МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

Кваліфікаційна наукова
праця на правах рукопису

ПРИСЛУПСЬКИЙ АНДРІЙ ІВАНОВИЧ

УДК 621.391

ДИСЕРТАЦІЯ

ПІДВИЩЕННЯ ПОКАЗНИКІВ ЯКОСТІ СПРИЙНЯТТЯ ІНФОКОМУНІКАЦІЙНИХ ПОСЛУГ В ІНТЕЛЕКТУАЛЬНИХ МЕРЕЖАХ НОВОГО ПОКОЛІННЯ

172 – Телекомунікації та радіотехніка
(шифр і назва спеціальності)

17 «Електроніка та телекомунікації»
(галузь знань)

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____ / Прислупський Андрій Іванович /

Науковий керівник Бешлей Микола Іванович д.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

ЛЬВІВ – 2022

АНОТАЦІЯ

Прислупський А.І. Підвищення показників якості сприйняття інфокомунікаційних послуг в інтелектуальних мережах нового покоління. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 172 – Телекомунікації та радіотехніка. – Національний університет «Львівська політехніка» Міністерства освіти і науки України, Львів, 2022.

В дисертаційній роботі розв’язано науково-практичне завдання підвищення якості сприйняття послуг в сучасних інфокомунікаційних системах шляхом розробки нових методів інтелектуального моніторингу стану мережі, розподілу мережевими ресурсами та управління якістю обслуговування в умовах адаптації до мінливих вимог користувачів та обмеженості мережевих ресурсів.

Метою представленої роботи є підвищення показників якості сприйняття послуг шляхом розроблення інтелектуальних методів розгортання інфраструктури, моніторингу функціонування, маршрутизації та ініціації хендоверу в програмно-конфігурованих мережах на основі машинного навчання.

Об'єктом дослідження є процеси управління мережевими ресурсами та інформаційними потоками в програмно-конфігурованих мережах.

Предметом дослідження є моделі, методи та алгоритми управління якістю сприйняття послуг та розгортання інтелектуальних програмно-конфігурованих мереж.

В процесі досліджень використано методи теорії графів, алгоритмів, систем масового обслуговування, оптимізації, імітаційного моделювання, математичної статистики та машинного навчання.

У вступі обґрунтовано актуальність теми дисертаційної роботи, констатовано зв’язок роботи з науковими програмами, темами, сформульовано

мету і завдання дослідження, наукову новизну та практичне значення отриманих результатів. Наведено дані про впровадження результатів роботи, її апробацію, публікації та особистий внесок здобувача.

У першому розділі «**Аналіз існуючих методів та моделей управління якістю сприйняття послуг в сучасних телекомунікаційних мережах**» проведено огляд архітектури програмно-конфігурованих мереж та виділено основні переваги у використанні над традиційними мережами щодо управління якістю надання послуг. Встановлено, що методи забезпечення якості обслуговування (QoS, Quality of Service) мають вирішальне значення для всіх організацій, які хочуть гарантувати найкращу якість сприйняття своїх найважливіших додатків та послуг. Традиційно центри експлуатації та обслуговування мережі використовують параметри QoS, орієнтовані на мережеві технології, такі як затримка передавання, пропускна здатність, втрати пакетів тощо, щоб вимірювати якість мережі. Проте продемонстровано, що QoS в першу чергу націлений на покращення якості обслуговування щодо технічних параметрів на рівні додатків, де недостатньо враховується фактичне сприйняття та відчуття користувача. Щоб вирішити цю проблему, введено орієнтоване на користувача вимірювання якості обслуговування з поняттям якості сприйняття послуг (QoE), яке привернуло велику увагу як в наукових колах, так і серед телекомунікаційних операторів послуг.

Загалом, оцінка QoE може здійснюватися як суб’єктивним, так і об’єктивним способом, де суб’єктивна оцінка зазвичай реалізується за допомогою опитувальників і рейтингових шкал. Такий підхід можна розглядати як більш прямий і надійний спосіб оцінки показників QoE. Однак це трудомістко, дорого і незручно. У цьому відношенні впровадження штучного інтелекту і машинного навчання в управління QoE підвищує точність процедур моделювання, покращує ефективність процесу моніторингу та розробляє інноваційні методології оптимізації та контролю. Відповідно для інтелектуальних мереж нового покоління актуальним є забезпечення кінцевим

користувачам доступ до мультимедійних послуг з високою якістю сприйняття (QoE, Quality of Experience) у будь-який час та в будь-якому місці без обмежень за технологією та середовищем передавання. Для задоволення цих вимог на часі є розроблення нових структурно-функціональних моделей побудови інформаційно-комунікаційних систем та інтелектуальних схем для контролю та управління QoE в майбутніх мережах.

У другому розділі «**Моделі та методи побудови інтелектуальних мереж з адаптивним управлінням ресурсами на основі показника якості сприйняття послуг**» запропоновано концептуальну модель інтелектуальної інтенційно-орієнтованої мережі (IBN, Intent-based networking), що розгортається на основі технології програмно-конфігурованих мереж (SDN, Software-Defined Network). Згідно концептуальної ідеології IBN пропонує мережевим адміністраторам простий спосіб вираження бізнес-цілей у вигляді намірів, одним із яких є забезпечення необхідного рівня якості сприйняття сервісів, даючи змогу мережному програмному забезпеченню автоматично досягати поставлених цілей на основі інтелектуального аналізу стану ресурсів та управління трафіком. У даному розділі запропоновано систему моніторингу QoE для майбутніх програмно-конфігурованих мереж на основі намірів, яка покращить якість обслуговування кінцевих користувачів і дасть змогу ефективніше використовувати мережеві ресурси. Для цього у розділі представлені методи вимірювання параметрів функціонування програмно-конфігурованої мережі: пропускної здатності, затримки і втрати пакетів. Проведено дослідження для оцінки ефективності запропонованої системи QoE-моніторингу шляхом генерації аудіо- та відеотрафіку в мережі Mininet. На основі досліджень визначено математичну функцію кореляції параметрів QoS/QoE та розроблено метод маршрутизації, метрика якого базується на інтегральному критерії якості обслуговування.

У даному розділі також розроблено модуль машинного навчання для інтеграції в програмно-конфігуровані мережі. Це дозволяє прогнозувати рівень

якості сприйняття послуги кінцевого користувача, враховуючи такі параметри мережі, як затримка та втрата пакетів. Для машинного навчання обрано алгоритм Random Forest, який характеризується високим ступенем точності прогнозування та низькими системними вимогами для обчислення. Впровадження модуля машинного навчання в архітектуру IBN для системи моніторингу дало змогу до 30% зменшити обсяг сигнального трафіку в каналах зв'язку між мережевим обладнанням і контролером, а також реагувати на несприятливі поєднання значень показників якості і попереджати ситуації, коли користувач незадоволений якістю отриманих сервісів для адаптивного прогнозування моменту переконфігурації мережі.

Розвинуто метод управління якістю сприйняття послуг в інтелектуальних мережах, який, на відміну від відомих, для забезпечення замовленої якості послуги базується на намірах користувачів визначених у вигляді суб'єктивних QoE оцінок, що дає змогу на основі аналізу QoE намірів проводити автоматизовано конфігурацію мережі для трафіку інжинірингу, а з допомогою алгоритму машинного навчання Randon Forest прогнозувати моменти погіршення якості сприйняття послуг для швидкої переконфігурації мережі націленої на підвищення якості обслуговування користувачів.

Розроблено модифікований метод для міграції комутаторів від одного контролера до іншого з врахуванням розподілу відповідно до QoE пріоритетів. Правильний вибір комутатора для міграції є дуже важливим, адже це може критично вплинути на кінцеву якість послуг, що надаються в мережі. Показано поступовий розрахунок міграційних коефіцієнтів та проведено порівняльний аналіз щодо ефективності функціонування за критерієм затримки передавання даних звичайного міграційного методу із запропонованим. За підсумками дослідження встановлено, що запропонований підхід скорочує час обробки пріоритетних послуг.

Запропоновано модель побудови гібридної SDN/MPLS транспортної системи для підвищення якості обслуговування в інтелектуальних мережах.

Така мережа забезпечує можливість інтелектуальної організації транспортних потоків, що дає змогу більш ефективно використовувати пропускну здатність каналів та підтримувати високу якість обслуговування. Проаналізовано час побудови нового каналу для звичайної мережі MPLS та з використанням централізованого контролера. Оцінюється ефективність технологій MPLS та MPLS з контролером SDN щодо затримки мережі в процесі передачі пакетів.

У третьому розділі «**Розроблення унікального відмовостійкого контролера для клієнт-орієнтованого управління якістю обслуговування в програмно-конфігурованих інтелектуальних мережах нового покоління**» розроблено унікальний IBN контролер для інтелектуальних програмно-конфігурованих мереж, який забезпечує клієнтам надійне з'єднання. Це досягається створенням інтенцій в мережі, які перетворюють зрозумілий набір команд від користувача в код, який розуміє мережа SDN. Контролер забезпечує відповідні мережні конфігурації для забезпечення замовленого рівня якості сприйняття послуг в залежності від потреб користувача, або його фінансової можливості. Контролер IBN отримує наміри, які виражають усі види очікувань. Також контролер IBN оснащений політиками та моделями штучного інтелекту (AI), які реалізують можливості, необхідні для аналізу стану системи та пошуку оптимізованих операційних дій на основі спостережень із керованого середовища. Обробник намірів також повідомляє про виконання та статус своїх намірів. Даний контролер надає велику перевагу та зменшує вплив людини на мережу, що збільшує швидкість реагування. Перевагою є модульність контролера, який можна розгортати для усіх типів програмно-конфігурованих мереж у тому числі для ядра майбутньої мережі 5G/6G. Даний контролер має функцію авторизації, для того щоб користувачі мали змогу авторизуватись та використовувати свій акаунт для всіх маніпуляцій в мережі. Також контролер можна постійно удосконалювати, та додавати дедалі більше нових і корисних функцій, які можуть розвиватись паралельно розвитку самої мережі.

Запропоновано автоматизовану систему відновлення доступності серверів на яких розгортаються SDN/IBN контролер та IoT брокер. Розроблено архітектуру системи відновлення доступності серверів. Створено систему моніторингу функціонування серверів, що дає змогу підвищити відмовостійкість централізованого контролера управління інтелектуальною мережею. Для цього розроблено ряд алгоритмів функціонування, а саме блок схеми роботи Jenkins конвеєра, моніторинга за віддаленим сервером та скрипта моніторинга віддаленого сервера.

Передбачається, що також запропонована система дасть змогу в умовах техногенних та природних катастрофах автоматизовано управляти ресурсами, здійснювати діагностику та відновлювати дані серверної інфраструктури з метою забезпечення безперервності роботи і високої доступності бізнес сервісів.

У четвертому розділі «**Практична реалізація інтелектуальної мережі на основі використання технології SDN ZODIAC та автоматизації розроблених методів управління якістю сприйняття послуг**» розроблено модуль для інтелектуального управління процедурою хендовера на основі параметра QoE з метою інтеграції у безпровідні програмно-конфігуровані мережі. Використання розробленого модуля дає змогу проводити процедуру хендовера не лише за рівнем потужності сигналу точки доступу, але й з врахуванням таких параметрів мережі, як затримка та втрати пакетів. Врахування цих параметрів дозволило поєднати хендовер та динамічну QoE-маршрутизацію, для забезпечення високого рівня якості сприйняття. Згідно з отриманих результатів запропонований алгоритм дає змогу швидко реагувати на раптові погіршення у мережі та забезпечувати необхідну якість сприйняття для кінцевого користувача.

Проведено інтеграцію модуля машинного навчання для передбачення рівня якості сприйняття на основі аналізу параметрів QoS. На основі проведеного дослідження встановлено, що запропоновані рішення для

побудови інтелектуальних мереж дають змогу підвищити показник якості сприйняття послуги від QoE–3 до QoE–5. А використання інтелектуальної системи QoE-моніторингу збільшує швидкість реагування у процесі переконфігурації мережі в умовах погіршення якості сприйняття послуг на 10 секунд у порівнянні із відомими.

У роботі для практичної реалізації інтелектуальної мережі нового покоління використано обладнання технології SDN Zodiac, яке, на відміну від пропрієтарних виробників мережевого обладнання є відкритою для модифікацій та дає змогу програмно реалізовувати власні рішення щодо управління ресурсами.

Встановлено, що згідно стратегічного розвитку перспективних інформаційно-комунікаційних мереж створення національної системи зв'язку слід проводити з урахуванням можливості її подвійного призначення. Це дасть змогу використовувати її з метою надання послуг зв'язку для загального, відомчого та спеціального використання. На сьогодні, одним із найважливіших викликів в системі національної безпеки та оборони України, безумовно, є система захисту інформації та кібербезпеки в інформаційно-телекомунікаційних мережах. Відповідно використання технології IBN є доцільним для того, щоб автоматизовано розгортати інформаційні мережі зв'язку подвійного призначення в межах однієї фізичної інфраструктури на основі розробленого мережевого обладнання з підтримкою методу автоматизації процесу декомпозиції структури шляхом віртуалізації ресурсів для організації ізольованих захищених мереж.

Для підвищення інформаційної безпеки розроблено алгоритми для системи виявлення вторгнень (IDS), заснованих на статистичному аналізі та глибокому навчанні, що спрямовані на виявлення аномальної поведінки в сучасних та майбутніх програмно-конфігурованих мережах. Запропонований підхід базується на вивченні часових рядів нормальної поведінки мережі та виявляє помітні аномалії мережі, одночасно зменшуючи час навчання на порядок.

Дослідження довели що використання запропонованого алгоритму виявлення та блокування шкідливого трафіку дало змогу зменшити на 5% втрати в загальному каналі зв’язку та відповідно для користувачів законного трафіку покращити якість обслуговування та сприйняття послуг.

Висновки до дисертації включають узагальнені результати дослідження та рекомендації щодо їх практичного застосування. Зокрема, розроблені науково-прикладні рішення щодо управління мережевими ресурсами, процедури хендоверу на основі QoE критерію та якістю обслуговування зможуть на практиці застосовувати науково-дослідні організації, компанії, оператори мобільного зв’язку для покращення якості сприйняття послуг з боку користувачів у мережах із централізованим управлінням.

Результати дисертаційної роботи використано при формуванні навчальних дисциплін, що викладаються студентам (за навчальним планом) у навчальному процесі кафедри телекомунікацій Національного університету «Львівська політехніка», зокрема для студентів спеціальності 172 «Телекомунікації та радіотехніка» в курсі лекцій з дисципліни «Побудова та протоколи гетерогенних мереж мобільного зв’язку», а також у навчальному процесі спеціальності 126 «Інформаційні системи та технології» в курсі лекцій з дисципліни «Мережеві інформаційно-комунікаційні технології.

Основні результати дисертаційної роботи використано і впроваджено з метою підвищення показників якості сприйняття послуг та гнучкості управління ресурсами в телекомунікаційній корпоративній мережі ТзОВ «МаксіТех», що підтверджено актом впровадження.

Ключові слова: Інтелектуальна мережа, програмно-конфігурована мережа, інтенційно-орієнтована мережа, якість обслуговування, якість сприйняття послуг, хендовер, машинне навчання.

Список публікацій здобувача:

Наукові праці, у яких опубліковані основні результати дисертації

1. W. Song, M. Beshley, K. Przystupa, H. Beshley, O. Kochan, A. Pryslupskyi, D. Pieniak, J. Su, “A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection,” *Sensors*, vol. 20, no. 6, pp. 1637-1–1637-41, March 2020. (Scopus/Web of Science Q1).

2. M. Beshley, P. Vesely, A. Prislupskiy, H. Beshley, M. Kyryk, V. Romanchuk, I. Kahalo, “Customer-Oriented Quality of Service Management Method for the Future Intent-Based Networking,” *Applied Sciences*, vol. 10, no. 22, pp. 8223-1– 8223-38, Nov. 2020. (Scopus/Web of Science Q2).

3. A. Prislupskiy, M. Beshley, H. Beshley, Y. Pyrih, A. Branytskyy, “QoE-oriented routing model for the future intent-based networking,” *Lecture Notes in Electrical Engineering: Future intent-based networking. On the QoS robust and energy efficient heterogeneous software defined networks,* vol. 831, pp.128–144, 2022.

4. V. Romanchuk. M. Beshley, A. Prislupskiy, H. Beshley, O. Panchenko, “Method of multiservice infrastructure decomposition with network resource slicing for IoT,” *Internet of Things (IoT) and Engineering Applications (Canada)*, vol. 3, no.1, pp. 22–23, May 2018.

5. В.І. Романчук, М.І. Бешлей, А.І. Прислупський, Г.В. Бешлей, “Метод декомпозиції структури мережного пристрою з віртуалізацією ресурсів,” *Наукові записки Української академії друкарства*, №1(56), с. 31– 42, 2018.

6. М.І. Бешлей, А.І. Прислупський, Г.В. Бешлей, “Методи розподілу радіоресурсів та балансування навантаження в мережі 5G/NB-IoT для надання критично важливих сервісів Інтернету речей,” *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки*. – Т.32 (71), ч. 1, № 5, с. 36–45, 2021.

7. М.І. Бешлей, А. І. Прислупський, Г. В .Бешлей, “Управління якістю обслуговування в гетерогенній інтенційно-орієнтованій мережі на основі мобільного QoE додатку,” *Проблеми телекомунікацій*, № 1 (28, с. 45–64, 2021.

8. М.Б. Медвецький, М.І. Бешлей, А.І. Прислупський, Г.В. Бешлей “Метод ініціації хендоверу в програмно-конфігурованій безпровідній мережі на основі показника якості сприйняття послуг,” *Infocommunication Technologies and Electronic Engineering = Інфокомунікаційні технології та електронна інженерія,* Vol. 1, № 2, P. 1–10, 2021.

9. М.Б. Медвецький, М.І. Бешлей, А.І. Прислупський “ Метод управління якістю сприйняття послуг для програмно-конфігурованих мереж заснованих на намірах,” *Infocommunication Technologies and Electronic Engineering = Інфокомунікаційні технології та електронна інженерія,* Vol. 1, № 1,P. 76–85, 2021.

Наукові праці, які засвідчують апробацію матеріалів дисертації

10. M. Beshley, M. Medvetskyi, S. Jun, A. Pryslupskyi, Y. Bobalo and H. Beshley, "QoE-Aware Intelligent Handover Method for Intent-Based Software-Defined Wireless Network," *2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, 2022, pp. 534-538, doi: 10.1109/TCSET55632.2022.9767075.

11. C. Wang, L. Yuan, M. Medvetskyi, M. Beshley, A. Pryslupskyi and H. Beshley, "Machine Learning-Enabled Software-Defined Networks for QoE Management," *2021 IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT)*, 2021, pp. 234-238, doi: 10.1109/AICT52120.2021.9628961.

12. M. Beshley, A. Pryslupskyi, O. Panchenko and M. Seliuchenko, "Dynamic Switch Migration Method Based on QoE- Aware Priority Marking for Intent-Based Networking," *2020 IEEE 15th International Conference on Advanced Trends in*

Radioelectronics, Telecommunications and Computer Engineering (TCSET), 2020, pp. 864-868, doi: 10.1109/TCSET49122.2020.235559.

13. M. Beshley, A. Pryslupskyi, O. Panchenko and H. Beshley, "SDN/Cloud Solutions for Intent-Based Networking," *2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)*, 2019, pp. 22-25, doi: 10.1109/AIACT.2019.8847731.

14. A. Pryslupskyi, O. Panchenko, M. Beshley and M. Seliuchenko, "Improvement of Multiprotocol Label Switching Network Performance using Software-defined Controller," *2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM)*, 2019, pp. 106-109, doi: 10.1109/CADSM.2019.8779316.

ABSTRACT

Prislupskiy A.I. Improving the quality of experience of infocommunication services in the next generation intelligent networks. – Qualification research paper as a manuscript.

The thesis for the Doctor of Philosophy Degree in the specialty 172 – Telecommunications and Radio Engineering. – Lviv Polytechnic National University, Ministry of Education and Science of Ukraine, Lviv, 2022.

The thesis solves the scientific and practical task of improving the quality of experience of services in modern infocommunication systems by developing new methods for intelligent monitoring of network state, network resource allocation, and quality of service management in the conditions of adaptation to changing user requirements and limited network resources.

The purpose of this thesis is to improve the quality of experience of service by developing intelligent methods for infrastructure deployment, performance monitoring, routing, and handover initiation in software-defined networks based on machine learning.

The object of research is the processes of network resources and information flows management in software-defined networks.

The subject of research is models, methods and algorithms of quality of experience of services management, and deployment of intelligent software-defined networks.

In the process of research, methods of graph theory, algorithms, the mass service systems, optimization, simulation modeling, mathematical statistics and machine learning are used.

The introduction substantiates the relevance of the topic of the thesis work, states the relationship of the work with scientific programs, topics, formulates the purpose and objectives of research, scientific novelty and practical significance of the results obtained. Data on the implementation of the results of the work, its approbation, publications and personal contribution of the applicant are given.

In the first chapter «**Analysis of existing methods and models of quality of experience management in modern telecommunication networks**» the architecture of software-defined networks is reviewed and the main advantages of using traditional networks of quality of service management are highlighted. The Quality of Service (QoS) methods have been found to be critical for all organizations that want to guarantee the best possible quality of experience for their critical applications and services. Traditionally, network operation and maintenance centers have used network-centric QoS parameters such as transmission delay, throughput, packet loss, etc. to measure network performance. However, it has been demonstrated that QoS is primarily aimed at improving the quality of service of technical parameters at the application level, where the actual user perception and experience is not sufficiently taken into account. To address this issue, a user-centric measurement of quality of service with the notion of Quality of Experience (QoE) has been introduced, attracting much attention both in academia and among telecommunications service providers.

In general, QoE can be assessed in both subjective and objective ways, where the subjective assessment is usually implemented by means of questionnaires and rating scales. This approach can be seen as a more direct and reliable way to assess QoE. However, it is time-consuming, expensive, and uncomfortable. In this respect, the introduction of artificial intelligence and machine learning in QoE management improves the accuracy of modeling procedures, improves the efficiency of the monitoring process, and develops innovative optimization and control methodologies. Accordingly, it is relevant for next-generation intelligent networks to provide end-users with access to multimedia services with a high quality of experience QoE, at any time and place without restrictions on technology and transmission medium. Developing new structural and functional models for building information and communication systems and intelligent schemes to control and manage QoE in future networks is relevant to meeting these requirements.

In the second chapter «**Models and methods for designing intelligent networks with adaptive resource management based on quality of experience metrics**» proposes a conceptual model of intelligent Intent-based networking (IBN), deployed based on Software-defined networking (SDN) technology. According to the conceptual ideology IBN offers network administrators a simple way to express business goals as intents, one of which is to provide the necessary level of quality of experience of services, allowing network software to automatically achieve its goals based on intelligent analysis of the state of resources and traffic management. This section proposes an intent-based QoE monitoring system for future software-defined networks that will improve end-user experience and enable more efficient use of network resources. For this purpose, the section presents ways to measure the performance characteristics of the Software Defined Network: throughput, latency, and packet loss. Studies have been conducted to evaluate the effectiveness of the proposed QoE monitoring system by generating audio and video traffic in the Mininet network. Based on the research, the mathematical correlation function of

QoS/QoE parameters was determined and a routing method was developed, whose metric is based on the integral criterion of the quality of service.

This section develops a machine learning module for integration into software-defined networks. It allows predicting the QoE of end-user service, taking into account such network parameters as delay and packet loss. The Random Forest algorithm is selected for machine learning, characterized by a high degree of prediction accuracy and low computational system requirements. Implementation of the machine learning module in the IBN architecture for the monitoring system has allowed to reduce the signal traffic in the communication channels between the network equipment and the controller by up to 30%, as well as to react to unfavorable combinations of quality parameter values and prevent situations when a user is not satisfied with the received quality of services.

The method of QoE management in intelligent networks is developed, which, in contrast to the known, ensures the ordered quality of service is based on user intents defined in the form of subjective QoE evaluations. This method allows, based on the analysis of QoE intents, to conduct an automated network configuration for traffic engineering and use a machine learning algorithm, Randon Forest, to predict the moments of deterioration of QoE for rapid reconfiguration of the network, aimed at improving the quality of service.

It develops a modified method for migrating switches from one controller to another, taking into account the allocation according to QoE priorities. Choosing the right switch for migration is very important as it can critically affect the final quality of services provided in the network. The gradual calculation of migration coefficients is shown, and a comparative analysis of the efficiency by the criterion of data transmission delay of the usual migration method with the proposed one is made. Based on the study, it is found that the proposed approach reduces the processing time of priority services.

A model for developing a hybrid SDN/MPLS transport system for improving the quality of service in intelligent networks is proposed. Such a network provides the

possibility of intelligent organization of transport flows, which allows using of the channel bandwidth more efficiently and maintains a high quality of service. We analyze the time of construction of a new channel for a conventional MPLS network and using a centralized controller. The network delay in the packet transmission process evaluates the efficiency of MPLS and MPLS technologies with SDN controller.

In the third chapter «**Development of a unique fault-tolerant controller for client-oriented quality of service management in the next generation software-defined intelligent networks**», develops a unique IBN controller for intelligent software-defined networks that provide clients with a reliable connection. This is accomplished by creating intents in the network that translate an understandable set of user commands into code that the SDN understands. The controller provides appropriate network configurations to provide the ordered level of QoE depending on the user's needs or financial capability. The IBN controller receives intents expressing all kinds of expectations. The IBN controller is also equipped with policies and artificial intelligence (AI) models that implement the capabilities needed to analyze system states and find optimized operational actions based on observations from the managed environment. The intent handler also reports on the execution and status of its intentions. This controller gives a great advantage and reduces human influence on the network, which increases responsiveness. The advantage is the modularity of the controller, which can be deployed for all types of SDN, including the core of a future 5G/6G network. This controller has an authorization function so that users can authorize and use their account for all network manipulations. Also, the controller can be constantly improved and more new and useful features can be added, which can be developed in parallel with the development of the network itself.

An automated system for restoring the availability of the servers on which the SDN/IBN controller and IoT broker are deployed is proposed. The architecture of the system to restore the availability of servers was developed. A system for monitoring the functioning of servers was created, which allows to increase the fault tolerance of

the centralized control controller of the intelligent network. For this purpose, several functioning algorithms developed, namely the block scheme of Jenkins conveyor, remote server monitoring and remote server monitoring script.

The proposed system is expected to allow under conditions of technogeneous and natural disasters to automatically manage resources, diagnose and recover server infrastructure data to ensure business continuity and high availability of business services.

In the fourth chapter «**Practical implementation of the intelligent network based on the use of SDN ZODIAC technology and automation of the developed methods of QoE management**» the module for intelligent management of the handover procedure based on the QoE parameter for integration into wireless software-defined networks is developed. The developed module enables handover not only according to the access point signal strength but also taking into account such network parameters as delay and packet loss. Accounting for these parameters allowed to combine handover and dynamic QoE routing to ensure a high level of QoE. According to the results, the proposed algorithm can quickly respond to sudden degradation in the network and provide the required QoE for the end-user.

The integration of a machine learning module for predicting the QoE level based on the analysis of QoS parameters has been carried out. Based on the study, it has been found that the proposed solutions for intelligent networks increase the QoE index from QoE-3 to QoE-5. Using an intelligent QoE-monitoring system increases the response time in the reconfiguration of the network in conditions of deterioration of QoE perception for 10 seconds compared to the known.

In work on the practical implementation of an intelligent network of a new generation, SDN Zodiac technology equipment was used. Unlike proprietary network equipment manufacturers, it is open for modifications and can be implemented programmatically with its own solutions for resource management.

It is established that according to the strategic development of prospective information and communication networks, the creation of a national communication

system should be carried out with the possibility of its dual purpose. This will allow its use to provide communication services for general, departmental and special use. To date, one of the most important challenges in the system of national security and defense of Ukraine, of course, is the system of information protection and cybersecurity in information and telecommunication networks. Accordingly, the use of IBN technology is expedient in order to automate the deployment of dual-purpose information communication networks within one physical infrastructure on the basis of the developed network equipment with the support of the method of automation of the structure decomposition process by means of virtualization of resources for the organization of isolated protected networks.

Intrusion Detection System (IDS) algorithms based on statistical analysis and deep learning, aimed at detecting abnormal behavior in current and future software-configured networks, are developed to improve information security. The proposed approach is based on learning a time series of normal network behavior and detects notable network anomalies while reducing the learning time by order of magnitude. Studies have shown that using the proposed algorithm for detecting and blocking malicious traffic has reduced the loss in the overall link by 5% and, consequently, for users of legitimate traffic, improved the QoS and QoE.

Scientific and practical results of the research performed are used in the educational process of the Department of Telecommunications of the Lviv Polytechnic National University, particularly for students of specialty 172 «Telecommunications and Radio Engineering» in the course of lectures on «Construction and protocols of heterogeneous networks of mobile communication», as well as in the educational process of specialty 126 «Information systems and technologies» in the course of lectures on the discipline «Network information and communication technologies».

The main results of the thesis work were used and implemented to improve the quality of experience of services and flexibility of resource management in the

telecommunications corporate network of MaxiTex, which is confirmed by the act of implementation.

Key words: Intelligent network, software-define network, intent-based network, quality of service, quality of experience, handover, machine learning.

The list of author's publications:

Proceedings where basic scientific results of thesis were published

1. W. Song, M. Beshley, K. Przystupa, H. Beshley, O. Kochan, A. Pryslupskyi, D. Pieniak, J. Su, "A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection," *Sensors*, vol. 20, no. 6, pp. 1637-1–1637-41, March 2020. (Scopus/Web of Science Q1).

2. M. Beshley, P. Vesely, A. Prislupskiy, H. Beshley, M. Kyryk, V. Romanchuk, I. Kahalo, "Customer-Oriented Quality of Service Management Method for the Future Intent-Based Networking," *Applied Sciences*, vol. 10, no. 22, pp. 8223-1– 8223-38, Nov. 2020. (Scopus/Web of Science Q2).

3. A. Prislupskiy, M. Beshley, H. Beshley, Y. Pyrih, A. Branytskyy, "QoE-oriented routing model for the future intent-based networking," *Lecture Notes in Electrical Engineering: Future intent-based networking. On the QoS robust and energy efficient heterogeneous software defined networks,* vol. 831, pp.128–144, 2022.

4. V. Romanchuk. M. Beshley, A. Prislupskiy, H. Beshley, O. Panchenko, "Method of multiservice infrastructure decomposition with network resource slicing for IoT," *Internet of Things (IoT) and Engineering Applications (Canada)*, vol. 3, no.1, pp. 22–23, May 2018.

5. V.I. Romanchuk, M.I. Beshey, A.I. Pryslupskiy, H.V. Beshley, " Method of decomposing the structure of a network device with virtualization of resources," *Sientific notes of Ukrainian Printing Academy*, №1(56), pp. 31– 42. 2018.

6. M.I. Beshey, A.I. Pryslupskiy, H.V. Beshley, “ Radio resource allocation and load balancing methods in a 5G/NB-IoT network to provide critical iot services,” *Scientific Notes of V.I. Vernadsky Tavrida National University. Series: Technical Sciences*. – T.32 (71), p. 1, № 5, pp. 36–45, 2021.

7. M.I. Beshey, A. I. Pryslupskiy, H.V. Beshley, “Quality of service management for intent-based heterogeneous network using mobile QoE application,” *Problems of Telecommunications,* No. 1 (28), pp. 45-64, 2021.

8. M.B. Medvetskyi, M.I. Beshey, A. I. Pryslupskiy, H.V. Beshley, “Handover initiation method in a software-defined wireless network based on quality of experience indicator,” *Infocommunication Technologies and Electronic Engineering,* Vol. 1, № 2, P. 1–10, 2021.

9. M.B. Medvetskyi, Medvetskyi, “ QoE management method for intent-based software-defined networks,” *Infocommunication Technologies and Electronic Engineering,* Vol. 1, № 1, P. 76–85, 2021.

Proceedings that certify an approvement of thesis materials

10. M. Beshley, M. Medvetskyi, S. Jun, A. Pryslupskyi, Y. Bobalo and H. Beshley, "QoE-Aware Intelligent Handover Method for Intent-Based Software-Defined Wireless Network," *2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, 2022, pp. 534-538, doi: 10.1109/TCSET55632.2022.9767075.

11. C. Wang, L. Yuan, M. Medvetskyi, M. Beshley, A. Pryslupskyi and H. Beshley, "Machine Learning-Enabled Software-Defined Networks for QoE Management," *2021 IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT)*, 2021, pp. 234-238, doi: 10.1109/AICT52120.2021.9628961.

12. M. Beshley, A. Pryslupskyi, O. Panchenko and M. Seliuchenko, "Dynamic Switch Migration Method Based on QoE- Aware Priority Marking for Intent-Based Networking," *2020 IEEE 15th International Conference on Advanced Trends in*

Radioelectronics, Telecommunications and Computer Engineering (TCSET), 2020, pp. 864-868, doi: 10.1109/TCSET49122.2020.235559.

13. M. Beshley, A. Pryslupskyi, O. Panchenko and H. Beshley, "SDN/Cloud Solutions for Intent-Based Networking," *2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)*, 2019, pp. 22-25, doi: 10.1109/AIACT.2019.8847731.

14. A. Pryslupskyi, O. Panchenko, M. Beshley and M. Seliuchenko, "Improvement of Multiprotocol Label Switching Network Performance using Software-defined Controller," *2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD*

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

QoS – Quality of Service, якість обслуговування.

SDN – Software-Defined Networking, програмно-конфігурована мережа.

IBN – Intent-Based Networking, інтенційно-орієнтована мережа.

API – Application Programming Interface, прикладний програмний інтерфейс.

QoE – Quality of Experience, якість сприйняття, ступінь задоволеності користувача.

IoT – Internet of Things, Інтернет речей.

WAN – Wide Area Networ, глобальна мережа.

WLAN – Wireless Local Area Network, безпровідна локальна мережа

ACL – Access Control List, список контролю доступу.

VLAN – Virtual Local Area Network, віртуальна локальна комп'ютерна мережа

LTE – Long Term Evolution, довготерміновий розвиток.

NFV – Network Functions Virtualization, віртуалізація мережевих функцій.

EC – Edge Computing, граничне обчислення.

RAT – Radio Access Technology, технологія радіо доступу.

MVNO – Mobile Virtual Network Operator, віртуальний оператор стільникового зв'язку.

UE – User Equipment, обладнання користувача.

ToS – Type of Service, тип обслуговування.

IDS – Intrusion Detection System, система виявлення вторгнень.

IPS – Intrusion Prevention System, система запобігання вторгнень.

SLA – Service Level Agreements, угоди про рівень обслуговування.

ELA – Experience Level Agreements, угоди про рівень очікуваної якості сервісу.

IBSDN – Intent-Based Software-Defined Network, програмно-конфігурована інтенційно-орієнтована мережа.

CC – Cloud Computing, хмарні обчислення.

EC – Edge Computing, крайові обчислення.

JSON – JavaScript Object Notation, це текстовий формат обміну даними між комп'ютерами.

CLI – Command-line Interface, інтерфейс командного рядка.

IP – Internet Protocol, інтернет протокол, в мережах з комутаціє пакетів.

TCP – Transmission Control Protocol, протокол керування передачею.

DPI – Deep Packet Inspection, глибока перевірка пакетів.

DNS – Domain Name System, служба доменних імен.

RTP – Real-time Transport Protocol, протокол передачі даних в реальному часі.

HTTP – HyperText Transfer Protocol, протокол передачі гіпертексту.

uTP – Torrent UDP, UDP торент протокол

ISP – Internet Service Provider, провайдер інтернет мереж

RRM – Radio Resource Management, Управління радіоресурсами.

E2E – End-to-End, з кінця в кінець.

SINR – Signal to interference plus noise ratio, відношення сигналу/шум.

RAN – Radio Access Network, мережа радіодоступу.

VM – Virtual Machine, віртуальна машина.

OvS – Open vSwitch, віртуальний комутатор.

DMCQR – Deterministic multiconstrained centralized QoS routing, централізована детермінована багатокритеріальна QoS маршрутизація.

SSL – Secure Sockets Layer, рівень захищених сокетів.

низькою затримкою.

ВСТУП

Актуальність теми.

З появою смартфонів і хмарних технологій світ переживає низку великих технологічних революцій, включаючи Інтернет речей, машинне навчання та мережі мобільного зв'язку 5G/6G. Сьогодні в умовах лабораторного тестування фіксовані та мобільні мережі об'єднуються у напрямку розвитку інтелектуальних мереж нового покоління шляхом інтеграції штучного інтелекту в ядро системи. Така інтеграція покликана в майбутньому забезпечити доступ до будь-яких послуг з найкращою якістю сприйняття для кінцевих користувачів використовуючи сучасні мережеві технології. Останнім часом мережева технологія програмно-конфігурованих мереж (SDN, Software-Defined Networking) привернула найбільшу увагу та отримала широке визнання серед компаній у всьому світі. Програмно-конфігурована мережа актуальна серед постачальників хмарних послуг, але ця популярність ще не зменшилася в секторі, який покладається на автоматизацію телекомунікаційних мереж. За офіційними даними, велика кількість організацій у цьому секторі все ще керують своїми мережами вручну. Іншими словами, адміністратори вручну вводять інтерфейси командного рядка для будь-якої необхідної конфігурації своїх мереж. Це призвело до затримок у реагуванні та опосередковано чи прямо перешкоджало конкурентоспроможності.

Згідно проведеного аналізу наукових та практичних робіт встановлено, що ні численні засоби централізованого управління, ні велика кількість моніторингових даних, доступних ІТ-персоналу, не допомагають вирішити проблему автоматизованого інтелектуального управління мережевими ресурсами адаптуючись під мінливі потреби користувачів для мереж нового покоління. У зв'язку із тим нещодавно з'явилася ще одна мережева тенденція інтенційно-орієнтованих мереж (IBN, Intent-based Networking), що розвивається на основі SDN рішення. Інтенційно-орієнтовані мережі – це те, що теоретизували майже 5 років, але рішення з'явилися лише нещодавно. IBN – це

автоматизований інструмент, який допомагає мережевим інженерам планувати, проектувати й керувати мережами з допомогою централізованого контролера. Це дає змогу адміністратору відійти від налаштування бажаних результатів у командних рядках, специфічних для пристрою, і замість цього використовувати природну мову або графічний інтерфейс для вираження своїх намірів. IBN все ще знаходиться в стадії розробки та є закритими для відкритого тестування, що у свою чергу привертає особливу увагу в науковому товаристві щодо розвитку майбутніх інтелектуальних IBN мереж. Серед провідних наукових досліджень авторів: Christian Esteve Rothenberg, Adeel Rafiq, Dean H Lorenz, Zheng Xu, О. Лемешко, М. Климаш, Л. Глоба останнім часом виникає одноголосне твердження, що для задоволення динамічно мінливих вимог користувачів щодо високої якості обслуговування майбутні мережі вимагатимуть комплексної інтеграції технології SDN, NFV, певної міри хмарних ресурсів, машинного навчання, нових методів управління ресурсами та програмних засобів моніторингу якістю сприйняття послуг (QoE, Quality of Experience). Відповідно інтелектуальні мережі нового покоління повинні забезпечити кінцевим користувачам доступ до мультимедійних послуг з високою якістю сприйняття у будь-який час та в будь-якому місці без обмежень за технологією та середовищем передавання. Для задоволення цих вимог необхідно розробити нові архітектури та інтелектуальні схеми для контролю та управління QoE в майбутніх мережах.

Таким чином, зростання різноманітності та обсягів інформаційних потоків в телекомунікаційних мережах, спонукають до розв’язання науково-практичного завдання підвищення якості сприйняття послуг в сучасних інфокомунікаційних системах шляхом розробки нових методів інтелектуального моніторингу стану мережі, розподілу мережевими ресурсами та управління якістю обслуговування в умовах адаптації до мінливих вимог користувачів та обмеженості мережевих ресурсів.

Зв'язок роботи з науковими програмами, планами, темами. Тематика дисертаційного дослідження виконувалась у відповідності до наукового напряму кафедри телекомунікацій Національного університету «Львівська політехніка» - «Інфокомунікаційні системи та мережі», в межах держбюджетної науково-дослідної роботи: «Розробка методів та уніфікованих програмно-апаратних засобів для розгортання енергоефективних інтенційно - орієнтованих інфокомунікаційних мереж подвійного призначення» (№ держреєстрації 0120U102201, (2020-2022 рр.)). Окрім того, дисертація виконана в межах госпдоговірної роботи «Розроблення автоматизованої системи резервного копіювання, відновлення даних та доступності серверних інфраструктур» (ГД №0679) ТзОВ " МаксіТех " (04.11.2021 р. – 20.12. 2021 р.).

Мета і завдання дослідження. Метою представленої дисертаційної роботи є підвищення показників якості сприйняття послуг шляхом розроблення інтелектуальних методів розгортання інфраструктури, моніторингу функціонування, маршрутизації та ініціації хендоверу в програмно-конфігурованих мережах на основі машинного навчання.

Досягнення поставленої мети здійснюється розв'язанням таких завдань:

1. Аналіз існуючих методів та моделей управління якістю сприйняття послуг в сучасних телекомунікаційних мережах.
2. Розроблення концептуальної моделі інтелектуальної інформаційно-комунікаційної мережі з автоматизованими методами розгортання та моніторингу функціонування на основі намірів користувачів.
3. Удосконалення методу маршрутизації інформаційних потоків на основі QoE-орієнтованої метрики.
4. Розроблення інтелектуальної система моніторингу якості функціонування програмно-конфігурованої мережі за показником QoE.
5. Розроблення методу динамічного розгортання та міграції віртуальних комутаторів між мультиконтролерами SDN на основі пріоритетного аналізу замовленої якості сприйняття послуг кінцевих користувачів.

6. Розроблення відмовостійкого контролера програмно-конфігурованої мережі для автоматизації процесу розгортання та управління якістю обслуговування.

7. Розробка та дослідження QoE-орієнтованого методу ініціації хендовера для інтелектуальних безпровідних програмно-конфігурованих мереж .

8. Практична реалізація прототипу інтелектуальної мережі та оцінювання ефективності запропонованих рішень.

9. Формування стратегічних напрямків розгортання інтелектуальних мереж подвійного призначення із забезпеченням кіберзахищеності інформаційної системи.

Об'єктом дослідження є процеси управління мережевими ресурсами та інформаційними потоками в програмно-конфігурованих мережах.

Предметом дослідження є моделі, методи та алгоритми управління якістю сприйняття послуг та розгортання інтелектуальних програмно-конфігурованих мереж.

Методи дослідження. Під час досліджень використано методи теорії графів, алгоритмів, систем масового обслуговування, оптимізації, імітаційного моделювання, математичної статистики та машинного навчання.

Наукова новизна отриманих результатів.

1. Удосконалено метод маршрутизації потоків даних в програмно-конфігурованих інтелектуальних мережах, який, на відміну від класичних алгоритмів розв’язання задач маршрутизації, що оперують лише одним чи двома параметрами оптимізації для встановлення вартості шляху, використовує адаптивну QoE-орієнтовану метрику маршруту, що автоматизовано розраховується контролером мережі на основі математичної моделі кореляції нормалізованого значення замовленого рівня якості сприйняття сервісу та прогнозованого інтегрального адитивного критерію поточних показників QoS , що дало змогу покращити якість сприйняття послуг в умовах адаптації до мінливих вимог користувачів та обмеженості мережевих ресурсів.

2. Удосконалено метод управління якістю сприйняття послуг в інтелектуальних мережах, який, на відміну від відомих, для забезпечення замовленої якості послуги базується на намірах користувачів визначених у вигляді суб'єктивних QoE оцінок, що дає змогу на основі аналізу QoE намірів проводити автоматизовано конфігурацію мережі для трафіку інжинірингу, а з допомогою алгоритму машинного навчання Randon Forest прогнозувати моменти погіршення якості сприйняття послуг для швидкої переконфігурації мережі націленої на підвищення якості обслуговування користувачів.

3. Розвинуто метод динамічного розгортання та міграції віртуальних комутаторів між мультиконтролерами SDN на основі пріоритетного аналізу замовленої якості сприйняття послуг кінцевих користувачів, що дало змогу забезпечити ефективне використання мережевих ресурсів в інтелектуальних мережах нового покоління для гарантування клієнт-орієнтованої якості обслуговування.

4. Вперше запропоновано метод ініціації хендоверу в програмно-конфігурованій безпровідній Wi-Fi мережі, який, на відміну від відомих, під час прийняття керуючого рішення щодо вибору точки доступу обслуговування орієнтується на прогнозованому значенні інтегрального критерію QoE сформованого на основі вимірювання параметрів, рівня сигналу, пропускної здатності, втрати даних та затримок у мережі Wi-Fi, що дало змогу покращити якість сприйняття послуг для кінцевих користувачів.

Практичне значення одержаних результатів полягає в тому, що:

1. Розроблено алгоритми моніторингу та аналізу мережевого трафіку, що дали змогу підвищити ефективність використання стандартних систем виявлення та запобігання вторгненню шляхом використання інтелектуальних мультифрактальних процесів аналізу вхідного трафіку. Експериментальним шляхом доведено, що використання розроблених алгоритмів в комунікаційній інфраструктурі дало змогу в умовах присутності шкідливого трафіку в каналах зв’язку зменшити втрати даних до 5%.

2. Розробка програмного модуля машинного навчання для системи моніторингу інтелектуальної мережі дозволило до 30% зменшити обсяг сигнального трафіку в каналах зв'язку між мережевим обладнанням і контролером, а також реагувати на несприятливі поєднання значень показників якості і попереджати ситуації, коли користувач незадоволений якістю отриманих сервісів для адаптивного прогнозування моменту переконфігурації мережі.

3. Комплексне використання QoE-орієнтованих методів маршрутизації та ініціації хендовера дало змогу підвищити від 3.5 до 5 показник якості сприйняття послуг, оціненого за п’ятибальною школою, де вище значення характеризує кращу якість обслуговування.

4. Розроблено програмний контролер для інтенційно-орієнтованої інтелектуальної мережі, який оснащений унікальними функціональними модулями аналізу QoE-інтенцій та моделями штучного інтелекту, використання якого дало змогу реалізувати можливості, необхідні для аналізу стану системи та пошуку оптимізованих операційних дій на основі спостережень із керованого середовища. Даний контролер надає велику перевагу та зменшує вплив людини на мережу, що збільшує швидкість реагування у процесі переконфігурації мережі в умовах погіршення якості сприйняття послуг на 10 секунд у порівнянні із відомими.

5 Запропоновано автоматизовану систему відновлення доступності серверів на яких розгортаються SDN/IBN контролер та IoT брокер, що дало змогу в умовах техногенних та природних катастрофах автоматизовано управляти ресурсами, здійснювати діагностику та відновлювати дані серверної інфраструктури з метою забезпечення безперервності роботи і високої доступності бізнес сервісів.

Розроблені науково-прикладні рішення щодо управління мережевими ресурсами, процедури хендоверу на основі QoE критерію та якістю обслуговування зможуть на практиці застосовувати науково-дослідні

організації, компанії, оператори мобільного зв’язку для покращення якості сприйняття послуг з боку користувачів у мережах із централізованим управлінням.

Результати дисертаційної роботи використано при формуванні навчальних дисциплін, що викладаються студентам (за навчальним планом) у навчальному процесі кафедри телекомунікацій Національного університету «Львівська політехніка», зокрема для студентів спеціальності 172 «Телекомунікації та радіотехніка» в курсі лекцій з дисципліни «Побудова та протоколи гетерогенних мереж мобільного зв’язку», а також у навчальному процесі спеціальності 126 «Інформаційні системи та технології» в курсі лекцій з дисципліни «Мережеві інформаційно-комунікаційні технології.

Основні результати дисертаційної роботи використано і впроваджено з метою підвищення показників якості сприйняття послуг та гнучкості управління ресурсами в телекомунікаційній корпоративній мережі ТзОВ «МаксіТех», що підтверджено актом впровадження.

Особистий внесок здобувача. Основні наукові результати дисертаційної роботи отримано автором самостійно. У працях, опублікованих у співавторстві, внесок Прислупського А.І. є вирішальним, зокрема авторові належать (нумерація згідно Додатку Б: у роботах [1] – розроблення алгоритму моніторингу трафіку для виявлення та блокування мережевих атак, [2,11] – розроблення методу управління якістю сприйняття послуг; [3,14] – удосконалення методу маршрутизації на основі показника якості сприйняття послуг, [4-7] – моделювання та дослідження ефективності впровадження методів управління ресурсами та якістю обслуговування; [8,10] – розроблення методу ініціації хендоверу в програмно-конфігурованій безпровідній мережі на основі показника якості сприйняття послуг; [9] – реалізація методу управління якістю обслуговування в програмно-конфігурованих мережах, [12,13] – метод динамічного розгортання та міграції віртуальних комутаторів між

мультиконтролерами SDN на основі пріоритетного аналізу замовленої якості сприйняття послуг кінцевих користувачів.

Апробація результатів дисертації. Основні наукові результати та положення дисертації представлені, доповідались та обговорені на 5-ми міжнародних науково-технічних конференціях та наукових семінарах: International IEEE Conferences on Advanced Information and Communication Technologie (м. Львів, 2019, 2021 рр.); Міжнародних науково-технічних конференціях «Досвід розробки та застосування приладо-технологічних САПР в мікроелектроніці» (м. Львів-Поляна, 2019.); Міжнародних науково-технічних конференціях «Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії» (м. Львів-Славське 2020, 2022 рр.). Крім цього, дисертаційна робота у повному обсязі представлена на наукових семінарах кафедри телекомунікацій Національного університету «Львівська політехніка»..

Публікації. За результатами досліджень, які викладені у дисертаційній роботі, опубліковано 14 наукових праць, з них 3 статті у наукових фахових виданнях України, 3 статті у науковому періодичному виданні інших держав, що входять до наукометричних баз Scopus/Web of Science (2 з них з індексом цитування (імпакт-фактором, квартиль Q1-Q2)), 1 стаття у науковому періодичному виданні інших держав та 2 статті у періодичному виданні України, 5 у збірниках матеріалів і тез доповідей міжнародних та всеукраїнських конференцій індексованих у наукометричній базі Scopus та Web of Science.

Структура та обсяг роботи. Робота складається з переліку умовних скорочень, вступу 4 розділів, висновків, списку використаних джерел і 2 додатків. Загальний обсяг роботи складає 277 сторінок друкарського тексту, із них 8 сторінок вступу, 228 сторінок основного тексту, 175 рисунків, 22 таблиці, список використаних джерел із 140 найменувань та 2 додатків. Додатки містять акти впровадження результатів дисертаційної роботи та список праць автора.

РОЗДІЛ 1. АНАЛІЗ МЕТОДІВ ТА МОДЕЛЕЙ УПРАВЛІННЯ ЯКІСТЮ СПРИЙНЯТТЯ ПОСЛУГ В СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

1.1 Основні поняття та характеристики якості обслуговування в сучасних телекомунікаційних мережах

Розвиток мобільного зв'язку, особливо четвертого та п'ятого покоління (4G та 5G), та поява нових технологічних пристроїв привели до масової зміни та росту обсягу даних у мережах [1]. Завдяки цим фактам важливість механізму якості обслуговування QoS в мережах не перестає зростати з роками, оскільки зросла потреба пропонувати різні типи контенту з їхніми вимогами щодо якості та безпеки [2]. Серед найбільших проблем надання QoS від пристрою до пристрою є сценарій забезпечення QoS в безпровідних мереж зв'язку, коли користувач перебуває в русі разом із різними місцями локалізації, які спричиняють суттєві зміни сигналу, що ускладнює процес якісного надання послуг [3].

Інтернет-протоколи намагаються запропонувати послугу з максимально можливою продуктивністю, тобто з найвищим бітрейтом і найменшою затримкою та втратами даних, якщо в мережі немає перевантажень. Перевантаження мережі неминуче, оскільки мережевий трафік збільшується в геометричній прогресії, а вдосконалення інфраструктури є повільним і дорогим. Таким чином, важливо впровадити наскрізну якість обслуговування для тих сервісів, які передаються в режимі реального часу, наприклад, відеодзвінки, передача голосу через Інтернет-протокол [VoIP], IPTV телебачення, IoT комунікації критичної інфраструктури або інші програми, орієнтовані на світ розваг, як потокове відео за запитом.

QoS вважається основною характеристикою мережі, оскільки без неї неможливо гарантувати обслуговування в критичних інфраструктурах або надати хорошу якість сприйняття кінцевому користувачеві. Загалом, QoS

вважається такою ж важливою, як і безпека [4]. ITU під терміном QoS розуміють сукупність характеристик телекомунікаційної послуги, які впливають на її здатність задовольняти заявлені та неявні потреби користувача послуги [5]. До основних параметрів QoS відноситься:

- Пропускна здатність: швидкість з'єднання. Пропускна здатність – це кількість успішно переданих повідомлень в одиницю часу. Вона контролюється доступною смугою пропускання, доступним співвідношенням сигнал/шум та апаратними обмеженнями. Максимальна пропускна здатність мережі може бути, відповідно, вищою, ніж фактична пропускна здатність, що досягається у повсякденному використанні. Терміни "пропускна здатність" і "смуга пропускання" часто сприймаються як одне й те саме, проте це різні поняття. Смуга пропускання це потенційний вимір каналу зв'язку, тоді як пропускна здатність це фактичний вимір того, наскільки швидко ми можемо передавати дані. Пропускна здатність вимірюється шляхом підрахунку кількості даних, переданих між декількома точками протягом певного періоду часу, зазвичай в одиницях вимірювання біт за секунду (bps), які надалі перетворилися на байти за секунду (Bps), кілобайти за секунду (KBps), мегабайти за секунду (MBps) та гігабайти за секунду (GBps). На пропускну здатність можуть впливати численні фактори, такі як перешкоди, створювані аналоговим фізичним середовищем, доступна обчислювальна потужність компонентів системи та поведінка кінцевого користувача. При врахуванні численних протокольних витрат швидкість використання даних, що передаються, може бути значно нижчою за максимально досяжну пропускну здатність. QoS може вказати маршрутизатору, як використовувати смугу пропускання. Наприклад, призначити певний обсяг пропускної здатності різним чергам для різних типів трафіку.

Максимальна пропускна здатність лінії зв'язку визначається на основі ємності інтерфейсу. На пропускну здатність шляху, впливає ділянка каналу зв’язку із низькою пропускною здатністю. Умова 1.1 пояснює вимірювання пропускної здатності на шляху, де t_p це доступна пропускна здатність для

шляху p, а t_{ij} це доступна пропускна здатність для будь-якого каналу зв'язку *(i,j)* на шляху.

$$t_p \geq \min\left\{t_{ij} \middle| (i,j) \in p\right\} \tag{1.1}$$

Доступна пропускна здатність каналу обчислюється на основі коефіцієнта використання каналу зв'язку u_{ij} та максимально можливої пропускної здатності каналу B_{ij} за умовою 1.2

$$t_{ij} \geq T_{ij} \cdot (1 - u_{ij}) \tag{1.2}$$

- Затримка: Час, який потрібно пакету, щоб пройти від джерела до кінцевого пункту призначення. На цей показник часто впливає затримка у черзі, яка виникає під час навантаження, коли пакет очікує у черзі перед передачею. QoS дозволяє організаціям уникнути цього шляхом створення пріоритетної черги для певних типів трафіку.

В телекомунікаційних мережах виникає чотири типи затримок, що формують загальну затримку в каналі зв'язку (i, j), як показано на рис. 1.1 та рівнянні 1.3.

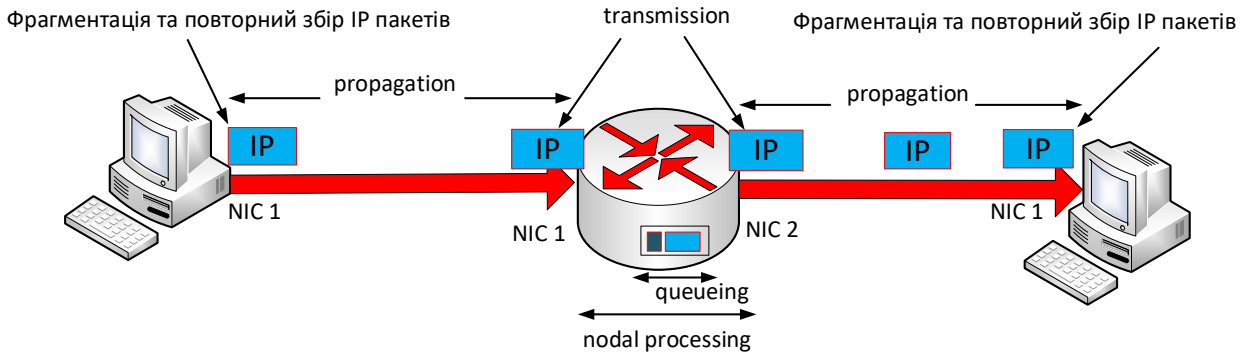


Рис. 1.1. Затримка в мережі комутації пакетів [6]

Формула для визначення загальної затримки в мережі:

$$d_{ij} = d_{Transmission} + d_{\Pr opagation} + d_{\Pr oces\sin g} + d_{Queuing} \tag{1.3}$$

Затримка передачі це час, необхідний для передачі даних по лінії зв'язку. Та визначається як:

$$d_{Transmission}\left[\sec\right]=\frac{packet.size\left[bit\right]}{link.bandwidth\left[bps\right]} \quad (1.4)$$
$$(on.the.order.of.1\times10^{-3}\sec onds)$$

Затримка поширення це час, протягом якого переданий біт переміщується з одного кінця шляху на інший кінець. Це залежить від швидкості сигналу середовища передачі та довжини лінії зв'язку (метра). Цей тип затримки є найбільш значним компонентом затримки в глобальній мережі (Wide Area Network).

$$d_{\Pr opagation}\left[\sec\right]=\frac{link.length\left[m\right]}{link.propagation.speed\left[mps\right]} \quad (1.5)$$
$$(on.the.order.of.1\times10^{-6}\sec onds)$$

Затримка обробки це час перевірки пакетів на бітові помилки та пошуку таблиці маршрутизації для визначення вихідних даних перед передачею їх у вихідну чергу. Його діапазон становить 1×10^{-6} секунд або менше, що часто є незначним для потужного мережевого пристрою мережі.

Затримка черги це час, витрачений пакетом на очікування в вихідних буферах, і залежить від інтенсивності та характеру трафіку, що надходить у черги. Затримка черги може суттєво відрізнятися від пакета до пакета, оскільки кількість раніше прибулих пакетів у черзі, які очікують на передачу через шляху, впливатиме на час очікування в черзі.

Затримка черги найскладніший компонент загальної затримки. Оскільки швидкість надходження пакетів і довжина пакетів є випадковими, прогнозування поведінки мережі та затримка черги стають складним завданням. У величезній кількості статей та книг обговорюється модель масового обслуговування за допомогою використання теорії черг, процесів Пуассона та Маркова [7], щоб зробити тривалість черги та час очікування передбачуваними в традиційній мережі IP. Ті самі методи перевіряються в середовищі SDN за допомогою експериментальних досліджень. Наприклад, автори в [8] стверджують, що модель черги M/M/1 для контролера SDN та

модель черги M/G/1 для елементів мережі можуть покращити час перебування пакетів та продуктивність системи. Залежно від моделі масового обслуговування, затримка черги дотримується різних правил та принципів. Формула 1.6 дає інтуїтивну формулу високого рівня середньої затримки черги. Середня довжина черги залежить від коефіцієнта завантаження, який є відношенням спроби швидкості передачі каналу зв'язку до максимальної швидкості передачі каналу зв'язку.

$$d_{Queuing}\left[\text{sec}\right] = \frac{packet.size\left[bits\right] \times queue.length}{link.bit.rate\left[bps\right]} \quad (1.6)$$
$$(on.the.order.of.1\times10^{-6}\,\text{sec}onds.to.1\times10^{-3}\,\text{sec}onds)$$

Отже, загальна затримка шляху від одного джерела до пункту призначення обчислюється підсумовуванням затримки на кожній ланці шляху. Формула 1.7 формулює затримку на шляху p, де d_p відноситься до затримки шляху, а d_{ij} відноситься до затримки кожної ланки (i, j), з якої складається шлях p.

$$d_p = \sum_{(i,j)\in p} d_{ij} \quad (1.7)$$

- Втрати: обсяг даних, втрачених внаслідок втрати пакетів, що зазвичай відбувається через навантаження мережі. QoS дозволяє організаціям вирішувати, які пакети в цьому випадку відкидати.

Середня втрата пакетів може залежати від багатьох точок на TCP-з'єднанні, таких як фізична помилка передачі та обмеження пропускної здатності каналу зв'язку. Розмір буфера в пункті призначення або навіть у проміжних вузлах може також вплинути на ймовірність втрати пакетів. Якщо він не був належним чином розроблений з урахуванням майже реальної швидкості надходження трафіку, вузол починає скидати пакети через перевантаження та відсутність місця в буфері черги. Тому розмір буфера може бути одним із вузьких місць у зменшенні пропускної здатності TCP. Якщо шлях має достатню пропускну здатність, доступний розмір буфера у вхідному вузлі також спричиняє обмеження.

Коефіцієнт втрати пакетів між парою вузлів розраховується за формулою 1.8:

$$Packet.loss.ratio = \frac{number.of.sent.packet.from.source - number.of.received.packet.in.destination}{number.of.sent.packet.from.source} \times 100\% \quad (1.8)$$

Якщо розглядати сучасні програмно-конфігуровані мережі то у мережевих елементах OpenFlow налаштовано три різні черги на основі підходу до класифікації послуг. Однак механізм масового обслуговування має прямий вплив на втрату пакетів різних типів класів, рівняння 1.8 може бути використано для оцінки коефіцієнта втрати пакетів на каналі зв'язку *(i, j)*:

$$pl_{ij} = \begin{cases} (T_{PQ} + T_{Q1} + T_{Q2} - b_{ij}) / (T_{PQ} + T_{Q1} + T_{Q2}), \\ 0, \end{cases} \quad (1.9)$$

$$\begin{aligned} for (T_{PQ} + T_{Q1} + T_{Q2}) > t_{ij} \\ for (T_{PQ} + T_{Q1} + T_{Q2}) \le t_{ij} \end{aligned} \quad (1.10)$$

де T_{PQ} позначає кількість пакетів, що очікують в черзі PQ, T_{Q1} як кількість пакетів, що очікують в черзі *Q1*, T_{Q2} як кількість пакетів у черзі *Q2*, а t_{ij} як доступну пропускну здатність по каналу *(i , j)*.

Втрата пакетів є мультиплікативною метрикою. Коефіцієнт втрат пакетів по шляху визначається у формулі 1.11, де pl_p відноситься до коефіцієнта втрат пакетів для шляху *p*, а pl_{ij} це відношення втрат пакетів для певної лінії зв'язку *(i,j)* шляху *p*. Коефіцієнт втрати пакетів по шляху визначається у рівнянні 1.8, де pl_p відноситься до коефіцієнта втрат пакетів для шляху p, а pl_{ij} - відношення втрат пакетів для конкретного каналу *(i, j)* шляху *p*:

$$pl_p = 1 - \prod_{(i,j) \in p} (1 - pl_{ij}) \quad (1.11)$$

Якщо коефіцієнт втрат пакетів у мережевих каналах зв’язку дуже малий і близький до нуля, міру втрати пакетів можна розглядати як додаткову міру і може бути приблизно спрощений за допомогою виразу 1.12:

$$pl_p = \sum_{(i,j) \in p} pl_{ij} \quad (1.12)$$

- Джиттер: Нерівномірна швидкість руху пакетів у мережі внаслідок перевантаження, що може призвести до того, що пакети надходять із запізненням і не по порядку. Це може призвести до спотворення або розривів у аудіо- та відеофайлах, що передаються.

1.2 Огляд моделей забезпечення якості обслуговування в традиційних мережах

Постачальники мережних послуг часто вважають за краще надмірно розширювати свої мережі замість того, щоб впроваджувати належні механізми якості послуг (QoS), які дозволяють диференціювати трафік та забезпечувати передбачувану якість [10]. Така тенденція до надмірного надання ресурсів не є стійкою з тієї простої причини, що мережеві ресурси обмежені. Отже, щоб протистояти цій тенденції, існуючі механізми QoS повинні стати більш простими у розгортанні та експлуатації, щоб мотивувати провайдерів використовувати методи QoS замість надмірного надання ресурсів [11].

Мережеве обладнання з фіксованими функціями, таке як комутатори та маршрутизатори, є основою традиційної мережі. Кожен із цих пристроїв виконує певну роль, яка добре поєднується з іншими та допомагає підтримувати роботу мережі.

Традиційні мережі постійно стикаються із проблемою гнучкості [12]. Формалізований набір визначень для взаємодії програмного забезпечення (API Application Programming Interface), для надання послуг нечисленні, а більшість комутаційного обладнання та програмного забезпечення є конфіденційними. Традиційні мережі часто ефективно працюють із пропрієтарним програмним забезпеченням; однак це програмне забезпечення не може бути змінено так швидко, як це необхідно проводити під динамічні вимоги користувачів.

Традиційні функції мережі зазвичай виконуються спеціалізованими пристроями, такими як комутатори, маршрутизатори і контролери доставки додатків, які використовують один або кілька комутаторів. Традиційні мережеві

функції переважно реалізуються у спеціалізованому устаткуванні, такому як інтегральні схеми, орієнтовані конкретні додатки (ASIC) [13]. Обмеження традиційної мережі, орієнтованої на апаратне забезпечення, є одна із її недоліків.

Для традиційних мереж існують три моделі якості обслуговування [14-18]:

Рис.1.2. Основні моделі QoS

Інтегровані модель обслуговування послуг — це структура, яка призначена для забезпечення гарантій якості обслуговування в IP-орієнтованих середовищах для окремих сеансів. Дана модель використовує протокол резервування ресурсів [RSVP]. RSVP зазвичай реалізується в маршрутизаторах. Ці маршрутизатори містять бази даних із записами ресурсів, доступних у кожен момент [19]. Домен IntServ поширюється від хоста до вузла призначення, кожен маршрутизатор на маршруті між хостом і гостем повинен резервувати ресурси для забезпечення QoS, коли відбувається виклик RSVP. Ці ресурси зазвичай мають пропускну здатність.

Диференційовані модель обслуговування послуги [20], на відміну від IntServ, ділять інтернет-трафік на різні класи, призначаючи кожному класу різні

пріоритети та QoS. Пропонуючи масштабованість, гнучкість, простішу сигналізацію ніж RSVP та пріоритезацію трафіку.

Слід згадати суттєві відмінності:

- DiffServ має кращу масштабованість, ніж IntServ, оскільки підтримувати стани на маршрутизаторах, коли середовище є високошвидкісною мережею, є складним завданням.
- Сигналізація набагато простіше за допомогою DiffServ, ніж RSVP [IntServ]. Від простих функцій у базовій мережі до більш складних функцій ідентифікації, формування та видалення в граничних маршрутизаторах.

Технологія MPLS призначена для прискорення комутації пакетів в транспортних мережах. Основною відмінністю цієї технології від розглянутих раніше в тому, що *MPLS* не є технологією забезпечення якості обслуговування, а стає нею тільки при використанні протоколу *RSVP TE (Resource ReSerVation Protocol Traffic Engineering)* [22] і має назву *MPLS TE*. Ця технологія поєднує техніку віртуальних каналів та функціональність стеку *TCP/IP (Transmission Control Protocol/IP).* Поєднання відбувається за рахунок того, що один мережевий пристрій, який називається комутуючим по мітках маршрутизатором *(Label Switch Router, LSR),* виконує функції *IP*-маршрутизатора та комутатора віртуальних каналів. Протоколи маршрутизації використовуються для визначення топології мережі, а для передавання даних в межах мережі одного постачальника послуг застосовується техніка віртуальних каналів. На границі мережі *MPLS TE* маршрутизатори позначають пакети спеціальними мітками, які визначають подальший маршрут просування пакета до місця призначення. В результаті аналізуються не адреси *IP*, а короткі цифрові мітки, що значно знижує мережеву затримку та вимоги до продуктивності маршрутизаторів. Шляхи комутації по мітках, які в цій технології називаються *TE*-тунелями, не прокладаються автоматично. *TE*-тунелі прокладаються тільки за ініціативою адміністратора мережі.

MPLS TE підтримує тунелі двох типів:

- строгий ТЕ-тунель (визначає всі проміжні вузли між двома граничними пристроями мережі);
- вільний ТЕ-тунель (визначає тільки частину проміжних вузлів від одного граничного пристрою до іншого, а інші проміжні вузли обираються пристроєм LSR самостійно).

Якщо для з'єднання потрібна гарантія визначеного рівня якості, то для розподілу міток використовується протокол *RSVP-TE,* і на маршруті резервуються необхідні ресурси. В *RSVP-TE* передбачені контроль та оновлення встановленого з'єднання, тобто, у випадку пошкодження в мережі, можна динамічно перевести потоки навантаження на резервний маршрут . Основною метою технології є досягнення збалансованого завантаження всіх ресурсів мережі, однак при цьому також створюється основа для надання транспортних послуг з гарантованими параметрами *QoS*, так як навантаження по *TE*-тунелях передається з дотриманням деякого максимального рівня коефіцієнта використання ресурсів, що в свою чергу впливає на процес утворення черги, отже потоки даних передаються з деяким гарантованим рівнем *QoS.* Щоб забезпечити параметри *QoS* для різних класів навантаження, постачальнику послуг необхідно для кожного з них встановити в мережі окрему систему тунелів. Технологія *MPLS TE* стандартизована, характеризується високою масштабованістю та розглядається як найперспективніша для передачі навантаження *IP* [23] .

Останні досягнення у галузі мережевих технологій спрямовані на спрощення побудови та управління мережами. Software Defined Networking (SDN) являє собою такий зсув парадигми, який докорінно змінює архітектуру мережевих пристроїв і, як наслідок, усієї комунікаційної мережі [24-26]. Зокрема, SDN сприяє розподілу площини управління та даних у мережевих пристроях. Такий розділ дозволяє централізувати логіку управління в структурі під назвою SDN Controller (SDNC). Таким чином, мережні пристрої стають

простими елементами пересилання, які обробляють пакети даних відповідно до вказівок логіки, що знаходиться в SDNC.

Традиційні мережеві архітектури мають розподілену логіку площини управління, яка добре інтегрована і пов'язана з функціями площини даних у мережевих пристроях. Операції управління традиційними мережевими пристроями зазвичай виконуються через інтерфейс командного рядка (CLI) [27]. У цьому відношенні SDN вносить значні зміни, дозволяючи SDNC програмно керувати поведінкою пристроїв пересилання. Більш того, завдяки централізації логіки управління, SDNC має глобальний погляд на всю мережу, що дозволяє йому використовувати ресурси площини даних більш ефективно, ніж за наявності лише локальних знань, як це роблять традиційні мережеві пристрої. Використовуючи програмування та глобальне бачення мережі, SDN може спростити роботу мережі, а також підвищити ефективність використання мережевих ресурсів [28-30].

1.3 Принципи та переваги функціонування програмно-конфігурованих мереж (SDN) та віртуалізації мережевих функцій (NFV)

SDN відрізняється від традиційних мереж тим, що вона заснована на програмному забезпеченні, тоді як традиційні мережі зазвичай базуються на апаратному забезпеченні. SDN гнучкіша, оскільки вона заснована на програмному забезпеченні, що дає користувачам більше можливостей та зручності в управлінні ресурсами практично на всій площині управління [31]. Традиційні мережі, з іншого боку, створюють з'єднання та керують мережею за допомогою комутаторів, маршрутизаторів та іншої фізичної інфраструктури.

Північний інтерфейс на контролерах SDN взаємодіє з API. Завдяки цьому зв'язку замість використання протоколів, необхідних традиційними мережами, розробники додатків можуть безпосередньо програмувати мережу [32].

SDN дозволяє IT-адміністраторам спрямовувати мережеві канали та проактивно організовувати мережеві послуги, дозволяючи користувачам

постачати нові пристрої за допомогою програмного забезпечення, а не фізичної інфраструктури. SDN, на відміну традиційних комутаторів, також може ефективніше з'єднуватися з мережевими пристроями [33].

Основну різницю між SDN і традиційними мережами можна простежити з прикладу віртуалізації. Увипадку віртуалізації всієї мережі за допомогою SDN, можна отримути абстрактну копію фізичної мережі, якою можна керувати з одного місця [34].

У традиційній мережі, з іншого боку, фізичне розміщення площини управління ускладнює IT-адміністратора управління потоком трафіку. У SDN площина управління стає програмною, що робить її доступною через підключений пристрій. Такий доступ дозволяє IT-менеджерам краще керувати потоком трафіку з централізованого інтерфейсу користувача (UI). Користувачі отримують більше контролю над тим, як працюють та налаштовуються їхні мережі завдяки цьому єдиному місцю. Оскільки SDN дозволяє IT-адміністраторам надавати ресурси та пропускну здатність у міру необхідності без необхідності інвестувати у додаткову фізичну інфраструктуру, він став популярною альтернативою традиційним мережам [35]. Для розширення пропускної здатності традиційні мережі вимагають нового устаткування.

Типове уявлення архітектури SDN включає три рівні: прикладний рівень, рівень управління і рівень інфраструктури (рис.1.3). Ці рівні взаємодіють між собою за допомогою північних та південних інтерфейсів прикладного програмування (API) [36].

Прикладний рівень містить типові мережеві програми або функції, які використовуються організаціями. Сюди можуть входити системи виявлення вторгнень, балансування навантаження чи брандмауери [37]. Якщо у традиційній мережі використовується спеціалізований пристрій, наприклад, брандмауер або балансувальник навантаження, то в програмно-визначуваній мережі пристрій замінюється програмою, яка використовує контролер для керування поведінкою площини даних.

Рівень управління є централізованим програмним забезпеченням контролера SDN, яке діє як мозок програмно-визначуваної мережі. Цей контролер розміщується на сервері та управляє політиками та потоками трафіку CI. у всій мережі.

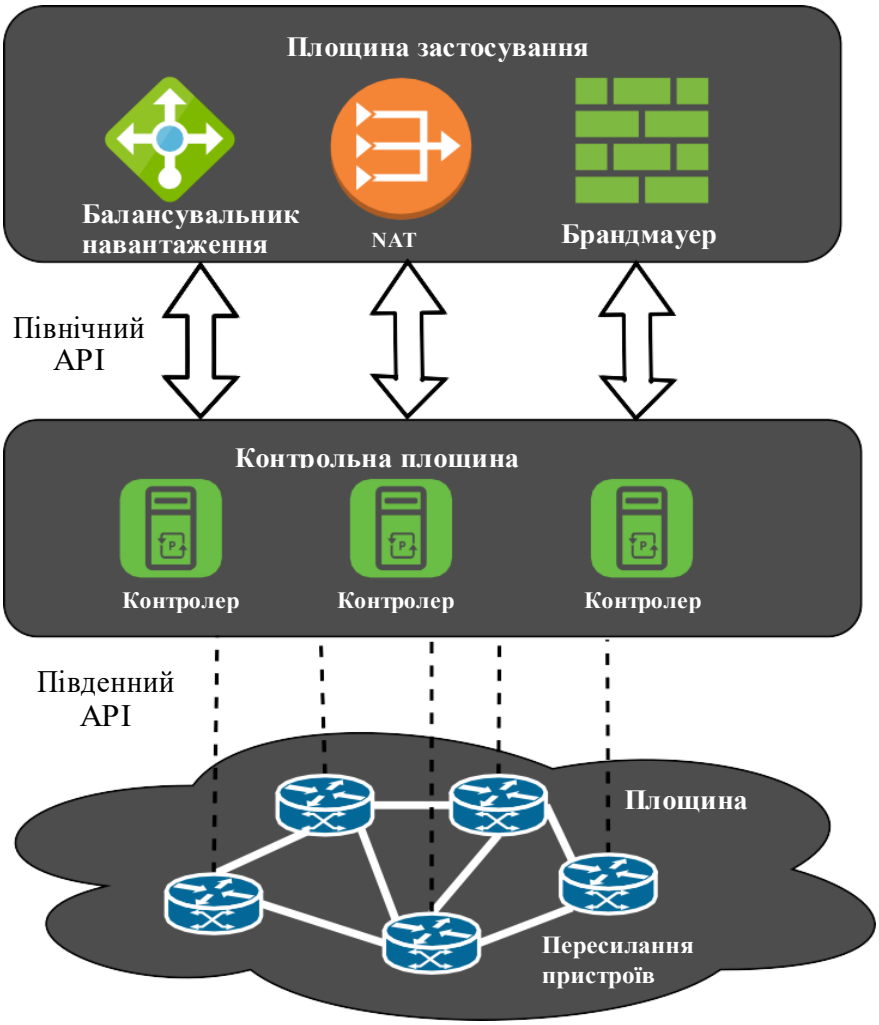


Рисунок 2.3: Спрощен Рис.1.3. Базова архітектура мереж SDN

Інфраструктурний рівень складається з фізичних комутаторів у мережі. Ці комутатори спрямовують мережевий трафік за призначенням.

Ці три рівні взаємодіють між собою за допомогою відповідних північних та південних API. Програми спілкуються з контролером через його північний інтерфейс. Контролер та комутатори взаємодіють за допомогою південних інтерфейсів, таких як OpenFlow, хоча існують інші протоколи [38]. В даний час не існує офіційного стандарту для північного інтерфейсу API контролера, який

відповідав OpenFlow як загальному південному інтерфейсу. Цілком імовірно, що API північного напрямку контролера OpenDaylight з часом може стати стандартом де-факто з огляду на його широку підтримку постачальниками [39].

Розвинута архітектура SDN представляє роз'єднану архітектуру, в якій логіка площини управління централізована в об'єкті під назвою SDN Controller (SDNC), в той час як площина даних залишається розподіленою як прості елементи пересилання. Ця розділена архітектура, проілюстрована на рис. 1.4, містить три логічні площини (також називаються шарами): площину даних, площину контролера та площину застосування. Нижче наведено короткий огляд архітектури [40].

Ключовим компонентом архітектури SDN є інтерфейс між площиною даних, що містить пристрої пересилання, і SDNC (рис. 1.4). Цей інтерфейс називається інтерфейсом даних до контролера (D-CPI) [4]. Найбільш часто використовуваним протоколом на D-CPI для реалізації архітектури SDN є OpenFlow (OF) [41]. Через OF SDNC інструктує пристрої пересилання про те, як обробляти пакети даних, якщо пристрої підтримують протокол OF.

Усередині SDNC логіка керування часто поділяється на кілька модулів, кожен з яких має чітко визначене призначення (рис. 1.4). Більше того, ці модулі пропонують послуги для кожного іншого модуля в SDNC, надбудовуючи один одного для створення повної логіки рівня управління. На рис. 1.4 показана загальна архітектура контролера, проте репрезентативна для багатьох існуючих реалізацій SDNC [42]. На найнижчому рівні в SDNC є модуль OF, який реалізує протокол OF для реалізації зв'язку з площиною даних в D-CPI. Іншим типовим модулем в існуючих SDNC є менеджер топології, який підтримує логічне представлення базової інфраструктури площини даних. Це логічне представлення топології створюється шляхом використання протоколу OF для виявлення зв'язків між пристроями пересилання OF. Інші модулі зазвичай будуються на основі основних функцій, наданих цими двома модулями, описаними вище. Наприклад, модуль пересилання (forwarding) на рис.1.4.

інструктує пристрої площини даних про те, як пересилати потоки трафіку, надсилаючи пристроям команди OF, таким чином, використовуючи модуль OF. Крім того, модуль маршрутизації (routing) використовує логічне представлення топології, яке підтримується менеджером топології, для обчислення маршрутів передавання даних в мережі [43]. Крім того, модуль маршрутизації використовує функції, надані модулем пересилання, для налаштування обчислених маршрутів у площині даних. Іншими прикладами, які зображені на рис. 1.4, є модуль брандмауера та модуль, який може надавати пропускну здатність за запитом (BoD) [44-46].

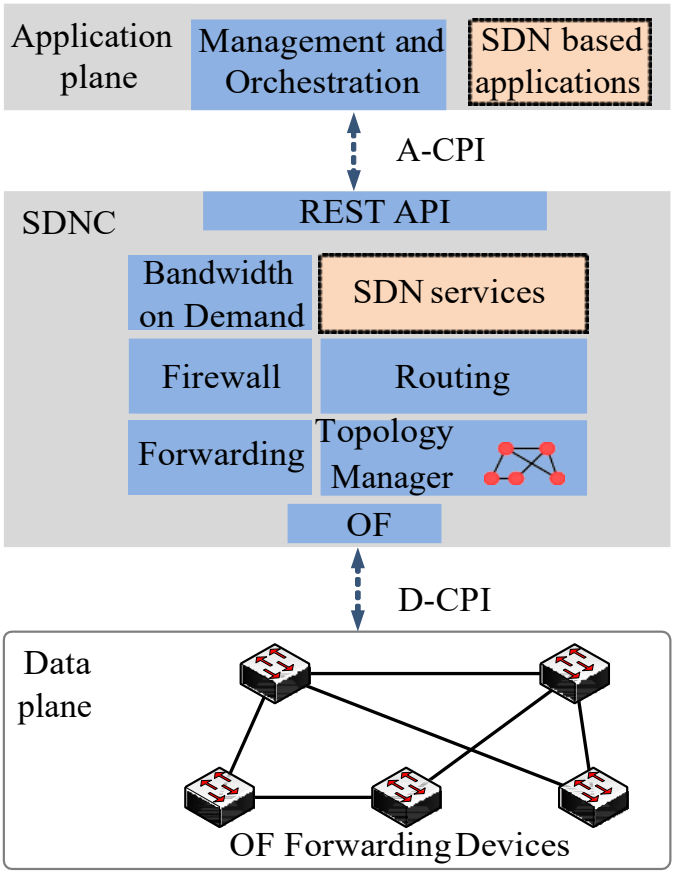


Рис 1.4. Розвинута архітектура SDN
Figure 2.1: SDN architecture

Враховуючи, що деякі з цих модулів забезпечують розширені функції, такі як брандмауер і резервування пропускної здатності, їх називають розширеними послугами SDN. По суті, вони надають певні мережеві послуги в архітектурі

SDN. Більше послуг SDN можна створити всередині контролера на основі функцій, доступних для існуючих модулів SDNC.

Площина програми містить програми на основі SDN, які використовують функціональні можливості, надані SDNC. Ця взаємодія між програмами на базі SDN та контролером увімкнено через інтерфейс площини від програми до контролера (A-CPI). A-CPI зазвичай реалізується в існуючих реалізаціях SDN як інтерфейси прикладного програмування (API) для передачі стану репрезентації (REST) (рис 1.4) [46]. На рис. 1.4 зображено приклад програми SDN для керування та оркестрування мережевих послуг. Ця програма буде орієнтована на адміністраторів, але також може надавати власні API для взаємодії з іншими об’єктами.

