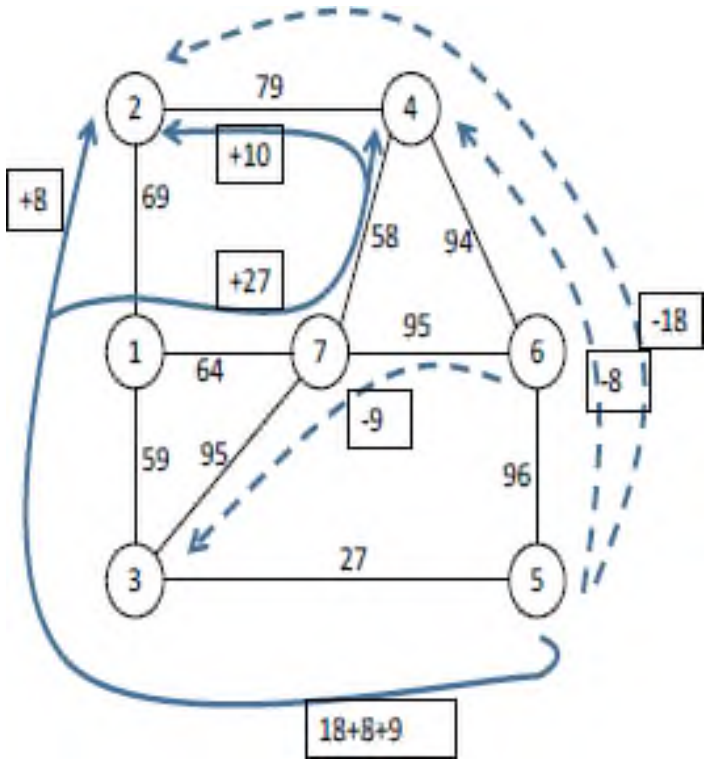



Рис. 3.22 Схема перерозподілу навантаження відповідно до результатів маршрутизації з використанням удосконаленої моделі

Порівняння середнього значення та стандартного відхилення для значень завантаження мережевих каналів показало, що на першому етапі ( з використанням лише протоколу EIGRP) середнє завантаження каналу становило 73%, а стандартне відхилення – 22,73%.

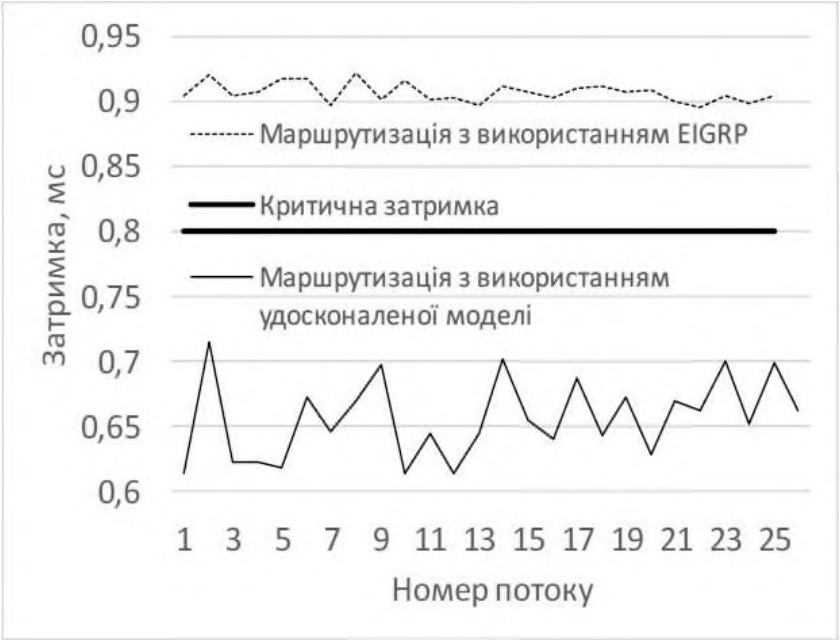



Рис. 3.23 Характеристика затримки потоків у мережі після перерозподілу потоків для рівномірного завантаження каналів

Після застосування удосконаленої моделі маршрутизації середнє завантаження каналів зросло до 79%, стандартне відхилення зменшилося до 10,86%, а коефіцієнт варіації знизився з 0,31 до 0,14.

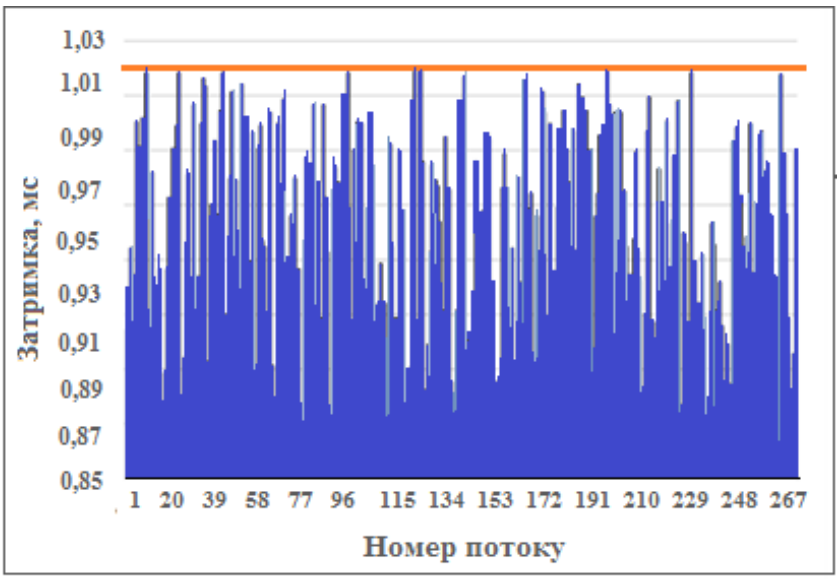



Рис. 3.24 Характеристика середньої затримки пакетів для потоків у каналі 1-3 після застосування удосконаленого методу маршрутизації

У процесі дослідження продемонстровано, що удосконалена модель маршрутизації дає змогу досягнути більш рівномірного розподілу навантаження в мережі порівняно з протоколом EIGRP та забезпечити необхідну якість обслуговування для всіх потоків.

У результаті проведення описаних вище експериментів доведено, що комплексне застосування запропонованих у роботі наукових рішень дало змогу покращити затримку для потоків реального часу на 15% ( рис.3.24) та рівномірність завантаження мережевих ресурсів на 30%.

# ВИСНОВКИ

Огляд стану безпроводового зв’язку показав зростання обсягів і розширення функціональних можливостей сервісів, яке тягне за собою ускладнення механізмів управління та підвищення вимог до обладнання мережевої інфраструктури, що призводить до підвищення собівартості мережевої інфраструктури, або до виникнення перевантажень і зниження якості наданих сервісів.

