ВСТУП

У сучасному світі стрімкого розвитку цифрових технологій та зростаючої залежності від високошвидкісного мобільного зв’язку, мережі п’ятого покоління (5G) відіграють ключову роль у формуванні нової телекомунікаційної інфраструктури. Вони забезпечують не лише значне збільшення пропускної здатності та швидкості передачі даних, але й створюють умови для функціонування критично важливих сервісів, що вимагають наднизьких затримок та високої надійності. У цих умовах впровадження технологій програмно-визначених мереж (SDN) набуває особливої актуальності, оскільки дозволяє забезпечити гнучке, централізоване та ефективне управління трафіком у складних, багаторівневих середовищах мобільних мереж 5G.

Мобільні 5G-мережі є основою для розвитку сучасних сервісів - від Інтернету речей і промислової автоматизації до телемедицини та систем Smart City. Проте з розширенням спектра їхнього застосування та збільшенням кількості підключених пристроїв виникає нагальна потреба у вдосконаленні механізмів керування мережею. Традиційні архітектури вже не здатні забезпечити необхідну масштабованість і адаптивність, тому саме SDN стає одним із ключових інструментів для оптимізації трафіку, підвищення продуктивності та покращення якості обслуговування користувачів.

Зі зростанням обсягів даних, різноманітності типів трафіку та підвищеними вимогами до стабільності й надійності мережі, виникає необхідність у більш інтелектуальних і динамічних системах керування. SDN дозволяє реалізувати централізоване управління маршрутизацією, автоматизацію мережевих процесів та забезпечувати гнучкий розподіл ресурсів у режимі реального часу, що є критично важливим для мереж 5G. Завдяки відокремленню площини керування від площини даних оператори отримують можливість оперативно реагувати на зміни навантаження та адаптувати мережеву інфраструктуру до поточних потреб.

Проєктування системи для впровадження SDN у мобільних 5G-мережах є актуальним завданням у контексті сучасних вимог до швидкості, надійності та

ефективності управління трафіком. Використання SDN відкриває нові можливості для оптимізації роботи мережевих функцій 5G Core, підвищення їхньої продуктивності та підсилення стабільності мережевих сервісів, особливо у сценаріях з високими навантаженнями.

Основним завданням даної роботи є дослідження та розробка ефективних підходів до гнучкого управління трафіком у мережах 5G із застосуванням SDN-технологій, що дозволить операторам оптимізувати мережеві ресурси та забезпечити високу якість обслуговування для кінцевих користувачів.

Дана робота має важливе значення для подальшого розвитку телекомунікаційної інфраструктури та підвищення ефективності роботи мобільних мереж. Запропоновані підходи сприятимуть удосконаленню методів управління трафіком, підвищенню продуктивності мереж та забезпеченню стабільної роботи критичних сервісів у період активного розвитку цифрових технологій.

Актуальність дослідження також підкріплюється тим, що технології SDN сьогодні впроваджуються у провідних телекомунікаційних компаніях та операторів зв’язку, включно з міжнародними IP-провайдерами. Масштаб сучасних телекомунікаційних мереж, їхня складність та висока інтенсивність трафіку роблять використання SDN та гнучкого управління ресурсами критично важливими елементами у конкурентному середовищі ринку зв’язку.

Мета роботи – дослідження та впровадження програмно-визначених мереж (SDN) у 5G для забезпечення гнучкого та ефективного управління мережевим трафіком.

Об’єкт дослідження – процеси взаємодії мережевих функцій 5G Core та механізмів управління трафіком у мобільних мережах.

Предмет дослідження – методи застосування SDN-технологій для оптимізації, маршрутизації та балансування трафіку в мережах п’ятого покоління.

1 АНАЛІЗ СУЧАСНИХ ТЕХНОЛОГІЙ ПОБУДОВИ МОБІЛЬНИХ МЕРЕЖ 5G

1.1 Еволюційний розвиток систем зв'язку як технологічна передумова для 5G

У кваліфікаційній магістерській роботі здійснено аналіз еволюції поколінь мобільного бездротового зв’язку представлено на рисунку 1.1 - від першого покоління 1G до сучасної технології п’ятого покоління 5G. Для кожного етапу розвитку розкрито його принципові характеристики, технологічні новації та зміни в архітектурі
мереж.

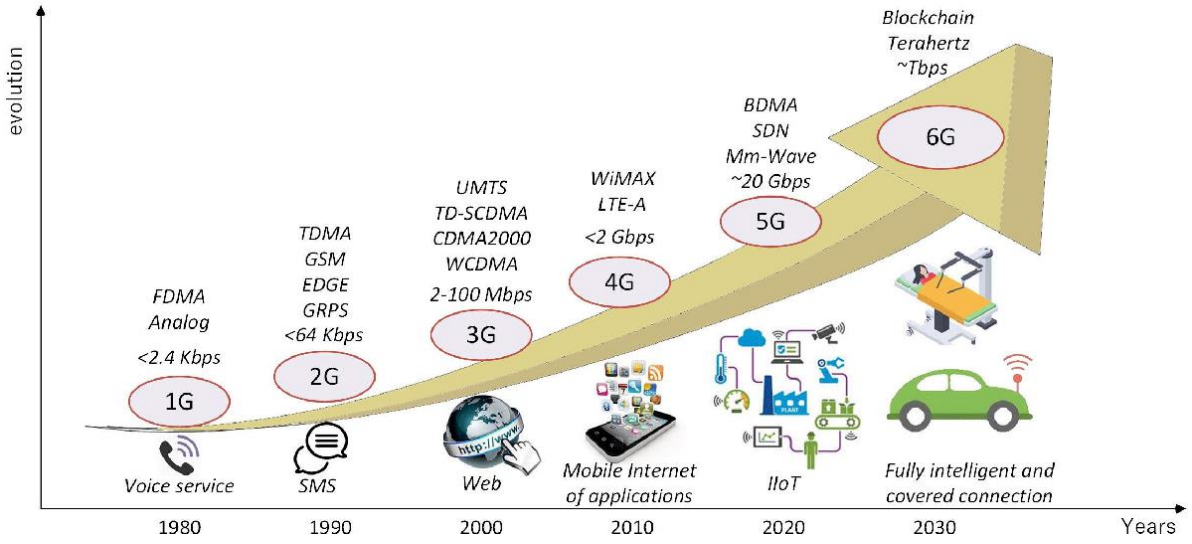


Рис. 1.1 Еволюція мобільного бездротового зв’язку

Початковим етапом становлення стільникового зв’язку стала система 1G, що сформувалася наприкінці XX століття як перше покоління аналогових мереж. Вона функціонувала в аналоговому режимі в діапазоні частот близько 150 МГц, підтримувала виключно голосовий трафік і фактично не передбачала механізмів захисту переданих даних. Таким чином, 1G забезпечувала базову можливість мобільної голосової комунікації, однак не відповідала подальшим вимогам до якості, безпеки та функціональності.

Запровадження мереж другого покоління 2G стало якісним стрибком у розвитку мобільного зв’язку завдяки переходу від аналогового до цифрового способу передавання сигналів. У межах 2G були впроваджені такі стандарти, як GSM (Global System for Mobile Communications) та CDMA (Code Division Multiple Access), що забезпечило шифрування голосових викликів, покращення якості мовлення та можливість передавання коротких текстових і мультимедійних повідомлень (SMS, MMS), а згодом - і простих голосових та графічних сервісів. Подальше збільшення пропускної здатності було реалізовано в проміжному поколінні 2.5G на основі технологій GPRS та EDGE, які надали змогу ефективніше передавати пакетні дані [20].

Перехід до мереж третього покоління 3G став суттєвим проривом у сфері мобільних телекомунікацій. Швидкість передавання даних у 3G-мережах досягла принаймні 2 Мбіт/с, що відкрило можливості для повноцінного доступу до інтернет-ресурсів, відеостримінгу та розвитку IP-орієнтованих сервісів. Стандарти 3G були розроблені та формалізовані в межах організації 3GPP, що забезпечило уніфікований підхід до побудови високошвидкісних і надійних мобільних мереж.

Наступним етапом еволюції стало четверте покоління 4G, яке базується на технології LTE (Long-Term Evolution). Мережі 4G відзначаються істотно більшою шириною смуги пропускання, підвищеним рівнем інформаційної безпеки та можливістю забезпечення високошвидкісного доступу до інтернету. Це дало змогу реалізувати стабільний потоковий перегляд відео у високій роздільній здатності (HD) та досягти швидкостей мобільного доступу до мережі до 1 Гбіт/с.

П’яте покоління мобільного зв’язку 5G визначено в рамках специфікацій 3GPP, починаючи з релізу Release 15, завершеного наприкінці другого десятиліття XXI століття. На відміну від попередніх поколінь, стандарти 5G охоплюють не лише радіодоступ (радіоінтерфейс), а й повний комплекс мережевих протоколів, що регламентують керування сесіями, мобільністю абонентів, наданням послуг та взаємодією обладнання різних виробників. Така всеосяжна стандартизація забезпечила глобальну уніфікацію мобільних технологій: нині сотні операторів експлуатують мережі LTE, а значна їх частина вже впровадила або впроваджує

комерційні рішення на основі 5G.

Розгортання системи 5G відбувається поетапно. Реліз Release 15 заклав першу фазу розвитку, визначивши новий радіоінтерфейс NR, суттєве скорочення затримок, підвищення надійності та запровадження гнучкої, сервісно-орієнтованої архітектури мережі. На відміну від попередніх поколінь, орієнтованих переважно на масового мобільного користувача, 5G спроєктовано як універсальну платформу як для споживчого сегмента, так і для критично важливих промислових застосувань. Це стало можливим завдяки інтеграції низки ключових технологічних підходів:

- віртуалізації мережевих функцій (NFV) та «мережевого нарізання» (network slicing), що дає змогу формувати ізольовані логічні мережі під конкретні сценарії використання;
- обчислень на межі мережі (edge computing), які мінімізують затримку та підвищують ефективність оброблення даних поблизу джерела їх виникнення;
- неназемних мереж (non-terrestrial networks), які забезпечують глобальне покриття за рахунок супутникових та інших позаземних платформ.

Додатковим чинником підвищення пропускної здатності є залучення високочастотного спектра у діапазоні приблизно 30–300 ГГц, що дає можливість досягати швидкостей понад 1 Гбіт/с на обмежених відстанях. Сукупність цих технологічних компонентів формує основу для надання широкого спектра послуг, зокрема:

- розширеного мобільного широкосмугового доступу (eMBB) зі швидкостями до десятків Мбіт/с у зовнішніх умовах та до гігабітних значень у приміщеннях;
- наднадійного зв’язку з малою затримкою (URLLC) із надійністю на рівні 99,9999% та затримкою менше ніж 50 мс;
- масового Інтернету речей (mMTC), здатного підтримувати мільйонні підключення пристроїв на квадратний кілометр.

Гнучкість 5G забезпечується масштабованою модульною архітектурою, можливістю інтеграції з іншими типами мереж, уніфікованими механізмами кіберзахисту та наявністю відкритих програмних інтерфейсів (API) для

розроблення нових сервісів. Перспективи застосування 5G охоплюють практично всі ключові галузі суспільного та економічного життя: концепції «розумного» міста, автономні транспортні системи, логістику, енергетику, медицину, медіа та індустрію розваг, промислову автоматизацію та роботизовані комплекси. Завдяки поєднанню високої швидкості, мінімальної затримки та здатності обслуговувати надвелику кількість підключених пристроїв 5G стає фундаментом для подальшого розвитку Інтернету речей, телемедицини, інтелектуальних транспортних систем і нових бізнес-моделей цифрової економіки [20].

Отже, впровадження технології 5G визначає наступний етап еволюції мобільного зв’язку та створює підґрунтя для формування комплексних комунікаційних рішень майбутніх поколінь.

1.2Архітектура наземних мереж радіодоступу п’ятого покоління

Архітектура мережі 5G розроблена для забезпечення підвищених швидкостей передавання даних, наднизької затримки, масового підключення та підтримки новітніх застосувань, таких як інтернет речей (IoT) і критично важливі сервіси. Вона дає змогу ефективно й масштабовано надавати послуги 5G відповідно до зростаючих потреб користувачів та індустрій.

Архітектуру мережі 5G можна поділити на два основні типи - NSA (Non-Standalone) та SA (Standalone). Архітектура NSA є початковим варіантом розгортання мереж 5G, який використовує наявну інфраструктуру 4G LTE. У режимі NSA технологія 5G NR розгортається паралельно з наявною інфраструктурою LTE, використовуючи LTE як опорну систему для керування сигналізацією. 5G NR відповідає за забезпечення підвищених швидкостей передавання даних, збільшеної ємності та покращеної продуктивності порівняно з LTE [2].

Ядро мережі в архітектурі NSA здебільшого базується на наявному ядрі LTE evolved packet core (EPC). Воно обробляє функції площини керування, зокрема керування мобільністю та керування сеансами, як для з’єднань LTE, так і для 5G

NR. Існуючі компоненти LTE EPC, такі як сутність керування мобільністю (MME) та шлюз обслуговування (S-GW), використовуються для виконання функцій площини керування.

Архітектура SA є повністю незалежним варіантом розгортання мережі 5G, який не покладається на наявну інфраструктуру LTE. Архітектура мережі 5G розроблена для забезпечення підвищених швидкостей передавання даних, наднизької затримки, масового підключення пристроїв та підтримки новітніх застосувань, таких як Інтернет речей (IoT) і сервіси критично важливого зв'язку. Така структура забезпечує ефективну та масштабовану доставку послуг 5G, відповідаючи на зростаючі потреби сучасних користувачів і галузей. Архітектурно 5G може працювати у двох основних режимах розгортання: Non-Standalone (NSA) і Standalone (SA). NSA є початковим етапом упровадження 5G, що базується на наявній інфраструктурі 4G LTE. У цьому режимі 5G New Radio (NR) працює паралельно з LTE, при цьому LTE виконує роль якоря для сигналізації керування. Поки LTE відповідає за керування мобільністю та сесіями, інтерфейс радіодоступу 5G NR забезпечує вищу пропускну здатність, більшу ємність і покращену спектральну ефективність. Ядро мережі NSA використовує LTE Evolved Packet Core (EPC), включаючи наявні мережеві елементи, такі як Mobility Management Entity (MME) і Serving Gateway (S-GW), для підтримки як LTE, так і 5G NR.

На відміну від NSA, архітектура Standalone (SA) є повністю незалежним розгортанням 5G, яке не залежить від LTE. 5G NR виступає основним інтерфейсом радіодоступу, забезпечуючи повний спектр можливостей 5G, включно з високими швидкостями, наднизькою затримкою та підтримкою передових функцій, таких як мережеве нарізання (network slicing), масові комунікації між пристроями (mMTC) та наднадійний зв'язок із низькою затримкою (URLLC). SA упроваджує нове, хмарно-орієнтоване ядро 5G (5GC), яке замінює LTE EPC. До складу 5GC входять ключові функціональні елементи: Access and Mobility Management Function (AMF), Session Management Function (SMF), User Plane Function (UPF) і Network Slice Selection Function (NSSF). Така архітектура забезпечує більш гнучке керування мережею, оптимізовану доставку послуг і динамічний розподіл ресурсів. Хоча NSA

дає змогу швидко розгорнути 5G завдяки використанню інфраструктури LTE, архітектура SA є довгостроковим баченням розвитку 5G, яке розкриває повний потенціал технології. У процесі розширення та зрілості мереж 5G оператори поступово переходять від NSA до SA для підтримки більш розвинених сервісів і підвищення ефективності роботи мережі. У цій роботі далі розглядаються характеристичні можливості обох архітектур - NSA та SA - для визначення різниці між ними [24].

5G non-standalone architecture (NSA). Архітектура 5G NSA є першою версією мережевої архітектури 5G і вважається перехідним етапом до повноцінної мережі 5G, тобто 5G SA. Як випливає з назви, 5G NSA не є автономною - вона розроблена таким чином, щоб розгортатися поверх наявної інфраструктури мереж 4G LTE.

5G NSA дає змогу розгортати радіодоступ 5G (5G RAN) та інтерфейс NR і підключати їх до мережі 4G LTE, тобто використовувати радіодоступ 4G для керування (control plane signalling) та ядро EPC. Як показано на Рис. 1.2, у цій архітектурі радіочастина 5G (NR) не може самостійно підключитися до ядра керування 4G LTE. Замість цього, радіопідсистема 5G залежить від макростільникової базової станції 4G LTE eNodeB (eNB) для всіх сигналів керування, тоді як радіоинтерфейс 5G NR використовується для передачі даних (user plane).