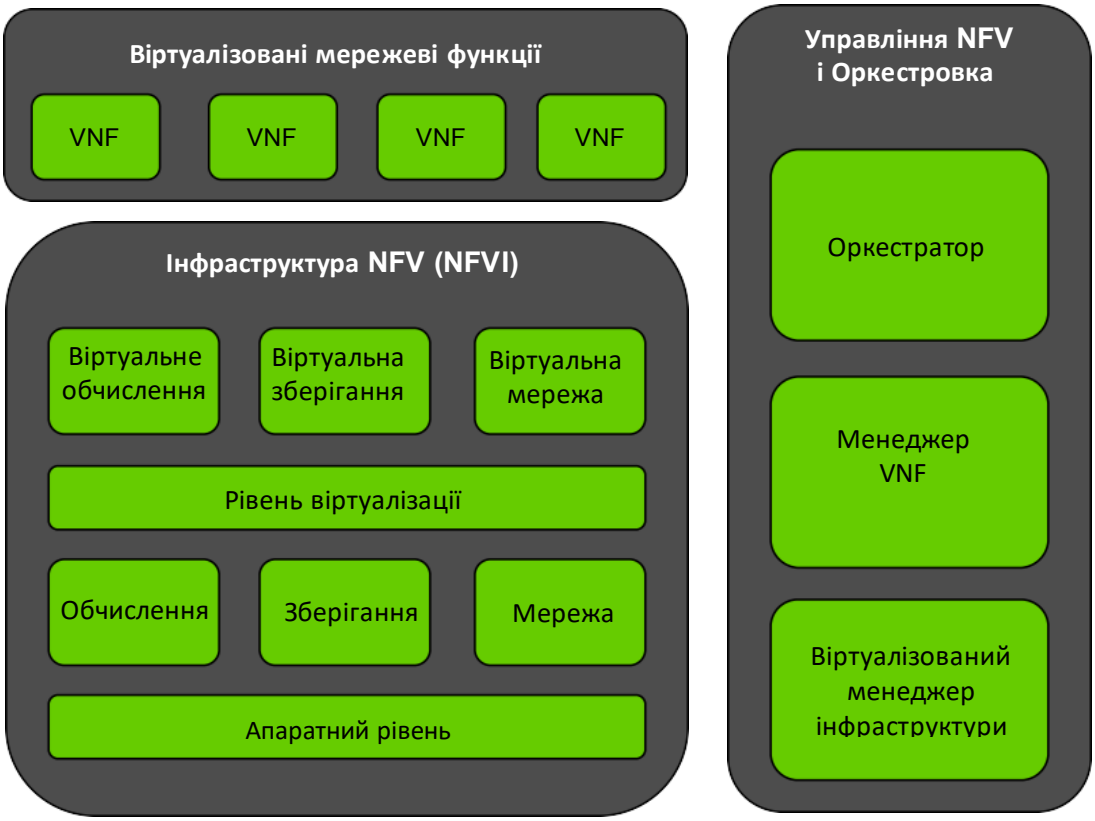
Як загальне зауваження, важлива відмінність між традиційними мережевими архітектурами та SDN полягає в організації функціональних можливостей рівня даних, контролю та управління [47]. Площина даних чітко визначена в SDN і містить функціональні можливості пересилання пакетів, подібні до традиційних мережевих пристроїв (рис. 1.4). Однак функціональні можливості рівня контролю та керування не розділені чітко і зазвичай реалізуються як спеціальні модулі в SDNC або як програми SDN у площині програми. У таких випадках SDNC стає платформою, яка містить звичайну логіку керування, а також додаткову функціональність, навіть функції керування мережею, побудовані на основі логіки рівня керування. З цієї причини термінологія, що використовується для позначення SDNC, є площиною контролера, а не площиною керування.

Отже, якщо коротко, обмеження застарілих мереж[48]:

- Запатентовані механізми конфігурації мережевих пристроїв постачальників.
- Складність конфігурації для відображення конкретних мережевих політик.
- Майже немає механізмів реагування на зміни мережі.

- Перешкода для інновацій.
- Відсутність гнучкості для негайного застосування нових технологій, таких як IPv6.
- Збільшення операційних та капітальних витрат.

NFV — це концепція мережевої архітектури, яка відокремлює функції мережі від відповідного спеціалізованого обладнання, що робить їх більш модульним блоком, який можна розгорнути або зв’язати для створення мережевої служби. Необхідність відокремити функції мережі від мережевих пристроїв виникає, коли використання нових послуг у мережі стає складнішим, оскільки попит на мережу зростає. У застарілій мережі існує багато середніх блоків, тісно пов'язаних з однією або кількома пов'язаними мережевими службами. Зокрема, проміжні блоки — це мережні об’єкти або пристрої, які здатні передавати, трансформувати, фільтрувати, перевіряти або контролювати мережевий трафік, щоб краще керувати мережею [49].



Малюнок 2.4: Спрощена архітектура NFV від ETSI [3].

Рис.1.5. Спрощена архітектура NFV

Технічно всі функції мережі, які пропонуються застарілими мережевими пристроями, можна віртуалізувати і назвати функцією віртуалізованої мережі (VNF). VNF можуть бути створені та розгорнуті в будь-яких об’єктах інфраструктури NFV (NFVI). VNFs можуть бути пов'язані разом, щоб утворити спеціалізовані мережеві послуги для забезпечення необхідних і різноманітних запитів користувачів. Переваги NFV підсумовані нижче:

- Гнучкість у впровадженні нових мережевих послуг.
- Незалежне розгортання від постачальника з COTS.
- Висока масштабованість.
- Скорочення часу на розгортання нових послуг у мережі.
- Зменшення капітальних витрат та операційних витрат.
- Висока продуктивність і управління мережею шляхом розподілу ресурсів на вимогу.

1.4 Необхідність розробки нових моделей управління якістю сприйняття послуг для сучасних та майбутніх телекомунікаційних мереж

Вимірювання якості обслуговування (QoS) з використанням мережевих параметрів (наприклад, пропускної здатності, втрати пакетів, затримки та джиттера) розглядалися протягом багатьох років для визначення рівня задоволеності користувачами послуги. Хоча QoS вказує на рівень якості функціонування мережі, він не обов'язково кількісно визначає сприйняття та рівень задоволеності користувачів [50]. Тому в останні роки вимірювання на основі показника якості сприйняття послуги QoE, крім метриків QoS, широко використовуються на практиці для оцінки якості мультимедійних послуг [51]. QoE враховує суб'єктивне ставлення користувача до конкретної послуги. QoE визначається як "ступінь задоволення або роздратування користувача від перегляду послуги [52]. Розуміння очікувань та сприйняття користувачів від послуги є важливим для провайдерів з точки зору надання кінцевих послуг [53].

QoE в цьому контексті можна визначити як загальне вимірювання продуктивності мережевої системи, яке залежить від прийнятності послуги з точки зору користувача. Наприклад, середня оцінка думки (MOS) — це показник QoE, що забезпечує уявлення користувача про якість мережі [54]. Зокрема, MOS – це середнє арифметичне всіх індивідуальних балів, отриманих за результатами суб'єктивних тестів, і може варіюватися від 1 (найгірший) до 5 (найкращий). Тут MOS забезпечує кількісний аналіз більш загальної форми QoE, тоді як QoS — це фактична пропускна здатність, яку мережа пропонує користувачеві. Значення кожної оцінки проілюстровано в таблиці 1.1 з точки зору якості та погіршення. Зокрема, якість варіюється від поганого, що відповідає дуже дратівливому погіршенню, до відмінного, що відповідає непомітному погіршенню сприйняття послуги. Розширене відображення QoE описано в таблиці 1.1.

Таблиця 1.1

Середні оцінки та відповідні якості, порушення та відео

MOS/QoE	Якість	Погіршення сприйняття	Відео 720p, 24 кадри в секунду
5	Відмінно	Непомітний	>9 Мбіт/с
4	Добре	Відчутно, але не дратує	5,8-9 Мбіт/с
3	Задовільно	Трохи дратує	4,5-5,8 Мбіт/с
2	Погано	Дратує	3,4-4,5 Мбіт/с
1	Неприйнятно	Дуже дратує	3,4 Мбіт/с

Попит кінцевих користувачів на послуги з найкращою якістю від постачальників послуг викликав тенденцію серед традиційних та майбутніх мереж до використання QoE в управлінні мережею за допомогою ефективного використання мережевих ресурсів. Для того, щоб задовольнити вимоги кінцевих користувачів до QoE та їх очікування, кілька питань QoE (наприклад, моніторинг QoE, контроль та управління QoE) створюють проблеми для постачальників послуг [55]. Такі проблеми обумовлені існуючими технологіями, які або не здатні адаптуватися до різноманітних умов мережі, або

обмежені в доступних ресурсах. Крім того, існуючі підходи до адаптації QoE обмежують здатність мережі надавати інтелектуальні та ефективні рішення, оскільки вони реагують лише при виникненні проблеми, що призводить до неоптимальної продуктивності мережі. Ці проблеми вимагають узгодження інтеграції передових інтелектуальних архітектур у майбутніх мережах із розробкою інтелектуальних механізмів адаптації з урахуванням QoE [56]. Тому функції з підтримкою QoE, такі як QoE-орієнтована маршрутизація, моніторинг QoE-доступу, розподіл ресурсів і механізми хендоверу в майбутніх мережах повинні бути адаптивними до умов мережі, що змінюються, для поліпшення QoE кінцевих користувачів.

Важливо згадати та уточнити відмінності та взаємозв'язки між QoS, якістю досвіду [QoE] та продуктивністю мережі [NP], детальна схема показана на рис.1.6.

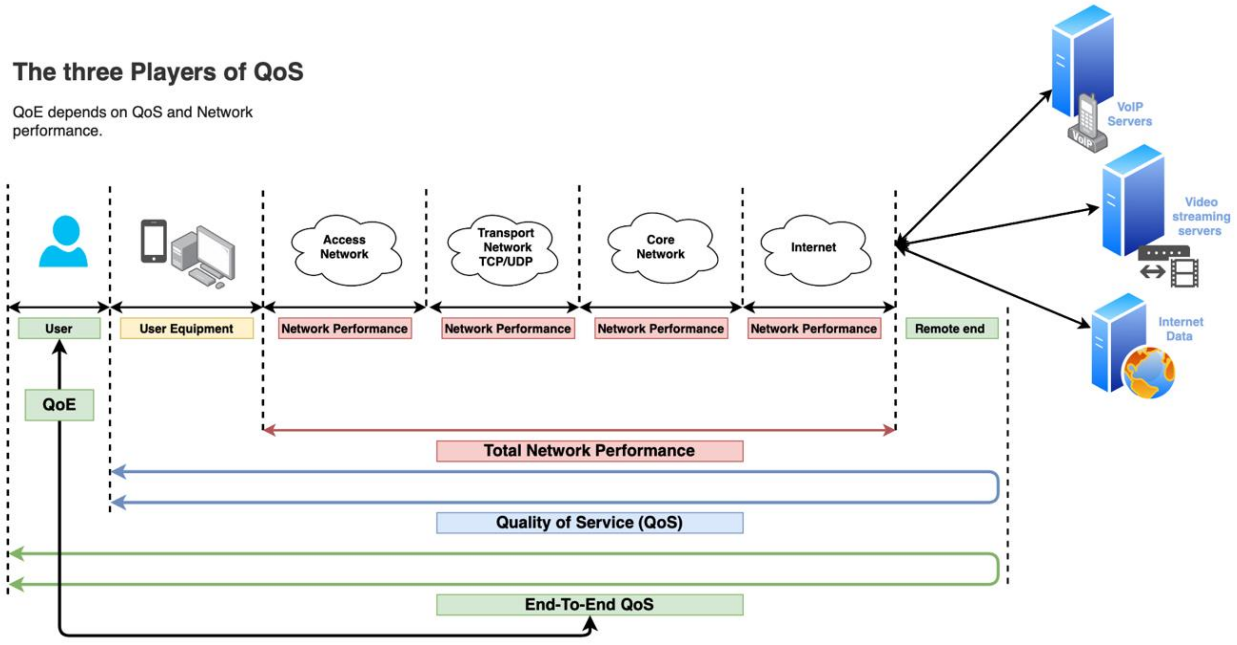


Рис.1.6. Параметри QoS, QoE та Network Performance, зображені в мережевій інфраструктурі [57]

Сьогодні кінцеві користувачі звикли до більш вимогливих ресурсів послуг з кращою якістю від постачальників послуг (SP). Однак досягнення хорошої

якості обслуговування (QoE) є складним завданням через різні клієнтські пристрої/шаблони запитів, змінюваного медіа-місту та змінних умов передачі/мереж. Як у наукових колах, так і на практиці були докладені великі зусилля для оптимізації ланцюжка доставки відеоконтенту та підвищення якості обслуговування кінцевих користувачів. Деякі з поширених механізмів, що використовуються для покращення QoE кінцевих користувачів, засновані або на оптимізації мережі (наприклад, розподіл мережевих ресурсів з урахуванням QoE та маршрутизація з урахуванням QoE), або на запитах/відповідях клієнт-сервер (наприклад, адаптивна потокова передача відео з урахуванням клієнта) та маршрутизації з урахуванням QoE [58-64].

1.5 Аналіз наукових робіт в напрямку розвитку методів управління якістю сприйняття послуг в інформаційно-комунікаційних мережах

Зростання попиту серед користувачів високої якості сприйняття послуг спонукали операторів зв'язку модернізувати свої системи та інвестувати в нові передові парадигми трансформації мереж, такі як програмно-конфігуровані мережі (SDN), віртуалізація мережевих функцій (NFV), граничні обчислення (EC) та хмарні/туманні обчислення (C/FoC). Ця трансформація та модернізація їх систем також обумовлені зростаючим тиском нових сценаріїв використання, починаючи від відео з розширенням (4K/8K), комунікацій машинного типу (MTC) і масового Інтернету речей (MIoT) [65]. З цією метою нові парадигми, такі як SDN та NFV, були визначені як критичні технології для забезпечення програмованого, централізовано-керованого, адаптованого та економічно-ефективного управління мережею в майбутньому. Дійсно, SDN та NFV можуть дозволити автоматизувати управління мережею та забезпечити виконання вимог кінцевого користувача до QoS/QoE, а також угод про рівень сприйняття (ELA, Experience Level agreement) у гетерогенних середовищах [66].

Що ще важливіше, SDN та NFV можуть забезпечити наскрізне оркестрування ресурсів, інфраструктури та послуг у багатопрограмному

домені, що належить різним операторам або постачальникам послуг. У зв'язку з цим ведуться дослідження, наскільки майбутні мережі та різні допоміжні технології можуть бути програмно-конфігуровані з інтелектуальним управлінням ресурсів. Відповідно до науково-дослідницької діяльності, що відбувається в теперішній момент часу існує нагальна необхідність вивчати і досліджувати побудову інтелектуальних мереж нового покоління розгорнутих на основі SDN /NFV на предмет того, як вони вносять значні зміни в роботу, управління та надання послуг з урахуванням QoE.

Концепція QoE може стати однією з ключових провідних структур контролю якості майбутніх мереж [67]. Безпосередньо пов’язаний із суб’єктивним сприйняттям кінцевого користувача інформаційних сервісів, QoE дозволяє глибше, більш цілісно уявляти змінні, які впливають на функціональність мережі, доповнюючи традиційні уявлення, засновані на технічних показниках, таких як якість обслуговування (QoS).

Хоча QoE залежить від QoS, звичайні методи планування та управління мережею, які покладаються виключно на оптимізацію ключових показників ефективності мережі (KPI) для покращення якості обслуговування, недостатні для задоволення різноманітних вимог в парадигмі майбутніх інтелектуальних мереж. Конфігурація та оптимізація мережі на основі машинного навчання ML, навпаки, має потенціал для максимізації рівня QoE мережі, одночасно задовольняючи вимоги до обслуговування в умовах мінливих вимог користувачів [68].

У цьому підрозділі розглядаються сучасні результати та обговорюються нові відомі наукові підходи та проблеми, пов’язані з керуванням QoS/QoE за допомогою ML для майбутніх мереж. У світлі зростаючих змін, таких як перехід до віртуалізованих і програмних мереж, розгортання концепції нарізки мережі та поступове зростання нових сценаріїв використання 5G породжує особливу актуальність використання ML в управлінні QoE.

У статті [69] розглядається більшість досліджень SDN для підтримки наскрізних гарантій QoS, використовуючи SDN як окрему систему, яка може забезпечити та покращити функціональність QoS. Згідно з оглядом та аналізом у цій статті, існує безліч областей досліджень, в яких автономне забезпечення QoS може бути покращено. Наприклад, моніторинг мережі на основі SDN досліджувався в літературі без виміру шляху або затримок зв'язку [70]. Крім того, мало або зовсім немає робіт з маршрутизації QoS на основі вимог користувача для SDN архітектур [71-73]. Методи машинного навчання також можуть бути використані для побудови інтелектуальної QoS-маршрутизації, а також потужніших функцій аналізу для автономного забезпечення QoS [74-76].

У [77] Лі та ін. запропонували методи QoS на основі планування черг для забезпечення якості обслуговування хмарних додатків в SDN. При такому підході визначаються програми та встановлюються необхідні рівні QoS для кожного типу програм. У ньому реалізовані методи планування черг для виключення із черги даних, чутливих до затримки, та відправлення їх першими. На етапі проектування системи існує три основні модулі для контролю та управління повідомленнями.

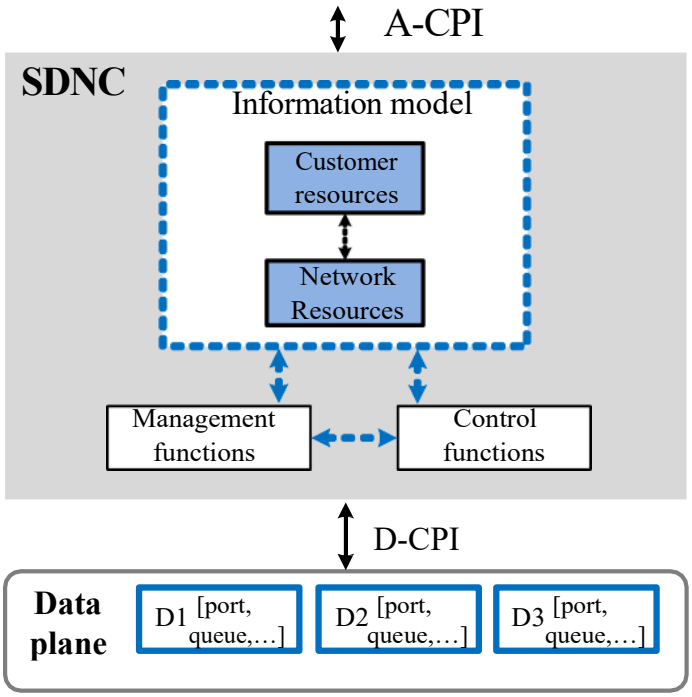


Рис.1.7. Загальна архітектура для надання послуг з підтримкою QoS

Модуль керуючих повідомлень пересилає повідомлення відповідно до правил таблиці потоків, а модуль управління чергами налаштовує черги на основі інформації про конфігурацію. Модуль планування черг розподіляє пакети з черг із різними пріоритетами. Цей підхід був оцінений за допомогою експериментального та теоретичного аналізу. Згідно з теоретичним аналізом, даний метод може забезпечити диференційоване обслуговування потоку додатків та надати різні рівні QoS. Результати показали, що за достатньої пропускної здатності інтерфейсу джерела затримка може бути знижена в середньому на 28%. Тим часом, для послуг з найбільш важливими запропонованими рішеннями затримка може бути знижена на 99,99% або більше в середньому на 90,17%, коли пропускна спроможність інтерфейсу джерела близька до максимального обмеження пропускної здатності.

Дурнер та інші [78] визначають вплив на мережевий трафік при застосуванні динамічних механізмів QoS у SDN-комутаторах із підтримкою OpenFlow. У дослідженні вимірювання супроводжуються двома принципово різними техніками QoS, названими Priority Queue та Bandwidth Guaranteeing Queue. Результат показує помітну різницю у продуктивності для різних комутаторів із підтримкою OpenFlow. З іншого боку, різні реалізації черг, тобто FIFO-черга або SFQ-черга істотно впливають на продуктивність мережі.

Один із найбільш ефективних підходів до маршрутизації потоків у SDN був запропонований у [79]. Автори розробили та впровадили централізовану детерміновану багатокритеріальну модель QoS (DMCQR) у Mininet для дослідження SDN. Результати експериментів показали, що запропонований алгоритм DMCQR має кращі показники ефективного використання коефіцієнта завантаження каналу, мінімізації втрат пакетів, пропускної здатності та затримки в порівнянні з традиційними алгоритмами та запропонованим методом багатошляхової маршрутизації для SDN [80]. Розглянувши кілька робіт з маршрутизації, можна сказати, що їх поєднує одна спільна риса:

нездатність враховувати наміри користувачів, що змінюються, щодо замовленого рівня QoS/QoE.

У роботі [81] була розроблена адаптивна схема поділу потоків для досягнення багатошляхової передачі при динамічних змінах стану мережі, використовуючи механізм тайм-ауту правил, який поставляється з використанням протоколу OpenFlow. Автори запропонували використовувати графову нейронну мережу для прогнозування затримки з'єднання, щоб допомогти адаптивному поділу потоків та інтелектуальному виборі шляхів пересилання. Результати моделювання показали, що графова нейронна мережа має гарну збіжність і узагальнюваність при прогнозуванні затримок, а механізм поділу потоків на основі тайм-ауту правил реалізує адаптивний поділ потоків відповідно до змін у стані мережі. Ця схема загалом перевищує існуючі типові рішення щодо часу обробки, наскрізної затримки, часу завершення потоку та пропускної здатності.

Більше того, SDN не має унікальної методики вимірювання, яка могла б підтвердити рівень задоволеності послуг, що надаються [82-84]. В результаті завжди існує розрив між постачальником послуг та користувачем, щоб інформація про задоволеність послуг враховувалася при прийнятті рішення про вибір постачальника послуг, що створює відсутність прозорості між постачальниками послуг та споживачами [85]. Наведені вище порівняльні дослідження також демонструють відсутність унікального стандарту якості обслуговування (QoS) SDN, який може бути адаптований до архітектури SDN на основі SOA [86]. У статті [87] наголошується, що все ще недостатньо серйозних робіт із застосування функцій автономії, таких як самоконфігурації або управління QoS/QoE на основі політик, без участі людини.

Таким чином, для забезпечення максимального надання QoS в SDN ключовою вимогою для додатків, що запитують користувачі, є дотримання послідовного процесу, який допоможе їм вести переговори, вибирати, контролювати і управляти потрібним типом мережі з провайдерами, які можуть

задовольнити їх конкретні вимоги. Якщо цей процес не дотримується, існує дуже висока ймовірність того, що мережа QoS не буде відповідати вимогам. Реалізація цього процесу для забезпечення QoS у SDN вимагає зміни парадигми у тому, як формується та керується мережа як послуга, порівняно з тим, як це робиться у традиційній SDN.

Одним із важливих етапів управління QoE в майбутніх мережах є моделювання QoE, оскільки результати моделі визначатимуть послідовність і точність наступних кроків у процедурі управління. Ці моделі враховують загальні фактори впливу та спрямовані на прогнозування загальної задоволеності кінцевого користувача [88]. Визначення вимог до мережевих послуг і впливу збоїв на якість, яку сприймає кінцевий користувач, вимагає розробки моделей для конкретних програм і відображень, які пов’язують вимірювані параметри зі значеннями QoE [89].

На відміну від ключових показників ефективності, які надають лише специфічну для мережі статистику, метрики QoE базуються на ключових індикаторах якості (KQI), серії показників, які пропонують інформацію про якість обслуговування на рівні програми показано у роботі [90]. Суб’єктивні метрики QoE часто використовуються на практиці, але їх обмеження полягає в тому, що їх оцінка займає багато часу та трудомістка і не може бути використана для моніторингу роботи в реальному часі [91]. Обмеження суб’єктивних показників збільшили потребу в реалізації об’єктивних моделей, які вимірюють або передбачають якість, яку сприймають кінцеві користувачі [92].

Концепція відображення QoS/QoE базується на обчисленні значень QoE з набору вимірюваних вхідних параметрів. Об'єктивні параметри QoS відносяться до ступеня адекватності обслуговування та включають KPI продуктивності мережі, такі як затримка, пропускна здатність, втрата пакетів і джитер. QoE можна отримати з цих показників за допомогою процесу відображення QoS/QoE, де застосовуються відповідні математичні функції.

Однак фактори впливу на QoE додатково включають суб'єктивні параметри, орієнтовані на користувача, які неможливо виміряти безпосередньо з мережі, але можуть впливати на загальну якість сприйняття кінцевого користувача [93]. Беручи до уваги не лише метрики QoS, але й фактори впливу користувача, значення QoE можна опосередковано передбачити з високим ступенем точності, використовуючи алгоритми ML (рис.1.8), щоб зіставити ці параметри з оціненими значеннями QoE [94].

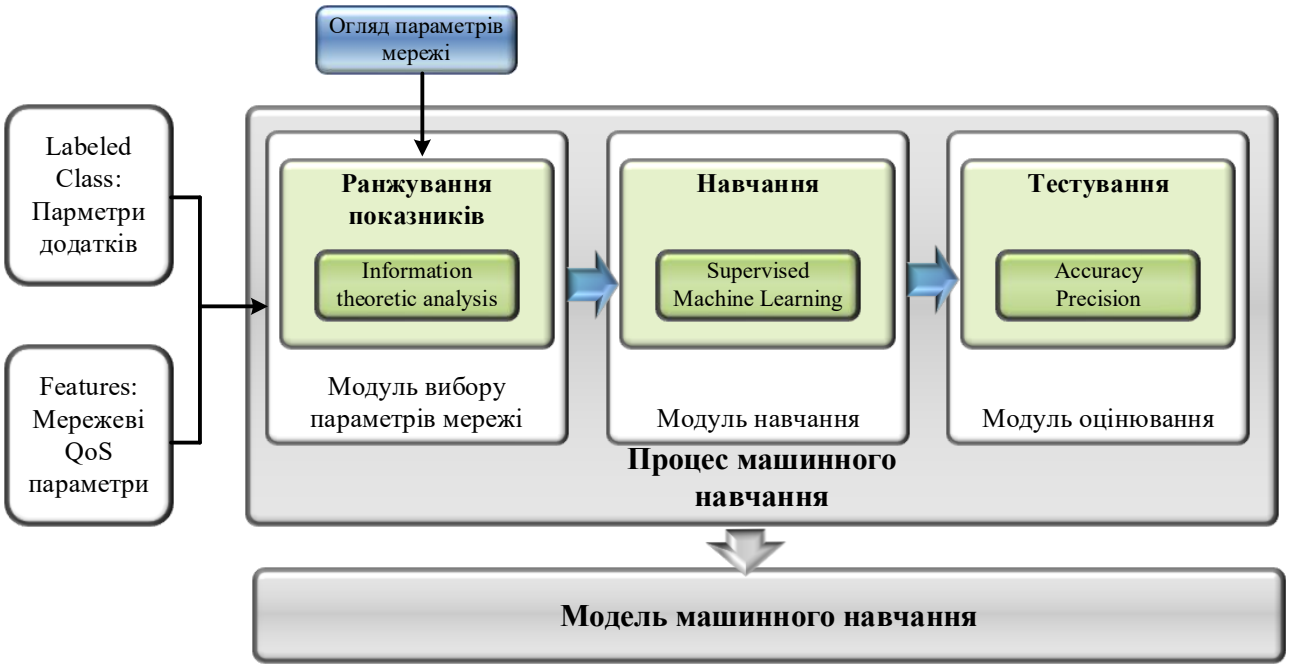


Рис.1.8. Процес машинного навчання для прогнозування параметрів функціонування мережі

Хоча метрики QoS і QoE дуже різні, вони мають високий ступінь кореляції. Тому визначення зв'язку між орієнтованими на користувача та мережевими параметрами є надзвичайно важливим [95]. Методи оцінки QoE дозволяють перевести вимоги, пов'язані з програмою, системою та мережею, у метрику QoE [96]. Теоретична та методологічна основа підтримується ML для оцінки зв'язку QoE-QoS, яка надає низку методів для побудови моделі кореляції для автоматичного прогнозування значення QoE [97].

Моніторинг QoE є однією з найважливіших процедур, які виконують провайдери, щоб забезпечити найвищу можливу якість сприйняття для своїх клієнтів. Виміряні значення використовуються для отримання уявлення про фактичний стан мережі, а також для керування трафіком і забезпечення зворотного зв'язку для виставлення рахунків і дій безпеки. Отже, необхідно гарантувати, що отримані дані є точними, щоб надати CSP чесне уявлення про якість послуг, яку відчувають кінцеві користувачі [97].

Розробка трафіку (TE) є фундаментальною проблемою мережі, враховуючи діапазон мережевих потоків із вузлами джерела та призначення, щоб знайти спосіб пересилання трафіку даних для максимізації функції корисності. Для завдань TE, таких як управління трафіком і розподіл ресурсів у складному комунікаційному середовищі мереж 5G розглянуто у роботі [98], роль ML полягає в моніторингу мережевого трафіку та визначенні найкращої політики розподілу ресурсів, забезпечуючи наскрізну (E2E) функціональність оркестровки, що включає класифікацію послуг і пріоритезацію для гарантування відповідних рівнів QoS [99-102].

У новій системі нарізки мережі вимоги до QoS послуг, що пропонуються в різних сегментах, будуть диференційовані залежно від типу зв'язку (наприклад, розширений мобільний широкосмуговий зв'язок (eMBB), зв'язок масового машинного типу (mMTC) або ультра надійний зв'язок із низькою затримкою. (uRLLC)) підтримується кожним зрізом, що робить критично важливим розробку механізму динамічного розподілу ресурсів, який контролюватиме продуктивність і використання ресурсів усіх зрізів мережі та, відповідно, розподілятиме мережеві ресурси для задоволення різноманітних вимог QoS [103]. Механізми розподілу ресурсів на основі ML запровадять інтелект у процес прийняття рішень для відповідного розподілу доступних ресурсів на зрізи мережі, так що кожен з них буде в змозі задовольнити свій необхідний рівень QoS незалежно від змін умов мережі [104].

Постійне зростання попиту на використання мультимедійних послуг через технологію Wi-Fi роблять актуальною тематикою дослідження розвитку методів ініціації хендовера в безпровідних локальних мереж (Wireless Local Area Network, WLAN), які дозволяють користувачам досягати високошвидкісної передачі даних із гарантованою якістю обслуговування [105-107]. Крім того, мобільні пристрої, такі як планшети та смартфони, також стають все більш популярними через їхню низьку вартість та простоту використання, і очікується, що зростання використання мобільних пристроїв прискориться в найближчі роки разом із доступністю та використанням таких програм, як послуги в режимі реального часу та онлайн-ігри. Як правило хендовер (handover, HO) у великомасштабних середовищах Wi-Fi вважається важливим процесом для забезпечення плавного переходу користувачів мобільних пристроїв між різними точками доступу для підтримки додатків у реальному час [108]. Саме тому у роботі розглянуто існуючі рішення, що стосуються алгоритмів та методів ініціації хендовера в безпровідних Wi-Fi. На основі аналізу відомих робіт [109-111] сформовано обмеження існуючих рішень, такі як недостатня поінформованість про вимоги кінцевих користувачів щодо якості обслуговування, а також відсутність методів моніторингу основних параметрів (Quality of service, QoS). Встановлено, що хоча деякі існуючі рішення щодо хендовера здатні охопити вимоги до продуктивності станції (Station, STA), їх реалізація часто призводить до високої складності. Більше того, такі підходи, які зосереджуються на певному показнику продуктивності та на певній безпровідній технології, не можуть бути адаптовані для підтримки інших показників продуктивності або роботи з різними безпровідними технологіями. Традиційні методи хендовера, швидше за все, не відповідатимуть вимогам мобільних пристроїв для сучасних додатків через відсутність інтелекту, недостатню обізнаність щодо якості обслуговування QoS та якості сприйняття (Quality of Experience, QoE) мобільних користувачів. Таким чином QoE також є важливим параметром, який слід враховувати при розробці

стратегій хендовера у мережах Wi-Fi, щоб гарантувати необхідну якість сприйняття послуг.

Тому розробка концептуальних архітектур, які підтримують горизонтальний хендовер за критерієм якості сприйняття послуг в однорідних мережах Wi-Fi є актуальним завданням Ця архітектура заснована на концепції програмно-конфігурованої безпровідної мережі (Software-Defined Wireless Network, SDWN), де безпровідна мережа керується централізовано, а точки доступу (Access Point, AP) програмуються. У цій архітектурі алгоритми HO допоможуть користувачам безпровідного зв'язку знайти мережу, яка найкраще підтримає вимоги додатків через політику керування якістю обслуговування (QoS) та якістю сприйняття (QoE).

Отже провівши детальний аналіз, щодо використання мережевої технології для майбутніх мереж встановлено, що SDN – це мережева парадигма, яка сприяє поділу між площиною керування та площиною даних, що дає змогу централізувати управління мережею в єдине ціле. SDN має певні особливості, які роблять його привабливим підходом до вирішення проблеми безперебійної мобільності, а саме зниження складності розгортання та конфігурування мережі, детальний моніторинг мережі та покращена масштабованість. Однією з головних особливостей функціонування SDN є можливість моніторингу та вимірювань основних параметрів якості обслуговування в режимі реального часу. Таким чином, SDN пропонує гнучкість і надійність з точки зору моніторингу мережі, що також є ключовим компонентом HO як частина фази збору інформації. Методи традиційного моніторингу та вимірювання поділяються на дві методики, пасивну та активну. Пасивні методи вимірюють мережевий трафік лише шляхом спостереження, тоді як активні методи вимірюють трафік шляхом введення додаткових пакетів у мережу та моніторингу їх поведінки. У конкретному випадку SDN контролер отримує статистику моніторингу кожного потоку через OpenFlow, який є протоколом, що використовується як інтерфейс між площиною керування та площиною

даних. Такий підхід дає змогу контролеру SDN мати загальне бачення мережі та всіх потоків, що робить моніторинг ефективнішим і в майбутньому може допомогти покращити продуктивність НО в безпровідних мережах.

На сьогоднішній день SDN використовується в багатьох середовищах, однак, знадобилося багато років, щоб розгорнути SDN також у безпровідному середовищі. Це пояснюється тим, що середовище безпровідної мережі є складнішим, ніж багато провідних мереж, через проблему динамічності перешкод між сигналами, що вимагає більшого керуючого трафіку. Більше того, збільшення споживання даних прямо пропорційне збільшення кількості користувачів і якості програми.

Проблема виконання хендоверу виникає у випадку знаходження абонента в зоні покриття двох і більше точок доступу. В класичному розумінні ініціалізація процесу хендоверу відбувається за ініціативи пристрою користувача, та перемикання відбувається до точки доступу з найкращим рівнем сигналу, якщо таку знайдено. Тобто прийняття рішення відбувається лише з врахуванням рівня сигналу точки доступу. В такому випадку система НО ігнорує потенційну точку доступу з гіршим рівнем сигналу, але з кращими параметрами QoS, як зображено на рис. 1.9.

До прикладу користувач обслуговується точкою доступу 1 з рівнем сигналу *X*, крім цього знаходиться в зоні дії точки доступу 2 з рівнем сигналу *Y*. Зважаючи що рівень сигналу AP1 кращий, користувач отримує середню якість сприйняття від наданих послуг, через велику затримку та низьку пропускну здатність на ділянці мережі AP1-Switch 1-Switch 2-Media Server. Проте ділянка мережі AP2-Switch_3-Switch_2-Media Server, через меншу завантаженість, може забезпечити кращу якість сприйняття для користувача. В такому випадку доцільним було б провести процедуру НО та перевести користувача на обслуговування до AP2.

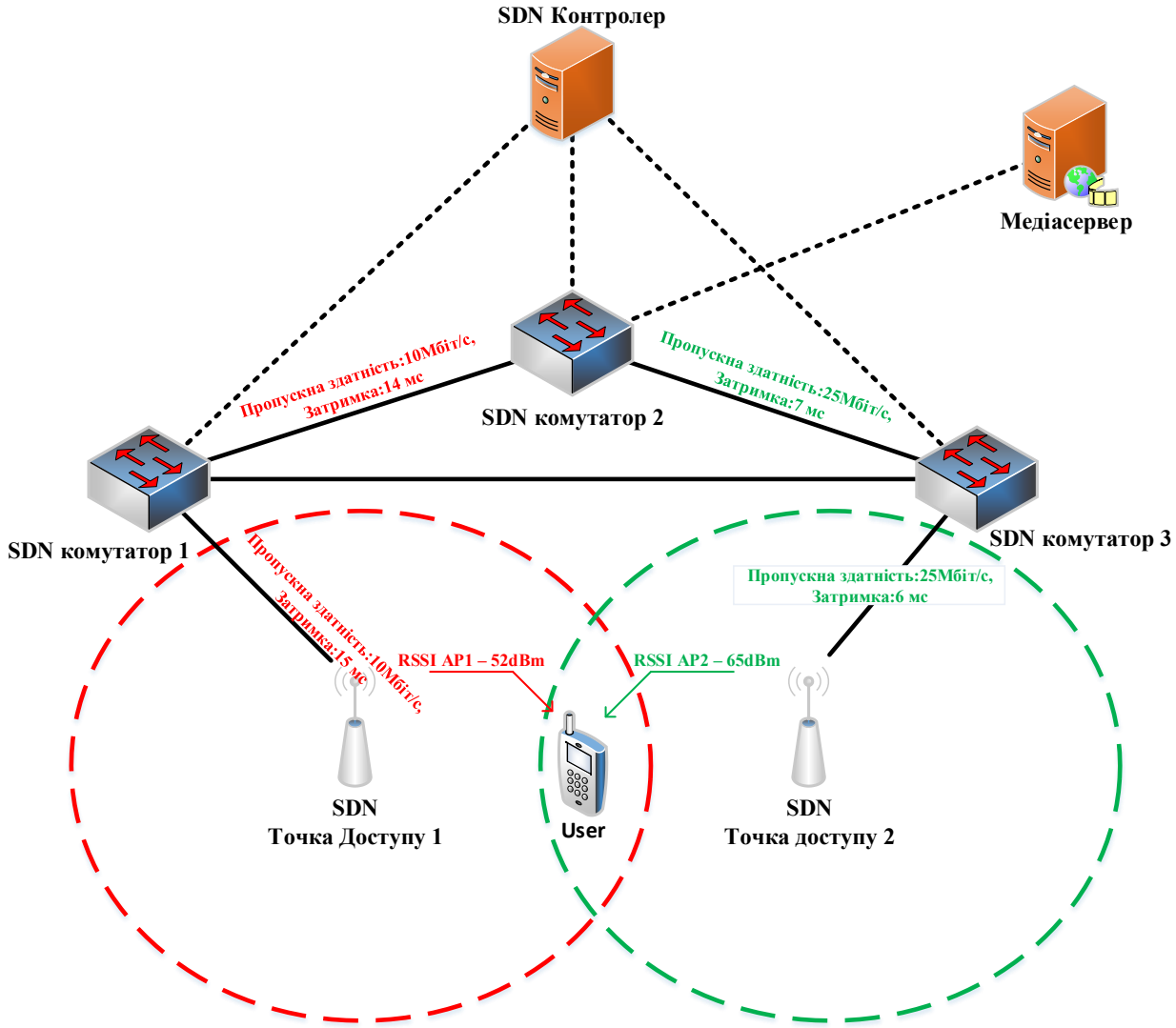


Рис.1.9. Приклад проблеми виконання HO в SDWN

Хоча існуючі програмно-конфігуровані мережі (SDN) автоматизували більшість процесів управління мережею, вони вимагають ручної участі кваліфікованих мережевих адміністраторів. Але людська участь є повільною, непостійною і часто дорогою. Поява мереж на основі намірів (IBN) вирішує вищезгадані проблеми, забезпечуючи швидке та автономне управління. IBN це концепція інтелектуального управління мережею, яка поєднує SDN, штучний інтелект (AI), ML та мережеве оркестрування для автоматизації адміністративних функцій. Ця ідея не нова, але в міру того, як автоматизація управління мережею стає більш поширеною, IBN все ще розглядається як рання

технологія. Відомо, що IBN і SDN мають багато спільного, хоча є деякі відмінності [112]. У SDN адміністратори створюють команди, які визначають імена або типи пристроїв, діапазони IP, VLAN та інші мережеві конструкції. IBN, на відміну від SDN, дає мережевим адміністраторам можливість віддавати команди контролеру з погляду бізнесу зрозумілою користувачеві мові. Потім контролер використовує штучний інтелект (AI) та ML для перекладу команд та організації завдань у набір правил управління мережею [113-115]. В даний час у IBN відсутні механізми для інтелектуального управління хендовером у безпровідних мережах, спрямовані на підвищення або задоволення замовленого QoE рівня користувачів.

1.6 Постановка науково-практичного завдання дисертаційного дослідження

На основі проведеного аналізу робіт дотичних по тематиці дисертаційного дослідження встановлено, що інформаційно-комунікаційні мережі знаходяться у центрі неминучого еволюційного переходу до цифрової трансформації суспільства. Цифровізація перетворює способи взаємодії підприємств із партнерами, співробітниками та споживачами. Продукти та послуги можуть бути налаштовані, замовлені та надіслані з веб-програми одним натисканням кнопки. Бізнес-дані збираються, аналізуються та передаються практично в режимі реального часу. Проте традиційні архітектури корпоративних мереж і центрів обробки даних важко адаптуються до вимог цього динамічного середовища. Програми переміщуються у публічні, приватні та гібридні хмарні середовища та використовуються на основі підписки, стираючи кордон між неперевіреними доменами та корпоративною мережею. Зі зростанням використання відкритого програмного забезпечення, контейнерів, мікросервісів та SDN/NFV запуск бізнес-програми тепер займає не місяці чи роки, а дні. Для співробітників та клієнтів доступ до мережі та інформації, незалежно від розташування, пристрою або часу, стає актуальною потребою для бізнесу. У

міру розвитку Інтернету речей (IoT) до мережі підключається дедалі більше датчиків та автономних пристроїв. У той же час кіберзагрози стають все більш виявленими і небезпечними для репутації та фінансового благополуччя організацій.

Традиційні архітектури та операційні процедури корпоративних мереж та центрів обробки даних повинні розвиватися, щоб йти в ногу з цими тенденціями. Зокрема, майбутні інтелектуальні мережі нового покоління мають:

- підтримувати, а не стримувати цифрові бізнес-ініціативи;
- володіти гнучкістю і швидкою адаптацією до бізнес-цілей, що змінюються;
- бути простим у створенні, експлуатації та обслуговуванні, незалежно від масштабу і складності (операційні моделі, що використовуються в даний час, не є масштабованими або стійкими);
- всебічно контролювати свою роботу, забезпечувати підтримку поточних бізнес-ініціатив та дотримання нормативних вимог, усувати неполадки та рекомендувати коригувальні дії;
- виявляти та нейтралізувати загрози безпеці до того, як вони завдадуть шкоди.

Згідно основної ідеології дисертаційної роботи така концепція мережі нового покоління отримала назву IBN, яка здатна прораховувати поведінку додатків та користувачів, навчатися та реконфігуруватися у процесі роботи з метою мінімізації експлуатаційних витрат, підвищення надійності та безпеки мережевих процесів. Очікується, що SDN відіграє свою роль у реалізації IBN, які обіцяють дати мережевим адміністраторам більший контроль над мережами завдяки поєднанню автоматизації та машинного навчання. Хоча SDN і мережі на основі намірів часто розглядаються як те саме, це різні концепції зі схожими цілями. IBN все ще знаходиться в стадії розробки та є закритими для відкритого тестування, що у свою чергу привертає особливу увагу в науковому товаристві

щодо розвитку майбутніх інтелектуальних IBN мереж націлених на підвищення якості сприйняття послуг.

Таким чином, зростання різноманітності та обсягів інформаційних потоків в телекомунікаційних мережах, спонукають до розв'язання науково-практичного завдання підвищення якості сприйняття послуг в сучасних інфокомунікаційних системах шляхом розробки нових методів інтелектуального моніторингу стану мережі, розподілу мережевими ресурсами та управління якістю обслуговування в умовах адаптації до мінливих вимог користувачів та обмеженості мережевих ресурсів.

Висновки до 1-го розділу

Розглянуто основні принципи побудови, архітектури та процеси функціонування традиційних та програмно-конфігурованих мереж. Виділено основні переваги у використанні над традиційними мережами щодо управління якістю надання послуг. Встановлено, що методи забезпечення якості обслуговування (QoS, Quality of Service) мають вирішальне значення для всіх організацій, які хочуть гарантувати найкращу якість сприйняття своїх найважливіших додатків та послуг. Традиційно центри експлуатації та обслуговування мережі використовують параметри QoS, орієнтовані на мережеві технології, такі як затримка передавання, пропускна здатність, втрати пакетів тощо, щоб вимірювати якість мережі. Проте продемонстровано, що QoS в першу чергу націлений на покращення якості обслуговування щодо технічних параметрів на рівні додатків, де недостатньо враховується фактичне сприйняття та відчуття користувача. Щоб вирішити цю проблему, введено орієнтоване на користувача вимірювання якості обслуговування з поняттям якості сприйняття послуг (QoE), яке привернуло велику увагу як в наукових колах, так і серед телекомунікаційних операторів послуг.

Загалом, оцінка QoE може здійснюватися як суб'єктивним, так і об'єктивним способом, де суб'єктивна оцінка зазвичай реалізується за

допомогою опитувальників і рейтингових шкал. Такий підхід можна розглядати як більш прямий і надійний спосіб оцінки показників QoE. Однак це трудомістко, дорого і незручно. У цьому відношенні впровадження штучного інтелекту і машинного навчання в управління QoE підвищує точність процедур моделювання, покращує ефективність процесу моніторингу та розробляє інноваційні методології оптимізації та контролю. Відповідно для інтелектуальних мереж нового покоління актуальним є забезпечення кінцевим користувачам доступ до мультимедійних послуг з високою якістю сприйняття (QoE, Quality of Experience) у будь-який час та в будь-якому місці без обмежень за технологією та середовищем передавання. Для задоволення цих вимог на часі є розроблення нових структурно-функціональних моделей побудови інформаційно-комунікаційним систем та інтелектуальних схем для контролю та управління QoE в майбутніх мережах.

РОЗДІЛ 2. МОДЕЛІ ТА МЕТОДИ ПОБУДОВИ ІНТЕЛЕКТУАЛЬНИХ МЕРЕЖ З АДАПТИВНИМ УПРАВЛІННЯМ РЕСУРСАМИ НА ОСНОВІ ПОКАЗНИКА ЯКОСТІ СПРИЙНЯТТЯ ПОСЛУГ

2.1 Концептуальна модель побудови інтелектуальної інформаційно-комунікаційної мережі з автоматизованими методами розгортання та моніторингу функціонування на основі намірів користувачів

На сьогоднішній час для підвищення продуктивності та характеристик якості функціонування майбутніх інтелектуальних мереж більшість наукових досліджень зосереджено на використанні технології штучного інтелекту та SDN для прогнозування параметрів QoE/QoS, класифікації трафіку, оптимізації маршрутизації і т.д. Відповідно у даній роботі, робиться акцент на тому, що наступним кроком буде те, як інтегрувати дані рішення разом, щоб побудувати наскрізну інтелектуальну систему управління мережею. Саме тому дисертація присвячена дослідженню інтелектуальних мереж нового покоління, яка окрім вище перелічених існуючих наукових розробок базується на нових методах і моделях управління ресурсами та якістю обслуговування на основі намірів користувачів. Пропоновані методи орієнтовані на підвищення показника QoE, що характеризує якість сприйняття послуг кінцевими користувачами з використанням машинного навчання та технології SDN.

Таким чином, у роботі пропонується концептуальна модель новітньої інтелектуальної IBN мережі, яка може використовуватися для цивільних потреб та в інтересах оборонних відомств нашої держави шляхом використання розроблених програмно-апаратних засобів централізованого автоматизованого управління мережею, методів інтелектуального забезпечення гарантованої якості та високого рівня забезпечення інформаційної безпеки.

Згідно пропонованої в дисертації ідеології мережа на основі намірів IBN — це тенденція інтелектуального керування мережею, яка включає штучний

інтелект, машинне навчання та мережеву оркестрацію для автоматизації адміністративних завдань.

Намір в автономній системі ідеально виражається декларативно, тобто як ціль на рівні корисності, яка описує властивості задовільного результату, а не прописує конкретне рішення. Це дає системі гнучкість щодо вивчення різних варіантів рішення та пошуку оптимального. Це також дозволяє системі автоматично оптимізуватися, вибираючи власні цілі, які максимізують корисність.

На відміну від традиційних програмних систем, де вимоги аналізуються в автономному режимі для виявлення та вирішення конфліктів перед впровадженням, наміри додаються до автономної системи під час виконання. Таким чином, адаптація до змінених намірів, а також виявлення та вирішення конфліктів є основними можливостями автономної системи.

Однією з переваг вираження намірів як цілей на рівні корисності є те, що це допомагає системі впоратися з суперечливими цілями кількох намірів. Це важливо протягом усього життєвого циклу функціонування, оскільки автономна система часто має враховувати кілька намірів, перш ніж приймати рішення. Наприклад, автономна система може мати один намір надавати послугу з високою QoE (зокрема у роботі QoE розглядається як основний намір для пропонованої IBN), а інший — мінімізувати витрати ресурсів (чи енергетичні чи мережеві). Використання спеціалізованої бази знань може вирішувати такі конфлікти або явно за допомогою ваг, які вносять відносну важливість, або неявно з властивостей преференційних результатів, визначених у цілях на рівні корисності.

Очікування щодо якості обслуговування випливають з контрактів або бізнес-стратегії і залишаються незмінними, коли базова система замінюється або змінюється. Отже, під час налаштування намірів важливо, щоб вони були сформульовані незалежним від інфраструктури способом, щоб їх можна було

передавати між різними поколіннями систем мобільного зв’язку в тому числі і в умовах подвійного розгортання мережі.

Саме тому, намір в пропонованій парадигмі інтелектуальної системи встановлює універсальний механізм для визначення очікувань для різних рівнів функціонування мережі. IBN виражає цілі, корисність, вимоги та обмеження. Також визначає очікування щодо надання послуг, та поведінку автономної системи.

Крім усіх специфічних для служби намірів, які повинна мати автономна система, вона також вимагає вказівок щодо того, як вирішувати стратегічні та поведінкові проблеми. Традиційно розгортання та налаштування мережі реалізовується у формі політик, кодованих вручну, цей тип керівництва керує загальною поведінкою системи та підтримує тип прийняття рішень, який традиційно базувався на людській інтуїції та досвіді, а також знаннях про контекст і стратегію оператора. Операція на основі намірів дає можливість операторам, які хочуть впоратися з цими проблемами більш динамічно, замінити закодовані вручну політики стратегічними та поведінковими намірами.

Це корисно, наприклад, у випадках, коли у оператора компанія вимагає мінімальний рівень безпеки за замовчуванням, який відрізняється від того, який реалізовано в системах спеціального чи військового зв’язку. У цих випадках спеціальний намір можна використовувати для встановлення рівня безпеки для всіх служб, які не вказують його безпосередньо.

Оскільки завжди існує ризик погіршення якості обслуговування, коли починаються зміни, а ризиковані дії іноді можуть призвести до більшої маржі, наміри управління ризиками можна використовувати, щоб передати, як оператор хоче, щоб автономна система збалансувала ризики та потенційну вигоду. Автономна система вимагає, щоб наміри були формально визначені машино-читаним і оброблюваним способом, але широкий спектр залучених міркувань та їхню абстрактну семантику часто важко структурувати. Прийоми

управління знаннями та семантичне моделювання дозволяють створити наміри, засновані на розширюваній мета моделі. Для моделювання знань можна використовувати стандарти Resource Description Framework (RDF) [116] і RDF Schema [117].

Технічні функції, такі як управління контрактами та замовленнями, будуть безпосередньо використовувати об’єкти RDF для передачі намірів. Намір, визначений безпосередньо людьми-операторами, вимагатиме інтуїтивно зрозумілого інтерфейсу, який потенційно використовує природну мову.

Функціонування служб у мережі на основі намірів також вимагає введення функцій обробки намірів у стек операцій і функціональну архітектуру. Функція обробки намірів отримує наміри, вирішує, які дії необхідно зробити, щоб оптимально виконати всі ці наміри, і реалізує свої рішення.

Функції обробки намірів мають базу знань, яка містить онтологію намірів. Вони також мають здатність до машинного мислення, щоб реалізувати процеси прийняття рішень, керовані знаннями на основі штучного інтелекту (AI).

Машинне навчання відіграє ключову роль в обробці намірів, завдяки його здатності розуміти абстрактні поняття з різних областей і надавати точні, спеціалізовані висновки, засновані на прецеденті та спостереженні. Імовірнісне моделювання сприяє кількісній оцінці ризику та невизначеності, що важливо для прийняття обґрунтованих рішень, коли стикаються з суперечливими цілями та новими ситуаціями.

На рис.2.1 показано, як працює функція обробки намірів. Хоча його реалізація є специфічною для певного домену та призначення мережі, його інтерфейс є загальним. Контролер IBN отримує наміри, які виражають усі види очікувань. Також контролер IBN оснащений політиками та моделями штучного інтелекту (AI), які реалізують можливості, необхідні для аналізу стану системи та пошуку оптимізованих операційних дій на основі спостережень із керованого середовища. Обробник намірів також повідомляє про виконання та статус впевненості своїх намірів.

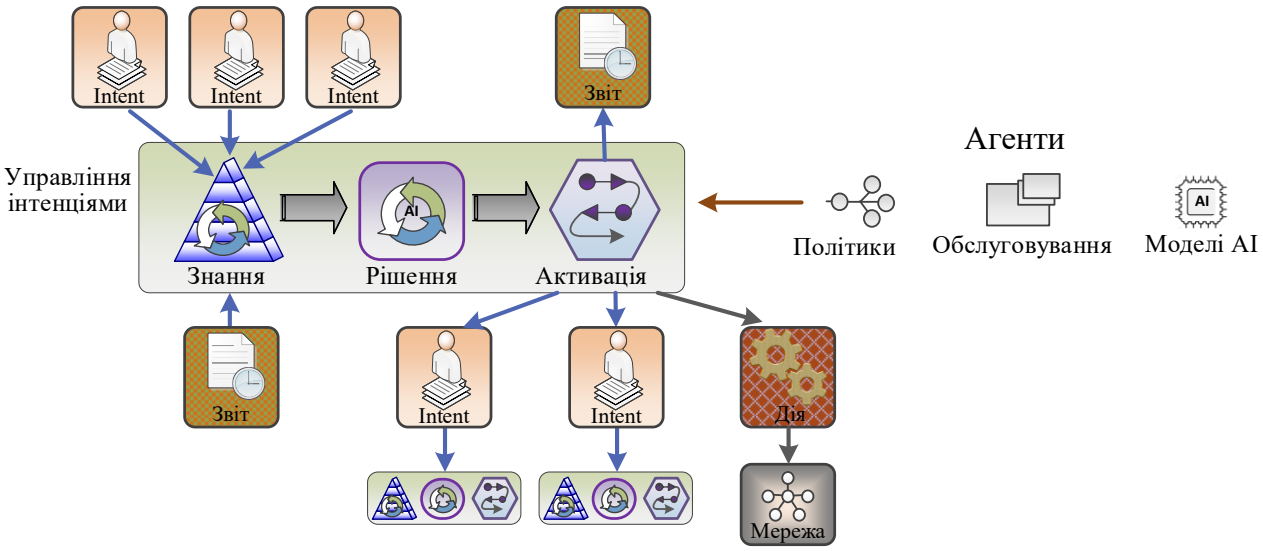


Рис.2.1. Функціональна схема обробки інтенцій (намірів) в умовах розгортання інтелектуальної IBN мережі нового покоління

Завдяки підтримці API (інтерфейс прикладного програмування) функції обробки намірів не залежить від домену. Головне завдання API — керувати життєвим циклом намірів. Він реалізує методи встановлення, зміни та видалення намірів та надсилання звітів. Намір будується на основі загальної мета-моделі намірів, а її деталі визначаються відповідно до інформаційних моделей, що стосуються предметної області. Таким чином, управління намірами — це насамперед управління знаннями.

На рис.2.2 наведено приклад того, як функції обробки намірів можна об'єднати, щоб реалізувати повну операційну систему, керовану наміром. Кожен основний системний рівень і домен підсистеми, включаючи Системи підтримки операцій (OSS, Operation Support System) (BSS, Business Support System) оркестровку та керування мережею, містить функцію обробки намірів. Намір походить від таких функцій, як управління контрактами та замовленнями якістю сприйняття послуг. Додаткові наміри можна ввести безпосередньо через спеціальні веб-портали користувачів.

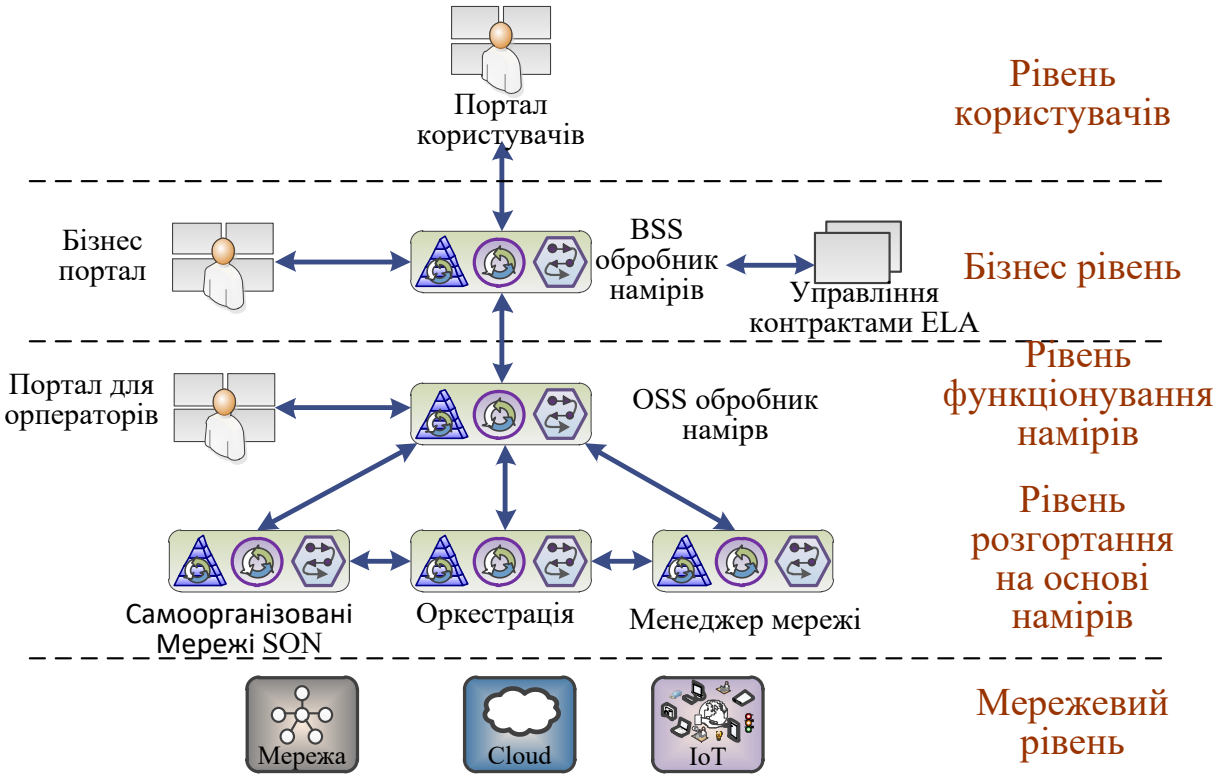


Рис.2.2. Багаторівнева інтелектуальна система для розгортання IBN, орієнтована на наміри

Створення функції обробки намірів, яка розуміє складну та абстрактну семантику наміру, виводить оптимальний цільовий стан і планує дії для переходу системи в цей стан. Функція повинна мати можливість досліджувати варіанти, вчитися на прецедентах і оцінювати доцільність дій на основі їх очікуваних наслідків.

Об’єднавши добре зрозумілі методи штучного інтелекту в рамках гнучкої архітектури у роботі пропонується концептуальна модель інтелектуальної мережі нового покоління (рис.2.3).

Інтелектуальний рівень складається з чотирьох основних компонентів: бази знань, сховища даних, механізму навчання та архітектури агента. Сховище даних відстежує мережеві об'єкти та використовується для ефективного зберігання даних. База знань містить онтологію намірів разом із специфічними знаннями, такими як поточний стан системи. Доменно-незалежний механізм

навчання використовує знання і служить центральною функцією координатора для пошуку дій, оцінки їх впливу та впорядкування їх виконання.

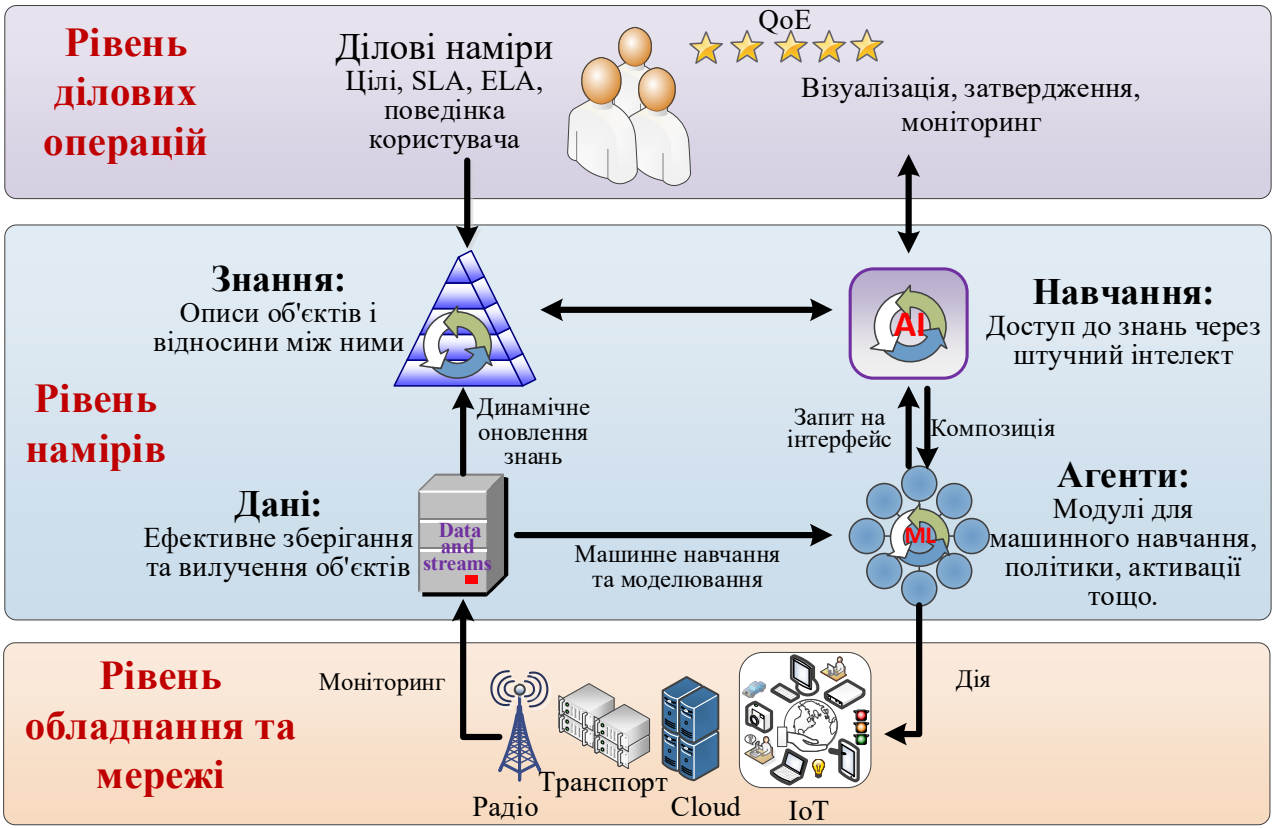


Рис. 2.3. Функціональна архітектура IBN з інтелектуальним автоматизованим методом розгортання та моніторингу на основі намірів

Архітектура агента дозволяє використовувати будь-яку кількість моделей і сервісів. Агенти можуть містити моделі машинного навчання або політику, засновану на правилах, або впроваджувати послуги, необхідні в процесі інтелектуального навчання [118].

Щоб можна було використовувати агента, його потрібно зареєструвати та описати в базі знань. Опис агента можна додавати та змінювати в будь-який час, дозволяючи відокремити життєвий цикл моделей, політик та додаткових послуг від загального життєвого циклу інтелектуального рівня.

Метадані агента містять опис інтерфейсу агента, а також його функції, роль і можливості. Наприклад, можна розробити модель машинного навчання, яка може запропонувати конфігурації базової радіостанції для оптимізації

обслуговування. Ця модель реєструється як агент у ролі «пропонатора» для конфігураційних дій. Окремий життєвий цикл дає можливість замінити модель покращеною версією, якщо вона доступна, незалежно від циклів вивільнення інтелектуального рівня.

Також можна розробити агенти у ролі «провісника» зі здатністю оцінити вплив дій на ключові показники ефективності (KPI, Key Performance Indicators). Агент у ролі «спостерігача» буде стежити за джерелами даних, підтримуючи інформацію про стан в актуальному стані. Агент у ролі «актуатора» може виконувати дії в мережі, використовуючи, наприклад, встановлені функції керування мережею.

Успішна робота інтелектуального рівня залежить від плавної взаємодії між механізмом навчання і базою знань. Механізм навчання безперервно виконує процес, який намагається знайти дії, щоб закрити розрив між поточним спостережуваним станом і шуканим станом відповідно до наміру. Він збирає пропозиції, отримує прогнози щодо ефекту кожної пропозиції, оцінює виграш у порівнянні з ризиком і впевненістю, визначає пріоритети дій і виконує свої рішення. На кожному етапі процесу інтенсивно використовуються спеціальні засоби.

Механізм навчання — це адаптивний композитор, який керується знаннями, який може ініціювати інтелектуальний процес після змін намірів, стану та контексту. Він може динамічно створювати спеціалізовані агенти і додавати їх у процес, якщо їхні можливості та ролі відповідають потребам відповідно до намірів та контексту. Так, наприклад, інтелектуальний рівень отримує пропозиції дій від агентів, які реалізують відповідні моделі.

У випадках, коли можливості кількох агентів відповідають вимогам ролі, кожен з них може використовуватися одночасно для створення альтернативних стратегій вирішення, що призводить до різноманітного набору варіантів для наступних кроків прогнозування та оцінки. Таке співіснування агентів дає змогу поєднувати реалізації на основі правил і політик з альтернативами,

засвоєними на машині, в одній системі, дозволяючи отримувати нові передові здібності без втрати поточних. Схема інтелектуального методу архітектурних розв'язань побудови баз знань та їх експертування для розгортання інфокомунікаційної IBN систем показано на рис.2.4.

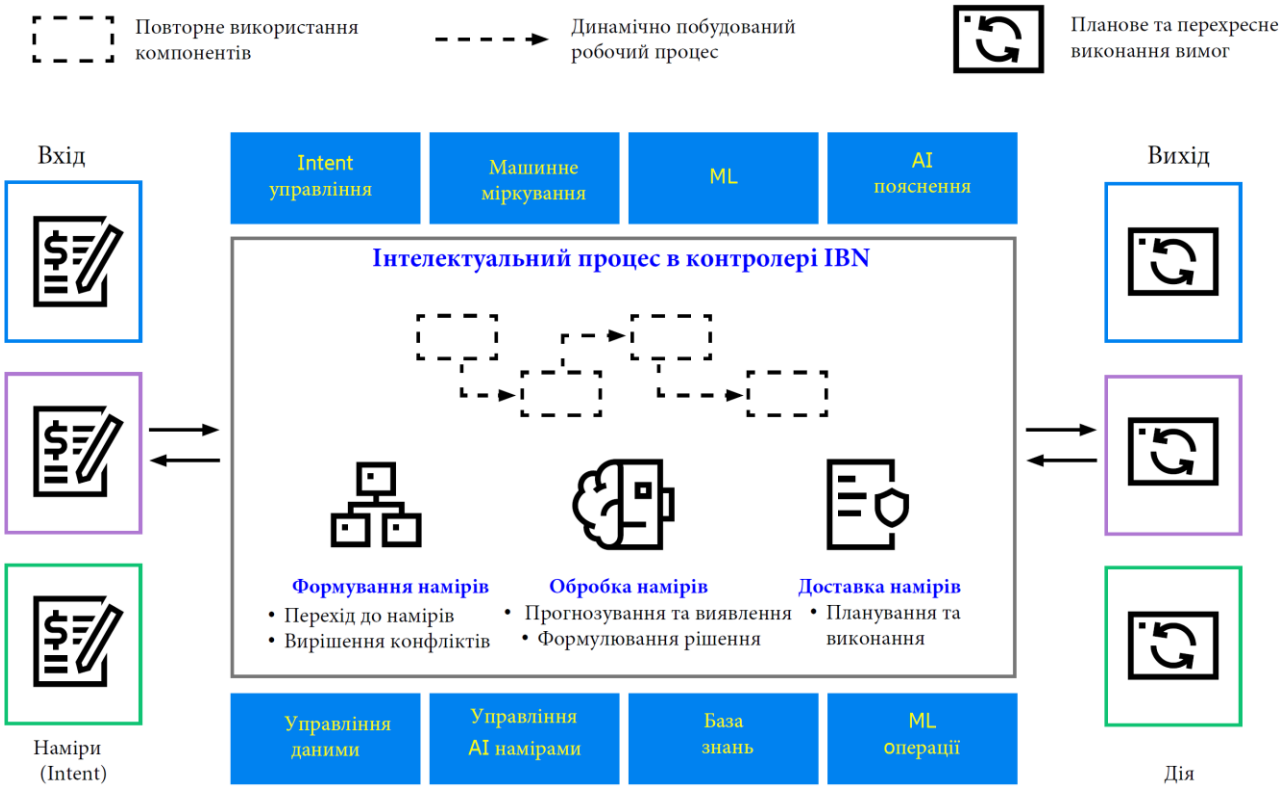


Рис.2.4. Схема інтелектуального методу архітектурних розв'язань побудови баз знань та їх експертування для розгортання інфокомунікаційної IBN системи

Інтелектуальний процес це вічний цикл, який починається знову відразу після завершення попередньої ітерації. Будь-яка деградація якості функціонування мережі або проблеми з наданням послуг будуть помітні в спостережуваному стані. Намагаючись закрити розрив до бажаного стану, встановленого наміром. Навіть без явних проблем безперервний інтелектуальний процес все одно шукатиме дії для подальшої оптимізації. Наприклад, він може спробувати надати ті ж послуги з обмеженими ресурсами.

Завдяки своєму основному процесу, заснованому на навчанні, інтелектуальний рівень досягає високого ступеня динамічної адаптації до нових

ситуацій. Це різко контрастує з системами, які були реалізовані за допомогою політик, заснованих на правилах, і фіксованих робочих процесів, де кожна підтримувана ситуація потребує розгляду під час розробки через відповідні гілки в дереві рішень і правила диверсифікації. Однак існуючі політики, засновані на правилах, все ще можуть використовуватися на інтелектуальному рівні через інтеграцію як агентів. Це відкриває шлях до нової автоматизації, коли моделі на основі штучного інтелекту додаються поступово.

Щоб продемонструвати приклад, як працює інтелектуальний рівень, ми проекспериментували з варіантом використання, який оптимізує рішення щодо надання послуг на вимогу користувачів Джерелом наміру є угода про рівень обслуговування ELA, яка визначає замовлену якість сприйняття послуги згідно оцінок QoE, яку необхідно надати, разом із цільовими показниками KPI, які були обіцяні клієнту.

У нашому експерименті побудова мережі відбувається в режимі реального часу– від отримання угоди про рівень обслуговування до оптимізованого розгортання – є повністю автономним і контролюється процесом навчання інтелектуального рівня, що знаходиться у контролері IBN. Коли намір, отриманий з ELA, надходить до бази знань, цикл міркування починає його обробляти. Модуль штучного інтелекту виявляє, що агент, який дізнався в тестовому середовищі про розгорнуту продуктивність мережі, відповідає потребам. Агент надає модель, повністю налаштовану й оптимізовану для запитуваного цільового показника ефективності та пропонує розгорнути архітектуру чи використати спеціальні методи управління трафіком відповідно до намірів.

Потім інтелектуальний рівень використовує засоби прогнозування та оцінки рівня QoE для замовленої пропозиції. У цьому випадку наш агент прогнозування містить модель стану-дія – імовірнісний графік, заснований на моделюванні процесу прийняття рішень. Модель постійно вивчається на основі станів спостереження та результатів спостережуваних дій. Вона має здатність

оцінювати ймовірність очікуваних станів результату для пропонованих дій, що дозволяє приймати обґрунтовані рішення про дії з урахуванням їх ризику.

За допомогою проактивних робочих процесів, керованих штучним інтелектом, потенційні проблеми можна виявити завчасно, а більшість із них також можна вирішити до фактичних порушень. Це не тільки зменшує відмови в мережі та порушення, але й допомагає знизити експлуатаційні витрати завдяки автоматизації на основі штучного інтелекту. Використовуючи штучний інтелект для прогнозування, запобігання та обробки подій, операційні витрати можна зменшити, одночасно керуючи підвищеною складністю.

2.2 Моніторинг основних параметрів якості обслуговування програмно-конфігурованої мережі для визначення необхідного рівня якості сприйняття послуг кінцевими користувачами

IBN відома як розширення концепції Software-Defined Networking. Незважаючи на безперервний розвиток SDN (програмно-конфігурованих мереж) з моменту його появи, існують деякі аспекти мережевих технологій, які не реалізовані належним чином.

З огляду на вимоги сучасних мережевих середовищ, необхідно використовувати різні методи підвищення якості обслуговування та інженерії трафіку для оптимізації потоків трафіку великої кількості додатків і різних типів трафіку, таких як голосовий трафік і відеотрафік [119-121]. Реалізація програм, які вирішували б ці проблеми, в деяких випадках може бути занадто складною і не завжди підтримується північними інтерфейсами.

Існуючі методи управління якістю послуг в основному орієнтовані лише на технічні параметри якості обслуговування, тоді як сьогодні необхідні ефективні методи врахування мінливої думки користувачів при управлінні якістю послуг даючи змогу враховувати їх наміри щодо переконфігурації мережі. Отже, можливість врахування мінливих намірів користувачів щодо замовленого рівня QoE є досить важливим для розвитку основних завдань трафіку інжинірингу у

контексті реалізації майбутніх IBN.

У зв’язку з розвитком технологій з’являється потреба в автоматизації процесів налагодження інформаційно-телекомунікаційної мережі у випадку надання неякісних послуг користувачеві. Нові рішення дадуть можливість пришвидшити моніторинг мережі на наявність вузлів мережі та оптимізувати час вирішення несправностей. Щоб конкурувати за значну частку ринку, різні оператори мережі та постачальники послуг повинні зберігати та збільшувати передплату клієнтів. Для цього вони повинні виконувати мультимедійні вимоги QoE користувача.

Для виконання цих вимог їм потрібен ефективний інструмент моніторингу та оцінки якості QoE. Проте QoE є суб'єктивною метрикою і може змінюватися залежно від сподівань користувачів та контексту. Крім того, суб'єктивне оцінювання QoE є дорогим і трудомістким, оскільки це вимагає участі людини [122]. Тому існує потреба в інструменті, який може об'єктивно вимірювати QoE з обґрунтованою точністю.

Саме тому виникає потреба розробити якісне програмне забезпечення для моніторингу основних параметрів якості обслуговування QoS (затримки, втрат пакетів та ін.) в SDN/IBN з метою автоматизованого визначення необхідного рівня якості сприйняття послуг кінцевими користувачами. Підхід, який використовується для того, щоб забезпечити збереження QoE на задовільних рівнях, це періодичний моніторинг та оцінка якості на основі їх статистичних даних.

Для реалізації вимірювання затримки в мережі використовується дослідження деяких відомих робіт [123], в яких для контролю часу затримки використовується контролер, який використовує повідомлення протоколу OpenFlow, описані в специфікації OpenFlow. Для даного рішення використовуються чотири типи повідомлень:

Таблиця 2.1

Типи повідомлень в OpenFlow

Packet_Out	Повідомлення від контролера до комутатора, яке містить пакет даних для пересилання через порт.
Packet_In	Повідомлення від комутатора до контролера, коли в таблиці потоків немає відповідного запису.
Statistics_Request	Повідомлення від контролера до комутатора із запитом статистичних даних.
Statistics_Reply	Повідомлення від комутатора до контролера, що містить запитувані статистичні дані.

У цьому рішенні для вимірювання затримки контролер створює простий кадр Ethernet (рис.2.5).

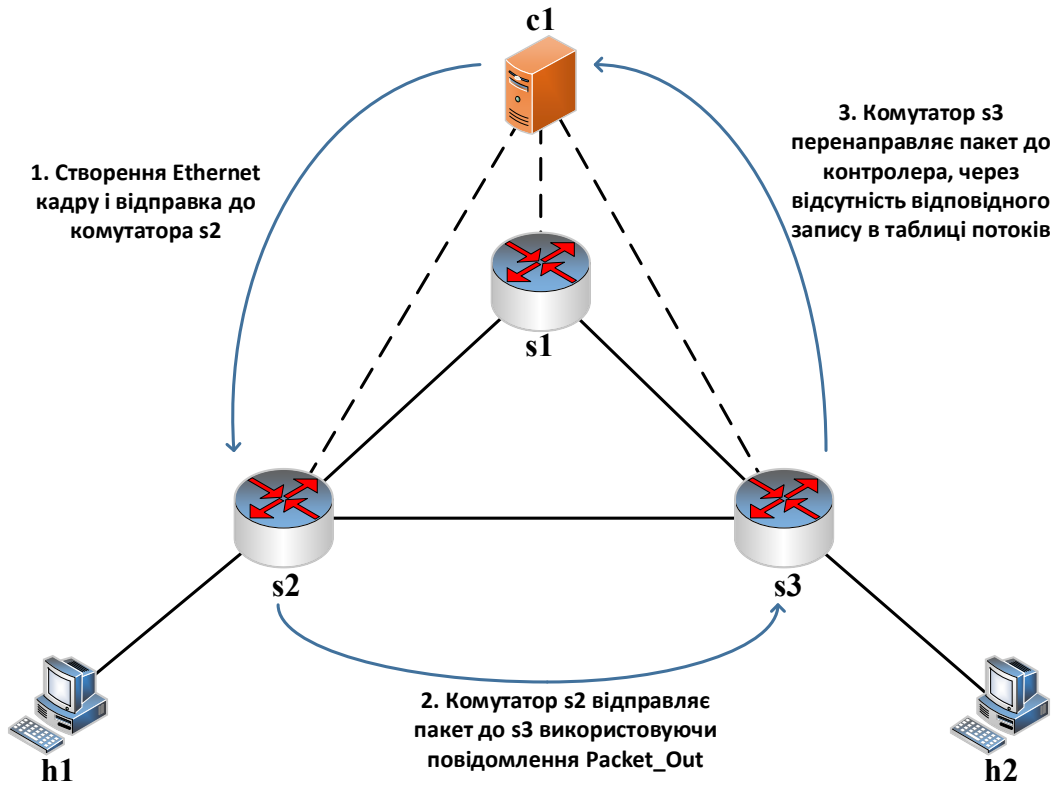


Рис.2.5. Процес вимірювання затримки пакетів в мережі

Потім контролер звертається до комутатора *s2* переслати цей пакет через певний порт за допомогою повідомлення Packet_Out. Комутатор s3 отримавши цей пакет, пересилає його до контролера за допомогою повідомлення Packet_In, оскільки для даного типу Ethernet немає відповіді. Затримка розраховується за

такою формулою (2.1):

$$Latency = D_{total} - \frac{D_{s1}}{2} - \frac{D_{s2}}{2} \quad (2.1)$$

де D_{total} – загальний час передачі, D_{s1} – RTT між комутатором *s1* та контролером, D_{s2} – RTT між комутатором *s2* та контролером.

Для реалізації вимірювання втрати пакетів в мережі контролер отримує статистику вихідних і вхідних пакетів комутаторів *s2* і *s3* (рис.4.3). Згідно з отриманою статистикою переданих і прийнятих пакетів на відповідних комутаторах, контролер підраховує загальну кількість втрачених пакетів за формулою (2.2).

$$packetLoss(report) = input\_pkts - output\_pkts \quad (2.2)$$

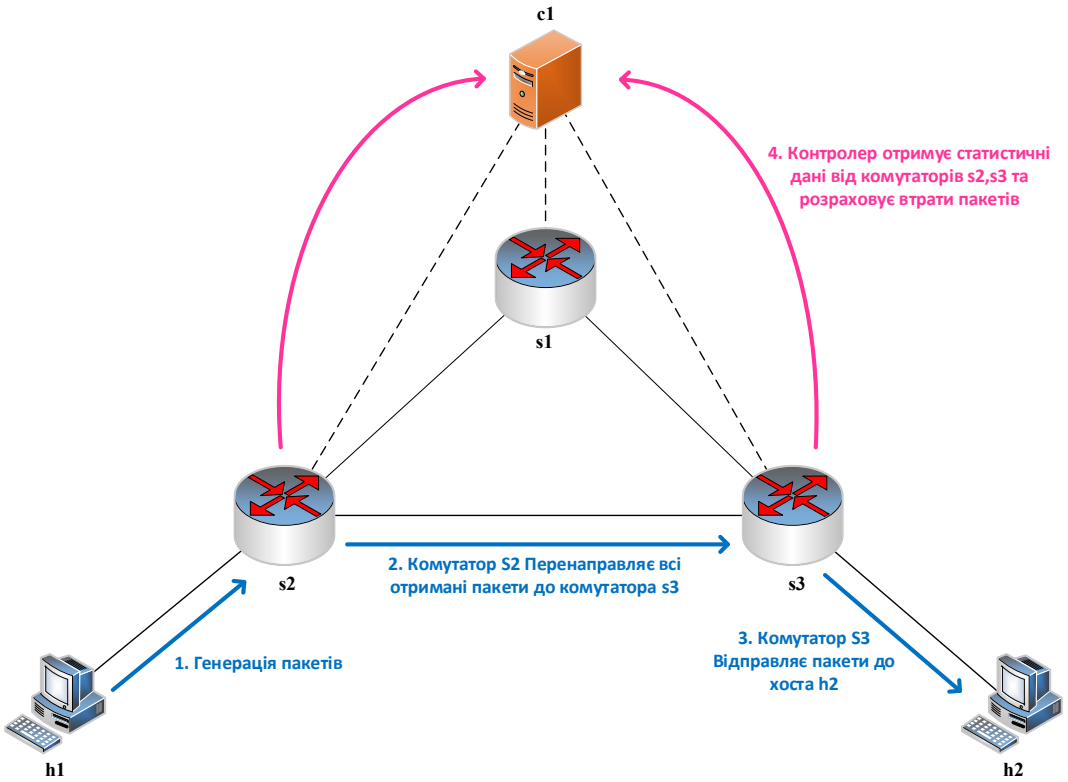


Рис.2.6. Процес вимірювання втрат пакетів [124]

У роботі проводиться дослідження впливу технічних мережних параметрів QoS у процесі передачі відеопотоків реального часу на показник якості сприйняття послуг за п’ятибальною шкалою MOS/QoE. Оцінювання якості

відео перегляду відбувається за допомогою спеціального додатку, що дає змогу кінцевим користувачам виставити особисту суб'єктивну оцінку якості сприйняття.