Для підвищення якості обслуговування своїх користувачів бездротові мережі все більше тісно інтегрують між собою існуючі, а також перспективні технології, що призводить до виникнення принципово нових науково-технічних завдань.

Для виконання першого поставленого завдання, мною було досліджено перспективні рішення реалізації та управління мереж п’ятого покоління.

Проведено огляд перспектив та стримуючих факторів поширення мереж 5G. Виконано прогноз кількості користувачів і кількості споживаного трафіку з урахуванням еволюційного розвитку мереж До перспективних напрямків можливо віднести застосування таких технологій як віртуалізації NFV, застосування програмно-конфігурованих мереж, хмарної інфраструктури Cloud RAN мережі радіодоступу NG-RAN та віртуалізації транспортної мережі (Virtualized Backhaul). Магістерська робота присвячена дослідженню саме застосування програмно-конфігурованих мереж для прикладу створення мереж п'ятого покоління. Тому далі мною було проаналізовано складності реалізації програмно-конфігурованих мереж та їх принципів функціонування .

Встановлено, що існуючі моделі управління трафіком не забезпечують диференціювання окремих потоків користувачів. Система управління ПКМ не гарантує виконання вимог до якості обслуговування окремих потоків, оскільки оперує неточною інформацією про стан мережевих ресурсів та не здатна оптимально обрати маршрут передавання даних.

Оптимізація процесу передавання даних у ПКМ здійснюється або за критерієм якості обслуговування трафіку, або за критерієм рівномірності розподілу ресурсів, що у першому випадку призводить до перевантаження основних маршрутів, а в другому – до низької якості обслуговування потоків реального часу.

Проведено порівняльний аналіз принципів побудови, архітектури та процесів функціонування традиційних (з децентралізованим керуванням) та ПКМ. Аналіз принципів побудови, функціонування систем управління, моделей та алгоритмів обслуговування інформаційних потоків у програмно-конфігурованих мережах, показав ефективність застосування концепції SDN, яка дозволяє значно розвантажити фізичне обладнання мережі та позбутися від необхідності підтримки безлічі службових протоколів, закріпивши за ним лише функції передачі даних. Досліджено систему моніторингу структурно-функціональних параметрів ПКМ, яка надає засоби для збору, обробки та представлення інформації для гетерогенних апаратних та програмних OpenFlow комутаторів. Система надає змогу розширювати функціональність моніторингу та впроваджувати нові рішення на основі використання узагальнених моделей зберігання параметрів комутаторів та процесів передавання даних. Досліджено методи та алгоритми управління процесами передавання даних в ПКМ, що забезпечує підвищення якості обслуговування мультисервісних потоків та запобігає перевантаженню і підвищенню ефективності розподілу мережних ресурсів.

У практичній частині виконано експерементальне дослідженя ефективності методу адаптації системи моніторингу до завантаження мережевих елементів та модель балансування навантаження. У результаті експерименту встановлено, що досліджувана модель балансування навантаження, за умов середнього завантаження каналів 90% та середньоквадратичного відхилення інтенсивності вхідного навантаження 10%, дає змогу знизити втрати в декілька разів.

Реалізовано тестове середовище на основі апаратних комутаторів та серверів. На основі цього середовища проведено дослідження розглянутого методу вимірювання затримки. У результаті проведення експериментів доведено, що комплексне застосування розглянутих рішень дає змогу зменшити затримку для потоків реального часу та підвищити рівномірність завантаження мережних ресурсів.

# ПЕРЕЛІК ПОСИЛАНЬ

1. Берлин А.Н. Телекоммуникационные сети и устройства: Учебное пособие / А.Н. Берлин — М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2008. — 319 с.

2. Гимадинов, Р.Ф. Кластеризация в мобильных сетях 5G. Случай частичной мобильности / Гимадинов, Р.Ф., Мутханна, А.С., Кучерявый, А.Е. // Информационные технологии и телекоммуникации. 2015. Т. 3. № 2. С. 44-52.

3. Голубев А.Н., Системы коммутации в конце XX – начале XXI века / А.Н. Голубев, А.Е. Кучерявый, А.С. Миков. // Проблемы разработки, внедрения и эксплуатации цифровых систем коммутации. Семинар РНТОРЭС, Пермь, 21- 23 апреля, 1997.

4. Гольдштейн А.Б., Гольдштейн Б.С. SOFTSWITCH. – СПб.: БХВ – С-П, 2006. – 368 с.

5. Гольдштейн Б.С. Протоколы сети доступа// М.: Радио и связь, 2001. – 256 с.

6. Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети святи: Учебник для вузов. - СПб.: БХВ – Петербург, 2010. – 400 с.

7. Дежардан Р. Реализация стандартов на взаимодействие открытых систем (ВОС) в мировом масштабе// Автоматика и вычислительная техника, 1988. – 87 с.

8. Кучерявый, А.Е. Сети связи общего пользования. Тенденции развития и методы расчета / А.Е. Кучерявый, А.И. Парамонов, Е.А.Кучерявый. – М.: ФГУП ЦНИИС, 2008.

9. Кучерявый А.Е., Сети связи следующего поколения. / А.Е. Кучерявый, А.Л. Цуприков // Центральный научно-исследовательский институт связи (ЦНИИС), Москва, 2006.

10. Нетес В.А., Трубникова Н.В. Управление сетями: стандарты, проблемы и перспективы// Вестник связи.– 2000.– № 2.

11. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы// Питер, 2012. – 992 с.

12. Парамонов А.И. Разработка и исследование комплекса моделей трафика для сетей связи общего пользования. Автореферат диссертации на соискание ученой степени доктора технических наук. СПбГУТ, СПб, 2014.

13. Рыжков А.Е., Системы и сети радиодоступа 4G: LTE, WiMax / Рыжков А.Е., Сиверс М.А., Воробьев В.О., Гусаров А.С., Слышков А.С., Шуньков Р.В. // – СПб: Линк, 2012. – 226с.

14. Тихвинский. В.О., Сети 5G и IoT – инновационная среда для цифровой экономики России // Электросвязь, №8, 2017, с.18-24

15. Самуйлов К. Сети и телекоммуникации. Учебник и практикум для СПО / Константин Самуйлов, Валерий Василевский, Анна Королькова. – Москва: Юрайт, 2019. – 363 с.

16. Agiwal, M. Next generation 5G wireless networks: A comprehensive survey / Agiwal, M., Roy, A. and Saxena, N // IEEE Communications Surveys & Tuto-rials, 18(3), pp.1617-1655, 2016.