У всьому світі архітектура 5G NSA широко застосовувалася операторами мобільного зв’язку для швидкого й простого надання 5G-послуг кінцевим користувачам. Використовуючи 5G NSA, оператори змогли запустити початкові послуги 5G для своїх клієнтів, паралельно вирішуючи технічні питання в 5G RAN і підтримуючи стабільність решти мережі 4G LTE [4].

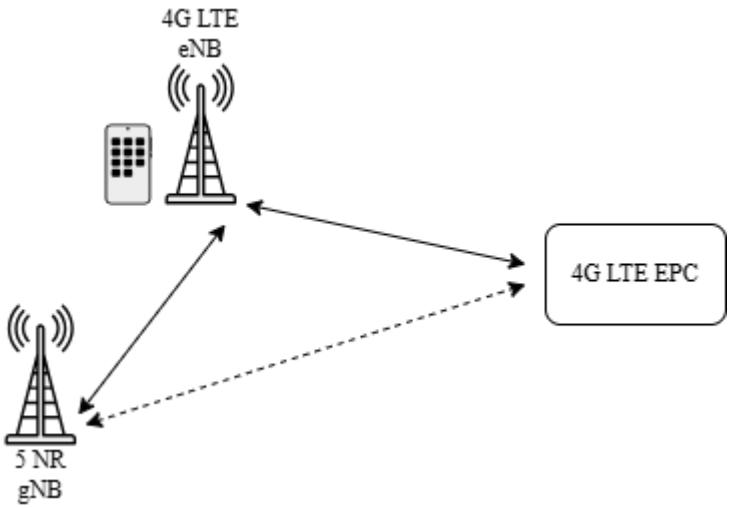


Рис. 1.2 Non-Standalone Architecture (NSA) 5G

Для кінцевих користувачів початковими перевагами використання 5G NSA стали краща зона покриття та вищі швидкості порівняно з послугами 4G LTE.

Таблиця 1.1

Порівняння переваг та недоліків NSA 5G

Переваги	**Недоліки**
Економічність - оскільки мережа 5G базується на існуючій 4G-інфраструктурі, немає потреби інвестувати в дорогий 5G Core.	Нездатність забезпечити низьку затримку, яка є однією з ключових переваг повноцінної мережі 5G.
Простота розгортання - архітектура 5G NSA легко впроваджується, адже оператори знайомі з наявною інфраструктурою та процесом її налаштування.	Вищі енерговитрати, оскільки одночасно використовуються дві мережеві технології - 4G та 5G.
Швидке введення в експлуатацію - завдяки наявній мережі 4G та досвіду роботи з нею, запуск 5G відбувається значно швидше.	Неможливість забезпечити максимальні можливості 5G, особливо на початковому етапі впровадження.

Попри недоліки, режим 5G NSA є оптимальним рішенням для початкового

розгортання послуг 5G у будь-якому регіоні.

5G standalone architecture (SA). Схематично система 5G використовує ті самі елементи, що й попередні покоління: користувацьке обладнання (UE), яке складається з мобільної станції та USIM; мережу радіодоступу (NG-RAN); а також ядро мережі (5GC), як показано на Рис. 1.3 нижче.

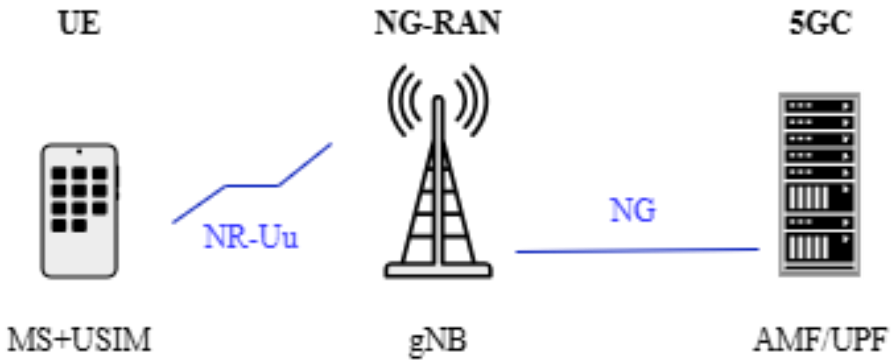


Рис. 1.3 Огляд інфраструктури 5GS

5G є принципово новою архітектурою мобільного зв'язку, яка дозволяє повністю реалізувати всі можливості п'ятого покоління, оскільки не залежить від наявної інфраструктури 4G LTE. Архітектура 5G SA передбачає використання нового пакетного ядра 5G, що дає змогу розгортати 5G-сервіси без потреби у будь-якому попередньому LTE-обладнанні в мережі.

Як показано на Рис. 1.3, у архітектурі 5G SA радіодоступ 5G RAN та інтерфейс New Radio (NR), до складу якого входять базові станції gNodeB (gNB), підключаються безпосередньо до ядра пакетної мережі 5G як повністю автономний елемент мережі.

В архітектурі 5G SA саме ядро 5G відповідає за сигнальний обмін у площині керування, тоді як радіомережа доступу 5G (RAN) забезпечує роботу користувацької (даної) площини, тобто передачу трафіку між пристроєм користувача та мережею. Таким чином, ця архітектура повністю усуває залежність від ядра або радіомережі 4G LTE [4].

Крім того, архітектура пакетного ядра 5G містить багато нових, нативно інтегрованих мережевих функцій та можливостей. Серед них - мережеве сегментування (network slicing), розділення площин керування та користувача

(CUPS), віртуалізація, автоматизація, підтримка багатогігабітних швидкостей та URLLC.

У результаті ядро 5G спеціально розроблене для максимального використання збільшеної пропускної здатності та зменшеної затримки, які забезпечує новий інтерфейс 5G NR. Більш детальну інформацію стосовно переваг та недоліків можна отримати в Таблиці 1.2.

Таблиця 1.2

Порівняння переваг та недоліків SA 5G

Переваги	**Недоліки**
Споживання енергії нижче, ніж у 5G NSA	Дороге впровадження на всіх етапах.
Підтримує широкий спектр сценаріїв використання 5G.	Потребує значного часу для фахівців на освоєння нової інфраструктури ядра.
Забезпечує зменшену затримку.	Складно розгорнути 5G у віддалених або важкодоступних регіонах через обмежену кількість SA-інфраструктури та пристроїв, що підтримують цю технологію.
Дозволяє збільшити пропускні можливості (bandwidth).	
Створює більш потужні, швидкі та масштабовані мережі.	

Core Network (5GC), сервісно-програмна структура. На рисунку 1.4 зображено ядро мережі 5G, що є кардинально новим етапом у порівнянні з попередніми поколіннями мобільних мереж. Сучасні мережі вже не розглядаються лише як канали для передачі даних — вони перетворюються на повноцінну сервісну платформу, що відкриває широкі можливості для монетизації та створення нових послуг [24].

Ядро 5G є програмно визначеним, що дає змогу гнучко розподіляти його функції по різних частинах мережі для забезпечення максимальної продуктивності.

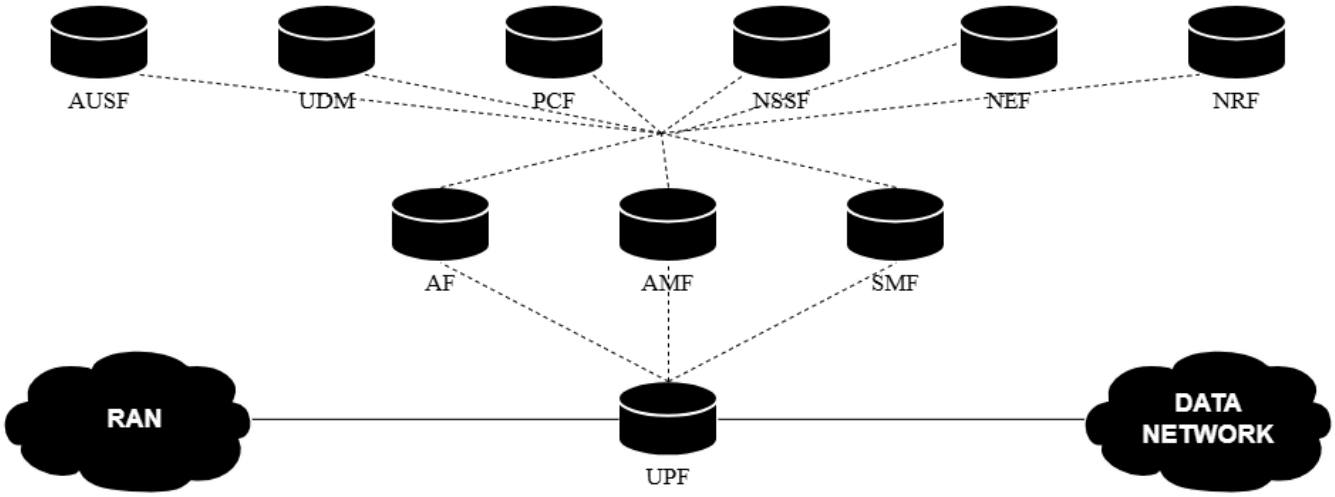


Рис. 1.4 Архітектура 5G core network

AUSF (Authentication Server Function) - AUSF перевіряє вашу ідентичність, щоб переконатися, що вам дозволено доступ до мережі, а також захищає вашу конфіденційність. Він взаємодіє з іншими функціями для забезпечення безпеки. Під час реєстрації саме AMF (Access and Mobility Function) обирає відповідний AUSF.

UDM (Unified Data Management) і UDR (User Data Repository). UDM - це «керівник користувачів». Він перевіряє вашу особу, визначає ваші дозволи та керує доступом. UDR зберігає інформацію про користувачів, якою користується UDM. Для завершення процесу автентифікації ця функція створює відповідні автентифікаційні ключі.

PCF (Policy Control Function) - PCF встановлює правила роботи 5G-мережі. Він допомагає мережі керувати сервісами та монетизацією, контролюючи, хто і що може робити. Policy Control Function спрощує розробку та впровадження політик у 5G-мережі.

NSSF (Network Slicing Selection Function) - 5G може розділяти мережу на окремі частини (слайси) для різних застосувань. NSSF допомагає обрати відповідний слайс для кожного сервісу або застосунку користувача.

NEF (Network Exposure Function) - це стандартизована мережева функція ядра 5G, визначена 3GPP, яка забезпечує уніфікований, захищений та контрольований механізм експонування мережевих можливостей зовнішнім і внутрішнім застосункам. NEF виступає посередником між сервісами ядра 5G та сторонніми системами, включаючи додатки операторів, партнерів і вертикальних індустрій (enterprise).

NRF (Network Repository Function) - Це своєрідна «велика телефонна книга» для всіх важливих компонентів 5G-мережі. Вона допомагає різним частинам мережі знаходити одна одну та легко взаємодіяти. Усі мережеві функції (NF) оператора зберігаються централізовано в Network Repository Function (NRF).

AF (Application Function) у 5G Core - це мережева функція, яка дозволяє зовнішнім або внутрішнім застосункам впливати на роботу мережі через механізми політик та QoS. AF взаємодіє з PCF (Policy Control Function) та/або NEF (Network Exposure Function), передаючи інформацію про сервіс (наприклад, вимоги до QoS, пріоритет трафіку, правила маршрутизації), щоб мережа могла оптимально обслуговувати конкретні додатки чи послуги.

AMF (Access and Mobility Management Function) у 5G Core — це мережева функція, яка відповідає за управління доступом та мобільністю користувача. AMF забезпечує реєстрацію та автентифікацію UE, управління сигналізацією, handover та tracking area updates, а також маршрутизацію сигналізації між UE і іншими функціями ядра. AMF не обробляє користувацькі дані.

SMF (Session Management Function) у 5G Core — це функція керування сесіями користувача (PDU sessions). SMF відповідає за створення, зміну та завершення сесій, призначення IP-адрес, застосування політик маршрутизації та QoS, а також контроль і взаємодію з UPF.

UPF (User Plane Function) у 5G Core — це функція користувацької площини, яка відповідає за передачу та маршрутизацію даних між UE і зовнішніми мережами. UPF виконує застосування QoS, packet forwarding, traffic steering, а також може підтримувати edge computing і оптимізацію трафіку.

Архітектура ядра 5G перевершує попередні покоління завдяки своїй

програмно визначеній природі та побудові на основі сервісно-орієнтованої архітектури (SBA). Такий підхід дозволяє робити ядро 5G розподіленим, хмарно-орієнтованим і гнучко масштабованим. Однією з ключових переваг 5G Core є можливість оптимально розміщувати мережеві функції, що забезпечує максимальну ефективність, високу продуктивність і мінімальну затримку — усе це разом формує найкращий користувацький досвід.

Основні архітектурні принципи ядра 5G включають:

1. SBA: На відміну від точкової (point-to-point) архітектури попереднього ядра EPC з перехресними функціями, 5G Core використовує сервісно-орієнтовану модель з ортогональними функціями, які можуть масштабуватися незалежно одна від одної.
2. Message bus та API: 5G Core значно спрощує інтеграцію нових функцій завдяки концепції «message bus» для взаємодії в площині керування, а також застосовує REST-подібні API на базі HTTP/2, що забезпечують високу гнучкість.

У підсумку, ядро 5G спроєктоване як хмарно-орієнтоване, розподілюване, масштабоване та динамічне. EPC попередніх поколінь не здатне забезпечити такий рівень функціональності та сервісів, як сучасне 5G Core.

Архітектура 5G RAN. 5G RAN складається з кількох протокольних рівнів:

Рівень 3 (Layer 3) протокольного стеку включає:

- RRC (Radio Resource Control) - відповідає за керування радіоресурсами, трансляцію системної інформації, а також встановлення, підтримку та звільнення радіоз'єднання UE.
- NGAP (NG Application Protocol) - забезпечує передачу NAS-повідомлень між UE та пакетним ядром 5G.
- Xn - дозволяє обмінюватися інформацією між двома RAN для швидшого виконання handover.

Рівень 2 (Layer 2) протокольного стеку включає:

- PDCP (Packet Data Convergence Protocol) - забезпечує шифрування даних по повітрю, «якоріння» даних під час handover та дублювання пакетів через кілька радіодоступів для підвищення надійності.

- RLC (Radio Link Control) - відповідає за сегментацію та збирання даних по повітрю, а також за повторну передачу у разі втрати пакетів.
- MAC (Medium Access Control) - реалізує планувальник, адаптацію лінку, керування радіокадрами та механізм HARQ для повторної передачі на рівні блоків [3].

Фізичний рівень (Physical Layer) виконує базові функції обробки сигналу: модуляцію, генерацію хвильової форми, кодування каналу тощо. Згенеровані цифрові сигнали передаються до радіомодуля для передачі по повітрю.

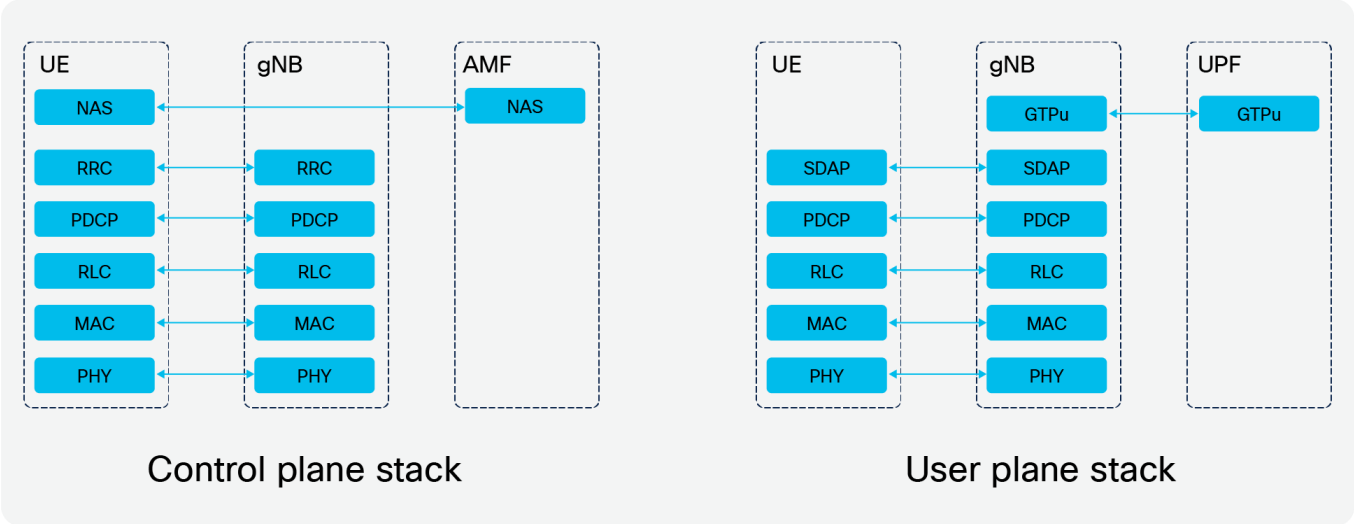


Рис. 1.5 Рівень стеку протоколів доступу 5G

Ранні реалізації стільникових систем інтегрували всі ці рівні, включно з елементами RF, в одному пристрої. Пізніше цифрові радіоінтерфейси дозволили відокремити базову смугу (baseband) від RF-блоку. Це забезпечило більшу гнучкість та спростило встановлення в макромережах та великих будівлях. Піко- та малі коміркові станції (small cells) продовжували використовувати інтегрований підхід з варіантами зовнішніх та внутрішніх антен.