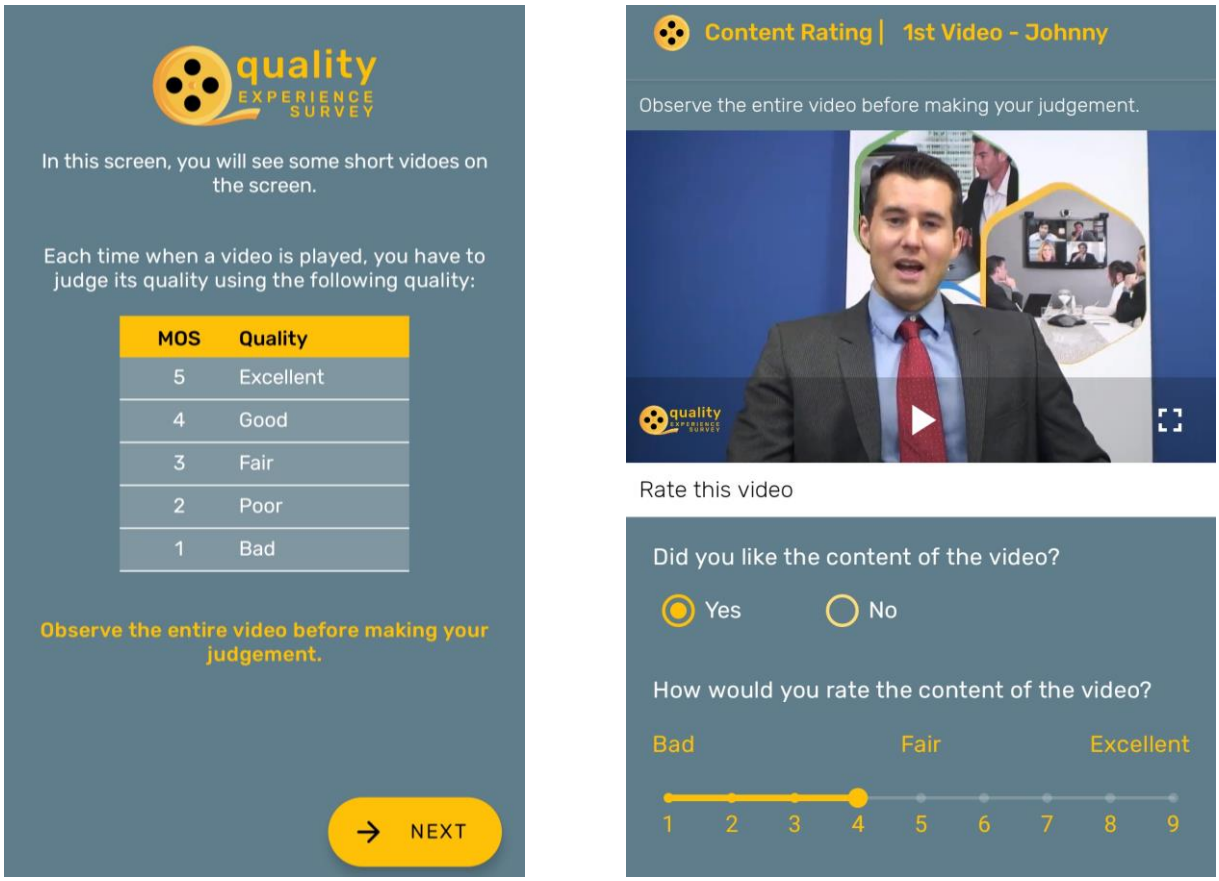


Рис.2.7. Додаток користувачів для суб'єктивної оцінки якості сприйняття відео

Експерименти проводяться на виділеній топології мережі SDN де у процесі дослідження створюються різні випадки, коли може відбуватися деградація QoE в умовах передавання відепотоків. Погіршення якості обслуговування спостерігається через обмеження, що накладаються мережними умовами, а також через нестабільність мережі, наприклад, відмови каналу. В результаті експериментів проілюстровано безліч випадків, коли QoE в мережі страждає від деградації через мережеві умови, і показано необхідність розробки системи моніторингу параметрів QoS для пошуку математичної моделі кореляції QoS/QoE з метою реалізації маршрутизації QoE в майбутніх програмно-конфігурованих мережах на основі намірів.

Отже, метою дослідження є оцінка якості передачі відеопотоку в режимі реального часу з віртуального хоста у віртуальній програмно-конфігурованій мережі Mininet в умовах зміни параметрів QoS.

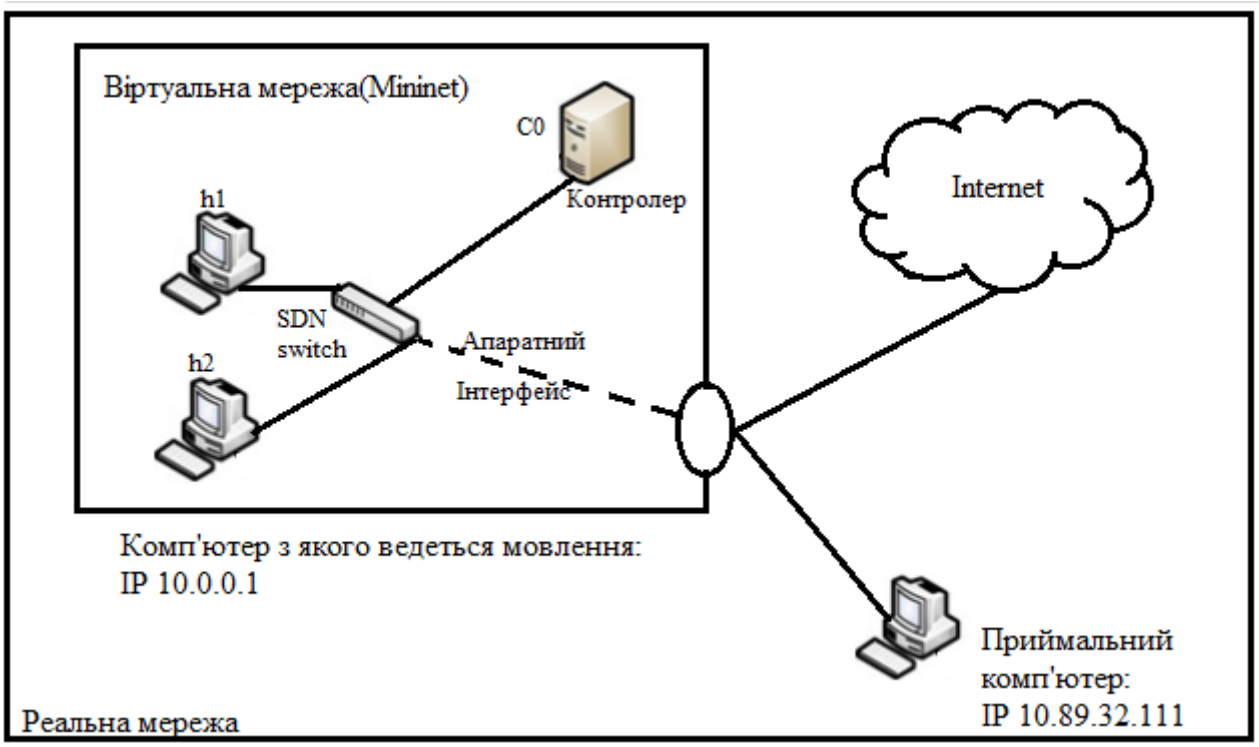


Рис.2.8. Структурна схема програмно-конфігурованої мережі

Під час дослідження використано: 2 віртуальних хости, 1 віртуальний SDN комутатор, 1 контролер. Традиційна мережа використовувала персональний комп’ютер, який був на прийомі відеопотоку.

У програмному середовищі використовувався Python script для налаштування топології мережі та її параметрів, його код можна побачити на рис.2.9. У скрипті описані мережеві QoS параметри з’єднань між комутатором і хостами, які у разі потреби можна легко змінити: пропускна здатність, втрати, затримка.

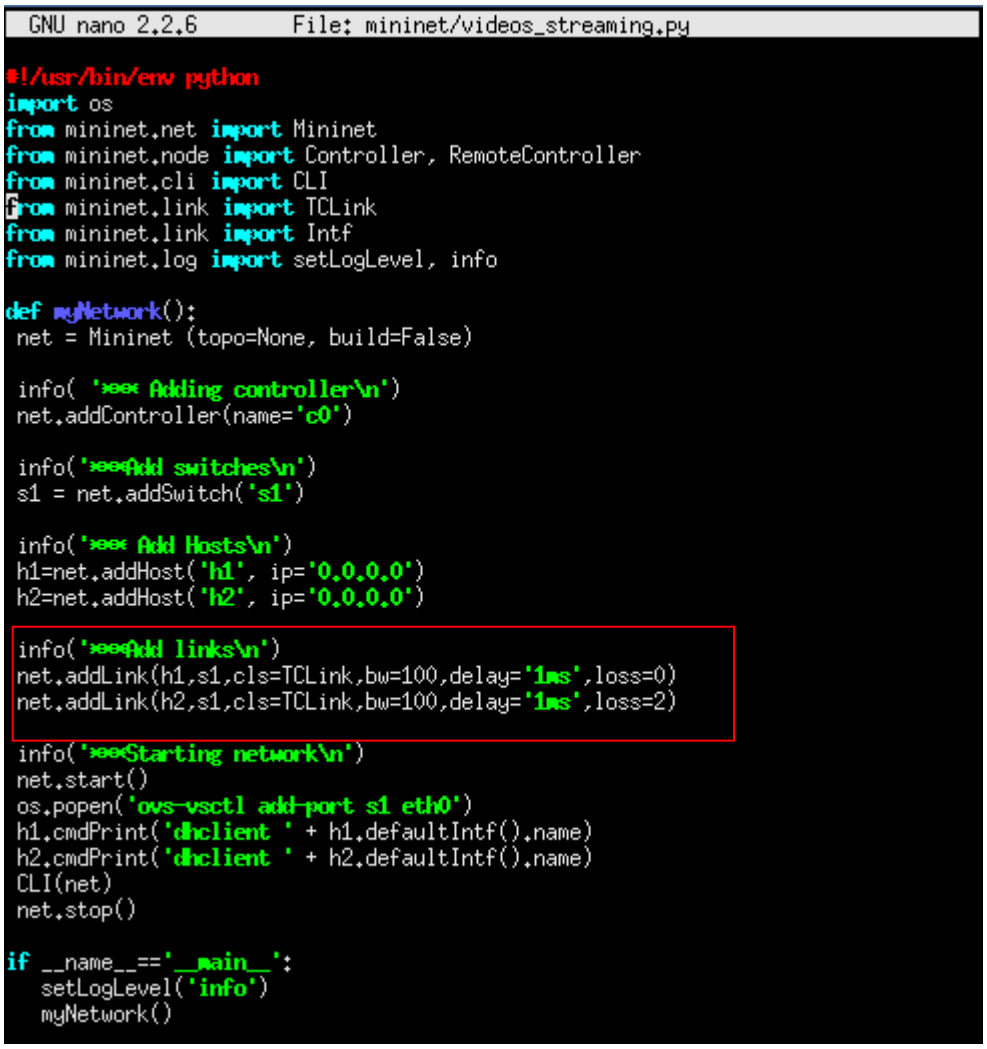


Рис.2.9. Код Python скрипта

Під час проведення досліджень використовувалося таке програмне забезпечення:

- Медіапрогравач VLC для проведення відео стріму.
- WireShark 2.6.8 для перехоплення трафіку та отримання необхідних даних

Порядок передачі відео у режимі реального часу:

1. Налаштування VLC плеєра на передавальному та приймальному хості.

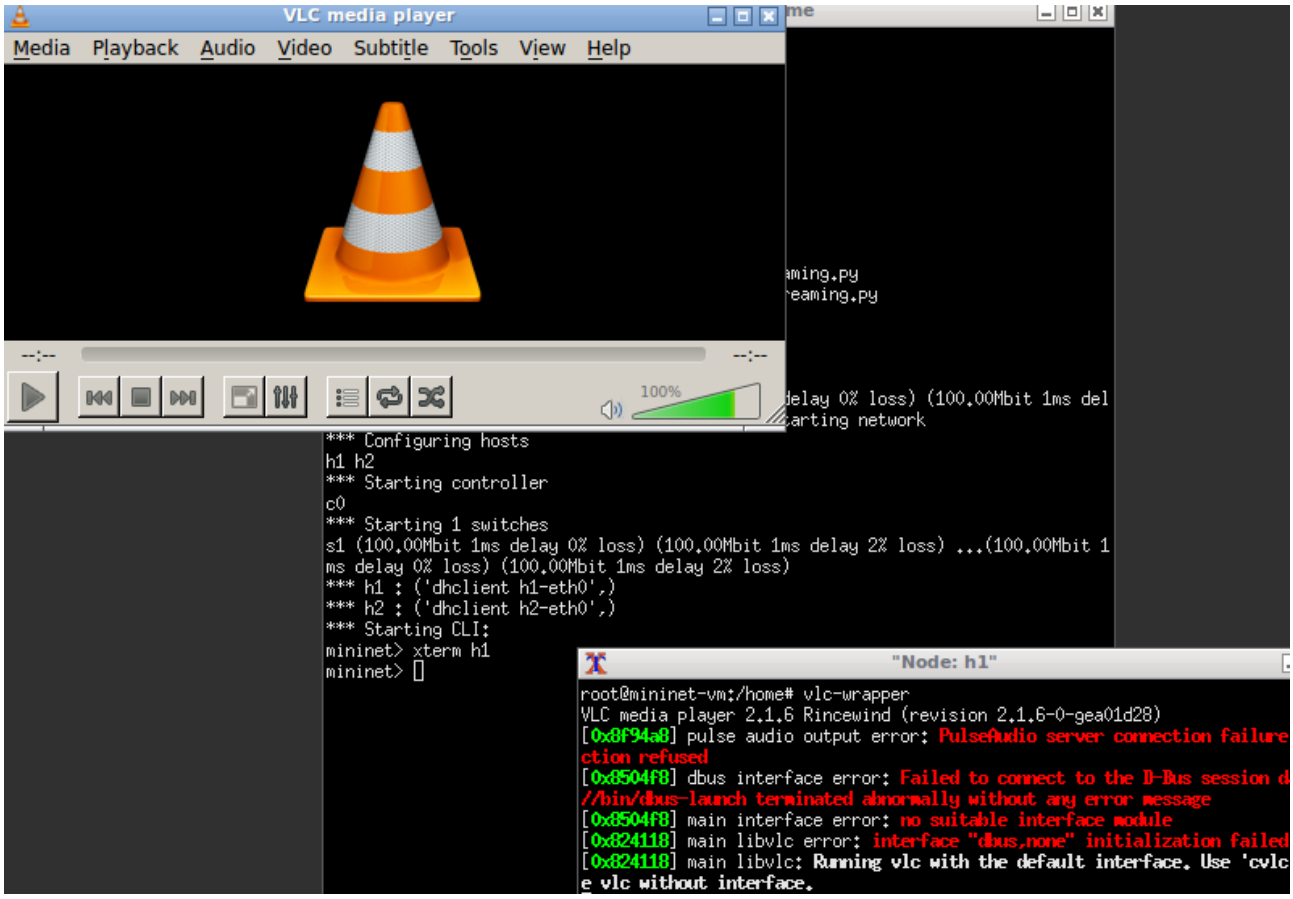


Рис.2.10. Налаштування VLC плеєра на віртуальному хості

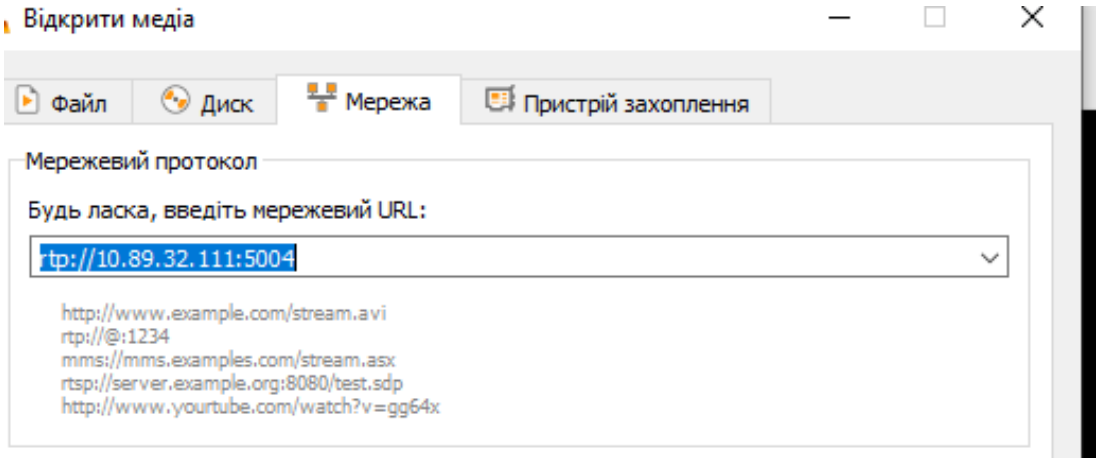


Рис.2.11. Налаштування VLC плеєра на реальному приймаючому хості

У налаштування VLC приймального пристрою потрібно ввести мережевий URL, який складається з абревіатури протоколу який використовується, IP адреса комп'ютера, який буде приймати потік, номер відкритого порта для передавання відео потоку.

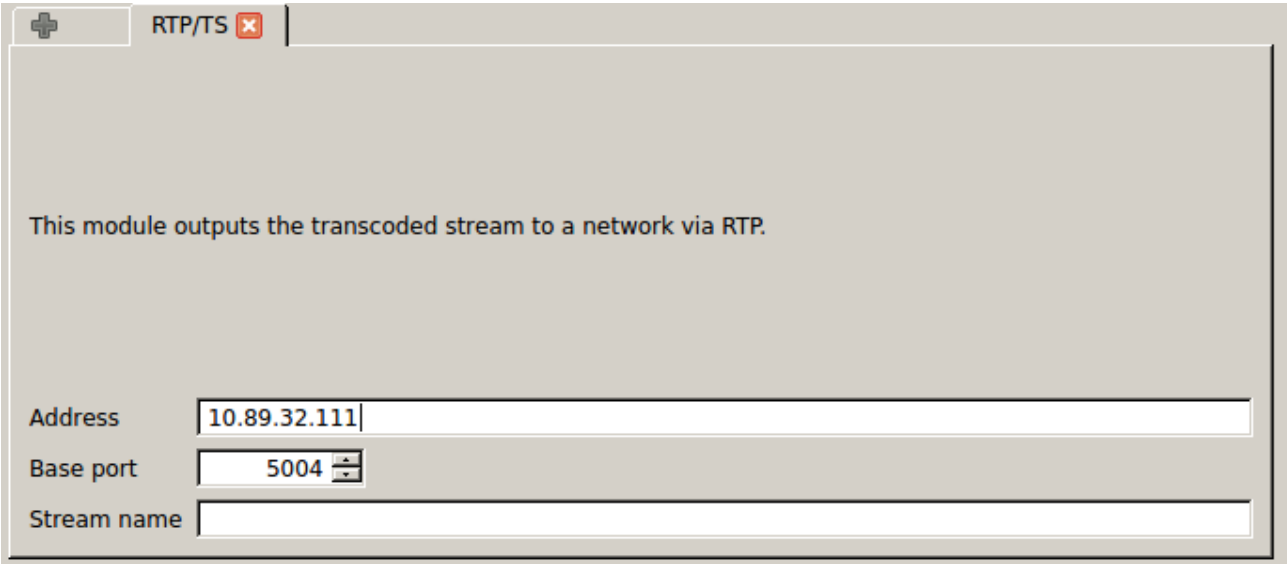


Рис.2.12. Встановлення адреси призначення на пристрої передавання

Після останнього підтвердження буде відбуватися трансляція відео потоку, яка повинна відтворитися і на приймальному хості. Для дослідження передачі потоку відео проведено дослідження з внесеними втратами, та з різною пропускною здатністю. За допомогою налаштувань в SDN комутаторі можемо оперувати такими параметрами задля кращої якості і коректності передачі відео потоку.

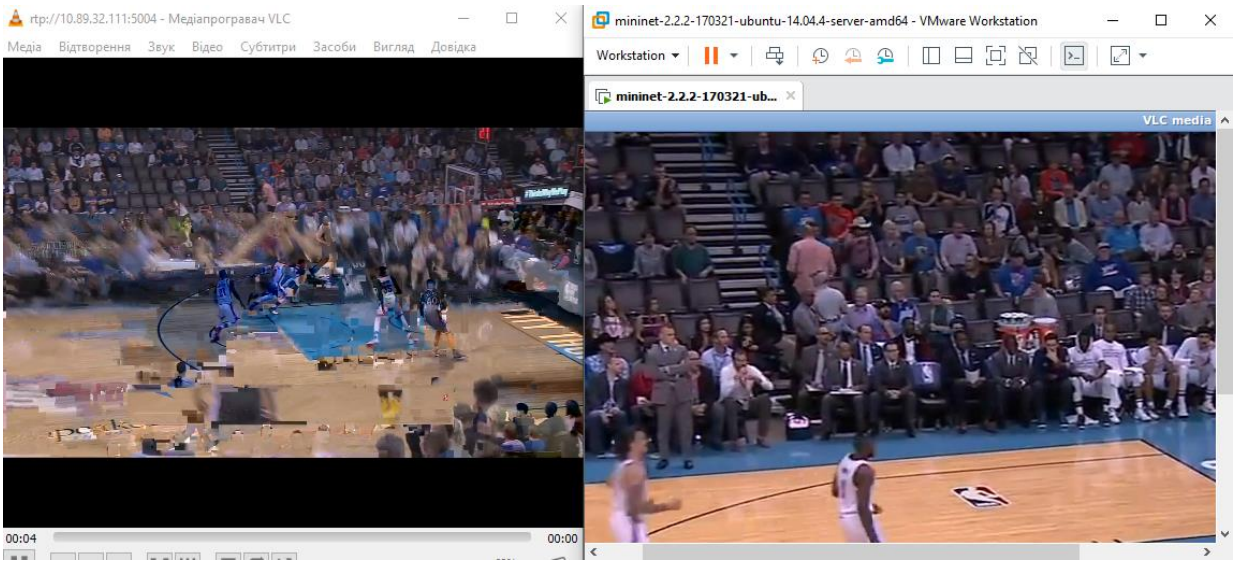


Рис.2.13. Приклад зображення із внесеними втратами 30% (QoE 2)

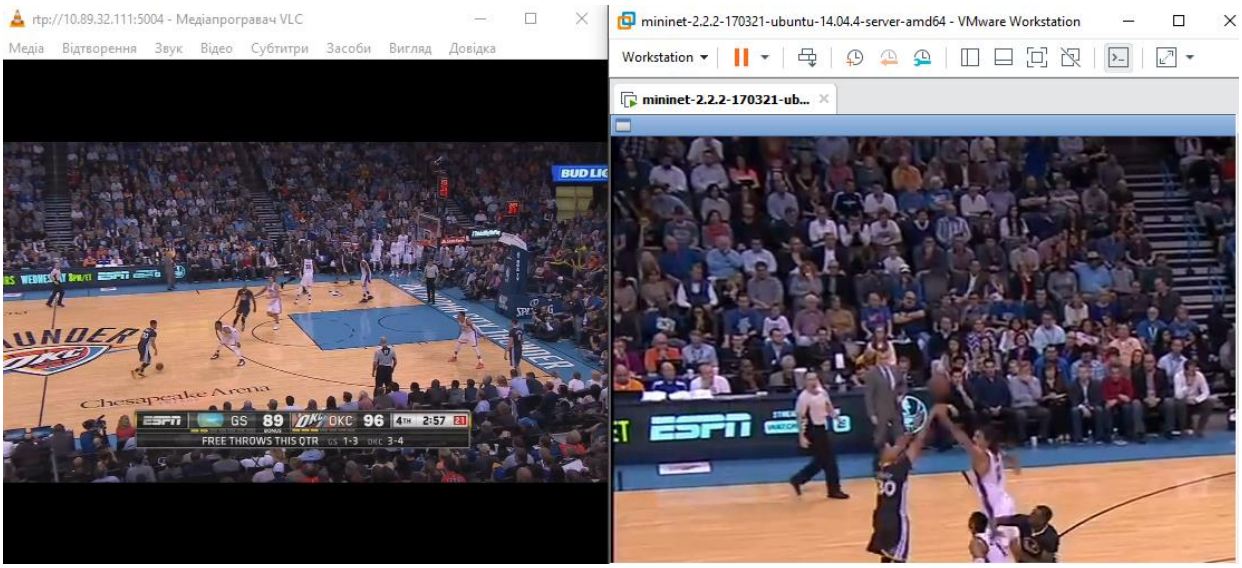


Рис.2.14. Приклад зображення, яке транслюється без втрат, але із затримкою (QoE 4)

На рис.2.14 відео потік йде без втрат, але відбувається незначна затримка в 1-2с, яка дозволяє покращити якість зображення.

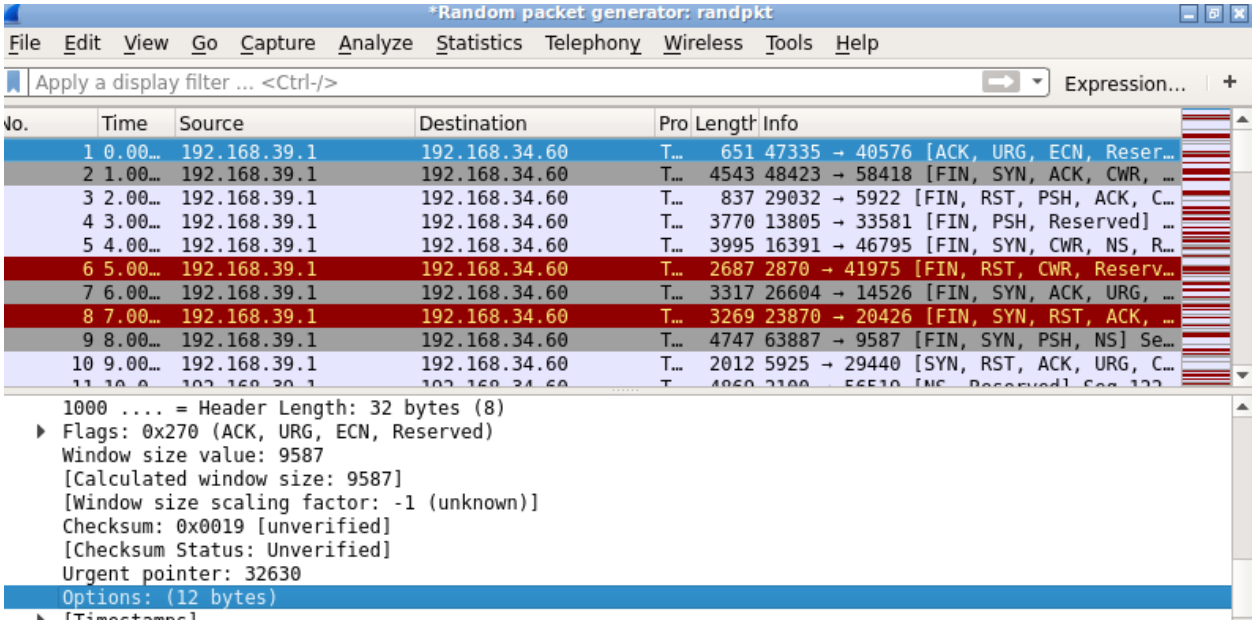


Рис.2.15. Перехоплення трафіку відеопотоку, в режимі реального часу

В результаті проведення значної кількості експериментів виявлено певну кореляцію між параметрами QoS та QoE. На основі цього отримано математичну модель для визначення суб'єктивного рівня задоволеності

користувача за оцінкою QoE залежно від зміни об'єктивних показників QoS, що надаються в мережі SDN для відео в реальному часі. Формалізація математичної моделі співвідношення QoS/QoE проведена на основі отриманих результатів власних експериментальних досліджень, проведених у реальному SDN-обладнанні.

Таблиця 2.2

Оцінка QoS параметрів та їх влив на рівень QoE при перегляді відеопотоку реального часу визначеного методом експертного оцінювання

QoS параметр	Добре (Excellent)	Допустимо (Fair)	Погано (Bad)
Затримка, *D* [мс]	<150	150–200	>200
Втрати, *P* [%]	0–1	1-2%	>2
Пропускна здатність, *C* [мбіт/с]	>2	1–2	<1
Середня оцінка *MOS/QoE* користувачів визначеного на основі додатку	5–4	3.5–4	<3.5

З метою визначення відхилення параметрів QoS в оцінці QoE, необхідно нормалізувати процедуру розрахунку QoS. Тому в роботі визначаються стандартні значення параметрів QoS, при яких забезпечується висока якість сприйняття досліджуваного відеопотоку. Під час проведення дослідження також у процесі роботи рівень важливості параметрів QoS під час перегляду відео встановлено у вигляді таблиці 2.3.

Таблиця 2.3

Рівень важливості параметрів QoS

QoS параметр	Рівень важливості	Ваговий коефіцієнт
Втрата пакетів, *P*	35 %	0.35
Затримка пакетів, *D*	45 %	0.45
Пропускна здатність, *C*	20%	0.2

Нормалізоване значення інтегрального адитивного критерію якості розраховується за формулою (2.3) [125]:

$$Q = QoS(X) = 1 - (w_1(\frac{P_{min}}{P}) + w_2(\frac{T_{min}}{T}) + w_3(\frac{D}{D_{max}})), \quad (2.3)$$

де w_1, w_2, w_3 є ваговими коефіцієнтами важливості параметрів *QoS(X)*, які *t* сумі дорівнюють 2 та коливаються в діапазоні значень [0 – 1].

Відповідно визначенні та усередненні експериментальним шляхом значення оцінок QoE в умовах поступової зміни нормалізованого значення інтегрального адитивного критерію якості представлення точками графічним методом. Після чого зробивши апроксимуючу функцію формалізовано математичну модель кореляції параметрів QoS/QoE:

$$QoE_{video} = f_v(Q) = 5(1-Q^2)^{15Q^5}. \quad (2.4)$$

Відповідно, графіки функції 2.4 показано на рис.2.16.

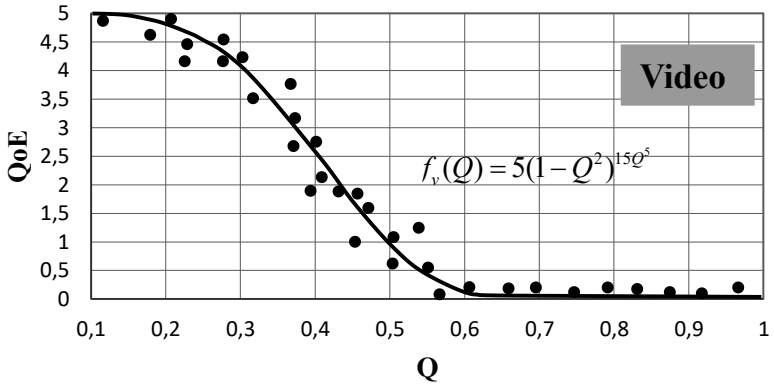


Рис. 2.16. Математична модель кореляції параметрів QoS/QoE для відеопотоку [125]

Таблиця 2.4

Оцінка QoS параметрів та їх влив на рівень QoE при перегляді відеопотоку реального часу визначеного методом експертного оцінювання

QoS параметр	Добре (Excellent)	Допустимо (Fair)	Погано (Bad)
Нормований критерій якості *Q*	0–0.3	0.3–0.35	<1
Середня оцінка *MOS/QoE* користувачів визначеного на основі додатку	5–4	3.5–4	<3.5

При такому підході завдання гарантованого забезпечення замовленого рівня якості сприйняття послуг користувачами за оцінками QoE зводиться до знаходження необхідного нормованого значення інтегрального адитивного

критерію QoS. Вирішення цього завдання може бути здійснено шляхом адаптивного управління мережевими ресурсами та їх раціонального перерозподілу. Зокрема, одним із таких підходів є розробка маршрутизації потоків даних, метрика яких заснована на тому ж інтегральному адитивному критерії.

2.3 Метод маршрутизації інформаційних потоків в програмно-конфігурованих мережах на основі QoE-орієнтованої метрики маршруту

Термін "Мультипотік" (на відміну від більш простого потоку) пов'язаний з тим, що в систему можуть одночасно надходити численні вимоги до QoS та вимагати маршрутизації ресурсів у мережі, що дуже часто зустрічається в сучасних телекомунікаційних мережах. У мультипотоковому середовищі кожен потік має унікальний набір характеристик, це означає, що система не може задовольнити попит на один потік іншим потоком. Завданням проблеми мультипотоковості MCFP (Multicommodity Flow Problem) є передача різних потоків (вимог) трафіку з різних джерел до різних пунктів призначення через мережу з мінімальними витратами, не перевищуючи пропускну здатність мережі.

Маршрутизація на основі обмежень CBR (Contact-based routing) позначає клас алгоритмів маршрутизації, які базують рішення щодо вибору шляху на наборі вимог або обмежень, крім пункту призначення. Ці обмеження можуть бути накладені адміністративною політикою або вимогами щодо якості обслуговування (QoS). Обмеження, накладені вимогами QoS, такі як пропускна здатність, затримка або втрата, відомі як обмеження QoS, а пов'язана з ними маршрутизація відома як маршрутизація QoS. Якщо в мережі немає обмежень пропускної здатності, кожна пара вузлів може спілкуватися по найкоротшому шляху між собою, щоб мінімізувати затримку та вартість. Отже, у реальних телекомунікаційних мережах всі мережеві канали зв’язку мають обмеження пропускної здатності. Крім того, у роботі розглядаються певні обмеження

затримки та втрати пакетів на забезпечення необхідного рівня якості сприйняття послуг. Основне завдання яке необхідно врахувати для QoE маршрутизації це знайти найдешевший можливий спосіб передачі певної кількості потоку через мережу із забезпеченням замовленого рівня якості сприйняття послуг. Тому у роботі зроблено припущення, що мережа нового покоління складатиметься в реальності із взаємопов'язаних вузлів, де кожен канал зв'язку має свою пропускну здатність. Припускаючи, що всі мережеві вузли підтримують OpenFlow і підключені до одного централізованого SDN-контролера введемо деякі визначення та позначення, що використовуються у роботі. Основна мережа на основі SDN (така ж, як традиційна обчислювальна мережа) може бути описана пов'язаним графом $G = (V, E)$, де $V = \{1, 2, ..., v\}$ позначає набір вузлів (Елементи мережі з підтримкою OpenFlow) та E, $E = \{(i, j)\}$ позначає набір ребер, які посилаються на двонаправлені зв'язки між елементами мережі OpenFlow. Кожен канал зв'язку (i, j) має відповідну максимальну пропускну здатність T_{ij}, доступну пропускну здатність t_{ij}, затримку d_{ij} і коефіцієнт втрати пакетів pl_{ij}.

K, $K = \{1, 2, ..., k\}$ *та* $| K | = k$, являє собою сукупність різних потоків. Для кожного потоку k задано три параметри: Sk як джерело потоку, Tk як пункт призначення та Fk як обсяг потоку. Обсяг переданого трафіку формує необхідну пропускну здатність між парою вузлів. Важливим моментом є те, що одиниця обсягу пропускної здатності комутатора повинна відповідати одиниці пропускної здатності каналу зв'язку, яка може становити мегабіт в секунду (Мбіт/с) або пакетів в секунду. Нехай T_k^S L_A, PL_k *SLA та* B_k^S L_A є прийнятними значеннями затримки, коефіцієнта втрат пакетів та середньої необхідної пропускної здатності відповідно, які узгоджені в SLA для послуги k. Матриця M_{pio} (S_k, D_k, F_k) із врахуванням вимог QoS встановлених згідно SLA D_k^{SLA}, P_k^{SLA} *та* T_k^{SLA} розглядаються як вхідні дані для пропонованої QoE- маршрутизації. Метод враховує дану інформацію для кожного потоку, а також інформацію про

мережеві канали зв'язку *(t_{ij}, d_{ij} та pl_{ij})* і обчислює найкращий можливий шлях p_k для кожного запиту k через мережу SDN з мінімальними витратами ресурсів.

В пропонованій мережі метод маршрутизації може забезпечити кілька шляхів для будь-якого потоку k, прагнучи не порушувати висунуті від користувачів вимоги щодо обмеження якості сприйняття сервісу. Всі визначені шляхи обслуговування k ведуть від джерела S_k до пункту призначення D_k, так що кожен з них направляє частину всього обсягу потоку F_k. Для простоти розуміння зробимо припущення, що не існує пари потоків з однаковим початком і пунктом призначення.

Отже, завданням оптимізації є спрямовувати всі потоки в мережі з мінімальними витратами. Рівняння 2.5 як цільова функція являє собою мінімізацію витрат потоку, яка залежить від вартості каналу зв'язку, визначеної для всіх QoE вимог трафіку K. У літературі це формулювання називається формуванням вузлових зв'язків. C_{ij} – це собівартість одиниці каналу зв'язку *(i,j)*, а Xk_{ij} величина обсягу, що відповідає потоку k, направленому в каналі зв'язку *(i,j)*.

$$Minimize \sum_{(i,j)\in E} \sum_{k} C_{ij(QoE)} X_{ij}^{k} \tag{2.5}$$

Обмеження функції:

У роботі введено декілька типів умов, які накладаються на програмно-конфігуровану мережу та послуги, які надаються для кінцевих користувачів.

Обмеження затримки шляху для кожного потоку визначено у рівнянні 2.6, де d_p^k – наскрізна затримка маршруту маршрутизації, визначена для потоку k, а $D_{SLA(QOE)}^k$ максимально прийнятна затримка для потоку k при якому забезпечується необхідний рівень якості сприйняття послуги, погоджена згідно договору $SLA(QOE)$.

$$d_p^k \le D_{SLA(QOE)}^k \tag{2.6}$$

Обмеження втрати пакету шляху для кожної вимоги визначено у рівнянні 2.7, де pl_p^k – загальний коефіцієнт втрат пакету для маршруту маршрутизації p^k, визначений для потоку k, а рівень $PL_{SLA(QOE)}^k$ є максимально допустимою втратою пакету для потоку k, узгодженим у SLA.

$$pl_p^k \le PL_{SLA(QOE)}^k \tag{2.7}$$

Обмеження пропускної здатності шляху, яке повинно задовольняти шлях *pk* для потоку *k*, сформульовано у рівнянні 2.8. Обмеження пропускної здатності шляху, яке повинно задовольняти шлях p^k для потоку k, сформульовано у рівнянні 2.8:

$$t_p^k \ge T_{SLA(QOE)}^k \tag{2.8}$$

де b_p^k – пропускна здатність для шляху p^k для потоку k, а $T_{SLA(QOE)}^k$ – мінімально необхідна пропускна здатність для потоку k, погоджена в SLA.

Обмеження пропускної здатності каналу зв’язку сформульовано у рівнянні 2.9. У багатопотоковому середовищі кожен шлях може бути частиною безлічі шляхів маршрутизації, що використовуються різними потоками. Тоді підсумовування обсягу різного потоку в будь-якій лінії зв'язку *(i, j)* має бути меншим за доступну пропускну здатність лінії зв'язку t_{ij}. Це обмеження може відповідати контексту управління перевантаженнями в мережі. Оскільки в мережі SDN ми могли б оцінити доступну пропускну здатність зв’язку за допомогою доступу до лічильників елементів мережі, наявну пропускну здатність зв’язку можна було б розглядати замість максимальної пропускної здатності зв’язку.

$$\sum_{k \in K} X_{ij}^k \le t_{ij}, \forall (i,j) \in E \tag{2.9}$$

Обмеження використання балансування навантаження в каналі зв’язку . Щоб зменшити ймовірність перевантаження та збалансувати обсяг трафіку в каналах зв’язку , ми прагнемо також розглянути використання каналу в процесі розподілу шляхів. Загалом, коефіцієнт використання на лінії зв'язку

вимірюється діленням поточного навантаження на лінію з максимальною пропускною здатністю лінії, в одиниці відсотка. З урахуванням інформації про стан мережевого зв’язку, зібраної контролером SDN, використання зв’язку *(i,j)* можна розрахувати за рівнянням 2.10.

$$Utilization.rate.in.link(i,j) = \frac{T_{ij} - t_{ij}}{T_{ij}}, \forall (i,j) \in E \qquad (2.10)$$

Щоб урівноважити розподіл трафіку за мережевими лініями та уникнути перевантажень, ми враховуємо обмеження на коефіцієнт використання каналу. Алгоритм маршрутизації виключає канали з вищим коефіцієнтом використання каналу, ніж обмеження, зі сценарію розрахунку шляху, щоб запобігти перевантаженню та мати збалансоване навантаження. Взагалі, зв'язок із коефіцієнтом використання більше ніж приблизно 75%-80% вважається перевантаженими зв'язками, тому поріг використання може бути встановлений у цьому діапазоні. У нашому випадку значення за замовчуванням може бути заздалегідь визначене в базі даних, а в якості альтернативи контролер SDN може динамічно регулювати межу використання каналу на основі ситуації в мережі, наприклад обсягу трафіку та швидкості надходження потоку. Крім того, якщо в найгіршому випадку через сплеск трафіку жоден шлях не задовольняє вимоги до пропускної здатності, враховуючи заздалегідь визначений ліміт використання каналу зв'язку, його можна обережно збільшити.

Якщо $U_{Threshold}$ представляє межу використання лінії зв'язку в пропонованій мережі SDN, то межі використання записується згідно формули 2.11:

$$(\sum_{k \in K} X_{ij}^{k} + T_{ij} - t_{ij}) / T_{ij} \le U_{Threshold}, \forall (i,j) \in E \qquad (2.11)$$

і, отже, принцип балансування навантаження для маршрутизації формується у вигляді умови:

$$(\sum_{k \in K} X_{ij}^{k} + T_{ij} - t_{ij}) / T_{ij} \le U_{Threshold}, \forall (i,j) \in E \qquad (2.12)$$

Закон збереження потоку. Цей закон стверджує, що загальний вхідний потік у кожен вузол мережі дорівнює загальному вихідному потоку з цього вузла, за винятком вузлів джерела та призначення потоку. Якщо розглянутий вузол є джерелом потоку, загальний вихідний потік мінус загальний вхідний потік повинен дорівнювати обсягу потоку. Якщо розглянутий вузол є пунктом призначення потоку, загальний вхідний потік мінус загальний вихідний потік повинен дорівнювати обсягу потоку [126]. Таким чином закон збереження потоку для запропонованої мережі записується рівнянням 2.13, яке гарантує однакову пропускну здатність у всіх шляхах через визначені маршрути:

$$\sum_{(i,j)\in E} X_{ij}^{k} - \sum_{(j,i)\in E} x_{ji}^{k} = \begin{cases} F^{k}, i = S^{k} \\ -F^{k}, i = D^{k} \\ 0, i \neq S^{k}, i \neq D^{k} \end{cases} \quad (2.13)$$

У цьому підрозділі описано показники вартості шляху, що використовуються для QoE-орієнтованого методу маршрутизації. Мета полягає в тому, щоб зважити шлях на основі відповідних показників, щоб визначити вартість різних шляхів і відповідно зрозуміти, чи слід обирати один шлях над іншим. У традиційній схемі мережі більшість розроблених протоколів маршрутизації враховують лише один параметр, пов'язаний із QoS (наприклад, ймовірність втрати пакетів, пропускну здатність, джитер та затримку) або інший параметр, такий як кількість стрибків та довжина каналу в процесі прийняття рішення про шлях. Наприклад, OSPF (Open Shortest Path First) як найвідоміший протокол маршрутизації в традиційних мережах IP використовує пропускну здатність лінії зв'язку як метрику вартості лінії зв'язку в алгоритмі обчислення найкоротшого шляху.

Показниками вартості маршруту необхідних для забезпечення вимог QoE, що розглядаються в роботі, є пропускна здатність, коефіцієнт втрат пакетів та затримка. Він представлений у вигляді зваженої суми цих метрик у рівнянні 2.14, де $C_{ij(QoE)}$ представляє собівартість одиниці зв'язку *(i, j)*, метрики t_{ij}, pl_{ij} та

d_{ij} посилаються на доступну пропускну здатність лінії зв'язку, коефіцієнт втрати пакетів та затримку у каналі *(i, j)* відповідно .

$$C_{ij(QoE)} = \alpha \times t_{ij} + \beta \times pl_{ij} + \gamma \times d_{ij} \tag{2.14}$$

Коефіцієнти α, β, γ – коефіцієнти масштабування кожної метрики із співвідношенням, вираженим у рівнянні 2.15. Отже, кожна метрика може мати різну вагу, щоб надати пріоритет конкретній.

$$\alpha + \beta + \gamma = 1, 0 \le \alpha, \beta, \gamma \le 1 \tag{2.15}$$

Це обчислення дозволяє зважувати мережеві шляхи на основі важливості затримки, втрати пакетів і пропускної здатності для конкретної послуги щодо підходу до класифікації трафіку. Наприклад, програма контролю та моніторингу заторів, яка обслуговується камерою чи датчиками, потребує суворих вимог до наскрізної затримки та дуже низької втрати пакетів. Додаток камер спостереження потребує високої пропускної здатності. Навпаки, додаток для аналітичних даних не має суворих вимог. Отже, пріоритет, що надається ваговими коефіцієнтами для метрики маршруту може бути різним у кожному випадку. Тому у роботі запропоновано динамічну метрику вартості шляху залежно від типу сервісу та її вимог щодо замовленого рівня якості сприйняття послуги через угоду SLA.

Щоб виразити зважену суму незалежних метрик, значення цих метрик потрібно відкоригувати до умовно загальної шкали. Ми використовуємо метод нормалізації мін-максу характеристик, щоб нормалізувати діапазон цих незалежних метрик. Цей метод масштабує діапазон усіх значень і приводить все в діапазон [0, 1]. Загальна формула методу нормалізації подана як:

$$x' = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \tag{2.16}$$

де x – вихідне значення, а ′x – нормоване значення, припускаючи, що x має обмежений діапазон [x_{min}, x_{max}]. Вирази 2.17-2.19 формалізують нормування показників QoS:

$$t'_{ij} = \frac{t_{\max} - t_{ij}}{t_{\max} - t_{\min}}, t_{\min} \le t_{ij} \le t_{\max}, t_{\max} \ne t_{\min} \quad (2.17)$$

$$pl'_{ij} = \frac{pl_{ij} - pl_{\min}}{pl_{\max} - pl_{\min}}, pl_{\min} \le pl_{ij} \le pl_{\max}, pl_{\max} \ne pl_{\min} \quad (2.18)$$

$$d'_{ij} = \frac{d_{ij} - d_{\min}}{d_{\max} - d_{\min}}, d_{\min} \le d_{ij} \le d_{\max}, d_{\max} \ne d_{\min} \quad (2.19)$$

Беручи до уваги той факт, що більша доступна пропускна здатність призводить до нижчої вартості лінії зв'язку, отже, до нижчої вартості каналу, 2.17 обчислює нормоване значення доступної пропускної здатності лінії зв'язку t_{ij}, тоді як b_{max} і b_{min} представляють максимальний і мінімальний діапазон пропускної здатності лінії зв'язку в основній транспортній мережі відповідно. Вони можуть мати постійне значення або динамічно скориговане значення на основі інформації про топологію мережі в будь-який момент часу. Існує прямий зв’язок між коефіцієнтом втрати пакетів і вартістю лінії зв'язку, так що нижчий коефіцієнт втрат пакетів лінії зв'язку, нижча вартість лінії зв'язку. Рівняння 2.18 обчислює нормоване значення коефіцієнта втрати пакетів pl_{ij} на лінії зв'язку *(i,j)*. Параметри pl_{min} та pl_{max} відносяться до мінімального та максимального діапазону для коефіцієнта втрати пакетних ліній зв'язку в мережі, pl_{min} може розглядатися як нуль, а pl_{max} може мати постійне значення або динамічно скориговане значення на основі інформації про коефіцієнт втрати пакетів у даній мережі. Подібність, затримка шляху має пряму залежність від вартості шляху. Рівняння 2.19 представляє нормоване значення затримки зв'язку. Параметри d_{min} та d_{max} є нижньою та верхньою межею затримки зв'язку відповідно. Нижня межа може бути нульовою, а верхня будь-яким постійним значенням відносно затримки лінії зв'язку в даній мережі. Відзначаючи, що якщо верхня межа в будь-якій з цих функцій дорівнює нижній межі, що рідко можливо в мережі, значення функції буде 1.

Таким чином, завдання забезпечення замовленого рівня якості сприйняття послуги користувачами згідно оцінок QoE, що вказують важливість сервісу для

конкретного бізнес процес полягатиме у пошуку необхідно нормалізованого значення інтегрального адитивного критерію QoS, розв’язання якого можна здійснити шляхом адаптивного управління мережними ресурсами та їх раціонального перерозподілу, шляхом використання вище запропонованої маршрутизації потоків даних, метрика якої, базується на цьому ж самому інтегральному адитивному критерію.

Таблиця 2.4а

Співвідношення між вартістю (метрикою маршруту) та рівнями MOS/QoE для відеопотоку реального часу [125]

QoS параметр	Добре (Excellent)	Допустимо (Fair)	Погано (Bad)
Нормований критерій якості тотожний метриці маршруту $Q = C_{ij(QoE)}$	0–0.3	0.3–0.35	<1
Середня оцінка *MOS/QoE*	5–4	3.5–4	<3.5

2.4 Інтелектуальна система моніторингу якості функціонування інтенційно-орієнтованої мережі за критерієм QoE

Сучасні мережі висувають високі вимоги щодо забезпечення прийнятного рівня якості сприйняття контенту [127-129]. Це пов'язано з великою конкуренцією різних видів потокових сервісів, як для перегляду фільмів, прослуховування музики, проведення бізнес-конференцій, так і для потокових ігрових сервісів. Якщо якість послуги погана, користувач може легко переключитися на конкурента, тому корпорації шукають нові способи підтримки якості сприйняття. Одним із таких способів є використання системи моніторингу параметрів мережі та розрахунок рівня QoE, згідно з яким може бути прийнято рішення про перенаправлення потоку даних іншим маршрутом до одержувача. Такий підхід дозволяє підтримувати необхідний рівень QoE та правильно розподіляти ресурси мережі. Однак цей метод має суттєві недоліки, це надмірність сигнальних даних і велике навантаження на мережеве обладнання та сам контролер SDN [130]. Що в критичний момент може

вплинути на загальну продуктивність мережі [131-133]. У цьому розділі пропонується використовувати машинне навчання для прогнозування рівня QoE на основі попередньо зібраної інформації про параметри підключення та рівень якості їх сприйняття. Таке рішення дозволить зменшити обсяг сервісного трафіку в каналах зв'язку та зменшити навантаження на мережеве обладнання.

Основною метою роботи є підвищення рівня QoE для кінцевого користувача, шляхом впровадження модуля машинного навчання в програмно-конфігурованих інтенційно-орієнтованих мережах, що в свою чергу забезпечить необхідний рівень QoE.

Необхідність забезпечення прийнятного рівня якості сприйняття для кінцевого користувача стає однією з головних вимог до сучасних потокових сервісів. Однак у попередньому підрозділі було доведено, що розгортання систем відстеження рівня якості сприйняття є складним і вимагає великих ресурсів як контролера, так і мережі, в якій відбувається розгортання. Тому було запропоновано використання машинного навчання для прогнозування та оцінки загального рівня якості сприйняття в програмно-визначених мережах. Машинне навчання та інструменти штучного інтелекту мають дуже широке застосування в задачах контролю та корекції помилок датчиків. Ці засоби та інструменти також знайшли своє застосування для покращення роботи мереж. Зокрема, Random Forest був обраний як один з найточніших методів машинного навчання для прогнозування. Згідно з результатами, наведеними в цих роботах [134], точність прогнозування становить 78-80% залежно від ступеня k-перехресної перевірки. Точність оцінок якості відео щодо суб’єктивних даних оцінюється за допомогою коефіцієнта кореляції Пірсона [135]:

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i - \bar{y})^2}} \tag{2.20}$$

де x_i та y_i – виміряні та прогнозовані значення MOS, $\bar{x}$ та $\bar{y}$ – відповідно середні значення виміряних та передбачених оцінок MOS.

Середньоквадратична помилка визначається:

$$RMSE = \sqrt{\frac{\sum_{i=1}^{n}(y_i - y_i)^2}{n}} \tag{2.21}$$

де y_i та y_i, прогнозовані та виміряні значення оцінки MOS відповідно.

Запропонована архітектура мережі IBN мережі з інтелектуальною QoE моніторинговою системою, показана на рис.2.17 [136].

Принцип пропонованої архітектури полягає в наступному, контролер SDN/IBN з індикацією модуля моніторингу QoE виконує вимірювання параметрів мережі (затримки, втрати пакетів та ін.). Вимірювання параметрів відбувається за схемою, що наводиться у підрозділі 2.2.

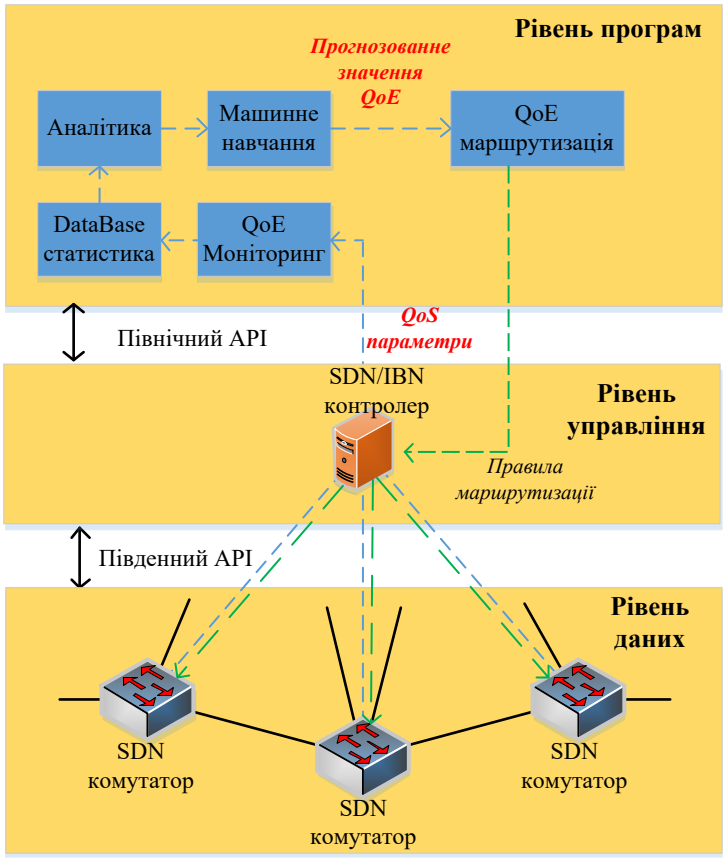


Рис. 2.17. Запропонована архітектура IBN з інтегрованим модулем ML [136]

Періодичне вимірювання параметрів мережі необхідно для перенавчання алгоритму машинного навчання, використовуючи отримані дані як навчальний

набір. Відстеження поточного рівня QoE і в разі критичної помилки система зможе швидко відреагувати та відновити встановлений рівень QoE. Оскільки стан мережі, вузли та кількість вузлів можуть динамічно змінюватися і без постійного оновлення статистики параметрів мережі, точність прогнозування знижується. Отже, отримані дані поміщаються в базу даних, де вони аналізуються та передаються в модуль машинного навчання, загальний вигляд алгоритму Random Forest показано на рис.2.18. Результатом роботи цього модуля є передбачений рівень QoE. На основі передбаченого рівня модуль QoE-маршрутизації приймає рішення про необхідність внесення змін у правила маршрутизації та надсилає відповідну команду контролеру SDN, який, у свою чергу, вносить зміни в таблиці потоків маршрутизаторів через Southbound API.

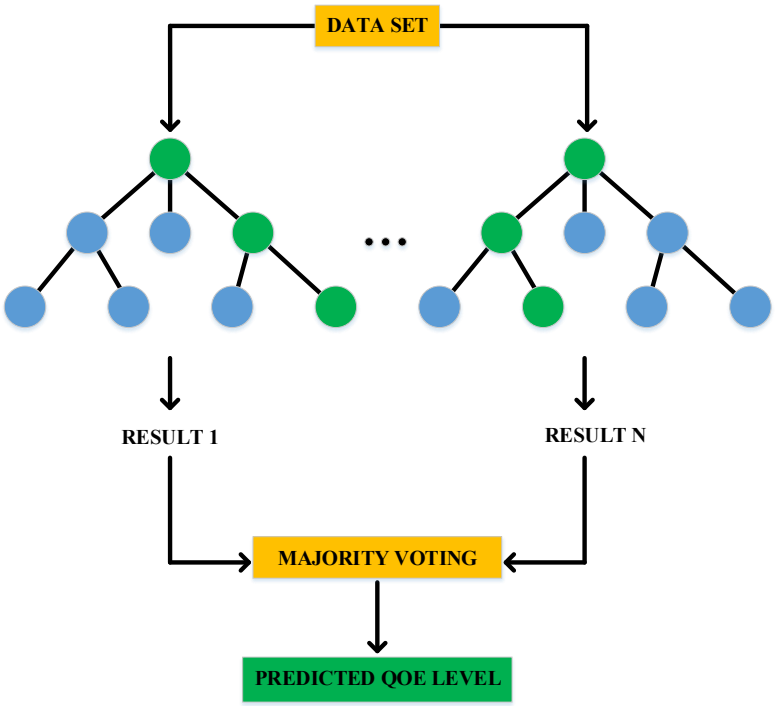


Рис. 2.18. Загальний вигляд Random Forest

Досліджено практичну інтеграцію модуля машинного навчання у віртуальній мережі SDN. Для побудови мережі використовувався емулятор Mininet. Це дозволяє розгорнути реалістичну віртуальну програмно-визначену мережу на одній машині за кілька секунд. На емуляторі мереж можна

розробляти та тестувати нові технології і кінцевий результат не буде відрізнятися від реалізації у фізичній мережі. На роль контролера SDN був обраний ONOS з підримкою IBN менеджера, як один з провідних SDN контролерів з відкритим кодом. Що також активно підтримується розробниками та доповнюється підтримкою передових технологій у сфері програмно-визначених мереж та віртуалізації мережевих функцій.

Таким чином, емулятор Mininet будує топологію мережі, показану на рис.2.19 Створюється мережа з 3 комутаторів SDN, 2 хостів і контролера SDN.

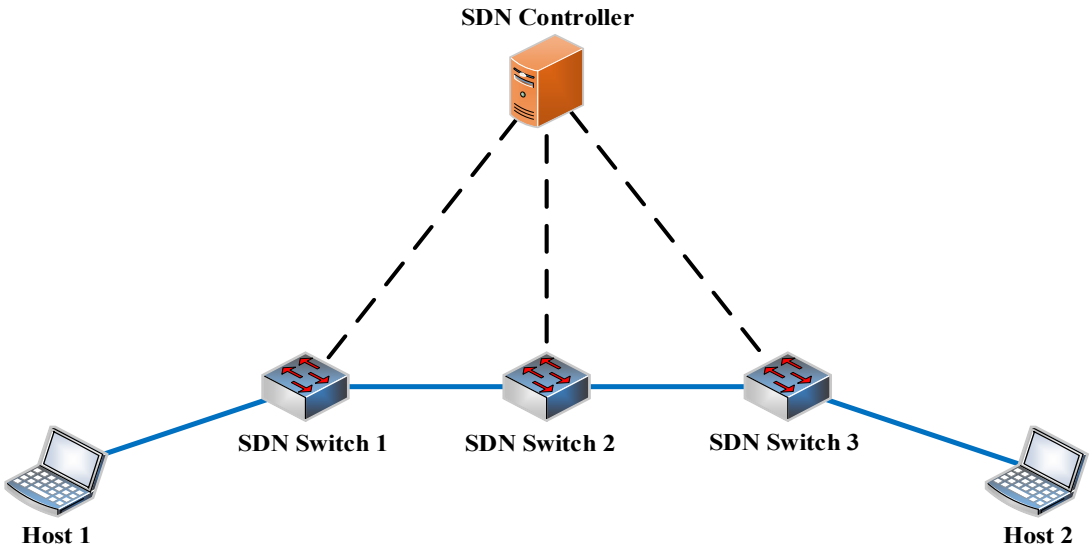


Рис. 2.19. Топологія мережі, створена в Mininet

У практичній реалізації інтеграції модуля машинного навчання в програмно-конфігуровану мережу було проведено дослідження з порівнянням передбачуваного рівня якості сприйняття і виміряного за допомогою системи моніторингу QoE для VoIP і потокового відео. Мережні параметри були згенеровані випадковим чином для затримки - 0,001-0,015 сек, втрати пакетів - 0,25-15%, і записані в скрипт Python.

Отримані значення виміряних і прогнозованих рівнів QoE показані графічно на рис. 2.20 та 2.21.

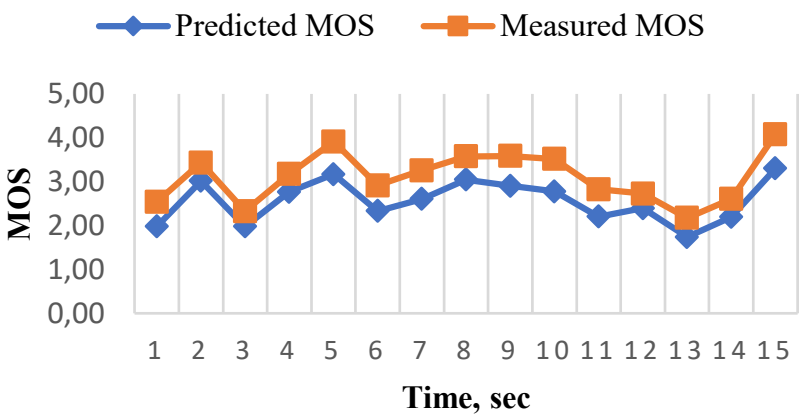


Рис. 2.20. Порівняння прогнозованого MOS та виміряного MOS для трафіку VoIP

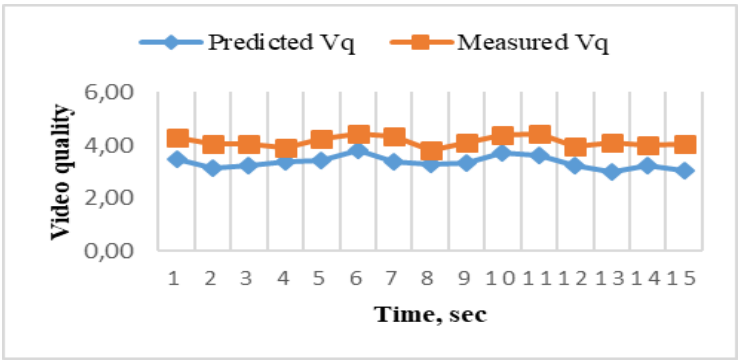


Рис. 2.21. Порівняння Vq між прогнозованими та виміряними даними [136]

За отриманими даними видно, що є помилка в прогнозах рівня QoE щодо виміряних значень за допомогою системи моніторингу. Як зазначалося в попередньому розділі, запропоноване рішення не може повністю виключити систему моніторингу через недостатню точність розрахункових результатів машинного навчання, як показано вище. Але основним недоліком систем моніторингу є надмірність сервісного трафіку. Надлишковість сигнального трафіку в обраній для порівняння системі моніторингу можна розрахувати так:

Припустимо, що необхідно вимірювати затримку мережі кожні 10 мс, тоді через 1 секунду буде передаватися:

$$pk = \frac{1000ms}{10ms} = 100\,packets \tag{2.22}$$

Враховуючи, що розмір пакету, який використовується для визначення затримки, становить 24-32 байти, через 1 секунду канал буде завантажений 1,92-2,56 кбіт/с, тільки на вибраній ділянці мережі. Крім того, якщо врахувати статистичні пакети, які використовуються для вимірювання втрат пакетів у мережі, зайнята пропускна здатність каналу лише сигнальними даними може досягати від 3,84 кбіт/с і до сотень кбіт/с і навіть Мбіт/с, залежно від розміру мережі та кількості вузлів.

Однак, якщо використовується модуль машинного навчання, обсяг сигнального трафіку в мережі зменшується приблизно на 30%, отримані результати показані на рис.2.22.

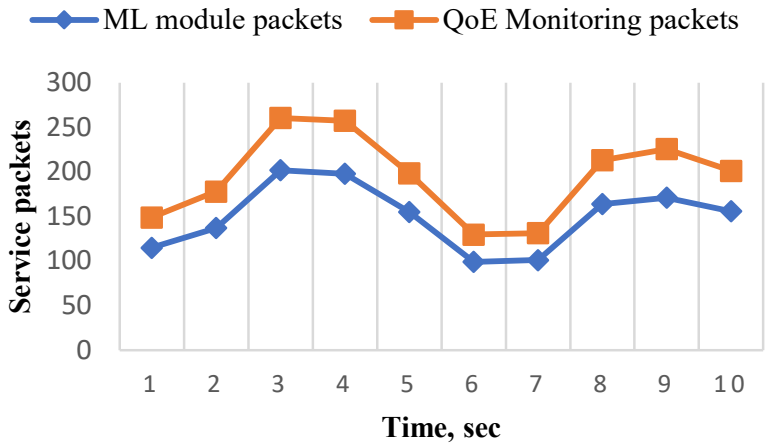


Рис. 2.22. Зменшення сигнального трафіку з прогнозуванням ML [136]

Якщо кількість сигнальних пакетів зменшено до 30%, модуль машинного навчання показує максимальну точність передбачення. Однак, якщо необхідно зменшити кількість сигнальних пакетів більш ніж на 30%, точність прогнозування знижується, але значно зменшується обсяг сервісного трафіку в мережі. Тому в реальних мережах параметр точності прогнозування і частота вимірювання параметрів мережі можуть змінюватися в залежності від потреб мережі.

2.5 Метод управління якістю сприйняття послуг в програмно-конфігурованих інтенційно-орієнтованих мережах на основі розробленої інтелектуальної QoE моніторингової системи

Пропонована інтелектуальна мережа на основі намірів на відміну від SDN переводить стратегію управління мережею у більш високий рівень, поєднуючи автоматизацію з інтелектом. IBN та SDN мають потенціал для розвитку один одного. Для реалізації мережі на основі намірів модифікується контролер SDN для виконання бажаних політик.

Метою IBN є створення розширюваної структури визначення мережевих вимог клієнтів з урахуванням природної мови на мову зрозумілій мережевій інфраструктурі. А саме, у пропонованій IBN клієнти можуть робити запит на отримання відповідного QoE рівня якості сприйняття послуг від кінця до кінця для будь-якої послуги у певний момент часу. Цей підхід організовано шляхом створення QoE намірів клієнтами мережі. Наміри QoE формуються у вигляді простих чисел від 1 до 5. Чим вище значення показника QoE, тим краща якість послуги гарантується, тим дорожче буде надання цієї послуги в мережі IBN. Після цього за допомогою заданого QoE-знання або інтелектуального механізму, що самонавчається, виділяються відповідні ресурси, які потім автоматично перетворюються в команди конфігурації мережевого обладнання та інтерфейсні операції.

Виходячи із сказаного вище, у роботі пропонується архітектура мережі IBN на основі SDN (рис.2.23).

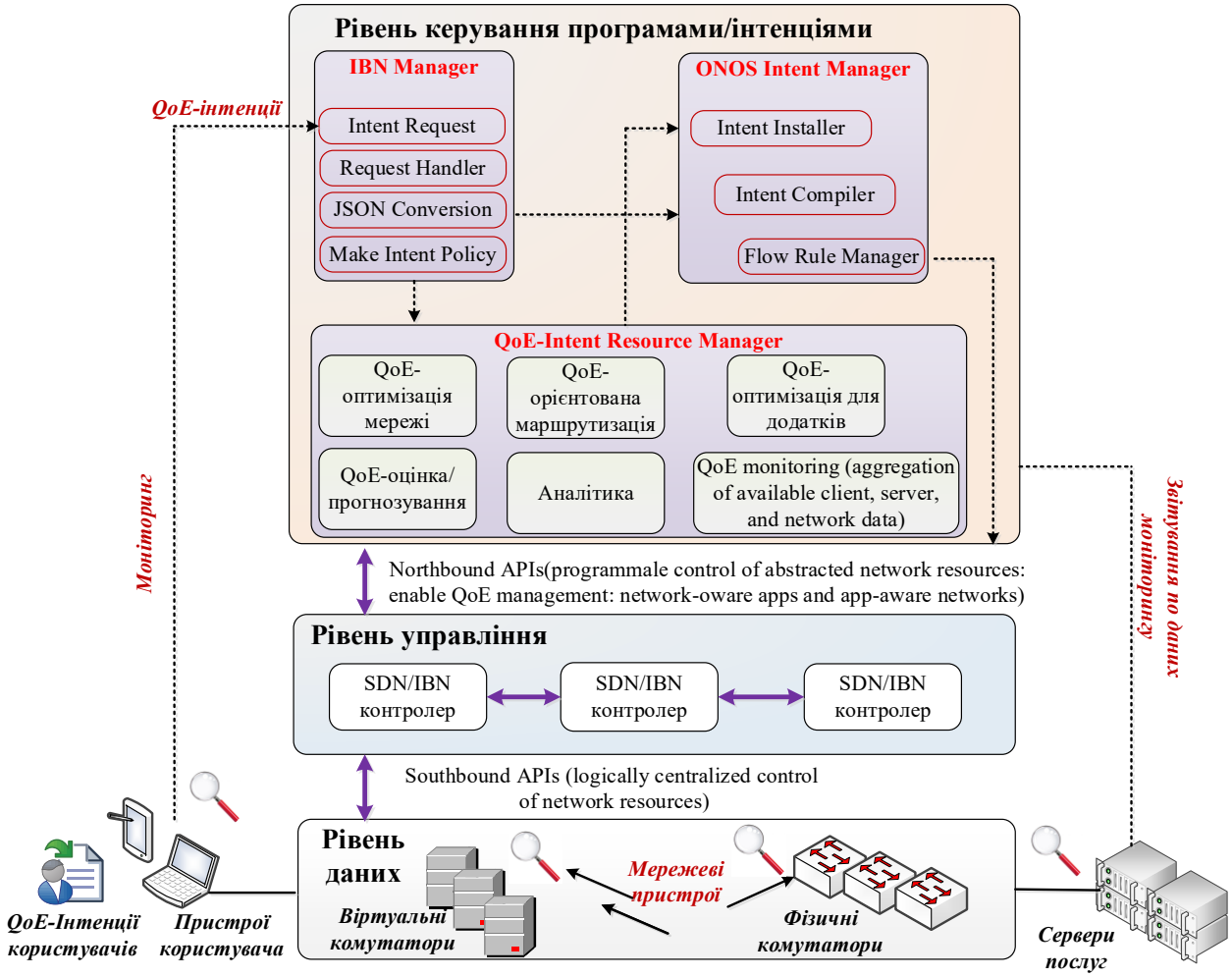


Рис.2.23. Архітектура IBN на основі SDN з QoE управлінням [125]

Архітектура пропонованої мережі IBN дещо відрізняється від SDN. Зокрема, їхньою загальною рисою є поділ площини мережі керування та мережі передачі даних, що дозволяє з центральної точки програмно за допомогою контролера гнучко конфігурувати інфраструктуру мережі. Зокрема в нашій роботі це контролер ONOS SDN. Який після удосконалення програмного забезпечення у роботі називатиметься SDN/IBN контролером. Така гнучкість конфігурації забезпечується відкритими для модифікацій інтерфейсами northbound та southbound API архітектури SDN, які дозволяють обмінюватися інформацією між різними функціональними об'єктами цієї архітектури. Відмінність існуючої SDN від запропонованої IBN полягає в тому, що в архітектурі SDN ми програмно вводимо нову площину application/intent

management plane. Основними елементами цієї площини є контролер ONOS IBN, пропонований менеджер IBN та менеджер ресурсів QoE-інтенції. Загальний принцип роботи описується наступним чином. Спочатку клієнти запитують QoE-інтенції у мережі IBN через спеціальні веб-портали чи мобільні додатки. На рівні площини додатків QoE-інтенції збираються та аналізуються розробленим IBN-менеджером. Контролер ONOS взаємодіє з IBN -менеджером на рівні керування через Northbound API. Модуль менеджера намірів контролера ONOS отримує запит від IBN Manager у формі JSON і після компіляції перетворює його на низькорівневу команду, яка виконується на комутаторах. Потім він відправляє намір (у формі JSON) до ONOS контролера мережі для конфігурації мережевого обладнання. Для цього контролер зв'язується з модулем менеджера правил потоку, щоб зберегти запис про намір, створений для відповідного вузла. Менеджер IBN звертається до менеджера ресурсів, щоб проаналізувати стан мережі та переконфігурувати її, коли намір QoE не забезпечується. Під реконфігурацією ми впершу чергу розуміємо зміну правил маршрутизації. Зокрема, ідея полягає в тому, щоб знайти оптимальний шлях передавання даних, яким буде забезпечений намір клієнта щодо замовленого рівня якості обслуговування. У дисертаційній роботі таку маршрутизацію називатимемо QoE-aware routing (QoE-орієнтована маршрутизація). Нижче ми докладно пояснимо, як працює пропонована QoE-маршрутизація на практиці.

Другою ключовою вимогою для ефективної IBN є моніторинг. З переходом від політик до намірів виникає необхідність забезпечити їхнє ефективне виконання. Політики, які наслідують традиційну модель дій за умовою події, не потребують моніторингу, оскільки в них не вказана мета. У разі намірів ціль явно виражена, тому моніторинг мережі для забезпечення успішного досягнення цієї мети є критично важливим.

Наприклад, припустимо, що мережа визначає намір, згідно з яким усі потоки відеоконференцій повинні мати розширення 720p і не повинні часто

перериватися. Без моніторингу відеотрафіку організації неможливо визначити, чи вдалося реалізувати цей намір. Насправді такий моніторинг має бути дуже специфічним, оскільки мережа повинна не тільки розуміти якість відеопотоків, що входять і виходять з мережі, але й розуміти їх джерела (наприклад, Skype Business або Youtube) і, можливо, їх мета (дзвінок по Skype члену сім'ї чи клієнту). Крім того, коли намір багаторівневий (наприклад, компанія хоче гарантувати високу швидкість завантаження файлів на додаток до вищезгаданого наміру потокового відео), стає ясно, що єдиний спосіб ефективно реалізувати намір це всебічний моніторинг усіх аспектів мережі з високою роздільною здатністю. Встановлено, що без моніторингу неможливо визначити справжній стан мережі, що унеможливлює ефективне налаштування мережі для забезпечення найвищої якості обслуговування.

Моніторинг QoE на рівні мережі оператором інфраструктури SDN спрощується, оскільки контролер автономно формує "глобальне уявлення" мережі на основі її топології та показників продуктивності (таких як пропускна здатність, затримка та статистика втрати пакетів). Це дозволяє оператору мережі застосовувати різні стратегії оптимізації, орієнтовані на QoE, та приймати оптимальні рішення щодо маршрутизації у всій мережі. Крім того, архітектура SDN надає відкриті інтерфейси, які полегшать складання звітів про QoE кінцевими споживачами та серверами додатків за факторами впливу QoE, що відслідковуються, на рівні управління додатками/інтенціями. Ці інтерфейси забезпечать основу реалізації спільного управління QoE між додатками кінцевих клієнтів і базової IBN. У майбутньому мережа з високорівневими вимогами клієнтів розумітиме ці QoE-інтенції контролюватиме себе і матиме можливість змінювати базову інфраструктуру для оптимізації самої платформи, і все це в режимі реального часу.

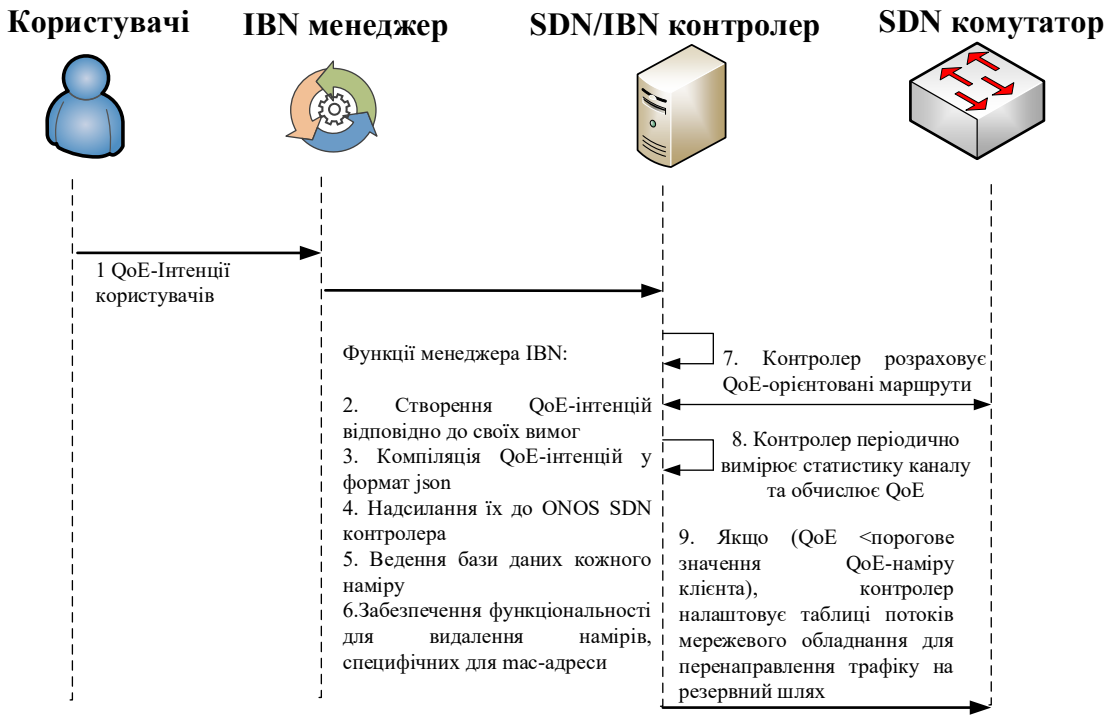


Рис.2.24. Процес роботи QoE-орієнтованої моделі маршрутизації для IBN

У цьому розділі представлено дослідження методу управління якістю сприйняття послуг з використанням розробленої інтелектуальної системи моніторингу QoE та маршрутизації потоків, щоб подолати зниження QoE і зберегти якість послуг, що надаються кінцевим користувачам, таких як VoIP і потокове відео. Метод заснований на використанні IBN контролера ONOS з реалізацією додаткової функціональності для перемикання маршруту передавання даних на резервний шлях на основі QoE-маршрутизації. Який забезпечує кращу QoE оцінку для певного типу послуг, якщо основний шлях не працює або має незадовільну оцінку QoE. Алгоритм методу управління якістю сприйняття послуг в програмно-конфігурованих інтелектуальних мережах показаний на рис. 2.25.

Рис.2.25. Блок схема методу управління якістю сприйняття послуг в програмно-конфігурованих мережах [124]

Реалізація, яка використовується для забезпечення підтримки QoE на прийнятному рівні, полягає в частому моніторингу QoS параметрів функціонування мережі, а саме: затримки, втрат даних та пропускної здатності на початку роботи системи з метою навчання. Після чого частий моніторинг замінюється на використанні інтелектуальної системи прогнозування параметрів в каналах зв'язку. Відповідно використовуючи запропоновану математичну модель кореляції параметрів QoS/QoE контролером мережі програмно оцінюється якість сприйняття послуг в залежності від виміряних/прогнозованих QoS параметрів для кожного маршруту передавання даних. Таким чином, контролер визначає найкоротший шлях між вузлами

призначення і другий шлях, який буде резервним, якщо основний шлях забезпечить неприйнятну якість. Таким чином, якщо розраховане значення нижче необхідного рівня, контролер змінює правила OpenFlow і перенаправляє трафік на альтернативний шлях.

Для оцінки досліджуваних систем або протоколів в мережевий інженерії рішення розгортається на симульованих або емулюючий мережах. Основною платформою для програмно-конфігурованих мереж є емулятор Mininet на базі Linux. Завдяки простій віртуалізації, його досить легко використовувати в дослідженнях, а також можливості моделювати повноцінну велику мережу з віртуальними комутаторами і хостами на одній машині. А оскільки Mininet емулює мережу, а не моделює, параметри, конфігурації і додатки, протестовані в середовищі Mininet, можуть бути застосовані безпосередньо до реальних мереж у тому числі і для розгортання майбутніх IBN. Mininet використовує Open vSwitch, широко підтримуваний програмний комутатор SDN, який використовує протокол OpenFlow для зв'язку з контролером. Цей протокол є найбільш поширеним південним інтерфейсом в SDN і є ключовим в стандарті програмно-конфігурованих мереж. Протокол OpenFlow зазвичай використовується як віртуальними, так і фізичними комутаторами і маршрутизаторами, наприклад, комутаторами Zodiac FX/GX/WX компанії NorthBound Networks.

Проблема забезпечення необхідної якості обслуговування існує як в традиційних, так і в програмно-конфігурованих мережах. Як відомо, в програмно-конфігурованих мережах площина управління відділена від площини даних, що дає змогу контролеру переглядати і управляти всією мережею (рис.2.26). Також відкритість мережевих операційних систем і зручний і повний доступ до налаштувань мережевого обладнання відкриває доступ для впровадження програм, які дозволять вирішити цю проблему.

Для прикладу розглянемо топологію мережі (рис.2.26) у якій існує два шляхи передачі даних від хоста1 (h1) до хоста2 (h2):

- Шлях №1, найкоротший шлях: h1-s2-s3-h2, зелені стрілки.
- Шлях №2, резервний шлях: h1-s2-s1-s3-h2, помаранчеві стрілки.

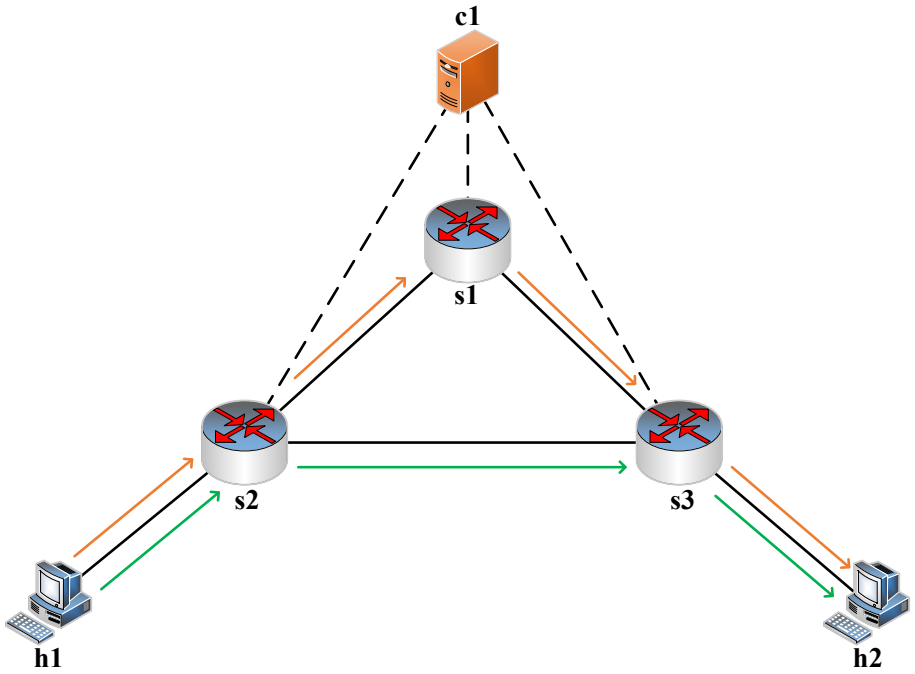


Рис.2.26. Доступні шляхи передачі даних в програмно-керованих мережах

За замовчуванням контролер вибирає найкоротший шлях до вузла призначення. З огляду на те, що в реальній мережі параметри каналу, по якому буде відбуватися передача, можуть не забезпечити необхідну якість послуг для кінцевого користувача. Хоча альтернативний шлях на один вузол є довшим, він може бути менш завантажений, що забезпечить необхідну користувачеві якість обслуговування.