17. Aijaz, A. Realizing the Tactile Internet: Haptic Communications over Next Generation 5G Cellular Networks / Aijaz, A., Dohler, M., Aghvami, A. H., Friderikos, V., Frodigh, M. // IEEE Wireless Communications, 24(2), pp.82-89, 2017.

18. Asadi, A. Network-assisted Outband D2D-clustering in 5G Cellular Networks: Theory and Practice / A. Asadi, V. Mancuso // IEEE Transactions on Mobile Computing. – December 2016, issue 99. –17 p.

19. Galinina, O. 5G Multi-RAT LTE-WiFi Ultra-Dense Small Cells: Performance, Dynamics, Architecture, and Trends / O.Galinina, A.Pyattaev, S.Andreev et al. // IEEE Journal on Selected Areas in Communications. – March 2015. –P.1224-1240

20. Hoymann C. Relaying Operation in 3GPP LTE: Challenges and Solutions / C.Hoymann, W.Chen, H.Montojo, A.Coltschek, C.Koutsimanis, X.Chen // IEEE Communications Magazine, v.50, n.2, February 2012.

# ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ

Кафедра
Телекомунікаційних систем та мереж

**МАГІСТЕРСЬКА ДИПЛОМНА РОБОТА**
на тему:

# «ПОБУДОВА МЕРЕЖ МОБІЛЬНОГО ЗВ'ЯЗКУ НА ОСНОВІ застосування ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖ »

**Виконав: студент гр. ТСДМ-63 Шевчук А.Ю.**

**Керівник: доцент кафедри ТСМ Лаврінець К.Г.**

**Київ -2025**

# МЕТА ТА ЗАВДАННЯ

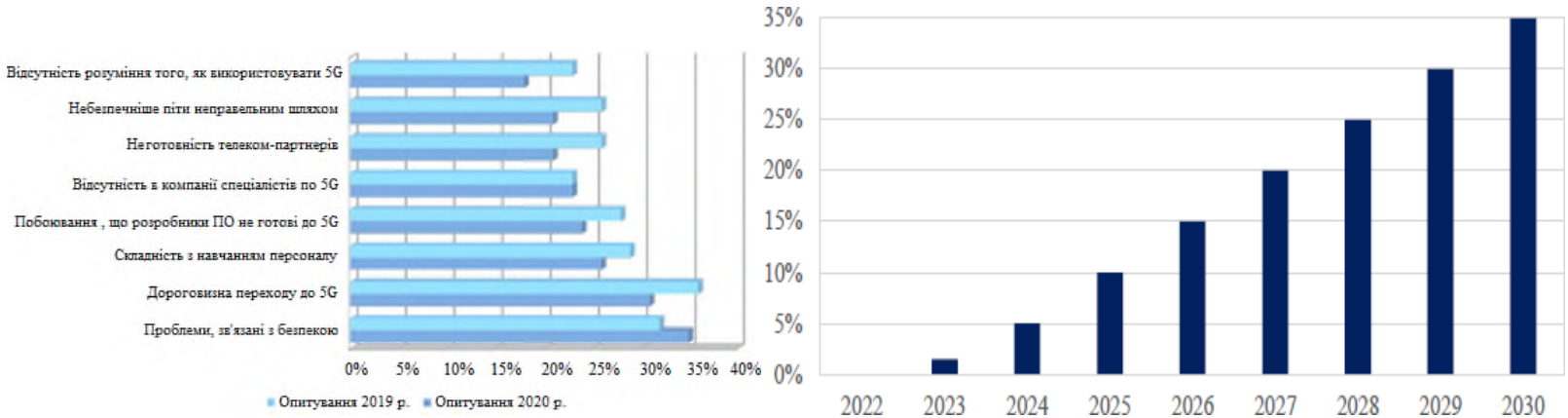
**Мета роботи** –дослідження принципів побудови мереж зв'язку п'ятого покоління із застосуванням технічного рішень SDN.

**Об’єкт дослідження**- процес реалізації мереж безпроводового зв’язку із застосуванням SDN.

**Предмет дослідження** – технічні рішення розподілу мережевих ресурсів у сучасних безпроводових мережах зв’язку.

# ПЕРСПЕКТИВИ ТА СТРИМУЮЧІ ФАКТОРИ ПОШИРЕННЯ МЕРЕЖ 5G



# ОСНОВНІ ХАРАКТЕРИСТИКИ ТА СФЕРИ ЗАСТОСУВАННЯ 5G

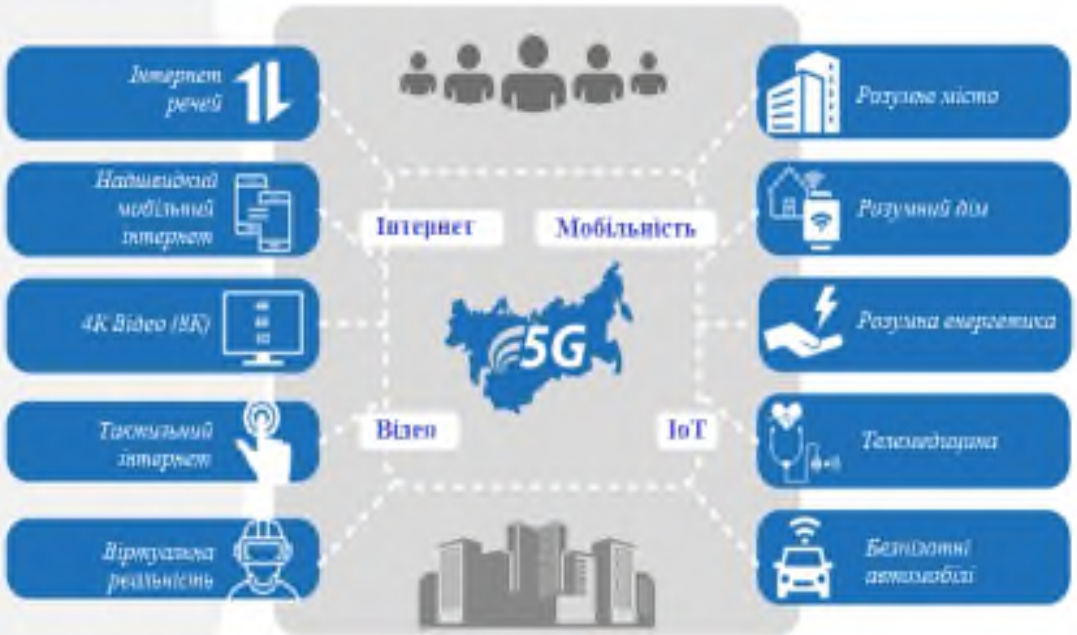
**Швидкість з'єднання**
До 20 Гб/с (пік DL - лінія вниз)