Якщо уважно проаналізувати функціональність кожного рівня стеку, можна побачити, що частину функцій можна централізувати, а решту - розподілити. Такий підхід дозволяє ефективно керувати обчислювальними та спектральними ресурсами відповідно до попиту, зменшувати взаємні перешкоди, підвищувати

пропускну здатність і надійність підключення для кожного користувача та покращувати досвід handover.

Технології MIMO. Технологія MIMO (Multiple Input Multiple Output) є однією з ключових у бездротових комунікаціях, включно з мобільними та Wi-Fi мережами. Вона дозволяє одночасно використовувати кілька антен на передачу та прийом, що підвищує швидкість передачі даних, покращує якість сигналу та знижує затримку.

Основні принципи MIMO

Багатовхідність (Multiple Inputs):

Сигнал передається одночасно через кілька незалежних каналів між антенами. Це дозволяє збільшити пропускну здатність і підвищити надійність мережі.

Просторова множинність (Spatial Multiplexing):

Сигнали передаються в різних просторових напрямках, що зменшує втрати через відбиття та розсіювання, підвищуючи ефективність передачі.

Масивність антен (Antenna Arrays):

Використання масивів антен на передачу та прийом дозволяє ефективніше використовувати просторові ресурси. Більша кількість антен забезпечує отримання більшої кількості незалежних сигналів і покращує якість зв’язку.

Оптимальні алгоритми обробки сигналів:

MIMO застосовує методи просторової обробки сигналів (Spatial Signal Processing) та просторової диверсії (Spatial Diversity) для оптимізації передачі та прийому, що забезпечує стабільний та високошвидкісний канал зв’язку [5].

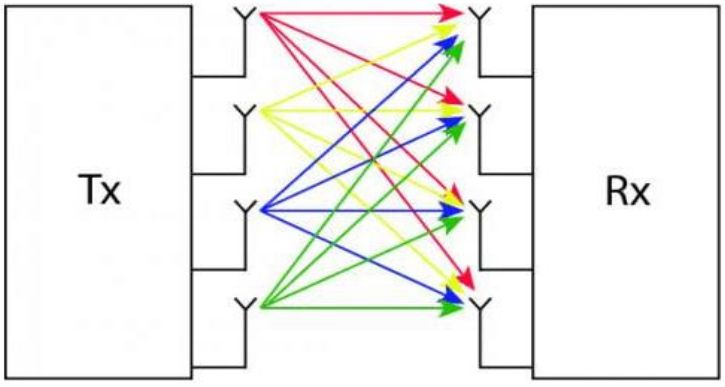


Рис. 1.6 Базова структура технології MIMO

MU-MIMO (Multi-User Multiple Input Multiple Output). MU-MIMO — це передова технологія бездротового зв’язку, яка дозволяє базовій станції або точці доступу одночасно обслуговувати кількох користувачів, передаючи їм окремі потоки даних через різні антенні канали. На відміну від класичного SISO або SU-MIMO (Single-User MIMO), MU-MIMO забезпечує одночасний доступ декількох користувачів, що значно підвищує ефективність використання спектру та пропускну здатність мережі.

Основні характеристики MU-MIMO:

Багатоантенність:

Базова станція оснащена декількома антенами, які можуть незалежно формувати промені для різних користувачів одночасно. Це дозволяє уникати перешкод між користувачами і підвищує якість сигналу.

Розділення потоків даних (Spatial Multiplexing):

Технологія дозволяє одночасно передавати різні потоки даних різним користувачам, оптимально розподіляючи доступний радіочас. Кожен користувач отримує власний незалежний канал, що підвищує загальну пропускну здатність мережі.

Зниження затримок:

Користувачі отримують одночасний доступ до каналу, що зменшує час очікування і затримку передачі даних. Це критично важливо для додатків реального часу, таких як відеоконференції, онлайн-ігри або AR/VR сервіси.

Покращена ефективність мережі:

MU-MIMO дозволяє більш ефективно використовувати наявний спектр і радіо ресурси, підвищуючи пропускну здатність і стабільність з’єднань для всіх користувачів у зоні покриття [5].

Сумісність з іншими технологіями:

MU-MIMO може інтегруватися з Beamforming, Massive MIMO та технологіями адаптивної модуляції, що дозволяє ще більше підвищити продуктивність мережі і стійкість сигналу в умовах багатопроменевої передачі.

Massive MIMO. Massive MIMO є еволюційним розвитком концепції MIMO і MU-MIMO. Вона передбачає використання великої кількості антен на базовій станції (десятки або сотні антен), що дозволяє одночасно обслуговувати багатьох користувачів і досягати екстремально високої пропускної здатності та енергоефективності.

Ключові аспекти технології Massive MIMO:

Велика кількість антен (Antenna Array):

Використання десятків і сотень антен дозволяє створювати вузьконаправлені промені для кожного користувача, знижуючи міжканальні перешкоди та підвищуючи ефективність спектру.

Просторове розділення (Spatial Multiplexing / Beamforming):

Кожна антена може направляти сигнал у конкретному напрямку до користувача, що мінімізує вплив мультипроменевих перешкод і покращує стабільність з’єднання.

Збільшена пропускна здатність:

Завдяки одночасному обслуговуванню великої кількості користувачів і ефективному використанню просторового розділення сигналів, загальна пропускна здатність мережі значно зростає.

Зниження затримки (Latency Reduction):

Ефективне керування каналами і точне спрямування променів дозволяє зменшити затримки в передачі даних, що критично для застосунків реального часу, таких як автономні транспортні системи, віддалене управління та індустріальні IoT мережі.

Енергоефективність:

Massive MIMO дозволяє більш точно направляти потужність сигналу, що знижує загальне споживання енергії та підвищує ефективність базової станції.

Покращена надійність та стійкість:

Завдяки високій кількості антен і просторовій диверсії мережа краще справляється з відбиттями, затуханням сигналу та шумом, забезпечуючи стабільне з’єднання навіть у складних умовах.

Технологія beamforming. Це метод просторової обробки сигналів, який використовується в сучасних безпроводових комунікаціях для формування вузьконаправлених променів радіосигналу. На відміну від традиційних всеспрямованих антен, які випромінюють сигнал у всі сторони, beamforming забезпечує можливість динамічного спрямування енергії у визначеному напрямку або до конкретного абонентського пристрою. Це підвищує якість зв'язку, збільшує дальність передачі та мінімізує вплив інтерференції (Рис. 1.7.).

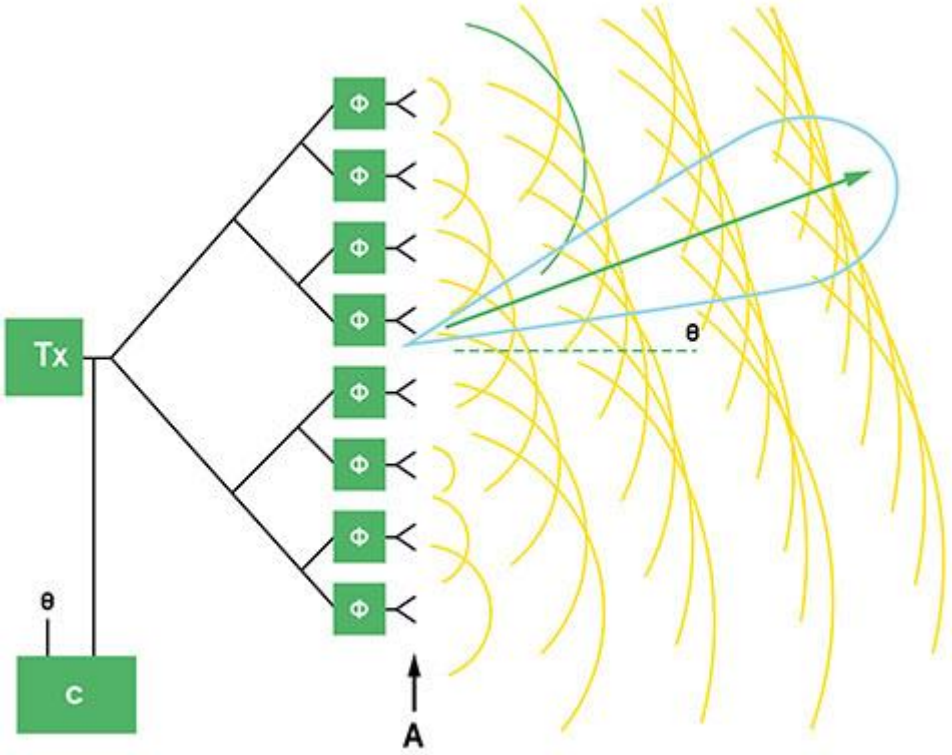


Рис. 1.7 Схематичне зображення роботи beamforming

Ключові аспекти технології beamforming:

1. Фазові антенні решітки (Phased Array): Beamforming базується на використанні антенних решіток, що складаються з великої кількості радіоелементів, розташованих у визначеній геометричній конфігурації (лінійній, плоскій або 3D). Кожен елемент антенної решітки має можливість індивідуального керування фазою та амплітудою сигналу. Завдяки цьому створюється можливість електронного управління характеристиками випромінювання без фізичного переміщення антени [5].

2. Формування променя (Beam Steering): Зміна фази сигналів між

елементами антенної решітки призводить до конструктивної та деструктивної інтерференції в різних напрямках. Це дозволяє «повертати» промінь у потрібну сторону, формувати кілька незалежних променів, а також швидко перенаправляти їх у просторі залежно від місцезнаходження користувачів. Така електронна мобільність променя відбувається за мікросекунди, що робить технологію високоефективною для 5G.

3. Спрямована передача та прийом (Directional Tx/Rx): Завдяки формуванню вузького променя переданий сигнал концентрується на конкретному абоненті, що значно збільшує відношення сигнал/шум (SNR). На прийомі beamforming дозволяє фокусуватися на сигналі від потрібного UE та пригнічувати сигнали з інших напрямків. Це зменшує рівень інтерференції, збільшує стабільність каналу та покращує параметри QoS.

4. Покращення продуктивності та спектральної ефективності: Beamforming підвищує спектральну ефективність мережі завдяки максимальному використанню просторових ресурсів та зменшенню взаємних перешкод між користувачами. Це особливо важливо для масивних антенних систем (Massive MIMO), де формування великої кількості незалежних променів дозволяє одночасно обслуговувати десятки UE. В результаті підвищується пропускна здатність, знижується затримка та збільшується покриття, особливо в середовищах зі складною радіообстановкою.

Випадки використання 5G та виклик забезпечення QoS. Технологія 5G створена для обслуговування трьох основних типів сценаріїв застосування, кожен із яких висуває власні вимоги до якості обслуговування (QoS):

Enhanced Mobile Broadband (eMBB) - це напрям, спрямований на забезпечення високошвидкісного доступу до інтернету та підтримку сервісів, що потребують значної пропускної здатності: відеострімінгу у високій якості, онлайн-ігор, мультимедійних застосунків. Для таких послуг критично важливими є високі швидкості передавання даних, низька затримка та стабільна пропускна здатність, щоб уникнути буферизації, затримок або розривів з’єднання. Оскільки 5G може забезпечувати швидкість до 20 Гбіт/с, механізми QoS повинні гарантувати плавний

та безперебійний доступ навіть під час пікового навантаження мережі.

Massive Machine Type Communications (mMTC) - цей сценарій орієнтований на масове підключення пристроїв IoT, що лежить в основі розвитку «розумних» міст та інфраструктур. Хоча такі додатки не потребують високих швидкостей, для них є визначальними висока доступність мережі, надійність та здатність обробляти величезні обсяги даних від мільярдів пристроїв одночасно. QoS у цьому випадку має забезпечити стабільне підключення всіх пристроїв, запобігаючи перевантаженню мережі.

Ultra-Reliable Low-Latency Communications (URLLC) - цей клас застосувань охоплює критичні сервіси, як-от автономний транспорт, дистанційна хірургія чи промислова автоматизація. Такі системи потребують наднизької затримки - менше однієї мілісекунди - та майже стовідсоткової надійності. Для URLLC механізми QoS повинні мінімізувати затримки та максимально підвищувати надійність, гарантуючи, що робота сервісу не перерветься за жодних умов [19].

Ключові компоненти QoS у мережах 5G. Щоб 5G могла забезпечити обіцяний високий рівень продуктивності під час передавання даних, необхідно ретельно управляти кількома ключовими компонентами QoS.

Класифікація та диференціація трафіку.

Одним із базових елементів QoS у 5G є здатність розподіляти трафік за його характеристиками та типом застосунку. Мережа має розрізняти відеопотоки, голосові виклики, масові завантаження даних чи керуючі сигнали. Кожен тип трафіку має свої вимоги до QoS: одні застосунки потребують високої пропускної здатності, інші — мінімальної затримки. Правильна класифікація дає змогу обробляти різні потоки відповідно до їхніх потреб. Наприклад, трафік з критично низькою затримкою — як у системах автономного транспорту — повинен мати вищий пріоритет, ніж великі завантаження файлів.

Пріоритезація та планування трафіку.

Після класифікації трафік необхідно розподілити за пріоритетами. У мережі 5G найважливіші або найбільш чутливі до часу дані мають передаватися першими, тоді як менш критичні можуть очікувати. Механізми планування передачі

гарантують, що високопріоритетний трафік буде доставлений у визначений часовий інтервал, а низькопріоритетний не погіршуватиме роботу критичних сервісів. У 5G ці процеси є динамічними й адаптуються до реального стану мережі - наприклад, до перевантаження або перешкод.

Розподіл пропускної здатності.

Управління доступним спектром — один із центральних аспектів QoS у 5G. Мережа повинна забезпечувати достатньо ресурсу для трафіку високого пріоритету та водночас запобігати перевантаженню. У ситуаціях великого навантаження мережа має вміти виділяти потрібні ресурси для URLLC-сервісів, навіть якщо значну частину спектра використовують eMBB-додатки. Це потребує застосування гнучких та адаптивних механізмів розподілу пропускної здатності.

Управління затримкою.

Затримка є критично важливою для застосувань реального часу, як-от дистанційна хірургія чи автономне керування. Мережі 5G повинні мінімізувати наскрізну затримку, щоб відповідати жорстким вимогам таких сервісів. Для цього використовують обчислення на периферії (edge computing), що дозволяє обробляти дані ближче до користувача, а також ультращільні мережі та малі стільники, які скорочують фізичну відстань між пристроєм і точкою доступу.

Надійність і доступність.

Для критичних сфер - наприклад, служб екстреного реагування чи промислової автоматизації - надзвичайно важливими є надійність та доступність мережі. Пакети мають доставлятися без втрат і затримок, навіть за умов перешкод або перевантаження. Цього досягають, зокрема, за допомогою мережевої сегментації (network slicing), коли окремий сегмент мережі виділяється виключно під певний сервіс із гарантованими рівнями продуктивності.

Резервування ресурсів.

Деякі сервіси потребують виділення окремих частин мережевих ресурсів, щоб забезпечити стабільний рівень QoS. Наприклад, для URLLC може резервуватися частина пропускної здатності, призначена лише для трафіку з мінімальною затримкою. Механізми резервування гарантують доступ до цих ресурсів у

потрібний момент, уникаючи конфліктів між різними сервісами.

Мережеве сегментування (Network Slicing).

Network slicing є одним із ключових інструментів забезпечення QoS у 5G. Віртуалізація дозволяє створювати окремі «слайси» мережі, оптимізовані під конкретний тип сервісу. Один слайс може мати налаштування для низької затримки й високої надійності, тоді як інший - для підтримки великої кількості IoT-пристроїв. Кожен сегмент має власні параметри QoS - пріоритет, пропускну здатність, допустиму затримку - що гарантує оптимальну роботу застосунків без взаємного впливу [11].

1.3 Актуальні релізи асоціації 3GPP стосовно мереж мобільного зв'язку п'ятого покоління

Release 15. Після публікації наприкінці 2017 року перших специфікацій нових радіоінтерфейсів 5G у режимі Non-Stand-Alone (NSA), у 2018 році основні зусилля були спрямовані на своєчасне завершення Release 15 3GPP - першого повного набору стандартів 5G - та на досягнення початкових етапів підготовки матеріалів для подання 3GPP у рамках програми IMT-2020.