Зокрема, пропоноване програмне забезпечення на контролері мережі обчислює найкоротший шлях між вихідним та кінцевим хостами, який буде як основний шлях передачі, а також другий найкоротший шлях (якщо такий існує), який буде резервним у випадку незадовільної якості обслуговування в процесі передавання відеопотоку реального часу. Потім починається процес моніторингу якості; контролер SDN/IBN періодично збирає статистику з комутаторів (різні статистичні дані для кожного типу програми) і використовує їх для обчислення QoE рівня за 5-бальною шкалою [124]. Якщо передбачуване

значення нижче вказаного порогу, тоді автоматично встановлюються відповідні правила для перенаправлення трафіку на альтернативний шлях.

Для демонстрації роботи програми було проведено кілька досліджень в середовищі моделювання Mininet з голосовим і відео трафіком. Дослідження з голосовим трафіком проводилося протягом 12 секунд, трафік генерувався між хостами h1 і h2. Кожні 4 секунди параметри каналів зв'язку погіршувалися за рахунок введення втрат пакетів. У таблиці 2.5 наведені результати, отримані без використання системи моніторингу. Як видно, контролер не реагує на погіршення оцінки QoE, що призводить до незадовільної якості обслуговування.

Таблиця 2.5

Виміряні параметри для VoIP-трафіку, без системи моніторингу QoE

Час, сек	**Затримка, сек**	**Втрати пакетів, %**	**QoE**
2	0,003	0	4,8
4	0,004	10,17	3,83
6	0,003	11,4	3,6
8	0,004	57,4	1
10	0,002	54,3	1
12	0,001	84,7	1

Таблиця 2.6

Виміряні параметри VoIP-трафіку з системою моніторингу QoE

Час, сек	**Затримка, сек**	**Втрати пакетів, %**	**QoE**
2	0,005	0	4,73
4	0,006	9,54	3,76
6	0,003	10,35	3,89
8	0,005	62,57	1
10	0,003	5,38	4,04
12	0,001	0	4,85

На рис. 2.27 показані результати, отримані вище для порівняння системи моніторингу QoE і її впливу на якість послуг, що надаються в порівнянні з випадком без моніторингу. Як видно, при досягненні критичного значення втрати пакетів контролер прийняв рішення перенаправити трафік по альтернативному шляху.

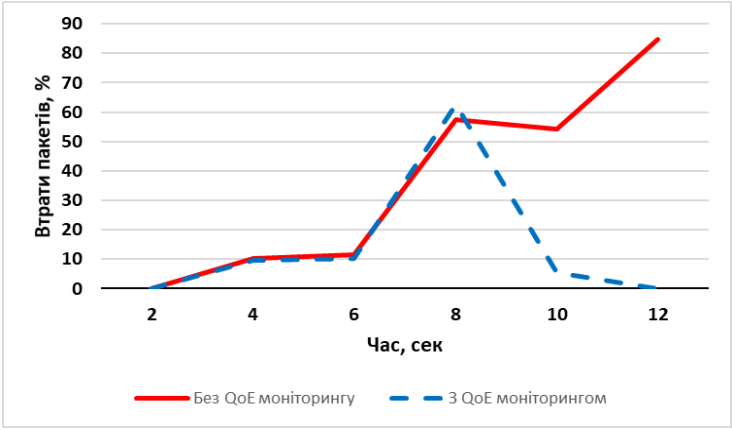


Рис.2.27. Порівняння втрат пакетів для трафіку VoIP

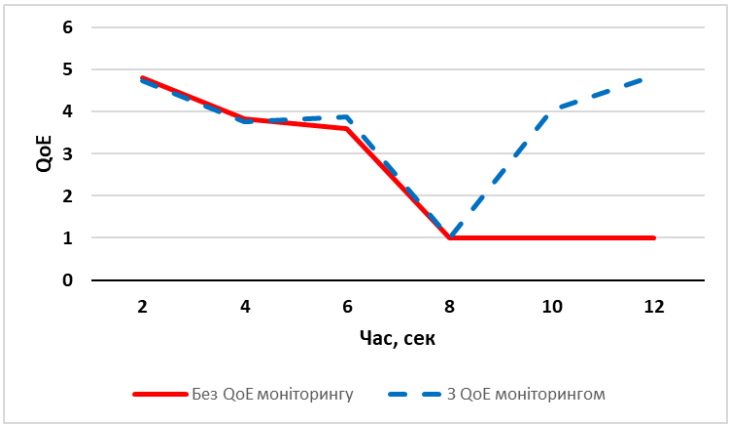


Рис.2.28. Порівняння QoE із запропонованим методом та без нього для аудіо трафіку [124]

В результаті запропоноване рішення забезпечує стабільну оцінку глобального QoE і підтримує його на необхідному рівні на основі виміряних даних в реальному тракті передачі даних, як показано на рис. 2.28.

Дослідження з потоковим відео проводилося протягом 12 секунд, трафік генерувався між хостами h1 і h2. Кожні 4 секунди параметри каналів зв'язку погіршувалися за рахунок введення втрат пакетів. Як видно, контролер не реагує на погіршення оцінки якості відео, що призводить до незадовільної якості обслуговування. Також був проведений експеримент для потокового відео з моніторингом QoE і перенаправленням трафіку в разі незадовільної оцінки надання послуги. При порівнянні отриманих результатів в графічному

поданні видно, що запропонована система моніторингу дозволяє знизити кількість втрат пакетів і в цілому поліпшити якість обслуговування в разі потокового відео (рис.2.29-рис.2.30).

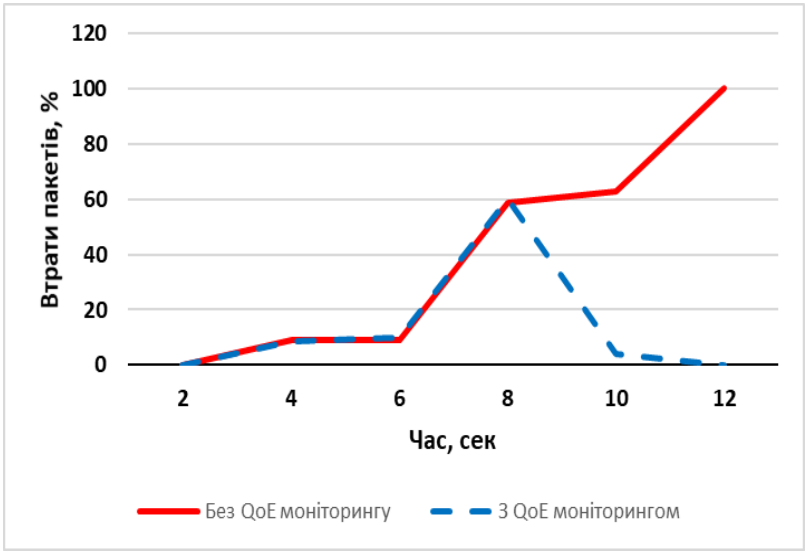


Рис.2.29 Порівняння втрат пакетів для потокової передачі відео

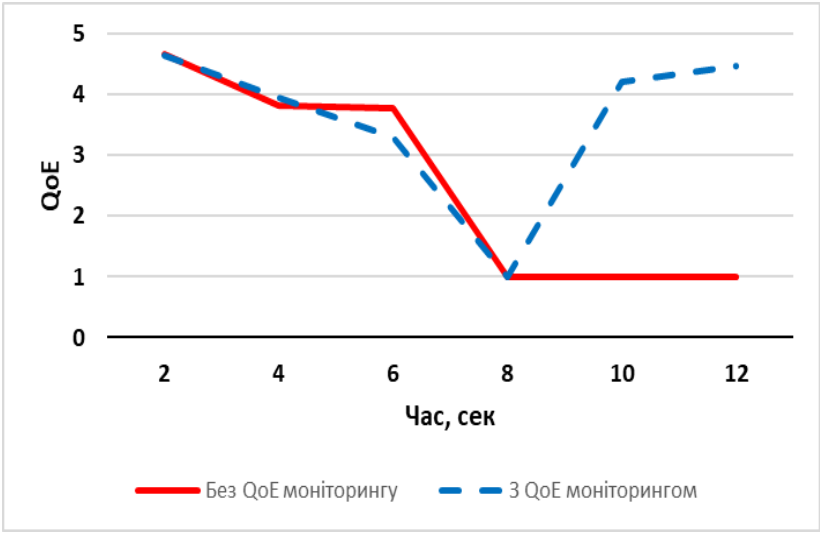


Рис.2.30 Порівняння QoE із запропонованим методом та без нього для відео трафіку [124]

Отже, існує безліч переваг запропонованої програмно-конфігурованої мережі на основі намірів, які в майбутньому дадуть змогу підвищити масштабованість, доступність, керованість та якість обслуговування інфокомунікаційних мереж. SDN надає централізовано керовану систему, яка забезпечує гнучкість для задоволення потреб споживача. Система IBN

забезпечує в цілому більш автоматизовану систему і гарантує, що конфігурація мережі не вимагатиме багато часу. IBN також може надає адміністратору гнучкість для виконання інших завдань, поки система IBN виконує свої завдання. Це гарантує, що ресурси можуть бути використані для інших, більш важливих намірів, зокрема щодо замовлення необхідного рівня управління якістю сприйняття послуг.

2.6 Метод динамічного розгортання та міграції віртуальних комутаторів між мультиконтролерами SDN на основі пріоритетного аналізу замовленої якості сприйняття послуг кінцевих користувачів

У роботі розвинуто метод динамічного розгортання та міграції віртуальних комутаторів між мультиконтролерами SDN на основі пріоритетного аналізу замовленої якості сприйняття послуг кінцевих користувачів, що дало змогу забезпечити ефективне використання мережевих ресурсів в інтелектуальних мережах нового покоління для гарантування клієнт-орієнтованої якості обслуговування [127].

Основна ідея методу полягає у міграції комутатора із завантаженого контролера на менш завантажений. Для підвищення відмовостійкості пропонується, щоб контролери інтелектуальної мережі були фізично розподілені, оскільки використання одного контролера негативно впливає на масштабованість та оперативність прийняття рішень, а також збільшення затримки. У попередніх підрозділах у роботі використовувався додатковий параметр QoE під час обслуговування трафіку. Його основне завдання – відображення бажаної якості обслуговування для кожного абонента мережі. Для цього абоненту пропонується обрати для себе бажаний пріоритет для послуг на основі інтенцій користувачів (від “1” – найнижчий, до “5” – найвищий). Обробка трафіку мережі відбувається з урахуванням цих пріоритетів. Тому даний показник обов'язково потрібно враховувати під час міграції комутаторів. Оскільки будь-які зміни в логічній топології мережі

можуть вплинути на якість послуг (особливо з найвищими пріоритетами). Тому вирішення питання про правильну міграцію є важливим завданням.

Можна виділити такі основні етапи прийняття міграційного рішення:

- Аналіз. Моніторинг мережі – один із найважливіших компонентів системи. Він дозволяє нам бачити стан мережі в режимі реального часу. Використовуючи мережні метрики, ми можемо реагувати на сплески трафіку та здійснювати необхідну адаптацію мережі. Якщо ми виявляємо необхідність оновлення топології, ми проводимо аналіз. Проводимо аналіз мережі – використовуючи існуючі метрики знаходимо потенційних кандидатів для міграції. Якщо ми виявили необхідність в оновленні топології проводимо аналіз розподілу трафіку потенційних кандидатів для міграції. Знаходимо можливі варіанти оновлення топології мережі.
- Розрахунок необхідних параметрів. Для потенційних кандидатів на міграцію ми розраховуємо коефіцієнти міграції та знаходимо розподіл трафіку відповідно до пріоритетів.
- Прийняття рішення. На основі попередньо розрахованих даних ми ухвалюємо найбільш оптимальне рішення про міграцію.
- Міграція. Проводимо безпосереднє оновлення логічної топології мережі. Спостерігаємо роботу мережі після змін.

Розглянемо наступний приклад мережі (рис.2.31). Ми маємо два сегменти ***A*** та ***B.*** До першого сегменту входять комутатори ***S1, S2, S3, S4***, з контролером ***C1***. До другого сегменту входять комутатори ***S5, S6, S7, S8*** з контролером ***C2*** відповідно.

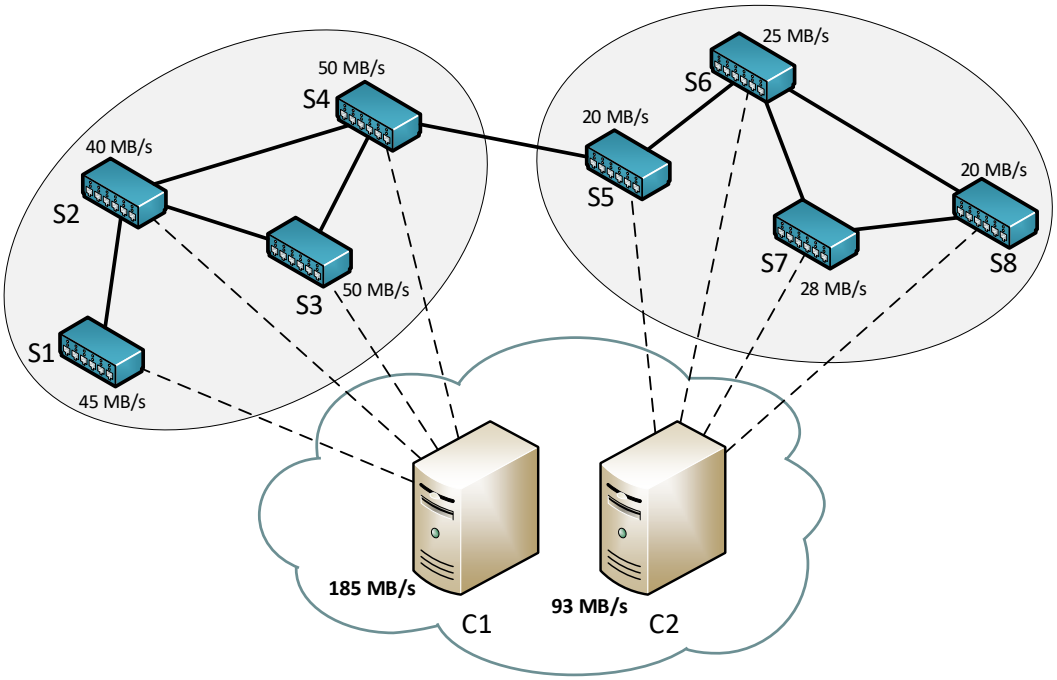


Рис.2.31. Топологія мережі

Кожен комутатор обробляє певне навантаження, дані подано в таблиці 1 для сегменту ***A*** та в таблиці 2 для сегменту ***B*** відповідно.

Знаходимо навантаження комутатора ***C1*** використовуючи формулу (2.23):

$$L_C = \sum_{i=1}^{n} S_i \qquad (2.23)$$

де i – номер комутатора, n – кількість комутаторів в сегменті.

$L_{C1} = 45+40+50+50 = 185\ MB/s$

$L_{C2} = 20+25+28+20 = 93\ MB/s$

Таблиця 2.7

Навантаження сегменту ***A***

C1					
Switch	S1	S2	S3	S4	L_{C1}
MB/s	45	40	50	50	185

Таблиця 2.8

Навантаження сегменту ***B***

C2					
Switch	S5	S6	S7	S8	L_{C2}
MB/s	20	25	28	20	93

Контролер ***C1*** є перевантаженим, тоді коли як контролер ***C2*** є недовантаженим. В такому випадку необхідно провести балансування мережі.

Навантаженими контролерами сегменту ***A*** є ***S3*** та ***S4***. Для того щоб прийняти правильне рішення який саме контролер повинен мігрувати необхідно розглянути тип трафіку який вони обробляють. На рис.2 подано розподіл трафіку по пріоритетах QoE. На основі наведених даних проведемо обрахунок. Знаходимо загальне навантаження на комутаторах з врахуванням пріоритетів. Розподіл по пріоритетах подано на рис.2.32.

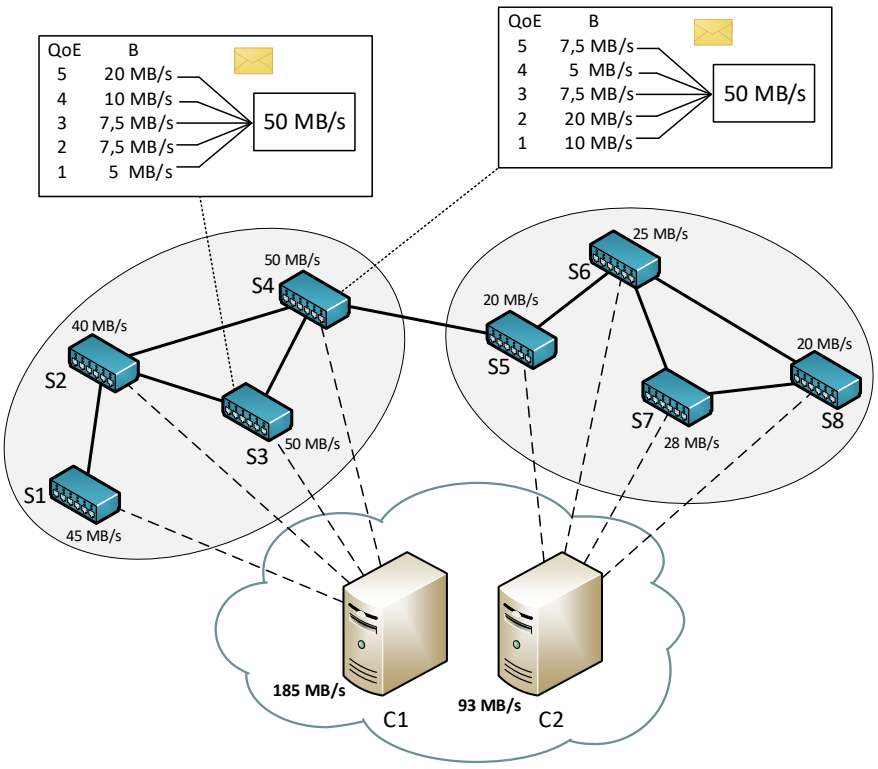


Рис.2.32. Розподіл трафіку за пріоритетами QoE [127]

Фільтруємо результати – залишаємо лише ті, значення яких перевищує встановлене мінімальне $\mathbf{L_{min}}$. В нашому випадку $\mathbf{L_{min}}$ = 50 MB/s. Комутатори із

значеннями більшими за мінімальне є потенційними кандидатами для мігрування. В таблиці 2.9 зеленим кольором позначено комутатори, які будуть аналізуватися в процесі міграції.

Таблиця 2.9

Навантаження комутаторів

QoE	5	4	3	2	1	∑ MB/s
s3	20	10	7,5	7,5	5	50
s1	15	10	2	4	4	35
s2	10	5	4	6	5	30
s4	8	5	8	20	10	51

Залишаємо лише потрібні нам комутатори – ***S3*** та ***S4*** (таблиця 2.10).

Таблиця 2.10

Фільтровані комутатори

QoS	5	4	3	2	1	∑ MB/s
s3	20	10	7,5	7,5	5	50
s4	8	5	8	20	10	51

Далі за формулою 2 для кожного комутатора знаходимо міграційний коефіцієнт MS. Він враховує розподіл трафіку по пріоритетах.

$$M_S = \sum_{i=1}^{5} L_{QoS(i)} / i \qquad (2.24)$$

M_{S3} = 20/5 + 10/4 + 7,5/3 + 7,5/2 + 5/1 = 17,75

M_{S4} = 8/5 + 5/4 + 8/3 + 20/2 + 10/1 = 25,51667

Результати подано в таблиці 5

Таблиця 2.11

Розрахунок міграційного коефіцієнту

QoS	5	4	3	2	1	∑ MB/s
M_{S3}	4	2,5	2,5	3,75	5	17,75
M_{S4}	1,6	1,25	2,666667	10	10	25,51667

Найвищі пріоритети є чутливими до затримок. При міграції комутатора з одного сегменту в інший виникає додатковий час на надсилання пакетів до

комутатора іншої мережі. Тому, щоб забезпечити найкращу якість для найвищих пріоритетів необхідно уникати додаткових затримок на обслуговування пакетів. Потрібно проводити міграцію комутаторів, трафік яких має найнижчий пріоритет. На основі обрахунків знаходимо комутатор із найбільшим міграційним коефіцієнтом. Обираємо комутатор з найвищим міграційним значенням MS. В нашому випадку MS4 > MS3. Міграцію будемо проводити для комутатора MS4.

Проводимо міграцію (рис. 2.33).

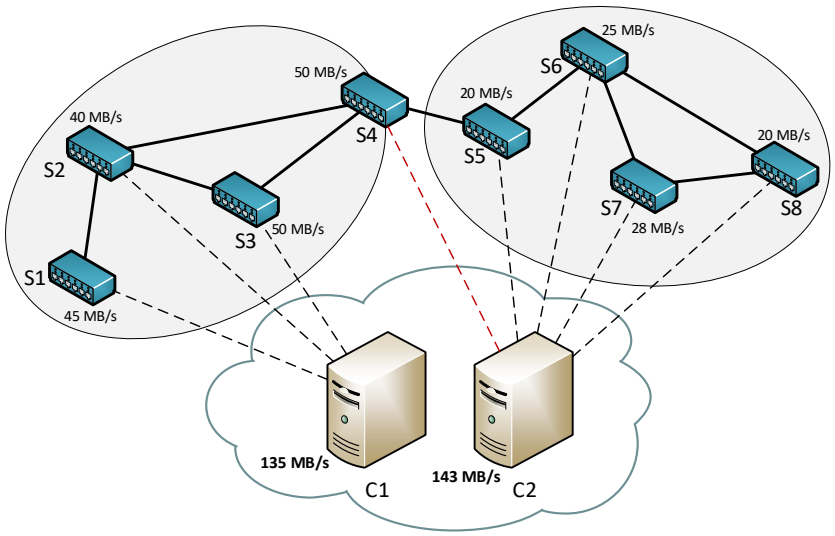


Рис.2.33. Можливі варіанти міграції

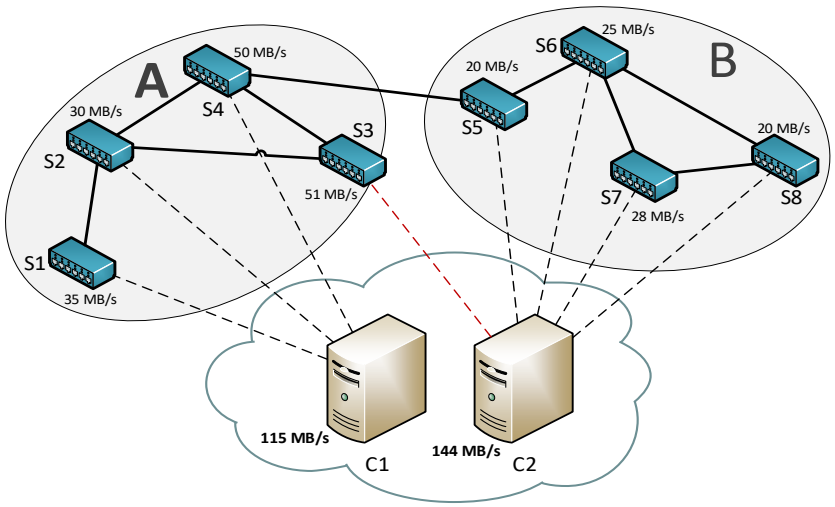


Рис.2.34. Можливі варіанти міграції

Проведемо порівняльний аналіз двох варіантів міграції - стандартного та пропонованого. Для цього розглянемо обробку пакетів по шляху від комутатора S1 до комутатора S6 (рис. 2.35).

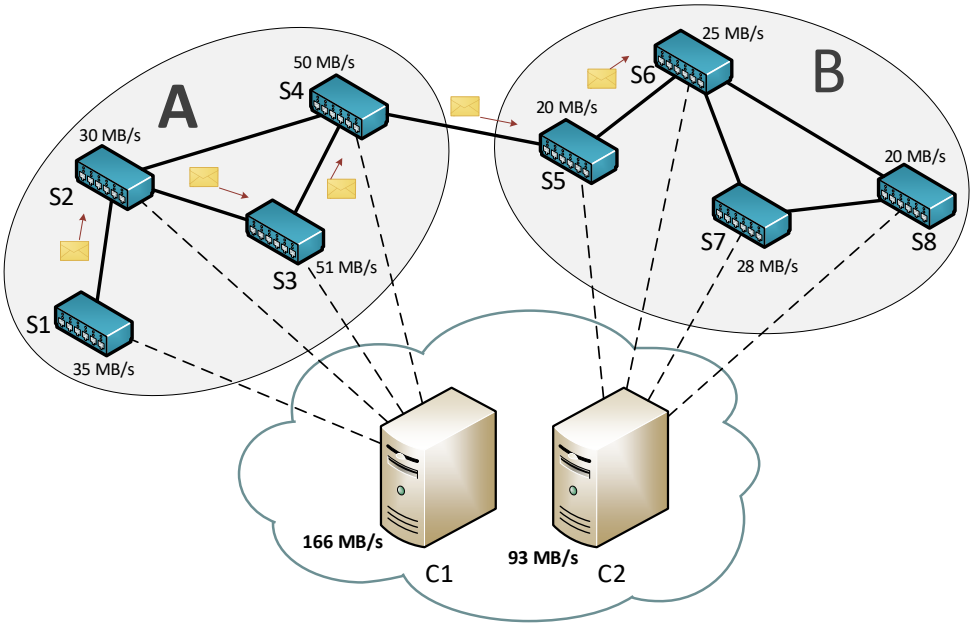


Рис.2.35. Схема порівняння методів міграції віртуального комутатора [127]

Для цього ми знайдемо час відправлення пакетів для різних пріоритетів міграції після міграції самого завантаженого комутатора і після міграції комутатора, визначеного запропонованим методом. Час відправлення пакетів складається з часу обробки пакетів в кожному комутаторі, часу транспортування між сусідніми комутаторами і часу обробки контролером. Алгоритми маршрутизації для простоти розуміння не розглядаються.

Час затримки міграції буде наступним:

$$T_{total} = t(S1S2) + t(S2S3) + t(S3S4) + t(S4S5) + t(S5S6) \quad (2.25)$$

де $t(SnSm)$ – час відправлення пакету від комутатора n до комутатора m.

$$t(S1S2) = t(C1) + t(S1) + t_{send}(S1S2)$$

$$t(S2S3) = t(C1) + t(S2) + t_{send}(S2S3)$$

$$t(S3S4) = t(C1) + t(S3) + t_{send}(S3S4)$$

$$t(S4S5) = t(C1) + t(S4) + t_{send}(S4S5)$$

$t(S5S6) = t(C2) + t(S5) + t_{send}\ (S5S6)$

де $t(S)$ – час обробки пакета комутатором, $t(C)$ – час обробки пакета контролером, $t_{пер}(SnSm)$ – час передачі по каналу зв'язку між комутаторами n і m.

Оскільки після міграції змінюється лише t (C1) і t (C2) для комутаторів S3 S4, ми розглядаємо компоненти, які безпосередньо до них відносяться.

В результаті ми матимемо час до міграції:

$$t_{before} = 4 \cdot t(C1) + t(C2) \tag{2.26}$$

Час після міграції:

$$t_{mig} = 3 \cdot t(C1) + 2 \cdot t(C2) + t_{sending} \tag{2.27}$$

де $t_{sending}$ – час надсилання пакетів із сегмента A до C2 (оскільки переміщений комутатор обслуговуватиме C2). Результати представлені у таблиці 2.12.

Таблиця 2.12

Час реакції контролера

Controller	Before		Standart		Modified	
	time	*load*	*time*	*load*	*time*	*load*
C1	1,66	166	1,15	115	1,16	116
C2	0,93	93	1,44	144	1,43	143

Далі знаходимо час обробки пакета для кожного варіанту. Результат представлено в таблиці 2.13

Таблиця 2.13

Час обробки пакета

	Before	Standart	Modified
t process	7,57	6,33	6,34

Використовуючи попередні дані, можемо знайти середній час обробки в залежності від пріоритету:

Таблиця 2.14

QoS					ied
					S4
5	1				53,55
4	2				89,25
3	2				142,8
2	3				285,6
1	3				357

Цей резул

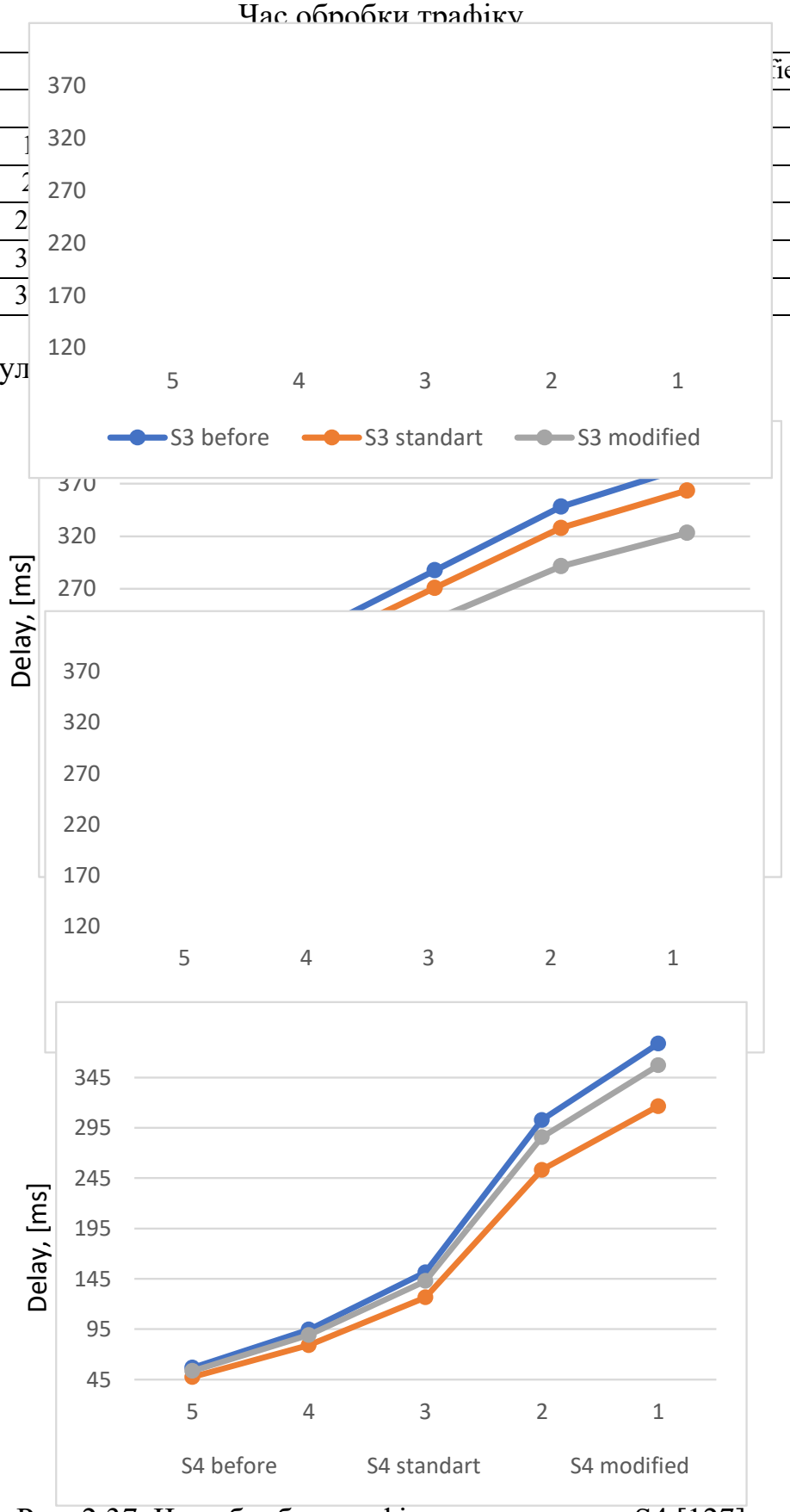


Рис. 2.37. Час обробки трафіку комутатором S4 [127]

У результаті ми маємо кращий час для обробки пріоритетних послуг за рахунок менш пріоритетних послуг. Однак, чим нижчий пріоритет, тим більше часу доступно для обслуговування.

Ми показали, що в поєднанні з віртуалізацією та хмарними обчисленнями технологія SDN/IBN може революціонізувати роботу організації, забезпечуючи зниження економічних витрат, підвищує ефективність управління мережевими ресурсами. У цій статті пропонується модифікований підхід для міграції комутаторів з одного контролера на інший з урахуванням розподілу відповідно до пріоритетів QoS. Вибір правильного комутатора для міграції дуже важливий, оскільки він може критично вплинути на кінцеву якість послуг. Ми запропонували модифікований метод міграції комутаторів. Показано поетапний розрахунок коефіцієнтів міграції та проведено порівняльний аналіз стандартного методу міграції із запропонованим. Пріоритетні послуги дуже чутливі до затримок. За підсумками аналізу можна сказати, що запропонований підхід скорочує час обробки пріоритетних послуг.

Також необхідно врахувати, що у міру зростання трафіку зростають вимоги до ресурсів мережного обладнання. Найбільш складними періодами в обслуговуванні трафіку є годинник найбільшого навантаження. У цей час генерується найбільший обсяг трафіку, найбільша кількість абонентів користується послугами та очікує отримати гарну якість. У моменти, коли кількість трафіку, що генерується, наближається і перевищує межі ресурсів мережевого обладнання, рівень QoS погіршується до неприйнятного рівня. На рис. 2.38 показані пропускна спроможність мережі та генерований трафік за два дні. У традиційних мережах у моменти перевантаження мережі переповнений трафік (червоний колір) зазнаватиме великих затримок і втрачатиметься. Щоб уникнути цієї ситуації, необхідно збільшити пропускну спроможність мережної інфраструктури. Однак це тривалий процес, що потребує великих грошових витрат. Для вирішення цієї проблеми для пропонованої у роботі концепції інтелектуальних мереж пропонується розгортати з допомогою віртуалізації

мережевих функцій та технології інфраструкти як код додаткові мережеві пристрої (контролери та комутаори) у хмарі та перенаправити активний мережевий трафік.

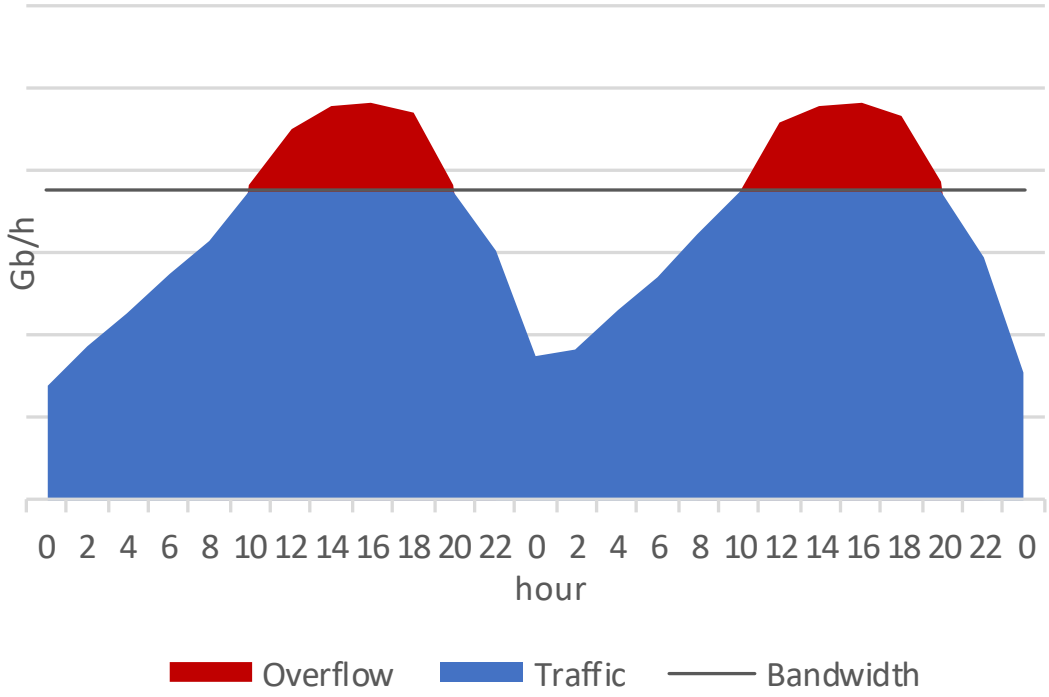


Рис.2.38. Втрати надлишкового трафіку у традиційній мережі

Основна відмінність запропонованого методу полягає в тому, що під час високого навантаження на мережу розгортання додаткових ресурсів відбуватиметься автоматично. Підхід до автоматизації конфігурації, управління та обслуговування мережі ґрунтується на використанні спеціального пристрою-контролера. Контролер формує профілі додатків, що описують характеристики мережі, необхідні додаткам для роботи, завантажує їх у мережні пристрої, після чого мережа починає підтримувати обмін даними для додатків. Контролер також стежить за сумісністю конфігурацій пристроїв один з одним. Він спрощує аудит конфігурації мережі: всередині контролера конфігурація представлена у вигляді об'єктної моделі, яку можна будь-якої миті завантажити через інтерфейс прикладного програмування (API) та отримати актуальну інформацію про конфігурацію мережі. Конфігурація підтримується

контролером у поточному стані: якщо профіль програми видаляється зі списку активних, його налаштування також будуть видалені з усіх мережних пристроїв.

Щоб це забезпечити, необхідно встановити додаткове програмне забезпечення на основні елементи мережі – комутатори та контролери. Основне завдання цього програмного забезпечення - збір даних для моніторингу поточного стану пристрою. Основними з них є завантаження процесора, обсяг пам'яті та завантаження мережі. На основі цих даних прийматиметься рішення про розгортання додаткових ресурсів.

Також для нормальної роботи пропонується використати прямий канал від кожного комутатора до Інтернету. Цей канал буде використовуватися для передачі трафіку, який обслуговуватиметься у хмарі. І тут ми зможемо розвантажити фізичну локальну мережу. В результаті ми покращимо рівень QoS для локального трафіку і зможемо обробляти надлишковий трафік. (Рис.2.39).

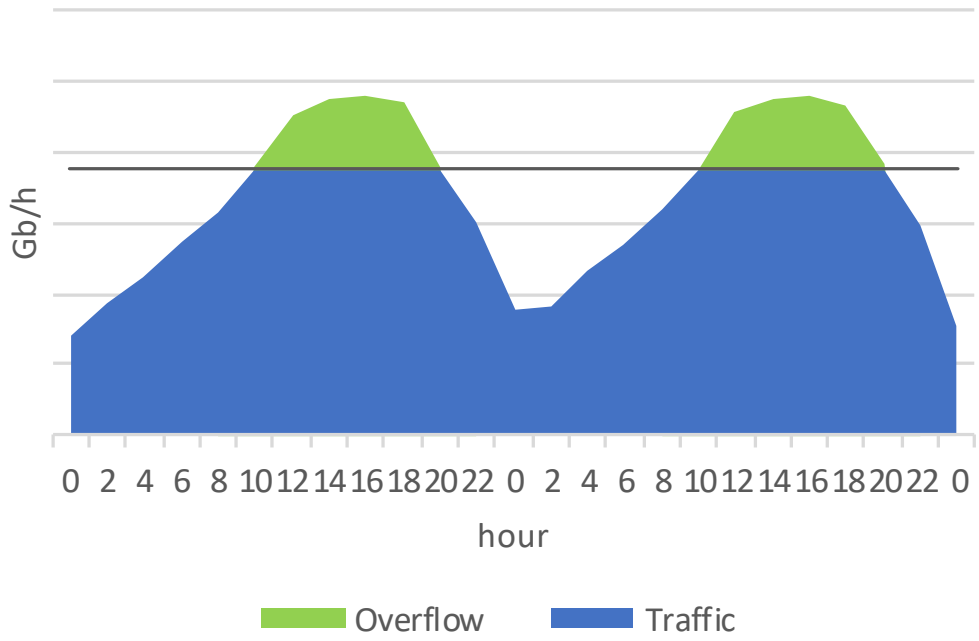


Рис.2.39. Обслуговування надлишкового трафіку за допомогою гібридної мережі

На рис. 2.40 зображена схема ненавантаженої традиційної програмно-конфігурованої мережі, що складається з кількох комутаторів, кінцевих користувачів та мережевих контролерів. Абонент PC1 надсилає дані абоненту PC2.

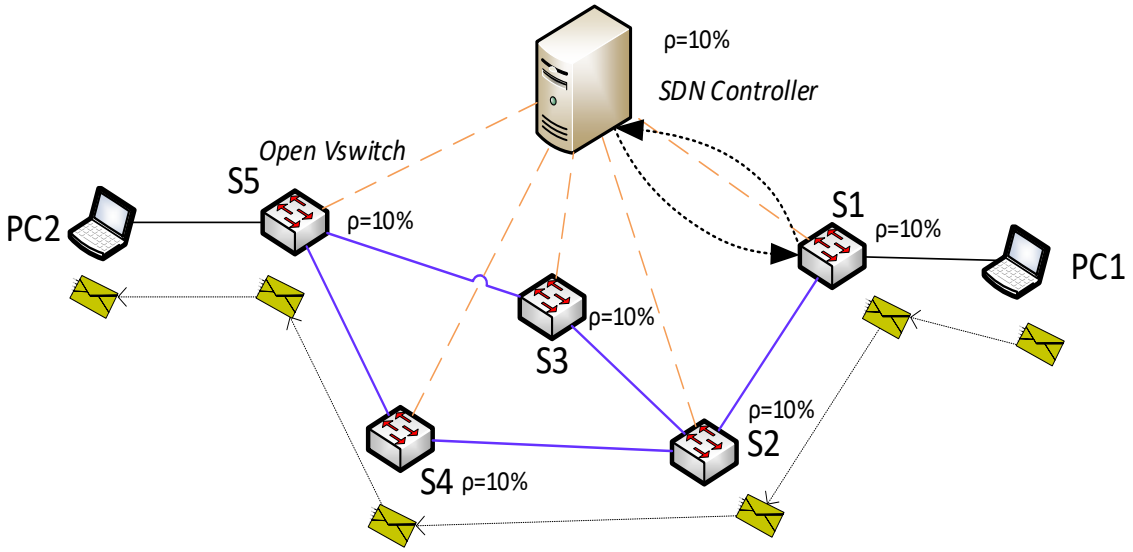


Рис. 2.40. Канал у ненавантаженій SDN-мережі [128]

При побудові маршруту комутатор S1 зв'язується з контролером для отримання інформації про маршрут, а потім встановлює канал передачі:

PC1 – S1 – S2 – S4 – S5 – PC2.

Якщо мережа не завантажена, сеанс успішно завершиться та проблем не виникне. Розглянемо випадок в годину найбільшого навантаження (рис. 2.41).

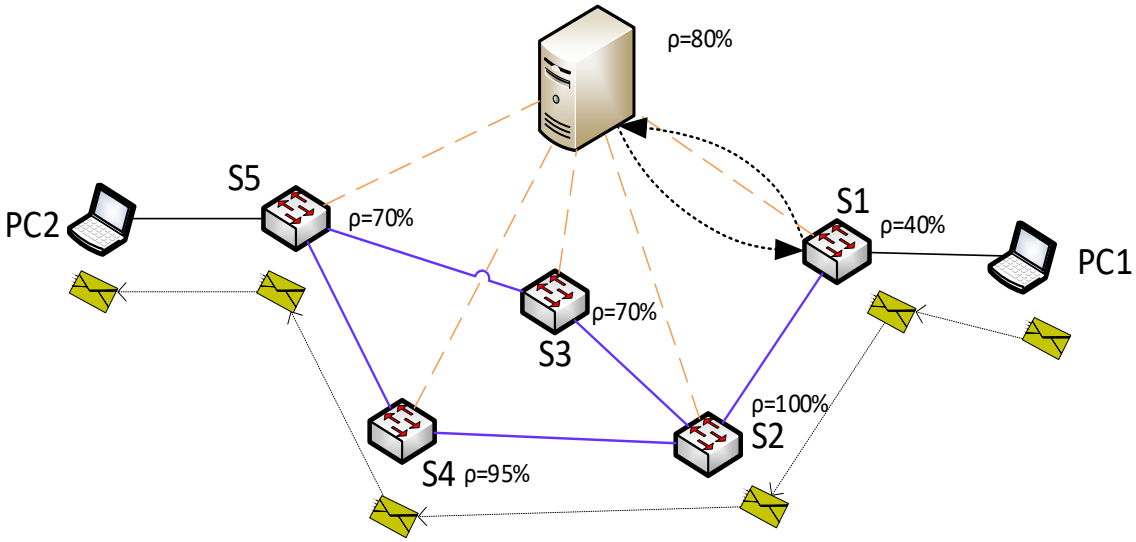


Рис.2.41. Канал у незавантаженій SDN-мережі

Комутатор S2 працює з максимальним навантаженням. Оскільки рівень QoS у мережі знижується зі збільшенням трафіку, необхідно перебудувати маршрути для зниження навантаження на мережу. Для балансу пропонується перенаправити трафік, обминаючи обслуговування у хмарі. На основі зібраних даних моніторингу ми можемо виявити завантажені елементи мережі. Вони мають найбільший вплив на загальне значення рівня QoS. Щоб компенсувати це ми розширюємо додаткову інфраструктуру в хмарі (рис.2.42.) і перенаправляємо трафік. Тим самим ми звільняємо ресурси для затримок критично важливих сервісів.

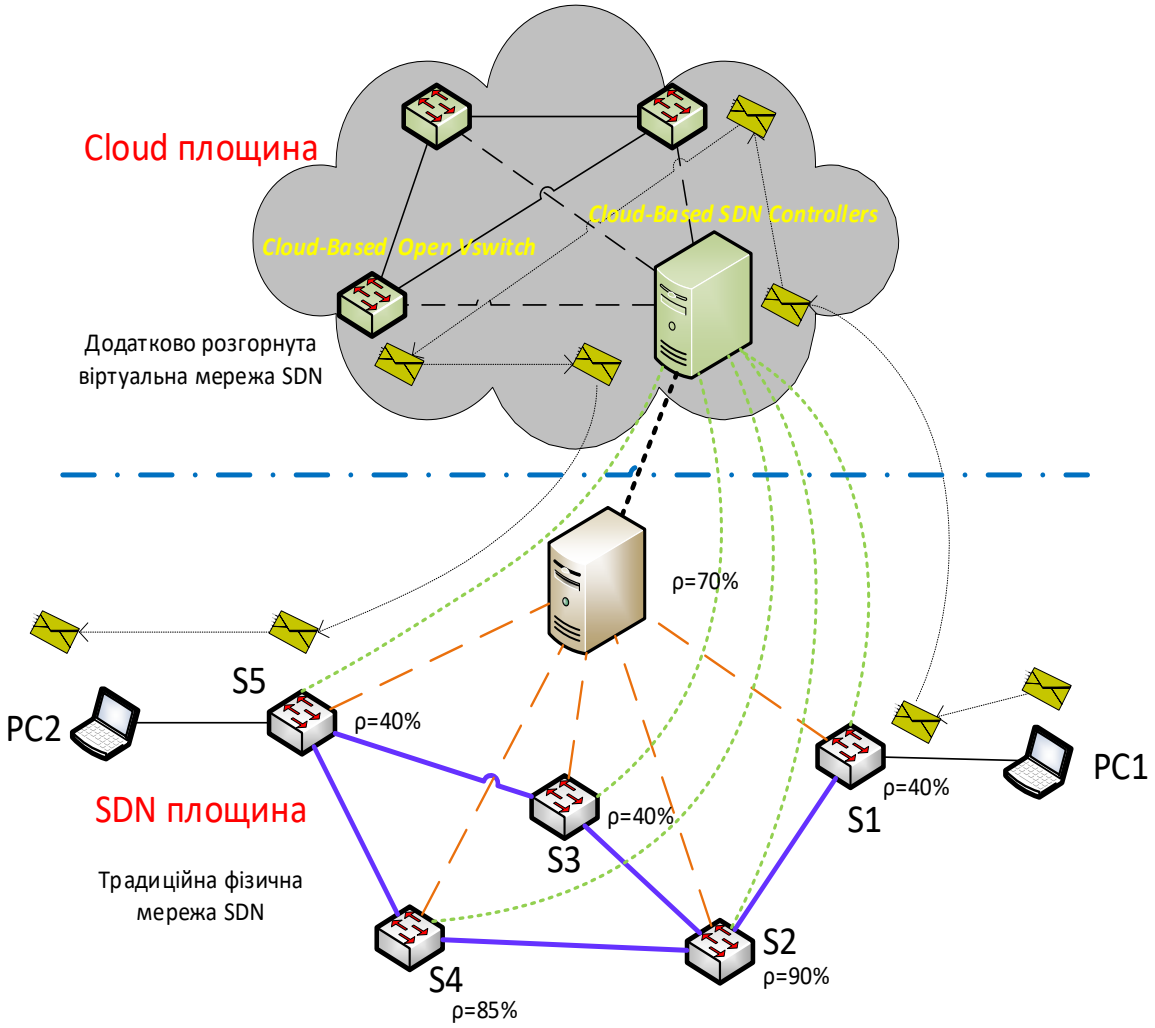


Рис. 2.42. Використання гібридної мережі мереж, що ґрунтуються на намірах, для обслуговування трафіку [128]

Використовуючи прямий канал до Інтернету, ми перенаправляємо трафік, що проходить через високонавантажені елементи, на сервіс у хмарі.

Новий маршрут для сервісу буде виглядати так:

PC1 – S1 – S6 – S8 – S5 – PC2.

Слід зазначити, що прямий та зворотний маршрути для відправки перенаправленого трафіку відрізняються. Прямий шлях будується з урахуванням мережного трафіку. Тоді як зворотний шлях буде найбільш оптимальним (зазвичай відразу на комутаторі, до якого підключений кінцевий користувач). Такий підхід дозволить максимально розвантажити мережу. При використанні нового методу надлишковий трафік більше не відкидатиметься, а перенаправлятиметься на обслуговування у хмарі. Для кінцевого користувача зміни будуть непомітні. Проведемо математичний аналіз. Для цього порівняємо алгоритми формування затримок, для традиційної та гібридної мережі. Оскільки ресурси традиційної мережі обмежені, кількість пакетів, що обслуговуються, також обмежена. При використанні гібридної мережі додається гнучкість за рахунок додаткових ресурсів. При цьому якщо якість QoS фізичної мережі знижується, є можливість компенсувати його за рахунок додаткових віртуальних ресурсів.

Для традиційної мережі QoSp – рівень QoS для локальної мережі:

$$QoS_p = QoS_p\left(\rho_{p\,sw}\right) + QoS_p\left(\rho_{p\,cont}\right) + QoS_p\left(\rho_{p\,tr}\right) \tag{2.27}$$

де:

$QoS_p(\rho_{p\,sw})$ – рівень QoS для комутаторів залежно від навантаження,

$\rho_{p\,sw}$ – навантаження комутаторів,

$QoS_p(\rho_{p\,cont})$ – рівень QoS для контролера в залежності від навантаження,

$\rho_{p\,cont}$ навантаження контролерів,

$QoS_p(\rho_{p\,tr})$ – рівень QoS для надсилання пакетів.

$\rho_{p\,tr}$ – час відправлення пакету.

Для інфраструктури хмарної мережі QoS_v – рівень QoS для хмарної структури:

$$QoS_v = QoS_v(\rho_{v\,sw}) + QoS_v(\rho_{v\,cont}) + QoS_v(\rho_{v\,tr}) \quad (2.28)$$

де: $QoS_v(\rho_{v\ sw})$ – рівень QoS для комутаторів в хмарі в залежності від навантаження, $QoS_v(\rho_{v\ cont})$ – рівень QoS хмари для надсилання пакетів, $\rho_{v\ cont}$ cloud's controllers load, $QoS_v(\rho_{v\,tr})$ – рівень QoS хмари для надсилання пакетів, $\rho_{v\,tr}$ – час відправлення пакету в хмарі.

Загальна затримка буде виглядати так:

$$QoS = QoS_p + QoS_v \quad (2.29)$$

Тоді введемо додаткові коефіцієнти, що описують навантаження на мережу:

$$QoS = x \cdot QoS_p + y \cdot QoS_v \quad (2.30)$$

Тоді, якщо x зменшується - це потрібно компенсувати y, щоб загальний результат не змінився. Описується алгоритм зміни додаткових ресурсів для компенсації навантаження на локальну мережу.

Для кінцевих користувачів результат буде незмінним - хороший рівень QoS, який досягається за рахунок балансування коефіцієнта *y* коефіцієнтом *x*.

2.7 Модель побудови гібридної SDN/MPLS транспортної системи для підвищення якості обслуговування в інтелектуальних мережах

Нова парадигма Software Defined Networking (SDN), хоч і має великий потенціал для вирішення складних проблем, що виникають у корпоративних мережах, має свої проблеми з розгортанням та масштабованістю. Крім того, повне розгортання SDN має свої власні ділові та економічні проблеми. Плавний перехід від традиційних мереж до SDN (без збоїв, з урахуванням бюджетних обмежень, з поступовим покращенням управління мережею) вимагає гібридної мережевої моделі як неминучий проміжний крок; це дозволяє гетерогенним парадигмам функціонувати разом, доки повний перехід здійснюється поетапно. Тому необхідно розробити стратегію поступового розгортання, що відповідає потребам організації. Актуальною технологією серед провайдерів є технологія

MPLS, яка має ряд протоколів управління мітками і процесом розподілу пакетів. Однак в традиційній MPLS технології все ще є певні недоліки. Вони потребують ручного налаштування. Вони повільно реагують зміни топології мережі. Вони вимагають збереження надмірної інформації та її розповсюдження через мережу. У той же час можливості керування активними сесіями та перебудови активних шляхів відповідно до реальної ситуації в мережі (зміна топології, вихід із ладу мережевих елементів, завантаження сегментів мережі, забезпечення найкращого QoS) реалізовані слабко. В результаті управління та ефективне використання мережевих ресурсів здійснюється неефективно.

Для вирішення цих проблем пропонується перенести керування мітками з мережних маршрутизаторів на мережевий контролер. До сегменту мережі із MPLS додамо централізований контролер з метою створення гібридної інтелектуальної мережі нового покоління (рис. 2.43). Для досягнення найкращої продуктивності він повинен мати канали обслуговування з усіма елементами мережі, що управляють. У цьому випадку контролер працюватиме з достатньою інформацією для ефективного керування. Такий підхід забезпечить нам поділ рівня управління та рівня даних.

Запропонований підхід дозволяє покращити моніторинг та діагностику. Оскільки формується загальне уявлення про продуктивність мережі , що даї змогу динамічно змінювати конфігурацію мережевих пристроїв для задоволення змін попиту або вимог користувачів [129]. У разі MPLS це може дозволити створити сітку LSP та оптимізувати LSP як програмні модулі в контролері, який працює у фоновому режимі, не втручаючись у роботу мережі.

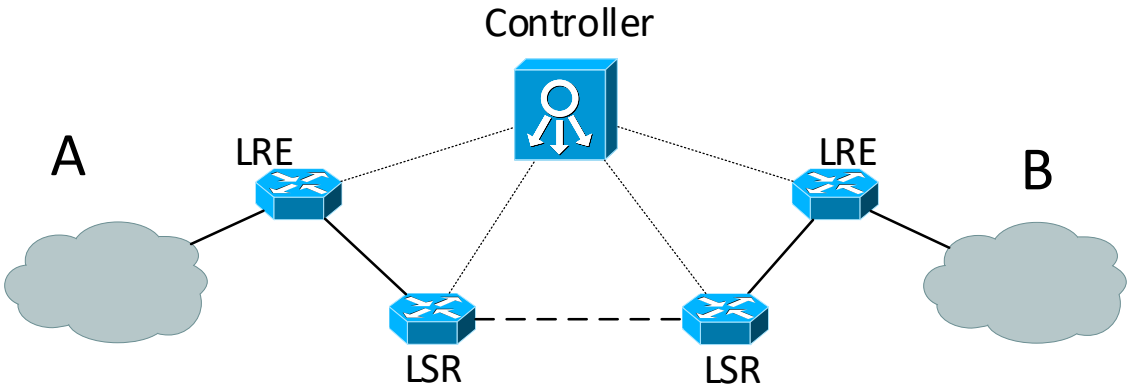


Рис.2.43. MPLS network with controller

Це дає нам деякі переваги:

- швидкість поширення міток по мережі по сервісних каналах;
- на основі службових даних (метрик), які отримують контролер від мережевих елементів, ми знаємо поточну топологію мережі, тому можемо швидко реагувати на її зміну;
- на основі метрик ми враховуємо навантаження на мережу при побудові нових та перебудові існуючих маршрутів;
- Обробляємо пакети з необхідними QoS та QoE вимогами.

Мережевий контролер, використовуючи отримані дані сервісу (метрики завантаження каналу, топологія мережі тощо), постійно відстежує актуальність побудованих шляхів. У цьому випадку ми зможемо коригувати лише необхідні шляхи, оновлюючи таблиці маршрутизації (за мітками) тільки на тих маршрутизаторах, через які проходять шляхи передачі даних і не завантажуючи елементи, що не використовуються.

Для забезпечення QoS пропонується використовувати мітки. Оскільки пакети можуть мати кілька міток (формується стек міток), ми можемо використовувати їх для визначення пріоритетів пакетів різних сервісів для підвищення показників якості обслуговування.

Таким чином, ми також можемо використовувати можливість коригування пріоритетів QoE. Мережа обслуговує велику кількість абонентів, проте вимоги

до якості обслуговування та стеку послуг, що використовуються, різні. Тому необхідно враховувати пріоритет, щоб використати це коригування [129].

Порівняємо процес встановлення мережевого з'єднання за допомогою звичайної MPLS (рис. 2.44) та з використанням SDN контролера (рис. 2.45). Знайдемо час встановлення з'єднання без контролера. На малюнку 3 показано процес передачі пакета. Для цього знайдемо час розподілу пакетів t_t, час зміни міток t_{label}, час обробки пакетів t_{packet} та час резервування ресурсів t_r.

Приймемо, що:

$$t_{ex} = t_{label} + t_{packet} \tag{2.31}$$

Використовуючи (1):

$$\Delta t = 2 \cdot \sum_{i=1}^{N-1} t_t + 2 \cdot \sum_{i=1}^{N-1} t_{ex} + \sum_{i=1}^{N-1} t_r \tag{2.32}$$

У разі централізованого управління (рис. 2.45) процес з'єднання виглядає так: LER звертається до контролера. Цей контролер аналізує потрібні ресурси. Якщо вільних ресурсів достатньо, вони виділяються. Будується канал LSP. Потім контролер відправляє оновлену таблицю міток на необхідні LSR. Якщо ресурси зарезервовані - контролер надсилає відповідь з новою міткою каналу

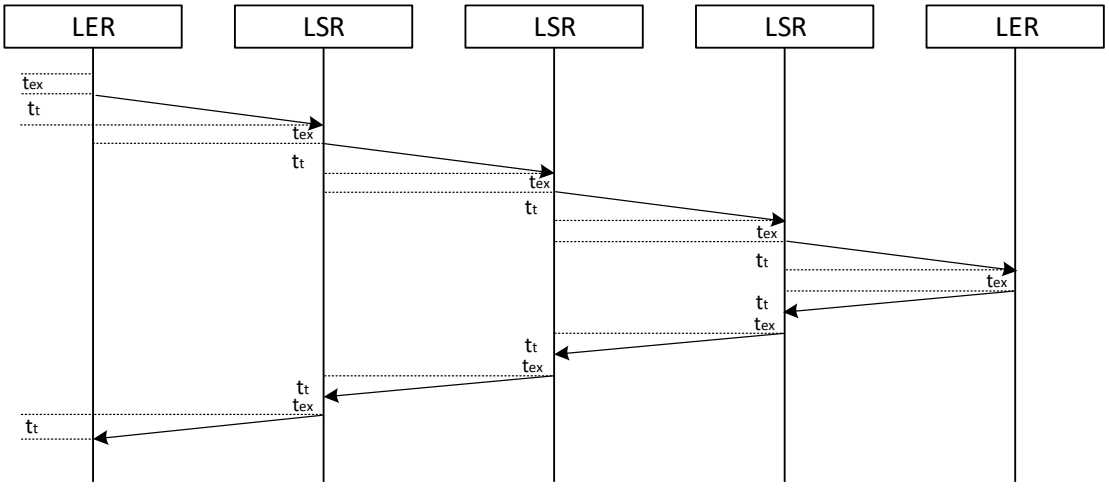


Рис. 2.44. Процес встановлення каналу в SDN/MPLS

Затримка складається з часу розповсюдження пакетів t_t, часу зміни міток у контролері t_{label}, часу обробки пакетів t_{packet}, часу резервування ресурсів t_r та часу оновлення таблиць LFIB t_{label}. Час обробки пакетів контролером залежить від його потужності. Зі зростанням вимог до мережі потужність контролера збільшується.

Тоді, використовуючи (2.31):

$$\Delta t = 3 \cdot t_t + \cdot 2 \cdot t_{ex} + t_r + t_{table} \qquad (2.33)$$

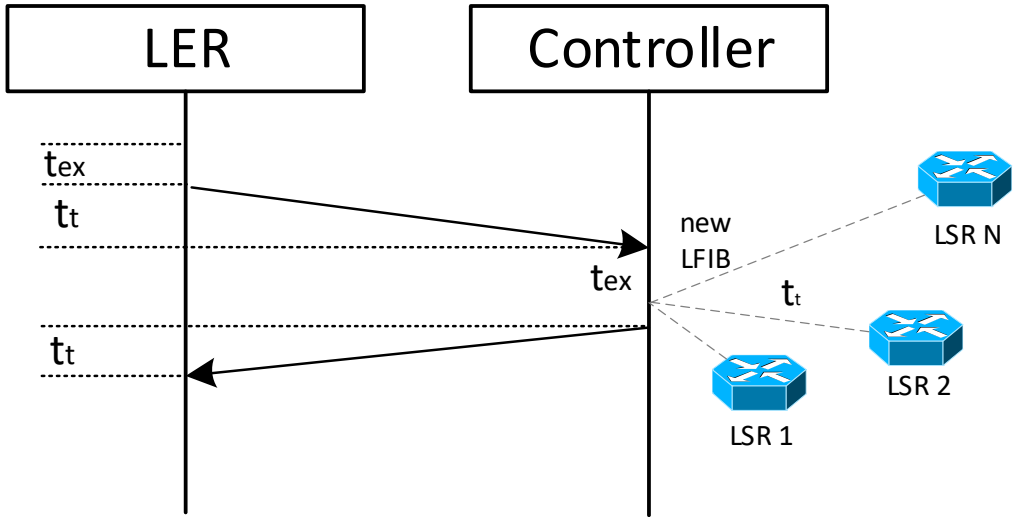


Рис. 2.45. Процес встановлення каналу в MPLS за допомогою контролера [129]

Проведемо порівняння. Припустимо, що.

t_{ex} = 2 одиниці часу;

t_r = 1 одиниця часу;

t_t = 1 одиниця часу;

t_{table} = 3 одиниці часу;

N = 10 (кількість LSR у тунелі).

Тоді час налаштування каналу мережі без контролера, використовуючи формулу (2.32), становить:

$$\Delta t_1 = 2 \cdot 9 \cdot 1 + \cdot 2 \cdot 9 \cdot 2 + 2 \cdot 9 \cdot 1 = 72 \text{ [умовна одиниця часу]} \qquad (2.34)$$

Використовуючи самі дані, знайдемо затримку для мережі з допомогою контролера. З формули (2.33):

$$\Delta t_2 = 3 \cdot 1 + \cdot 2 \cdot 2 + 1 + 3 = 11 \quad \text{[умовна одиниця часу]} \quad (2.35)$$

Порівняння результатів подано на рис. 5

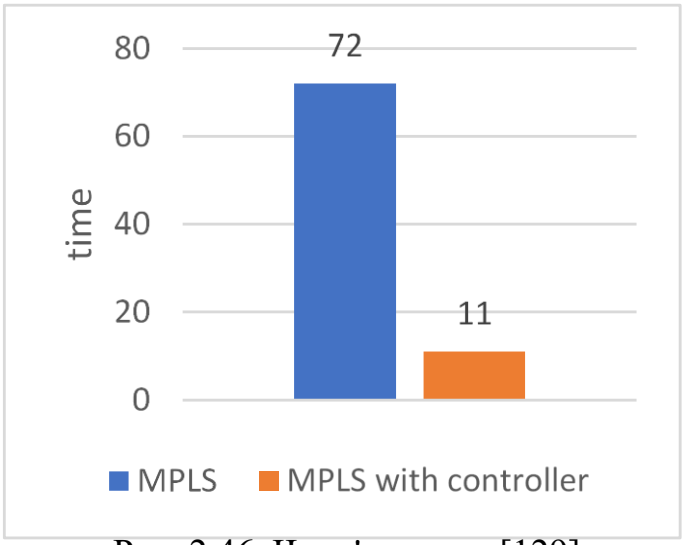


Рис. 2.46. Час з'єднання [129]

Наступним етапом удосконалення є використання алгоритмів машинного навчання мереж для інтелектуального керування маршрутами передавання. Оскільки контролер знає топологію мережі та її здатність обробки навантаження, ми можемо взяти цю інформацію за основу нейронної мережі. Топологія мережі змінюється дуже часто, тому ми можемо використовувати процес навчання мережі й надалі використовувати попередній досвід. Це дозволить збільшити швидкість встановлення маршруту для нової послуги та забезпечити його ефективність. Даний маршрут буде одним із найкращих, які мережа може запропонувати на даний момент часу із врахуванням мінливих вимог користувачів.

Висновки до 2-го розділу

У роботі запропоновано концептуальну модель інтелектуальної IBN (Intent-based networking) мережі, що базується на архітектурі SDN (Software-Defined Network) і являє собою одну з найбільш важливих нових можливостей

мережевої інфраструктури. IBN пропонує мережевим адміністраторам простий спосіб вираження бізнес-цілей, таких як забезпечення необхідного QoE, дозволяючи мережному програмному забезпеченню автоматично досягати поставлених цілей по забезпеченню рівня QoE. У даному розділі запропоновано систему моніторингу QoE (Quality of Expirience) для майбутніх програмно-конфігурованих мереж на основі намірів (IBSDN), яка поліпшить якість обслуговування кінцевих користувачів і дозволить більш ефективно використовувати мережеві ресурси. Для цього у розділі представлені методи вимірювання параметрів функціонування програмно-конфігурованої мережі: затримки і втрати пакетів. Проведено дослідження для оцінки ефективності запропонованої системи QoE-моніторингу шляхом генерації аудіо- та відеотрафіку в мережі Mininet. На основі досліджень визначено математичну функцію кореляції параметрів QoS/QoE та розроблено метод маршрутизації, метрика якого базується на інтегральному критерії якості обслуговування.

У даному розділі також розроблено модуль машинного навчання для інтеграції в програмно-конфігуровані мережі. Це дозволяє прогнозувати рівень якості сприйняття послуги кінцевого користувача, враховуючи такі параметри мережі, як затримка та втрата пакетів. Для машинного навчання було обрано алгоритм Random Forest, який за опублікованими роботами є одним з найбільш точних для прогнозування. Відповідно до результатів запропонований алгоритм машинного навчання дає результати з певною похибкою щодо розрахункового значення системи моніторингу. Покращення результатів прогнозування можна досягти шляхом точного налаштування кількості нейронів, прихованих шарів, збільшення обсягу навчальних даних і зміни алгоритму. Впровадження модуля машинного навчання в архітектуру IBN для системи моніторингу дозволило зменшити обсяг сигнального трафіку в каналах зв'язку між мережевим обладнанням і контролером, а також реагувати на несприятливі поєднання значень показників якості і попереджати ситуації, коли користувач

незадоволений якістю отриманих сервісів для адаптивного прогнозування моменту переконфігурації мережі.

В даній роботі запропоновано модифікований метод для міграції комутаторів від одного контролера до іншого з врахуванням розподілу відповідно до QoE пріоритетів. Правильний вибір комутатора для міграції є дуже важливим, адже це може критично вплинути на кінцеву якість послуг, що надаються в мережі. Показано поступовий розрахунок міграційних коефіцієнтів та проведено порівняльний аналіз звичайного міграційного методу із запропонованим. Представлено схему організації роботи мережі з використанням хмарних технологій.

Визначено необхідність створення нових мережевих архітектур, здатних успішно справлятися зі зростанням трафіку та забезпечувати QoS. На основі розглянутих матеріалів пропонується новий підхід щодо побудови MPLS-мережі із централізованим контролером. Цей контролер відповідатиме за побудову та підтримку існуючих шляхів, використовуючи актуальну інформацію про топологію мережі та завантаженість її сегментів. Оскільки контролер знає про поточний стан усієї мережі та її топологію, ми зможемо максимально ефективно використовувати наявні ресурси і, за необхідності забезпечити необхідний рівень QoS, перенаправляти канали з перевантажених ділянок. Така мережа забезпечує можливість організації трафіку, що дозволяє більш ефективно використовувати пропускну здатність каналів та підтримує якість обслуговування (QoS). MPLS знижує вимоги до обробки даних пристроями опорної мережі, оскільки вони просто пересилають пакети на основі міток. В результаті підвищується продуктивність мережі. Проаналізовано час побудови нового каналу для звичайної мережі MPLS та з використанням централізованого контролера. Оцінюється ефективність технологій MPLS та MPLS з контролером щодо тимчасової затримки мережі в процесі передачі пакетів.

РОЗДІЛ 3. РОЗРОБЛЕННЯ УНІКАЛЬНОГО ВІДМОВОСТІЙКОГО КОНТРОЛЕРА ДЛЯ КЛІЄНТ-ОРІЄНТОВАНОГО УПРАВЛІННЯ ЯКІСТЮ ОБСЛУГОВУВАННЯ В ПРОГРАМНО-КОНФІГУРОВАНИХ ІНТЕЛЕКТАЛЬНИХ МЕРЕЖАХ НОВОГО ПОКОЛІННЯ

3.1 Розробка програмного контролера для автоматизації процесу розгортання та управління якістю обслуговування програмно-конфігурованої мережі

Розгортання інтелектуальних інтенційно-орієнтованих мереж подвійного призначення в національному та регіональному масштабі дасть змогу в майбутньому знизити витрати державного бюджету для забезпечення телекомунікацій в інтересах органів державної влади, військового управління та органів місцевого самоврядування за рахунок спрощення процесу розгортання та експлуатаційного управління мережею, використовуючи інтелектуальні системи, центральним елементом яких є розумна машина (контролер), що знаходить потрібні зв’язки для корекції виконання поставленої задачі або прийняття заздалегідь правильного рішення у конкретній мережній ситуації. Даний контролер використовується для реалізації декількох інноваційних рішень в роботі, таких як автоматичне розгортання мережі, автоматизація QoS/QoE політик та централізований моніторинг функціонування мережі. Такий підхід робить процес керування мережею більш гнучким, а обслуговування мережі — більш інтелектуальним. База знань є головним ядром інтелектуальної управляючої системи IBN реалізованої на контролері у вигляді сукупності знань для вирішення конкретних задач необхідних для автоматизованого мережного управління засобами машинного навчання [130].

Саме тому, за допомогою мови програмування JS(JavaScript) розроблено власний IBN-контролер поверх відомого SDN ONOS контролера (рис.3.1). Для цього у роботі використано технологію віртуалізації операційної системи. Для

віртуалізації використано програму Oracle VM VirtualBox версії 6.1. Встановивши контролер ONOS версії Falcon 1.5.1 на віртуальну серверну машину на рис.3.1 показано його основні системні характеристики .

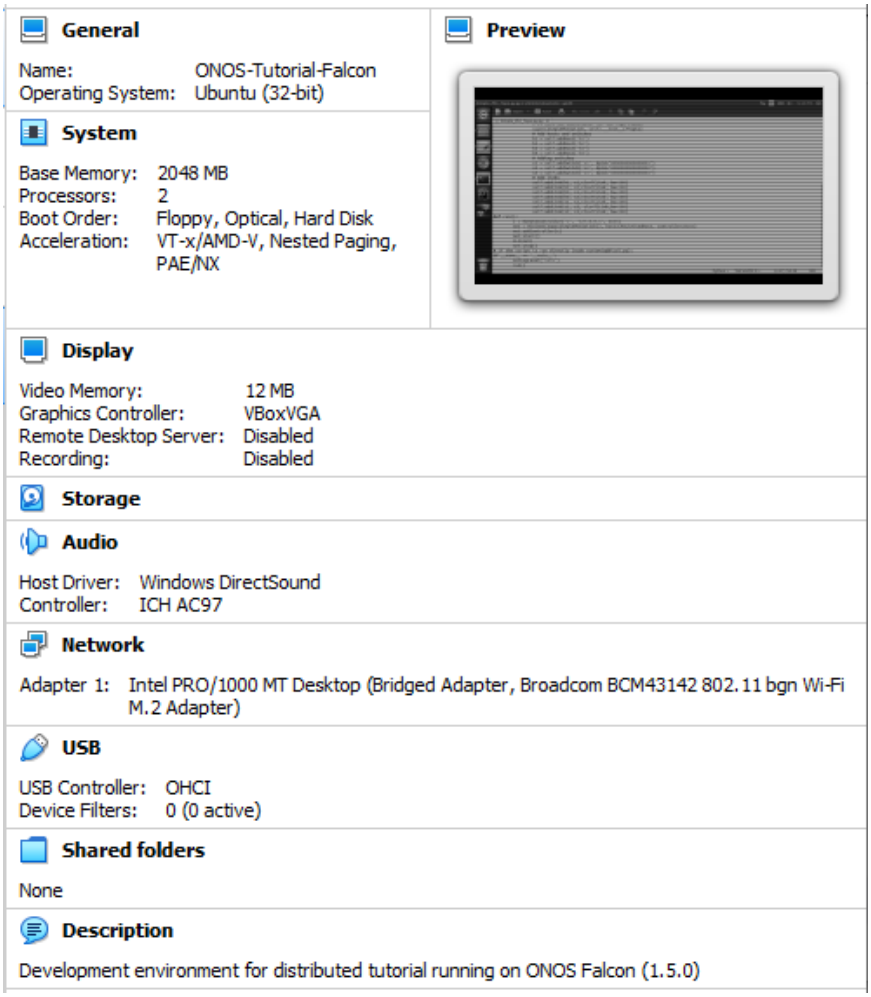


Рис.3.1. Характеристики VM ONOS SDN Controller

Дана версія ONOS запускається на операційній системі Ubuntu 14.04.4 LTS. Версія Mininet 1.0 який використовує OpenFlow 1.0. Створюємо файл з конфігурованою мережею «Simple_Pkt_Topo.py». Для прикладу створюємо топологію яка буде складатись із 3-х комутаторів та 4-х хостів, задаємо пропускні здатності в 100 Мбіт/с. Для запуску використовуємо наступні команди:

cd onos та ***ok clean***

Запускаємо mininet з конфігурованим файлом за допомогою команди:

sudo -E python Simple_Pkt_Topo.py.py --link tc, bw=1,delay=10ms

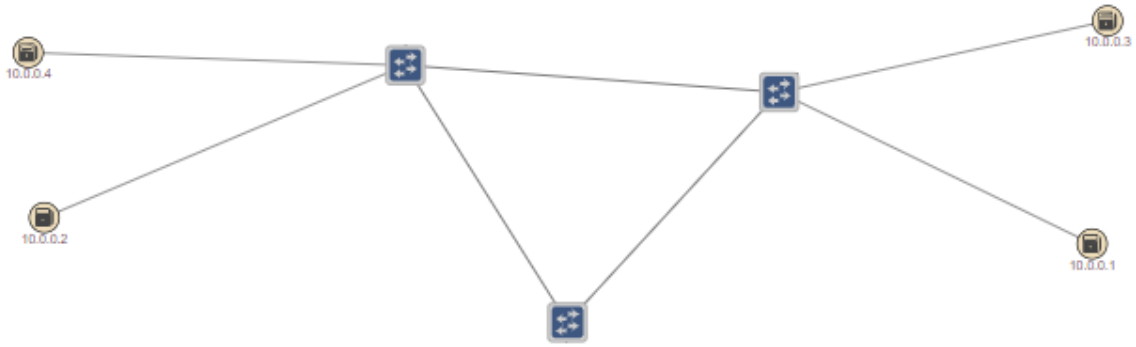


Рис. 3.2. Топологія мережі сконфігурованої в середовищі Mininet

На рис. 3.2 показано 4 кінцевих пристрої (хости) з такими IP адресами: host1-10.0.01, host2-10.0.02, host3-10.0.03, host4-10.0.04. Також на рисунку зображено 3 комутатори які мають відповідні назви: Swich1-of:0000000000000001, Swich2-of:0000000000000002, Swich3-of:0000000000000003.

Devices (3 total)

		Friendly Name	Device ID	Master Instance	Ports	Vendor	H/W Version	S/W Version	Protocol
✓		of:0000000000000001	of:0000000000000001	127.0.0.1	5	Nicira, Inc.	Open vSwitch	2.0.2	OF_10
✓		of:0000000000000002	of:0000000000000002	127.0.0.1	5	Nicira, Inc.	Open vSwitch	2.0.2	OF_10
✓		of:0000000000000003	of:0000000000000003	127.0.0.1	3	Nicira, Inc.	Open vSwitch	2.0.2	OF_10

Рис.3.3. Дані з UI ONOS контролера

Кожний комутатор має свою таблицю потоків, в якій містяться дані про правила, їхній пріоритет, статус встановлення, кількість пакетів та байтів.

Flows for Device of:0000000000000001 (3 total)

Flow ID	App ID	Group ID	Table ID	Priority	Timeout	Permanent	State	Packets	Bytes
0x70000487f5557	7	0x0	0	40000	0	true	Added	2,216	179,496
Criteria: ETH_TYPE:lldp									
Treatment Instructions: OUTPUT:CONTROLLER									
0x70000487f63a1	7	0x0	0	40000	0	true	Added	2,216	179,496
Criteria: ETH_TYPE:bddp									
Treatment Instructions: OUTPUT:CONTROLLER									
0x70000488ebd5d	7	0x0	0	40000	0	true	Added	7	294
Criteria: ETH_TYPE:arp									
Treatment Instructions: OUTPUT:CONTROLLER									

Рис.3.4. Таблиця потоків для swich1

Розроблення контролера було виконано на фреймворку vuejs та бібліотеці JQuery. Vue це прогресивний фреймворк для створення користувацьких інтерфейсів. На відміну від фреймворків-монолітів, Vue створений придатним для поступового впровадження. Його ядро в першу чергу вирішує завдання рівня представлення (view), що спрощує інтеграцію з іншими бібліотеками та існуючими проектами. З іншого боку, Vue повністю підходить і для створення складних односторінкових додатків (SPA, Single-Page Applications), якщо використовувати його спільно з сучасними інструментами та додатковими бібліотеками.

Основними концепціями Vue є: конструктор, компоненти, директиви, переходи. Vue надає різні способи застосування анімаційних ефектів, коли елементи намальовані, оновлені або видалені з DOM. Вони включають в себе інструменти для:

- автоматичного застосування класів для CSS-переходів і анімацій.
- інтеграції сторонніх бібліотек для CSS-анімації, таких як Animate.css.
- використання JavaScript для маніпуляції DOM-му.
- інтеграції сторонніх JavaScript бібліотек для анімацій, таких як Velocity.js.

jQuery це швидка, невелика та багатофункціональна бібліотека JavaScript. Завдяки простому у користуванні API, який працює у безлічі браузерів, такі речі, як обробка та маніпулювання документами HTML, обробка подій, анімація та Ajax, набагато простіші. Завдяки поєднанню універсальності та розширюваності jQuery змінив спосіб, по якому мільйони людей пишуть на JavaScript.

За допомогою vuejs розроблено контролер для додавання події і зміни налаштувань контролера програмно-конфігурованої мережі.

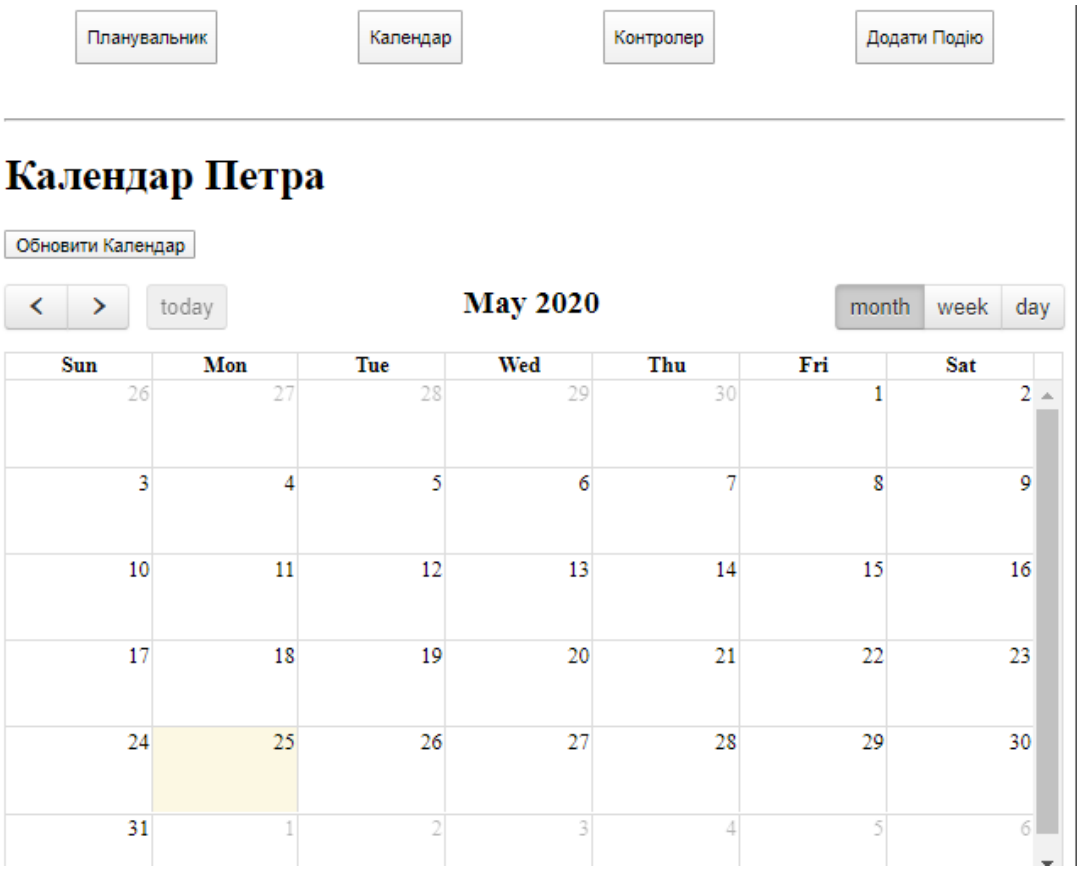


Рис.3.5. Графічний інтерфейс контролера для керування мережею створений за допомогою фреймворка vuejs

Також створено графічний календар в якому буде додаватись конкретний час події та, які зміни потрібно встановити для контролера. У вкладці «Планувальник» додаються події, які ми додаємо в ручну у вигляді таблиці та деякі дані про мережу(через які комутатори та їхні порти проходять пакети).