**Затримка сигнала**
1 мс (User Plane)

**Агрегація спектра**
Можливість агрегації до 16 смуг з різних або з одного діапазона в один канал

**Надійність мережі**
99 % для URLLC

**Кількість підключень**
1млн. 1 кв.км




**Вдосконалений широкосмуговий, рухомий зв'язок (eMBB)**

- Висока практична швидкість передачі даних
- Високий трафік на одиницю площі

**Надійна передача даних з малою затримкою (URLLC)**

- Велика пропускна здатність
- Надмала затримка та високий рівень готовності до обслуговування

**Великомасштабні системи міжмашинного зв'язку (IoT/M2M/D2D)**

- Велика щільність з'єднань і можливість функціонування великої кількості пристроїв в мережі
- Низька вартість пристроїв і енергоефективність

## ПЕРСПЕКТИВНІ ТЕХНІЧНІ РІШЕННЯ ДЛЯ РЕАЛІЗАЦІЇ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ 5G

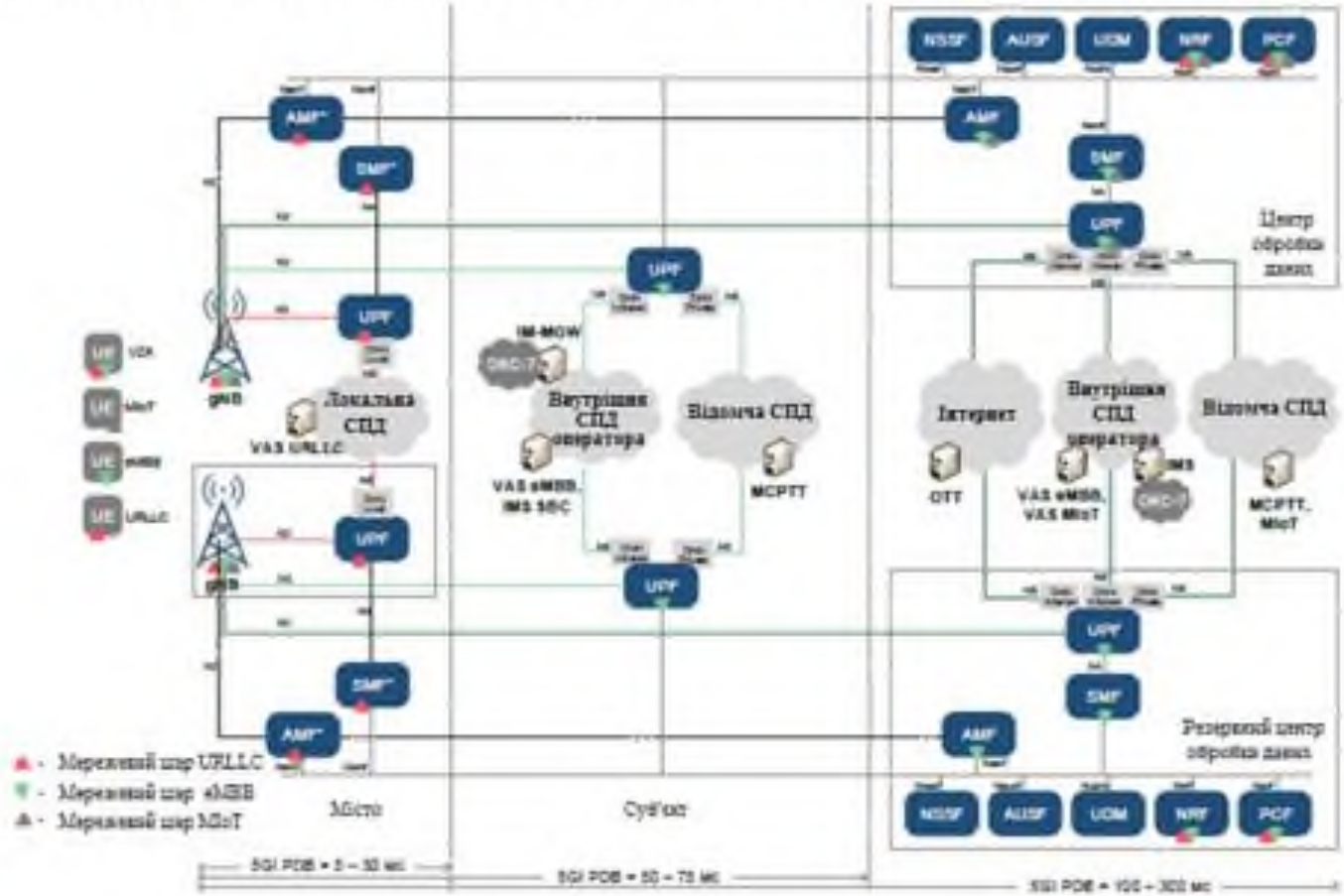



Рис.4. Приклад розгортання мережі 5G

## ПРИНЦИПІВ ФУНКЦІОНУВАННЯ ПРОГРАМНО- КОНФІГУРОВАНИХ МЕРЕЖ

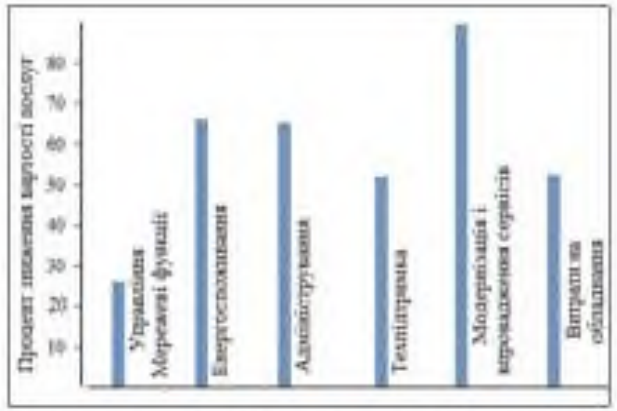



Рис.1. Відсоток зниженнявартості послуг при впровадженні SDN

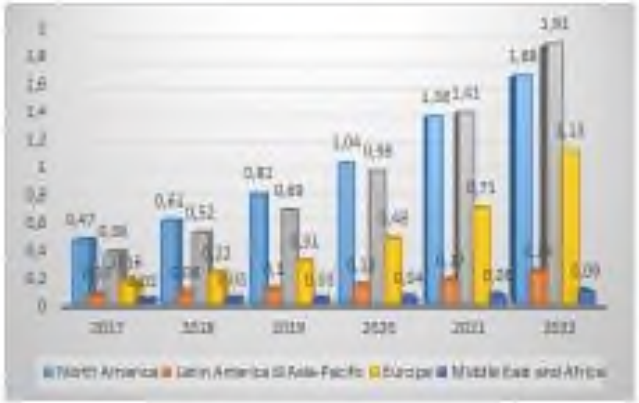



Рис 2 Прогноз розвитку мереж SDN

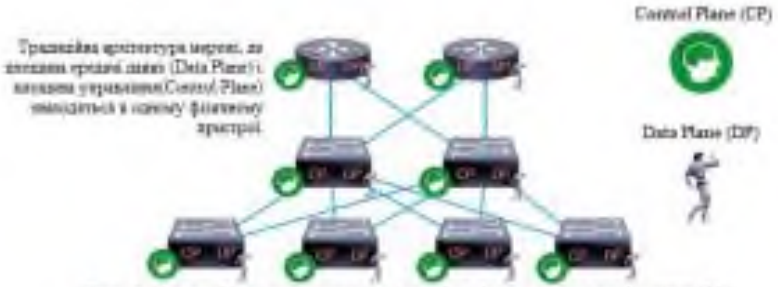



Рис. 3. Традиційна архітектура мережі з рівнями передачі даних DP і управління CP в кожному мережевому пристрої