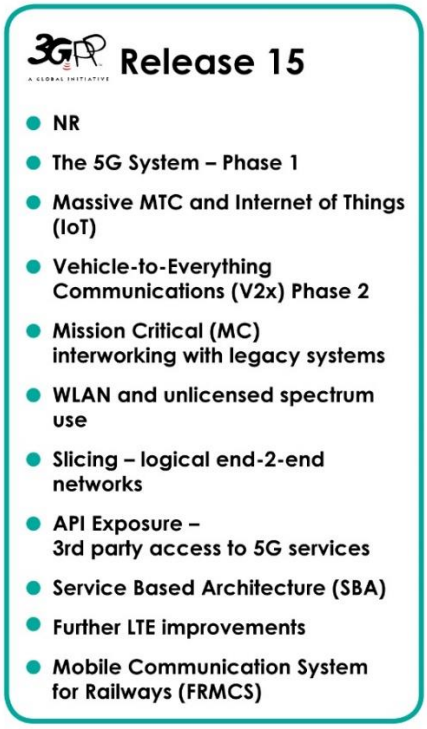


Рис. 1.8 Ключові аспекти 15 релізу організації 3GPP

Початкові специфікації дозволяли розгортати мережі 5G у режимі NSA, тобто інтегровані з існуючими LTE-мережами. У Release 15 сфера охоплення розширюється до Standalone (SA) - автономного режиму 5G із новою радіотехнологією та ядром наступного покоління (5G Core). Також стандарт включає покращення LTE та, опосередковано, Evolved Packet Core (EPC). Це стало ключовою точкою розвитку, яка дала змогу виробникам прискорити розробку чипсетів і розпочати впровадження перших реальних мереж у 2019 році.

У цей час активно розвивали й Release 16, який часто називають «другою фазою 5G». До кінця року тривали 83 дослідження в рамках Release 16 і ще 13 - у рамках Release 17. Тематика цих робіт була дуже широкою: від сервісів мультимедійного пріоритету та комунікацій Vehicle-to-Everything (V2X) до супутникового доступу 5G, підтримки локальних мереж у системі 5G, конвергенції бездротових і дротових мереж, систем позиціонування, комунікацій у вертикальних галузях, автоматизації мереж і нових радіотехнік. Також проводили дослідження щодо безпеки, кодеків, стримінгових сервісів, взаємодії з LAN, мережевого зрізання (network slicing) та IoT.

Паралельно велась робота над розширенням застосування технологій 3GPP для нетерестріальних систем доступу - супутників, повітряних базових станцій, морських застосувань, включаючи зв’язок «корабель-берег» та «корабель-корабель». Крім того, продовжувалось удосконалення функціоналу Professional Mobile Radio (PMR) для LTE, зокрема сервісів для залізничної галузі, що історично базувалися на GSM і нині поступово виходять з експлуатації [12].

Release 16. Release 16 став одним із ключових етапів розвитку стандартів 5G, оскільки саме з ним завершено подання 3GPP на відповідність вимогам IMT 2020, що визначає першу повноцінну систему 5G за міжнародними критеріями. Робота над Release 16 охопила значне розширення функціональних можливостей 5G, поглиблення технічних характеристик мережі та підготовку до масштабного комерційного впровадження. У межах цього релізу проводилось близько двадцяти п’яти досліджень, присвячених різним аспектам розвитку систем мобільного зв’язку. Серед них основну увагу приділяли мультимедійним пріоритетним

сервісам, розвитку прикладних рівнів комунікацій V2X, впровадженню супутникового доступу до мереж 5G, підтримці локальних комп'ютерних мереж у рамках мобільних систем п'ятого покоління, конвергенції бездротового і дротового середовищ, точному визначенню місцеположення користувачів, забезпеченню комунікацій у вертикальних індустріях, автоматизації мережі та впровадженню нових радіотехнологій. Паралельно тривало вивчення механізмів безпеки, роботи кодеків та потокових сервісів, взаємодії з локальними мережами, подальшого розвитку концепції мережевого зрізання та інтеграції IoT. Значна частина технічних звітів Release 16 була спрямована на розширення використання технологій 3GPP у нетерестріальних системах доступу, до яких належать супутникові системи, повітряні базові станції та морські мережі для забезпечення зв'язку між кораблями та наземними станціями. Водночас велика увага приділялась удосконаленню функціоналу професійного мобільного радіозв'язку на базі LTE, який повинен замінити застарілі залізничні сервіси GSM, що вже наближаються до завершення свого життєвого циклу. У межах Release 16 також відбулося розширення можливостей сервісів критичного призначення, які спочатку були розроблені переважно для служб безпеки та цивільної оборони. Їх адаптація до комерційних потреб, таких як диспетчеризація транспорту, управління залізничним рухом чи застосування в промислових вертикалях, дозволяє підвищити їхню надійність завдяки ширшому використанню та зменшити вартість впровадження через ефект масштабу.

Release 16 також став першим релізом, який повністю зосереджений на підвищенні ефективності 5G систем у промисловості, транспорті та автоматизації. Він містить численні покращення до роботоздатності URLLC, включаючи точніший контроль затримок, розширення механізмів дублювання пакетів та кращі алгоритми розподілу ресурсів, що забезпечує підвищену надійність у критичних застосуваннях від промислових роботів до систем автономного керування. Реліз також передбачає суттєве вдосконалення енергетичної ефективності завдяки новим режимам роботи радіоінтерфейсу та оптимізації передачі даних, що є важливим для масових IoT розгортань. Значну увагу приділено і точному позиціонуванню, де

завдяки новим алгоритмам та сигналам пошуку вдалося досягти точності до сантиметрового рівня, що відкриває можливості для логістики, транспорту, автономних систем та розумних фабрик. Розширені можливості мережевого зрізання дозволили забезпечити більш гнучкий розподіл ресурсів між різними категоріями сервісів, що є необхідним для великомасштабного впровадження 5G у вертикальних секторах економіки.

Процес підготовки IMT 2020 подання також мав три ключові етапи. Перший тривав з вересня 2017 року до грудня 2017 року і включав адаптацію критеріїв самооцінки та підготовку початкових описових матеріалів для подання до ITU R. Наступний етап від початку 2018 року до вересня 2018 року був присвячений оцінюванню продуктивності згідно з вимогами eMBB, mMTC та URLLC, оновленню технічних шаблонів та передачі результатів самооцінювання за Release 15. Третій етап тривав з вересня 2018 року до червня 2019 року та включав оновлення оцінок з урахуванням нововведень Release 16, підготовку фінальних описових документів і шаблонів відповідності, а також формування остаточного подання, що відображає можливості систем 5G у рамках як Release 15, так і Release 16. Таким чином, Release 16 став основою для переходу від початкових версій 5G до повноцінної, високопродуктивної та універсальної екосистеми, здатної підтримувати критичні сервіси, індустріальні сценарії, транспортні системи та масштабні IoT рішення [13].

Release 17. У березні 2022 року під час засідання TSG 95-е було завершено функціональне замороження Release 17, що стало важливим етапом еволюції стандартів 3GPP. Цей реліз охопив значну кількість удосконалень, спрямованих на підвищення ефективності, масштабованості та гнучкості мереж 5G. Серед ключових напрямів розвитку варто відзначити розширення можливостей Sidelink, що забезпечує ефективнішу взаємодію між пристроями на рівні підрозділу Device-to-Device, а також появу зменшеної складності пристроїв RedCap, орієнтованих на IoT сегмент із потребою в нижчій вартості та енергоспоживанні. Release 17 розширив діапазон роботи NR до частот до 71 ГГц, що відкриває шлях до надвисоких пропускних можливостей у міліметровому спектрі. Удосконалення

багатокористувацьких та багатопроменевих MIMO технологій забезпечили вищу спектральну ефективність та стабільність роботи мережі.

Важливою складовою релізу стало розширення підтримки неназемних мереж, що включає як NR NTN, так і IoT NTN, що дозволяє поширювати 5G послуги на супутникові та інші позаземні платформи. Було реалізовано нові функції енергозбереження для пристроїв NR, удосконалено інтегровані механізми доступу та транспортної мережі IAB, а також розширено функціональні можливості RAN slicing для більш точного розділення мережевих ресурсів між різними сервісами та вертикальними галузями. У реліз також увійшли нові вимоги до радіочастотних характеристик як для FR1, так і для FR2, що забезпечують високу відповідність обладнання сучасним умовам розгортання.

Суттєву увагу приділено покращенню покриття та точності позиціонування, удосконаленню підтримки непублічних мереж, розширенню функціональності для безпілотних літальних апаратів, інтеграції обчислень на периферії у 5G Core, а також розвитку сервісів на основі близького розташування пристроїв у 5GS. Було посилено механізми маршрутизації трафіку ATSSS та продовжено розвиток автоматизації мереж, що у Phase 2 забезпечує більшу автономність, керованість та оптимізацію ресурсів. Упродовж 2022 року розпочалася активна робота над Release 18, який від середини року став основним напрямом діяльності 3GPP [14].

Release 18. Release 18 є наступним кроком розвитку системи 5G Advanced і визначає подальше вдосконалення технологій п’ятого покоління шляхом розширення попередніх можливостей та впровадження нових функцій. Основна увага приділяється глибшій інтеграції супутникового доступу в архітектуру 5G, що забезпечує безперервне покриття та можливість обслуговувати віддалені території. Розширюється підтримка Інтернету речей та машинного типу комунікацій з акцентом на IoT через супутники, що робить систему більш універсальною для масштабних промислових застосувань. Значні удосконалення стосуються технологій прямого зв’язку між пристроями, механізмів близького доступу, точного позиціонування та навігації, що критично важливо для транспорту, логістики та автоматизованих виробничих систем [15].

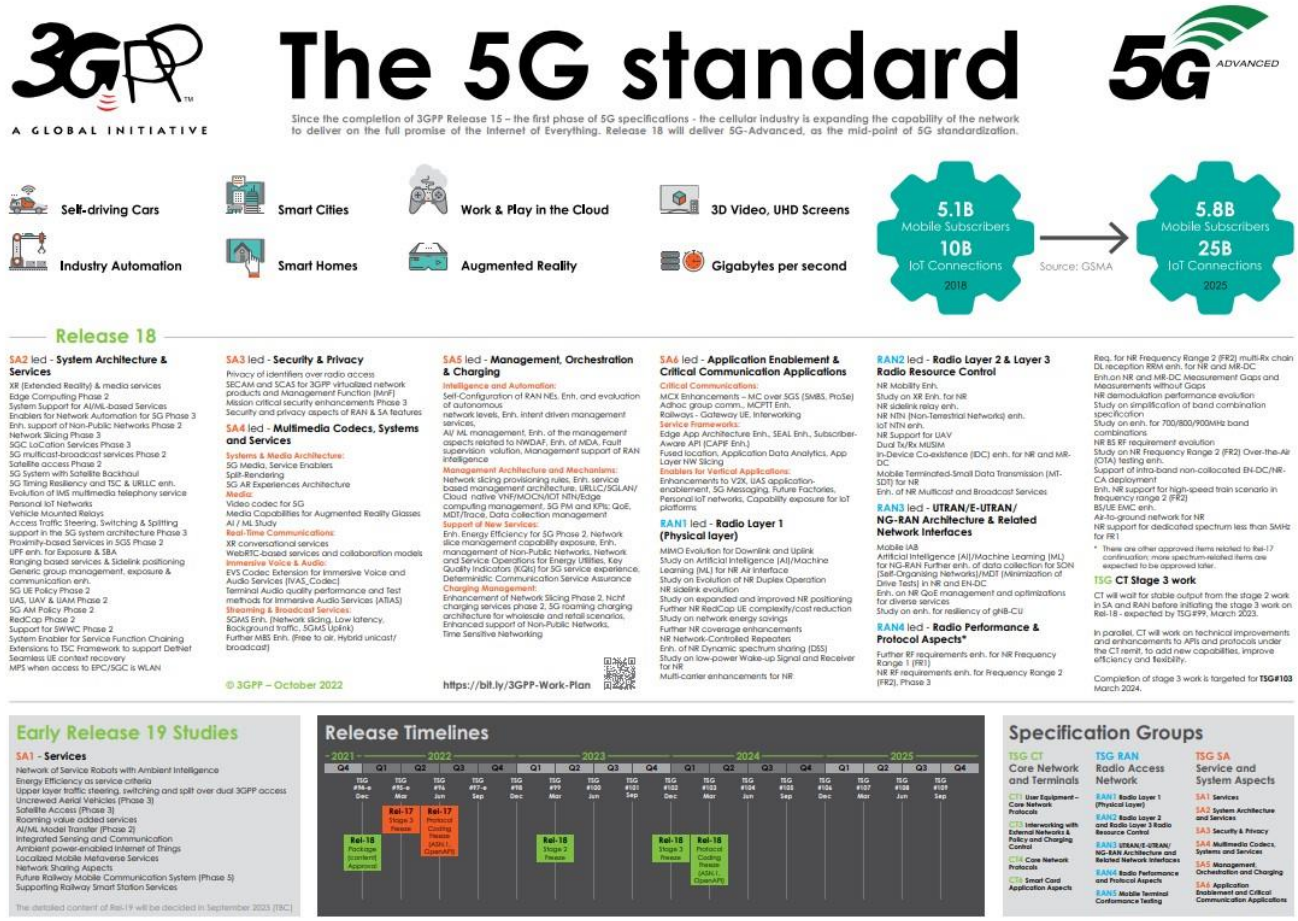


Рис. 1.9 Основні особливості Release 18

Release 18 також відповідає потребам вертикальних індустрій та промислових підприємств, розширюючи можливості API для взаємодії з мережею, покращуючи сервісну архітектуру та оптимізуючи мережеву взаємодію для фабрик та автоматизованих виробничих процесів. Удосконалюються функції мультимовленнєвих та багатоканальних сервісів, що дозволяє забезпечувати ефективніші рішення для широкомовних та групових комунікацій. Приділяється увага розвитку мережевого розподілу ресурсів для гнучкої підтримки різноманітних сервісів з урахуванням їх специфічних вимог. Значний прогрес спостерігається у сфері підтримки безпілотних літальних апаратів, де покращуються механізми управління, зв’язку та інтеграції у мобільну мережу. Окремим новим напрямом стає підвищення енергоефективності мережі, що дозволяє зменшити споживання енергії як на стороні обладнання, так і на рівні протоколів. Release 18 активно використовує технології штучного інтелекту та

машинного навчання для оптимізації роботи радіодоступу, прогнозування навантаження, адаптації параметрів мережі та покращення якості користувацького досвіду. Ще одним ключовим нововведенням є розвиток рішень у сфері XR, AR та VR, що забезпечує можливість створення високоякісних занурювальних сервісів з мінімальною затримкою та стабільною пропускною здатністю. Сукупність цих удосконалень визначає Release 18 як етап становлення 5G Advanced, який формує основу для майбутнього розвитку до 6G та забезпечує значно ширші можливості в усіх сферах цифрової економіки.

Release 19. Реліз 19 (3GPP Release 19) продовжує еволюцію «5G-Advanced», закладаючи місток до 6G.

Серед ключових технічних напрямів:

Покращене масивне MIMO: підтримка великих антенних масивів, гнучкіший beamforming, можливість роботи з розподіленими передавачами (D-MIMO) для підвищення покриття і пропускної здатності.

Покращена мобільність: запроваджується механізм L1/L2-triggered mobility (LTM) з коротшими інтеррупціями сервісу, підтримка UE-ініційованого звітування про вимірювання, handover між різними gNB, навіть у ситуації з NR-NR dual connectivity у FR1/FR2.

Підтримка Ambient IoT та енергоефективності: наприклад, low-power wake-up signal/receiver (LP-WUS/WUR) і оптимізація для IoT пристроїв із дуже низьким споживанням.

Інтеграція супутникового зв’язку (Non-Terrestrial Networks, NTN) і IoT у віддалених регіонах: реліз забезпечує розвиток NTN і розширення IoT покриття.

Оновлення моделей каналу та частотних діапазонів: зокрема, дослідження TR 38.901 для діапазону 7-24 GHz, що готує основу для 6G-частот.

Сервісні та системні аспекти: розширення XR (eXtended Reality), API-інтерфейси (CAPIF), незалежне управління даними для медіасервісів, вдосконалення мобільного стрімінгу, QoS-моніторинг.

У підсумку, реліз 19 концентрується на підвищенні ефективності, гнучкості, на підтримці нових кейсів (XR, IoT, NTN) та на покритті широкої технологічної

бази перед переходом до нових поколінь [16].