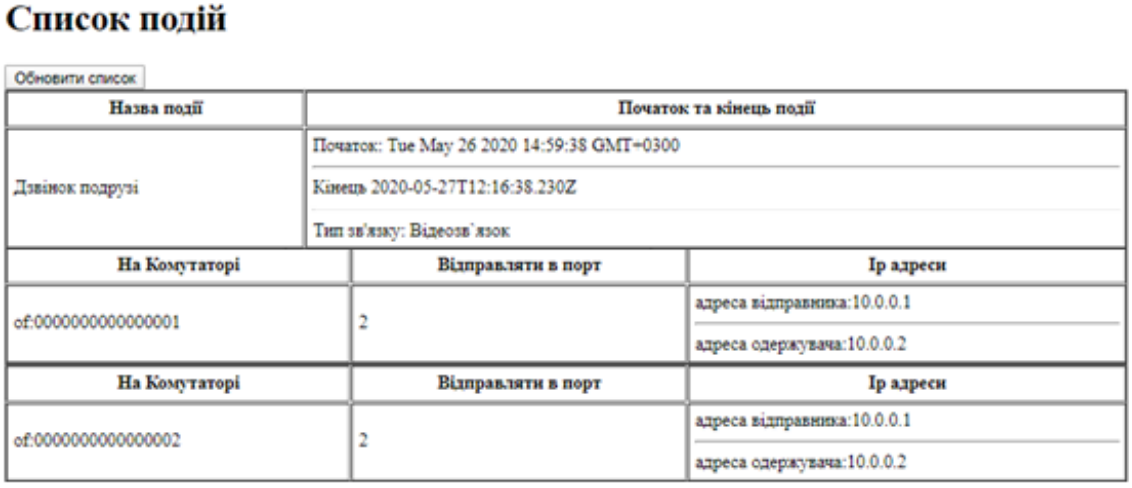


Рис.3.6. Вкладка «Планувальник»

У вкладці «Контролер» знаходиться ручне управління мережею, додавання та видалення правил мережі.

Рис. 3.7. Вкладка «Контролер»

При натисканні «Додати подію» появляється спливаюче меню в якому додається назва події, час події, кінець події та тип зв’язку (аудіо- та відео зв’язок).

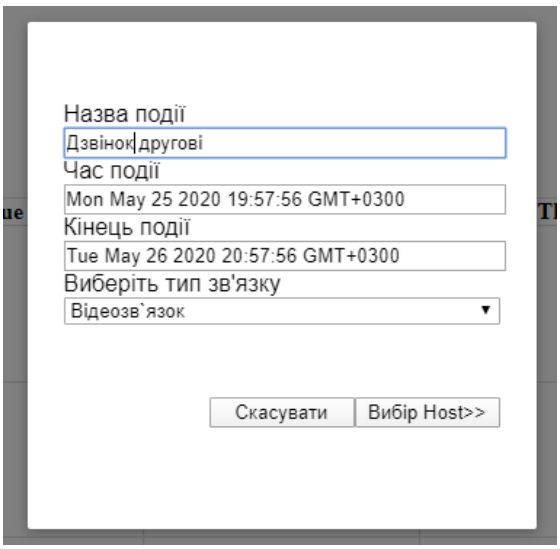


Рис.3.8. Створення події

При натисканні клавіші «Вибір Host>>» всі дані які ми заповнили будуть записані та будуть відображатись в календарі.

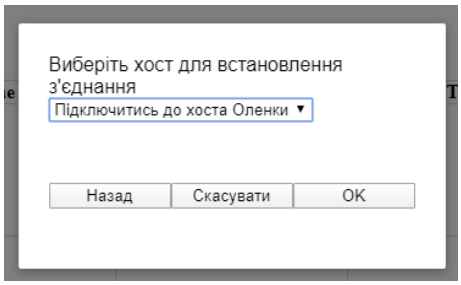


Рис.3.9. Вибір хоста для встановлення з’єднання

Після натискання кнопки «Ок» всі дані будуть збережені в масиві.

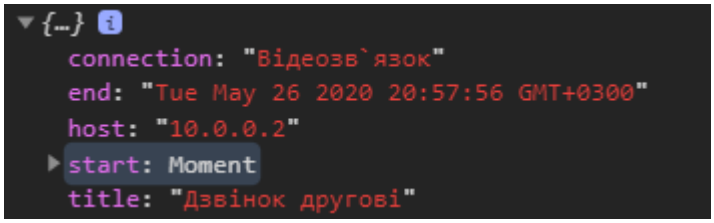


Рис.3.10. Дані які записуються після додавання події

На початку події відсилається запит на контролер та конфігуруються так звані правила мережі. Створюються правила для хостів з відповідними mac адресами (ETH_DST та ETH_SRC) для вхідного та вихідного порту комутатора, також додається пріоритет.

```
  "priority": 40000,
  "timeout": 0,
  "isPermanent": true,
  "deviceId": deviceId,
  "treatment": {
    "instructions": [
      {
        "type": "OUTPUT",
        "port": outPort
      }
    ]
  },
  "selector": {
    "criteria": [
      {
        "type": "ETH_TYPE",
        "ethType": "0x0800"
      },
      {
        "type": "ETH_DST",
        "mac": macDst
      },
      {
        "type": "ETH_SRC",
        "mac": macSrc
      },
    ]
  }
};
```

Рис.3.11. Фрагмент коду, створення правил мережі

На рис. 3.12 представлено графічний інтерфейс модуля контролера, який дає змогу проводити моніторинг завантаженості каналів мережі

Рис.3.12. Аплікація за допомогою бібліотеки JQuery

Щоб відобразити завантаженість каналу використано бібліотеку Highcharts. Highcharts - бібліотека програмного забезпечення для графіків, написаних в чистому JavaScript з їх допомогою ми зможемо виводити динамічно загруженість каналу в графік як для одного шляху так і для альтернативно шляху який було протестовано в четвертому експерименті. Для завантаження каналів трафіком використано програму iperf.

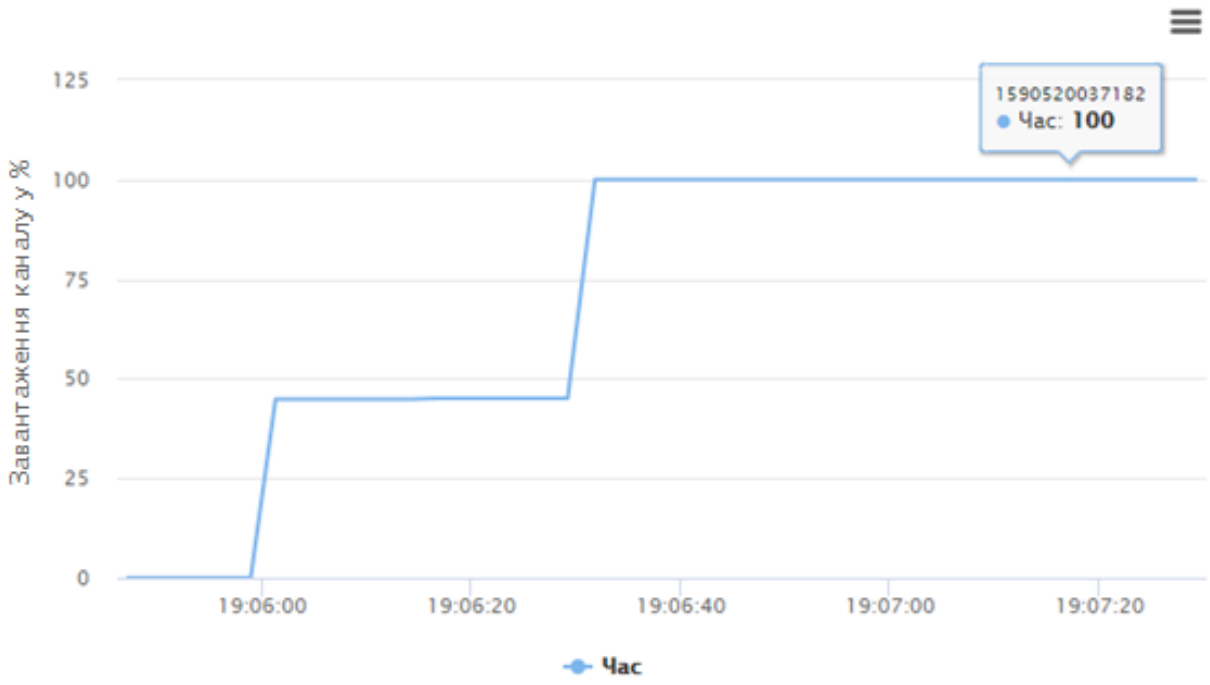


Рис.3.13. Завантаження каналу на шляху swich1-swich2

Вісь о-у відображає завантаження каналу в %, Вісь о-х відображає час оновлення даних які приходять із контролера.

Рис.3.14. Завантаження каналу на шляху swich1-swich3-swich2

Окрім автоматичного керування мережею, розроблений контролер дає змогу в ручному режимі змінювати правила та шляхи проходження пакетів по мережі. Це зроблено з метою тестування функціонування контролера в процесі його розроблення та покращення. Графіки показують завантаженість обраних каналів зв’язку.

3.2 Дослідження особливостей функціонування програмно-конфігурованої мережі нового покоління з використання розробленого контролера

Дослідження тривалості встановлення з’єднання за умов реактивного підходу до встановлення шляху

Суть експерименту полягає в тому, щоб перевірити з’єднання між кінцевими станціями. Коли правила створені в мережі та коли вони відсутні. За допомогою експерименту буде доведено те, що коли правила не встановлені

пакети не будуть надсилатись і тестування з’єднання між кінцевими станціями буде неможливе. Буде використано аплікацію Ui, а саме Reactive Forwarding App яка встановлює автоматично правила та протестуємо мережу, буде доведено чи спростовано, що при включенні Reactive Forwarding App затримка першого пакета буде високою.

В цьому експерименті буде зроблено наступні кроки:

Крок 1: Створення топології мережі та її запуску. Тестування з’єднання між кінцевими станціями за допомогою програми Ping коли правила не встановленні.

Якщо спробувати протестувати з’єднання між кінцевими станціями за допомогою програми Ping без правил мережі то передача пакетів не буде відбуватись.

Таблиця .3.1

Статистика тестування з’єднання між кінцевими станціями коли правила не встановленні

Кількість переданих пакетів	Середнє значення затримки	Втрати пакетів
7	200	100%

Крок 2: Встановлення правил за допомогою Reactive Forwarding App . Тестування з’єднання між кінцевими станціями за допомогою програми Ping при встановлених правилах мережі.

В пункті Applications вибираємо Reactive Forwarding App та тестуємо з’єднання між кінцевими станціями за допомогою програми Ping командою:

h1 ping h2

Таблиця 3.2

Тестування з’єднання коли підключено Reactive Forwarding App

Кількість переданих пакетів	Середнє значення затримки, мс	Мінімальне значення, мс	Максимальне значення, мс	Затримка першого пакета, мс
8	3.95	0.159	28.2	28.2

Отже, коли підключено реактивне встановлення потоків (Reactive Forwarding App) то затримка першого пакету буде набагато більшою ніж всі наступні, при високій завантаженості службових каналів може суттєво погіршити тривалість встановлення нового з'єднання, а це критично у випадку телефонного дзвінка чи термінової конференції.

Дослідження тривалості встановлення з'єднання з використання розробленого контролера за умов проактивного підходу до встановлення шляху. Суть експерименту полягає в тому щоб продемонструвати що з проактивним підходом який реалізує розроблений контролер, з'єднання буде встановлене ще до початку сеансу зв'язку і тому, затримка першого пакета буде набагато меншою ніж при встановленні реактивного встановлення потоків.

Крок 1:Додавання події в календарі та зміни правил мережі.

Вимикаємо Reactive Forwarding App та переходимо до створеної аплікації для встановлення події.

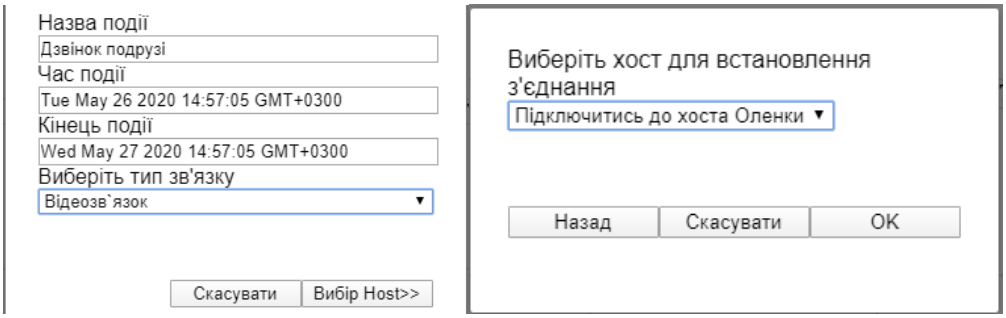


Рис.3.15. Додавання події в створеному додатку

Створивши подію перевіряємо її в календарі

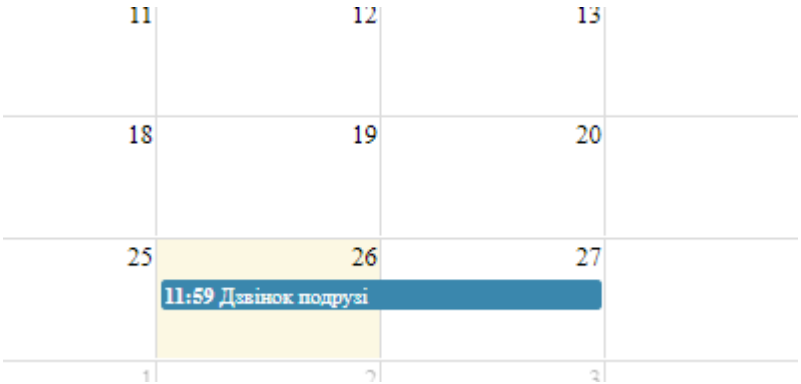


Рис.3.16. Відображення події в календарі

У вкладці Планувальник додаються всі дані про мережу та подію. Додається шлях проходження пакета на комутаторах та в які порти відправляється пакет, також показано IP адреси відправника та одержувача.

Список подій

Обновити список

Назва події	Початок та кінець події
Дзвінок подрузі	Початок: Tue May 26 2020 14:59:38 GMT+0300 Кінець 2020-05-27T12:16:38.230Z Тип зв'язку: Відеозв`язок

На Комутаторі	Відправляти в порт	Ір адреси
	0	адреса відправника:10.0.0.1 адреса одержувача:10.0.0.2

На Комутаторі	Відправляти в порт	Ір адреси
of:0000000000000001	2	адреса відправника:10.0.0.1 адреса одержувача:10.0.0.2

На Комутаторі	Відправляти в порт	Ір адреси
of:0000000000000002	2	адреса відправника:10.0.0.1 адреса одержувача:10.0.0.2

На Комутаторі	Відправляти в порт	Ір адреси
of:0000000000000003	3	адреса відправника:10.0.0.1 адреса одержувача:10.0.0.2

Рис.3.17. Список подій в календарі

Крок 2:Тестування з’єднання між кінцевими станціями за допомогою програми Ping при встановлених правилах мережі за допомогою події в календарі.

Таблиця 3.3

Тестування з’єднання мережі з встановленими правилами

Кількість переданих пакетів	Середнє значення затримки, мс	Мінімальне значення, мс	Максимальне значення, мс	Затримка першого пакета, мс
10	0.359	0.109	1.45	1.45

Отже, було доведено, що при встановленні власних правил мережі затримка першого пакета є значно меншою від затримки при реактивному підключенні, а це дає змогу значно покращити якість обслуговування для користувачів зокрема в умовах інтенсивного навантаження мережі.

Дослідження якості обслуговування потоків реального часу в умовах високого завантаження каналу

Суть експерименту полягає в тому щоб додати в мережу додаткові два кінцевих пристрої та завантажити мережу максимально можливо, перевірити затримку передачі пакетів між двома пристроями.

Крок 1: За допомогою події яка була додана в другому експерименті використовуємо правила мережі.

Крок 2: За допомогою Iperf протестуємо мережу навантаживши h1 та h2 і визначимо затримку каналу на h3 та h4 .

Вводимо команду ***xterm h1 h2***. У консолі Node:h1 прописуємо наступну команду: ***iperf -c 10.0.0.2 -p 5566 -t 120***

У консолі Node:h2 прописуємо: ***iperf -s -p 5566 -i 1***

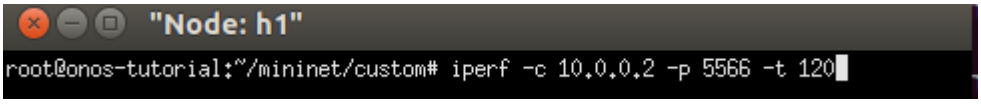


Рис.3.18. Тестування за допомогою iperf. Host 1

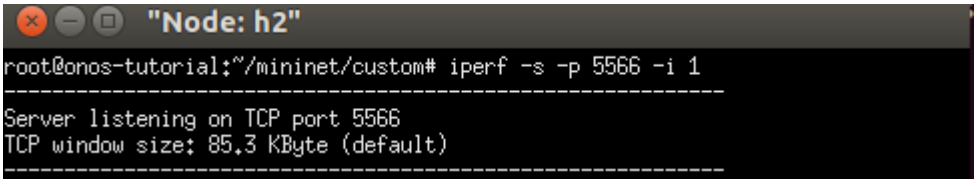


Рис.3.19. Тестування за допомогою iperf. Host 2

Одночасно запускаємо iperf та пінгуємо хости h3 та h4.

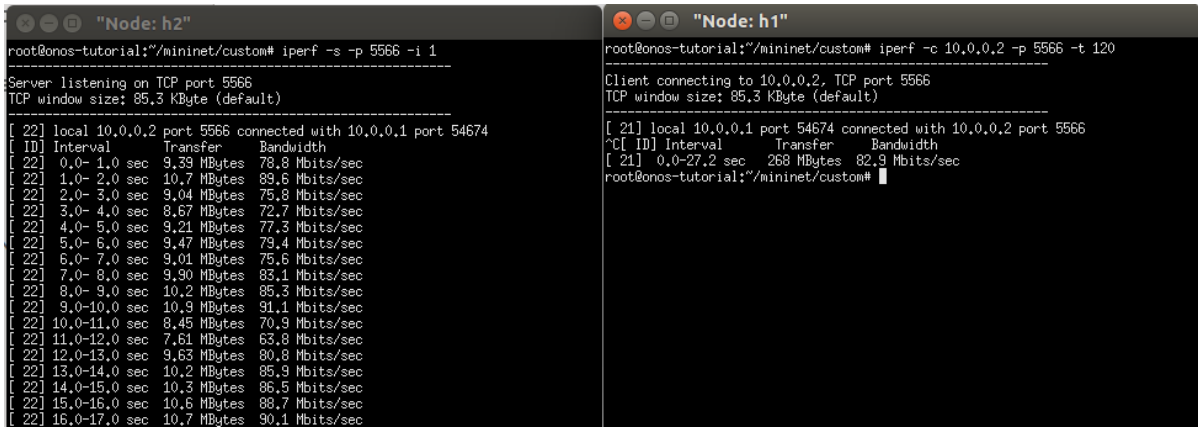


Рис.3.20. Запуск iperf на хостах h1 і h2

Таблиця 3.4

Статистика тестування з’єднання між кінцевими станціями при використанні Iperf на пристроях h1 та h2

Кількість переданих пакетів	Середнє значення затримки, мс	Мінімальне значення, мс	Максимальне значення, мс	Затримка першого пакета, мс
10	66.05	48.1	101	45.9

Таблиця 3.5

Статистика тестування з’єднання між кінцевими станціями при використанні Iperf на пристроях h3 та h4

Кількість переданих пакетів	Середнє значення затримки, мс	Мінімальне значення, мс	Максимальне значення, мс	Затримка першого пакета, мс
10	4.72	1.49	11.5	8.69

Завантаживши хости h1 та h2, на хостах h3 та h4 появляється середня затримка в 4.72 мс, що буде погано впливати на якість обслуговування користувачів.

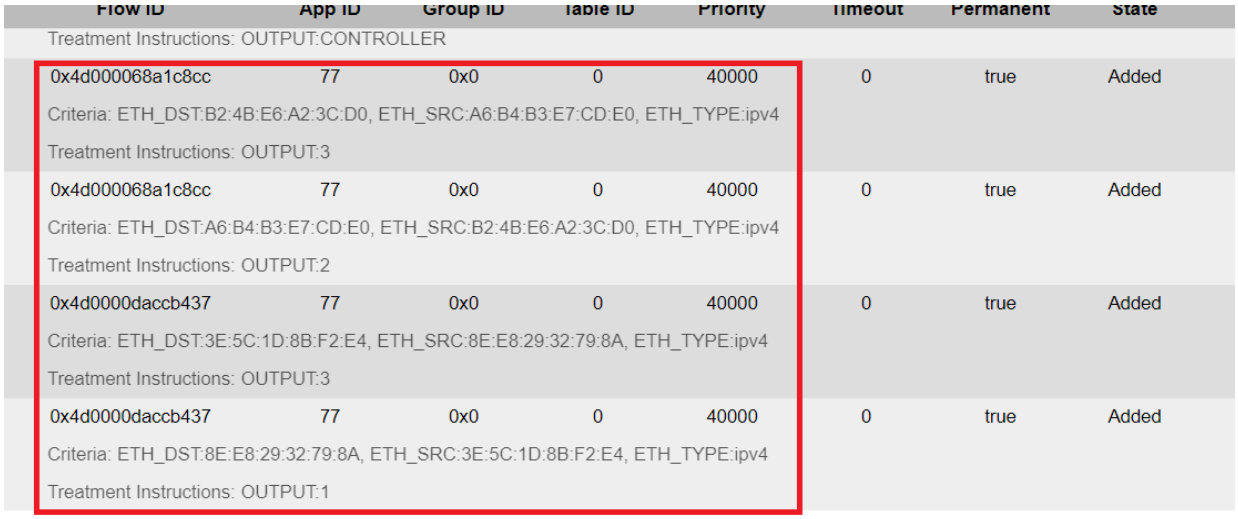


Рис.3.21. Таблиця потоків

В таблиці потоків додані всі правила. Отже, пакети усіх хостів проходять одним каналом через два комутатори of:0000000000000001 та

of:0000000000000002, через що мережа буде перевантажуватись, якщо один із хостів буде навантажувати мережу.

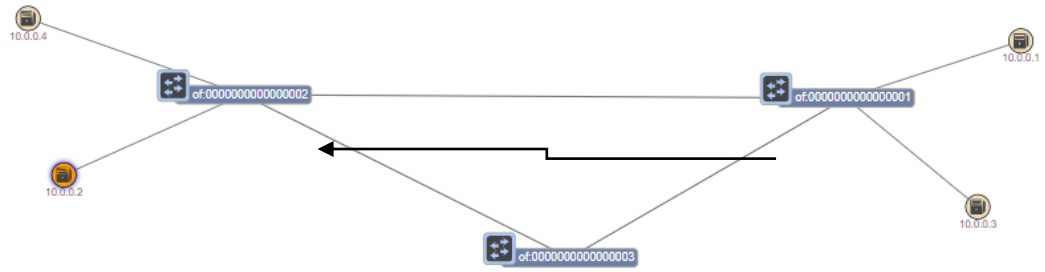


Рис.3.22. Топологія мережі

Дослідження забезпечення якості обслуговування потоків реального часу за допомогою розробленого контролера в рамках реалізації концепції інтенційно-орієнтованих мереж, а саме забезпечення контролю за якістю сеансу зв'язку.

Суть експерименту полягає в тому щоб продемонструвати ефективність розробленого контролера, який здійснює автоматичний моніторинг завантаженості каналів мережі і слідкує за тим щоб канали по яких проходять сеанси зв'язку не були перевантажені. Якщо канал в якому проходить сеанс зв'язку перевантажений то контролер спробує розвантажити такий канал перенаправивши трафік нижчого пріоритету альтернативними шляхами, тим самим зменшувати завантаженість каналу по якому буде відбуватись зустріч(тестування мережі за допомогою Ping).

Крок 1: Щоб уникнути перевантаження мережі на свічах розроблено нове правило яке буде перенаправляти потоки нереального часу (трафік з нижчим пріоритетом) альтернативними маршрутами. Якщо канал по якому проходять маршрути хостів h1 та h2 буде перевантажений то шлях передачі між хостами h3 та h4 буде прокладений через інші канали – альтернативним маршрутом перенаправленні на свіч 3(of:0000000000000003), що розгрузить мережу та зменшить затримки пакетів між хостами, якими відбувається сеанс зв'язку.

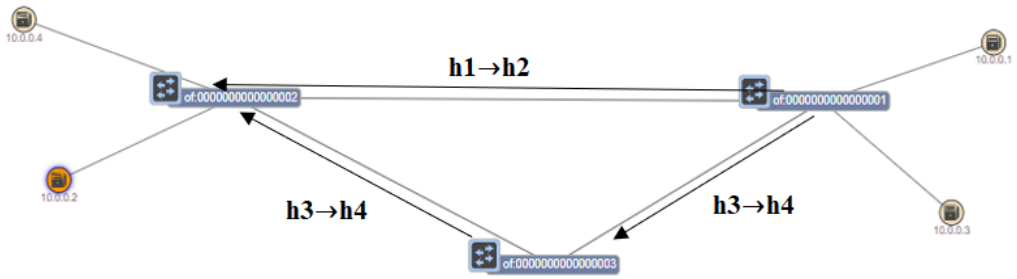


Рис.3.23. Топологія мережі при різних шляхах мережі

Крок 2: Після зміни правил мережі запускаємо iperf між хостами h1 та h2. Також тестуємо за допомого Ping хости h3 та h4 і перевіряємо їхню затримку.

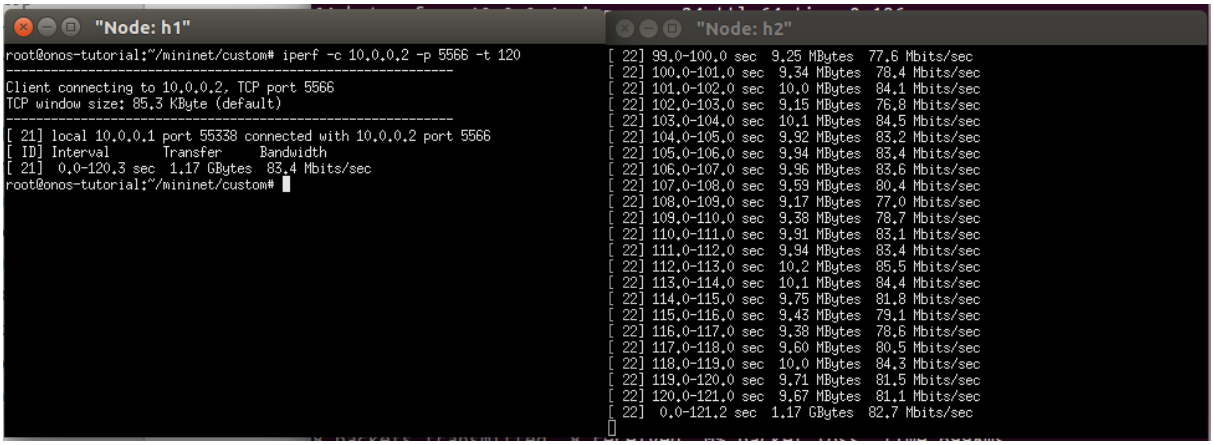


Рис.3.24. Результат iperf

Таблиця 3.6

Затримка на хостах h3 та h4 після зміни правил

Кількість переданих пакетів	Середнє значення затримки, мс	Мінімальне значення, мс	Максимальне значення, мс	Затримка першого пакета, мс
10	0.436	0.133	1.69	1.69

Рис.3.25. Завантаженість шляху swich1-swich2 до та під час підключення Iperf

Рис. 3.26. Завантаження шляху swich1-swich2 після динамічної зміни на альтернативний шлях

Із рис.3.26 видно, як розгружується шлях swich1-swich2 після динамічної зміни правил, тобто переходу на альтернативний шлях swich1-swich2- swich3

Отже, в результаті тестування підтверджено, що розроблений контролер, дав змогу не тільки проактивно прокласти з'єднання в мережі і тим самим гарантувавши готовність шляху до сеансу зв'язку, але і зміг виявити перевантаження каналу та розвантажити канал, по якому проходить сеанс зв'язку, таким чином забезпечивши необхідну якість обслуговування для користувачів.

3.3 Розробка унікального IBN-контролера для швидкого розгортання та управління мережевою інфраструктурою на основі QoE-інтенцій користувачів

У роботі також розроблено програмний контролер для інтенційно-орієнтованої інтелектуальної мережі, який оснащений політиками та моделями штучного інтелекту (AI), використання якого дало змогу реалізувати можливості, необхідні для аналізу стану системи щодо забезпечення замовленого рівня якості сприйняття послуг та автоматизованого пошуку оптимізованих операційних дій на основі спостережень із керованого середовища. Даний контролер надає велику перевагу та зменшує вплив людини на мережу, що збільшує швидкість реагування щодо переконфігурації мережі в умовах виявлення деградації якості обслуговування. Графічний інтерфейс розробленого контролера показано на рис.3.27.

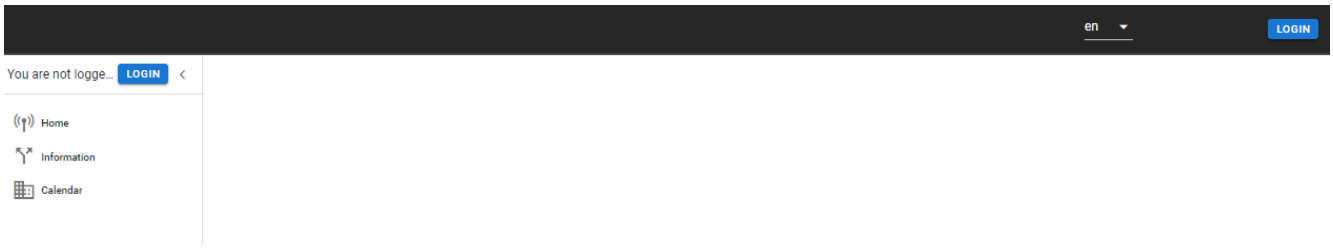


Рис.3.27. Графічний інтерфейс IBN-контролера

Перевагою є модульність контролера, який можна розгортати для усіх типів програмно-конфігурованих мереж у тому числі для ядра майбутньої мережі 5G/6G. Даний контролер має функцію авторизації (рис.3.28.), для того щоб користувачі мали змогу авторизуватись та використовувати свій акаунт для всіх маніпуляцій в мережі.

Авторизація реалізована за допомогою безкоштовної платформи для розробки мобільних та веб- застосунків **Firebase** за допомогою служби **Firebase Auth**. Firebase Auth - це служба, яка може аутентифікувати користувачів, використовуючи лише код на стороні клієнта. Він підтримує соціальні логін-провайдери Facebook, GitHub, Twitter і Google (і Google Play Games). Крім того,

вона включає в себе систему управління користувачами, за допомогою якої розробники можуть увімкнути автентифікацію користувача за допомогою входу з електронної пошти та пароля, що зберігаються в Firebase.

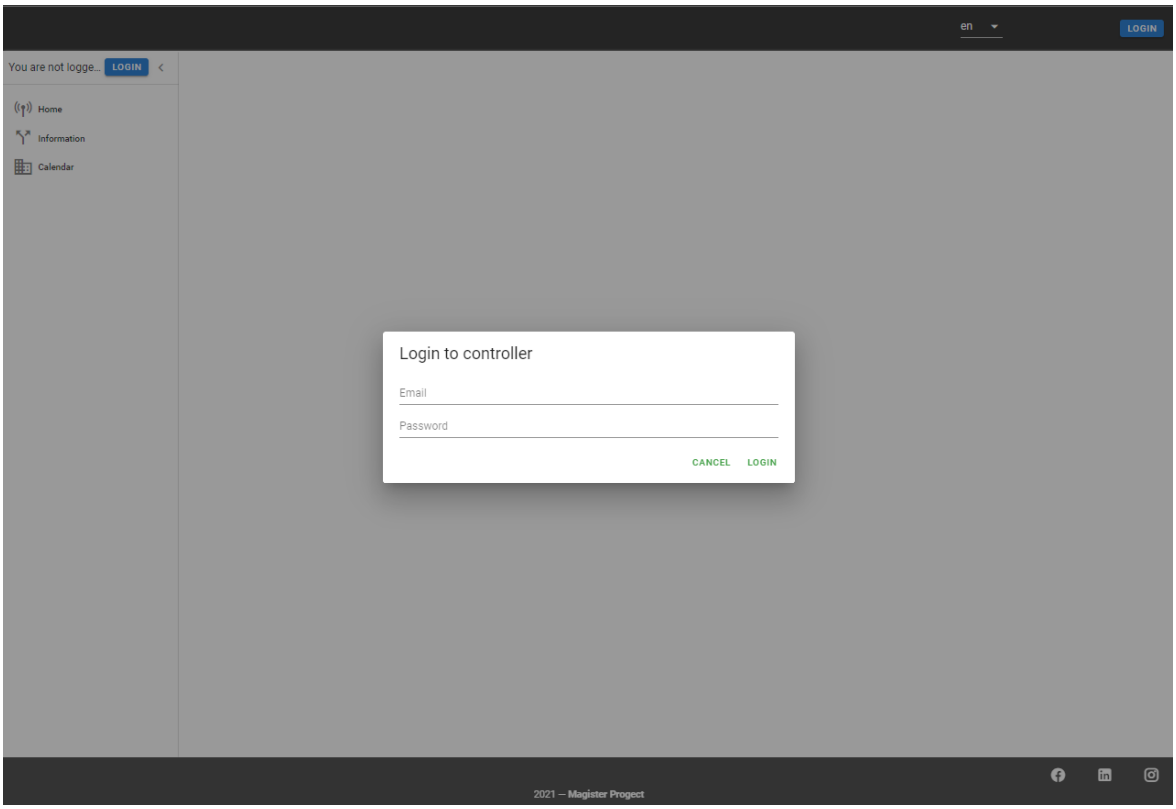


Рис.3.28. Авторизація за допомогою сервісу Firebase

Без авторизації клієнт не зможе переглядати меню контролера, додавати наміри, переглядати інформацію про мережу та будь-які інші маніпуляції із контролером.

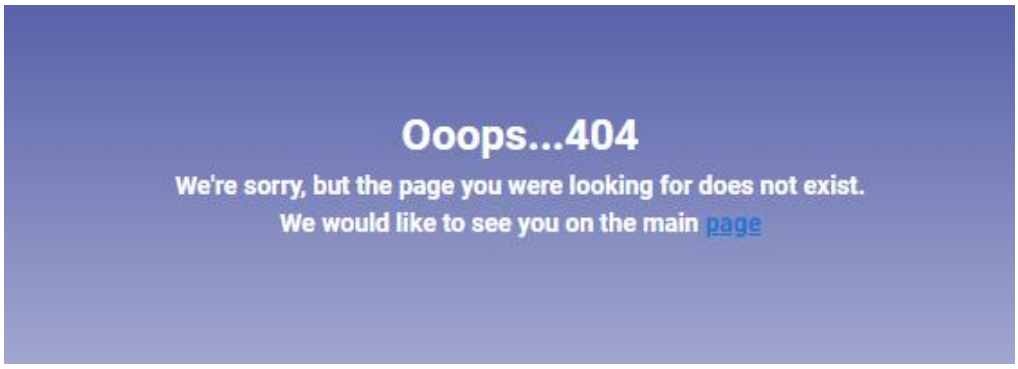


Рис.3.29. Тестування контролера без авторизації

Після авторизації перед користувачем будуть відкриті 3 меню (Home – меню де відображено топологію підключення та деяка статистика мережі у вигляді графіка, Information – Вся доступна інформація про користувачів, switch до яких вони підключенні і тд.) (рис.3.30). в лівому боковому меню та відображення деякої інформації користувача, чи він авторизований, його пошта та іконка. У верхньому правому кутку відображені дві кнопки за допомогою яких можна змінити мову відображення IBN-контролера та кнопка виходу користувача.

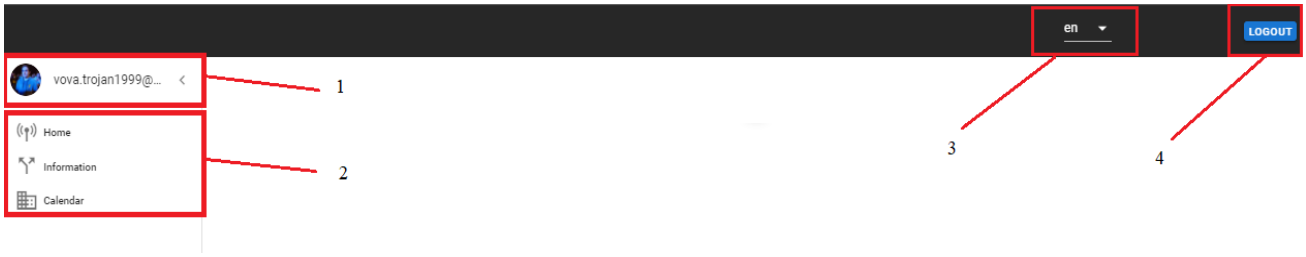


Рис.3.30. Графічне представлення авторизованого користувача в IBN-контролері: 1- деяка мінімальна інформація про користувача; 2- Меню доступні для користувача; 3- Кнопка для зміни мови відображення контролера; 4- Кнопка виходу користувача;

На вкладці **Home** знаходиться топологія підключеної мережі за допомогою Mininet та завантаженість вибраного каналу (рис.3.31) (за замовчуванням – нульові значення на графіку). На графіку зображено максимальність завантаження для деяких типів підключення, тобто, коли ми вибираємо якість зв'язку від 1 до 3, де 1 – найгірша якість зв'язку, а 3 – найкраща. Для найгіршої якості було вибрано завантаженість каналу в 90%, що буде істотно впливати на якість підключення до користувачів, якщо в шляху підключення будуть підключенні інші користувачі, що будуть завантажувати канал.

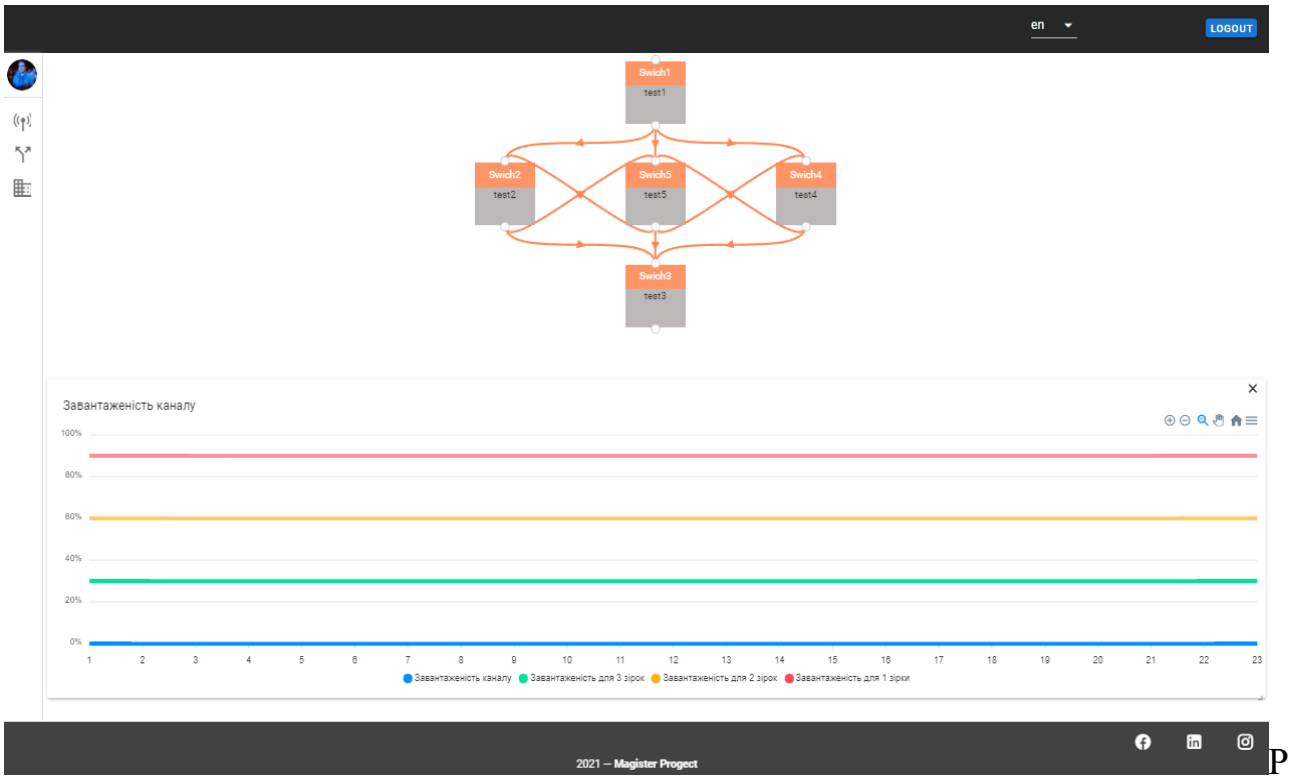


Рис.3.31. Вкладка **Home** IBN-контролера

На вкладці **Information** (рис.3.32) розміщена інформація в дві таблиці. В першій таблиці вся детальна інформація про Switch, які знаходяться в мережі (назва, тип, який в нього id, який протокол використовує та яка версія) (рис.3.33).

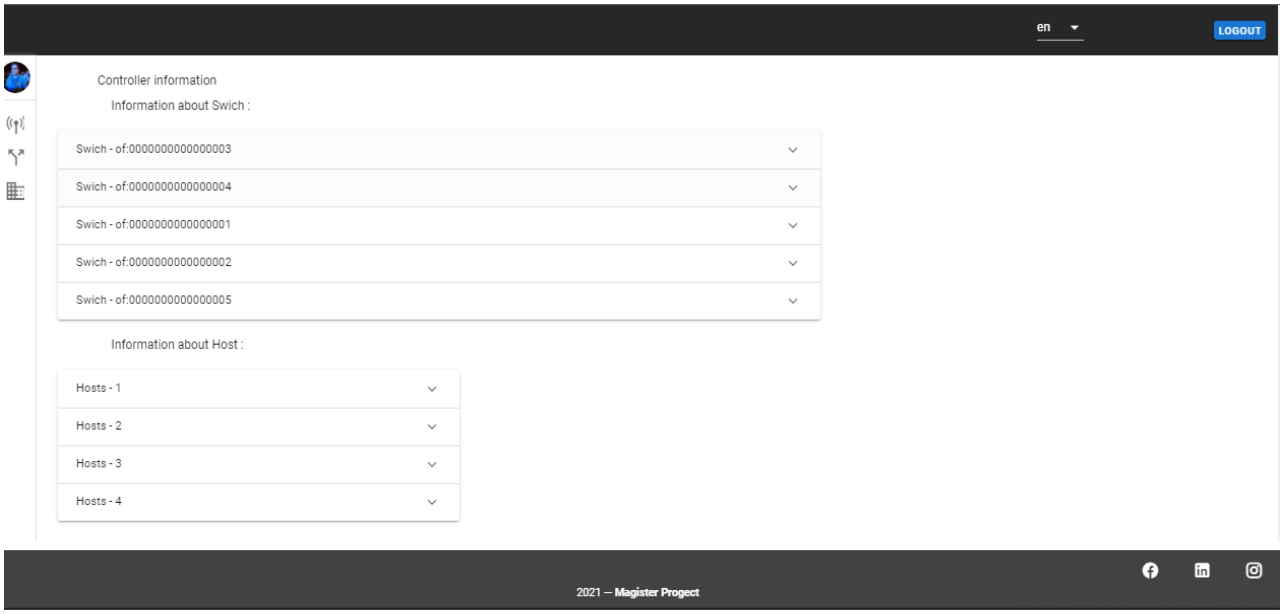


Рис.3.32. Вкладка **Information** IBN-контролера

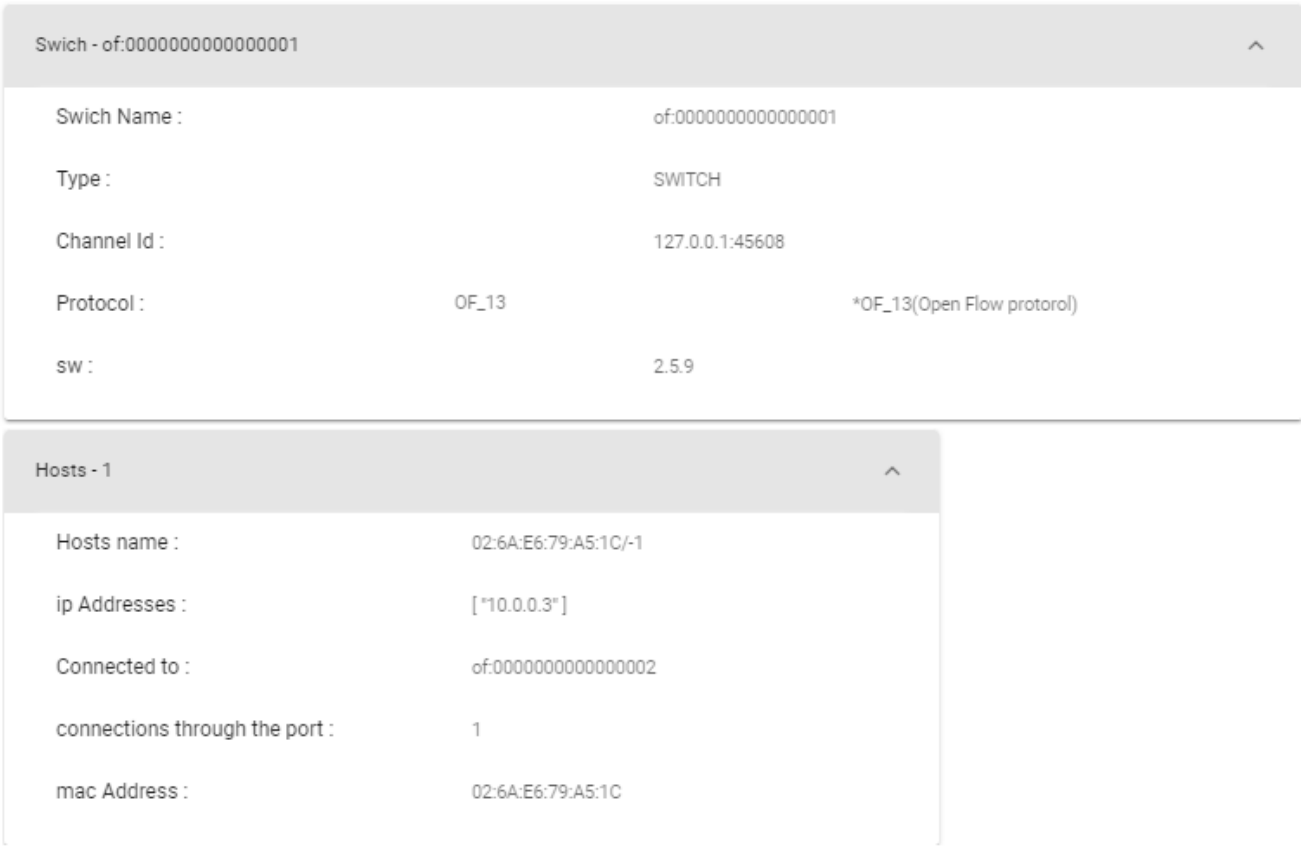


Рис. 3.33. Інформація про комутатори та контролери мережі Mininet

На вкладці **Calendar** (рис.3.34) відображено список створених QoE-намірів та можливість додавання своєї інтенції.

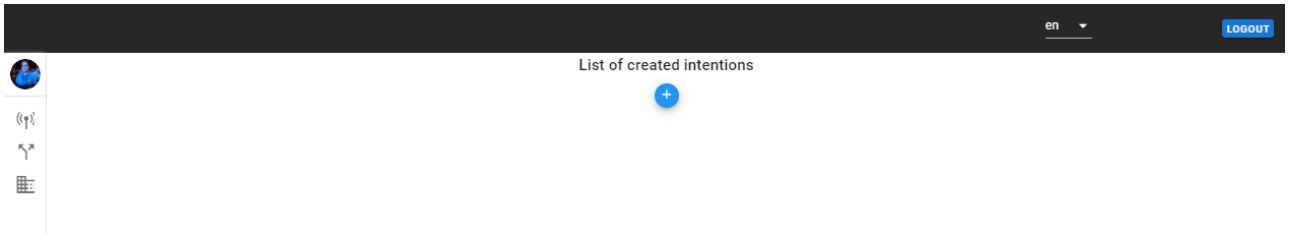


Рис.3.34. Вкладка **Calendar** IBN-контролера

При додаванні події (інтенції) додається модальне вікно (рис.3.35), в якому налаштовується дата створення, початок та кінець події, до якого хоста хочеш підключитись для зустрічі, тип мітингу (текстовий чат, аудіо конференція, відеоконференція, стрімінговой потік), та вибір замовленої QoE якості зв'язку. Для простоти зрозумілості серед користувачів даний показник замовленої

якості сприйняття послуг QoE реалізований за допомогою зірок, де одна червона зірка означає найгірший зв'язок, а три зірки це найвища якість зв'язку. Графічний інтерфейс розроблено з можливістю підтримки як англійської так і української мови.

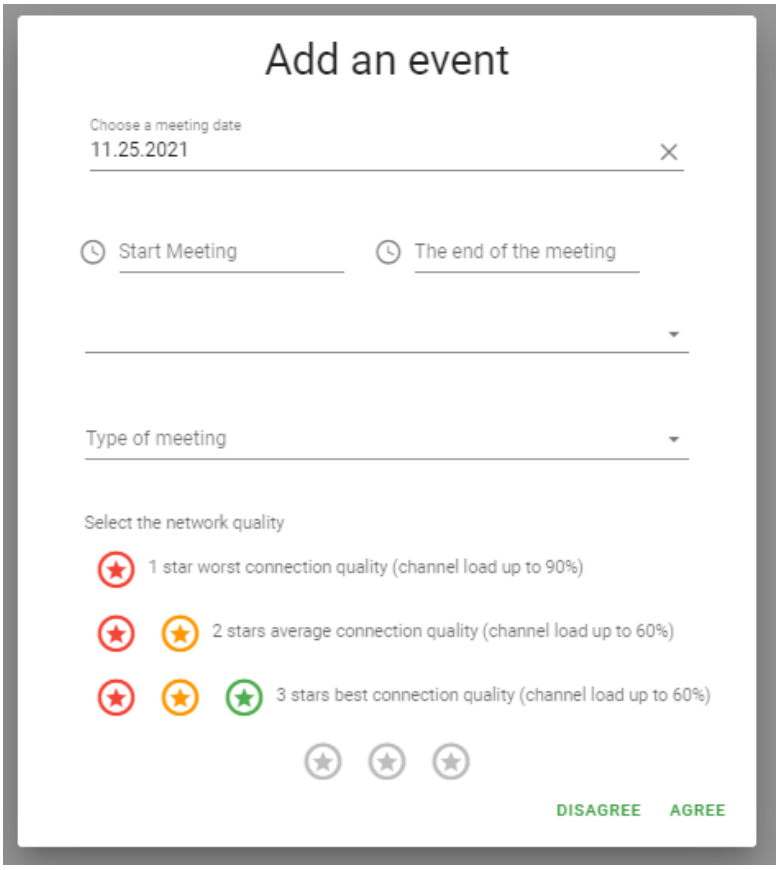


Рис.3.35. Створення інтенцій для користувача (інтерфейс англійською мовою)

Після того як вибрано всі пункти модального вікна, натиснувши **Agree (Підтвердити)** в списку створених намірів (рис.3.36), де відображено список подій. В даному списку подій відображено тип підключення, початок події, кінець події, якість обслуговування та дата створення. Під деякими даними розташовано два графіки. Перший графік відображає завантаженість каналу який створюється під час вибору хоста, та якості обслуговування. Другий графік показує додатковий шлях, на який будуть переміщатись всі завантаження мережі які будуть навантажувати мережу.

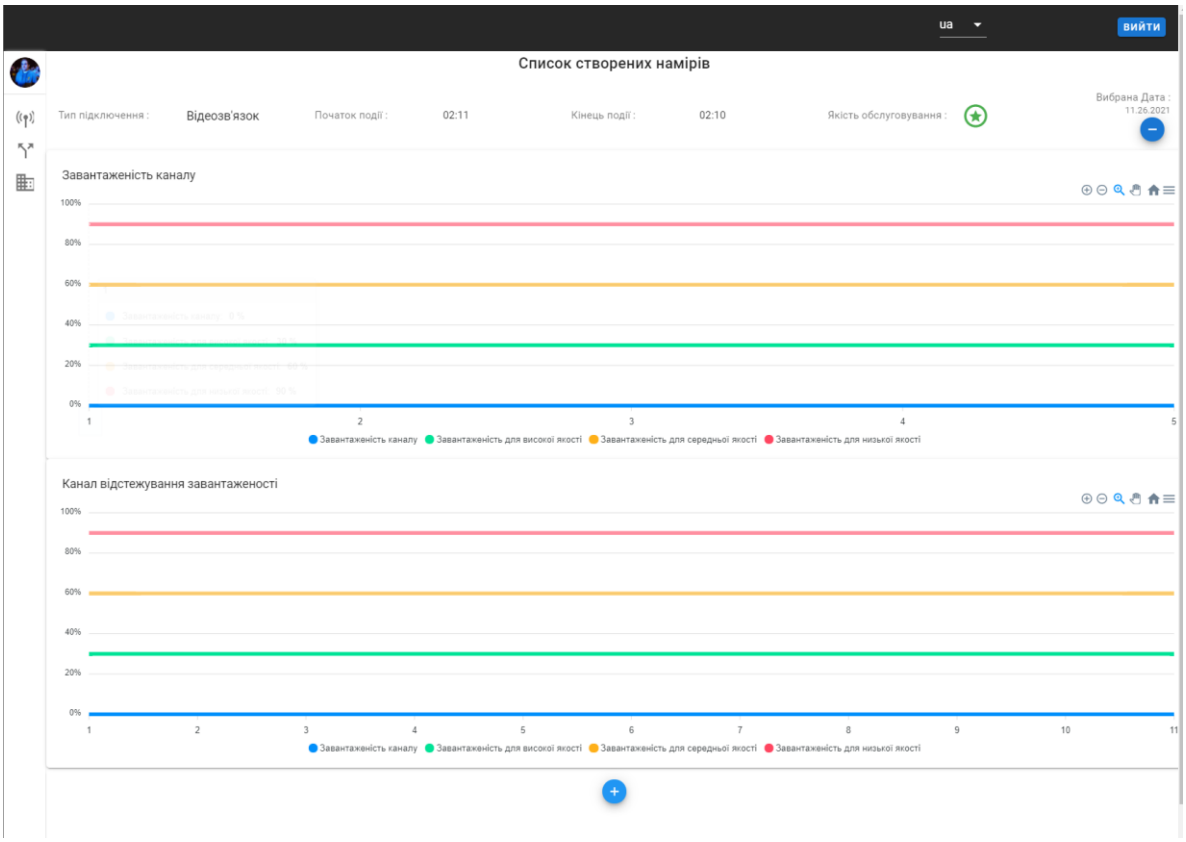


Рис.3.36. Система моніторингу події в IBN-контролері [130]

Для того щоб підключити розроблюваний контролер до мережі Mininet потрібно використати SDN-контролер ONOS який встановлюється по аналогії до Mininet. Скачуємо готовий образ та імпортуємо його до VirtualBox. Після імпорту контролера встановлюємо Mininet для цього контролера та підключаємо створену раніше топологію за допомогою команди:

sudo mn --custom ./mininet/examples/multi-hosts.py --controller=remote, ip=127.0.0.1 --topo=mytopo

Після підключення можна переглянути веб конфігурацію самого SDN контролера переходячи за посиланням:http://localhost:8181/onos/ui/index.html#/app. В якому ми побачимо чи є підключення даного контролера до Mininet.

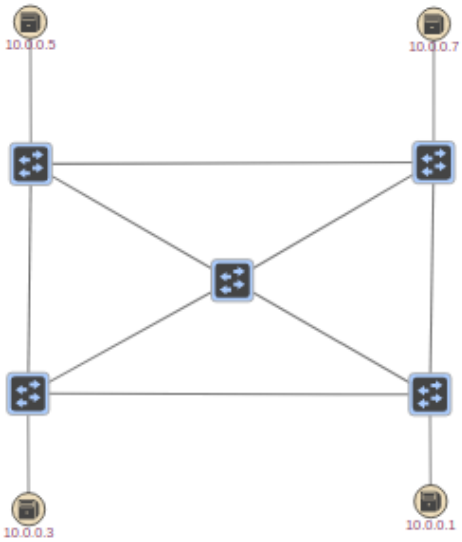


Рис.3.37. Відображення підключення топології Mininet до контролера ONOS

Розроблюваний контролер працює за рахунок API сервісів SDN контролера ONOS (Рис.3.38). API (Application Programming Interface) — це набір готових класів, процедур, функцій, структур і констант, що надаються додатком (бібліотекою, сервісом) для використання в зовнішніх програмних продуктах.

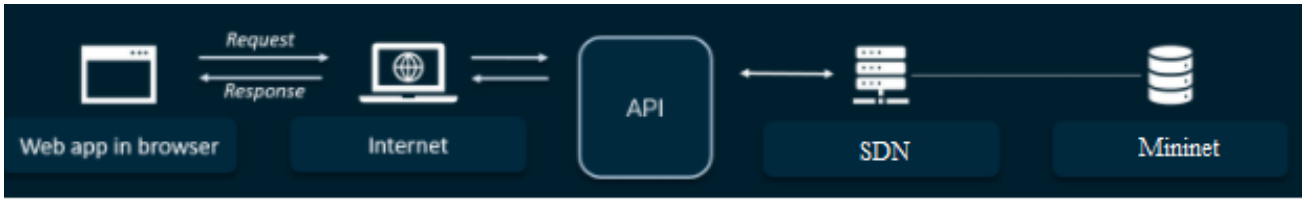


Рис.3.38. Структура підключення розробленого IBN контролера

SDN контролер має багато методів для доступу до даних мережі Mininet (рис.3.39), наприклад: дані про хости, комутатори, маршрути передавання, що були використані в розроблюваному IBN-контролері в меню Information. Доступ до цих методів реалізовано за допомогою бібліотеки axios js. Основні методи запиту які виконуються за допомогою API:

- GET – збирає інформацію (отримання даних із контролера).
- PUT – оновлює дані (оновлення даних із контролера).
- POST – створює (створення додаткових налаштувань для мережі).

• ВИДАЛИТИ – (видалення мережі, шляхів, хостів, свічів і тд.).

Axios - це широко відома JavaScript-бібліотека. Це HTTP-клієнт, заснований на промісах і призначений для браузерів і Node.js. Приклад використання даної бібліотеки зображено на рисунку 3.40.

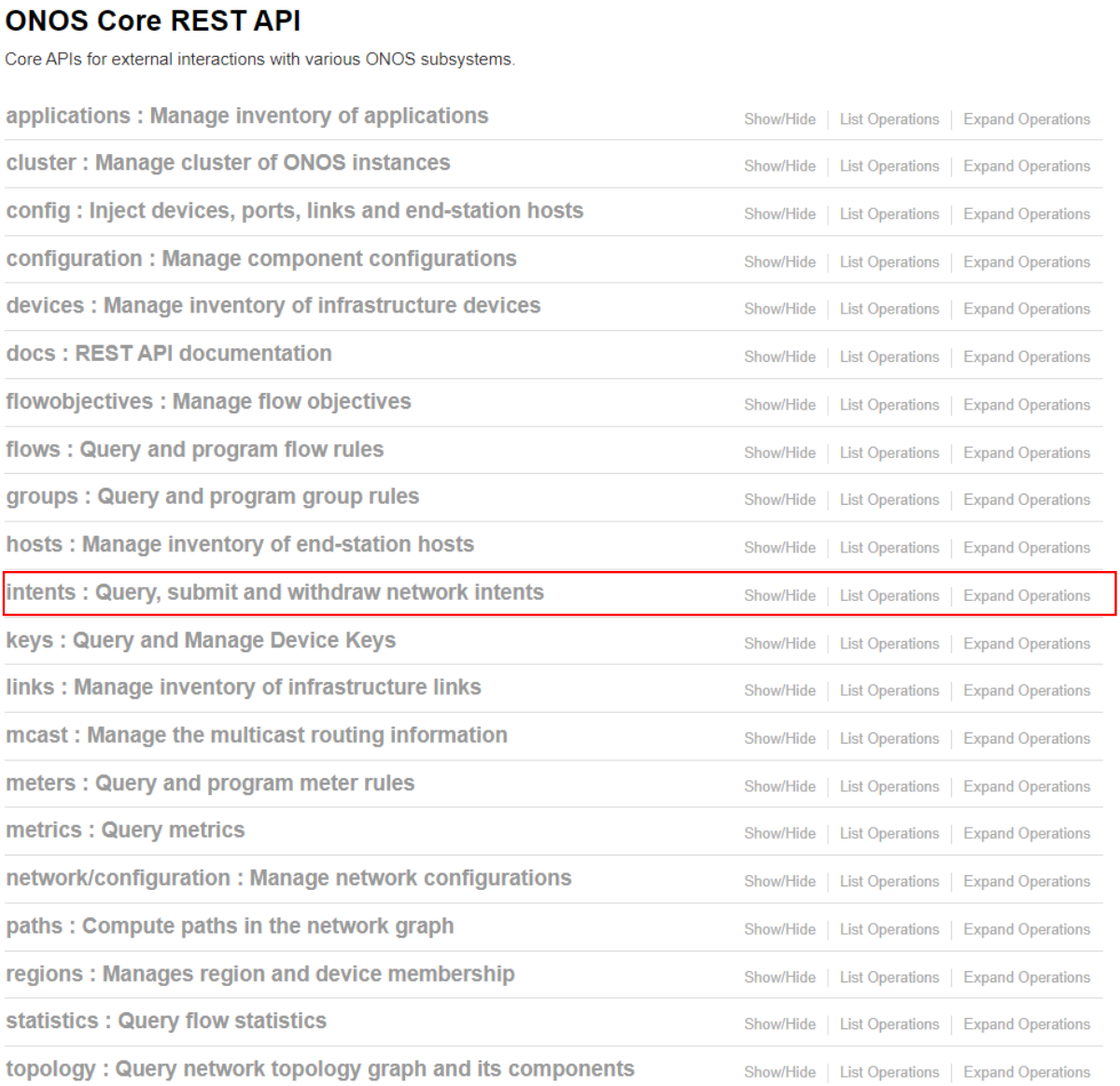


Рис.3.39. Деякі функції API розробленого IBN/ONOS контролера

```
import axios from "axios";

export default (routeUrl, Get, data) => {
  return axios({
    method: Get,
    url: routeUrl,
    data: data
  }).then(response => {
    return response;
  });
};
```

Рис.3.40. Приклад використання бібліотеки в розроблюваному IBN-контролері

Підключивши контролер до мережі тестуємо додавання та видалення інтенцій для деяких користувачів. Для початку пропінгувавши хости h1(даний хост було вибрано як хост з якого виконуються всі події), h5 щоб переконатись, що ніяких підключень не існує (рис.3.41).

Для того щоб пропінгувати використаємо команду:

h1 ping h5

```
mininet> h1 ping h5
PING 10.0.0.5 (10.0.0.5) 56(84) bytes of data.
^C
--- 10.0.0.5 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 999ms
```

Рис.3.41. Пінгування мережі Mininet

Як бачимо, пінгування не відбувається, оскільки 100% пакетів втратилось, це свідчить про те, що в мережі не існує підключення між хостами h1 та h5. Додаємо подію заповнюючи всі потрібні пункти в модальному вікні (рис.3.42), так щоб у нас зразу додалась подія і всі налаштування застосувались після чого перевіряєм пінгування тією ж командою, що і раніше. У даному випадку вибрано найкращу якість обслуговування (QoE-3).

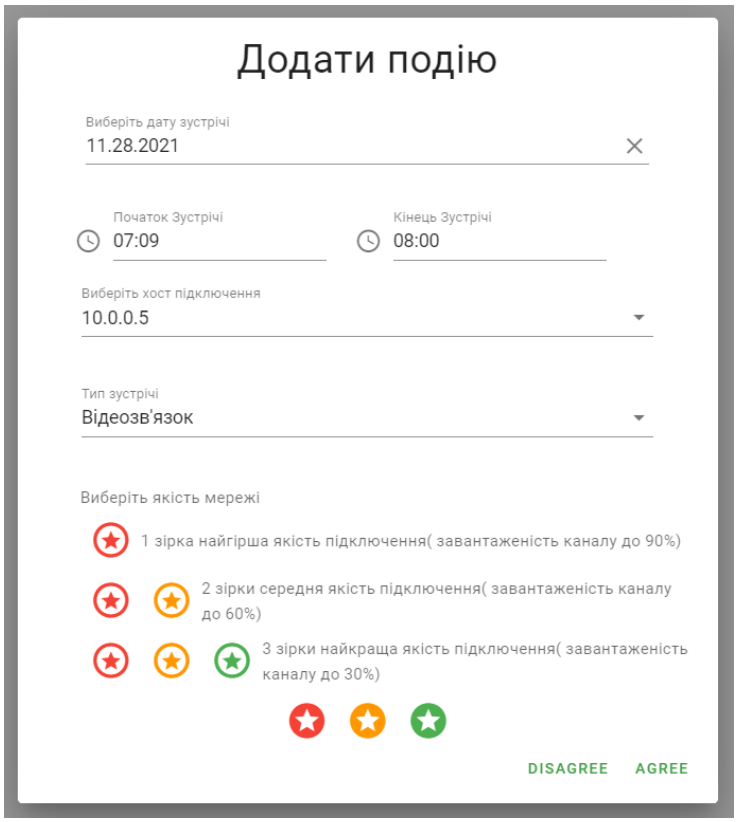


Рис.3.42. Вибір пунктів для події (інтенції)

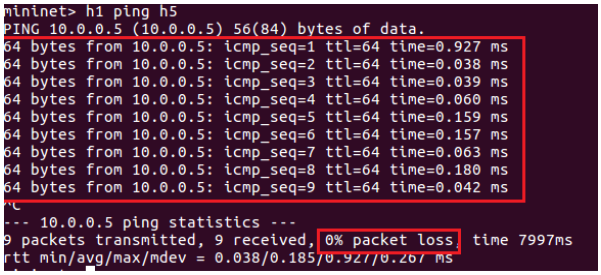


Рис.3.43. Пінгування після додавання події

Як бачимо із рисунку 3.43 пінгування проходить успішно і у нас втрата пакетів 0%. Отже, контролер працює та надаються потрібні правила мережі для того, щоб забезпечити підключення даного хоста h1 до хоста h5. Після закінчення часу інтенції, дана подія буде видалена із списку відображуваних інтенцій і всі правила, які були запропоновані для даних користувачів будуть також видалені із SDN контролера. Даний контролер використовує шляхи, які надходять із SDN контролера за допомогою API, та може автоматизовано

корегувати дані шляхи на основі вхідних інтенцій користувачів, додаючи нові шляхи, та видаляти їх згідно власної розроблювальної логіки маршрутизації.

3.4 Забезпечення гарантованої якості обслуговування користувачів системи спеціального зв'язку в умовах розгортання IBN

Отже, у роботі для реалізації інтенційно-орієнтованих мереж (рис.3.44) розроблено надбудову SDN контролера, який дає змогу: транслювати бізнес потреби в адаптивну мережну конфігурацію, а саме, прокладати канали в корпоративних мережах для сеансів зв'язку, покращувати якість обслуговування потокам реального часу, здійснювати моніторинг параметрів функціонування мережі та проводити динамічне балансування навантаження в мережі.

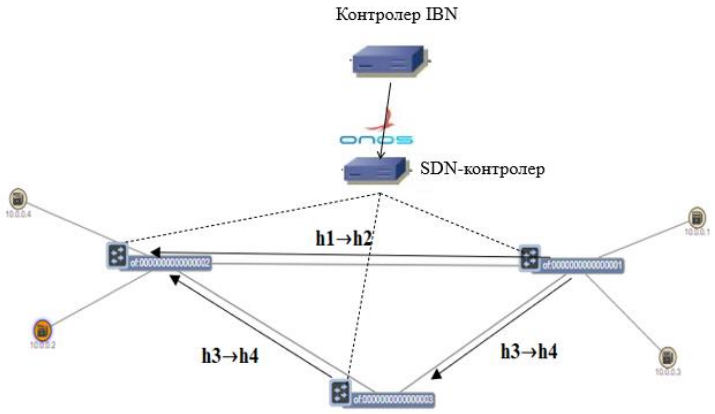


Рис. 3.44. Топологія інтенційно-орієнтованої мережі

Ідея роботи полягає в тому, щоб розробити ефективний контролер, який здійснює автоматичний моніторинг завантаженості каналів мережі і слідкує за тим щоб канали по яких проходять сеанси спецзв'язку (важливий пріоритет) не були перевантажені. Якщо канал в якому проходить сеанс зв'язку буде перевантажений, розроблений IBN контролер спробує розвантажити такий канал перенаправивши трафік нижчого пріоритету альтернативними шляхами, тим самим зменшить завантаженість каналу по якому буде відбуватись запланована онлайн зустріч спецзв'язку. За допомогою команди Ping

згенеровано потік в якому кожної секунди передавався пакет (Рис.3.45). Як видно з Рис.3.45 при завантаженні каналу генератором iperf, затримка пакетів, які проходять через даний канал є досить високою, що буде впливати на якість зв'язку запланованого сервісу, після розвантаження каналу на основі встановлених правил IBN контролером, починаючи з 11 пакета затримка пакетів становить не більше 1 мс, що вказує на можливість передавати потоки реального часу через даний канал.

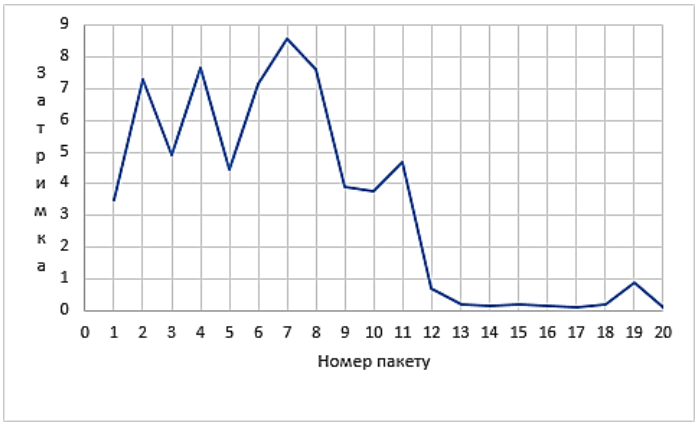
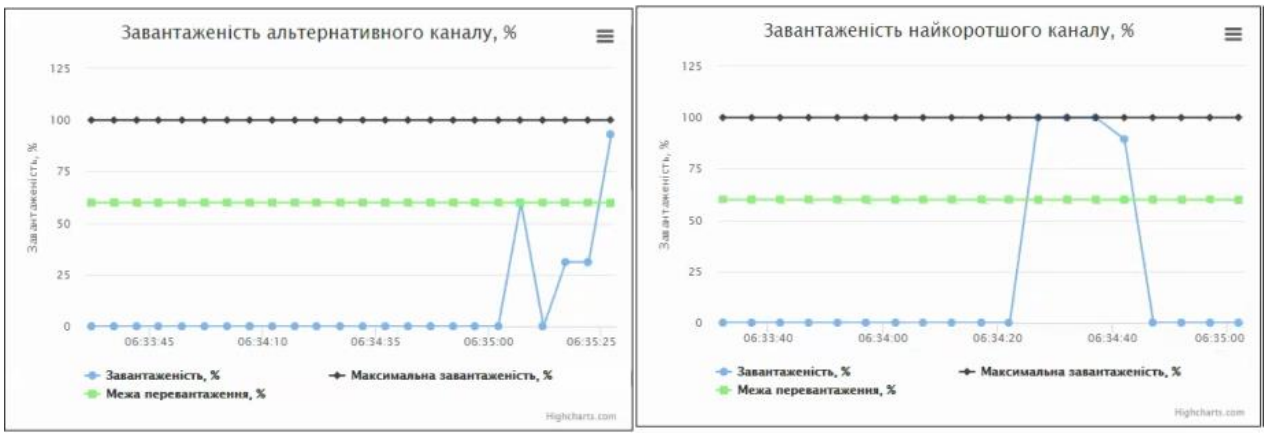


Рис. 3.45. Затримка пакетів при переходжені навантаження на альтернативний шлях



а) б)

Рис.3.46. Завантаженість каналів: а)найкоротшого каналу до та після переходу навантаження на альтернативний шлях; Б) Завантаженість альтернативного каналу після розвантаження найкоротшого шляху[130]

Таким чином, у роботі розроблено та протестовано IBN контролер для реалізації концепції інтенційно-орієнтованих мереж, який є надбудовою над контролером програмно-конфігурованих мереж і дає змогу автоматично та проактивно будувати маршрути в мережі для запланованих сеансів спец зв'язку, а також дає змогу стежити за завантаженістю каналів мережі та здійснювати динамічний перерозподіл потоків у мережі для забезпечення якості обслуговування трафіку реального часу в рамках сеансу зв'язку.

Управління якістю обслуговування в розробленому контролері відбувається за рахунок намірів. Коли користувач заповняє всі відповідні поля модального вікна (рис.3.47), всі ці дані перетворюються з даних які розуміє користувач в наміри які буде розуміти SDN мережа (рис.3.48) яка розгорнута в моделювальному середовищі Mininet.

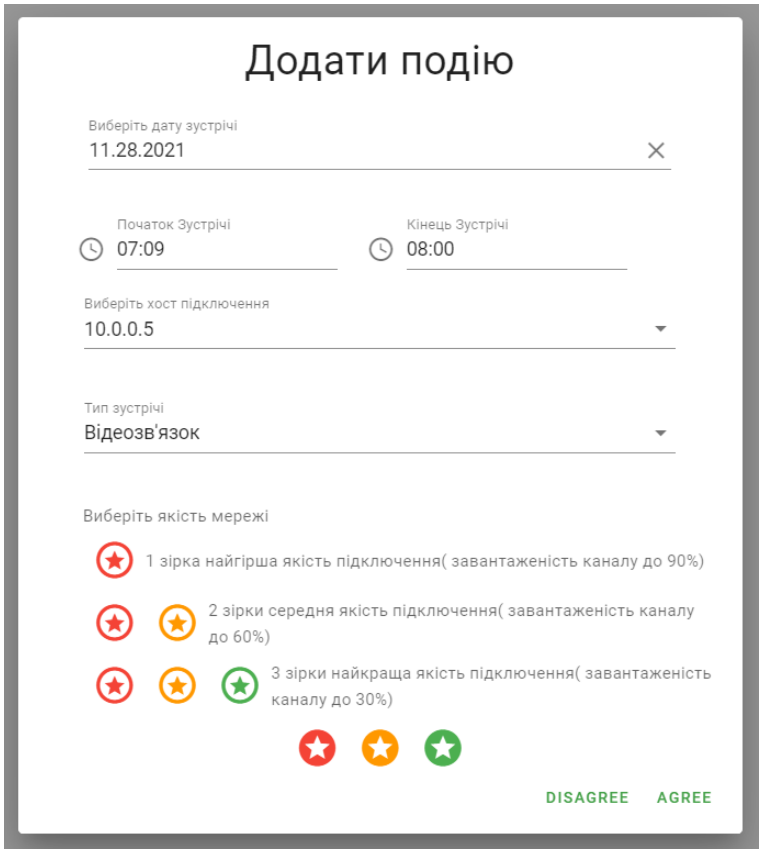


Рис.3.47. Модальне вікно додавання інтенції на стороні користувача (інтерфейс українською мовою)

Рис.3.48. Деякі дані, які перетворює розроблений IBN контролер в код зрозумілий для SDN мережі для створення шляху

В даному IBN-контролері реалізована якість обслуговування, на яку впливають різні фактори. Концепція полягає в тому, щоб створити такий контролер, який дасть змогу реалізовувати потреби користувача в залежності до його вимог у тому числі для організації каналу спецзв'язку. Наприклад, організатором спеціального зв'язку потрібно виділити канал для текстової переписки чи для відеоконференц зв'язку, для цього йому не потрібно окремо виділений канал зв'язку, оскільки таке з'єднання використовує не так багато ресурсів мережі, тому пропонується три види якості обслуговування: найгірша, середня та найкраща якість обслуговування. Якщо ж користувачу потрібна найкраща якість, користувач вибравши в контролері тип якості, наддасть контролеру інформацію про те, що мережа має забезпечити найвищу якість зв'язку. Контролер в реальному часі буде відслідковувати завантаженість мережі, яка буде сконфігурована в час початку зустрічі, якщо завантаженість

буде сягати більше 30% від загальної завантаженості то контролер розвантажить шлях для того, щоб забезпечити потрібну якість зв’язку, змінивши шляхи для тих користувачів у яких вибрана якість обслуговування є нижчою, тобто, якщо користувач підключений до шляху в якому присутній інший користувач і у нього якість зв’язку є нижчою то контролер при збільшені навантаження буде змінювати шлях для того користувача з нищим пріоритетом. У даному експерименті буде досліджено розроблюваний IBN-контролер, за умови, що будуть створені дві події, які будуть розміщені на одному шляху. Одна подія буде основною для якої буде створюватись найкраща якість спец зв'язку, Друга подія буде створюватись для того, щоб штучно навантажити шлях за допомогою Iperf (рис.3.49).

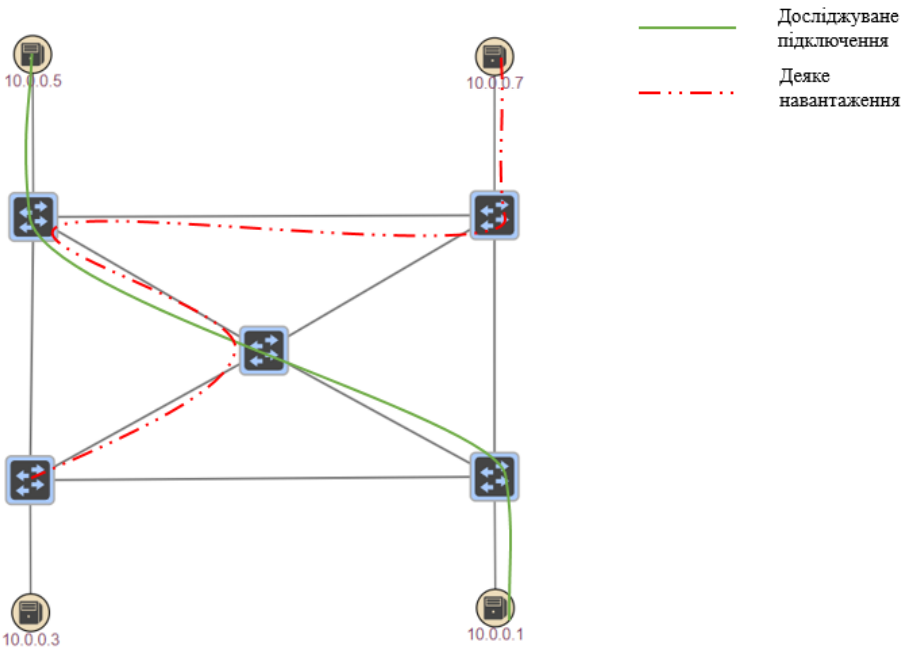


Рис.3.49. Досліджувані шляхи мережі Mininet

Створюємо подію з найвищою якістю підключення для хостів h1 та h5. Заповнюємо всі поля та натискаємо «Agree» (рис.3.50) після чого перевіряємо список усіх створених інтенцій у розроблюваному контролері в меню **Calendar** (рис.3.50).

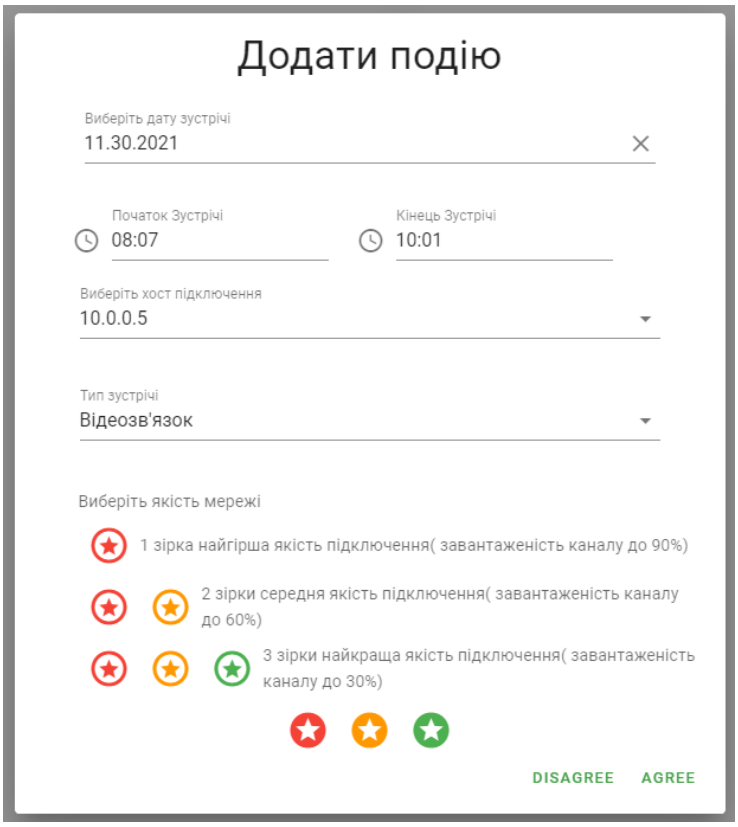


Рис.3.50. Створення експериментальної події

Рис.3.51. Відображення створеного наміру та відображення завантаженості

Оскільки даний контролер буде працювати окремо для кожних користувачів, задля простоти проведення експериментів із завантаженістю мережі було зроблено так, що коли додаєш подію для будь-якого хоста, автоматично додається подія для двох інших хостів (рис.3.52). У нашому випадку вибрано підключення хоста h1 та h5, то для хостів h3 та h7 будуть також створені події зі спільним шляхом (рис.3.52).