Рис. 4 Архітектура SDN-мережі



Рис. 5. Порівняння міського водіння з навігацією і без нього

# *АНАЛІЗ СИСТЕМИ КОНТРОЛЮ ПАРАМЕТРІВ ФУНКЦІОНУВАННЯ SDN*




Рис.1 Архітектура програмно-керованої мережі з інтегрованою системою моніторингу

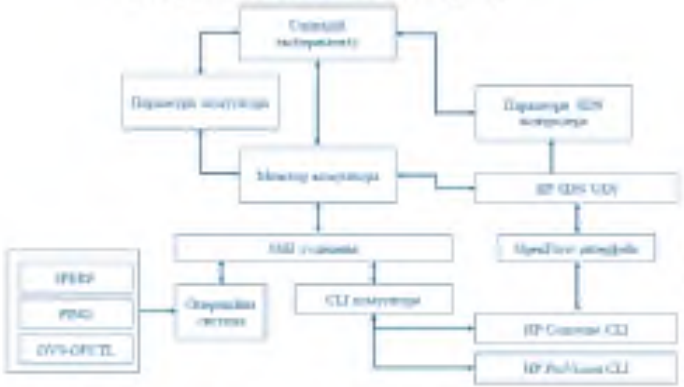


Рис.3. Архітектура центрального додатка моніторингу програмно-керованої мережі




Рис. 2. Модель даних для конфігурації системи моніторингу

Пріорітетом для оперативного управління мережею та перспективного планування є використання системи контролю. На **слайді 7 рис.1.** відображено архітектуру програмно-керованої мережі з інтегрованою системою моніторингу. Основним компонентом розглягутої системи є додаток моніторингу, який виконує ключову роль збору, форматування та представлення інформації. Модель даних для конфігурації системи моніторингу відображено на **рис.2**. Далі мною було розглянуто архітектуру центрального додатку моніторингу, яка представлена на **рис.3**.

## *МЕТОД ВИМІРЮВАННЯ ЗАТРИМКИ ПЕРЕДАВАННЯ ПАКЕТІВ*

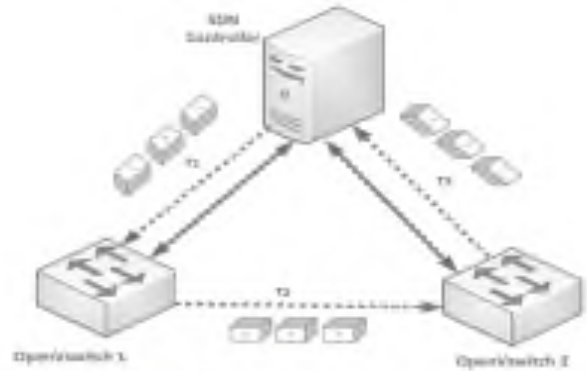


Рис.1.Схема вимірювання затримки окремого потоку в програмно-керованій мережі



Рис.3.Схема вимірювання затримки передачі окремого потоку в мережі

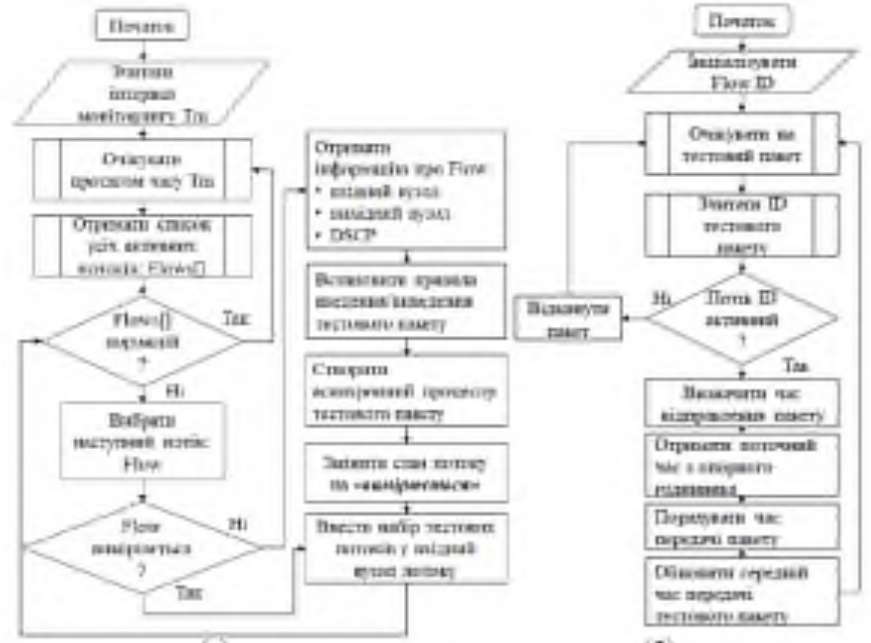


Рис.2Алгоритми відправки (а) та очікування (б) пакету для вимірювання затримки потоку

# МОДЕЛЬ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ ТА АЛГОРИТМ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ

Табл.1.Вимоги до QoS окремих додатків

| Тип потоку | Параметри QoS | | | | | | |
|---|---|---|---|---|---|---|---|
| | P, % | T, мс | J, мс | C, кбіт/с | Tc, мс | Pm | Cp |
| (голосовий дзвінок) (VoIP, Skype) | <0,25 | 150 | 10 | 64 | 900 | $10^{-3}$ | 2–256 |
| Відеоконференція (Skype) | <2 | 100 | 20 | 2048 | 800 | $10^{-3}$ | 256–512 |
| IPTV | <1 | 100 | 50 | 4096 | 1000 | $10^{-3}$ | 512–768 |
| Інтернет дані (HTTP, Online services) | <0,1 | 100 | 100 | 2048 | 1000 | $10^{-6}$ | 1280–1536 |
| Інтерактивні дані (FTP, Email) | <1 | 400 | 500 | 256–10000 | 950 | $10^{-6}$ | 768–1024 |
| Медіа зі стримінгом (Youtube) | <0,1 | 400 | 30 | 2048 | 700 | $10^{-6}$ | 1024–1280 |
| P – втрати пакетів; T – затримка(R); J - джиттер; C – пропускна здатність; Tc – тривалість встановлення з'єднання; Pm – чутливість перевищування пакетів; Cp – приорітет пакета | | | | | | | |