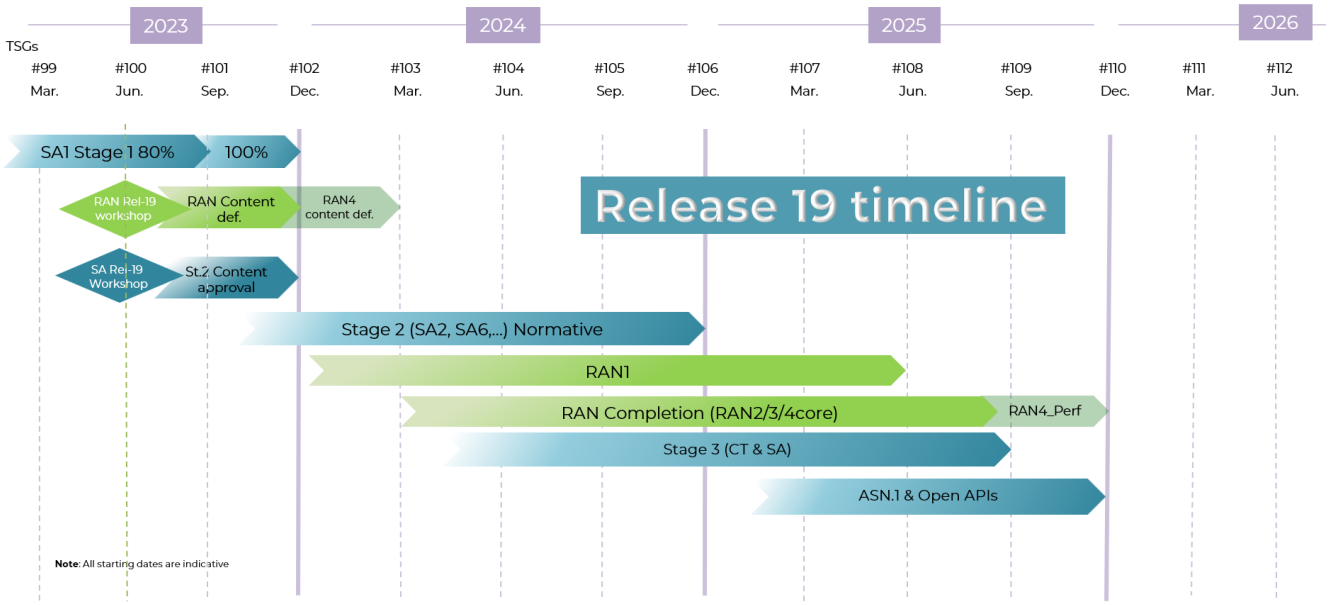


Рис. 1.10 Таймлайн Release 19

Release 20. Реліз 20 (3GPP Release 20) виступає як подвійна фаза - з однієї сторони доопрацьовує 5G-Advanced, з іншої починає підготовку до 6G.

Основні технічні особливості:

Часова лінія: сервісні вимоги (Stage-1) планується зафіксувати в червні 2025, система архітектури (Stage-2) - ~80 % до червня 2026 та остаточний freeze у вересні 2026, протокольні деталі (Stage-3) - до березня 2027, з ASN.1/OpenAPI у червні 2027. Все це зображено на рисунку 1.11.

Теми системного масштабу: енергоефективність мережі, звітність вуглецевого сліду для сервісів, вертикальні галузі, глобальна покритість, інтеграція наземних і неземних мереж.

Підтримка нових діапазонів частот: крім FR1/FR2, додається FR3 (7-24 GHz) як потенційний діапазон, а також дослідження в бік субтерагерцевих діапазонів для екстремальних швидкостей і сенсінгу.

Поглиблений AI/ML: використання машинного навчання як для радіоінтерфейсу (CSI-зворотний зв'язок, передбачення мобільності) так і для оптимізації мережі (мережева енергоощадність).

Безпека та квантова готовність: підготовка до пост-квантової криптографії

(PQC), інтеграція 256-бітових алгоритмів, сумісність із 128-бітовими системами.

Вертикальні випадки використання: NTN, залізнична мобільна система (FRMCS), E2E архітектура для критичних комунікацій, multi-hop relaying, підтримка громадської безпеки [17].

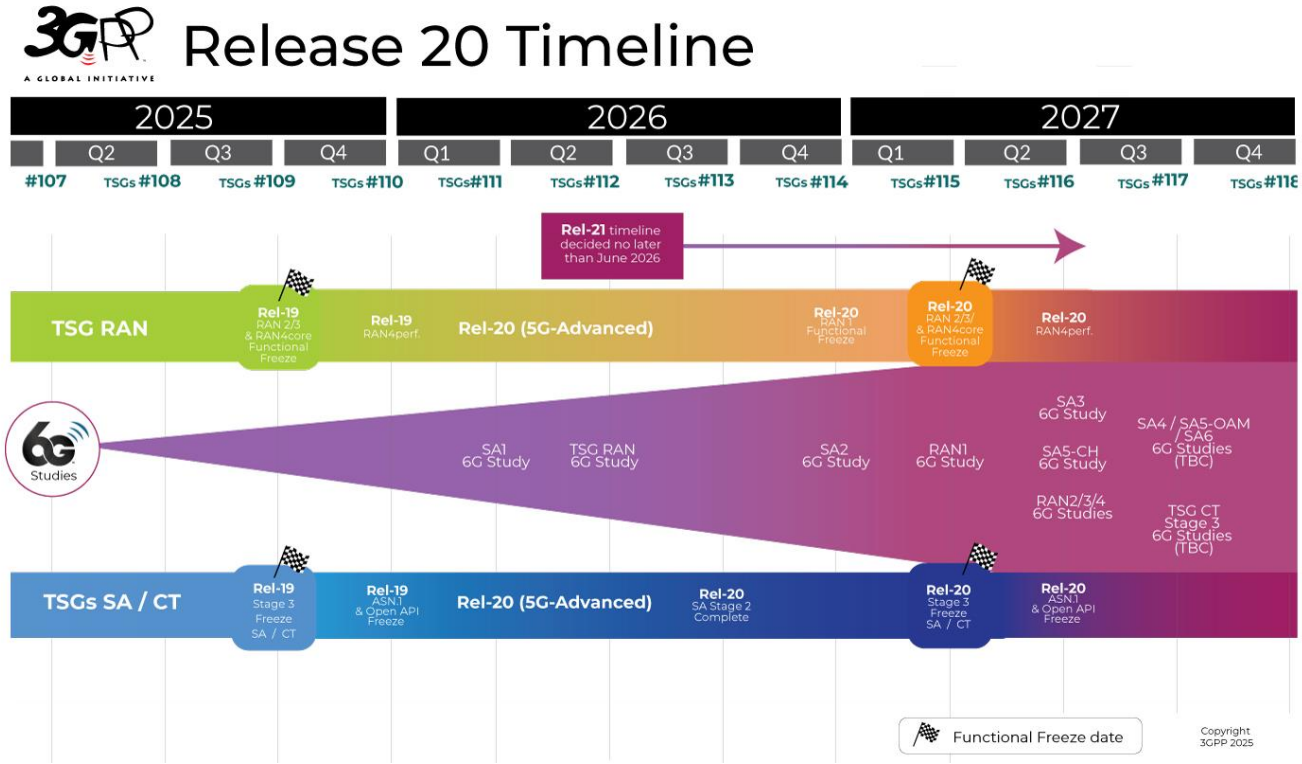


Рис. 1.11 Таймлайн Release 20 та плани розвитку

Таким чином, реліз 20 задає архітектурний та технологічний фундамент для майбутнього мобільного покоління (6G), одночасно укріплюючи і розвиваючи можливості 5G-Advanced.

2 SOFTWARE-DEFINED NETWORKING В МЕРЕЖАХ 5G

2.1 Інфраструктурні та технологічні підходи до модернізації інфокомунікаційних систем на базі SDN та NFV

Розвиток мобільних систем зв’язку вийшов на ключовий етап із впровадженням мереж п’ятого покоління (5G), які забезпечують надзвичайно низькі затримки, розширені пропускні можливості та підтримку масштабних підключень пристроїв. Такі можливості створили умови для стрімкого зростання кількості критично важливих застосувань, включно з автономним транспортом, дистанційною медициною та промисловою автоматизацією. Водночас ускладнення архітектури 5G та підвищення її неоднорідності формують нові виклики у сфері кібербезпеки та маршрутизації, зокрема щодо підтримання надійності й захищеності передавання даних в умовах динамічної топології.

Для ефективного управління такою інфраструктурою дедалі ширшого застосування набуває концепція програмно-конфігурованих мереж (SDN). SDN технологічно розділяє площину управління та площину пересилання, що забезпечує централізоване керування, гнучку конфігурацію та можливість реалізації мережевого сегментування (network slicing). Однак централізація контролю, яка є основною перевагою SDN, водночас створює єдину точку відмови та відкриває простір для появи нових типів атак, таких як перехоплення управлінської площини, модифікація таблиць потоків або зловмисні дії внутрішніх елементів мережі [18].

Крім того, наявні протоколи маршрутизації, що історично проєктувалися для статичних або децентралізованих середовищ, не мають інструментів оперативного визначення рівня довіри до мережевих вузлів. Це робить їх вразливими до широкого спектра атак, включно з «blackhole», «greyhole» та вибірковим перенаправленням трафіку. У зв’язку з цим особливої актуальності набувають підходи, засновані на довірчій маршрутизації, які дають змогу підвищити рівень захищеності в SDN-орієнтованих 5G-мережах.

Довірчі моделі використовують оцінку поведінкової надійності мережевих вузлів для формування рішень щодо вибору маршруту, тим самим дозволяючи заздалегідь виявляти потенційно шкідливі дії. Впровадження таких моделей у централізовану структуру SDN вимагає ретельного опрацювання питань масштабованості, оперативності оброблення даних та сумісності з наявними мережевими функціями.

У даному дослідженні запропоновано динамічну довірчу модель маршрутизації, орієнтовану на застосування в SDN-контрольованих 5G-мережах. Розроблена система обчислює значення довіри на основі прямих і непрямих показників, серед яких коефіцієнт доставлення пакетів, затримка та сигнали про потенційну шкідливу активність. Отримані значення інтегруються у процес обчислення маршрутів на рівні контролера. Моделювання підтверджує, що запропонований підхід підвищує захищеність мережі, покращує показники продуктивності та забезпечує адаптивність у сценаріях, що включають різні типи атак.

Програмно-конфігуровані мережі (Software-Defined Networking, SDN). Програмно-конфігурований підхід до побудови мереж розглядається як один із ключових напрямів підвищення гнучкості та керованості сучасних телекомунікаційних систем. Концепція SDN ґрунтується на використанні програмованих мережевих пристроїв, у яких функції керування трафіком відокремлено від функцій власне пересилання пакетів. Логіка керування зосереджується в програмному контролері, що виконує роль «мережевого мозку», тоді як множина комутаторів і маршрутизаторів формує «мережеві виконавчі органи», відповідальні за швидке транспортування пакетів даних.

У типовій архітектурі SDN, що ілюструється на рис. 2, виділяють площину керування та площину даних, пов’язані між собою через північний (northbound) і південний (southbound) інтерфейси. Північний інтерфейс надає абстрактне представлення мережевих ресурсів прикладним сервісам і системам керування, що дає змогу реалізовувати складні політики маршрутизації та моніторингу без прив’язки до конкретного обладнання. Південний інтерфейс, своєю чергою,

уніфікує обмін службовою інформацією між контролером і пристроями пересилання, забезпечуючи стандартизовану взаємодію різних реалізацій обладнання. Завдяки такому підходу SDN була успішно впроваджена в дата-центрах великих постачальників контенту, зокрема глобальних інтернет-компаній.

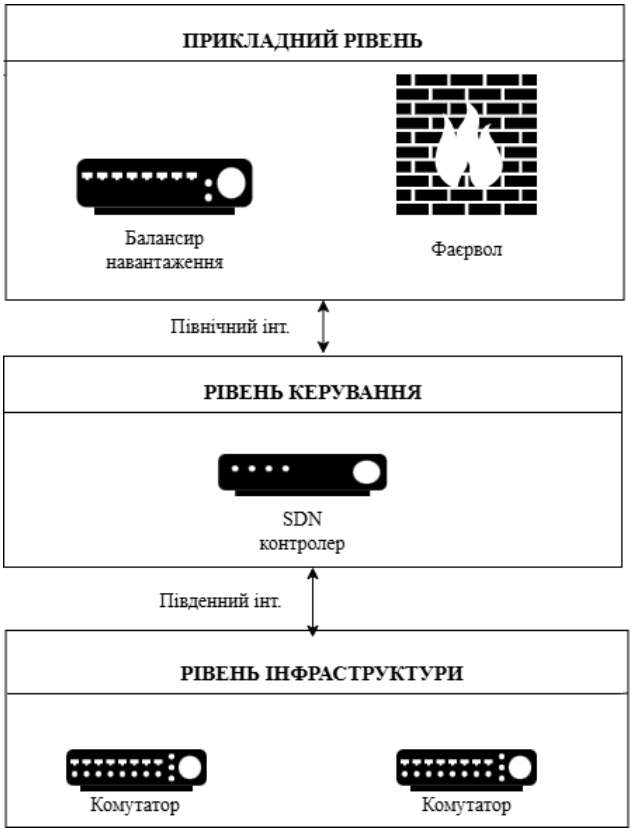


Рис. 2.1 Архітектура SDN

Архітектура програмно-конфігурованих мереж (SDN) традиційно розглядається як багаторівнева структура, у якій кожен рівень виконує чітко визначені функції та взаємодіє з іншими компонентами через стандартизовані інтерфейси. На базовому, інфраструктурному рівні розташовані фізичні мережеві елементи, серед яких комутатори, маршрутизатори, точки доступу та інші пристрої пересилання трафіку. Управління їхньою роботою здійснюється через SDN-контролер, який забезпечує централізований доступ до ресурсів та їх конфігурацію.

Ключовим елементом взаємодії між рівнями мережі є прикладні програмні інтерфейси (API), що виконують роль єдиної точки керування мережею. У SDN-архітектурі використовується два типи API: південний та північний. Південний інтерфейс забезпечує обмін керівними командами між контролером та

інфраструктурним рівнем, дозволяючи контролеру задавати правила пересилання та отримувати інформацію про стан пристроїв. Північний інтерфейс функціонує у зворотному напрямку — він забезпечує взаємодію між контролером і мережевими застосунками, передаючи їм абстрактне уявлення про мережу та надаючи можливість формувати політики управління.

Рівень управління (control plane) виконує функції централізованої координації та моніторингу всієї мережевої інфраструктури. У цьому шарі розташований SDN-контролер, який забезпечує інформаційний обмін між прикладним рівнем і пристроями пересилання. Контролер реалізує управління на основі північного та південного інтерфейсів, що дозволяє ефективно взаємодіяти з усіма компонентами мережі та оперативно змінювати політики її функціонування.

Прикладний рівень містить один або кілька спеціалізованих мережевих додатків, що виконують логіку високого рівня — системи виявлення вторгнень, механізми балансування навантаження, брандмауери, аналітичні модулі тощо. Використовуючи північний інтерфейс контролера, ці додатки отримують абстраговану модель мережі та формують правила, які далі реалізуються на нижчих рівнях [1].

Основою комунікації між контролером і пристроями інфраструктури в SDN є протокол OpenFlow (OFP), який визначає правила обміну керівними повідомленнями та структуру таблиць потоків. OpenFlow ґрунтується на TCP-транспорті, що забезпечує встановлення IP-з’єднання між контролером та комутаторами або іншими мережевими пристроями. Протокол передбачає три ключові складові.

Перемикачі. OpenFlow-комутатори функціонують на основі таблиць потоків, у яких зберігаються правила зіставлення пакетів і відповідні дії. Після надходження пакета пристрій порівнює його параметри з наявними елементами потоку та виконує визначену дію — перенаправлення, модифікацію або відкидання. З’єднання між комутатором і контролером встановлюється через процес ініціалізації, під час якого сторони обмінюються повідомленнями щодо найвищої версії OpenFlow, яку обидва підтримують. Підвищення кількості активних каналів

зв’язку дає змогу збільшити пропускну здатність мережевої взаємодії.

Записи потоків. Елемент потоку в таблиці є структурним блоком, що визначає правила зіставлення пакетів. Якщо пакет відповідає зазначеним параметрам, комутатор змінює набір дій і здійснює обробку відповідно до призначених політик, перенаправляючи дані на відповідні порти.