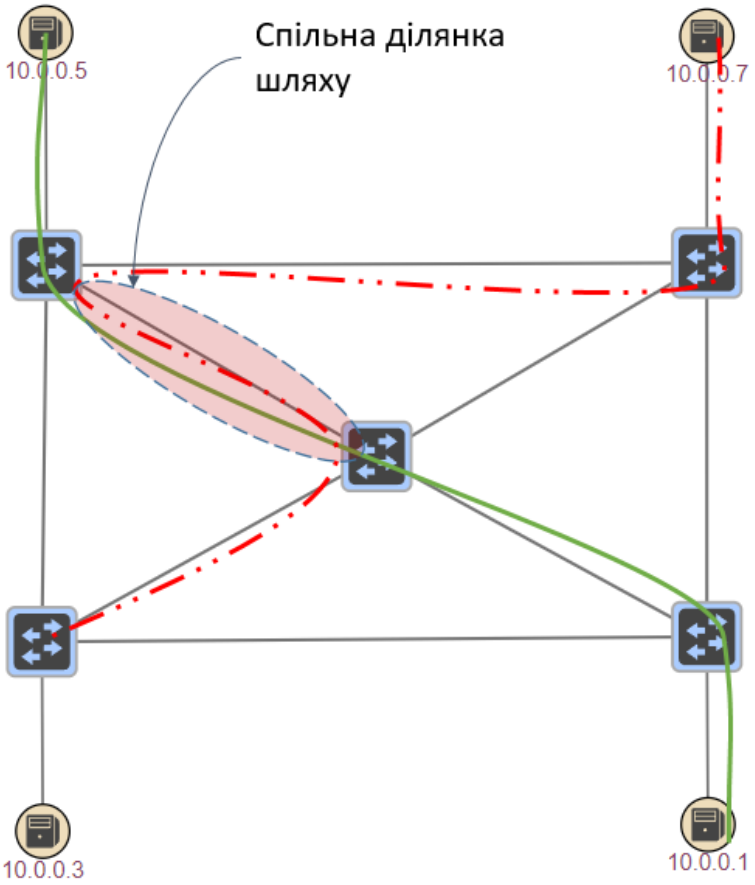


Рис.3.52. Ілюстрація ділянки мережі із спільним шляхом

```
mininet> h3 ping h7
PING 10.0.0.7 (10.0.0.7) 56(84) bytes of data.
64 bytes from 10.0.0.7: icmp_seq=1 ttl=64 time=0.667 ms
64 bytes from 10.0.0.7: icmp_seq=2 ttl=64 time=0.047 ms
64 bytes from 10.0.0.7: icmp_seq=3 ttl=64 time=0.055 ms
64 bytes from 10.0.0.7: icmp_seq=4 ttl=64 time=0.047 ms
^C
--- 10.0.0.7 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.047/0.204/0.667/0.267 ms
```

Рис.3.53. Підключення h3 до h7

Як бачимо із рисунка 3.50, створена подія відображається, тому можемо переходити до тестування навантаження мережі.

Для того, щоб створити завантаженість трафіку між хостами h1 та h5 використано Iperf який буде генерувати трафік відео зустрічі в 5Мб/с. Також для хоста h3 та h7 буже використано Iperf із завантаження мережі в 95Мб/с (Максимальна завантаженість створеної топології становить 100Мб/с), що дозволить завантажити мережу на більше ніж 90%.

Відкриваємо Iperf за допомогою команди:

xterm h1 h3 h5 h7

Після чого відкриються термінали кожного з хостів.

Прописуємо команди для генерування трафіку між хостами h1 та h5 (рис.3.54):

На хості h1:

iperf –u –s –p 5566 –I 1 –l190 > result

На хості h5:

iperf –c 10.0.0.1 –p 5566 –l190 –b5m –t 120 –d

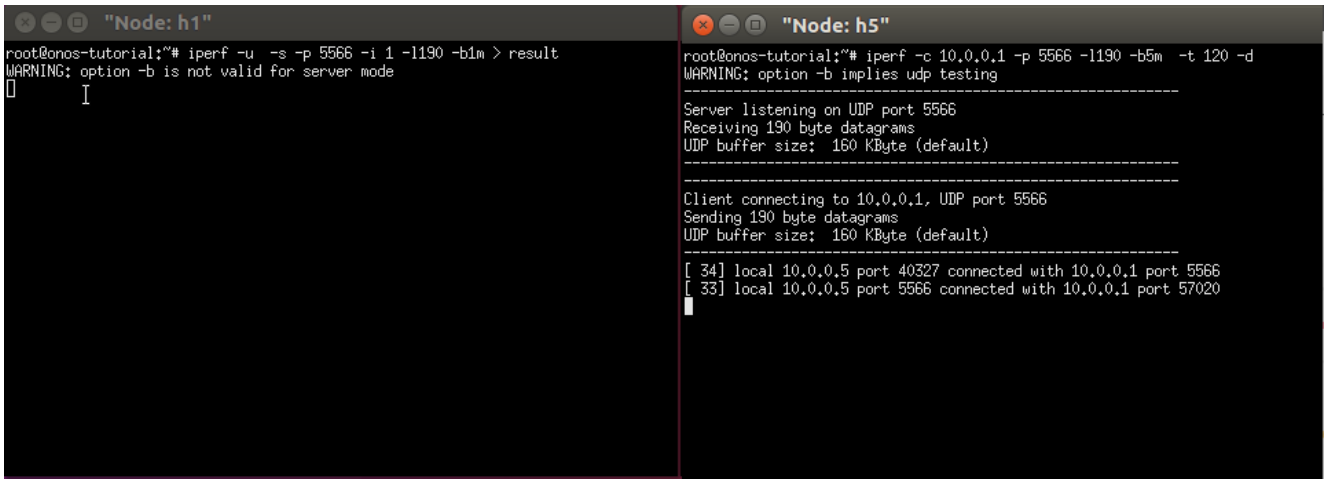


Рис.3.54. Додавання команд в програмі Xterm для хостів h1 та h5

Після того як запустили трафік, в розробленому контролері буде відображатись завантаження мережі на першому графіку (рис. 3.55), що свідчить про те, що iperf працює і подія розпочалась.

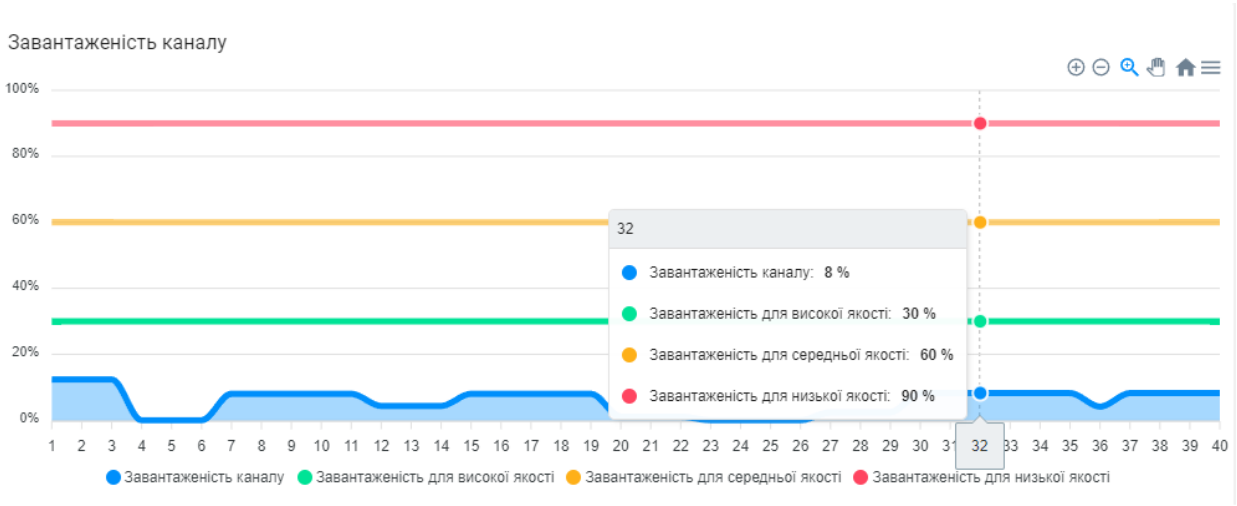


Рис.3.55. Відображення завантаженості каналу при використанні iperf

Для того щоб створити завантаженість h3 та h7 виконуємо наступні команди (рис. 3.56):

На хості h3:

iperf –u –s –p 5566 –I 1

На хості h7:

iperf –c 10.0.0.3 –p 5566 –l190 –b5m –t 120 –d

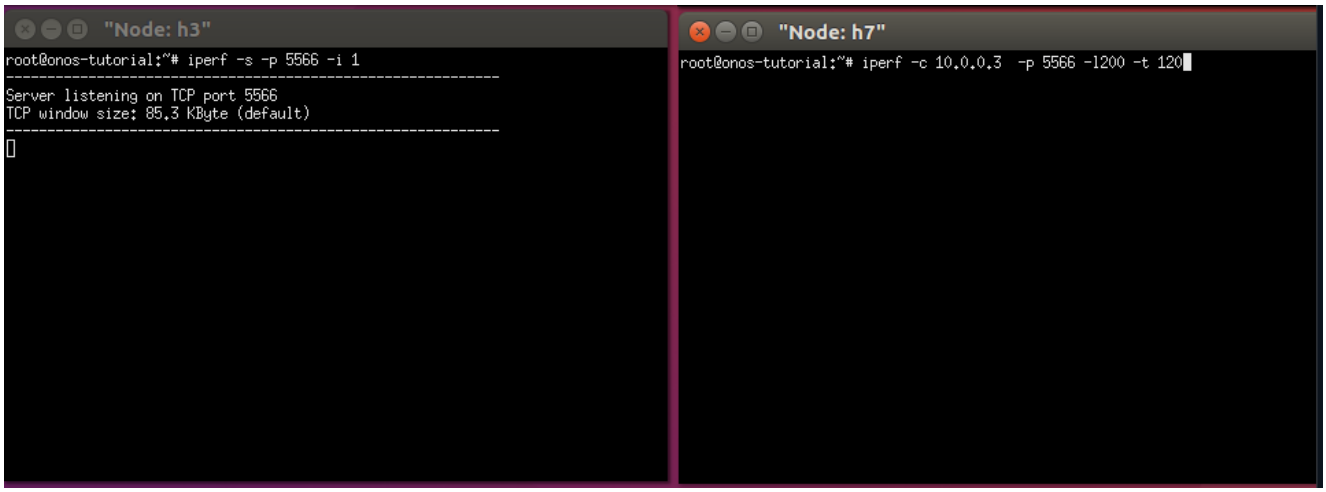


Рис.3.56. Додавання команд в програмі Xterm для хостів h3 та h7

Після додавання команд в мережі буде створено завантаження яке буде відображено на графіку, після чого контролер побачить завантаженість каналу та перенесе цю завантаженість на інший шлях.

На рис.3.57 показано як канал завантажився на 100% після чого контролер змінив інтенції і все завантаження, яке створювалось на даному шляху перенаправилось на інший канал в якому немає підключення, або присутня низька якість зв'язку.

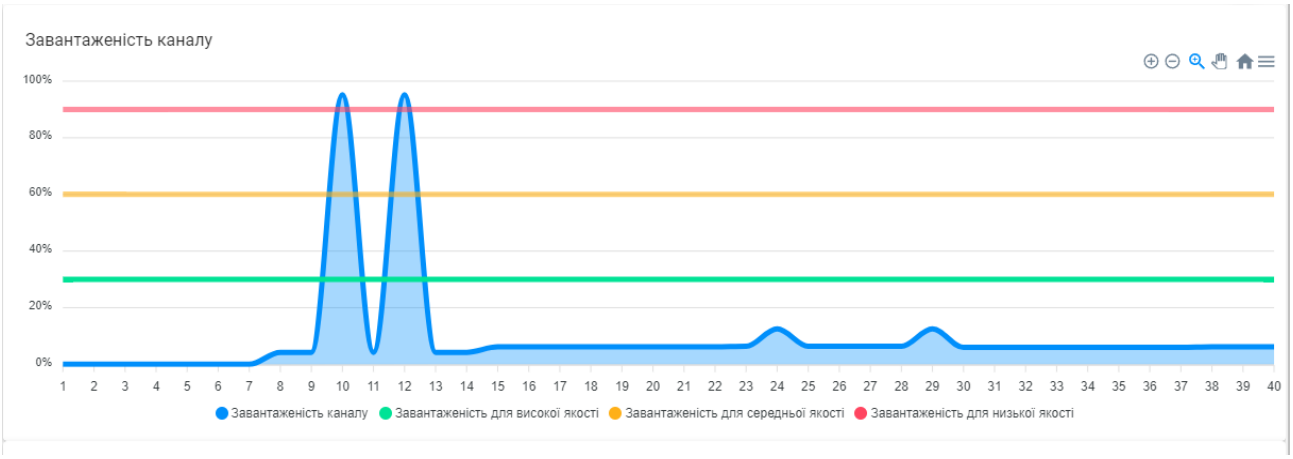


Рис.3.57. Графічне зображення завантаженості каналу

На рис.3.58 зображено топологію після того як контролер зафіксував перевантаження каналу та перенаправив його через інший шлях, який був вільним або відповідав іншим параметрам якості зв’язку.

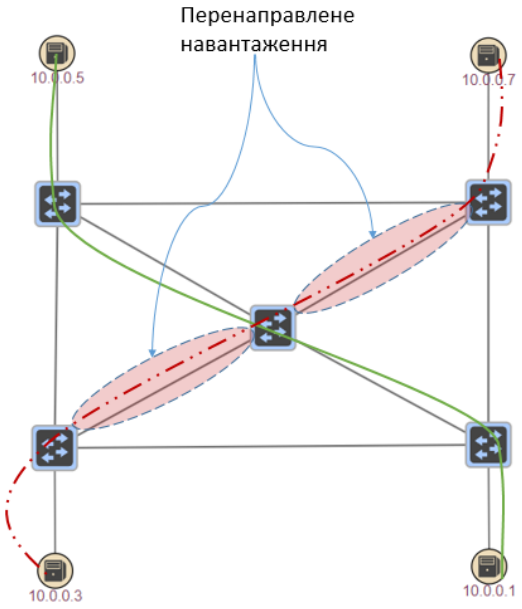


Рис.3.58. Ілюстрація топології після розвантаження

Після зміни інтенцій для даної мережі, вся завантаженість перейшла на інший канал про що свідчить другий графік (рис. 3.59) в меню **Calendar**, на якому зображено 95% завантаженість каналу, тобто така завантаженість яку генерує iperf.

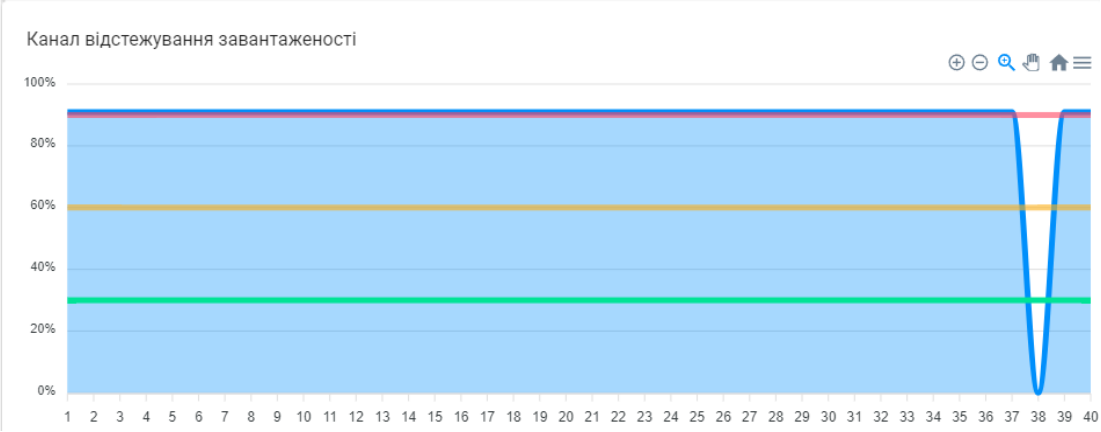


Рис.3.59. Завантаженість яка перейшла на інший шлях

3.5 Розроблення автоматизованої системи відновлення працездатності контролера програмно-конфігурованих інтенційно-орієнтованих мереж

Програмно-конфігуровані інтенційно-орієнтовані мережі (SDIBN) в даний час отримують все більшу популярність. На основі цієї технології можлива побудова як магістральних мереж, так і корпоративних мереж для середнього та малого бізнесу. Актуальним є побудова концепція IoT розумного міста, будинку з використанням SDN рішень. Така ідея дасть змогу гнучко управляти потоками різноманітних датчиків та забезпечувати необхідну якість обслуговування. В таких мережах за виконання всіх інтелектуальних функцій відповідає контролер SDN/IBN - сервер, який керує передачею трафіку крізь комутатори з допомогою протоколу openflow. Існує два варіанти реалізації контролера: при використанні одного фізичного сервера в межах домену мережі і при використанні серверів і їх віртуалізації в хмарному середовищі для підвищення надійності. Таким чином, приймається, що при відмові одного з

серверів контролер SDN не перестає функціонувати і працездатність мережі підприємства не страждає. Для цього у роботі пропонується універсальна автоматизована система моніторингу доступності до серверів різного призначення на одному із яких встановлений SDN/IBN контролер та на іншому IoT брокер (рис.3.60.). Дана система дасть змогу автоматизованого виявити несправності серверів та відновити їх роботу.

Критерієм оцінки готовності серверів є коефіцієнт готовності, який дорівнює частці часу перебування системи в працездатному стані і може інтерпретуватися як вірогідність знаходження системи в працездатному стані. Коефіцієнт готовності обчислюється як відношення середнього часу напрацювання на відмову до суми цієї ж величини і середнього часу відновлення. Системи з високою готовністю називають також відмовостійкими.

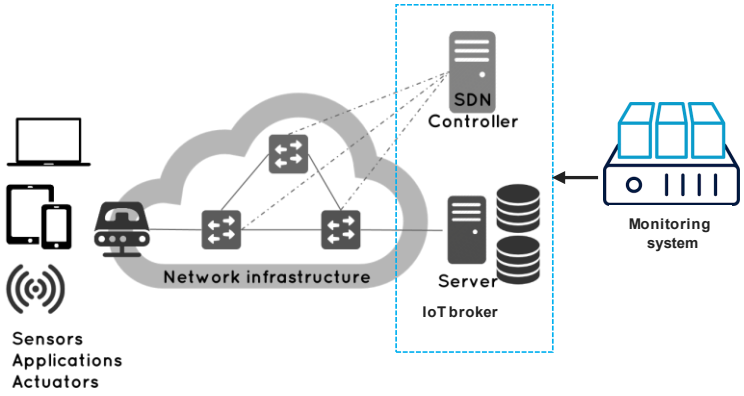


Рис.3.60. Приклад мережі SDN/IBN із автоматизованою системою моніторингу та відновлення працездатності серверних вузлів

У зв'язку з цим з метою організації відмовостійкої роботи всі мережеві елементи, через які проходять такі маршрути, обов'язково повинні бути зарезервовані: повинні бути резервні кабельні лінії, які можуть бути використані у разі виходу з ладу одного з основних кабелів, всі комунікаційні пристрої на магістральних шляхах повинні бути реалізовані за принципом стійкості до відмови схеми. з резервуванням всіх її основних компонентів або для кожного комунікаційного пристрою повинен бути резервований

аналогічний пристрій. Перехід від основного сервера до створеного резервного сервера може здійснюватися як автоматично, так і вручну за участю адміністратора. Звичайно, автоматична міграція підвищує доступність системи, оскільки час простою мережі в цьому випадку буде набагато меншим, ніж при втручанні людини. Процедури автоматичної реконфігурації вимагають наявності в мережі інтелектуальних комунікаційних пристроїв, а також централізованої системи керування, що допомагає пристроям розпізнавати і реагувати на збої в мережі..

Системний моніторинг відіграє невід'ємну роль у життєвому циклі будь-якої комп'ютерної та інфрормаційної мережі. Отже, знання фактичного стану поточної мережі може запобігти серйозній загрозі до того, як вона вразить саму мережу. Належна система моніторингу має охоплювати такі пріоритети: прийнятні швидкості доставки, постійна доступність, профілактичне обслуговування, виявлення вторгнень та моніторинг безпеки. Метою цієї системи було безперервний моніторинг сервера на якому розгорнутий SDN/IBN контролера, і його відновлення після серйозного збою.

Розроблена система моніторингу базується на хмарному сервері AWS (рис.3.61) на основі Jenkins та Docker [131].

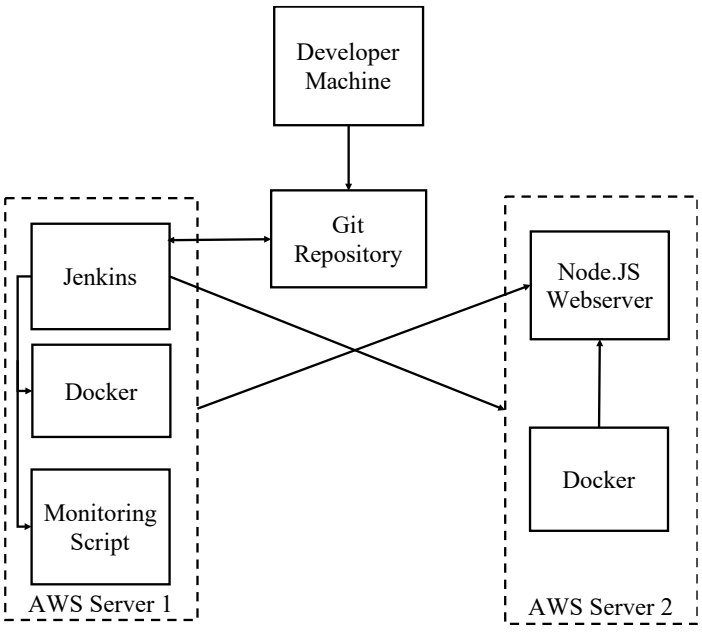


Рис.3.61. Архітектура системи відновлення доступності серверів

Сервер AWS займає місце в системі як хост, на якому встановлені Jenkins і Docker. Система щохвилини перевіряє стан сервера, що відстежується, і виконує дії на основі цієї інформації. Дана система побудована на основі двох Amazon AWS серверів, Git, Git Hub, Docker, Node.Js, Jenkins та bash скрипта власного розроблення. Весь процес можна розподілити на 2 основних частини:

• Моніторинг Git репозиторія на наявність нових змін.

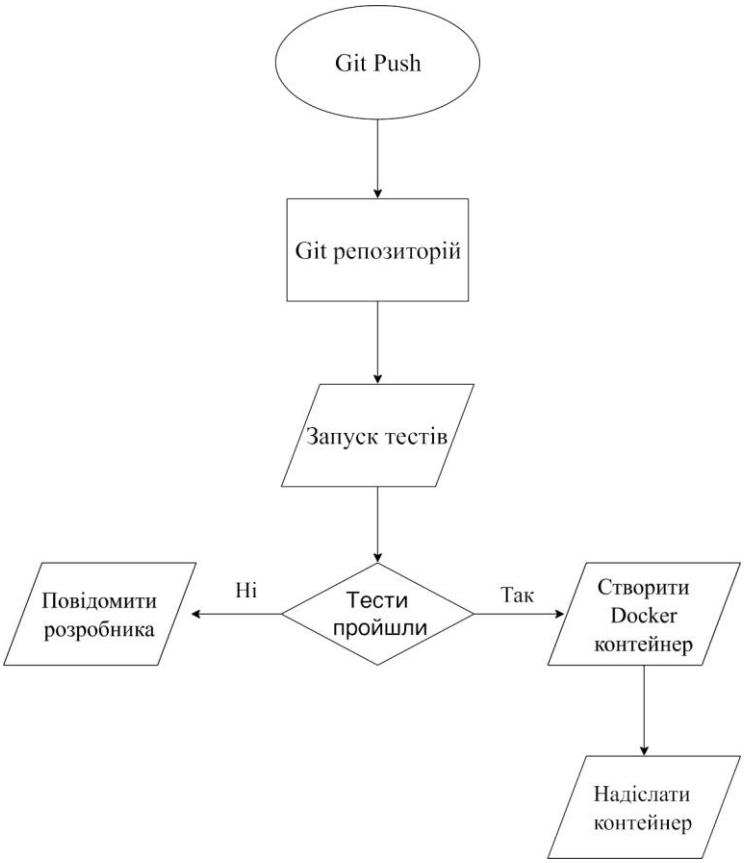


Рис.3.62. Блок схема роботи Jenkins конвеєра

Працює це наступним чином (рис. 3.62): розробник створює функціонал, вносить зміні у віддалений хмарний репозиторій на Git Hub. Конвеєр на основі Jenkins слідкує за змінами у репозиторії, після надходження commit'у автоматично запускаються unit тести. Далі за успішних результатів проходження тестування конвеєр створює docker контейнер та завантажує його в Docker Hub. Якщо тестування пройшло невдало, розробник отримає відповідне повідомлення.

- Моніторинг Node.JS сервера.

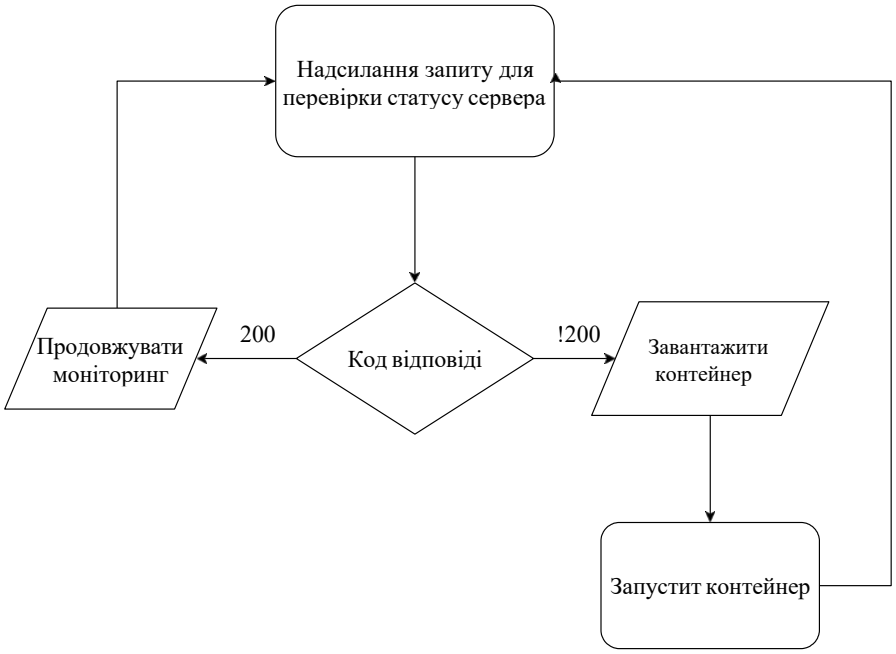


Рис.3.63. Блок схема роботи моніторинга за віддаленим сервером

Паралельно до першого конвеєра працює другий, який повністю відповідає за стан веб сервера (рис.3.63). Кожну хвилину виконується bash скрипт. В свою чергу скрипт посилає HTTP запити та приймає відповіді від сервера, за результатами відповіді відбувається аналізування стану веб сервера. На випадок отримання від сервера статус кода 400+, скрипт виконує додаткових 5 запитів. Якщо сервер працює – скрипт поверне 1, якщо до скрипта 5 разів повертається статус код 400+, скрипт повертає 0. На основі цих даних конвеєр вирішує що робити в подальшому. При 0 виконується команда docker run, котра з docker hub витягує останню версію контейнера та запускає його на сервері.

Перевірка статусу віддаленого сервера грає найважливішу роль в стадії автоматичного розгортання веб сервісів. Моніторинг нашого середовища має вирішальне значення, особливо при розгортанні нової програми. Сьогодні компанії використовують рішення з відкритим кодом для моніторингу системних ресурсів щодня. Існує багато різноманітного програмного забезпечення, яке своїм функціоналом дозволяє відстежувати активність

віддалених серверів, наприклад такі як: Nagios та Cacti. Однак, коли мова йде про моніторинг за певний проміжок часу, немає нічого краще за власно написаний сценарій, який би повністю відповідав заданим вимогам (рис.3.64).

Потрібно було вибрати інструмент, який би ідеально підійшов до системи за декількома чинниками: Нативна підтримка Linux сервером; Простота та надійність; Легкість в обслуговуванні; Відсутність модулів.

За даними параметрами було вибрано bash. Bash - це мова оболонки shell, яка є інтерпретатором команд між інтерфейсом командного рядка та операційними системами. Bash підтримується всіма Linux серверами, не потребує окремих оновлень та загалом постачається разом з системою Linux. Також для роботи з HTTP або HTTPS запитами не потребує встановлення окремих бібліотек чи модулів, адже у bash скрипті дозволяється використання Linux команд. Не дивлячись на свою простоту та легкість bash підтримує усі оператори та функції що й типова мова програмування.

Бібліотека підтримує роботу з протоколами FTP, FTPS, HTTP, HTTPS, TFTP, SCP, SFTP, Telnet, DICT, LDAP, а також POP3, IMAP и SMTP. Вона відмінно підходить для імітації дій користувача на серверах.

```
#!/bin/bash
url='http://35.158.125.187:3000/'
attempts=5
timeout=5
online=false

echo "Checking status of $url."

for (( i=1; i<=$attempts; i++ ))
do
  code=`curl -sL --connect-timeout 20 --max-time 30 -w "%{http_code}\\n" "$url" -o /dev/null`

  echo "Found code $code for $url."

  if [ "$code" = "200" ]; then
    echo "Website $url is online."
    online=true
    break
  else
    echo "Website $url seems to be offline. Waiting $timeout seconds."
  fi
done

if $online; then
  echo "Monitor finished, website is online."
  exit 0
else
  echo "Monitor failed, website seems to be down."
  exit 1
fi
```

Рис.3.64. Bash скрипт моніторингу сервера

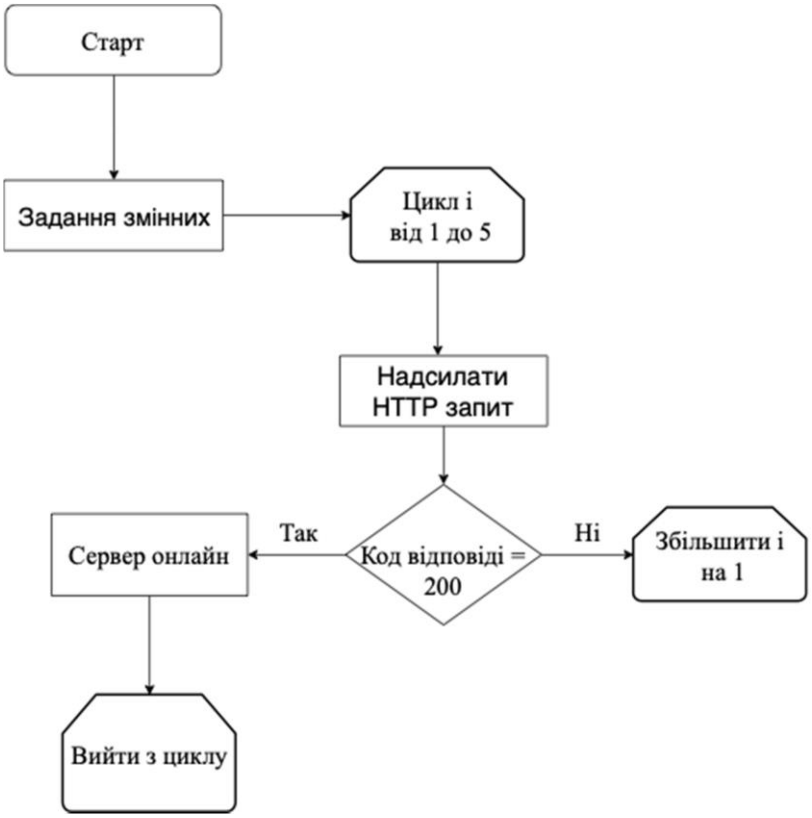


Рис.3.65. Блок схема роботи скрипта моніторинга віддаленого сервера

Після запуску скрипт входить у цикл який повторяється 5 разів (рис.3.65). Під час кожної ітерації виконується команда curl, яка надсилає HTTP GET запит на вказану адресу. У випадку коли код відповіді від сервера дорівнюватиме 200, що значить повноцінне функціонування сервера. Ставимо флаг, online = true, виходимо з циклу. Результатом роботи скрипта повертаємо 0, що означає повне функціонування, подальші дії виконувати не потрібно. У разі коли сервера не відповів кодом 200, цикл продовжує свою роботу. Після його завершення, якщо флаг online не змінився на true, зі скрипта повертаємо 1, що означатиме потрібність виконання подальших дій системою.

Процедура моніторингу розділена на 2 етапи. Щохвилинний сценарій моніторингу виконується. Відразу після цього переходить на 1 етап - перевірка стану сервера. Як ми можемо побачити на знімку екрана, він розділений тегами “MONITORING SCRIPT START/END” (рис.3.66).

Рис.3.66. Процес автоматизованого відновлення доступності сервера

Сценарій виконує кілька запитів до потрібного сервера для визначення його стану. Після завершення виконання сценарію було повернуто остаточний результат. За інформацією, отриманою від моніторингу скрипт, система вирішує свої подальші дії. Якщо сервер працює належним чином, ніяких додаткових дій застосовувати не слід. Якщо система отримала інформацію про несправність серверів, система переходить на 2 етап «Перезапуск невдалої служби» (рис.3.67).

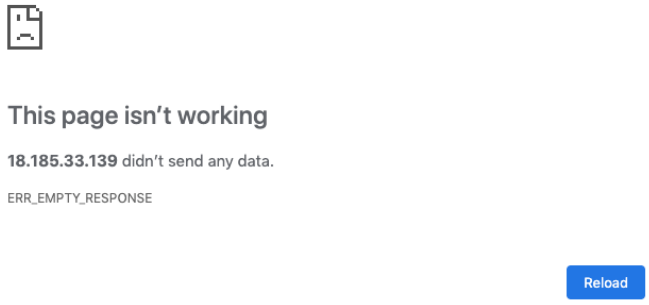


Рис.3.67. Відображення несправності сервера

Наступним чином система прийме автоматичне рішення щодо завантаження і запуску нового контейнера докерів замість недоступного сервера. Результат успішного перезапуску служби ми можемо спостерігати на 2-му скріншоті (рис.3.68).

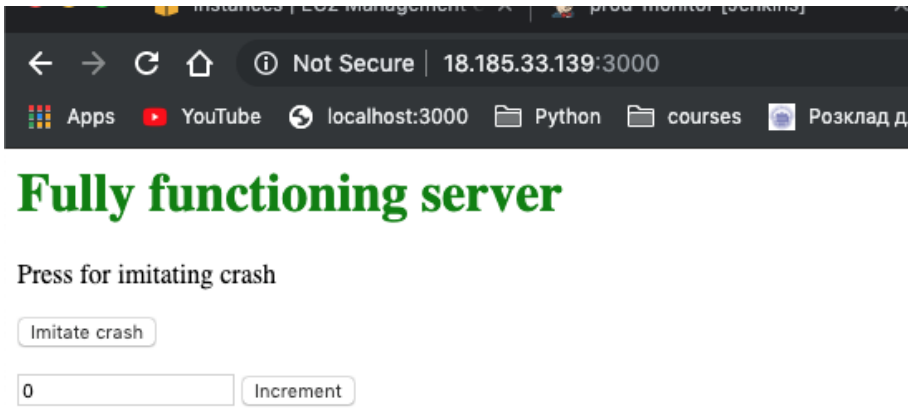


Рис.3.68. Відображення успішного доступу до відновленого сервера [73]

Технологія програмної віртуалізації, така як (Kernel-based Virtual Machine, KVM) забезпечує максимальне використання сервера, даючи змогу кільком віртуальним машинам (ВМ) спільно використовувати ту саму частину обладнання (тобто апаратна віртуалізація). Технологія програмних контейнерів, як Docker, пропонує додаткові переваги в порівнянні з ВМ, так як контейнери, можуть бути запущені та зупинені за набагато менший час, ніж ВМ. Вони характеризуються кращою ізоляція та переносимість програмного забезпечення. Відповідно на практиці розгортання контролерів SDN ONOS доцільно проводити на віртуалізованих серверах на основі контейнерів, що дасть змогу на іншій віртуальній машині запустити надбудово пропонованого IBN контролера. Для моніторингу основних характеристик серверної інфраструктури, або контейнеризованих контролерів пропонується використовувати існуючу систему моніторингу Grafana. Grafana — це потужна і найпопулярніша комбінація з відкритим вихідним кодом, яка поєднує велику гнучкість із бекендом, що забезпечує чудовий моніторинг показників контейнера Docker та і локального середовища в цілому. Відповідно вище

запропонований підхід відновлення доступності серверів легко можна імплементувати як додаткову програмну компоненту до Grafana. Детальніша візуалізація характеристик контролера SDN показана на Рис. 3.69.

Рис. 3.69. Приклад моніторингу характеристик Docker Containers на якому розгорнутий SDN контролер

Панель інструментів Docker Containers показує ключові показники для моніторингу запущених контейнерів:

- Total containers CPU load – завантаження ЦП запущеними контейнерами;
- Memory usage, storage usage – використання памяті;
- Running containers graph - графік запущених контейнерів;
- System load graph – графік завантаження системи;
- IO usage graph – графік використання IO;
- Container CPU usage graph - графік використання ЦП контейнерами;
- Container memory usage graph - графік використання пам’яті контейнерами;

- Container cached memory usage graph - графік використання кеш-пам’яті контейнера;
- Container network inbound usage graph - графік використання вхідної мережі контейнерів;
- Container network outbound usage graph - графік використання вихідної мережі контейнерів.

Таким чином, при плануванні інтенційно-орієнтованої мережі підприємства з серверами контролера SDN/IBN та IoT брокера, використання запропонованої системи дозволяє отримає більш надійну мережу навіть при значних часових проміжках до виявлення відмови за умови відпрацювання механізмів швидкого відновлення серверів.

У роботі розроблено автоматизовану систему відновлення доступності до серверів. Створено систему моніторингу функціонування серверів. Для цього використано наступні інструменти: Jenkins для тестування, створення контейнерів, моніторингу статусу віддаленого сервера, Docker як інструмент для контейнеризації функціонала та два AWS сервера на яких дана система працює. Запропоновано архітектуру мережі IBN для надання сервісів IoT з розробленою системою моніторингу.

Висновки до 3-го розділу

В роботі для майбутніх інтелектуальних мереж розроблено унікальний IBN – контролер який забезпечує клієнтам надійне з’єднання. Це досягається створенням інтенцій в мережі які перетворюють зрозумілий набір команд від користувача в код який розуміє мережа SDN. Контролер забезпечує деякі значення якостей зв’язку в залежності від потреб користувача, або його фінансової можливості. Контролер IBN отримує наміри, які виражають усі види очікувань. Також контролер IBN оснащений політиками та моделями штучного інтелекту (AI), які реалізують можливості, необхідні для аналізу стану системи та пошуку оптимізованих операційних дій на основі спостережень із

керованого середовища. Обробник намірів також повідомляє про виконання та статус своїх намірів. Даний контролер надає велику перевагу та зменшує вплив людини на мережу, що збільшує швидкість реагування. Також контролер можна постійно удосконалювати, та додавати дедалі більше нових і корисних функцій, які можуть розвиватись паралельно розвитку самої мережі.

У роботі запропоновано автоматизовану систему відновлення доступності серверів на яких розгортаються SDN/IBN контролер та IoT брокер. Розроблено архітектуру системи відновлення доступності серверів. Створено систему моніторингу функціонування серверів. Для цього розроблено ряд алгоритмів функціонування, а саме блок схеми роботи Jenkins конвеєра, моніторинга за віддаленим сервером та скрипта моніторинга віддаленого сервера. Передбачається, що також запропонована система дасть змогу в умовах техногенних та природних катастрофах автоматизовано управляти ресурсами, здійснювати діагностику та відновлювати дані серверної інфраструктури з метою забезпечення безперервності роботи і високої доступності бізнес сервісів.

РОЗДІЛ 4. ПРАКТИЧНА РЕАЛІЗАЦІЯ ІНТЕЛЕКТУАЛЬНОЇ МЕРЕЖІ НА ОСНОВІ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ SDN ZODIAC ТА АВТОМАТИЗАЦІЇ РОЗРОБЛЕНИХ МЕТОДІВ УПРАВЛІННЯ ЯКІСТЮ СПРИЙНЯТТЯ ПОСЛУГ

4.1 Побудова структурно-функціональної моделі інтелектуальної програмно-конфігурованої безпровідної мережі

З розвитком Інтернету речей та розумних мобільних пристроїв безпровідна локальна мережа IEEE 802.11 (WLAN) має великий попит у користувачів. Актуальність мережі Wi-Fi постійно вимагає від розробників мережевого обладнання та вчених розвитку методів покращення якості обслуговування (QoS), функцій управління ресурсами та хендовером (HO). Пропрієтарні архітектури WLAN, що існують в даний час, залежать від виробників, роблять інноваційний процес небажаним і є серйозною перешкодою для майбутніх мережевих послуг і додатків. Однією з проблем, що впливають на QoS існуючих WLAN є процес хендовера при керуванні мобільністю. Складність управління перемиканням виникає, коли зони покриття кількох точок доступу перетинаються. У традиційних WLAN процес перемикання зазвичай ґрунтується на показнику рівня сигналу (RSSI) мобільної станції (MS), що може призвести до дисбалансу навантаження. Тим часом під час перемикання MS може підключитися до перевантаженої точки доступу, але з кращим рівнем сигналу. Такі випадки призводять до погіршення параметрів QoS, а саме до зниження пропускної здатності, появи високої затримки, втрати пакетів і в результаті QoE для користувача стає неприйнятним. У передових архітектурах WLAN процедура вибору мережі керується централізованим контролером. Цей контролер збирає інформацію про точки доступу і централізовано надсилає її кожному MS. Для контролера RSSI є ключовим параметром для оцінки розташування кінцевих терміналів та вибору оптимальної точки доступу. На основі аналізу відомих робіт сформовано обмеження існуючих рішень

хендовера. А саме, недостатня обізнаність контролера про вимоги кінцевого користувача QoE, відсутність багатокритеріального параметра для хендовера та методів моніторингу ключових параметрів продуктивності (Quality of service, QoS) мережі в реальному часі. Управління мережею та інтелектуальний хендовер стають все більш складними та ресурсомісткими у швидко розвиваючих корпоративних середовищах Wi-Fi.

Хоча існуючі програмно-конфігуровані мережі (SDN) автоматизували більшість процесів управління мережею, вони вимагають ручної участі кваліфікованих мережевих адміністраторів. Але людська участь є повільною, непостійною і часто дорогою. Поява мереж на основі намірів (IBN) вирішує вищезгадані проблеми, забезпечуючи швидке та автономне управління. IBN це концепція інтелектуального управління мережею, яка поєднує SDN, штучний інтелект (AI), ML та мережеве оркестрування для автоматизації адміністративних функцій. Ці мережі є такими, що самокоректуються і самоналаштовуються на основі намірів користувача. Намір – це бізнес-мета, яку користувачі хотіли б досягти за допомогою мережі. Мережа, що базується на намірах, повністю відрізняється від того, як мережеві адміністратори управляють мережами сьогодні. Користувачі задають свої наміри, а мережа перетворює в дії. Ця ідея не нова, але в міру того, як автоматизація управління мережею стає більш поширеною, IBN все ще розглядається як рання технологія. В даний час у IBN відсутні механізми для інтелектуального управління хендовером у безпровідних мережах, спрямовані на підвищення або задоволення замовленого QoE рівня користувачів.

Саме тому у роботі запропоновано структурно-функціональну модель інтелектуальної мережі, що базується на SDN та намірах користувачів щодо управління якістю сприйняття послуг. Пропонована архітектура так званої інтенційно-орієнтованої програмно-конфігурованої безпровідної мережі (Intent-based software-defined wireless network, IBSDWN) показана на рис. 4.1.

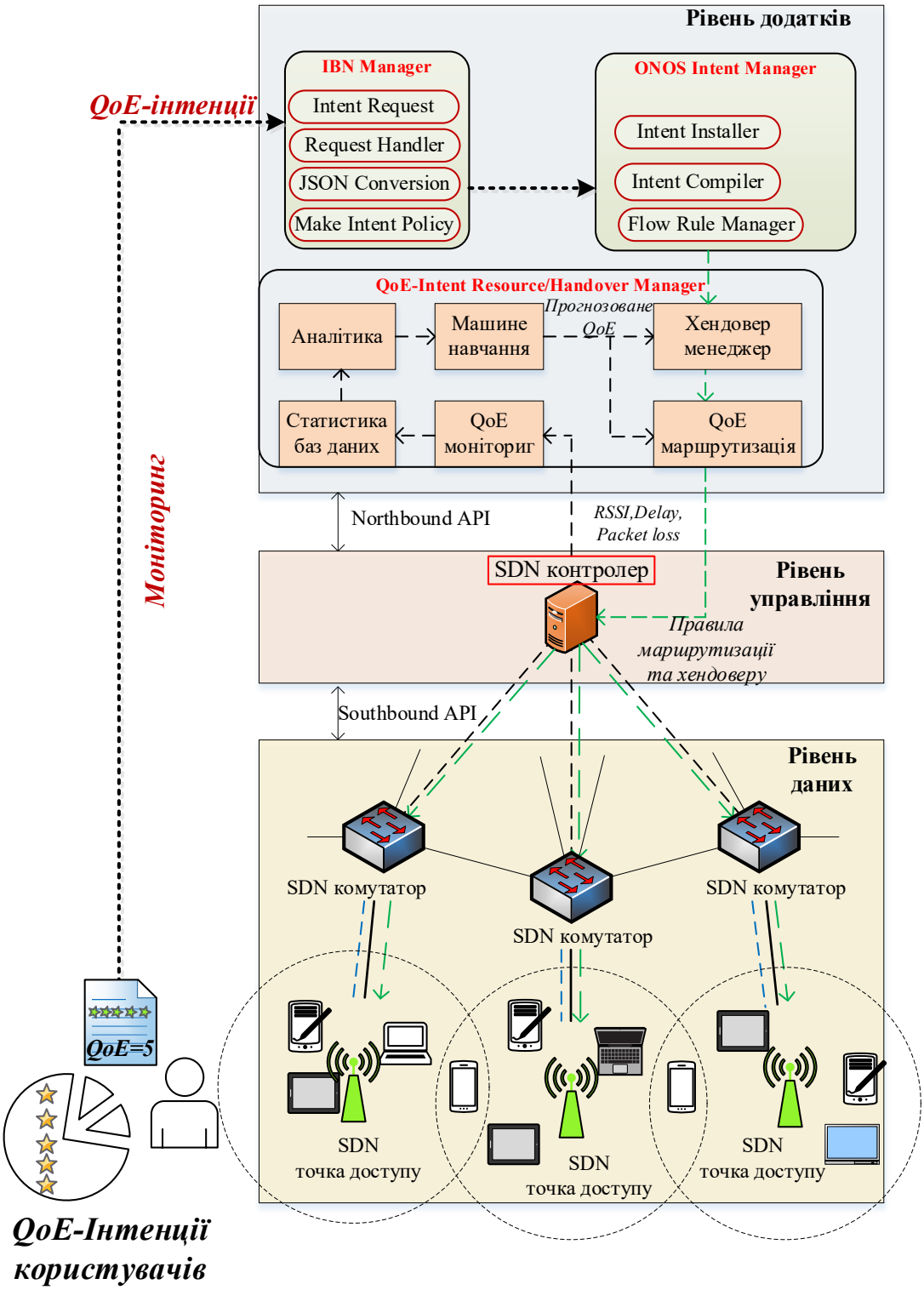


Рис.4.1. Запропонована, IBSDWN архітектура з інтегрованими новими структурно-функціональними модулями на рівні логіки контролера: “QoE маршрутизація”, “моніторинг QoE на основі машинного навчання” та “QoE менеджера хендоверу” [132]

Загалом пропонована архітектура складається з 3 рівнів. Площина даних або інфраструктурний рівень, де розташовані мережні пристрої. Площина керування, де контролер SDN/IBN управляє процесами у мережі, використовуючи протокол OpenFlow. Прикладна площина - це набір програм, орієнтованих на дотримання вимог бізнес-політики, які забезпечують функції управління мережею (балансування навантаження, моніторинг трафіку, хендовер тощо.). Контролер управляє всіма точками доступу, тим самим полегшуючи виконання НО. Більш того, централізована природа IBSDWN дозволяє контролеру отримати глобальне уявлення про мережу за допомогою інтелектуального моніторингу та вимірювань, які підтримуватимуть процес НО.

Відповідно до запропонованої концепції інтелектуальної IBSDWN, користувачі можуть зробити запит рівня QoE для конкретної послуги, яку мережа розуміє як намір. Наміри QoE формуються у вигляді простих зірочок або числового значення від 1 до 5. Чим вищий рівень наміру, тим краща якість послуги буде надано. Зокрема, цей підхід є цікавим для важливих бізнес-користувачів. Потім, використовуючи задані знання про QoE або інтелектуальний механізм самонавчання, виділяються відповідні ресурси, що автоматично перетворюються на команди конфігурації мережного обладнання та інтерфейсні операції.

Наміри QoE збираються та аналізуються на прикладному рівні розробленим IBN менеджером. Контролер ONOS взаємодіє з IBN Manager лише на рівні управління через Nortbound API. Модуль менеджера намірів контролера ONOS отримує запит від IBN Manager у форматі JSON і після компіляції перетворює його на низькорівневу команду, яка виконується на комутаторах та точках доступу. Після цього він відправляє намір (у формі JSON) модулю конфігурації ядра ONOS для розгортання. Розроблений графічний інтерфейс програми встановлення намірів пов'язується з модулем менеджера правил потоку для запису наміру, створеного для відповідного вузла

після успішного встановлення. Менеджер IBN зв'язується з менеджером ресурсів, щоб оцінити стан мережі та переконфігурувати її, коли намір QoE не забезпечується. Під реконфігурацією ми маємо на увазі зміну правил маршрутизації та вибір точки доступу. Зокрема, ідея полягає в тому, щоб знайти оптимальний шлях та точку доступу, через які буде забезпечено необхідний рівень QoE. У роботі називатимемо такий хендовер QoE-HO. Нижче докладно пояснимо, як працює пропонована QoE-HO.

Особливостями запропонованої архітектури IBSDWN є розроблені та інтегровані програмні модулі, що працюють на рівні додатків:

- Модуль “Моніторинг QoE” забезпечує вимірювання параметрів каналів зв’язку (затримка, втрати пакетів, пропускна здатність, RSSI) та оцінювання якості сприйняття користувача згідно виміряних параметрів [132].
- Модуль “База даних” представляє собою базу даних в якій зберігається параметри каналів зв’яку на відповідних ділянках мережі.
- Модуль “Менеджер хендоверу” приймає рішення про необхідності перемикання користувача, згідно виміряних параметрів та передбаченого рівня QoE на певній ділянці мережі.
- Модуль "Машинне навчання" на основі отриманих статистичних даних навчає алгоритм та передбачає оцінку QoE.
- Модуль “QoE маршрутизація” забезпечує зміну правил маршрутизації згідно вказівки “HandOver Manager” [132].

4.2 Розробка та дослідження методу ініціації хендовера в інтелектуальній IBSDWN на основі показника якості сприйняття послуг

В роботі досліджуються результати для 3-ох методів ініціації хендоверу: класичного HO, покращеного HO та пропонованого адаптивного HO.

Класичний HO

Як було раніше сказано, у класичному випадку, процедура хендоверу приймає до уваги параметр потужності сигналу як основний критерій для

прийняття рішення про підключення абонента до тієї чи іншої точки доступу. В такому випадку ігноруються важливі параметри мережі: затримка, втрати пакетів, джитер і т.д.

При ініціалізації мережі користувач автоматично підключається до точки доступу AP1, з найкращою потужністю сигналу. Контролер прокладає найкоротший шлях між користувачем та медіа сервером та встановлює правила OF для передачі даних. Згідно дерева шляхів, зображеного на рис. 4.6, для досліджуваної мережі, у випадку AP1: найкоротшим шляхом є AP1-S1-S3-Медіасервер.

Покращений QoE-HO

У випадку покращеного HO, спершу користувач автоматично підключиться до точки доступу з найкращим рівнем потужності. Після цього контролер визначить рівень QoE та порівняє з пороговим значенням. Якщо рівень QoE більший або рівний пороговому значенню, контролер прокладає найкоротший шлях між користувачем та медіа сервером та встановлює правила OF для передачі даних. В іншому випадку контролер порівняє значення рівня QoE для найкоротшого шляху точки доступу AP1: AP1-S1-S3-Медіасервер та AP2: AP2-S5-S3-Медіасервер. Якщо з врахуванням рівня потужності AP2 та оцінки рівня QoE для найкоротшого шляху точки доступу AP2, кінцеве значення рівня QoE переважатиме порогове значення, контролер прийме рішення про ініціалізацію процесу HO.

Адптивний QoE- HO

Даний метод доповнює попередній, можливістю вибору шляху маршрутизації враховуючи QoS метрики, не зважаючи на довжину шляху, (рис.4.6Б). Тобто, враховуючи приклад попереднього методу, контролер визначатиме рівень QoE для всіх доступних шляхів точки доступу. Та в процесі передачі даних зможе динамічно змінювати шлях підтримуючи необхідний рівень QoE.

Загалом, функція прийняття рішень щодо адаптивного QoE-хендовера базується як на функції вартості, так і на функції корисності. Зазвичай така стратегія включає суму зваженої функції деяких параметрів: RSSI, пропускної здатності, втрати пакетів та затримок в мережі Wi-Fi. Загальна формула вартісної функції QoE-хендовера для безпровідної мережі визначається як:

$$f_n(HO_{QoE_{1-5}}) = \sum_S \sum_i w_{S,i} \cdot p^{n_{s,i}} \tag{4.1}$$

У формулі 4.1 $p^{n_{s,i}}$ — це вартість і-го параметра для надання послуги S в мережі n з необхідним рівнем QoE, $w_{S,i}$ — вага (важливість), призначена за допомогою і-го параметра для надання послуг.

Канал зв'язку з найбільшою вартістю вибирається як оптимальний варіант для підключення. Таким чином, ця модель політики, заснована на функції витрат, оцінює динамічні умови мережі та включає період стабільності (період очікування перед хендоверами), щоб гарантувати, що передача обслуговування є доцільною для кожної STA.

Нормоване значення інтегрального адитивного критерію якості, що визначається за формулою (4.2) [132]:

$$Q = QoS(X) = 1 - (w_1(\frac{P_{min}}{P}) + w_2(\frac{D_{min}}{D}) + w_3(\frac{T}{T_{max}}) + w_4(\frac{RSSI}{RSSI_{max}})), \tag{4.2}$$

де w_1, w_2, w_3, w_3 змінюється в діапазоні від 0 до 1.

Математична модель співвідношення QoS/QoE для відеопослуги була представлена в [132], а саме:

$$QoE_{video} = f_v(Q) = 5(1 - Q^2)^{15Q^5}. \tag{4.3}$$

Дослідження з практичної інтеграції розроблених модулів проводилось у віртуальній мережі SDN з підтримкою технології Wi-Fi. Для побудови мережі використано емулятор Mininet Wi-Fi. Який дозволяє розгорнути реалістичну віртуальну програмно-конфігуровану мережу на одній машині за декілька секунд. Враховуючи активну розробку та підтримку проекту, на ємульованих мережах можна розробляти та тестувати нові технології і кінцевий результат не

відрізнятиметься від реалізації на фізичних мережах. В ролі SDN контролера обрано ONOS, як один з лідируючих opensource SDN контролерів. Який також активно підтримується розробниками та доповнюється підтримкою передових технологій в сфері програмно-конфігурованих мереж та віртуалізації мережевих функцій. Поверх контролера ONOS розгорнуто розроблений унікальний IBN контролер з підтримкою IBN менеджера.

Рис.4.2 відображає процеси, що відбуваються для реалізації запропонованого адаптивного QoE-орієнтованого хендовера та типи повідомлення, якими обмінюються об'єкти в запропонованій IBSDWN архітектурі.

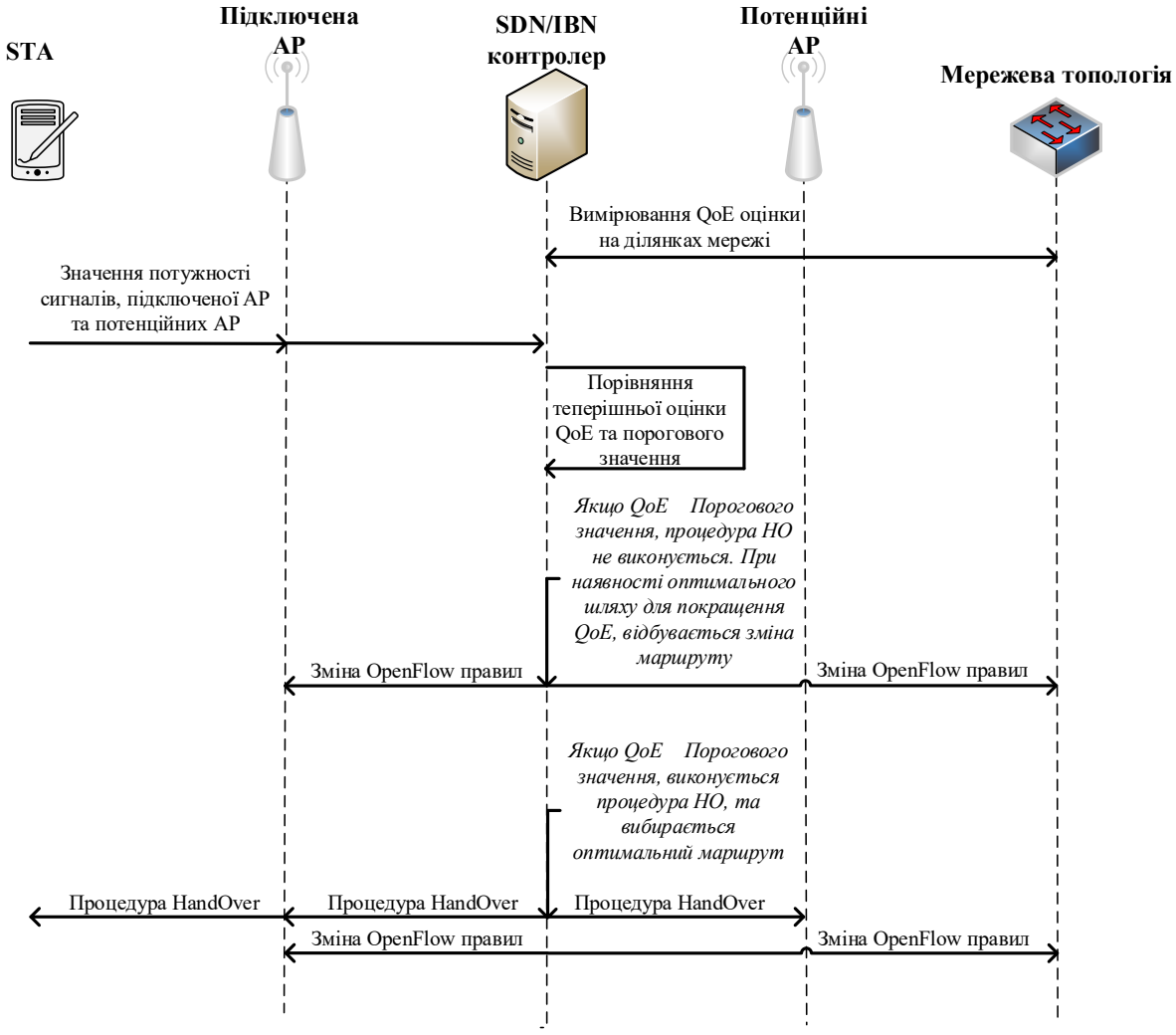


Рис.4.2. Метод ініціації хендовера в SDWN на основі показника QoE [133]

- STA інформують систему про поточний статус свого з'єднання, вимірюючи значення рівня сигналу, і періодично надсилатимуть їх через точки доступу до контролера мережі.
- Контролер оцінить поточний стан точки доступу та чи відповідає вона вимогам QoE STA чи ні. Зокрема, якщо поточна точка доступу не відповідає вимогам, контролер реалізовуватиме правила, щодо адаптивної маршрутизації, які будуть пояснені в наступному кроці, щоб вибрати оптимальну AP.
- Контролер надішле рішення через повідомлення про перемикання та підтвердження нового хендовера.
- Поточна точка доступу надішле сигнал перемикання підтвердження до STA та повідомлення про підтвердження HO.
- STA надішле запит асоціації цільовій точці доступу, який повториться з повідомленням про прийняття як підтвердження HO.

В практичній реалізації дослідження з порівнянням рівня якості сприйняття у випадках класичного хендоверу та з впровадженням HandOver Manager для відеопотоку. Параметри мережі, були згенеровані, для Latency – 0,001-0,015 сек, Packet Loss – 0,25-5%, та записані в python скріпт (Рис.4.3). Кожні 5 секунд відбувалась зміна параметрів згідно згенерованих даних.

```
def cDelay1():

        s1.cmdPrint('ethtool -K s1-eth0 gro off')
        s1.cmdPrint('tc qdisc del dev s1-eth0 root')
        s1.cmdPrint('tc qdisc add dev s1-eth0 root handle 10: netem delay 100ms')


    t=Timer(5.0, cDelay1)
    t.start()
```

Рис.4.3. Приклад функції для динамічної зміни затримки в каналі зв'язку

Отож, в емуляторі Mininet побудована топологія мережі, зображена на рис.4.4. Складається мережа з 5 SDN комутаторів, 2 точок доступу, 1 хоста, 1 медіа-серверу та SDN контролера.

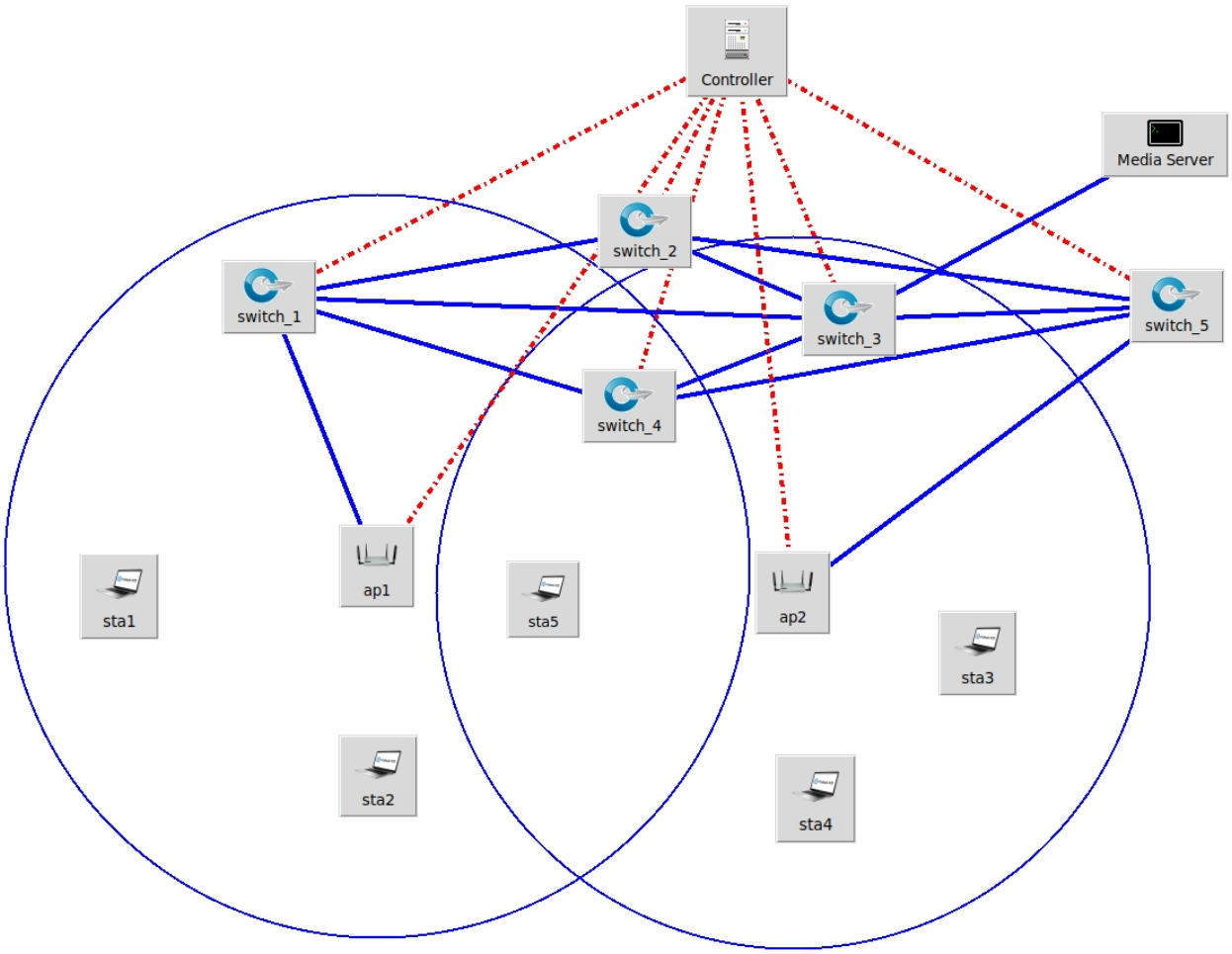


Рис.4.4. Топологія досліджуваної програмно-конфігурованої безпровідної мережі в середовищі Mininet [132]

```
File  Edit  View  Search  Terminal  Help
Packets: 524
Total delay is 8 ms
Total loss is 1%
RSSI AP1 is -51 dBm
RSSI AP2 is -66 dBm
QoE is 4.0
--------------------------------------------------------------------------------
Packets: 573
Total delay is 11 ms
Total loss is 0.2%
RSSI AP1 is -52 dBm
RSSI AP2 is -65 dBm
QoE is 4.7
--------------------------------------------------------------------------------
Packets: 552
Total delay is 9 ms
Total loss is 0.3%
RSSI AP1 is -54dBm
RSSI AP2 is -62dBm
QoE is 4.6
```

Рис.4.5. Процес вимірювання параметрів та визначення оцінки QoE контролером

Канал зв’язку з найбільшою вартістю вибирається як оптимальний варіант для підключення. Таким чином, ця модель політики, заснована на функції витрат, оцінює динамічні умови мережі та включає період стабільності (період очікування перед хендоверами), щоб гарантувати, що передача обслуговування є доцільною для кожної STA.

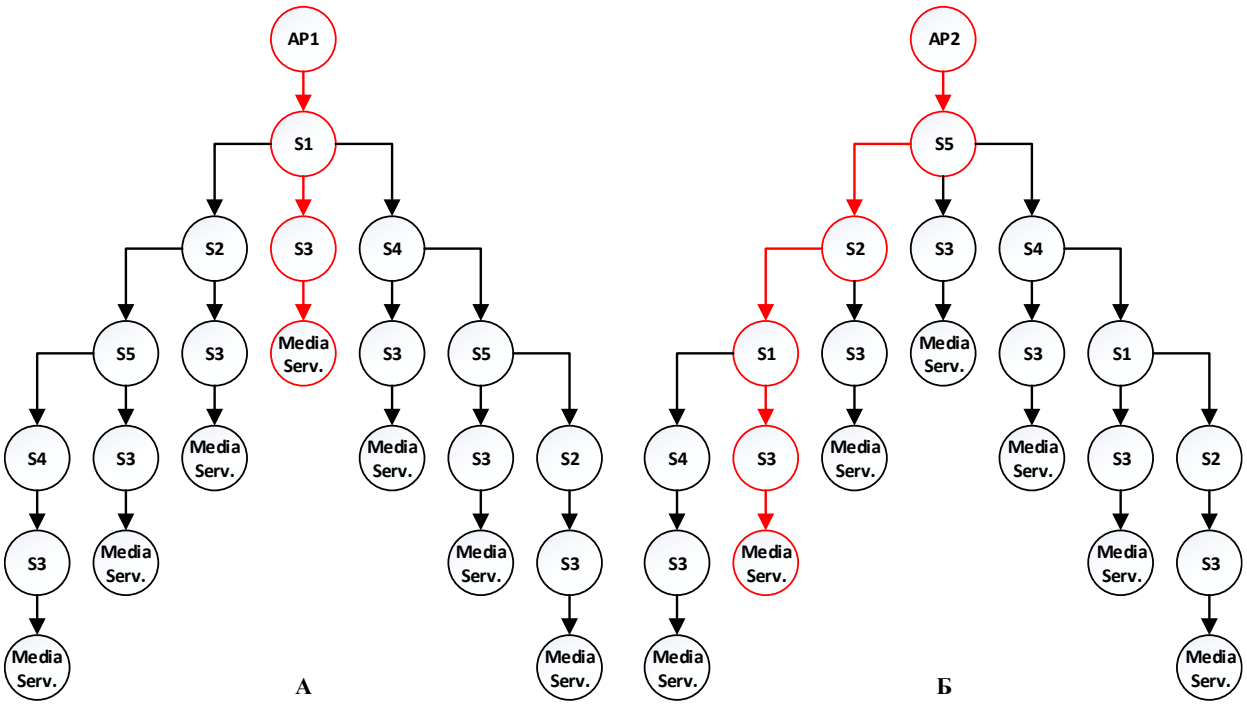


Рис.4.6. Дерево шляхів для досліджуваної топології, де а) доступні шляхи для AP1 та б) для AP2 [132]

На рис. 4.7, графічно зображено результати, отримані вище, для порівняння отриманого рівня QoE при класичному HO, покращеного HO та адаптивного HO.

З отриманих результатів видно, що у випадку класичного HO до 25 секунди точка доступу AP1 та вибраний найкоротший шлях рис.4.6а) забезпечував необхідний рівень QoE. Проте, на 30 секунді дослідження рівень QoE почав деградувати внаслідок внесених змін створеним скриптом, що симулювало завантажені точки доступу та каналів зв’язку найкоротшого маршруту. Рівень знизився до 3,5, що є нижчим ніж встановлений пороговий рівень. Впродовж дослідження контролер не проводив жодних змін та спроб

для покращення ситуації, так як точка доступу AP2 мала меншу потужність сигналу.

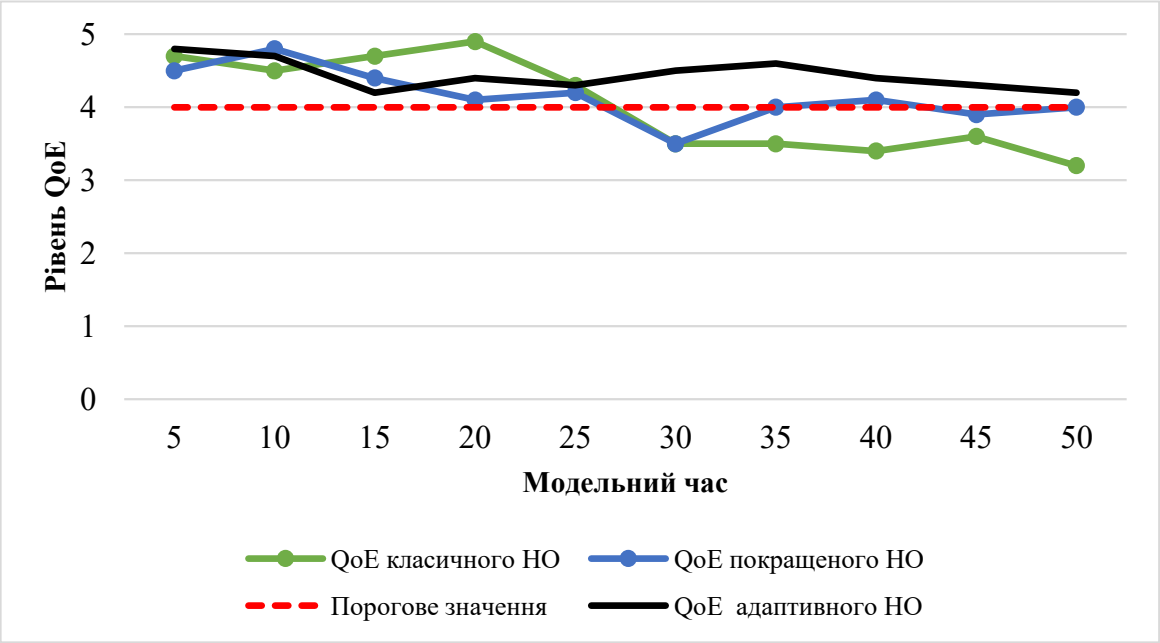


Рис.4.7. Оцінка ефективності запропонованого методу ініціації хендоверу за критерієм QoE [133]

У випадку з покращеним НО до 25 секунди, забезпечувався заданий пороговий рівень якості сприйняття, але на 30 секунді, після погіршення параметрів мережі контролер прийняв рішення про виконання процедури хендоверу до точки AP2 з найкоротшим шляхом до медіасерверу. Таке рішення забезпечило відновлення рівня якості сприйняття до порогового значення впродовж всього дослідження.

У випадку з адаптивним НО на 25 секунді при зміні параметрів каналів зв'язку відбулась процедура НО до точки доступу AP2 та вибором шляху передачі даних як зображено на рис.4.6 Б. Також між 35 та 45 секундою, що дві секунди змінювались параметри каналів зв'язку мережі, в результаті чого контролер приймав рішення про динамічну зміну маршрутів передачі даних та процедури НО використовуючи обидві точки доступу.

Згідно з отриманими результатами запропонований метод швидко реагує на раптову деградацію в мережі та забезпечує необхідну якість обслуговування кінцевого користувача STA5.

Однак недоліком даного методу є надмірність службових даних системи моніторингу в каналах зв'язку між мережевим обладнанням та контролером, відповідно збільшується навантаження на контролер та мережеве обладнання. Ця проблема може бути вирішена шляхом скорочення інтервалів вимірювання продуктивності каналу зв'язку та інтеграції ML модуля для прогнозування QoE.

На рис. 4.8. показано структурно-алгоритмічну схему прогнозування рівня задоволеності користувача за QoE оцінкою та визначення моменту реконфігурації мережі IBN і активації методу QoE-HO.

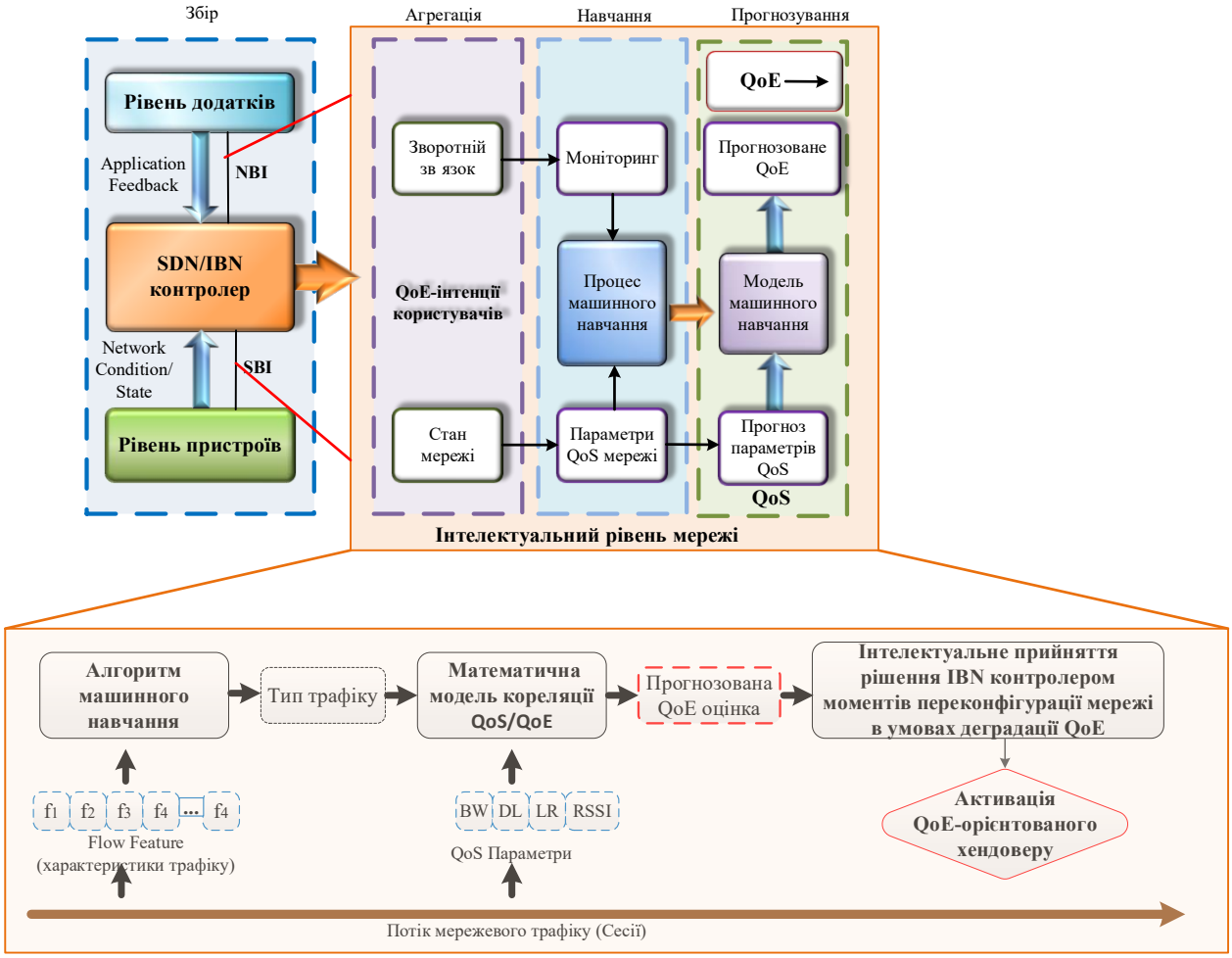


Рис. 4.8. Структурно-алгоритмічна схема функціонування інтелектуального рівня мережі для підвищення якості сприйняття послуг [132]

Інтелектуальна QoE-система моніторингу нормованого користувальницького критерію QoE відповідно до запропонованого алгоритму показана на рис. 4.9.

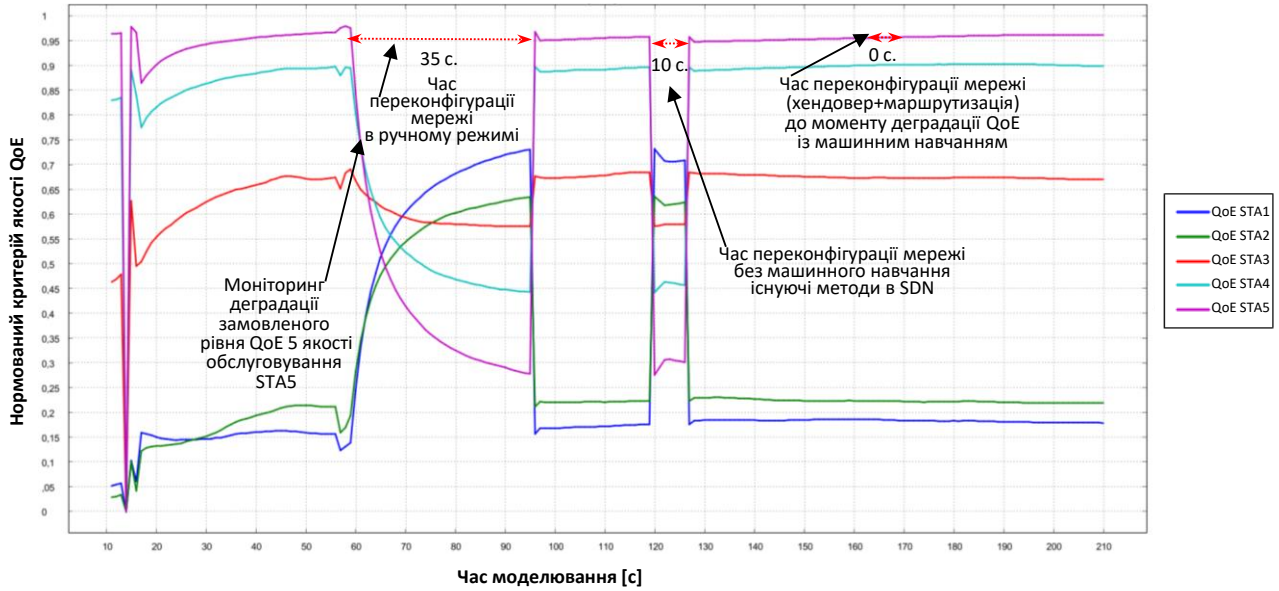


Рис. 4.9. Інтелектуальна система моніторингу якості мережі за критерієм QoE

Як бачимо з рис.4.9 на відміну від відомого методу управління хендовером та конфігурацією мережі запропонований підхід забезпечує швидше виявлення деградації рівня QoE на 25с, а у поєднанні із машинним навчанням відбувається переконфігурація мережі ще до моменту виявлення деградації якості сприйняття послуги, тим самим надаючи гарантовано високу якість обслуговування для важливих користувачів.

Для дослідження ефективності запропонованого методу ініціації хендоверу із відомим методом щодо оцінки якості сприйняття відео послуги проведено реальний експеримент в середовищі Mininet із використанням VLC плеєра. Експеримент проводився наступним чином, спершу було записано фрагмент відеопотоку запису руху руки в режимі реального часу. Після чого дане відео записано на віртуалізованому медіасервері в середовищі Mininet. Також в Mininet розгорнуто вище згадану топологію віртуалізованої SDN мережі із підтримкою програмно реалізованих додаткових модулів, що автоматизують

розроблений методи ініціації хендовера та управління якістю сприйняття послуг. Кінцевий пристрій знаходячись в зоні покриття двох Wi-Fi точок доступу робить запит на перегляд записаного відео. Під час відео перегляду користувач переміщається по запрограмованій траєкторії руху з метою перебування під обслуговуванні двох точок доступу з різними радіоумовами. Паралельно змінювалися QoS параметри каналів зв'язку на рівні комутаторів SDN, щоб змоделювати різні ступені навантаження на мережу та оцінити ефективність методів. Сценарії моделювання та вхідні дані є ідентичними як в умовах використання існуючого методу, так і з використанням запропонованого, що дає змогу оцінити ефективність їх роботи в процесі відеоперегляду в режимі реального часу. Зокрема на рис. 4.10 показано результат роботи методів з якого випливає, що в момент коли користувацький пристрій STA 1 знаходиться в зоні обслуговування двох точок доступу AP1 та AP2 при існуючому методі хендовера обслуговування відбувається саме точкою доступу AP2 це пов'язано із тим, що у AP2 кращі радіоумови у порівнянні із точкою AP1. Хоча у другому сценарії моделювання при тестуванні запропонованого методу в цей же момент часу обслуговування відбувалось точкою доступу AP1 із гіршими радіоумовами для кінцевого пристрою. Проте кінцева якість відео сприйняття послуги саме під час використання запропонованого методу є набагато кращою. Зокрема оцінивши якість сприйняття послуги за показником QoE отримано для відомого методу QoE=3,5 та для запропонованого QoE=5. Це пов'язано із тим, що маршрут передавання даних через точку доступу AP2 є більш завантаженим ніж коли б пристрій підключався через точку доступу AP1. Таким чином можна стверджувати, що запропонований метод ініціації хендовера є ефективнішим у порівнянні із відомим.