Табл.2.Класифікація вимог до параметрів якості обслуговування

| Параметри функціонування мережі | Клас трафіку | | | | | |
|---|---|---|---|---|---|---|
| | Клас 1 | Клас 2 | Клас 3 | Клас 4 | Клас 5 | Клас 6 (найнижчий клас) |
| Затримка, мс | 200 | 400 | 600 | 800 | 1000 | 0 |
| Джиттер, мс | 30 | 40 | 0 | 0 | 0 | 0 |
| Коефіцієнт втрат, % | 0,001 | 0,001 | 0,002 | 0,002 | 0,005 | 0 |
| Коефіцієнт помилок,% | 0,0001 | | | | | 0 |

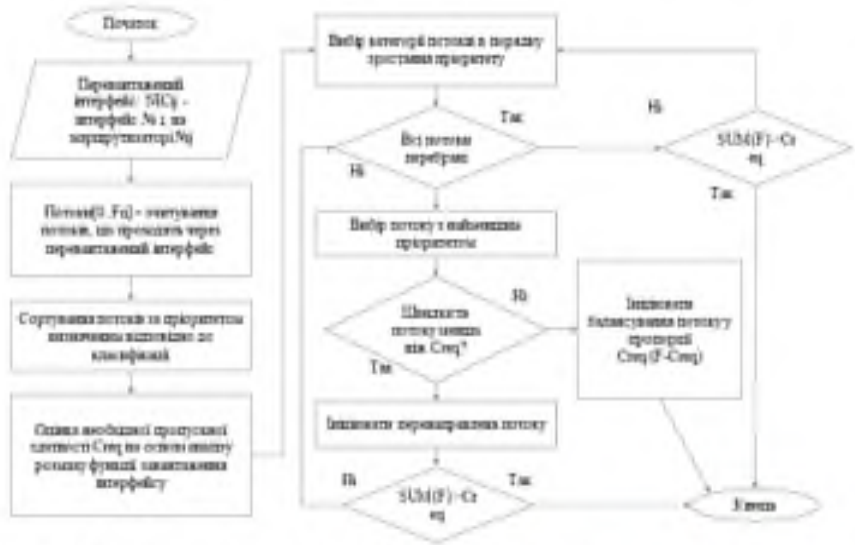



Рис.1. Алгоритм перерозподілу потоків у мережі для уникнення перевантаження

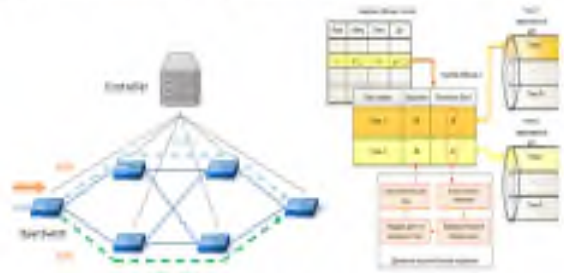


Рис.2. Принцип балансування трафіку

## ЕФЕКТИВНІСТЬ МОДЕЛІ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ

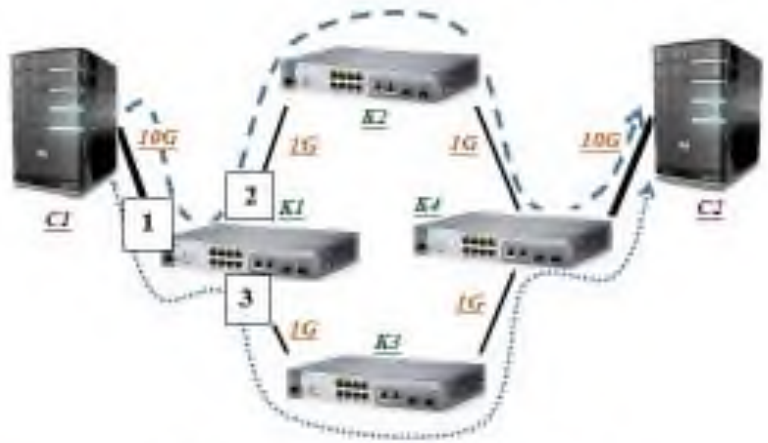



Рис 1. Конфігурація тестового середовища

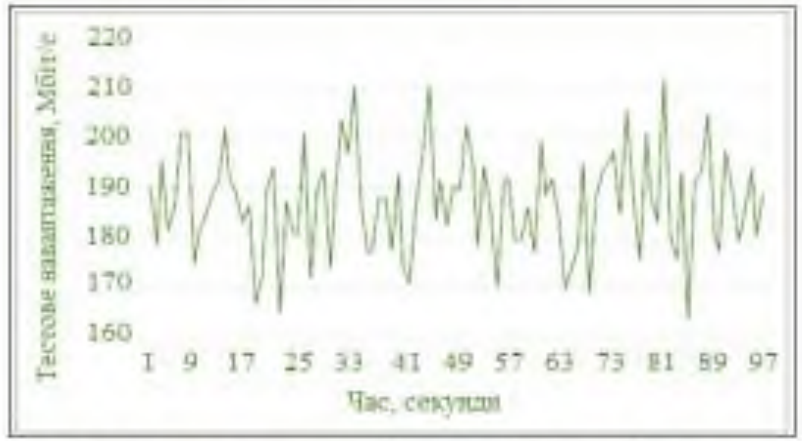



Рис.2.Згенерований мультисервісний агрегований потік

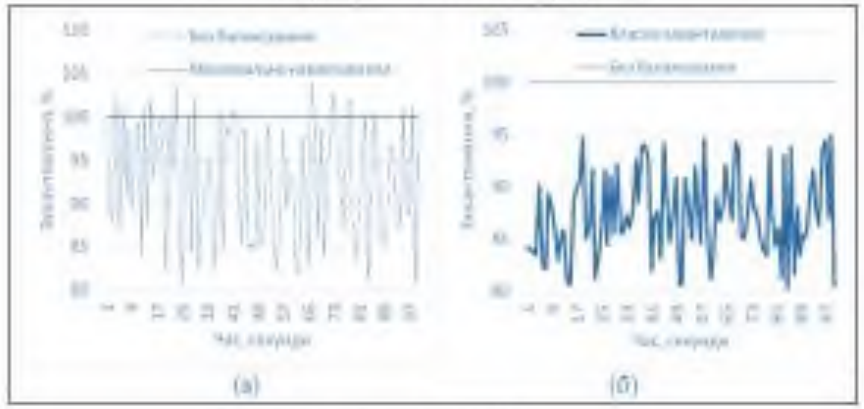



Рис.3. Завантаження каналів

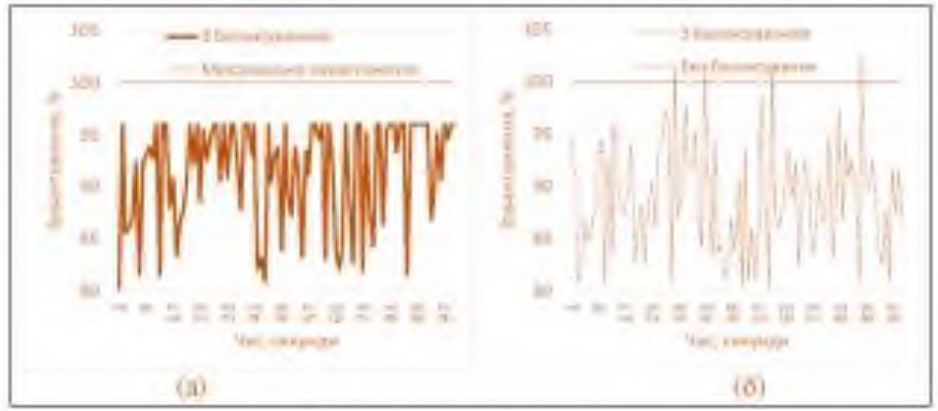



Рис.4. Завантаження каналів

## ОЦІНКА ТОЧНОСТІ ВИМІРЮВАННЯ ЗАТРИМКИ ПЕРЕДАВАННЯ ПАКЕТІВ

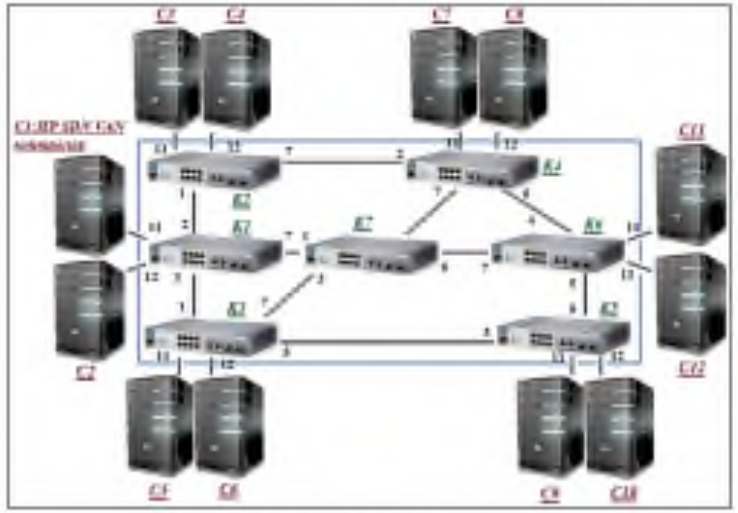


Рис.1. Схема тестового середовища