Контролери. Контролер координує зв’язок між двома або більше мережевими пристроями, фактично реалізуючи централізовану логіку пересилання трафіку. Його функції можна порівняти з роботою фізичного або віртуального пристрою, що керує переміщенням даних між компонентами мережі. OpenFlow виступає стандартом, який визначає протокол зв’язку між контролером і пристроями пересилання, забезпечуючи програмованість, централізовану обробку та абстрагування інфраструктури [9].

Важливою перевагою SDN є здатність оперативно адаптувати мережу до нових політик шляхом програмної зміни логіки управління. Централізована архітектура та гнучкість конфігураційних механізмів роблять SDN суттєво ефективнішою порівняно з традиційними мережами, орієнтованими на апаратні рішення. Крім того, централізована логіка спрощує діагностику та усунення несправностей, тоді як у класичних мережах статичність апаратних компонентів та їхня різнорідність ускладнюють процес технічного обслуговування.

З технологічної точки зору, рівень розвитку масового апаратного забезпечення (commodity hardware) нині дає змогу використовувати стандартні персональні комп’ютери для оброблення трафіку з пропускною здатністю у багаторазовому діапазоні гігабіт за секунду. Наявність значної кількості процесорних ядер у доступних за ціною ЦП та поява мережевих адаптерів нового покоління з підтримкою багатьох черг оброблення пакетів стимулювали інтерес до програмно-прискорених рішень для високошвидкісного вилучення та аналізу трафіку. Для цього застосовуються спеціалізовані програмні фреймворки, зокрема PF_RING, Netmap, DPDK і PFQ, які забезпечують високошвидкісний захват і оброблення даних на відносно недорогих ПК загального призначення. BEBA бібліотека PFQ була використана для прискорення модифікованої версії програмного OpenFlow-

сумісного комутатора OFSoftSwitch, що дало змогу виконувати оброблення пакетів на рівні повної лінійної швидкості каналу до 10 Гбіт/с.

Таблиця 2.1

Переваги використання SDN

Перваги	Опис
Централізоване управління	Концепція централізованого управління, що лежить в основі SDN, дозволяє мінімізувати операційну складність шляхом винесення функцій контролю з окремих мережевих пристроїв на централізований контролер. Такий підхід забезпечує уніфіковане управління мережею, спрощує координацію її складових та прискорює впровадження змін.
Керована площина управління	Особливістю SDN є чітке розділення площин управління, даних і адміністрування. Контрольна площина є програмованою, що надає можливість безпосередньо визначати поведінку мережі за допомогою програмних механізмів, без потреби у ручному налаштуванні кожного елемента інфраструктури.
Спрощене мережеве адміністрування	Завдяки наявності уніфікованих API, які абстрагують функції мережевих пристроїв, SDN значно підвищує рівень автоматизації та оптимізує управлінські процеси. Додатки можуть взаємодіяти з мережею через платформу контролера, що спрощує конфігурацію, моніторинг і масштабування сервісів.
Підтримка швидких інновацій	SDN прискорює інноваційні процеси, оскільки усуває залежність від ручного конфігурування

	пристроїв та очікування нових прошивок або програмних релізів від виробників. Функціональні зміни можуть впроваджуватися на рівні програмного забезпечення, що істотно скорочує цикл розробки та адаптації мережевих сервісів.
Програмованість мережі	Фундаментальною властивістю SDN є можливість програмного керування мережею шляхом розгортання додатків на контрольній площині. Це створює передумови для незалежності від конкретних постачальників обладнання, оскільки логіка роботи мережі визначається програмою, а не функціональними обмеженнями пристроїв.
Гнучка архітектура	SDN забезпечує відкриту та гнучку архітектуру мережі, здатну інтегрувати існуюче обладнання та водночас закладати основу для подальшого розвитку інфраструктури. Такий підхід дозволяє оптимізувати інвестиції та планувати еволюцію мережі в довгостроковій перспективі.
Механізм прийняття рішень при переспрямуванні	На відміну від традиційних мереж, що використовують орієнтацію на адресу призначення, SDN будує шлях переспрямування пакетів на основі правил потоків. Комбінація критеріїв відповідності та визначених дій дозволяє гнучко керувати передаванням трафіку та реалізовувати складні політики.
Управління політиками доступу	SDN надає адміністраторам можливість реалізовувати політики ACL у високоабстрактний, автоматизований і централізований спосіб. Такий підхід підвищує точність контролю над доступом до сервісів та спрощує підтримку політик безпеки.

Покращення якості користувацького досвіду	Централізований контроль та доступність глобальної інформації про стан мережі дозволяють прикладним сервісам оперативно реагувати на зміни умов експлуатації та потреб користувачів. Завдяки цьому SDN здатна ефективно підтримувати динамічні сценарії користування мережею.
Посилення мережевої безпеки	SDN підвищує рівень захищеності мережі шляхом забезпечення глобальної видимості, централізованого керування механізмами безпеки та оперативного розгортання захисних політик. Централізація управління дозволяє розробляти та впроваджувати ефективні механізми виявлення й запобігання атакам, забезпечуючи комплексний захист інфраструктури.

Віртуалізація мережних функцій (Network Function Virtualization, NFV). Концепція NFV спрямована на трансформацію підходів до проектування й експлуатації телекомунікаційних мереж та надання мережних послуг. Її сутність полягає у використанні технологій IT-віртуалізації для перенесення широкого спектра спеціалізованих мережевих пристроїв на уніфіковану інфраструктуру з продуктивних серверів, комутаторів та систем зберігання даних промислового класу.

В архітектурі NFV забезпечується можливість реалізації надійного надання послуг (service assurance), що досягається завдяки механізмам розподіленого резервування ресурсів та організованому збору експлуатаційних даних для обчислення показників ефективності KPI (Key Performance Indicators) як від апаратних, так і від програмних компонентів NFV [22].

Архітектура VNF визначає низку базових компонентів, показано на рисунку 2.2.

Віртуальні мережеві функції VNF (Virtual Network Functions) виконуються в інфраструктурі NFVI (NFV Infrastructure), яка ґрунтується на обладнанні класу COTS (комерційно доступне типове обладнання). Над всією цією інфраструктурою функціонує комплекс керування й адміністрування, що логічно поділяється на три основні підсистеми:

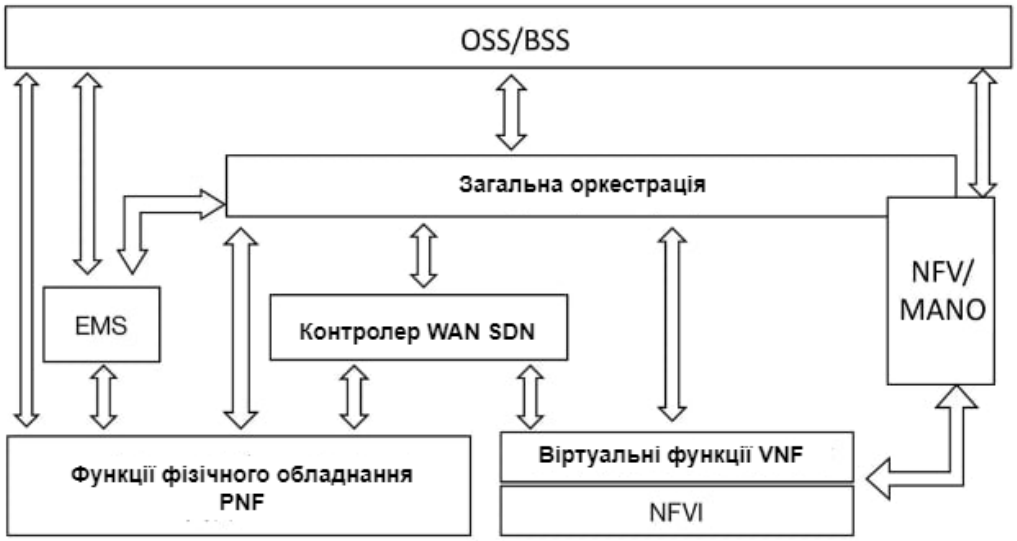


Рис. 2.2 Архітектура VNF

Підсистема NFV MANO (Management and Orchestration) відповідає за керування інфраструктурою NFVI та життєвим циклом віртуальних мережевих функцій. До її ключових завдань належать:

- Розподіл і вивільнення ресурсів NFVI – процес керування обчислювальними потужностями серверів, ємністю сховищ і комутаційними ресурсами мережі.
- Адміністрування мережевих зв’язків між віртуальними машинами (VM) і розгорнутими на них VNF, а також взаємодія з SDN-контролером дата-центру з метою керування внутрішньомережевою топологією.
- Створення VNF, побудова з них ланцюжків і сервісних графів, виконання оновлення (апгрейду) та деактивації функцій у рамках загального керування їхнім життєвим циклом.
- Моніторинг стану інфраструктури NFVI, включно з контролем продуктивності й виявленням відмов

Контролер SDN для магістральної мережі WAN (Wide Area Network) реалізується у вигляді одного або декількох централізованих SDN-контролерів, які керують наданням сервісів у різних мережевих доменах, зокрема мультивендорних і мультитехнологічних. Він відповідає за:

- узгодження політик керування трафіком між доменами;
- організацію наскрізної взаємодії сервісів, що реалізуються засобами PNF (Physical Network Functions) і VNF;
- побудову і підтримку магістральних з'єднань, необхідних для роботи сервісних ланцюжків.

Загальний оркестратор керує розміщенням і запуском VNF у середовищі NFVI, формує комплексні послуги з набору окремих функцій, поєднуючи їх у ланцюжки та сервісні графи. Для цього він взаємодіє з:

- підсистемою NFV MANO, ініціюючи розгортання та активацію компонентів NFV;
- контролером SDN магістральної мережі, який забезпечує наскрізні з'єднання через WAN;
- фізичними і віртуальними мережевими функціями, об'єднуючи їх у єдину послугу.

У типових схемах архітектури загальний оркестратор і NFV MANO часто подаються як єдиний логічний блок, хоча функціонально складаються з кількох окремих частин.

Головна відмінність між NFV MANO та SDN-контролером полягає в тому, що NFV MANO оперує фактом існування та станом віртуалізованої функції, не заглиблюючись у її внутрішню логіку, тоді як SDN-контролер знає, яку саме роль виконує функція в мережі, але не розрізняє, чи реалізована вона на фізичному чи віртуальному рівні.

Система EMS виконує функції управління окремими віртуальними мережевими функціями. Вона забезпечує налаштування параметрів, організацію експлуатації, керування відмовами та продуктивністю, тобто виконує для VNF ту саму роль, яку система управління мережею виконує для фізичних елементів.

Взаємодія між EMS і VNF зазвичай реалізується через закриті інтерфейси, тому точка зіставлення між ними наразі чітко не стандартизована. Одна система EMS може обслуговувати одну або кілька віртуальних функцій; можливий варіант, коли сама EMS реалізована як VNF і керується іншою системою управління.

Віртуальні мережеві функції є основними будівельними блоками архітектури NFV. Вони представляють собою програмні аналоги традиційних мережевих елементів, наприклад віртуальний маршрутизатор, віртуальну базову станцію чи окремі функціональні модулі, такі як підсистема пересилання пакетів. Один фізичний мережевий пристрій може бути представлений у вигляді кількох VNF, які разом відтворюють його повну функціональність. При цьому NFV виступає загальною технологічною концепцією, а VNF — конкретною реалізованою функцією в межах цієї концепції.

Комплекс систем OSS/BSS охоплює всі програмні засоби оператора, які використовуються для керування мережею та підтримки бізнес-процесів. NFV має бути інтегрована з цим комплексом, а не працювати окремо. Керування VNF та NFVI може виконуватися безпосередньо з існуючих систем OSS/BSS шляхом розширення їх можливостей. Водночас такий підхід часто пов’язаний із використанням закритих рішень окремих постачальників і, як наслідок, підвищує залежність оператора від конкретного вендора.

Інфраструктура NFVI. NFVI є середовищем, у якому розгортаються і функціонують віртуальні мережеві функції. Вона охоплює три групи ресурсів, схематично розміщено на рисунку 2.3:

- фізичні ресурси, до яких належать сервери, комутатори, маршрутизатори, системи зберігання та інше мережеве і обчислювальне обладнання;
- віртуальні ресурси, що утворюються під час процесу віртуалізації та використовуються безпосередньо для роботи VNF;
- рівень віртуалізації, де виконується перетворення фізичних ресурсів у віртуальні.

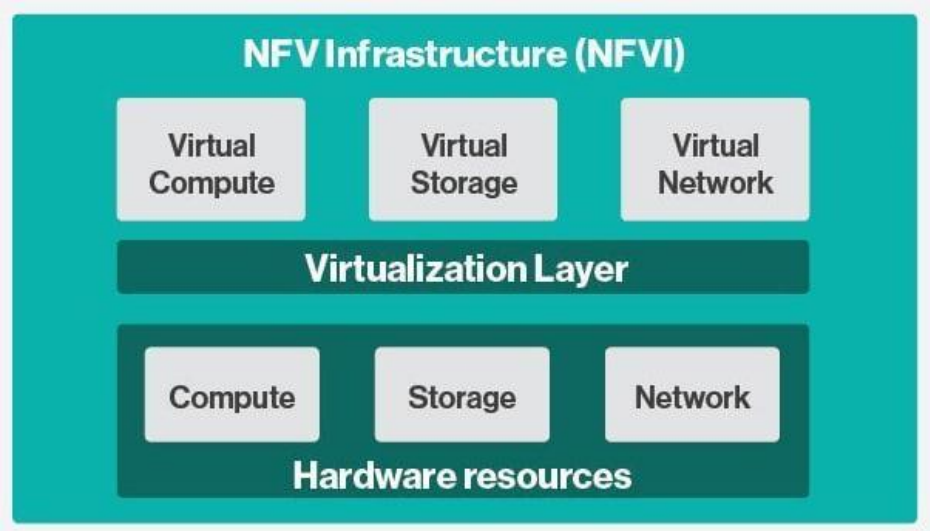


Рис. 2.3 Інфраструктура віртуалізації мережевих функцій NFVI

На рівні віртуалізації працює гіпервізор, який відокремлює програмні компоненти від апаратної платформи, дозволяючи запускати один і той самий програмний стек на будь-якому придатному фізичному сервері. Віртуальні ресурси NFV використовують фізичну інфраструктуру NFVI як базу, що дає змогу реалізувати гнучкі, масштабовані та програмно керовані мережеві сервіси.

Під час надання мережного сервісу вирішальну роль виконує оркестратор NFVO. По-перше, він є єдиною точкою доступу для всіх запитів на створення, зміну чи видалення сервісів; по-друге, забезпечує керування життєвим циклом мережних сервісів та SFC; по-третє, підтримує цілісний, «наскрізний» погляд на використання ресурсів, розподілених між різними сервісами та VNF, включно з керуванням життєвим циклом окремих віртуалізованих функцій [23].

2.2 SDN + NFV: взаємодія та роль в гнучкому управлінні трафіком та Network Slicing

Традиційні телекомунікаційні мережі історично будувалися за принципом жорсткого зв’язування площин передавання та керування, а також тісної прив’язки мережевих функцій до спеціалізованого апаратного забезпечення. Такий підхід обмежує гнучкість, ускладнює масштабування та впровадження нових сервісів, а також призводить до значних капітальних та операційних витрат. Концепції

Software-Defined Networking (SDN) та Network Function Virtualization (NFV) були запропоновані як взаємодоповнювальні технології, що покликані подолати зазначені обмеження.

SDN передбачає чітке розділення площини керування та площини даних, централізацію прийняття рішень у логічно централізованому контролері та програмований доступ до мережевої інфраструктури через стандартизовані інтерфейси (наприклад, OpenFlow, P4 Runtime). Це дозволяє оператору отримати глобальне уявлення про стан мережі та реалізовувати політики маршрутизації, балансування навантаження й забезпечення якості обслуговування (QoS) на рівні всієї доменної інфраструктури.

NFV, своєю чергою, зосереджується на відокремленні мережевих функцій (маршрутизатор, брандмауер, DPI, EPC/5GC-компоненти тощо) від спеціалізованих апаратних платформ шляхом перенесення їх у програмні віртуальні мережеві функції (VNF), що виконуються на універсальних обчислювальних ресурсах (COTS-сервери, хмарна інфраструктура). Завдяки NFV з’являється можливість гнучкого розгортання, масштабування та міграції мережевих функцій у відповідь на зміну навантаження, вимог абонентів або політик оператора.