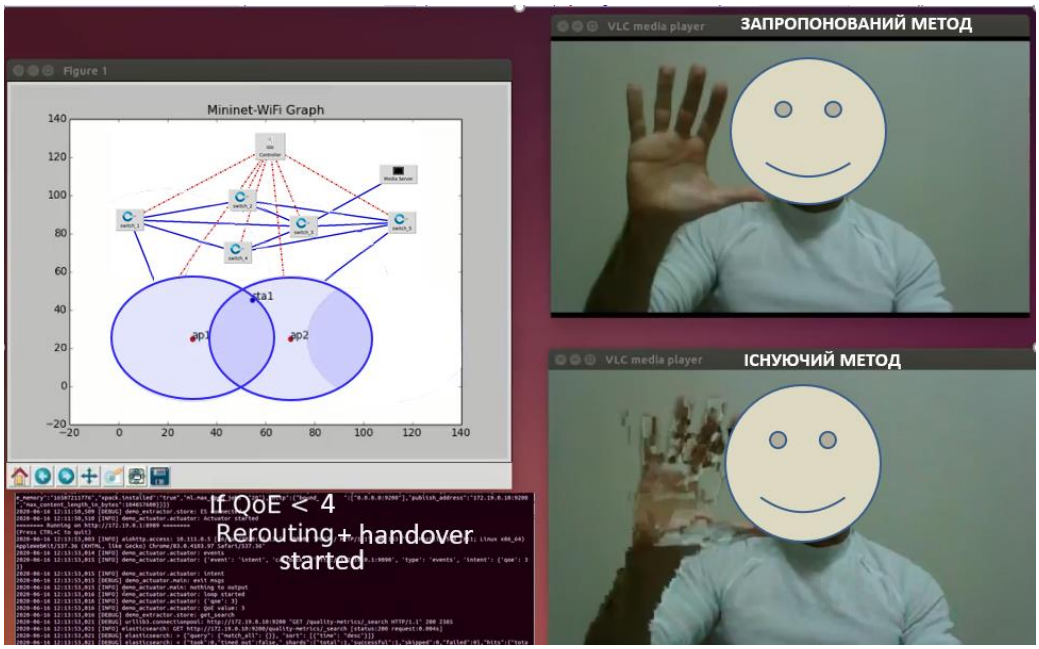


Рис.4.10. Порівняння ефективності методів за показником якості сприйняття відеопослуги QoE (Сценарій 1)

При наступному сценарію дослідження якості сприйняття послуги в умовах коли пристрій користувача STA 1 змінив своє місце розташування. Якість перегляду є високою в обох випадках використання методів. Хоча обслуговування відбувається через різні точки доступу.

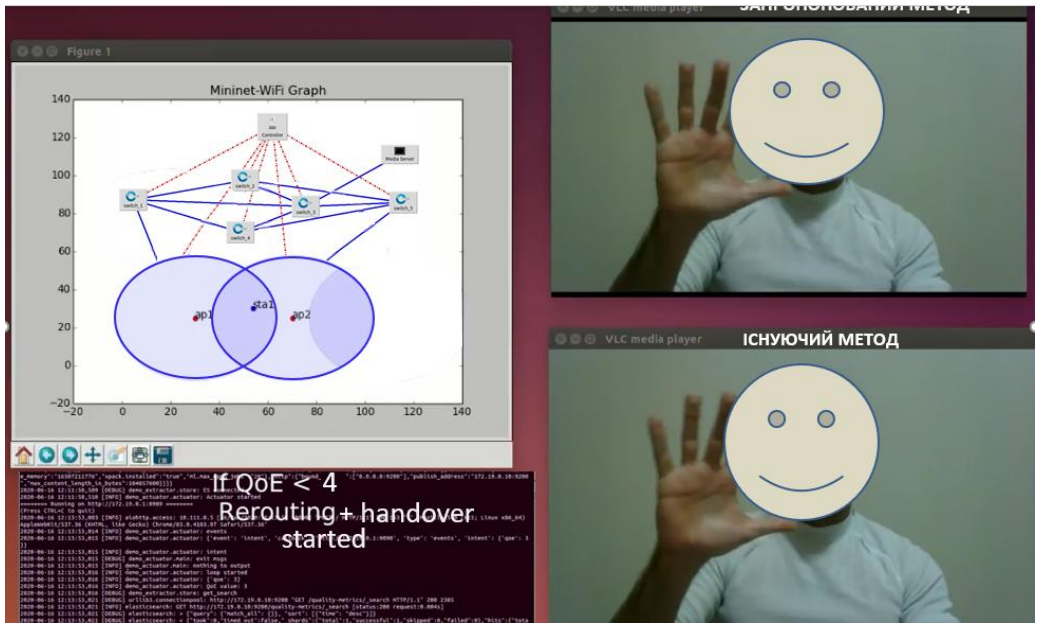


Рис.4.11. Порівняння ефективності методів за показником якості сприйняття відеопослуги QoE (Сценарій 2)

І також цікавим виявився наступний експеримент коли станція STA 1 знаходиться в зоні покриття тільки точки доступу AP2. В такій ситуації обслуговування для двох методів відбувається через AP2. Проте в умовах використання запропонованого методу якість є набагато кращою у порівнянні із відомим методом. Зокрема під час використання відомого методу якість перегляду відео була не допустимою (QoE 1), зокрема спостерігалися завмирання картинки та спотворенні пікселі. Це пов’язано із тим, що маршрут передавання даних при існуючому підході вибрано за принципом найкоротшого шляху (S5-S3), проте як виявилось в цей момент часу на ділянці (S5-S3) спостерігалось перевантаження каналу зв’язку. Таким чином використання запропонованої QoE-моніторингової системи в роботі дало змогу це виявити та використавши запропоновану QoE-маршрутизацію вибрати альтернативний оптимальний маршрут (S5-S4-S1-S3), який є довшим, але з кращими канальними характеристиками. Якість перегляду відео була високою та оцінена як QoE 5.

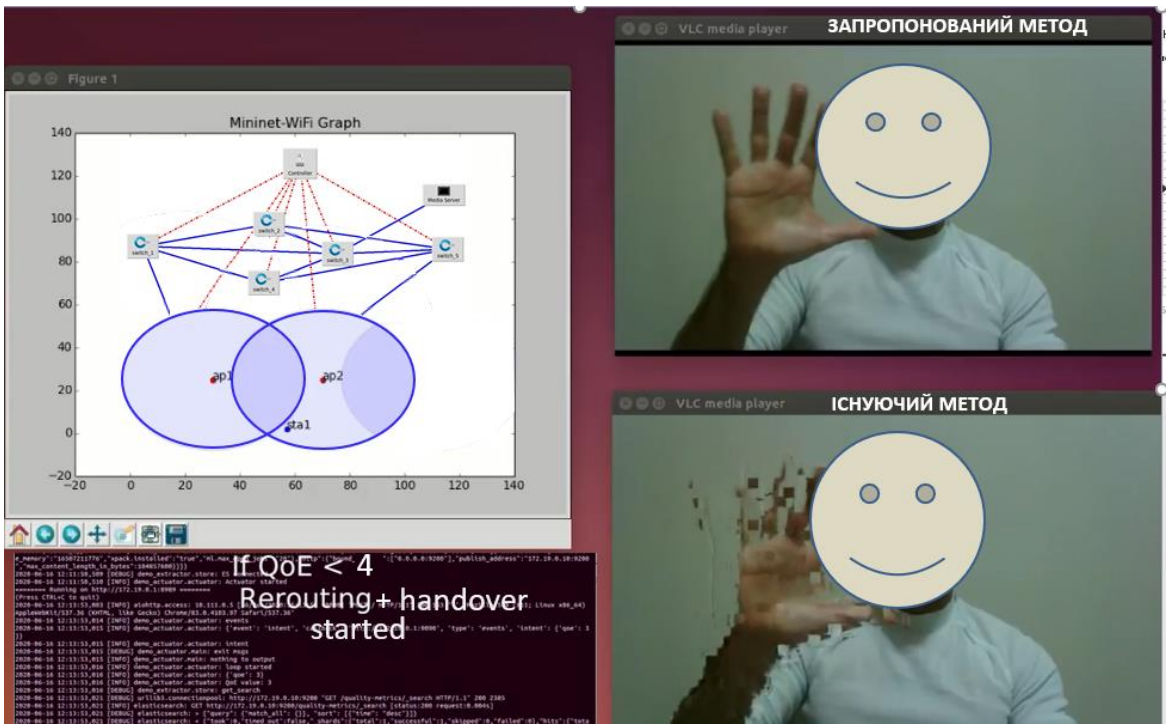


Рис.4.12. Порівняння ефективності методів за показником якості сприйняття відеопослуги QoE (Сценарій 3)

На рис.4.13 показано принцип роботи запропонованої інтелектуальної мережі з точки зору моніторингу QoS параметрів, визначення поточного показника QoE за допомогою QoS/QoE математичної моделі (зелена рамка), замовлена оцінка QoE-5 згідно інтенції користувачів та прогнозована поточна оцінка QoE-1 (синя рамка) та автоматична переконфігурація на знайдений альтернативний маршрут з прогнозованим значенням QoE-5 для підвищення якості сприйняття послуг до моменту виявлення деградації.

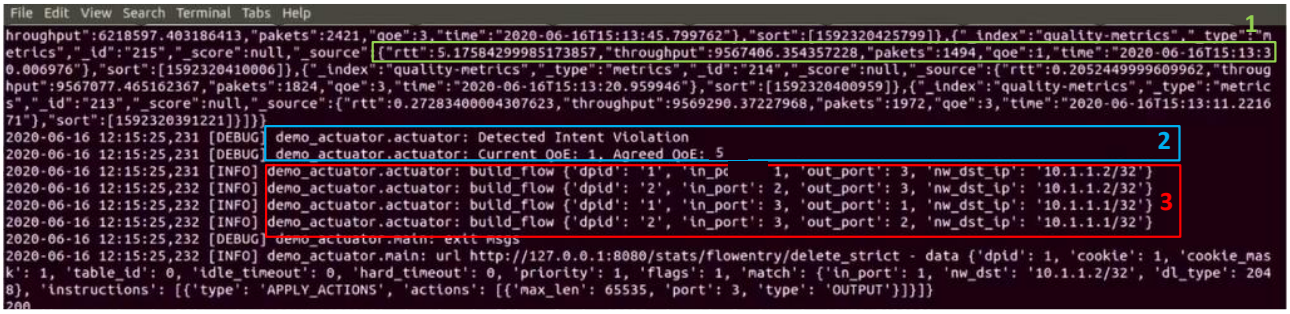


Рис.4.13. Демонстрація роботи запропонованого методу управління якістю сприйняття послуг на основі розроблених методів QoS/QoE моніторингової системи, QoE-маршрутизації та ініціації хендовера

4.3 Реалізація прототипу інтелектуальної програмно-конфігурованої мережі на основі мережевого обладнання Zodiac та розроблених програмних компонентів, що реалізують нові методи управління якістю надання послуг

У роботі для практичної реалізації інтелектуальної мережі нового покоління використано обладнання технології SDN Zodiac, яке, на відміну від пропрієтарних виробників мережевого обладнання є відкритим для модифікацій та дає змогу програмно реалізовувати власні рішення щодо управління ресурсами. Зокрема макет реалізованої мережі показано на рис.4.13, топологія якої є аналогічною із топологією інтелектуальної мережі модельованою в середовищі Mininet (рис.4.4).

Рис.4.14. Макет інтелектуальної програмно-конфігурованої мережі на основі мережевого обладнання

Для побудови інтелектуальної мережі використано наступне обладнання: 5 одиниць 4-х портових SDN, комутаторів Zodiac FX; 2 одиниці програмно-керованих Wi-Fi точок доступу Zodiac WX з підтримкою централізованого управління на основі протоколу OpenFlow; 1 контролер мережі розгорнутий на міні комп'ютері; 4 одиниці міні-комп'ютерів Raspberry PI model 3 B, 3 із яких виконують функції кінцевих пристроїв для генерації трафіку та 1 виконує функцію медіа сервера; 2 одиниці смартфонів Samsung Note 4 для організації безпровідного Wi-Fi з'єднання з метою дослідження нового методу QoE-хендовера. Також для повноцінної реалізації пропонованої інтелектуальної мережі з підтримкою управління якістю сприйняття послуг на основі QoE-інтенцій у роботі використано власні написані унікальні програмні компоненти, а саме: розроблений програмний IBN контролер; модуль моніторингу параметрів якості функціонування мереж; модуль машинного навчання для автоматизованого прогнозування QoS параметрів каналів зв'язку та відповідно прогнозування показника QoE, що характеризує рівень якості сприйняття

послуг кінцевими користувачами; модуль QoE-орієнтованої маршрутизації та QoE-орієнтованого хендовера.

Нище наведено детальний опис та конфігурацію прототипу інтелектуальної мережі.

Отже для розробки прототипу використано комутатор Zodiac FX. Zodiac FX - це комутатор OpenFlow, котрий легко поміщається на робочий стіл, а не в центрі обробки даних. Зображення даного комутатора подано на рис.4.15.

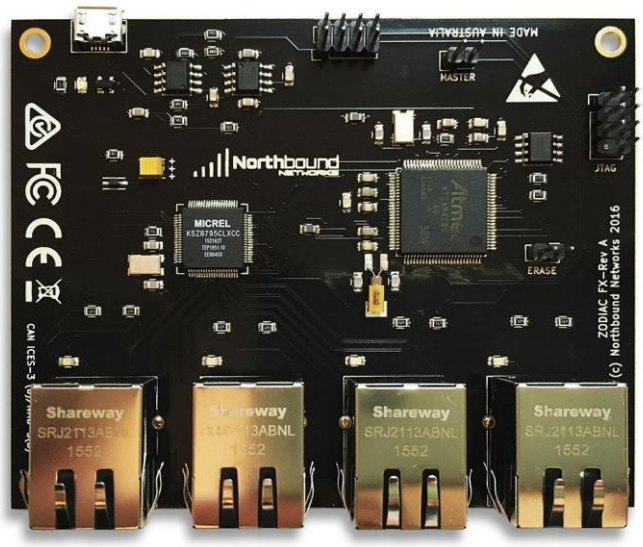


Рис. 4.15. Zodiac FX

Нижче подано список основних характеристик і переваг даного комутатора:

- 10/100Mbs Ethernet порти;
- Amtel SAM4E8CA процесор;
- Microchip KSZ8795CLX Managed Ethernet комутатор;
- USB Serial і Web Based налаштування;
- Підтримує OpenFlow 1.0 & 1.3;
- Відкритий код;
- Живлення від USB;
- Габарити: 100мм х 80мм;

- Вага: 115 грам;

Для первинного налаштування комутатора найкращим способом є через USB послідовний порт. Після успішного підключення та встановлення відповідних драйверів, комутатор готовий до налаштування (рис. 4.16.).

Рис. 4.16. Успішне підключення до терміналу Zodiac FX через COM3

Також рекомендовано відразу обновити програмне забезпечення даного комутатора. Тому встановлено на момент розробки прототипу останню версію з офіційного веб сайту даного комутатора версію програмного забезпечення 0.86.

Сам по собі комутатор у SDN мережі без підтримки класичної роботи комутатора, фактично нічого здійснювати не буде. Всі пакети будуть автоматично відкинуті (package drop). Тому наступним кроком буде створення базового OpenFlow контролера. Серед вже згаданих у роботі відкритих контролерів з підтримкою OpenFlow протоколу, потребують обчислювальні ресурси на функції котрі не є необхідними для даної роботи, хоч і досить універсальні та гнучкі. З цієї метою для створення більш ефективного простішого контролера було вирішено на базі Ryu фреймворка, створити власний контролер OpenFlow.

Ryu – фреймворк для побудови SDN мереж, побудований на компонентному підході. Ryu надає компонентам програмного забезпечення чітко визначений API, який полегшує розробникам створення нових програм

управління мережею. Ryu підтримує різні протоколи управління мережевими пристроями, такими як OpenFlow, Netconf, OF-config та інші. Про OpenFlow, Ryu повністю підтримує версії 1.0, 1.2, 1.3, 1.4, 1.5 та Nicira. Весь код є у вільному доступі за ліцензією Apache 2.0. Ryu написаний на мові програмування Python.

Так як Zodiac FX підтримує версію OpenFlow 1.3, відповідно контролер написаний саме для цієї версії. Запуск контролера зображено на рис.4.17. Контролер у даному прототипі може бути запущений як на ноутбуці так і на міні комп'ютері (Raspberry, Orange). Після цього необхідно налаштувати комутатор і підключити до даного контролера.

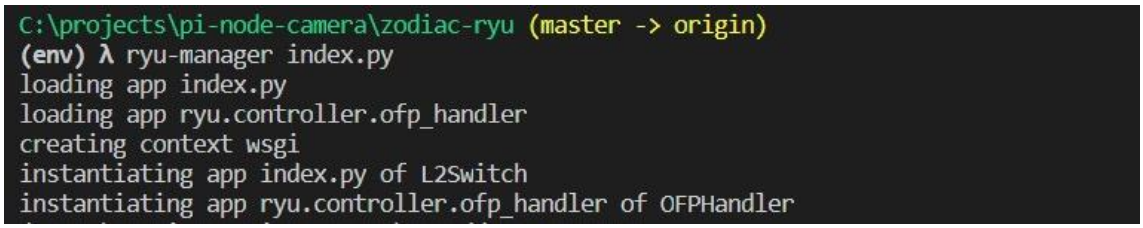


Рис. 4.17. Запуск контролера на базі Ryu

В першу чергу необхідно підключити комутатор до ноутбука через ethernet протокол ZodiacFX по замовчуванню має відсутні налаштування мережі, такі як IP адреса, мережева маска (Netmask), адреса шлюзу (Gateway). Дізнавшись IP адресу контролера - 169.254.154.173, для контролера необхідно налаштувати наступні параметри:

IP Address: 169.254.154.123

Netmask: 255.255.255.0

Gateway: 169.254.154.254

OpenFlow Controller: 169.254.154.174

OpenFlow Port: 6653

Встановлення цих параметрів, зображено на рис. 4.18.

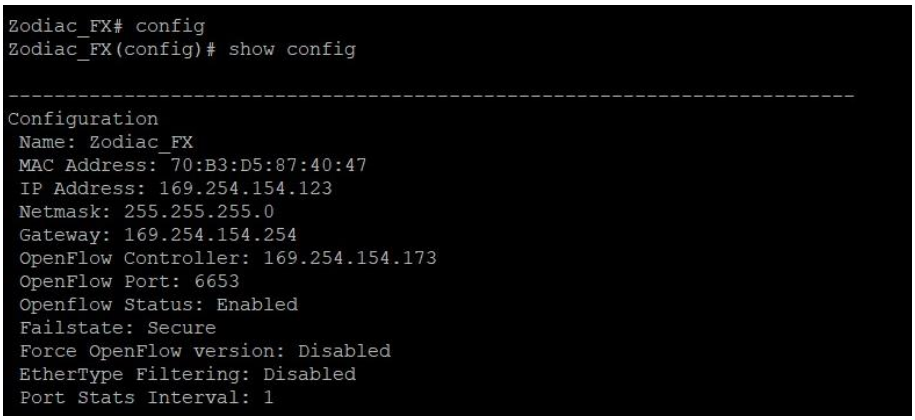


Рис. 4.18. Налаштування ZodiacFX комутатора

Після зберігання і перезапуску комутатора, контролер автоматично повинен розпізнати підключений комутатор, і відразу встановити перше значення у таблиці маршрутизації, що при відсутності правила для пакету, перенаправляти даний пакет на контролер (table-miss flow entry). Підключений комутатор до контролер показано на рис. 4.19. На рис. 4.20. зображено єдине значення таблиці (flow), котре має найнижчий пріоритет – 0, і дія – відправляти на контролер (рис.4.19).

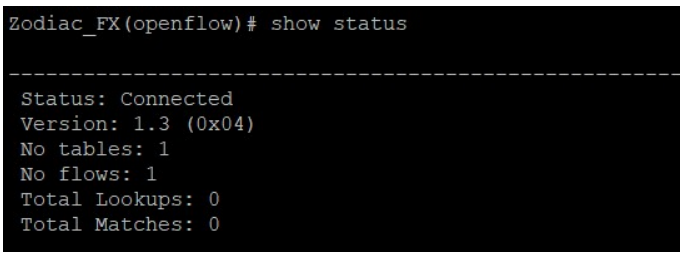


Рис. 4.19. Підключений комутатор до контролера

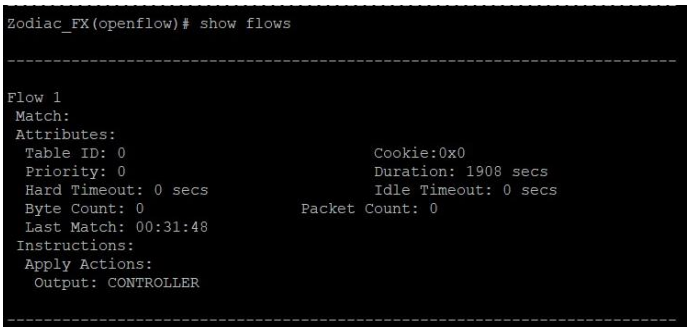


Рис.4.20. Таблиця маршрутизація з одним правилом за замовчуванням

Успішно налаштувавши контролер з комутатором, тепер необхідно підключати кінцеві пристрої для комутації (hosts). У даній роботі наразі це є сервер відеопотоку. Сервер відеопотоку підключено до першого порта, а відео сервіс до другого порта на хості, що встановлений на Raspberry. Підключившись до сервера відеопотоку, за допомогою команди $ ip addr show, на Ubuntu (операційна система встановлена на сервері) можна переглянути IP адресу ethernet порта. На рис. 4.21 видно що по ethernet порту, даний сервер має IP адресу 169.254.85.217.

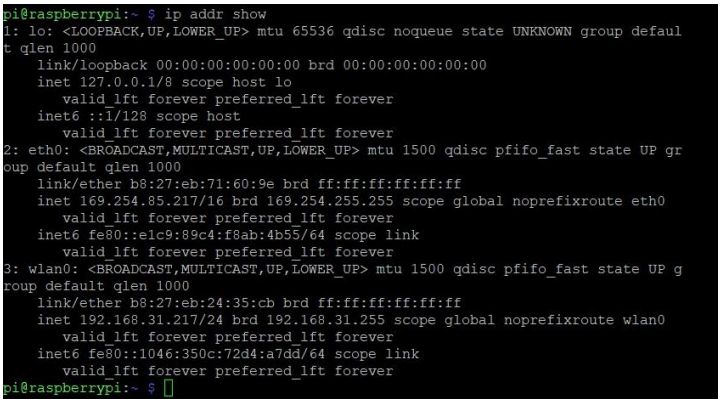


Рис. 4.21. Результат виконання ip addr show

Спробуємо доступитись через команду ping по протоколу ICMP до сервера відеопотоку через комутатор, котрий контролюється контролером. На рис. 4.22 видно що виконання ping команди було успішним.

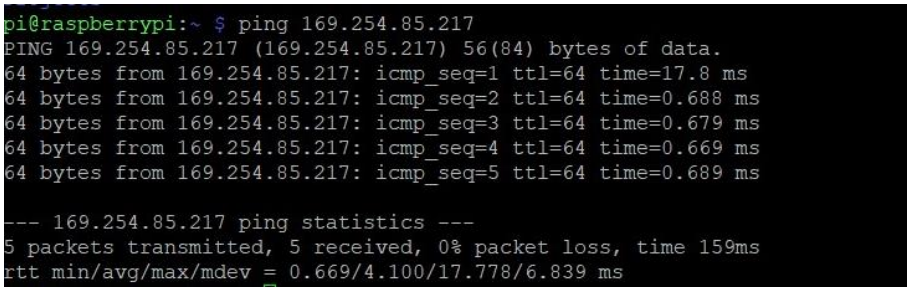


Рис. 4.22. Результат виконання ping команди через комутатор

Коли перший сервер надсилав запит на другий, комутатор отримавши такий пакет, мав одне правило у таблиці маршрутизації. Згідно цього правила він відправив пакет на контролер. Контролер у пам’яті немаючий жодної на той момент MAC адреси пункту призначення і відповідного порта, дав команду на

комутатор здійснити груповий запит (multicast) на всі порти (flood) для того щоб дізнатись порт, необхідної адреси, та відповідно зберегти їх для подальшого використання. Дізнавшись необхідний порт, контролер надіслав відповідно команду на комутатор, і також дав запит за запис нових правил у таблиці маршрутизації. На рис. 4.23 видно два нових правила.

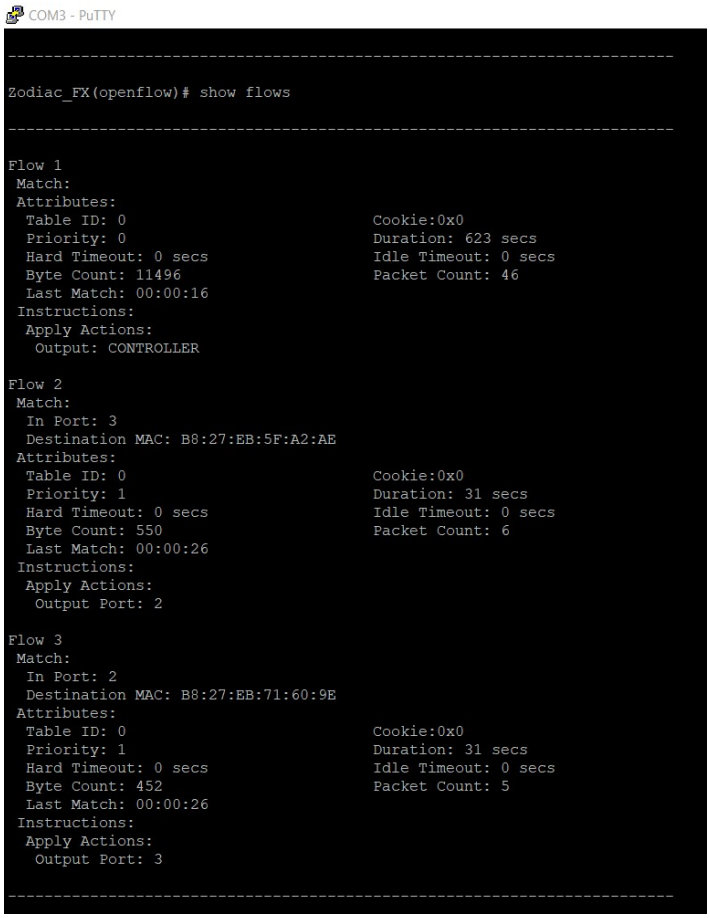


Рис. 4.23. Нові правила маршрутизації у комутаторі Zodiac FX

Також за допомогою команди $ show ports на комутаторі Zodiac FX можна переглянути статистику по портах. На рис. 4.24 видно що налаштовано 3 з 4 портів (один наразі не використовується). 4 порт використовується для спілкування з контролером, 2 і 3 для серверів відповідно. Видно також статистику по отриманих і переданих пакетів по кожному із портів. Втрачених пакетів не виявлено. Статистику подано на рис.4.24.

На рис.4.25. подано схему прототипу на даному етапі. Як видно зі схеми, сервер відеопотоку спілкується з сервісом відеопотоку через SDN комутатор, котрий контролюється через SDN контролер. На веб-клієнті успішно здійснюється трансляція відеопотоку реального часу із затримкою 860 мілісекунд, що є приблизно на 50 мілісекунд довше ніж у попередньо реалізованій схемі, і є незначною.

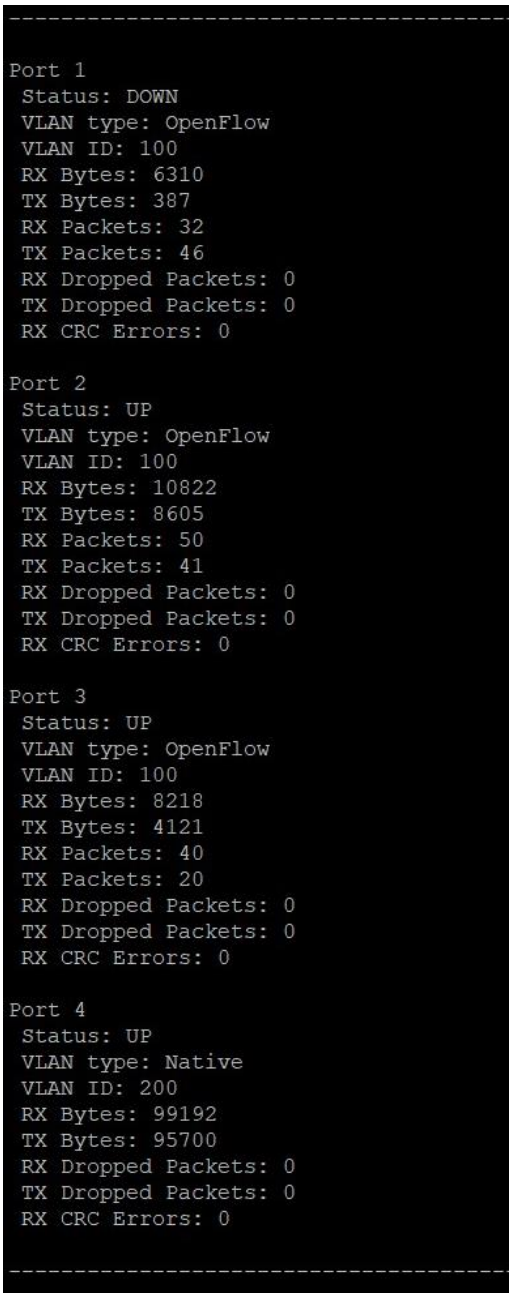


Рис. 4.24. Статистика по портах комутатора

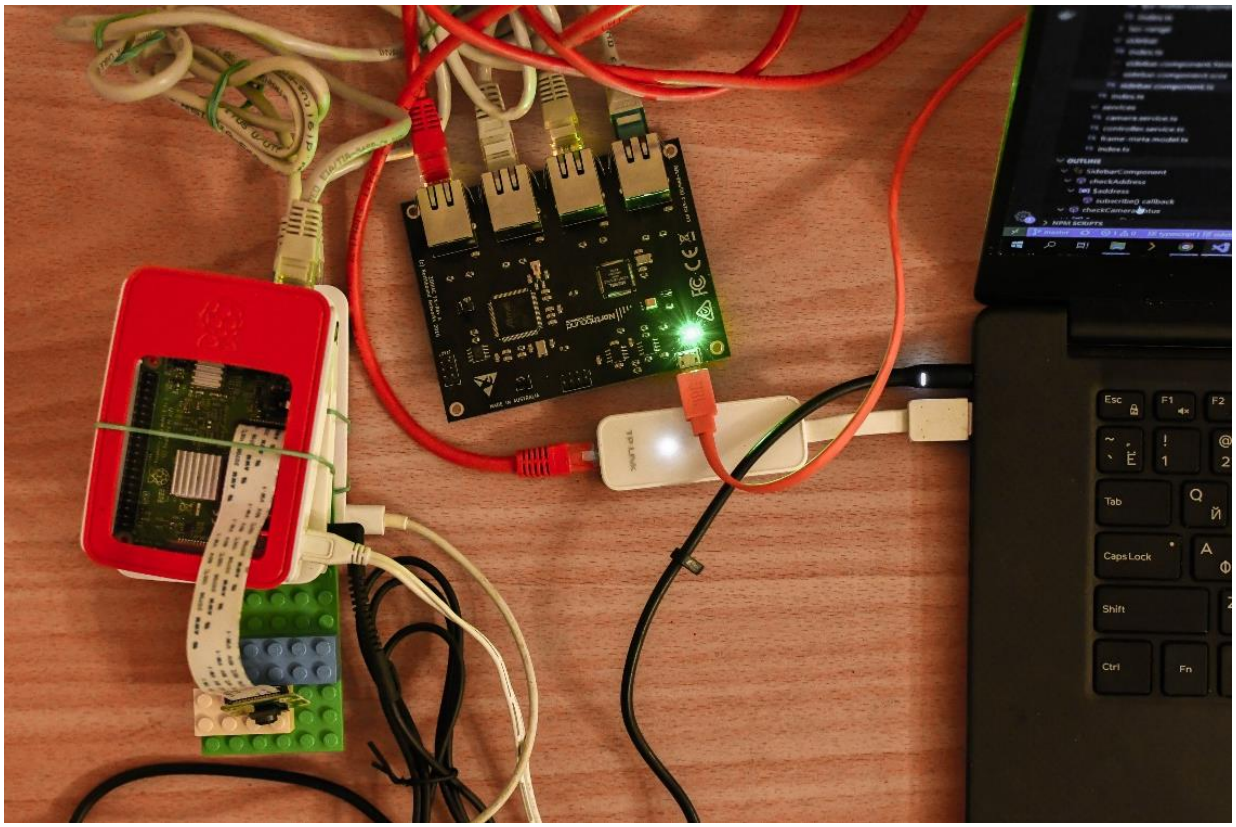


Рис.4.25. Розроблений фрагмент SDN інфраструктури для відеопотоку, вид зверху

Найпростіша мережа готова. Проте програмно-конфігуровані мережі мають невід'ємну складову – SDN контролер. Так як у даній мережі комутатор підтримує OpenFlow протокол, необхідно відповідно реалізувати контролер з підтримкою даного протоколу. На сьогоднішній день існує безліч готових рішень, і до найпопулярніших OpenFlow контролерів можна віднести:

При виборі OpenFlow контролера для даної моделі в першу чергу розглядались контролери з мінімальними системними вимогами, адже для SDN контролера планується використати одноплатний комп'ютер OrangePi Prime. Як згадувалось у першому розділі, дана плата має чотирьох ядерний процесор і два гігабайти оперативної пам'яті, що повинно бути достатньо для простого SDN контролера. У таблиці 2.1 приведено мінімальні апаратні вимоги для роботи SDN контролерів.

Таблиця 4.1

Таблиця мінімальних вимог апаратного забезпечення SDN контролерів

№	Назва SDN контролера	Апаратні вимоги
1	OpenDaylight	2 core CPU 4 GB RAM 20 GB hdd
2	ONOS	2 core CPU 2 GB RAM 10 GB hdd
3	OpenStack	2 core CPU 4 GB RAM 10 GB hdd
4	Floodlight	2 core CPU 2 GB RAM 10 GB hdd

Згідно таблиці, видно що тільки два контролери підходять по апаратних вимогах для OrangePi Prime – ONOS та Floodlight. Вивчивши базові компоненти обох контролерів, для реалізації моделі даної програмно-конфігурованої мережі було обрано саме контролер Floodligh, адже у його складі є менше компонент, і відповідно дана плата буде краще справлятись з поставленим завданням. До інших переваг Floodlight контролера можна віднести також:

- Пропонує систему завантаження модулів, що полегшує розширення та посилення.
- Легко встановити з мінімальними залежностями
- Підтримує широкий спектр віртуальних та фізичних комутаторів OpenFlow
- Може працювати з сумісними OpenFlow і не OpenFlow мережами - він може управляти кількома обладнанням OpenFlow
- Розроблений як високопродуктивний - багатопоточний з нуля
- Підтримка платформи керування хмарним середовищем OpenStack

Даний контролер буде підключено через Wi-Fi у внутрішню мережу. Floodlight у своїх системних вимогах вказує на необхідність операційної

системи Ubuntu або Debian. Через свою популярність було обрано операційну систему Ubuntu для Orange Pi Prime. Структурна схема SDN мережі з Floodlight контролером зображена на рис.4.26.

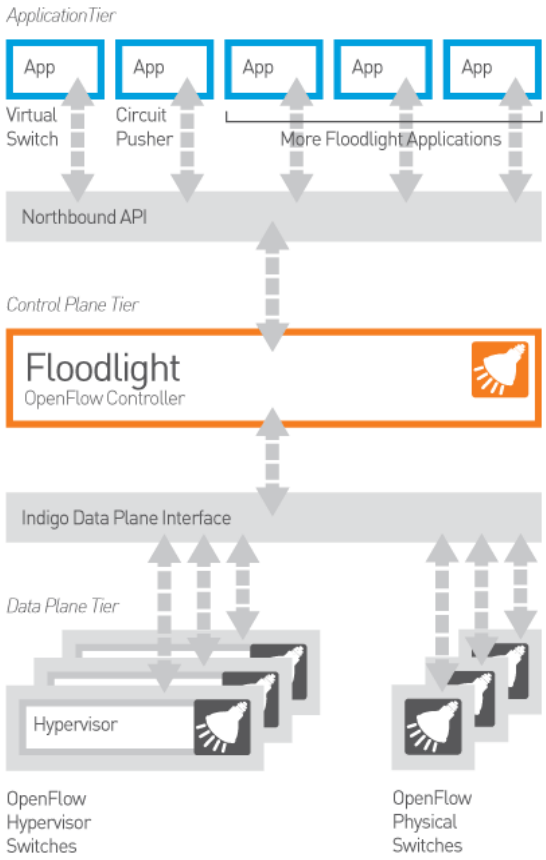


Рис.4.26. Структурна схема SDN мережі з Floodlight контролером

Після успішного встановлення Floodlight контролера необхідно його запустити. На рис.4.27 зображено при успішному встановлені та запущені програми Floodlight контролера.

Floodlight контролер у своєму інтерфейсі, має два зручних способи для керування мережами - REST API та GUI. GUI виконаний у вигляді веб клієнта. Найзручнішим способом є другий варіант. Для того щоб ним скористатись, достатньо у внутрішній мережі, у котрій працює даний контролер перейти по наступному посиланні: <ip адреса контролера>:8080/ . При переході, на дану адресу у браузері, буде показано головну сторінку Floodlight GUI контролера (рис. 4.28).

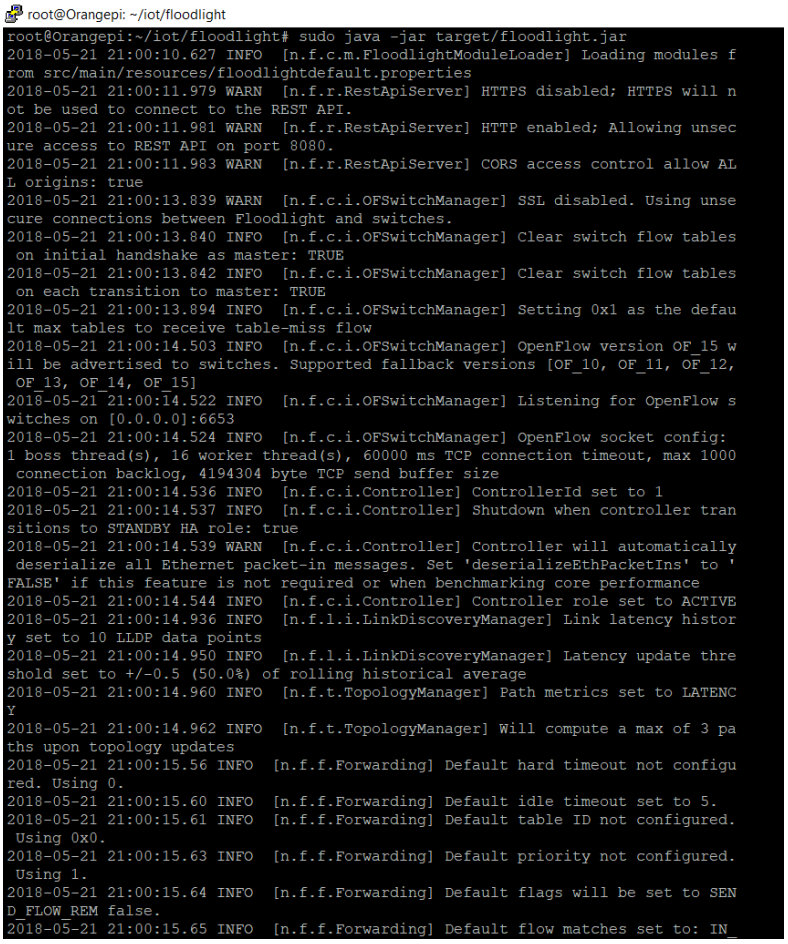


Рис.4.27. Успішно запущений Floodlight контролер

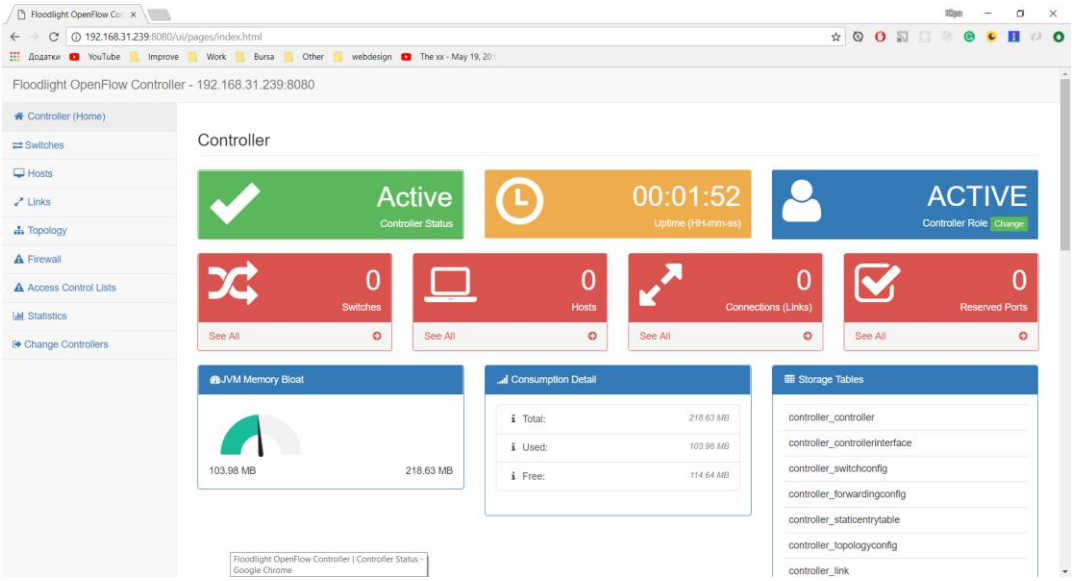


Рис.4.28. Головна сторінка Floodlight GUI

Як і з головної сторінки видно, що на даний момент немає жодного підключеного хоста чи комутатора. Тому необхідно Open vSwitch комутатору вказати контролер. Це можна зробити за допомогою наступної команди: $ ovs-vsctl set-controller mybridge tcp:0.0.0.0:6653 (6653 порт OpenFlow) (рис. 4.29).

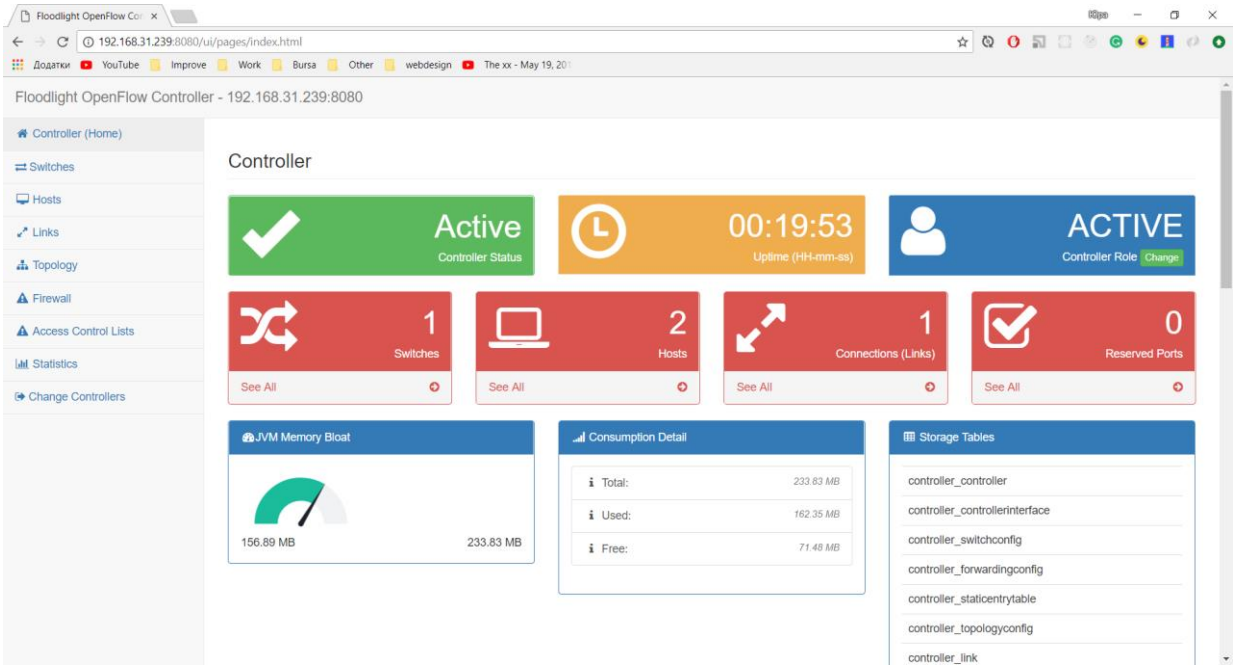


Рис.4.29. Floodlight має підключені два хости і один комутатор

У лівій панелі на сайті бачимо різні елементи меню для керування Floodlight контролера. Наприклад, при переході у вкладку топологія (Topology) можна побачити актуальну топологію мережі SDN (рис. 4.29). На даній топології видно комутатор Open vSwitch та хости – брокер WebSocket Server та модуль Bluetooth Master, котрі напряму з'єднанні до комутатора через кабель ethernet. У вкладці з'єднання (Links) можна побачити всі доступні з'єднання у даній мережі (рис. 4.30). Так як у даній мережі тільки два хости, існує тільки одне з'єднання, двонаправлене (bidirectional). У вкладці комутатори (Switches) можна переглянути деталі про доступні комутатори, та налаштувати їх (рис.4.31).

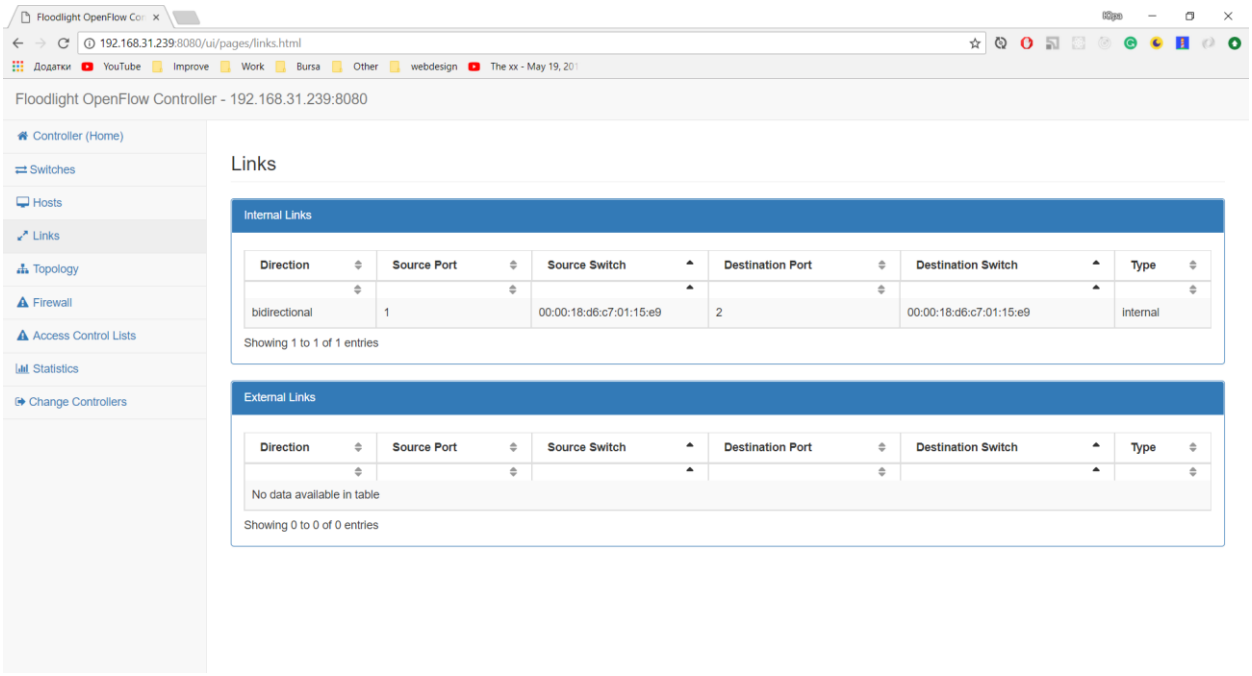


Рис.4.30. З’єднання мережі SDN

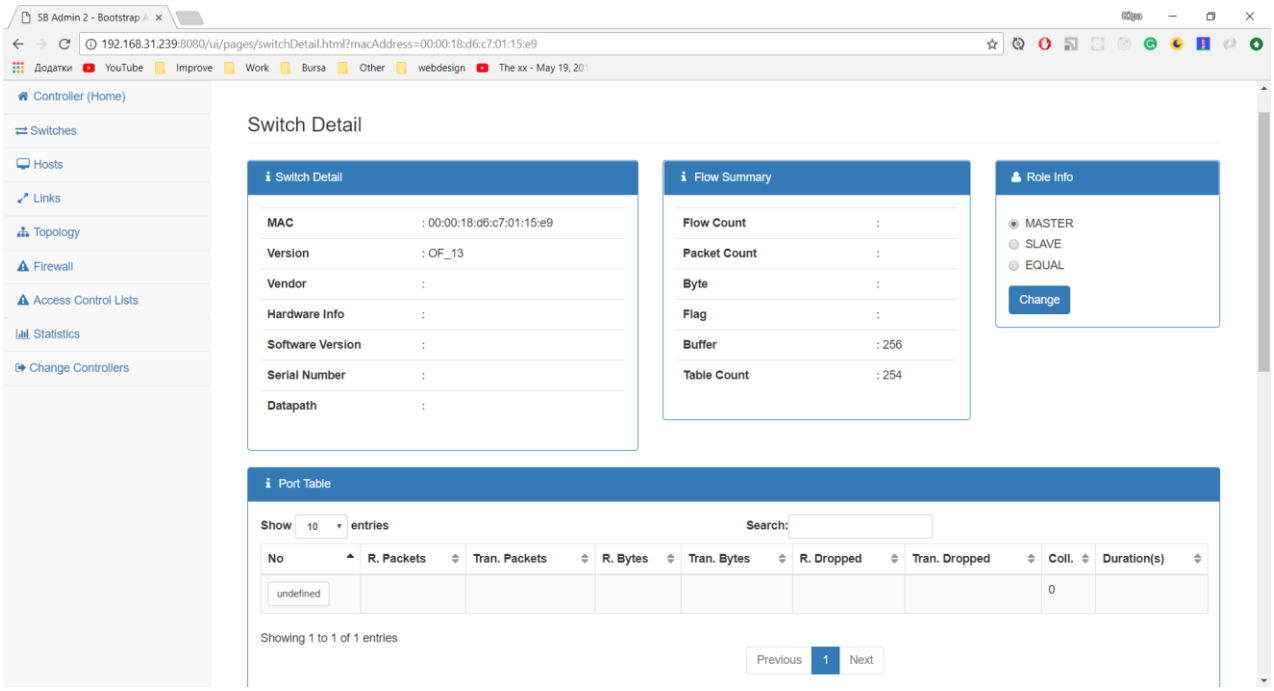


Рис.4.31. Деталі про Open vSwitch комутатор

Таблиця маршрутизації є пустою, і за допомогою веб-інтерфейсу можна додати значення до неї (рис. 4.32). Даний контролер надішле запит про створення нового значення у таблиці маршрутизації.

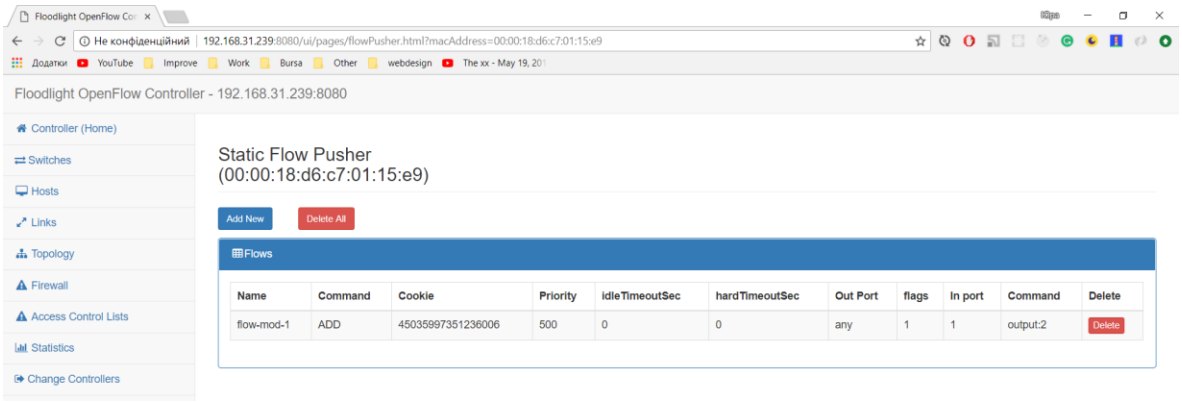


Рис. 4.32. Таблиця Static Flow Pusher

Іншим способом керування мережею є REST API. За допомогою REST API, можна виконувати ті самі функції що доступні і у веб інтерфейсі, проте це може буде зручно, коли створюється власна реалізація веб-інтерфейсу, написання програми для автоматизації керування мережею, чи навіть штучного інтелекту, тощо. Для створення запитів по HTTP/HTTPS протоколу одним із зручних способів є використання додатку Postman. Інтерфейс даної програми показано на рис.4.33.

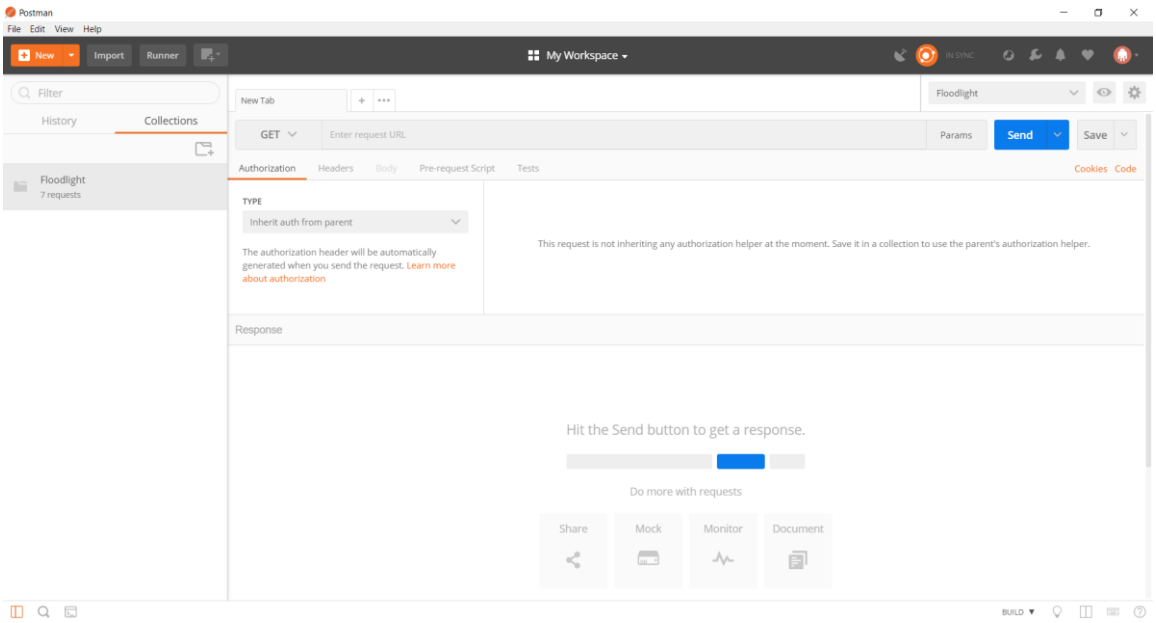


Рис.4.33. Інтерфейс додатку Postman

Даний додаток дозволяє у дуже зручному і зрозумілому інтерфейсі створювати HTTP запити, редагувати HTTP заголовки, додавати тіло запитів,

переглядати відповідь запитів, створювати колекції запитів, глобальні зміни, і до того ж це все зберігати у власному профілі користувача, також додатково було написано програмне забезпечення через розроблений унікальний IBN контролер з ip адресою нового контролера IBN 172.19.0.1, щоб можна було б створювати та аналізувати QoE-інтенції користувачів.

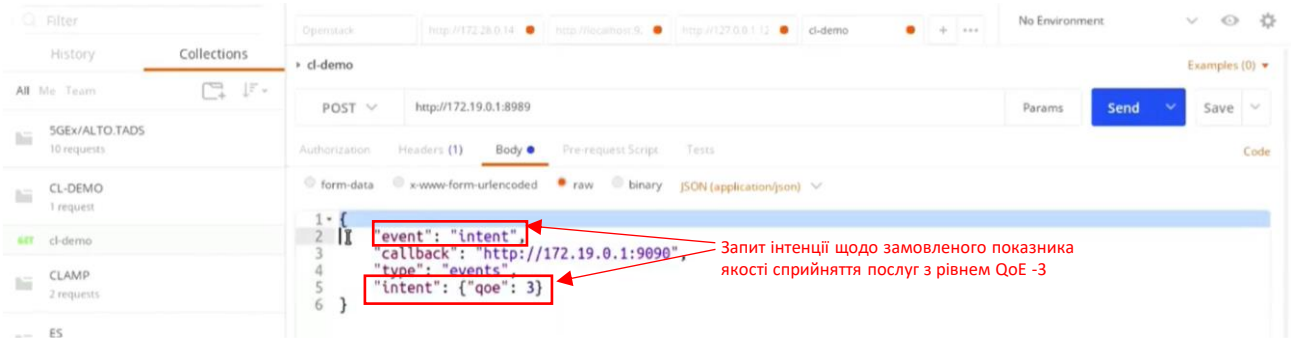


Рис.4.34. Створення QoE інтенцій через інтерфейс додатку Postman

Наприклад, за допомогою Postman і Rest API Floodlight контролера можна провірити об’єм вільної пам’яті на контролері. Щоб це провірити, достатньо зробити HTTP запит з методом GET за посиланням http://{{contoller-ip}}:8080/wm/core//memory/json , де {{contoller-ip}} необхідно замінити на ip адресу контролера. В результаті виконання даного запиту, отримали що загальний об’єм пам’яті 97517568 байтів (97 мегабайт) з котрих вільно 36231264 (36 мегабайт) (рис. 4.35).

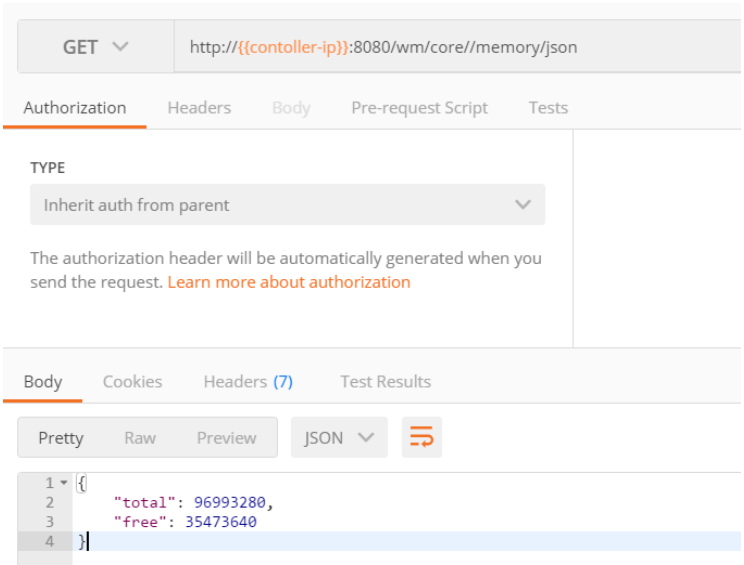


Рис.4.35. Отримання вільної пам’яті Floodlight контролера

Також за допомогою Rest API можна добавляти, видаляти, та змінювати значення в Static Flow Pusher. Static Flow Pusher – це таблиця, подібна до FlowTable на віртуальному комутаторі OpenFlow, проте зберігається на контролері Floodlight. При зміні цієї таблиці, контролер автоматично змінює значення у підключеному комутаторі для котрого записувалось значення. Щоб добавити значення через цей інтерфейс, спочатку потрібно переконатись що немає жодного значення у таблиці маршрутизації комутатора (рис.4.36).

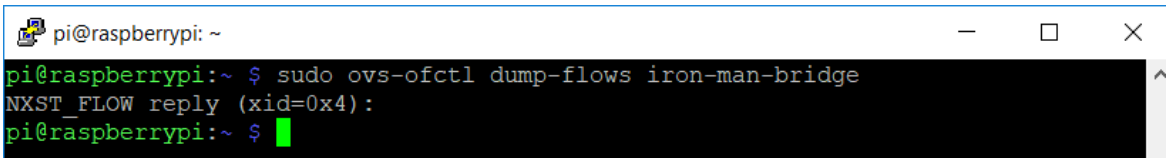


Рис.4.36. Open vSwitch пуста таблиця маршрутизації

Відповідно хост один не зможе доступитись до хоста два. Перевірити це можна за допомогою команди ping (рис.4.37.).

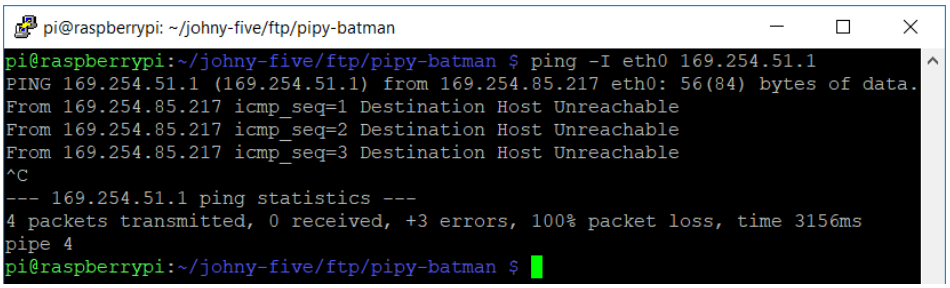


Рис. 4.37. Хост один не може доступитись до хоста два

Для того щоб додати значення в Static Flow Pusher необхідно виконати запит HTTP з методом POST на наступне посилання: http://{{contoller-ip}}:8080/wm/staticflowpusher/json . Вміст Body до запиту має бути форматом JSON, та містить наступні поля:

- switch – DPID комутатора
- name – назва Flow
- cookie – використовуються для фільтрації потоку,
- priority - пріоритет,

- in_port – вхідний порт
- active – стан Flow
- actions – необхідні дії

Тому для прикладу щоб комутатор обробив пакет котрий поступив на порт 1, відправився на порт 2 контент Body буде виглядати наступним чином (DPID_SWITCH – замінивши відповідним значенням):

{

"switch":"{{ DPID_SWITCH }}",

"name":"flow-mod-1",

"cookie":"0",

"priority":"500",

"in_port":"1",

"active":"true",

"actions":"output=2"

}

За допомогою Postman додано необхідні значення в Static Flow Pusher (рис.4.38). У відповідь отримуємо "status": "Entry pushed", що свідчить про успішно виконаний запит.

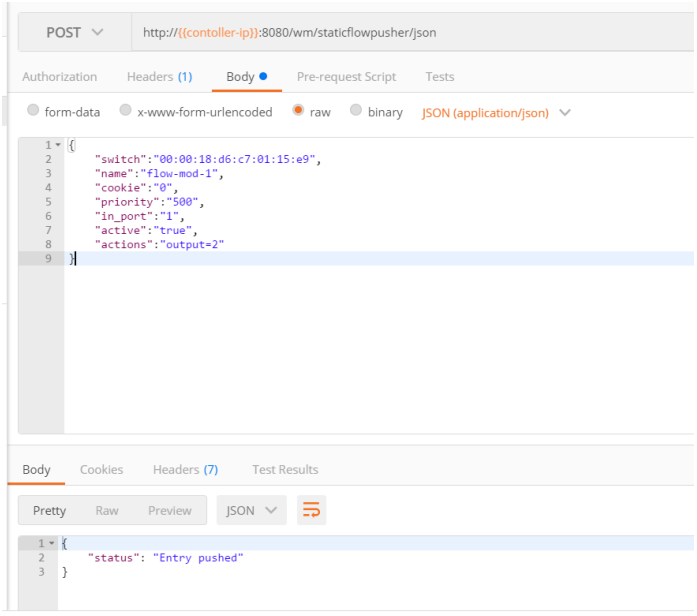


Рис.4.38. Успішно добавлено значення у Static Flow Pusher

Додавши ще відповідний Flow для другого порту, можна переконатись що таблиця маршрутизації обновилась у віртуального комутатора (рис.4.39).

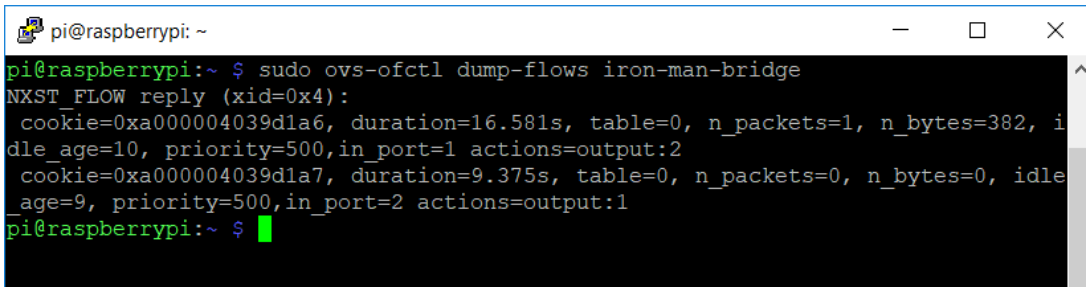


Рис. 4.39. Обновлена таблиця FlowTable у Open vSwitch

Відповідно тепер команда ping пройде успішно від одного хоста до іншого (рис.4.40).

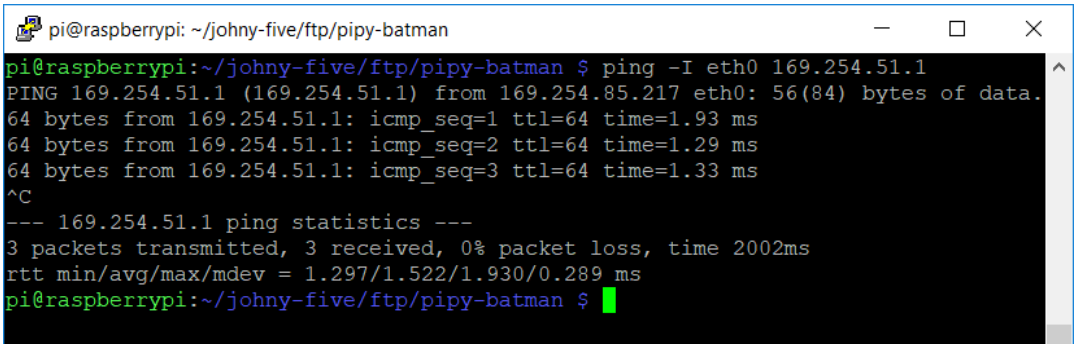


Рис.4.40. Тестування підключеності хостів

Особливістю Zodiac WX є підтримка протоколу OpenFlow [3]. Мережі на основі OpenFlow зазвичай існують виключно у програмному забезпеченні та використовують такий протокол, як Open vSwitch [4], наприклад, який дозволяє керувати трафіком між мобільними клієнтами та стаціонарною мережею набагато гнучкіше, ніж це дозволяють традиційні правила маршрутизації та брандмауера. Нещодавно випущена точка доступу є стабільним пристроєм (рис.4.41), який може працювати як від Power over Ethernet (PoE), так і від блоку живлення.

Рис.4.41. Точка доступу Zodiac WX.

Центральний процесор Zodiac WX – MIPS 74Kc. Система має 128 МБ оперативної пам'яті та два роз'єми для Gigabit Ethernet, один з яких також може використовуватись для живлення. Бездротовий інтерфейс підтримує швидкий стандарт 802.11ac (і повільніші варіанти b, g і n) на частотах 2,4 ГГц та 5 ГГц відповідно. Керування пристроєм здійснюється через веб-інтерфейс (рис.4.42), SSH або REST API контролера.

Рис.4.42. Керування Zodiac WX здійснюється через веб-інтерфейс.

У веб-інтерфейсі необхідно включити доступ до SSH; після цього можна отримати доступ, використовуючи обліковий запис адміністратора. Для привілейованого доступу, такого як команда nnofagent для перерахування встановлених потоків і груп, користувач admin повинен бути доданий файл sudoers; sudo-s також працює для повноцінної оболонки root.

Одним із важливих показників продуктивності пристроїв OpenFlow є кількість потоків, таблиць та груп, якими може керувати пристрій. Zodiac WX підтримує загалом вісім груп, 16 таблиць та 512 записів потоків.

API REST особливо важливий у контексті SDN, оскільки контролер SDN керує правилами потоків. Це був би повільний процес, якби адміністратору довелося налаштовувати мережу вручну – особливо якщо використовується кілька точок доступу. Натомість SDN-контролер може використовувати існуючий API для налаштування всього, що не охоплює OpenFlow.

До речі, якщо адміністратор не включає контролер SDN, пристрій працює як звичайна точка доступу.

Протокол OpenFlow дозволяє керувати потоками трафіку відповідно до правил. Простіше кажучи, ці правила складаються з блоку фільтрів, за яким слідує набір дій, що визначають, що має статися з пакетом. Дії можуть також використовуватися, наприклад, для перезапису полів у пакеті.

Фільтри та дії охоплюють рівні ISO від 1 до 4 (тобто поля рівня Ethernet до портів TCP, UDP та SCTP). У фільтрі OpenFlow вхідний порт пакета, а дії - його вихідний порт представляють рівень 1.

У фізичних комутаторах зазвичай очевидно, як вони поєднуються один з одним навіть якщо нумерація OpenFlow не завжди збігається з номерами портів пристрою. Порти в цьому випадку - це гнізда, в які вставляються мережеві кабелі. Звичайно, такі порти відсутні у бездротових клієнтів, тому навіть за завдання мети для пакета не вистачає одного елемента OpenFlow.

ZODIAC WX вирішує цю проблему, призначаючи дротовий порт на порт OpenFlow 65, клієнти 5 ГГц – на порти OpenFlow 1-32, а клієнти 2,4 ГГц – на

порти OpenFlow 33-64. Контролер SDN робить це, використовуючи MAC-адреси пакетів.

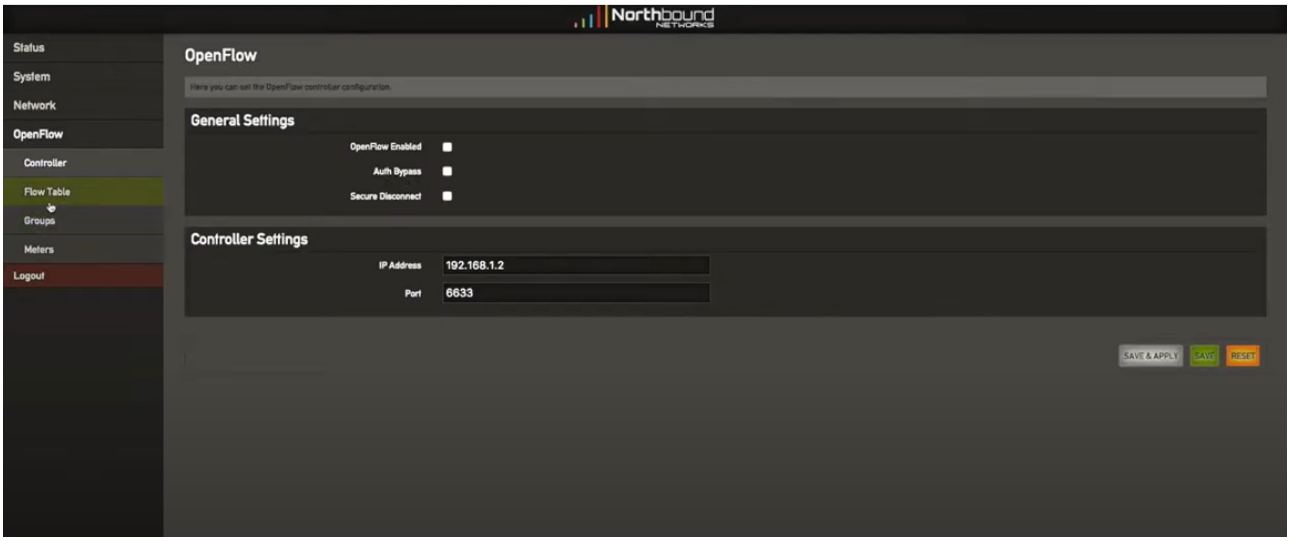


Рис.4.43. Інтерфейс таблиці потоків у SDN Zodiac WX

Аналогічно за сценарієм дослідження проведеним у розділі 4.2 запропоновані методи підтвердили свою ефективність на практиці у процесі перегляду відео реального часу.

а) існуючий метод б) запропонований метод

Рис.4.44. Якість надання відеопослуг існуючий метод а) та запропонований метод б)

4.4 Стратегічні напрямки розгортання інтелектуальних мереж подвійного призначення шляхом логічного розділення мережевої інфраструктури

У дисертаційній роботі пропонується технологія програмно-конфігурованих інтенційно-орієнтованих 5G, яка матиме великі перспективи для майбутніх оборонних мереж. Поряд із штучним інтелектом, кібербезпекою, програмно-конфігурованими та хмарними технологіями розширення можливостей систем командування, контролю та зв'язку є одним із стратегічних напрямків цифрової модернізації Міністерства оборони на 2022/2023 рік.

Завдяки підтримці як безпровідного, так і провідного доступу 5G матиме потенціал для забезпечення повсюдного рівня доступу для оборонних операцій. Його можливості динамічного розділення мережі відіграватимуть ключову роль у підвищенні ефективності та безпеки майбутньої архітектури оборонної мережі. Для досягнення наскрізної організації мережевої інфраструктури знадобиться модернізація транспортної мережі Міністерства оборони, причому автоматизація відіграє вирішальну роль у підтримці ключових функцій 5G.

Одним з найважливіших аспектів 5G є його здатність надавати «мережеві зрізи або віртуальні логічні сегменти мережі» для конкретних користувачів та їхніх додатків, які мають особливі вимоги до мережі. Наприклад, камери відеоспостереження потребують гарантованої високої пропускної здатності, тоді як керування дроном потребує дуже короткого часу реакції.

Кожен сегмент мережі може бути створений для забезпечення конкретної продуктивності мережі, необхідної кожній програмі. Як правило, захист мережі має багато різних рівнів класифікації, і в межах сегменту може організовуватись підвищений рівень безпеки для окремої віртуальної мережі, які повністю захищають послуги з різними класифікаціями, навіть якщо всі мають однакову фізичну інфраструктуру.

Нарізку можна виконувати за допомогою мережі 4.5G/LTE, але не динамічно. З випуском 17 стандарту 5G, який планується офіційно запуститися в Україні, можна буде створювати наскрізні віртуальні мережі для організації зв'язку спеціального призначення та видаляти їх після завершення, таким чином оптимізуючи використання таких ресурсів, як спектр, пропускна здатність і затримки, а не пов'язувати їх із службами, які не використовуються. Інтенційно-орієнтована мережа подвійного призначення з віртуальним розділенням інфраструктури показана на рис.4.45.

Рис.4.45. Інтенційно-орієнтована мережа подвійного призначення з віртуальним розділенням інфраструктури

Кожен логічний сегмент мережі можна швидко налаштувати для підтримки операційних вимог з використання IBN контролера. Існує велика різноманітність варіантів використання. На військово-морських базах інтенційно-орієнтовані 5G мережі можуть забезпечувати відео- та тактильний зворотний зв'язок з віддаленими операторами кранів і порталів, які завантажують і розвантажують судна. Такі мережі можуть дати точне розташування транспортних засобів і активів і відстежувати логістичні операції. Кораблі можуть розпочати завантаження даних до того, як вони стикуються, використовуючи 5G для підключення даних.

Висока пропускна здатність і надзвичайно низький час відгуку 5G дають змогу ширше розгортати віртуальну та доповнену реальність усередині та на вулиці, поблизу об'єктів і на місцях. Це може уможливити кілька випадків використання, включаючи навчання персоналу та обмін інформацією в реальному часі для покращення обізнаності про ситуацію. 5G також може підтримувати відео високої роздільної здатності (8K) для дистанційного керування транспортними засобами та дронами, а також малопотужні датчики для широкого моніторингу навколишнього середовища. Приклад розгортання інтенційно-орієнтованої 5G мережі військового призначення показано на рис.4.46.

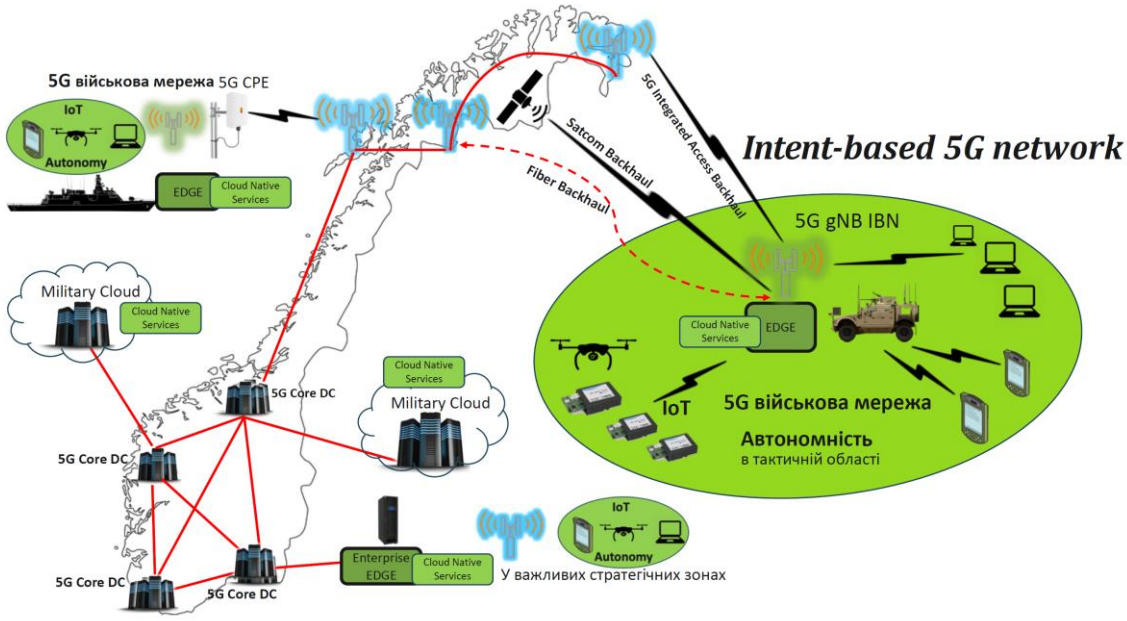


Рис.4.46. Приклад розгортання інтенційно-орієнтованої 5G мережі військового призначення

Проте забезпечення параметрів продуктивності конкретного наскрізного сегмента мережі не є просто функцією радіомережі 5G. Слайс – це віртуальна мережа, яка з'єднує програми, які працюють у хмарі, з пристроями та користувачами. Управління віртуальними сегментами повинно мати можливість взаємодіяти з радіо, транспортними та основними сегментами, щоб забезпечити необхідний рівень продуктивності в усій мережі. Зокрема, базова

транспортна мережа повинна також гарантувати, що пропускна здатність і продуктивність мережі та затримки на наскрізному каналі відповідають вимогам радіомережі [134].

З сучасними транспортними архітектурами таке розгортання мережевих ресурсів на вимогу через IP, супутникову, наземну та підводну оптичну мережу неможливе через відсутність рівня програмної конфігурації. Наприклад, для налаштування наскрізного сегмента мережі з сучасною технологією віртуальної приватної мережі знадобляться дні або навіть місяці.

Крім того, у міру зростання оборонної транспортної мережі зростають і проблеми оперативного управління. Цифрові послуги, які працюватимуть у розподіленій хмарній інфраструктурі, будуть множитися, створюючи величезний обсяг трафіку та вимагаючи значного збільшення кількості та потужності мережевих вузлів. Це підвищить складність мережі, створить експлуатаційні проблеми, щоб гарантувати продуктивність і надійність, необхідні всім цим додаткам, і ускладнить налаштування вручну.

Відповідно, налаштування наскрізного сегмента на різних транспортних рівнях має виконуватися в автоматизований спосіб, щоб повідомити вимоги до продуктивності для даного сегмента мережі і всім різним вузлам на кожному мережевому рівні та забезпечити реалізацію початкового наміру.

Після того, як віртуальний сегмент створений і всі базові мережеві ресурси розподілені, також необхідно проводити постійні вимірювання з використанням даних моніторингу, щоб гарантувати, що кожен рівень мережі продовжує працювати в межах допустимих вимог. В умовах погіршення продуктивності мережі, яке призводить до погіршення вимог QoS конкретного сервісу, мережа повинна мати можливість отримати доступ до нових ресурсів, таких як резервні схеми або нові віртуальні ресурси обробки, щоб забезпечити виконання організації критично важливої місії.

Автоматизація IBN мережі не тільки дає змогу підтримувати послуги та віртуальні сегменти мережі на вимогу, але й підвищує рівень ефективності для

розвитку навичок, знижуючи потребу в інформаційно-технологічному персоналі для участі у складній мережевій інженерії. А також знижує загальні витрати на експлуатацію, доставку, оптимізацію та забезпечення послуг.

Оскільки архітектура цифрового захисту стає складною, оборонні організації починають усвідомлювати, що настав час коли краще автоматизувати свою транспортну мережу для 5G використовуючи технологію інтенційно-орієнтованих мереж .

Перед майбутніми інтелектуальними системами зв'язку п'ятого покоління та шостого покоління (5G/6G) стоїть завдання підтримки широкого спектру додатків, таких як мобільний широкосмуговий та масовий машинний зв'язок, критично важливі програми, а також традиційна передача голосу та даних. Очевидно, що єдина мережева структура не може одночасно задовольняти диференційовані вимоги цих додатків. Щоб упоратися з цією різноманітністю, створення мережної інфраструктури, специфічної для кожного випадку, є простим рішенням. Проте значні експлуатаційні та капітальні витрати, а також складність обслуговування є економічно невигідними для постачальників послуг. Концепція нарізки мережі (NS) розглядається як ефективне рішення задоволення різноманітних вимог додатків у мережах 5G/6G. Шляхом нарізки фізичної інфраструктури створюється кілька наскрізних логічних мереж (E2E), що дають змогу операторам надавати відповідні послуги паралельно, управлятися незалежно і розгортатись на вимогу. Кожен логічний зріз відповідає абстракції підмножини мережевих ресурсів фізичної інфраструктури. Наприклад, один мережевий зріз призначений для додатків доповненої реальності з наднадійним з'єднанням з низькою затримкою, а інший зріз - для послуг відео на запит із надзвичайно високою пропускною здатністю.

У дисертаційній роботі розроблено інтелектуальну систему нарізки мережі на основі намірів [135], яка може ефективно розділяти та керувати ресурсами основної мережі та мережі радіо доступу (RAN) 5G/6G [136]. Це автоматизована система, де користувачам просто потрібно надати конфігурації

мережі вищого рівня у вигляді намірів/контрактів для мережевого фрагмента, а система відповідно розгортає та налаштовує запитувані ресурси. Крім того, система забезпечує автоматизацію процесу налаштування мережі та зменшує ручні зусилля для IT-операторів. Важливим елементом для архітектури даної мережі є контролер, який може належним чином контролювати, керувати та відстежувати ресурси мережевого слайсу на основі намірів (IBN) користувачів. Крім того, для управління мережевими ресурсами використовується SDN/NFV технології та новітні моделі штучного інтелекту, а також пропоновані модулі у роботі: як QoE моніторинг, QoE маршрутизація та хендовер.