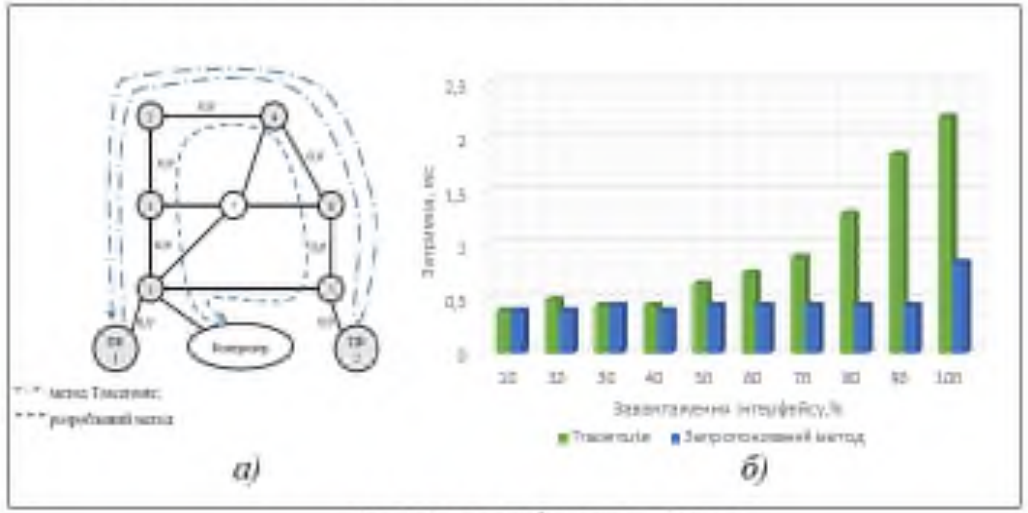



Рис.2. Схема вимірювання затримки

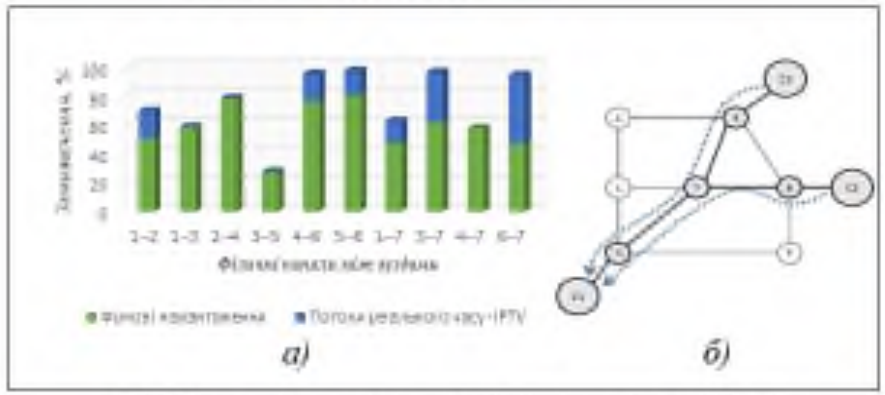



Рис.3.Завантаження каналів мережі після маршрутизації IPTV

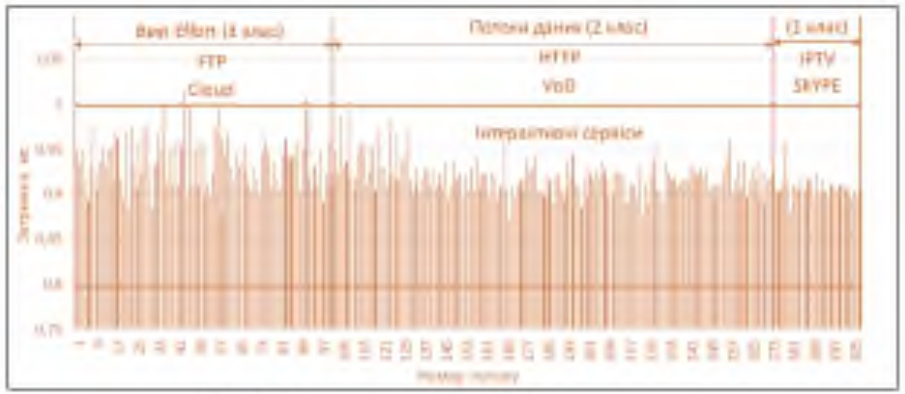



Рис.4. Середні затримки передавання пакетів

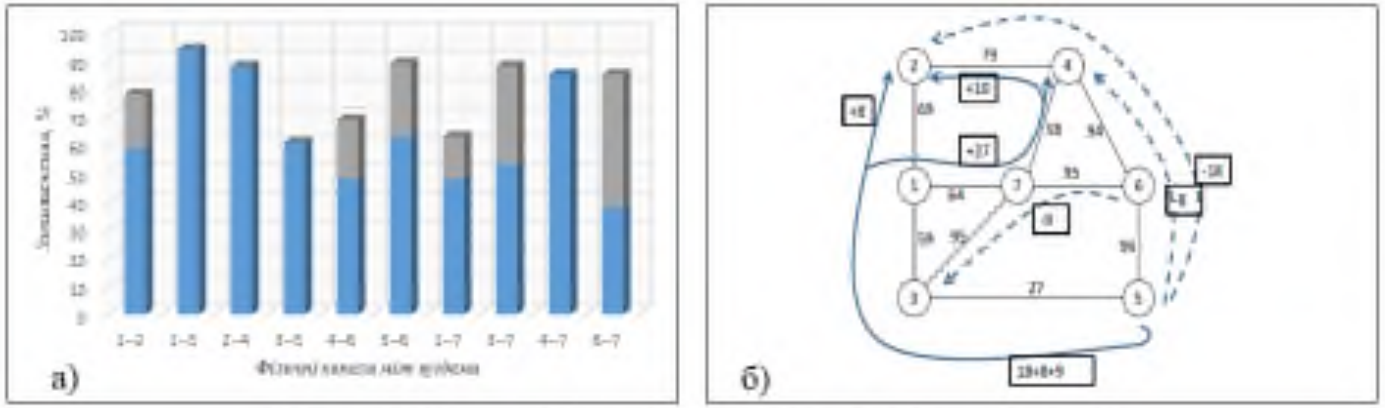



Рис.1.Розподіл завантаження мережевих каналів та схема перерозподілу потоків

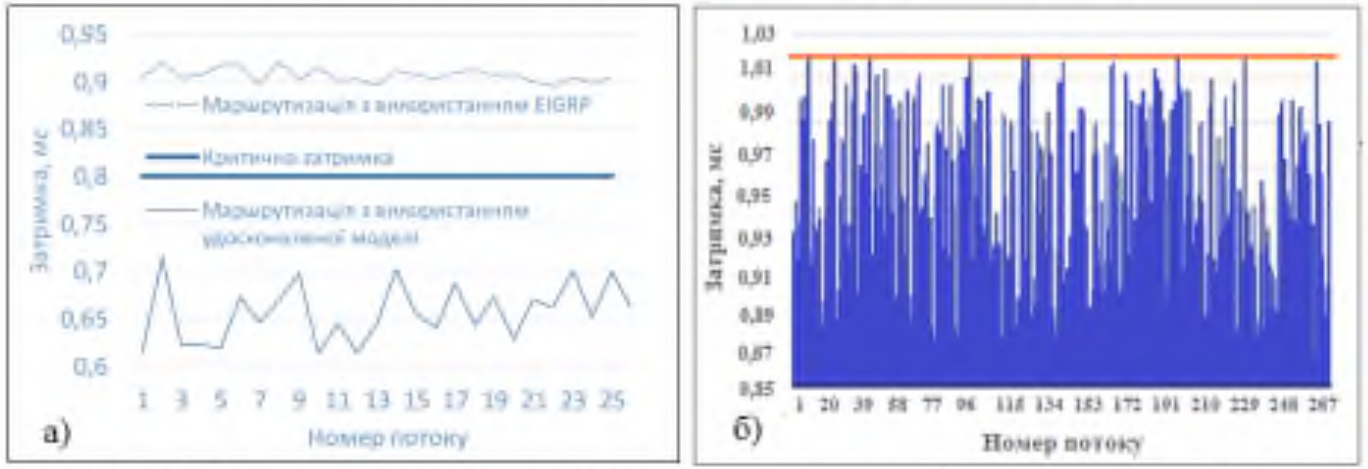



Рис.2.Значення середніх затримок після застосування досліджуваної моделі маршрутизації для потоків реального часу та потоків даних

Для підвищення якості обслуговування потоків реального часу здійснено розвантаження каналу 3-7 з використанням алгоритму перерозподілу потоків. Розподіл завантаження каналів та схему перерозподілу потоків після застосування методу відображено на рис.1. Порівняння середньої затримки потоків першого класу з використанням протоколу EIGRP та удосконаленої моделі маршрутизації відображено на рис. 2а. Середню затримку потоків двох інших класів у каналі 3- 7, в тому числі і переспрямованих потоків, відображено на рис. 2б.

# ВИСНОВКИ

1.Аналіз принципів побудови, функціонування систем управління, моделей та алгоритмів обслуговування інформаційних потоків у програмно-конфігурованих мережах, показав ефективність застосування концепції SDN, яка дозволяє значно розвантажити фізичне обладнання мережі та позбудеться від необхідності підтримки безлічі службових протоколів, закріпивши за ним лише функції передачі даних.

2. Досліджено методи та алгоритми управління процесами передавання даних в ПКМ, що забезпечує підвищення якості обслуговування мультисервісних потоків та запобігає перевантаженню і підвищенню ефективності розподілу мережних ресурсів.

3. У результаті експерименту встановлено, що досліджувана модель балансування навантаження, за умов середнього завантаження каналів 90% та середньоквадратичного відхилення інтенсивності вхідного навантаження 10%, дає змогу знизити втрати в декілька разів.

4. Реалізовано тестове середовище на основі апаратних комутаторів та серверів. На основі цього середовища проведено дослідження розглянутого методу вимірювання затримки. У результаті проведення експериментів доведено, що комплексне застосування розглянутих рішень дає змогу зменшити затримку для потоків реального часу та підвищити рівномірність завантаження мережних ресурсів.

**Дякую за увагу, доповідь закінчив.**