Взаємодія SDN та NFV забезпечує основу для побудови динамічних, програмно-керованих і сервісно-орієнтованих мереж. SDN-контролер виступає «мозком» інфраструктури, який керує трафіком і топологією, тоді як NFV-оркестратор забезпечує життєвий цикл VNF, включно з розгортанням, масштабуванням і видаленням. У такій гібридній архітектурі гнучке управління трафіком досягається завдяки поєднанню програмованих механізмів маршрутизації (SDN) та можливості динамічно змінювати набір мережевих функцій на шляху проходження потоків (NFV). Це, зокрема, дозволяє реалізовувати SLA-орієнтовані сервіси, диференціацію класів трафіку, адаптивну інженерію трафіку та автоматизоване відновлення при відмовах [26].

Передумови та ключові концепції мережевого сегментування (Network Slicing). Ресурси. У загальному розумінні ресурс — це керована одиниця, що

характеризується певним набором атрибутів або функціональних можливостей і використовується для надання мережевої послуги. Мережевий зріз (network slice) являє собою сукупність таких ресурсів, які у відповідній комбінації забезпечують виконання вимог конкретного сервісу або сценарію використання.

Мережеві функції — це функціональні блоки, що реалізують визначені мережеві можливості, необхідні для підтримки конкретних послуг. Зазвичай вони виконуються у вигляді програмних екземплярів, що працюють на інфраструктурних ресурсах.

Мережеві функції можуть бути:

- фізичними (PNF) — коли програмне забезпечення жорстко прив’язане до спеціалізованого апаратного забезпечення, утворюючи традиційний апаратний мережевий елемент;
- віртуалізованими (VNF) — коли функціональність відокремлена від апарату, а ПЗ може виконуватися на різних типах обчислювальних платформ.

Інфраструктурні ресурси охоплюють різнорідне апаратне забезпечення та необхідне системне програмне забезпечення для розміщення та з’єднання мережевих функцій. До них належать: обчислювальні потужності, системи зберігання даних, мережеве обладнання та канали зв’язку, що забезпечують маршрутизацію й комутацію, радіодоступні фізичні елементи.

Для використання цих ресурсів у мережевому сегментуванні необхідним є їх абстрагування та логічне розділення за допомогою механізмів віртуалізації. У результаті формуються віртуальні ресурси, що за своїми властивостями функціонально еквівалентні фізичним.

Оркестрація є ще одним ключовим процесом у реалізації мережевого сегментування. У широкому розумінні оркестрацію можна визначити як процес узгодженого поєднання та координації різнорідних елементів у цілісну функціональну систему. У контексті network slicing, де задіяно велику кількість різних суб’єктів та процесів, оркестратор виконує роль координатора, який забезпечує узгоджену взаємодію між мережевими компонентами під час створення, управління та надання мережевих послуг.

На сьогодні не існує єдиного чіткого трактування обсягу та функціональних меж процесу оркестрації. Відповідно до підходу Open Network Foundation (ONF), оркестрація визначається як безперервний процес вибору ресурсів для забезпечення сервісних вимог клієнта оптимальним чином. Поняття оптимальності залежить від політики оптимізації, яка визначає поведінку оркестратора та має відповідати політикам постачальника інфраструктури (InP) і умовам угод про рівень надання послуг (SLA) для клієнтів (орендарів або кінцевих користувачів), що запитують відповідні сервіси. Термін безперервний підкреслює, що доступність ресурсів, вимоги до сервісів і критерії оптимізації можуть змінюватися з часом.

Цікаво, що в ONF оркестрація також розглядається як одна з визначальних функцій SDN-контролера, де клієнтом вважається суб'єкт, який отримує послуги, – відповідно до термінології SDN.

ONF також зазначає, що ключові функції оркестратора включають:

- перевірку відповідності запиту клієнта можливостям системи,
- конфігурацію ресурсів відповідно до сервісних вимог,
- обробку подій та повідомлення про них.

Проте у контексті мережевого сегментування оркестрація не може виконуватися одним централізованим елементом. Це зумовлено не лише значною складністю та широким функціональним охопленням завдань оркестрації, але й необхідністю забезпечення незалежності управління та підтримки рекурсивної структури взаємодії між суб'єктами.

Ізоляція є критично важливою вимогою для забезпечення коректного та надійного функціонування декількох мережевих зрізів, які співіснують на спільній інфраструктурній підкладці. Вона передбачає, що робота, продуктивність та стан одного зрізу не повинні впливати на інші, незалежно від навантаження, відмов чи порушень безпеки. У контексті продуктивності кожен мережевий зріз проєктується для задоволення конкретних сервісних вимог, що зазвичай визначаються через ключові показники ефективності (KPI). Забезпечення ізоляції продуктивності має кінець-у-кінець характер та передбачає підтримання необхідних параметрів якості послуг незалежно від стану або перевантаження інших зрізів, тобто робота одного

зрізу не повинна погіршуватися через деградацію або надмірний трафік у паралельних сегментах. Водночас ізоляція повинна гарантувати безпеку та конфіденційність, що означає відсутність можливості передачі атак, збоїв чи вразливостей між зрізами. Кожен зріз має використовувати автономні функції безпеки, які забезпечують запобігання несанкціонованому доступу до конфігураційної, управлінської та облікової інформації, а також здатність реєструвати спроби доступу незалежно від їх законності. Крім того, кожен зріз повинен розглядатися як незалежна логічна мережа з власними процедурами моніторингу, контролю та конфігурації, а управлінські операції не повинні впливати на інші зрізи або вимагати доступу до їхніх ресурсів. Для реалізації високого рівня ізоляції необхідно визначити та впровадити узгоджені політики та механізми на кожному рівні віртуалізації. Політики визначають, які сутності повинні бути ізольованими, без деталізації способів досягнення цього, тоді як механізми передбачають конкретні технічні засоби та процеси, що забезпечують реалізацію заданих правил. Досягнення необхідного рівня ізоляції можливе лише завдяки комплексній взаємодії віртуалізації та оркестрації: перша забезпечує створення незалежних логічних ресурсів, тоді як друга координує їх використання, гарантує відповідність сервісним вимогам і забезпечує оптимальне використання ресурсів [21].

Переваги мережевого розподілення (Network Slicing). Використання технології мережевого розподілення в транспортних мережах забезпечує низку ключових переваг, серед яких варто виокремити: ізоляцію ресурсів та безпеки, гарантування детермінованої затримки, можливість гнучкої конфігурації топології з’єднань, а також автоматизоване керування життєвим циклом мережевих сегментів.

Ізоляція. З позиції забезпечення якості обслуговування, основною метою ізоляції між мережевими сегментами є запобігання впливу пікових навантажень або аномального трафіку в одному фрагменті на інші сервіси, що співіснують у спільній інфраструктурі. Такий підхід забезпечує незалежність роботи сервісів різних сегментів та мінімізує їх взаємний вплив. Це має особливе значення для

критичних галузей — наприклад, систем розумних електромереж, медичної інфраструктури або портової автоматизації — де спостерігаються жорсткі вимоги до затримки та варіації затримки, а продуктивність суттєво залежить від зовнішніх впливів.

З точки зору інформаційної безпеки, розмежування стає необхідним у випадках, коли дані служб або користувачів (особливо приватних, наприклад банківських чи державних сервісів) не повинні бути доступними іншим абонентам мережі. Це потребує впровадження якісних механізмів безпекової сегментації.

Транспортне мережеве розподілення реалізує три рівні ізоляції: сервісну, ресурсну та експлуатаційну.

- Сервісна ізоляція. Передбачає повне логічне відокремлення пакетів однієї служби від маршрутів іншої в межах єдиної мережевої інфраструктури. Фактично це означає, що з'єднання різних орендарів є взаємно прозорими, що унеможливлює доступ одних користувачів до сервісів інших.

- Ресурсна ізоляція. Спрямована на розділення мережевих обчислювальних та пропускних ресурсів між сегментами. Існують дві моделі: жорстка ізоляція - окремі ресурси виділяються у виключне користування та не можуть бути використані іншими службами; м'яка ізоляція - сегменти можуть поєднувати власні ресурси з ресурсами спільного пулу, що забезпечує певний рівень статистичного мультиплексування.

Комбінування цих підходів надає операторам можливість гнучко адаптувати інфраструктуру під різні SLA, забезпечуючи варіативність сервісних моделей на базі однієї фізичної мережі [10].

Експлуатаційна (O&M) ізоляція. Передбачає можливість автономного управління виділеними сегментами з боку орендарів, що наближає модель використання до приватних мереж. Ізоляція реалізується за рахунок розмежування доступу на рівні інтерфейсів керування.

Детермінована затримка. Сучасні сервіси характеризуються різними вимогами до пропускної спроможності та часових параметрів. Для традиційних послуг допустимими є затримки на рівні понад 100 мс, тоді як критично важливі

застосування — наприклад, системи релейного захисту електромереж — потребують часових показників на рівні 2 мс з гарантованою стабільністю.

Механізми мережевого розподілення дозволяють рознести сервіси з різними вимогами по окремих сегментах, забезпечуючи визначену, передбачувану затримку для сервісів, що функціонують у режимі реального часу або здійснюють промисловий контроль.

Гнучка персоналізація мережевої топології. Еволюція сервісних моделей призводить до переходу від лінійних схем передачі даних до багатовекторних, складних та динамічних з’єднань.

Мережеве розподілення забезпечує можливість формування індивідуальних логічних топологій для різних секторів, додатків або категорій користувачів, що дозволяє задовольняти специфічні потреби у структурі мережевих взаємозв’язків.

Користувачі мережевого сегмента оперують лише власною логічною топологією, не маючи доступу до деталей базової мережі, що з одного боку зменшує складність сприйняття, а з іншого - обмежує розкриття внутрішніх параметрів оператора, посилюючи загальний рівень безпеки.

Автоматизоване керування сегментами мережі. Зі зростанням масштабів і різноманітності сервісів значно збільшується складність адміністрування мережевої інфраструктури, що робить традиційні ручні підходи малоефективними.

Менеджер мережевих сегментів забезпечує повний життєвий цикл керування, починаючи з інтерпретації користувацьких намірів та завершуючи реалізацією сервісу, включно з плануванням, розгортанням, моніторингом, адаптацією та оптимізацією конфігурації. Такий підхід створює можливості для прецизійного управління сервісами на рівні окремих орендарів.

Поступове впровадження інтелектуальних технологій у процеси управління є логічним подальшим етапом розвитку, який сприятиме переходу до інтелектуальних, самоадаптивних мережевих систем.

Мережеве розподілення формує технологічну базу для побудови гнучких, безпечних, масштабованих та ефективних транспортних мереж, здатних задовольняти різноманітні вимоги сервісів та галузей за умов високої динаміки та

складності мережевого трафіку.

Архітектура мережевого розподілення транспортної мережі. Як показано на рисунку 2.4, архітектура мережевого розподілення в транспортній IP-мережі структурно поділяється на три рівні: рівень переспрямування трафіку, рівень керування мережевими сегментами та рівень управління їх життєвим циклом.

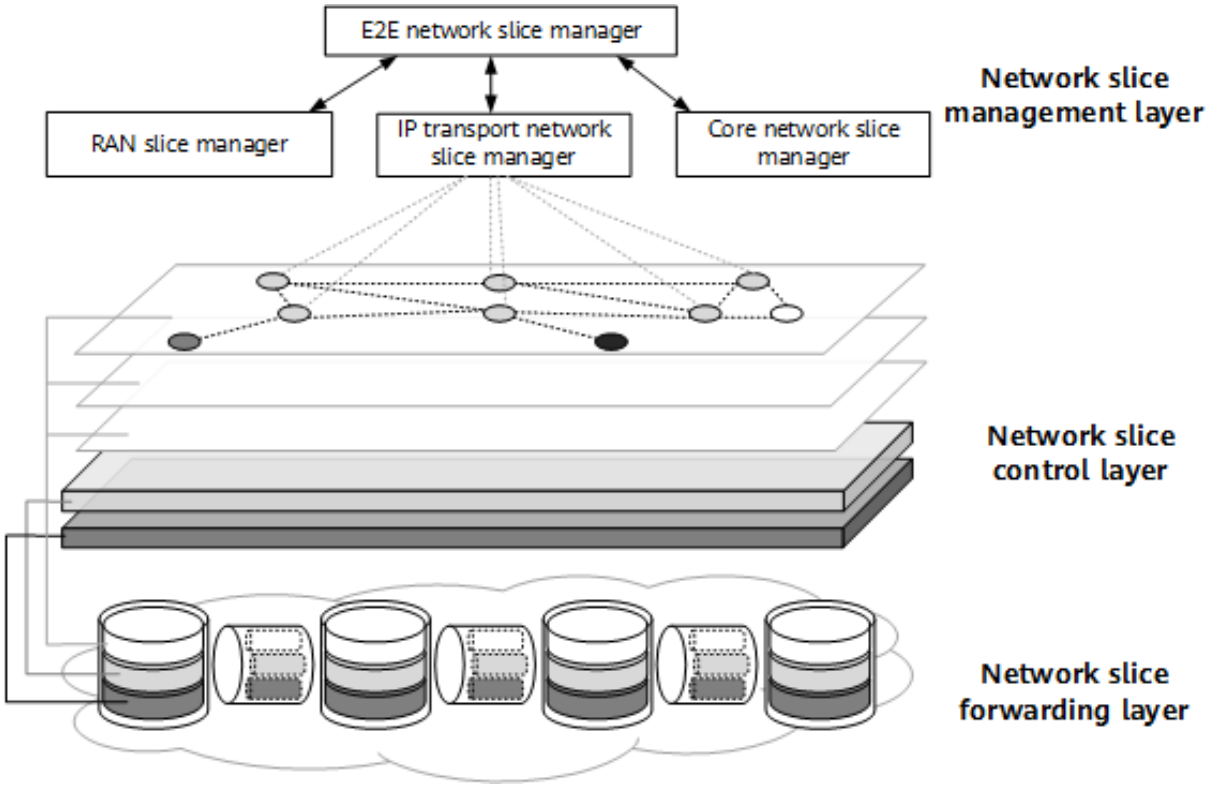


Рис. 2.4 Архітектура розподілення транспортної мережі

Network slice forwarding layer. На рівні переспрямування необхідна наявність гнучких механізмів резервування та деталізованого розподілу ресурсів, що дозволяють сегментувати фізичну інфраструктуру на множину взаємно ізольованих ресурсних пулів, виділених під окремі мережеві сегменти.

Така сегментація реалізується шляхом використання технологій типу FlexE субінтерфейсів, каналізованих субінтерфейсів та ієрархічного QoS (HQoS), що забезпечують диференційований доступ до канальних ресурсів і дозволяють гарантувати їх ізоляцію.

Network slice control layer. Рівень керування мережевими сегментами. Рівень керування забезпечує формування логічних екземплярів мережевих сегментів поверх фізичної мережі, створення індивідуальних топологій та їх відображення на

відповідні набори ресурсів. У результаті формуються мережеві сегменти, здатні задовольняти специфічні вимоги окремих сервісів або груп користувачів.

Даний рівень зазвичай поділяють на площину керування та площину даних.

- Площина керування відповідає за розподіл, агрегацію та обчислення необхідної інформації щодо стану й параметрів мережевих сегментів.
- Площина даних виконує функції ідентифікації належності трафіку до певного сегмента та фізичне переспрямування пакетів відповідно до політик.

Сучасними технологічними механізмами реалізації даного рівня є, зокрема, SRv6 та Flex-Algo, що дозволяють масштабоване та розподілене управління ресурсами.

Network slice management layer. Рівень управління забезпечує повний життєвий цикл функціонування мережевих сегментів, включно з їх плануванням, ініціалізацією, експлуатаційною підтримкою та адаптивною оптимізацією. По суті, він формує інструментарій для оркестрації ресурсів та сервісів у багатосегментному середовищі, забезпечуючи сталість роботи та гнучкість масштабування [7].

Ідентифікація адрес у мережевих сегментах. Найсуттєвішою трансформацією, що супроводжує впровадження мережевого розподілення, є перехід від двовимірної фізичної мережі до багатовимірного середовища з численними логічними мережами, що існують паралельно.

У традиційній мережі кожен вузол має унікальну IP-адресу, і саме вона використовується як ідентифікатор під час маршрутизації. Проте у середовищі з великою кількістю логічних сегментів даний підхід створює значне ускладнення: оскільки різні сегменти можуть мати окремі маршрути та виділені ресурси, було б необхідно призначити окрему IP-адресу кожному вузлу у кожному сегменті.

За умов, наприклад, 1000 фізичних вузлів і 200 сегментів, загальна кількість адрес зростає до 200 000, що призводить до експоненційного зростання складності конфігурації та погіршення продуктивності.

Для мінімізації зазначених проблем використовується двовимірна схема адресації, у якій логічний вузол визначається комбінацією IP-адреси фізичного

вузла та ідентифікатора сегмента (slice ID). Така модель дозволяє планувати лише одну множину IP-адрес, незалежно від кількості сегментів, та не потребує додаткового адресного планування при розширенні інфраструктури.