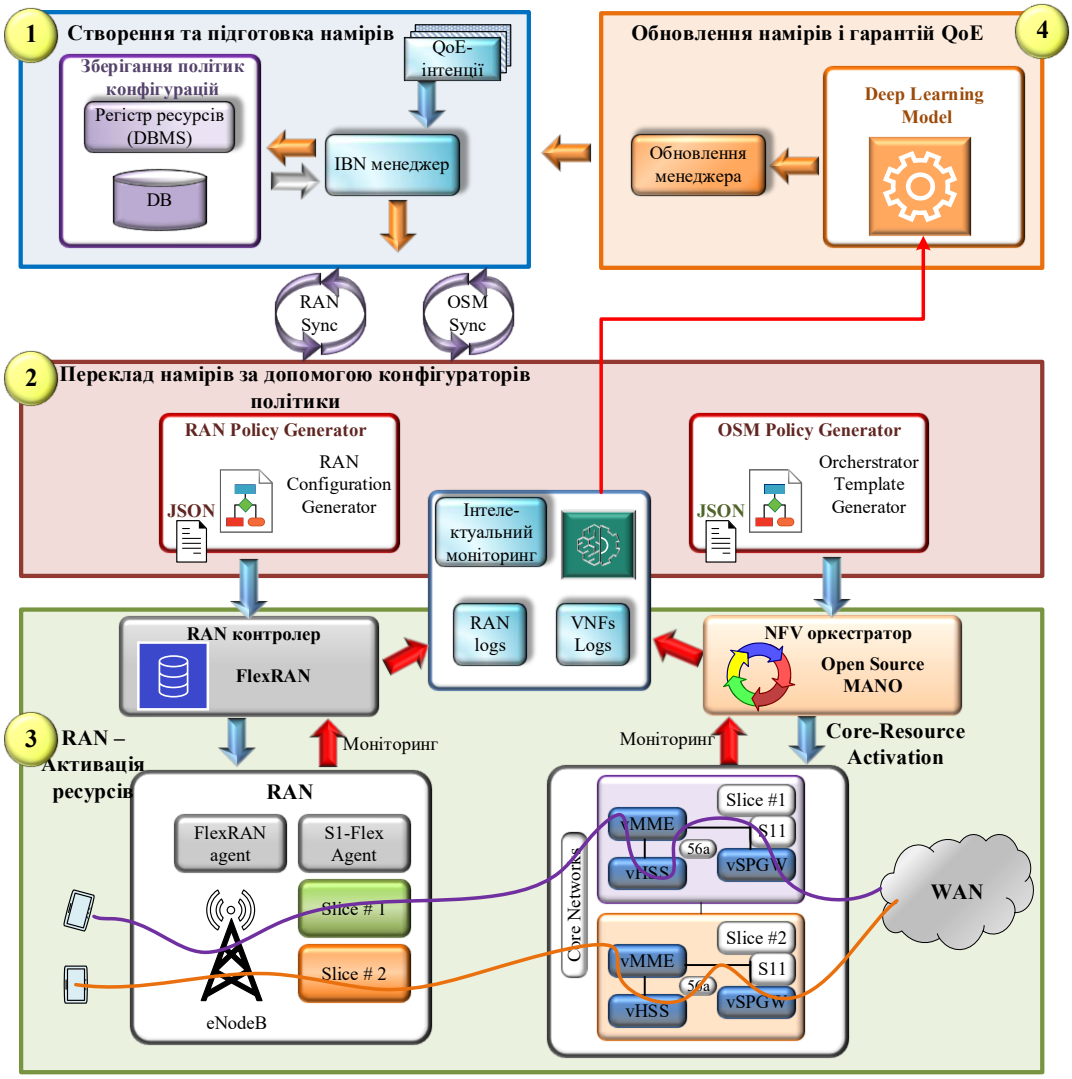


Рис.4.47. Структурно-функціональна схема інтелектуальної мережі подвійного призначення шляхом логічного розділення мережевої інфраструктури

Інтелектуальна система мережевого слайсингу на основі намірів включає чотири основні модулі: контролер/менеджер IBN, Network Orchestrator та Open-Source Mano (OSM), контролер мережі радіо доступу (RAN) і модуль машинного навчання. Ця система може виконувати розділення фізичної інфраструктури на віртуальні E2E як для транспортної мережі, так і для мережі радіодоступу. Майбутні інтелектуальні мережі 5G/6G вимагатимуть наявності автоматизованої системи керування для створення, видалення та оновлення віртуальних мереж на вимогу, надаючи лише конфігурації абстрактного рівня. Таким чином, наша система може автоматизувати процедуру створення зрізу мережі за допомогою інструменту IBN та підтримувати в межах окремої віртуальної мережі запропоновані вище методи підвищення якості сприйняття послуг на основі замовлених оцінок QoE у вигляді намірів.

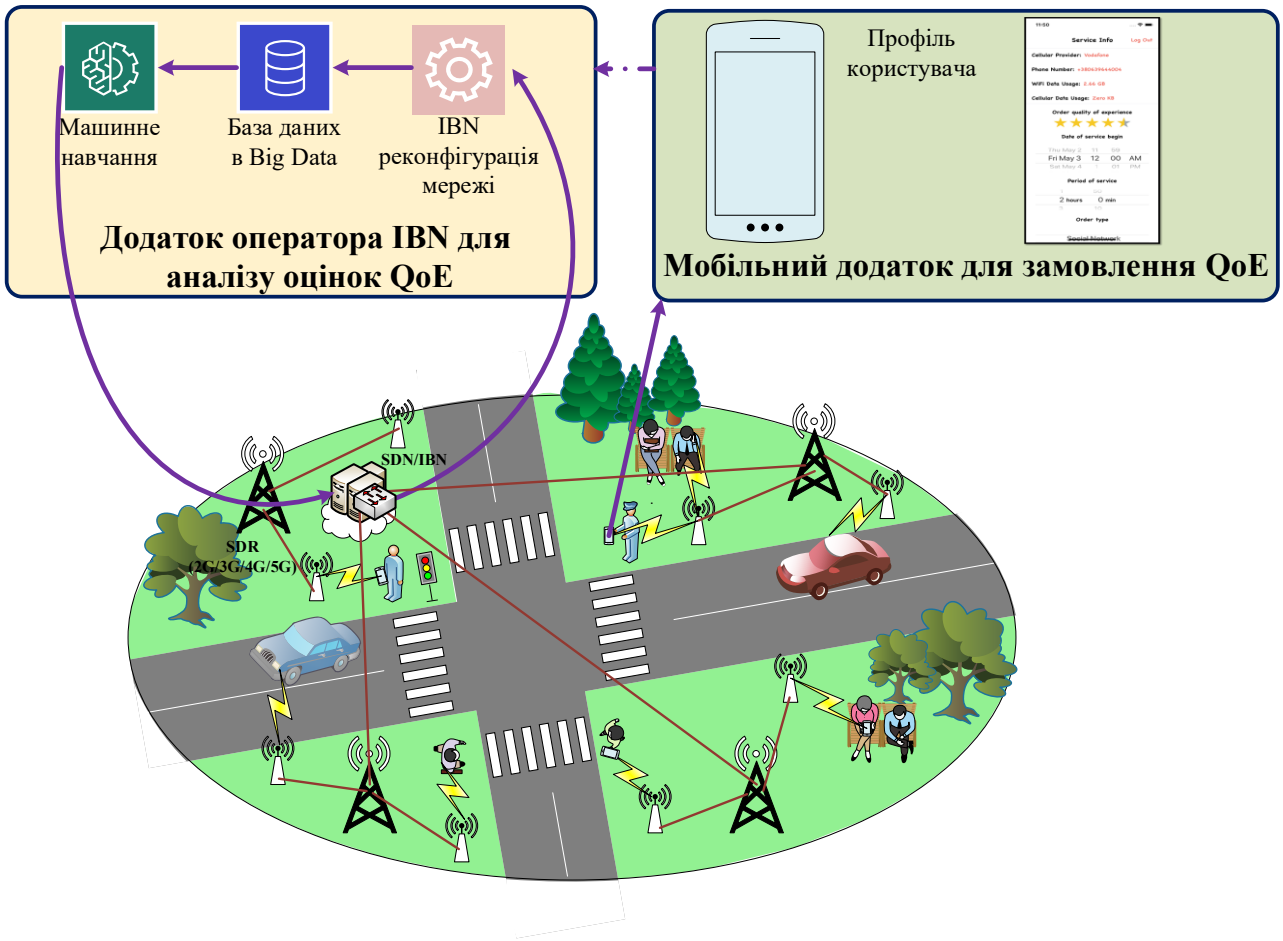


Рис.4.48. Управління якістю обслуговування в гетерогенній інтенційно-орієнтованій мережі на основі мобільного QoE додатку користувачів [137]

Інструмент IBN має можливість приймати високо рівневі конфігурації для віртуальної мережі та генерувати шаблон мережевого фрагмента відповідно до прийнятного формату мережевого оркестратора, наприклад, рядок JSON для оркестратора OSM і файл JSON для контролера RAN. Концепція також містить модуль машинного навчання, який постійно відстежує статистику мережевих ресурсів і зберігає їх у сховищі ресурсів бази даних IBN. Щоразу, коли надходить запит на організацію нової віртуальної мережі інформація спочатку надається модулю машинного навчання, щоб вирішити, чи прийняти запит чи ні, перевіряючи статус RAN і ресурсів основної мережі. Якщо доступно достатньо ресурсів, запит на автоматизоване розгортання мережі успішно приймається, а іншим чином відхиляється.

4.5 Інтелектуальні алгоритми моніторингу та аналізу мережевого трафіку для виявлення мережевих атак в програмно-конфігурованих мережах

Виявлення та класифікація аномалій передбачає безперервний процес моніторингу подій в інформаційних системах і мережах, у зв'язку з чим необхідна обробка великих обсягів даних, що генеруються цими джерелами. Одне з основних обмежень сучасних систем полягає в тому, що вони вимагають тривалого навчання над великими наборами даних, що не завжди можливо в реальних робочих програмах. Для цього використовуються автоматизовані системи виявлення вторгнень у системі DPI. DPI поєднує в собі функціональність системи виявлення вторгнень (IDS) та системи запобігання вторгнень (IPS) із традиційним брандмауером із встановленим станом.

У роботі пропонується алгоритм для DPI системи (4.49), який заснований на глибокому навчанні, що дозволяє вивчати адекватну поведінку мережі та виявляти будь-які аномалії без тривалого навчання на великих наборах даних. Ключовою особливістю запропонованої IDS є оптимальне вилучення сигнатур

для зменшення обчислювальної складності та покращення виявлення раніше невідомих атак.

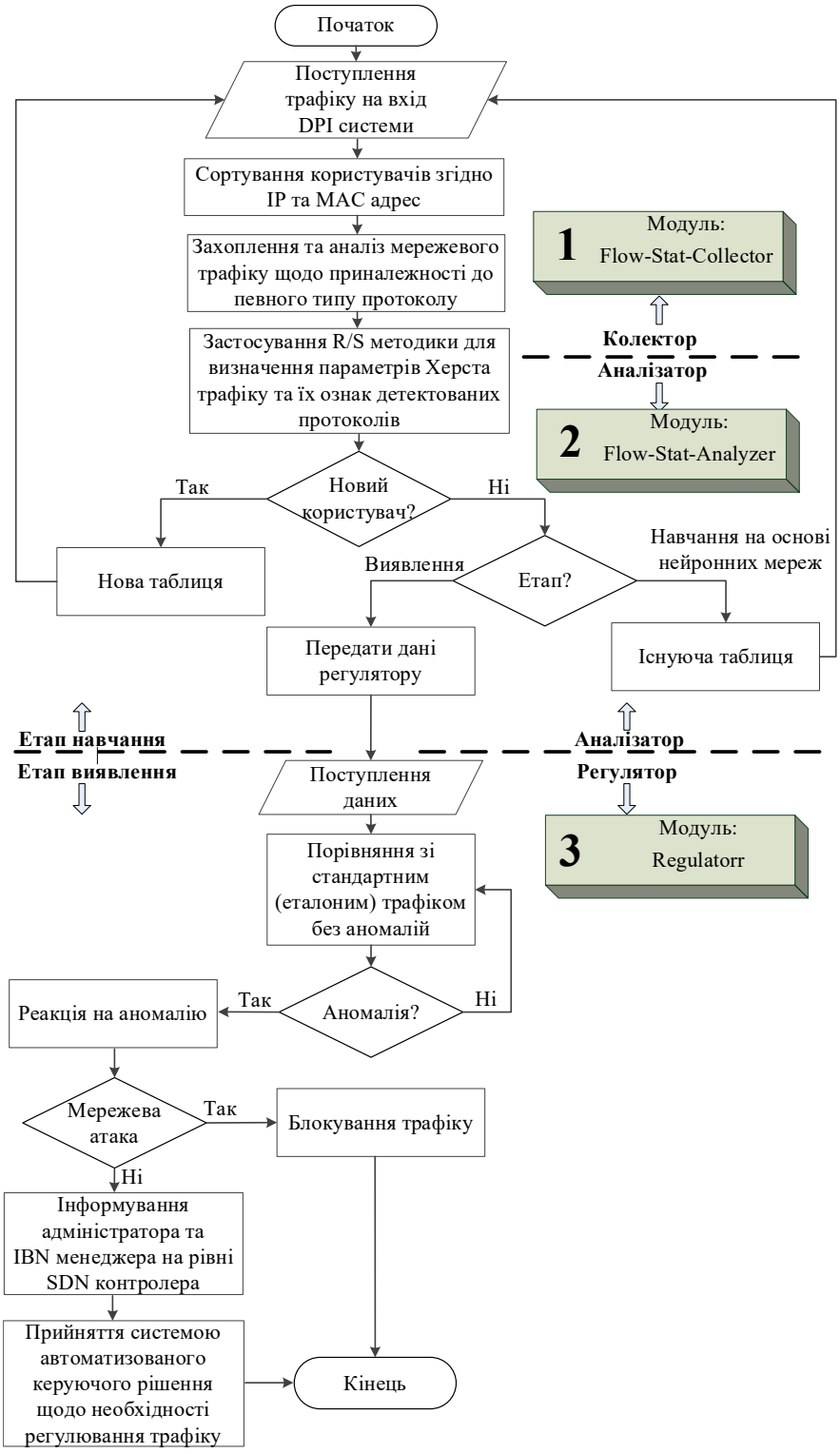


Рис.4.49. Алгоритм системи виявлення та блокування вторгнень на основі глибокого навчання для інтелектуальних програмно-конфігурованих мереж [138]

Запропонований алгоритм може бути реалізований або як самостійне рішення, або як частина більш складної IDS з іншими моделями глибокого навчання та DPI. Продуктивність запропонованої моделі перевіряється на різних наборах даних з точки зору розподілених атак відмови в обслуговуванні (DDoS). Зазвичай рішення на основі глибокого навчання для виявлення атак DDoS базуються на контрольованому навчанні великого набору даних відомих атак із звичайним мережевим трафіком. Ці набори даних складаються з вхідних параметрів, які передаються в глибоку нейронну мережу, а вихідні мітки націлюються, щоб модель могла дізнатися будь-які приховані залежності між входом і виводом. Під час навчання нейронна мережа оцінює різні вхідні характеристики, у тому числі і параметр Херста трафіку в результаті чого прогнозує вихідні значення. Потім вихідні значення порівнюються з цільовими значеннями і обчислюється відповідна функція втрат. З кожною ітерацією процесу навчання (епохи) вага між нейронами оновлюється, щоб зменшити функцію втрат. Цей процес навчання триває до тих пір, поки функція втрат не буде зведена до прийнятного порогу.

Запропонований алгоритм DPI системи складається з трьох модулів, розміщених у контролері інтелектуальної мережі. Ці три модулі описані нижче:

1. Модуль Flow-Stat-Collector відповідає за збір статистичних даних про потоки з таблиць потоків комутаторів OpenFlow і зберігає їх у базі даних статистики потоку (FSD). FSD зберігає статистику активних потоків, таких як кількість пакетів, кількість байтів, тривалість потоків, IP-адреси джерела-призначення та номери портів, і періодично оновлює їх новою статистикою потоку. Ці статистичні дані потоку можуть бути використані для виявлення потенційних DDoS-атак. Модуль Flow-Stat-Collector збирає дані з комутаторів через захищений канал і надсилає їх до модуля Flow-Stat-Analyzer.

2. Модуль Flow-Stat-Analyzer запускає алгоритм виявлення статистичної аномалії та виконує аналіз зібраних даних, що зберігаються в базі даних FSD.

Це найважливіший крок, оскільки контролеру потрібно з’ясувати, чи є атака, чи це законний трафік. Цей модуль додатково розділений на два компоненти. Перший компонент Analyzer 1 видає попередження про підозрілий трафік, коли інтенсивність трафіку перевищує поріг контролю. Подальший аналіз проводиться другим компонентним Аналізатором 2, щоб з'ясувати, чи відповідає даний шаблон трафіку законному трафіку або DDoS-атаці в даному випадку може відбуватися навчання та порівняння еталону за певними сигнатурами. Якщо відбувається атака, Flow-Stat-Analyzer видає попередження модулю Regulator Attack.

3. Регулятор атаки негайно вживає заходів після отримання попередження. Regulator формує правила OpenFlow до комутаторів на основі типу атаки. Ці правила можуть варіюватися від зниження трафіку атаки до дозволу законного трафіку з певними IP-адресами джерела або призначення.

Для прикладу розглянемо режим виявлення атак типу SYN механізм виявлення визначає закономірності траіфку аномалій як ознаки атак за параметром Херста. Механізм виявлення поділяється на три фази виявлення атак. Перша фаза виявлення атак використовує вимірювання статистики трафіку на основі вікон часових рядів. Алгоритм виявлення постійно контролює швидкість надходження пакетів SYN у кожне фіксоване вікно розміром Δw та оцінює параметр Херста трафіку після чого порівнює його з пороговим значенням в кінці кожного часового вікна. Алгоритм виявлення швидко видає попередження, коли швидкість пакетів SYN перевищує порогове значення. Однак сплеск законного трафіку також може збільшити швидкість SYN-пакетів, що надходять на контролер. Таким чином, на другій фазі виявлення атак, подальший аналіз проводиться шляхом порівняння вихідних IP-адрес усіх потоків до бази даних, що містить дійсні IP-адреси джерела. Інформаційні потоки, що мають певну відповідність, вважаються законними. Після цього контролер переходить до третьої фази, де обчислює відношення однопакетних потоків до загальної кількості потоків і порівнює це відношення з

пороговою величиною. Ідея використання одиночних пакетних потоків для виявлення атак виникла в [139], в якій автор зауважив, що потоки, що містять менше 3 пакетів, є аномальними, отже, можуть бути генеровані DDoS-атакою. У нашому методі виявлення потоки, що містять один пакет, вважаються аномальними, оскільки в DDoS-атаках з підробленими адресами, наприклад атаки потоку SYN, генерується лише один пакет на потік. Якщо протягом трьох послідовних вікон коефіцієнт відсотка перевищує поріг, оголошується атака SYN, і контролер вживає відповідних заходів.

Для виявлення DDoS є два основних параметри: розмір вікна Δw та пороги параметра Херста. У роботі прийнято, що розмір вікна є фіксованим. Розмір вікна моніторингу впливає на роботу алгоритму виявлення. Якщо розмір вікна занадто великий, система буде повільно реагувати на атаки. Якщо розмір вікна замалий, не буде достатньо зібраних зразків даних для точного аналізу трафіку. Крім того, він також використовує більшу пропускну здатність і вимагає більше обробних ресурсів. У цій роботі вибрано розмір вікна 3 секунди. Здається, це значення забезпечує хороший компроміс.

Запропонований алгоритм виявлення вимагає двох адаптивних порогів. Замість використання заздалегідь визначених порогових значень, алгоритм виявлення адаптивно обчислює порогові значення. Ці порогові параметри можуть бути налаштовані адміністратором мережі для адаптації до мінливих умов трафіку в мережі. Для того, щоб зробити порогові значення адаптивними до характеристик трафіку мережі, ми будемо використовувати середнє та стандартне відхилення параметрів трафіку та оцінювати за R/S методикою параметр Херста для виведення відповідних порогових еталоних значень. Для обчислення середнього та стандартного відхилення контролер збирає конкретні параметри трафіку у кожному вікні та використовує для їх обчислення.

На першій фазі виявлення алгоритм виявлення безперервно відстежує кількість SYN-пакетів, що надходять до контролера, у трисекундне вікно і підраховує кількість SYN-пакетів. Нехай Xn - кількість пакетів SYN, що

надійшли у вікно nth, тоді алгоритм оновлює середнє та стандартне відхилення в кінці вікна using, використовуючи такі рівняння:

$$Mean = EWMA = \bar{X}_n = \bar{X}_{n-1} + \alpha(X_n - \bar{X}_{n-1}) \quad (4.4)$$

$$Std.Dev. = EWMSTD = S_n = \sqrt{\alpha * (X_n - \bar{X}_{n-1})^2 + (1-\alpha) * (S_{n-1})2} \quad (4.5)$$

де параметр налаштування $0 < \alpha \leq 1$, це коефіцієнт згладжування. Вибір значення α має значний вплив на ефективність виявлення. Значення $\alpha = 1$ надає більшу вагу останнім даним і меншу вагу старим даним; невелике значення α надає більшої ваги старим даним. У роботі приймемо значення α 0,5, що надає однакову вагу поточним та минулим даним. $\bar{X}_n$ та S_n це середнє та стандартне відхилення, розраховане відповідно у вікні n^{th}.

Динамічний поріг δ_n, обчислений у вікні n^{th}, встановлюється відповідно до рівняння (4.6):

$$\delta_n = \bar{X}_n + kS_n \quad (4.6)$$

Де параметр налаштування k є константою. Вибір k являє собою компроміс між хибнопозитивним та помилково негативним. Більше значення k збільшує частоту хибнонегативних, тоді як менше значення k збільшує частоту хибнопозитивних. У роботі для k встановлено значення 1. Для цього вибирається невелике значення, оскільки воно використовується на першій фазі виявлення. Будь-які помилкові спрацьовування, введені на цій стадії, можуть бути виправлені на пізніших етапах виявлення. З іншого боку, вибираючи меншу величину, алгоритм може виявити атаку раніше і скоротити коефіцієнт помилково негативних наслідків [140].

Для того, щоб отримати другий поріг, який алгоритм виявлення використовує на третій фазі виявлення, система виявлення шукає потоки з одиночними пакетами даних. Визначимо параметр Pr як відношення кількості однопакетних потоків до загальної кількості потоків. Нехай C_{Single} - кількість

однопакетних потоків, а C_{Total} загальна кількість потоків. Потім коефіцієнт відсотка (Pr) обчислюється за допомогою рівняння 4.7:

$$\Pr = \left(\frac{C_{Single}}{C_{Total}} \right) * 100 \tag{4.7}$$

Параметр Pr обчислюється в кінці кожного часового вікна. За допомогою Pr алгоритму виявлення обчислюють середнє та стандартне відхилення для отримання адаптивного другого порогу. Нехай $\Pr_n$ це процентне співвідношення потоків одного пакету у часовому вікні,, тоді алгоритм оновлює середнє та стандартне відхилення в кінці вікна n^{th}, використовуючи такі рівняння:

$$Mean = \overline{\Pr}_n = \overline{\Pr}_{n-1} + \alpha(\Pr_n - \overline{\Pr}_{n-1}) \tag{4.8}$$

$$Std.Dev. = Sr_n = \sqrt{\alpha * (\Pr_n - \overline{\Pr}_{n-1})^2 + (1-\alpha) * (Sr_{n-1\,prev})^2} \tag{4.9}$$

У наведених рівняннях (4.8) та (4.9) $\overline{\Pr}_n$ та Sr_n середнє та стандартне відхилення відповідно.

Другий поріг ϕ_n, обчислений у вікні n^{th}, встановлюється відповідно до наступного рівняння (4.10):

$$\phi_n = \overline{\Pr}_n + Sr_n \tag{4.10}$$

Суть використання параметра Херста у тому, що у процесі дослідження характеристик інформаційних потоків можна знайти унікальний взаємозв'язок між конкретним протоколом, яким передається трафік, і характерним йому параметром Херста. Таким чином, провівши ряд контрольних вимірювань та записавши для кожного користувальницького трафіку певну таблицю, ми можемо робити висновки про нормальність або аномальність трафіку на підставі відстані отриманих фактичних значень параметра Херста від значень еталонного трафіку без аномалії, які заздалегідь навчені та задані у користувач подальших спостереженнях.

У роботі проведено дослідження запропонованого алгоритму виявлення та блокування мережевих атак шляхом програмної реалізації системи DPI. Для цього було вимушено згенеровано мережеву атаку від кінцевого пристрою . Після чого відбувалось захоплення мережевого трафіку від різних користувачів. Зокрема в процесі аналізу мережевого трафіку виявлено шкідливий аномальний трафік, що є одним із різновидів DDoS атак. На рисунку крива зеленого кольору показує замасковану атаку під торент трафік та його основні статистичні характеристики.

Рис. 4.50. Демонстрація процесу роботи алгоритму моніторингу та аналізу мережевого трафіку на етапі виявлення мережевих атак в програмно-конфігурованих мережах [138]

У даному підрозділі проведено повторне дослідження з використанням того ж файлу із тими ж вихідними параметрами моделі, але із увімкнутим режимом блокування трафіку, функцію якого реалізовує модуль регулятора. На рисунку показано проміжок на якому відсутній торрент навантаження. Це повязано із тим, що шкідливий трафік-атака зеленого кольору успішно

заблокована системою. Як бачимо рівень загальних втрат, при навантаженні на вхід інтерфейсу 53.736 Мбіт/с, знизився від 7.19% (в умовах присутності шкідливого трафіку) до 2.2% (в умовах блокування шкідливого трафіку), а характер втрат змінився на стрибкоподібний, а не потоковий.

Рис. 4.51. Демонстрація процесу роботи алгоритму моніторингу та аналізу мережевого трафіку на етапі блокування мережевих атак в програмно-конфігурованих мережах [138]

Якщо порівняти дані отримані у результаті виконаних дій, то очевидно, що при високому навантаженні шкідливого трафіку у каналі доцільно автоматично блокувати цей трафік, щоб забезпечити відповідний рівень QoS іншим потокоам.

Висновки до 4-го розділу

У роботі розроблено модуль для управління процедурою хендовера на основі параметра QoE для інтеграції у безпровідні програмно-конфігуровані мережі. Використання розробленого модуля дає змогу проводити процедуру НО не лише за рівнем потужності сигналу точки доступу, але й з врахуванням

таких параметрів мережі, як затримка та втрати пакетів. Врахування цих параметрів дозволило поєднати хендовер та динамічну QoE-маршрутизацію, для забезпечення високого рівня якості сприйняття. Згідно з отриманих результатів запропонований алгоритм дозволяє швидко реагувати на раптові погіршення у мережі та забезпечувати необхідну якість сприйняття для кінцевого користувача. Проте недоліком даного методу є надлишковість службових даних моніторингової системи у каналах зв'язку між мережевим обладнанням та контролером, відповідно, збільшується навантаження на контролер та мережеве обладнання. Для вирішення даного недоліку у роботі зменшено періодичність вимірювання параметрів каналів зв’язку та проведено інтеграція модуля машинного навчання для передбачення рівня якості сприйняття на основі аналізу параметрів QoS..На основі проведеного дослідження встановлено, що запропоновані рішення для побудови інтелектуальних мереж дають змогу підвищити показник якості сприйняття послуги від QoE-3 до QoE-5.

У роботі для практичної реалізації інтелектуальної мережі нового покоління використано обладнання технології SDN Zodiac, яка, на відміну від пропрієтарних виробників мережевого обладнання є відкритою для модифікацій та дає змогу програмно реалізовувати власні рішення щодо управління ресурсами.

Встановлено, що згідно стратегічного розвитку перспективних інформаційно-комунікаційних мереж створення національної системи зв’язку слід проводити з урахуванням можливості її подвійного призначення. Це дасть змогу використовувати її з метою надання послуг зв’язку для загального, відомчого та спеціального використання. На сьогодні, одним із найважливіших викликів в системі національної безпеки та оборони України, безумовно, є система захисту інформації та кібербезпеки в інформаційно-телекомунікаційних мережах. Загалом система військового зв’язку має завжди бути в постійній готовності до управління військами, мобільною в розгортанні

та зміні топології, стійкою до вогневого, радіоелектронного й кібернетичного впливів противника, забезпечувати визначену пропускну спроможність і надійно захищеною від засобів розвідки противника. Проте на сьогоднішній час більшість інфокомунікаційних мереж, у тому числі військові системи зв'язку побудовані на основі пропрієтарного обладнання, функціонал якого реалізований апаратно, вимагає спеціалізованих знань системного адміністратора та є закритим для внесення змін щодо функціонування мережі напрямленої на потреби користувачів. Відповідно використання технології IBN є доцільним для того, щоб автоматизовано розгортати інформаційні мережі зв'язку подвійного призначення в межах однієї фізичної інфраструктури на основі розробленого мережевого обладнання з підтримкою методу автоматизації процесу декомпозиції структури шляхом віртуалізації ресурсів для організації ізольованих захищених мереж.

Розроблено алгоритми для системи виявлення вторгнень (IDS), заснованих на статистичному аналізі та глибокому навчанні, які спрямовані на виявлення підозрілої поведінки в сучасних та майбутніх програмно-конфігурованих мережах. Запропонований підхід базується на вивченні часових рядів нормальної поведінки мережі та виявляє помітні аномалії мережі., одночасно зменшуючи час навчання на порядок. Дослідження довели що використання запропонованого алгоритму виявлення та блокування шкідливого трафіку дало змогу зменшити на 5% втрати в загальному каналі зв’язку та відповідно для користувачів законного трафіку покращити якість обслуговування та сприйняття послуг.

ОСНОВНІ РЕЗУЛЬТАТИ ТА ВИСНОВКИ

Сукупність наукових положень, сформульованих та обґрунтованих в дисертаційній роботі, становить розв'язок науково-практичного завдання підвищення якості сприйняття послуг в сучасних інфокомунікаційних системах шляхом розробки нових методів інтелектуального моніторингу стану мережі, розподілу мережевими ресурсами та управління якістю обслуговування в умовах адаптації до мінливих вимог користувачів та обмеженості мережевих ресурсів.

Основні результати роботи полягають у наступному:

1. Проведено аналіз основних вимог щодо якості обслуговування в телекомунікаційних мережах. Встановлено, що використання показника QoE може стати однією із ключових функцій контролю якості обслуговування в майбутніх мережах. Хоча QoE залежить від QoS, звичайні методи планування та управління мережею, які покладаються виключно на оптимізацію ключових показників ефективності мережі для покращення якості обслуговування, недостатні для задоволення різноманітних вимог користувачів в парадигмі майбутніх інтелектуальних мереж. Для задоволення динамічних вимог користувачів актуальним завданням є розроблення нових структурно-функціональних моделей побудови програмно-конфігурованих інформаційно-комунікаційних систем та інтелектуальних схем для контролю та управління QoE в майбутніх мережах.

2. Запропоновано концептуальну модель інтелектуальної інтенційно-орієнтованої мережі, що розгортається на основі технології програмно-конфігурованих мереж. Згідно концептуальної ідеології IBN пропонує мережевим адміністраторам простий спосіб вираження бізнес-цілей у вигляді намірів, одним із яких є забезпечення необхідного рівня якості сприйняття сервісів, даючи змогу мережному програмному забезпеченню автоматично досягати поставлених цілей на основі інтелектуального аналізу стану ресурсів та управління трафіком. Дана концепція розробляється для автоматизації та

прискорення розгортання життєвого циклу мережі. Таким чином, IBN включає механізми розпізнавання, розуміння і розширення намірів, які визначають запити щодо якості обслуговування.

3. Розвинуто метод маршрутизації інформаційних потоків для програмно-конфігурованих інтелектуальних мережах. Новизною методу є те, що використовується адаптивна QoE-орієнтована метрика маршруту, яка автоматизовано розраховується контролером програмно-конфігурованої мережі на основі математичної моделі кореляції нормалізованого значення замовленого рівня якості сприйняття сервісу та прогнозованого інтегрального адитивного критерію поточних показників QoS, що дало змогу покращити якість сприйняття послуг в умовах адаптації до мінливих вимог користувачів та обмеженості мережевих ресурсів.

4. Розроблено інтелектуальну систему моніторингу QoE для майбутніх програмно-конфігурованих мереж на основі намірів, яка покращить якість обслуговування кінцевих користувачів і дасть змогу ефективніше використовувати мережеві ресурси. Представлено сучасні методи вимірювання параметрів функціонування програмно-конфігурованої мережі: пропускної здатності, затримки і втрати пакетів. Проведено дослідження для оцінки ефективності запропонованої системи QoE-моніторингу шляхом генерації аудіо- та відеотрафіку в мережі Mininet. На основі досліджень визначено математичну функцію кореляції параметрів QoS/QoE. Розроблено модуль машинного навчання щодо прогнозування рівня якості сприйняття послуг кінцевого користувача, враховуючи такі параметри мережі, як затримка та втрата пакетів для інтеграції в програмно-конфігуровані мережі. Для машинного навчання обрано алгоритм Random Forest, який характеризується високим ступенем точності прогнозування та низькими системними вимогами для обчислення. Впровадження модуля машинного навчання в архітектуру програмно-конфігурованих мереж для системи моніторингу дало змогу до 30% зменшити обсяг сигнального трафіку в каналах зв'язку між мережевим

обладнанням і контролером, а також забезпечити швидше відновлення рівня якості сприйняття в умовах його погіршення.

5. Удосконалено метод динамічного розгортання та міграції віртуальних комутаторів від одного контролера до іншого з врахуванням розподілу навантаження на основі аналізу QoE пріоритетів. Правильний вибір комутатора для міграції є дуже важливим, адже це може критично вплинути на кінцеву якість послуг, що надаються в мережі. Показано поступовий розрахунок міграційних коефіцієнтів та проведено порівняльний аналіз щодо ефективності функціонування за критерієм затримки передавання даних звичайного міграційного методу із запропонованим. За підсумками дослідження встановлено, що запропонований підхід скорочує час обробки пріоритетних послуг. Запропоновано модель побудови гібридної SDN/MPLS транспортної системи для підвищення якості обслуговування в інтелектуальних мережах. Така мережа забезпечує можливість інтелектуальної організації транспортних потоків, що дає змогу більш ефективно використовувати пропускну здатність каналів та підтримувати високу якість обслуговування. =

6. Розроблено унікальний IBN контролер для інтелектуальних програмно-конфігурованих мереж, який забезпечує клієнтам надійне з’єднання. Це досягається створенням інтенцій в мережі, які перетворюють зрозумілий набір команд від користувача в код, який розуміє мережа SDN. Це дає змогу адміністратору відійти від налаштування бажаних результатів у командних рядках, специфічних для пристрою, і замість цього використовувати природну мову або графічний інтерфейс для вираження своїх намірів. Також контролер IBN оснащений політиками та моделями штучного інтелекту (AI), які реалізують можливості, необхідні для прогнозування аналізу стану системи з метою підвищення швидкості реагування на погіршення функціональності мережі. Перевагою є модульність контролера, який можна розгортати для усіх типів програмно-конфігурованих мереж у тому числі для ядра майбутньої мережі 5G/6G. Для забезпечення високої відмовостійкості контролера

розроблено автоматизовану систему відновлення доступності серверів на яких віртуалізуються SDN/IBN контролери, що дало змогу в умовах техногенних та природних катастрофах автоматизовано управляти ресурсами, здійснювати діагностику та відновлювати дані серверної інфраструктури з метою забезпечення безперервності роботи і високої доступності бізнес сервісів.

7. Вперше запропоновано метод ініціації хендоверу в програмно-конфігурованій безпровідній Wi-Fi мережі, який, на відміну від відомих, під час прийняття керуючого рішення щодо вибору точки доступу обслуговування орієнтується на прогнозованому значенні інтегрального критерію QoE сформованого на основі вимірювання параметрів, рівня сигналу, пропускної здатності, втрати даних та затримок у мережі Wi-Fi, що дало змогу покращити якість сприйняття послуг для кінцевих користувачів. Також розроблена QoE-система моніторингу дозволила прогнозувати деградацію значень QoE та запобігти ситуації, коли користувач не задоволений отриманим QoS для адаптивного прогнозування моменту реконфігурації мережі. На основі імітаційної моделі доведено, що запропоновані рішення дозволяють покращити якість надання мультимедійних послуг кінцевим користувачам. Зокрема, комплексне використання QoE-орієнтованих методів маршрутизації та ініціації хендовера дало змогу підвищити від 3.5 до 5 показник якості сприйняття послуг, оціненого за п’ятибальною школою, де вище значення характеризує кращу якість обслуговування

8. Для практичної реалізації інтелектуальної мережі нового покоління використано обладнання технології SDN Zodiac, яке, на відміну від пропрієтарних виробників мережевого обладнання є відкритим для модифікацій та дає змогу програмно реалізовувати власні рішення щодо управління ресурсами. На основі імітаційної моделі доведено, що запропоновані рішення дозволяють покращити якість надання мультимедійних послуг кінцевим користувачам.

9. Сформовано стратегічні напрямки розвитку перспективних інформаційно-комунікаційних мереж подвійного призначення. Відповідно використання запропонованої в дисертаційній роботі ідеології побудови інтелектуальних мереж є доцільним для того, щоб автоматизовано розгортати інформаційно-комунікаційні системи зв'язку подвійного призначення в межах однієї фізичної інфраструктури з допомогою організації віртуальних мереж. Доведено, що автоматизація IBN мережі не тільки дає змогу підтримувати послуги та віртуальні сегменти мережі на вимогу, але й підвищує рівень ефективності розгортання та обслуговування, знижуючи потребу в інформаційно-технологічному персоналі для участі у складній мережевій інженерії. А також знижує загальні витрати на експлуатацію, доставку, оптимізацію та забезпечення послуг. Для підвищення інформаційної безпеки розроблено алгоритм для системи виявлення вторгнень (IDS), що базується на статистичному аналізі та глибокому навчанні, який спрямований на виявлення аномальної поведінки в сучасних та майбутніх програмно-конфігурованих мережах. Запропонований підхід базується на вивченні часових рядів нормальної поведінки мережі та виявляє аномалії мережі, одночасно зменшуючи час навчання на порядок. Дослідження довели, що використання запропонованого алгоритму виявлення та блокування шкідливого трафіку дало змогу зменшити на 5% втрати в загальному каналі зв’язку та відповідно для користувачів законного трафіку покращити якість обслуговування та сприйняття послуг.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. M. Agiwal, H. Kwon, S. Park and H. Jin, "A Survey on 4G-5G Dual Connectivity: Road to 5G Implementation," in *IEEE Access*, vol. 9, pp. 16193-16210, 2021, doi: 10.1109/ACCESS.2021.3052462.

2. F. Karniavoura and K. Magoutis, "Decision-Making Approaches for Performance QoS in Distributed Storage Systems: A Survey," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 8, pp. 1906-1919, 1 Aug. 2019, doi: 10.1109/TPDS.2019.2893940.

3. P. Fazio, F. De Rango and M. Tropea, "Prediction and QoS Enhancement in New Generation Cellular Networks With Mobile Hosts: A Survey on Different Protocols and Conventional/Unconventional Approaches," in *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1822-1841, thirdquarter 2017, doi: 10.1109/COMST.2017.2684778.

4. M. D. Arienzo, "Precise QoS Metrics Monitoring in Self-Aware Networks," *2010 Second International Conference on Advances in System Testing and Validation Lifecycle*, 2010, pp. 120-124, doi: 10.1109/VALID.2010.25.

5. N. Seitz, "ITU-T QoS standards for IP-based networks," in *IEEE Communications Magazine*, vol. 41, no. 6, pp. 82-89, June 2003, doi: 10.1109/MCOM.2003.1204752.

6. S. Jun, K. Przystupa, M. Beshley, O. Kochan, H. Beshley, M. Klymash, J. Wang, D. Pieniak, “A Cost-Efficient Software Based Router and Traffic Generator for Simulation and Testing of IP Network,” *Electronics*, vol. 9, no. 1, p. 40, Jan. 2020, doi: 10.3390/electronics9010040.

7. A. Kirpichnikov and A. Titovtsev, "Practical Recommendations On The Application Of Markov Queuing Models With A Restricted Queue," *2019 3rd School on Dynamics of Complex Networks and their Application in Intellectual Robotics (DCNAIR)*, 2019, pp. 81-82, doi: 10.1109/DCNAIR.2019.8875563

8. M. Beshley, M. Seliuchenko, O. Panchenko, O. Zyuzko and I. Kahalo, "Experimental performance analysis of software-defined network switch and

controller," *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2018, pp. 282-286.

9. R. Simmonds and B. W. Unger, “Towards scalable network emulation”, *Denver, CO*, Jul. 2001, pp. 252–262, doi: 10.1117/12.434401.

10. U. Shirwadkar and N. Chilamkurti, "A Reliable Mechanism to guarantee QoS Over DiffServ using video Differentiator," *TENCON 2006 - 2006 IEEE Region 10 Conference*, 2006, pp. 1-4, doi: 10.1109/TENCON.2006.343859.

11. M. Klymash, B. Strykhalyuk, M. Beshley, T. Maksymyuk, “Research and Development the Methods of Quality of Service Provision in Mobile Cloud Systems”, *IEEE International Black Sea Conference on Communications and Networking - 2014, Odessa, Ukraine - Chisinau, Moldova*, May 27-30, 2014, P. 165-169.

12. D. Doherty, T. Morawski, R. Sackett, B. Tang, Carlos-Urrutia-Valdes and J. Zhao, "Next generation networks - multi-service network design," *Networks 2008 - The 13th International Telecommunications Network Strategy and Planning Symposium*, 2008, pp. 1-14, doi: 10.1109/NETWKS.2008.4763684.

13. L. L. Zhang, B. Beacham, M. R. Hashemi, P. Chow and A. Leon-Garcia, "A scheduler ASIC for a programmable packet switch," in *IEEE Micro*, vol. 20, no. 1, pp. 42-48, Jan.-Feb. 2000, doi: 10.1109/40.820052.

14. Minghai Xu, Zhengkun Mi, Xiaofang Feng and Wenke Xie, "Implementation techniques of IntServ/DiffServ integrated network," *International Conference on Communication Technology Proceedings, 2003. ICCT 2003.*, Beijing, China, 2003, pp. 231-234 vol.1.

15. Y. Bernet et al., "A Framework for Integrated Services Operation over DifIServ Networks", *RFC*, vol. 2998, November 2000.

16. R Braden, L Zbads, S. Berson, S. Herzog and S. Jamin, "Resource ReSerVation Protocol (RSVP) - Functional Specification", *RFC*, vol. 2205, September 1997.

17. N. Rouhana and E. Horlait, "Differentiated services and integrated services use of MPLS," *Proceedings ISCC 2000. Fifth IEEE Symposium on Computers and Communications*, Antibes-Juan Les Pins, France, 2000, pp. 194-199.

18. М. М. Климаш, О. В. Корецький, М. І. Бешлей, В. Б. Янишин, “Дослідження побудови технологічних ресурсів у конвергентній мережі на базі мобільного оператора для надання послуги Triple Play”, *Вісник Національного університету “Львівська політехніка”*, серія “Радіоелектроніка та телекомунікації ”, №. 705, с. 176–183, 2011.

19. B. Moon and H. Aghvami, "RSVP extensions for real-time services in wireless mobile networks," in *IEEE Communications Magazine*, vol. 39, no. 12, pp. 52-59, Dec. 2001.

20. A. Abella, V. Friderikos and H. Aghvami, "Differentiated services versus over-provisioned best-effort for pure-IP mobile networks," *4th International Workshop on Mobile and Wireless Communications Network*, Stockholm, Sweden, 2002, pp. 450-457

21. N. Wang and J. Jiang, "Extending RSVP for QOS Support in Heterogeneous Wireless Networks," *2006 10th IEEE Singapore International Conference on Communication Systems*, 2006, pp. 1-5, doi: 10.1109/ICCS.2006.301481.

22. М. М. Климаш, М. І. Бешлей, Ю. Д. Дещинський, О. М. Панченко, “Розробка методу балансування навантаження в SDN мережах на основі модифікованого протоколу STP,” *Комп’ютерні технології друкарства*, № 2, с. 146-155, 2015.

23. I. Nedyalkov and G. Georgiev, "Performance Comparison of IP Network Using MPLS and MPLS TE," *2021 12th National Conference with International Participation (ELECTRONICA)*, 2021, pp. 1-4, doi: 10.1109/ELECTRONICA52725.2021.9513712.

24. А. А. Терешкевич, А. Н. Зубалов, “Обзор технологии "программно-конфигурируемые сети ПКС/sdn",” *Газовая промышленность*. №12 (746), с. 64-71, 2016.

25. M. Hayes, B. Ng, A. Pekar and W. K. G. Seah, "Scalable Architecture for SDN Traffic Classification," *in IEEE Systems Journal*, vol. 12, no. 4, pp. 3203-3214, Dec. 2018.

26. M. Karakus and A. Durresi, "A survey: Control plane scalability issues and approaches in software-defined networking (SDN)", *Comput. Netw.*, vol. 112, pp. 279-293, Jan. 2017.

27. K. Phemius, M. Bouet and J. Leguay, "Disco: Distributed multi-domain SDN controllers", *Proc. IEEE Netw. Oper. Manage. Symp. (NOMS)*, pp. 1-4, May 2014

28. P. Berde, M. Gerola, J. Hart, Y. Higuchi, M. Kobayashi, T. Koide, et al., "ONOS: Towards an open distributed SDN OS", *Proc. 3rd Workshop Hot Topics Softw. Defined Netw. (HotSDN)*, pp. 1-6, 2014.

29. J. Medved, R. Varga, A. Tkacik and K. Gray, "OpenDaylight: Towards a model-driven SDN controller architecture", *Proc. IEEE Int. Symp. World Wireless Mobile Multimedia Netw. (WoWMoM)*, pp. 1-6, Jun. 2014.

30. S. Lange, S. Gebert, J. Spoerhase, P. Rygielski, T. Zinner, S. Kounev, et al., "Specialized heuristics for the controller placement problem in large scale SDN networks", *Proc. 27th Int. Teletraffic Congr. (ITCs)*, vol. 12, no. 1, pp. 210-218, 2015.

31. M. Hayes, B. Ng, A. Pekar and W. K. G. Seah, "Scalable Architecture for SDN Traffic Classification," *in IEEE Systems Journal*, vol. 12, no. 4, pp. 3203-3214, Dec. 2018.

32. W. Braun and M. Menth, "Software-defined networking using OpenFlow: Protocols applications and architectural design choices", *Future Internet*, vol. 6, no. 2, pp. 302-336, 2014.

33. M. Karakus and A. Durresi, "A survey: Control plane scalability issues and approaches in software-defined networking (SDN)", *Comput. Netw.*, vol. 112, pp. 279-293, Jan. 2017.

34. S. V. Krishna, A. Shrivastava and S. J. Wagh, "SDN in High Performance Computing for Scientific and Business Environment (SBE)," *2017 International Conference on Computational Intelligence in Data Science(ICCIDS)*, Chennai, 2017.

35. W. Wang, Q. Qi, X. Gong, Y. Hu and X. Que, "Autonomic QoS Management Mechanism in Software Defined Network," in *China Communications*, vol. 11, no. 7, pp. 13-23, July 2014.

36. H. Zhou *et al.*, "Improving QoS in SDN with Lossless Multi-Domain Reconfigurations," *2015 IEEE 23rd International Symposium on Quality of Service (IWQoS)*, Portland, OR, 2015, pp. 77-78.

37. Ardiansyah, Y. Choi, M. R. K. Aziz and D. Choi, "Latency Minimization for Energy Internet Communications with SDN Virtualization Infrastructure," *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Beijing, China, 2019, pp. 1-7.

38. D. Erickson, "The beacon OpenFlow controller", *Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw.*, pp. 13-18, 2013.

39. A. Tootoonchian, S. Gorbunov, Y. Ganjali, M. Casado and R. Sherwood, "On controller performance in software-defined networks", *2nd USENIX Workshop Hot Topics Manage. Internet Cloud Enterprise Netw. Services*, 2012.

40. M. Alsaeedi, M. M. Mohamad and A. A. Al-Roubaiey, "Toward Adaptive and Scalable OpenFlow-SDN Flow Control: A Survey," in *IEEE Access*, vol. 7, pp. 107346-107379, 2019.

41. W. Braun and M. Menth, "Software-defined networking using OpenFlow: Protocols applications and architectural design choices", *Future Internet*, vol. 6, no. 2, pp. 302-336, 2014.

42. F. Hu, Q. Hao and K. Bao, "A survey on software-defined network and OpenFlow: From concept to implementation", *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 2181-2206, 4th Quart. 2014.

43. A. Mendiola, J. Astorga, E. Jacob and M. Higuero, "A Survey on the Contributions of Software-Defined Networking to Traffic Engineering," in *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 918-953, Secondquarter 2017

44. Z. Cai and A. Cox, ‘‘Maestro: A system for scalable OpenFlow control,’’ *Rice Univ*., Houston, TX, USA, Tech. Rep., 2011.

45. Z. Guo et al., ‘‘STAR: Preventing flow-table overflow in software-defined networks,’’ *Comput. Netw.*, vol. 125, pp. 15–25, Oct. 2017.

46. Kim, E. et al. “Enhanced Flow Table Management Scheme With an LRU-Based Caching Algorithm for SDN.” *IEEE Access* 5 (2017): 25555-25564.

47. O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani and H. Alsariera, "A Comprehensive Survey: Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-VANET," in *IEEE Access*, vol. 8, pp. 91028-91047, 2020.

48. Ardiansyah, Y. Choi, M. R. K. Aziz and D. Choi, "Latency Minimization for Energy Internet Communications with SDN Virtualization Infrastructure," *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Beijing, China, 2019, pp. 1-7.

49. A. Lara, A. Kolasani, and B. Ramamurthy, “Network innovation using OpenFlow: A survey,” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 493–512, First Qu. 2014.

50. M. Beshley, V. Romanchuk, V. Chervenets and A. Masiuk, "Ensuring the quality of service flows in multiservice infrastructure based on network node virtualization," *2016 International Conference Radio Electronics & Info Communications (UkrMiCo)*, Kiev, 2016.

51. R. Stankiewicz and A. Jajszczyk, “A survey of QoE assurance in converged networks,” *Turk Journal of Electrical Engineering*, vol. 55, no. 7, pp. 1459–1473, 2011.

52. S. Barakovi and L. Skorin-Kapov, “Survey and Challenges of QoE Management Issues in Wireless Networks,” J. Computer Networks and Communication, pp. 1–28, 2013.

53. D. Rivera and A. Cavalli, “QoE-driven service optimization aware of the business model,” 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 725–730, 2016.

54. S. Pezzulli, M. G. Martini and N. Barman, "Estimation of Quality Scores From Subjective Tests-Beyond Subjects’ MOS," in *IEEE Transactions on Multimedia*, vol. 23, pp. 2505-2519, 2021, doi: 10.1109/TMM.2020.3013349.

55. M. Seufert, S. Egger, M. Slanina, T. Zinner, T. Hoßfeld, and P. Tran-Gia, “A Survey on Quality of Experience of HTTP Adaptive Streaming,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 469–492, First quarter 2015.

56. A Survey of Emerging Concepts and Challenges for QoE Management of Multimedia Services,” *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, vol. 14, pp. 2 –28, May 2018.

57. Perez-Chuecos Alcaraz, Pedro Alfonso, “Study on Quality of Service in 4G and 5G networks” (2020).

58. V. Andrushchak, M. Beshley, L. Dutko, T. Maksymyuk, T. Andrukhiv, “Intelligent traffic engineering for future intent-based software-defined transport network,” *Lecture Notes in Electrical Engineering. – 2022. – Vol. 831 : Future intent-based networking. On the QoS robust and energy efficient heterogeneous software defined networks*. – P. 161–181.

59. M. Medvetskyi, M. Beshley and M. Klymash, "A Quality of Experience Management Method For Intent-Based Software-Defined Networks*," 2021 IEEE 16th International Conference on the Experience of Designing and Application of CAD Systems (CADSM)*, 2021, pp. 59-62, doi: 10.1109/CADSM52681.2021.9385250

60. O. Panchenko, A. Polishuk, M. Seliuchenko and M. Beshley, "Method for adaptive client oriented management of quality of service in integrated SDN/CLOUD networks," *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 452-455.

61. A. A. Barakabitze, L. Sun, I.-H. Mkwawa, and E. Ifeachor, “A Novel QoE-Centric SDN-based Multipath Routing Approach of Mutimedia Services over 5G Networks,” *IEEE International Conference on Communications,* May 2018.

62. P. Juluri, V. Tamarapalli, and D. Medhi, “Measurement of Quality of Experience of Video-on-Demand Services: A Survey,” I*EEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 401–418, Firstquarter 2016.

63. W. Robitza, A. Ahmad, P. A. Kara, L. Atzori, M. G. Martini, A. Raake, and L. Sun, “Challenges of future multimedia QoE monitoring for internet service providers,” *Multimedia Tools and Applications*, pp. 1–24, June 2017.

64. V. Joseph and G. de Veciana, “NOVA: QoE-driven optimization of DASH-based video delivery in networks*,” in INFOCOM, 2014 Proceedings IEEE*, 2014, pp. 82–90.

65. A. Yastrebova, R. Kirichek, Y. Koucheryavy, A. Borodin and A. Koucheryavy, "Future Networks 2030: Architecture & Requirements," *2018 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, 2018, pp. 1-8, doi: 10.1109/ICUMT.2018.8631208

66. M. Varela, P. Zwickl, P. Reichl, M. Xie and H. Schulzrinne, "From Service Level Agreements (SLA) to Experience Level Agreements (ELA): The challenges of selling QoE to the user," *2015 IEEE International Conference on Communication Workshop (ICCW)*, 2015, pp. 1741-1746, doi: 10.1109/ICCW.2015.7247432.

67. Schatz, R. *et al.* , “QoE Management for Future Networks”. In: Ganchev, I., van der Mei, R., van den Berg, H. (eds) Autonomous Control for a Reliable Internet of Services. Lecture Notes in Computer Science, vol 10768. Springer, Cham. (2018). https://doi.org/10.1007/978-3-319-90415-3_3

68. A. A. Barakabitze *et al*., "QoE Management of Multimedia Streaming Services in Future Networks: A Tutorial and Survey," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 526-565, Firstquarter 2020, doi: 10.1109/COMST.2019.2958784.

69. Binsahaq, T. R. Sheltami and K. Salah, "A Survey on Autonomic Provisioning and Management of QoS in SDN Networks," *in IEEE Access*, vol. 7, pp. 73384-73435, 2019, doi: 10.1109/ACCESS.2019.2919957.

70. P.-W. Tsai, C.-W. Tsai, C.-W. Hsu and C.-S. Yang, "Network monitoring in software-defined networking: A review", *IEEE Syst. J*., vol. 12, no. 4, pp. 3958-3969, Dec. 2018.

71. C. Yu, J. Lan, Z. Guo and Y. Hu, "DROM: Optimizing the routing in software-defined networks with deep reinforcement learning", *IEEE Access*, vol. 6, pp. 64533-64539, 2018.

72. S. Ren, Q. Feng and W. Dou, "An end-to-end QoS routing on software defined network based on hierarchical token bucket queuing discipline", *Proc. Int. Conf. Data Mining Commun. Inf. Technol. (DMCIT)*, 2017.

73. C. Lin, K. Wang and G. Deng, "A QoS-aware routing in SDN hybrid networks", *Procedia Comput. Sci*., vol. 110, pp. 242-249, Jan. 2017.

74. J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu and Y. Liu, "A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges", *IEEE Commun. Surveys Tuts*., vol. 21, no. 1, pp. 393-430, 1st Quart. 2019.

75. Y.-S. Yu and C.-H. Ke, "Genetic algorithm-based routing method for enhanced video delivery over software defined networks", *Int. J. Commun. Syst*., vol. 31, no. 1, pp. e3391, 2018.

76. C. Yu, J. Lan, Z. Guo and Y. Hu, "DROM: Optimizing the routing in software-defined networks with deep reinforcement learning", *IEEE Access*, vol. 6, pp. 64533-64539, 2018.

77. F. Li, J. Cao, X. Wang and Y. Sun, "A QoS Guaranteed Technique for Cloud Applications Based on Software Defined Networking," in *IEEE Access*, vol. 5, pp. 21229-21241, 2017, doi: 10.1109/ACCESS.2017.2755768.

78. R. Durner, A. Blenk and W. Kellerer, "Performance study of dynamic QoS management for OpenFlow-enabled SDN switches," *2015 IEEE 23rd International Symposium on Quality of Service (IWQoS)*, 2015, pp. 177-182, doi: 10.1109/IWQoS.2015.7404730.

79. S. Zhu, Z. Sun, Y. Lu, L. Zhang, Y. Wei and G. Min, "Centralized QoS *Routing Using Network Calculus for SDN-Based Streaming Media Networks," in IEEE Access*, vol. 7, pp. 146566-146576, 2019

80. S. Fu and F. Wu, “Investigation of multipath routing algorithms in software defined networking,” in Proc. Int. Conf. Green Inform., Aug. 2017, pp. 269-273.

81. B. Yan, Q. Liu, J. Shen, and D. Liang, “Flowlet-level multipath routing based on graph neural network in OpenFlow-based SDN”, *Future Generation Computer Systems*, vol. 134, pp. 140–153, Sep. 2022, doi: 10.1016/j.future.2022.04.006.

82. J. Son, A. V. Dastjerdi, R. N. Calheiros and R. Buyya, "SLA-aware and energy-efficient dynamic overbooking in SDN-based cloud data centers", *IEEE Trans. Sustain. Comput*., vol. 2, no. 2, pp. 76-89, Apr./Jun. 2017.

83. Q. Wu, F. Ishikawa, Q. Zhu and D. H. Shin, "QoS-aware multigranularity service composition: Modeling and optimization", *IEEE Trans. Syst. Man Cybern*. Syst., vol. 46, no. 11, pp. 1565-1577, Nov. 2016.

84. M. Teixeira, R. Ribeiro, C. Oliveira and R. Massa, "A quality-driven approach for resources planning in service-oriented architectures", *Expert Syst*. Appl., vol. 42, no. 12, pp. 5366-5379, 2015.

85. A. Mohsin and N. K. Janjua, "A review and future directions of SOA-based software architecture modeling approaches for system of systems*", Service Oriented Comput. Appl*., vol. 12, no. 4, pp. 183-200, 2018.

86. N. Bessis, X. Zhai and S. Sotiriadis, "Service-oriented system engineering", Future Gener. Comput. Syst., vol. 80, pp. 211-214, Mar. 2018.

87. A. A. Barakabitze et al., "QoE Management of Multimedia Streaming Services in Future Networks: A Tutorial and Survey," *in IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 526-565, Firstquarter 2020, doi: 10.1109/COMST.2019.2958784.

88. N. Barman and M. G. Martini, “QoE Modeling for HTTP Adaptive Video Streaming—A Survey and Open Challenges,” *IEEE Access*, 7, March 2019, pp. 30831 – 30859, doi:10.1109/ACCESS.2019.2901778.

89. T. Hobfeld, R. Schatz, M. Varela and C. Timmerer, “Challenges of QoE management for cloud applications,” *IEEE Communications Magazine*, 50, 4, April 2012, pp. 28 – 36, doi:10.1109/MCOM.2012.6178831.

90. J. Mendoza, I. de-la-Bandera, D. Palacios and A. Herrera-García, "On the Capability of QoE Improvement Based on the Adjustment of RLC Parameters," *Sensors*, 20, 9, April 2020, doi:10.3390/s20092474.

91. S. M. Al-Shehri, P. Loskot, T. Numanoglu and M. Mert, "Common Metrics for Analyzing, Developing and Managing Telecommunication Networks," *arXiv:1707.03290*, July 2017.

92. E. Liotou, D. Tsolkas and N. Passas, "A roadmap on QoE metrics and models," *in 23rd International Conference on Telecommunications (ICT), Thessaloniki*, May 2016, doi:10.1109/ICT.2016.7500363.

93. 5G NORMA, "Deliverable D5.1: Definition of connectivity and QoE/QoS management mechanisms," November 2016.

94. V. A. Machado, C. Natalino, M. Silva and C. R. Frances, "A new proposal to provide estimation of QoS and QoE over WiMAX networks: An approach based on computational intelligence and discrete-event simulation," in *2011 IEEE Third Latin-American Conference on Communications*, Belem do Para, October 2011, doi: 10.1109/LatinCOM.2011.6107419.

95. S. Rivera, H. Riveros, C. Ariza-Porras, C. Lozano- Garzon and Y. Donoso, "QoS-QoE Correlation Neural Network Modeling for Mobile Internet Services," in *International Conference on Computing, Management and Telecommunications*

(ComManTel), Ho Chi Minh City, January 2013, doi: 10.1109/ComManTel.2013.6482369.

96. S. Khatibi, "5G-MONARCH Deliverable D6.1: Documentation of Requirements and KPIs and Definition of Suitable Evaluation Criteria," September 2017.

97. W. Robitza et al., “Challenges of future multimedia QoE monitoring for internet service providers,” *Multimedia Tools and Applications*, 76, 3, November 2017, doi: 10.1007/s11042-017-4870-z.

98. L. Skorin-Kapov, M. Varela, T. Hossfeld and K.-T. Chen, “A Survey of Emerging Concepts and Challenges for QoE Management of Multimedia Services”, ACM Transactions on Multimedia Computing Communications and Applications, May 2018, doi:10.1145/3176648.

99. J. Su, M. Beshley, K. Przystupa, O. Kochan, B. Rusyn, R. Stanisławski, O. Yaremko, M. Majka, H. Beshley, I. Demydov, J. Pyrih and I. Kahalo, "5G multi-tier radio access network planning based on voronoi diagram", *Measurement*, vol. 192, p. 110814, 2022. Available: 10.1016/j.measurement.2022.110814.

100. M. Beshley, N. Kryvinska , M. Seliuchenko, H. Beshley, E. Shakshuki, A. Yasar, “End-to-End QoS “Smart Queue” Management Algorithms and Traffic Prioritization Mechanisms for Narrow-Band Internet of Things Services in 4G/5G Networks,” *Sensors*, vol. 20, no.8, p. 2324, Apri; 2020 doi: 10.3390/s20082324.

101. H. Beshley, M. Beshley, M. Medvetskyi, and J. Pyrih, “QoS-Aware Optimal Radio Resource Allocation Method for Machine-Type Communications in 5G LTE and beyond Cellular Networks”, *Wireless Communications and Mobile Computing*, vol. 2021, pp. 9966366-1–9966366-18, May 2021.

102. M. Beshley, N. Kryvinska, H. Beshley, M. Medvetskyi, and L. Barolli, "Centralized QoS Routing Model for Delay/Loss Sensitive Flows at the SDN-IoT Infrastructure*," Computers, Materials & Continua*, vol. 69, no. 3, pp. 3727–3748, 2021.

103. R. Ferrús, O. Sallent, J. Pérez-Romero and R. Agustí, "Management of Network Slicing in 5G Radio Access Networks: Functional Framework and

Information Models," *Computing Research Repository (CoRR) arXiv:1803.01142*, 2018.

104. X. Shen, J. Gao, W. Wu, K. Lyu, M. Li, W. Zhuang, X. Li and J. Rao, "AI-Assisted Network-Slicing Based Next-Generation Wireless Networks," *IEEE Open Journal of Vehicular Technology*, 1, January 2020, pp. 45 – 66, doi:10.1109/OJVT.2020.2965100.

105. Q.-T. Nguyen-Vuong, N. Agoulmine, E. H. Cherkaoui, and L. Toni, "Multicriteria Optimization of Access Selection to Improve the Quality of Experience in Heterogeneous Wireless Access Networks," *Veh. Technol. IEEE Trans*., vol. 62, no. 4, pp. 1785–1800, 2013.

106. X. Wu, D. C. O'Brien, X. Deng and J. -P. M. G. Linnartz, "Smart Handover for Hybrid LiFi and WiFi Networks," in *IEEE Transactions on Wireless Communications*, vol. 19, no. 12, pp. 8211-8219, Dec. 2020, doi: 10.1109/TWC.2020.3020160.

107. Y. -Y. Li, C. -Y. Li, W. -H. Chen, C. -J. Yeh and K. Wang, "Enabling seamless WiGig/WiFi handovers in tri-band wireless systems," *2017 IEEE 25th International Conference on Network Protocols (ICNP)*, 2017, pp. 1-2, doi: 10.1109/ICNP.2017.8117571.

108. A. Sarma, S. Chakraborty and S. Nandi, "Deciding Handover Points Based on Context-Aware Load Balancing in a WiFi-WiMAX Heterogeneous Network Environment," in *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 348-357, Jan. 2016, doi: 10.1109/TVT.2015.2394371.

109. A. Ahmed, L. M. Boulahia, and D. Gaiti, "Enabling Vertical Handover Decisions in Heterogeneous Wireless Networks: A State-of-the-Art and A Classification*," IEEE Commun. Surv. Tutorials*, vol. 16, no. 2, pp. 776–811, Jan. 2014.

110. M. Kassar, B. Kervella, and G. Pujolle, "Autonomic-oriented architecture for an intelligent handover management scheme," *Proc. 6th Annu. Commun. Networks Serv. Res. Conf. CNSR 2008*, pp. 139–146, 2008.

111. R. P. Ray and L. Tang, “Hysteresis Margin and Load Balancing for Handover in Heterogeneous Network,” vol. 4, no. 4, pp. 231–235, 2015.

112. A. Luntovskyy, M. Beshley, “Designing HDS under considering of QoS robustness and security for heterogeneous IBN,” *Lecture Notes in Electrical Engineering. – 2022. – Vol. 831 : Future intent-based networking. On the QoS robust and energy efficient heterogeneous software defined networks*. – P. 19–37.

113. M. Gharbaoui, B. Martini and P. Castoldi, "Implementation of an Intent Layer for SDN-enabled and QoS-Aware Network Slicing," *2021 IEEE 7th International Conference on Network Softwarization (NetSoft)*, 2021, pp. 17-23, doi: 10.1109/NetSoft51509.2021.9492643.

114. C. E. Rothenberg *et al*., "Intent-based Control Loop for DASH Video Service Assurance using ML-based Edge QoE Estimation," *2020 6th IEEE Conference on Network Softwarization (NetSoft)*, 2020, pp. 353-355, doi: 10.1109/NetSoft48620.2020.9165375.

115. S. Aroussi and A. Mellouk, "Survey on Machine Learning-based QoE-QoS Correlation Models," in *International Conference on Computing, Management and Telecommunications (ComManTel)*, Da Nang, April 2014, doi:10.1109/ComManTel.2014.6825604.

116. W3C, RDF 1.1 Concepts and Abstract Syntax, W3C Recommendation, February 25, 2014

117. W3C, RDF Schema 1.1, W3C Recommendation, February 25, 2014

118. M. Beshley, M. Klymash, H. Beshley, O. Urikova, Y. Bobalo, “Future intent-based networking for QoE-driven business models,” *Lecture Notes in Electrical Engineering. – 2022. – Vol. 831 : Future intent-based networking. On the QoS robust and energy efficient heterogeneous software defined networks*. – P. 1–18.

119. M. Klymash et al., “The researching and modeling of structures of mobile networks for providing of multiservice radio access”, *Proceedings of International Conference on Modern Problem of Radio Engineering, Telecommunications and Computer Science*, Lviv-Slavske, 2012, pp. 281–282.

120. S. Khorsandroo and A. S. Tosun, “An experimental investigation of SDN controller live migration in virtual data centers”, *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, Berlin, 2017, pp. 309–314.

121. M. Pham, “SDN applications – The intent-based Northbound Interface realisation for extended applications”, *2016 IEEE NetSoft Conference and Workshops (NetSoft)*, Seoul, 2016, pp. 372–377.

122. V. Chervenets, V. Romanchuk, H. Beshley and A. Khudyy, “QoS/QoE correlation modified model for QoE evaluation on video service”, *2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)*, 2016, pp. 664–666.

123. K. Phemius and M. Bouet, “Monitoring latency with OpenFlow”, *Proceedings of the 9th International Conference on Network and Service Management (CNSM 2013)*, Zurich, 2013, pp. 122–125, doi: 10.1109/CNSM.2013.6727820.

124. М.Б. Медвецький, М.І. Бешлей, А.І. Прислупський “ Метод управління якістю сприйняття послуг для програмно-конфігурованих мереж заснованих на намірах,” *Infocommunication Technologies and Electronic Engineering = Інфокомунікаційні технології та електронна інженерія* Vol. 1, № 1, с. 76–85, 2021.

125. A. Prislupskiy, M. Beshley, H. Beshley, Y. Pyrih, A. Branytskyy, “QoE-oriented routing model for the future intent-based networking,” *Lecture Notes in Electrical Engineering: Future intent-based networking. On the QoS robust and energy efficient heterogeneous software defined networks,* vol. 831, pp.128–144, 2022.

126. M. Beshley, N. Kryvinska, H. Beshley, M. Medvetskyi, and L. Barolli, "Centralized QoS Routing Model for Delay/Loss Sensitive Flows at the SDN-IoT Infrastructure," *Computers, Materials & Continua*, vol. 69, no. 3, pp. 3727–3748, 2021.

127. M. Beshley, A. Pryslupskyi, O. Panchenko and M. Seliuchenko, "Dynamic Switch Migration Method Based on QoE- Aware Priority Marking for Intent-Based Networking," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, 2020, pp. 864-868, doi: 10.1109/TCSET49122.2020.235559.

128. M. Beshley, A. Pryslupskyi, O. Panchenko and H. Beshley, "SDN/Cloud Solutions for Intent-Based Networking," *2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)*, 2019, pp. 22-25, doi: 10.1109/AIACT.2019.8847731.

129. A. Pryslupskyi, O. Panchenko, M. Beshley and M. Seliuchenko, "Improvement of Multiprotocol Label Switching Network Performance using Software-defined Controller," *2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM)*, 2019, pp. 106-109, doi: 10.1109/CADSM.2019.8779316.

130. W. Song, M. Beshley, K. Przystupa, H. Beshley, O. Kochan, A. Pryslupskyi, D. Pieniak, J. Su, “A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection,” *Sensors*, vol. 20, no. 6, pp. 1637-1–1637-41, March 2020.

131. M. Seliuchenko, M. Beshley, M. Kyryk and M. Zhovtonoh, "Automated Recovery of Server Applications for SDN-Based Internet of Things," *2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)*, 2019, pp. 149-152, doi: 10.1109/AIACT.2019.8847743.

132. M. Beshley, M. Medvetskyi, S. Jun, A. Pryslupskyi, Y. Bobalo and H. Beshley, "QoE-Aware Intelligent Handover Method for Intent-Based Software-Defined Wireless Network," *2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, 2022, pp. 534-538, doi: 10.1109/TCSET55632.2022.9767075.

133. М.Б. Медвецький, М.І. Бешлей, А.І. Прислупський, Г.В. Бешлей “Метод ініціації хендоверу в програмно-конфігурованій безпровідній мережі на основі показника якості сприйняття послуг,” *Infocommunication Technologies*

and Electronic Engineering = Інфокомунікаційні технології та електронна інженерія Vol. 1, № 2, с. 1–10, 2021.

134. В.І. Романчук, М.І. Бешлей, А.І. Прислупський, Г.В. Бешлей, “Метод декомпозиції структури мережного пристрою з віртуалізацією ресурсів,” *Наукові записки Української академії друкарства*, №1(56), с. 31– 42, 2018.

135. V. Romanchuk. M. Beshley, A. Prislupskiy, H. Beshley, O. Panchenko, “Method of multiservice infrastructure decomposition with network resource slicing for IoT,” *Internet of Things (IoT) and Engineering Applications (Canada)*, vol. 3, no.1, pp. 22–23, May 2018.

136. М.І. Бешлей, А.І. Прислупський, Г.В. Бешлей, “Методи розподілу радіоресурсів та балансування навантаження в мережі 5G/NB-IoT для надання критично важливих сервісів Інтернету речей,” *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки*. – Т.32 (71), ч. 1, № 5, с. 36–45, 2021.

137. М.І. Бешлей, А. І. Прислупський, Г. В .Бешлей, “Управління якістю обслуговування в гетерогенній інтенційно-орієнтованій мережі на основі мобільного QoE додатку,” *Проблеми телекомунікацій*, № 1 (28, с. 45–64, 2021.

138. W. Song, M. Beshley, K. Przystupa, H. Beshley, O. Kochan, A. Pryslupskyi, D. Pieniak, J. Su, “A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection,” *Sensors*, vol. 20, no. 6, pp. 1637-1–1637-41, March 2020. (Scopus/Web of Science Q1).

139. N. El Moussaid, A. Toumanari and M. El Azhari, "Security analysis as software-defined security for SDN environment," *2017 Fourth International Conference on Software Defined Systems (SDS)*, 2017, pp. 87-92, doi: 10.1109/SDS.2017.7939146.

140. V. T. Dang *et al*., "SDN-Based SYN Proxy—A Solution to Enhance Performance of Attack Mitigation Under TCP SYN Flood," in *The Computer Journal*, vol. 62, no. 4, pp. 518-534, April 2019, doi: 10.1093/comjnl/bxy117.

Додаток А. Акти впровадження

«ЗАТВЕРДЖУЮ»
Директор
ТзОВ «МаксіТех»

Заблоцький С.О.
“08” 06 2022 р.

АКТ
про використання результатів дисертаційної роботи
Прислупського Андрія Івановича
«Підвищення показників якості сприйняття інфокомунікаційних послуг в інтелектуальних мережах нового покоління»

Даний акт складений про те, що у ТзОВ «МаксіТех» для підвищення ефективності функціонування корпоративної інформаційно-комунікаційної мережі використані результати дисертаційної роботи Прислупського А.І. «Підвищення показників якості сприйняття інфокомунікаційних послуг в інтелектуальних мережах нового покоління», представленої на здобуття наукового ступеня доктора філософії.

Зокрема, представниками компанії ТзОВ «МаксіТех» за згодою автора Прислупського А.І. використано автоматизовану систему відновлення доступності серверів на яких розгортаються SDN/IBN контролер та IoT брокер, що дало змогу в умовах техногенних та природних катастрофах автоматизовано управляти ресурсами, здійснювати діагностику та відновлювати дані серверної інфраструктури з метою забезпечення безперервності роботи і високої доступності бізнес сервісів. А також, використано для корпоративної безпровідної Wi-Fi мережі QoE-орієнтовані методи маршрутизації та ініціації хендовера, що дало змогу підвищити від 3.5 до 5 показник якості сприйняття послуг, оціненого за п’ятибальною школою, де вище значення характеризує кращу якість обслуговування.

Результати експериментальних досліджень, виконаних на виробничих потужностях ТзОВ «МаксіТех», відповідають результатам досліджень, що представлені у дисертаційній роботі, похибка не перевищує 2%.

Директор С.О. Заблоцький

«Затверджую»
Проректор з наукової-педагогічної роботи
Національного університету
«Львівська політехніка»

_____ доц. О.Р. Давидчак
«12» 06 2022 р.

АКТ

про використання результатів дисертаційної роботи Прислупського Андрія Івановича на тему «Підвищення показників якості сприйняття інфокомунікаційних послуг в інтелектуальних мережах нового покоління», у навчальному процесі кафедри телекомунікацій.

Даний акт складений комісією у складі:

- д.т.н., Стрихалюка Б.М., директора Інституту телекомунікацій, радіоелектроніки та електронної техніки;
- д.т.н., проф., Кайдана М.В., декана магістратури Інституту телекомунікацій, радіоелектроніки та електронної техніки;
- д.т.н., проф. Климаша М.М., завідувача кафедри телекомунікацій.

проте, що в навчальному процесі кафедри телекомунікацій використано результати дисертаційної роботи Прислупського А.І «Підвищення показників якості сприйняття інфокомунікаційних послуг в інтелектуальних мережах нового покоління», метод ініціації хендоверу в програмно-конфігурованій безпровідній Wi-Fi мережі, що дає змогу покращити якість сприйняття послуг з боку кінцевих користувачів. Зокрема, результати використані для модернізації курсу лекцій (Лекція 8 «Алгоритми та методи забезпечення мобільному пристрою ефективного та безперервного обслуговування в гетерогенних безпровідних мережах») з дисципліни «Побудова та протоколи гетерогенних мереж мобільного зв'язку» спеціальності 172 «Телекомунікації та радіотехніка». А також використано імітаційну модель інтелектуальної мережі у якій реалізовано метод адаптивного клієнт-орієнтованого управління якістю послуг, що дає змогу досліджувати, як кінцеві користувачі замовляючи необхідну якість сприйняття сервісів впливають на функціональну конфігурацію мережі, а з допомогою машинного навчання реагувати на несприятливі поєднання значень показників якості і попереджати ситуації, коли користувач незадоволений якістю отриманих сервісів для адаптивного прогнозування моменту переконфігурації мережі для (Лабораторна робота 6 «Дослідження та моделювання методу адаптивного клієнт-орієнтованого управління якістю послуг в інтенційно-орієнтованій мережі» з дисципліни «Мережеві інформаційно-комунікаційні технології» спеціальності 126 «Інформаційні системи та технології».

Члени комісії:

_____ Стрихалюк Б.М.

_____ Кайдан М.В.

_____ Климаш М.М.

«Затверджую»
Проректор з наукової роботи
Національного університету
«Львівська політехніка»
д.т.н. І.В. Демидов
«__» _____ 2022 р.

АКТ

про використання результатів дисертаційної роботи Прислупського Андрія Івановича «Підвищення показників якості сприйняття інфокомунікаційних послуг в інтелектуальних мережах нового покоління».

Комісія у складі начальника науково-дослідної частини, д.т.н., Небесного Р.В., заступника начальника планово-фінансового відділу Чулой Т.М., завідувача кафедри телекомунікацій, д.т.н., проф. Климаша М.М., склала цей акт у тому, що у держбюджетній науково-дослідній роботі «Розробка методів та уніфікованих програмно-апаратних засобів для розгортання енергоефективних інтенційно-орієнтованих інфокомунікаційних мереж подвійного призначення» (ДБ/IBN), (№держреєстрації 0120U102201, (2020-2022 рр.)) використані наступні результати дисертаційної роботи Прислупського Андрія Івановича на тему «Підвищення показників якості сприйняття інфокомунікаційних послуг в інтелектуальних мережах нового покоління»:

- програмний контролер для інтенційно-орієнтованої інтелектуальної мережі, який оснащений політиками та моделями штучного інтелекту (AI), використання якого дало змогу реалізувати можливості, необхідні для аналізу стану системи та пошуку оптимізованих операційних дій на основі спостережень із керованого середовища;
- автоматизовану систему відновлення доступності серверів на яких розгортаються SDN/IBN контролер та IoT брокер;
- метод управління якістю сприйняття послуг в програмно-конфігурованих інтенційно-орієнтованих мережах на основі розробленої інтелектуальної QoE моніторингової системи.

Члени комісії:

Небесний Р.В.

Чулой Т.В.

Климаш М.М.

Додаток Б. Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. W. Song, M. Beshley, K. Przystupa, H. Beshley, O. Kochan, A. Pryslupskyi, D. Pieniak, J. Su, “A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection,” *Sensors*, vol. 20, no. 6, pp. 1637-1–1637-41, March 2020. (Scopus/Web of Science Q1).

2. M. Beshley, P. Vesely, A. Prislupskiy, H. Beshley, M. Kyryk, V. Romanchuk, I. Kahalo, “Customer-Oriented Quality of Service Management Method for the Future Intent-Based Networking,” *Applied Sciences*, vol. 10, no. 22, pp. 8223-1– 8223-38, Nov. 2020. (Scopus/Web of Science Q2).

3. A. Prislupskiy, M. Beshley, H. Beshley, Y. Pyrih, A. Branytskyy, “QoE-oriented routing model for the future intent-based networking,” *Lecture Notes in Electrical Engineering: Future intent-based networking. On the QoS robust and energy efficient heterogeneous software defined networks,* vol. 831, pp.128–144, 2022.

4. V. Romanchuk. M. Beshley, A. Prislupskiy, H. Beshley, O. Panchenko, “Method of multiservice infrastructure decomposition with network resource slicing for IoT,” *Internet of Things (IoT) and Engineering Applications (Canada)*, vol. 3, no.1, pp. 22–23, May 2018.

5. В.І. Романчук, М.І. Бешлей, А.І. Прислупський, Г.В. Бешлей, “Метод декомпозиції структури мережного пристрою з віртуалізацією ресурсів,” *Наукові записки Української академії друкарства*, №1(56), с. 31– 42, 2018.

6. М.І. Бешлей, А.І. Прислупський, Г.В. Бешлей, “Методи розподілу радіоресурсів та балансування навантаження в мережі 5G/NB-IoT для надання критично важливих сервісів Інтернету речей,” *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки*. – Т.32 (71), ч. 1, № 5, с. 36–45, 2021.

7. М.І. Бешлей, А. І. Прислупський, Г. В .Бешлей, “Управління якістю обслуговування в гетерогенній інтенційно-орієнтованій мережі на основі мобільного QoE додатку,” *Проблеми телекомунікацій*, № 1 (28, с. 45–64, 2021.

8. М.Б. Медвецький, М.І. Бешлей, А.І. Прислупський, Г.В. Бешлей “Метод ініціації хендоверу в програмно-конфігурованій безпровідній мережі на основі показника якості сприйняття послуг,” *Infocommunication Technologies and Electronic Engineering = Інфокомунікаційні технології та електронна інженерія* Vol. 1, № 2, с. 1–10, 2021.

9. М.Б. Медвецький, М.І. Бешлей, А.І. Прислупський “ Метод управління якістю сприйняття послуг для програмно-конфігурованих мереж заснованих на намірах,” *Infocommunication Technologies and Electronic Engineering = Інфокомунікаційні технології та електронна інженерія* Vol. 1, № 1, с. 76–85, 2021.

Наукові праці, які засвідчують апробацію матеріалів дисертації

10. M. Beshley, M. Medvetskyi, S. Jun, A. Pryslupskyi, Y. Bobalo and H. Beshley, "QoE-Aware Intelligent Handover Method for Intent-Based Software-Defined Wireless Network," *2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, 2022, pp. 534-538, doi: 10.1109/TCSET55632.2022.9767075.

11. C. Wang, L. Yuan, M. Medvetskyi, M. Beshley, A. Pryslupskyi and H. Beshley, "Machine Learning-Enabled Software-Defined Networks for QoE Management," *2021 IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT)*, 2021, pp. 234-238, doi: 10.1109/AICT52120.2021.9628961.

12. M. Beshley, A. Pryslupskyi, O. Panchenko and M. Seliuchenko, "Dynamic Switch Migration Method Based on QoE- Aware Priority Marking for Intent-Based Networking," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, 2020, pp. 864-868, doi: 10.1109/TCSET49122.2020.235559.

13. M. Beshley, A. Pryslupskyi, O. Panchenko and H. Beshley, "SDN/Cloud Solutions for Intent-Based Networking," *2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)*, 2019, pp. 22-25, doi: 10.1109/AIACT.2019.8847731.

14. A. Pryslupskyi, O. Panchenko, M. Beshley and M. Seliuchenko, "Improvement of Multiprotocol Label Switching Network Performance using Software-defined Controller," *2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM)*, 2019, pp. 106-109, doi: 10.1109/CADSM.2019.8779316.