Більше того, це рішення суттєво скорочує розмір таблиць маршрутизації, забезпечуючи масштабовану підтримку великої кількості сегментів.

Процес переспрямування трафіку на основі двовимірного ідентифікатора. У мережі, що використовує ідентифікацію на основі slice ID, мережевий пристрій підтримує дві незалежні таблиці переспрямування:

- Таблиця маршрутизації, яка визначає вихідний інтерфейс на основі IP-адреси призначення.
- Таблиця відповідності slice ID інтерфейсу, яка визначає, які ресурси (канали або субінтерфейси) зарезервовані за певним сегментом на цьому інтерфейсі.

Алгоритм роботи полягає у наступному: після отримання пакета пристрій спочатку визначає вихідний інтерфейс відповідно до таблиці маршрутизації, потім - на основі slice ID встановлює, які саме ресурси на цьому інтерфейсі повинні бути використані для передачі. Далі пакет передається через відповідний субінтерфейс або канал.

Таким чином, технологія забезпечує диференційоване використання ресурсів навіть у межах одного інтерфейсу, що дає змогу досягати високого рівня ізоляції та передбачуваності продуктивності [25].

2.3 Підходи до оптимізації та балансування трафіку за допомогою SDN. Огляд існуючих рішень та платформ SDN

Load Balancing. Методи балансування навантаження застосовуються для рівномірного розподілу обчислювальних та мережевих задач між вузлами обслуговування з метою мінімізації часу реакції системи. Вибір оптимального сервера для оброблення запитів здійснюється балансувальником навантаження з урахуванням показників завантаженості системних ресурсів. Зазвичай

виокремлюють два підходи до балансування навантаження: реактивний та проактивний.

Проактивні методи формують рішення на основі прогнозування майбутнього використання ресурсів, тоді як реактивні підходи динамічно коригують вагові коефіцієнти для різних ресурсів відповідно до поточної інтенсивності їхнього використання. Незважаючи на те, що проактивні стратегії здатні скоротити час відповіді системи, високий рівень змінності трафіку може зумовлювати значні похибки прогнозування, що робить такі методи менш ефективними у контексті роботи з нерегулярними та непередбачуваними навантаженнями.

У середовищі SDN балансування навантаження передбачає розподіл мережевого трафіку для досягнення оптимальної продуктивності. Така функціональність є ключовою в підвищенні ефективності мережі, особливо з огляду на притаманні SDN централізоване управління та програмованість. Механізми балансування забезпечують рівномірний розподіл трафіку, зменшення затримок, підвищення доступності та масштабованості, а також адаптацію до змінних моделей трафіку. Крім того, вони сприяють покращенню якості обслуговування, інтелектуальній маршрутизації, підвищенню задоволеності користувачів та динамічному управлінню навантаженням, що узгоджується з гнучкою архітектурою SDN.

Статичні алгоритми характеризуються низькою обчислювальною складністю та передбачуваною поведінкою, проте їх застосування обмежене стабільними умовами і вони не здатні ефективно адаптуватися до швидких змін навантаження, характерних для мобільних середовищ. Реактивні підходи базуються на аналізі поточного стану мережі, зокрема завантаження вузлів, довжини черги та пропускної здатності каналів, що забезпечує можливість оперативного реагування, однак підвищує ризик частих переналаштувань маршрутизації, які можуть спричиняти додаткові затримки.

Проактивні алгоритми вирізняються здатністю передбачати зміни трафіку, використовуючи історичні дані та моделі прогнозування. Вони дозволяють формувати політики, спрямовані на попередження перевантажень, а не їх усунення,

що є особливо важливим для сервісів з високими вимогами до надійності й затримки, таких як eMBB, URLLC чи промислові IoT-системи. Водночас точність прогнозів суттєво залежить від обсягу та якості даних. Значного поширення набули інтелектуальні методи балансування, які ґрунтуються на машинному навчанні та алгоритмах підкріплювального навчання. Вони забезпечують прогнозування пікових навантажень, адаптацію політик до поведінки користувачів та здатність до самоорганізації, проте потребують значних обчислювальних ресурсів, навчальних даних та складної інтеграції в загальну інфраструктуру.

Важливим напрямом оптимізації балансування у SDN є використання мультишляхової маршрутизації, яка передбачає розподіл потоків між кількома можливими шляхами для уникнення перевантаження окремих вузлів і підвищення загальної пропускної здатності. Такі рішення характеризуються високою масштабованістю і надійністю, але можуть потребувати складних механізмів синхронізації та уникнення колізій між потоками. У рамках мереж п’ятого покоління окрему увагу приділяють питанням енергетичної ефективності, оскільки значні обсяги інфраструктури, включно з базовими станціями та edge-вузлами, призводять до високих експлуатаційних витрат. Енергетично спрямовані алгоритми балансування застосовують механізми тимчасового відключення малонавантажених вузлів та консолідації трафіку у періоди низької активності.

Впровадження алгоритмів балансування у SDN-мережах супроводжується низкою викликів, серед яких: централізований контролер як потенційна точка відмови, затримки у прийнятті рішень через необхідність постійного збору та обробки даних, обмеження пропускної здатності каналу між контролером і комутаторами, а також можливість нестабільності алгоритмів при пікових навантаженнях. Додатковою проблемою є суперечність між підтримкою QoS та енергоефективністю, що вимагає розробки багатокритеріальних стратегій.

Узагальнюючи, алгоритми балансування навантаження в SDN-орієнтованих мережах п’ятого покоління є ключовим механізмом забезпечення продуктивності, надійності та сервісної якості, оскільки дозволяють оптимально розподіляти ресурси, запобігати утворенню перевантажень та адаптуватися до змінних

характеристик трафіку. Найбільш перспективними напрямами розвитку є використання прогнозуючих моделей, мультишляхових підходів та інтелектуальних алгоритмів, здатних забезпечити адаптивність та високу ефективність при мінімальних затримках, проте їхнє практичне впровадження потребує вирішення питань масштабування, розподіленого контролю та ресурсної оптимізації.

Традиційні алгоритми маршрутизації у контексті SDN та мереж 5G. Традиційні алгоритми маршрутизації, що походять з класичних IP-мереж, відіграли ключову роль у формуванні механізмів передачі даних в Інтернеті. До таких алгоритмів належать протоколи відстані-вектору (distance vector), стану каналу (link state) та гібридні схеми, які реалізовані, зокрема, в RIP, OSPF, BGP та інших протоколах маршрутизації. У традиційних мережах ці алгоритми функціонують у децентралізованому режимі, де кожен роутер самостійно приймає рішення на основі локальної інформації.

Перенесення цих алгоритмів у архітектуру Software-Defined Networking докорінно змінює парадигму управління, оскільки в SDN процес прийняття рішень централізується на рівні контролера. Таким чином, типовий механізм маршрутизації полягає не у самостійній обробці пакетів вузлом, а у встановленні правил пересилання за вказівкою контролера.

У контексті мереж 5G, де обсяг і швидкість трафіку суттєво зростають, а вимоги до затримки та надійності стають критичними, виявляється, що традиційні алгоритми не завжди здатні забезпечити оптимальну продуктивність без модифікацій. Зокрема, виникає потреба у:

- швидкій конвергенції після змін у топології,
- масштабуванні на великі та географічно розподілені мережі,
- підтримці SLA та QoS,
- безпеці контрольного каналу.

Інтеграція OSPF у SDN. Одним із найбільш досліджуваних традиційних алгоритмів у контексті SDN є Open Shortest Path First (OSPF), який базується на аналізі стану каналів і обчисленні найкоротших шляхів.

У SDN-середовищах OSPF може використовуватися для симуляції поведінки традиційних мереж або для забезпечення сумісності зі старими сегментами інфраструктури. Дослідження показують, що інтеграція OSPF у SDN дає можливість оцінити:

- час конвергенції після змін маршруту,
- стабільність передачі,
- якість сервісу в умовах динамічного трафіку.

Особливо актуальним це стає у 5G-середовищах, де характеристики каналів та навантаження змінюються дуже швидко. Проте накладні витрати на обробку таблиць можуть обмежувати масштабованість у макромережах.

Використання BGP у SDN. Іншим поширеним протоколом є Border Gateway Protocol (BGP), який традиційно застосовується для маршрутизації між автономними системами.

У SDN він може використовуватися як механізм обміну маршрутною інформацією між контролером та зовнішніми мережами, що важливо для побудови:

- міжоператорських 5G-мереж,
- мультидоменних інфраструктур,
- хмарних датацентрів з мобільним доступом.

Інтеграція BGP дозволяє SDN-контролеру динамічно налаштовувати правила пересилання, ґрунтуючись на отриманих маршрутах, що збільшує гнучкість мережі.

Поведінка BGP-клієнтів може бути керована через механізми OpenFlow або API, що надає можливість формувати політики на рівні сервісів.

Евристичні алгоритми оптимізації в SDN для 5G. Евристичні алгоритми розглядаються як один із найперспективніших підходів до оптимізації роботи SDN у мережах п’ятого покоління, оскільки вони дозволяють знаходити достатньо ефективні рішення в умовах високої складності, обмеженого часу обчислення та динамічних змін топології. На відміну від традиційних оптимізаційних методів, що часто орієнтовані на отримання точного оптимуму, евристичні підходи прагнуть знайти прийнятний розв’язок, який задовольняє ключові вимоги системи при

мінімальних витратах ресурсів, що особливо актуально у мобільних 5G-середовищах. У SDN ключовою метою евристичних алгоритмів є забезпечення збалансованого розподілу трафіку, вибору маршрутів з мінімальною затримкою, уникнення перенавантажень та підтримка якості сервісу у реальному часі.

Важливою особливістю застосування евристик у SDN є можливість адаптації до контексту трафіку, включно з аналізом пропускної здатності каналів, завантаженням вузлів, довжиною черг та історичними даними щодо навантаження. Це дозволяє формувати маршрути, які враховують не тільки топологічні характеристики мережі, а й її поточний стан. У разі різнорідності сервісів, що є типовою для мереж п’ятого покоління, евристичні методи здатні диференціювати потоки відповідно до їхніх вимог до QoS, забезпечуючи ефективну підтримку eMBB, URLLC та mMTC-орієнтованих сценаріїв.

Евристичні алгоритми активно застосовуються для балансування навантаження, де їхньою метою є запобігання перевантаженню вузлів та підвищення пропускної здатності шляхом динамічного розподілу потоків на кілька каналів. Такі підходи дозволяють збільшувати продуктивність мережі та скорочувати затримку, проте можуть призводити до фрагментації трафіку та збільшення накладних витрат на керування. Окрім балансування, вагоме значення має енергетична оптимізація, адже великі масштаби 5G-інфраструктури зумовлюють зростання операційних витрат. Евристичні алгоритми дозволяють знижувати енергоспоживання шляхом вимкнення малонавантажених вузлів або консолідації потоків у періоди низької активності, що є критичним для економічно ефективного функціонування мобільних мереж.

Попри значну гнучкість, евристичні алгоритми мають низку обмежень, які важливо враховувати при їх застосуванні у SDN-орієнтованих 5G-системах. Зокрема, рішення, отримані евристичними методами, часто наближені до оптимальних, але не гарантують глобальної оптимальності, що може призводити до нераціонального використання ресурсів у масштабних мережах. Додатковими труднощами є ймовірність потрапляння у локальні оптимуми, чутливість до вибору параметрів та нестабільність у середовищах з високою частотою змін. У разі

недостатнього налаштування алгоритмів може спостерігатися нестабільність рішень, що негативно впливає на QoS та загальну пропускну здатність.

Попри зазначені недоліки, евристичні підходи залишаються важливою складовою оптимізації SDN для мереж п’ятого покоління, оскільки забезпечують необхідний компроміс між якістю рішень і швидкістю їх обчислення, що є критичним для реалізації реального часу. Вони дозволяють формувати гнучкі механізми маршрутизації та розподілу ресурсів, що враховують багатокритеріальні обмеження, підтримують диференційовані сервіси та здатні адаптуватися до змінних характеристик мережі. Найбільш перспективним напрямом розвитку є інтеграція евристичних методів з прогнозуючими й інтелектуальними алгоритмами, що дозволить підвищити точність рішень, забезпечити проактивне управління трафіком та покращити ефективність використання ресурсів у масштабних 5G-інфраструктурах.

Алгоритми на основі штучного інтелекту та машинного навчання в SDN для мереж 5G. В умовах мереж п’ятого покоління, що характеризуються високою динамічністю трафіку, різнорідністю сервісів, великою кількістю пристроїв та вимогами до надзвичайно низької затримки, традиційні та евристичні алгоритми оптимізації часто виявляються недостатньо ефективними. Вони здатні забезпечувати реактивне управління, однак зазвичай не враховують складних залежностей у трафіку, не прогнозують майбутній стан мережі й не забезпечують відповідний рівень автономності. Тому дедалі більше уваги приділяється алгоритмам, які застосовують технології штучного інтелекту та машинного навчання для створення адаптивних, прогнозуючих і самонавчальних механізмів управління SDN-мережами у середовищі 5G. Їх ключовою особливістю є здатність аналізувати великі обсяги даних, виявляти приховані закономірності, адаптувати конфігурацію мережі у реальному часі та формувати політики на основі попереднього досвіду.

Методи машинного навчання забезпечують широкий спектр функціональних можливостей для оптимізації SDN у 5G. Алгоритми навчання з учителем використовуються для класифікації трафіку, прогнозування показників QoS,

виявлення аномалій та прийняття рішень щодо маршрутизації на основі емпіричних даних. Натомість алгоритми без учителя застосовують для групування потоків, аналізу поведінкових патернів та виявлення аномалій, що не мають попередньо визначених ознак. Особливе значення для 5G має підкріплювальне навчання, яке дозволяє формувати політики управління шляхом взаємодії з мережею, оцінки наслідків прийнятих рішень та поступового покращення стратегії. Такий підхід забезпечує здатність до самоорганізації, автономності та адаптації до мінливого середовища, що є критично важливим у високонавантажених та розподілених мережах.

Одним із ключових напрямів застосування алгоритмів ШІ є прогнозування мережевого трафіку та QoS-параметрів, оскільки знання майбутніх змін дозволяє завчасно формувати оптимальні маршрути, запобігати перевантаженням, керувати пріоритетами потоків та коригувати політики розподілу ресурсів. У цьому контексті використовуються як класичні часові моделі, так і глибокі нейронні мережі, що здатні враховувати нелінійні залежності та складні взаємозв’язки між різними параметрами мережі. Особливо актуальним прогнозування стає для сервісів URLLC, що вимагають гарантованої надійності та мінімальної затримки, а також для сценаріїв мобільності, коли топологія мережі може змінюватися у реальному часі.

Алгоритми машинного навчання також активно застосовуються для виявлення і реагування на аномалії, що є важливим аспектом безпеки SDN-мереж. Використання моделей кластеризації, автоенкодерів та нейронних мереж дозволяє ідентифікувати нестандартні патерни поведінки, включно з кіберзагрозами, які не можуть бути виявлені традиційними сигнатурними методами. Інтеграція таких рішень у SDN-контролер забезпечує оперативне реагування на інциденти, ізоляцію атакованих сегментів та перенаправлення трафіку, що сприяє підвищенню надійності та безпеки мереж.

Попри очевидні переваги алгоритмів штучного інтелекту, їх впровадження в SDN для 5G супроводжується низкою викликів. Серед них — потреба у значних обчислювальних ресурсах, необхідність доступу до великих масивів якісних даних, складність забезпечення швидкодії у реальному часі, а також недостатня прозорість рішень, що формуються складними моделями глибокого навчання. Крім того, алгоритми машинного навчання можуть бути чутливими до змін середовища, що вимагає постійного перенавчання або адаптації моделей, а процес прийняття рішень іноді може суперечити вимогам SLA або пріоритетам мережевих сервісів.

У загальному підході алгоритми штучного інтелекту трансформують SDN із реактивної системи управління у проактивну, здатну передбачати мережеві події, автоматично адаптуватися до потоку даних та оптимізувати політики з урахуванням сервісних вимог і динаміки середовища. У довгостроковій перспективі вони формують технологічну основу для побудови автономних, самонавчальних комунікаційних систем, що поступово наближає концепцію 5G до повної автономності та створює передумови для розвитку мереж шостого покоління.

Порівняльний аналіз алгоритмів оптимізації трафіку для SDN у мережах п’ятого покоління. Різноманіття алгоритмів, що застосовуються для оптимізації маршрутизації та управління трафіком у SDN-мережах, зумовлено складністю мережевого середовища та різнорідністю сервісних вимог у 5G. Враховуючи високу варіативність навантаження, мобільність користувачів та критичність QoS-параметрів, постає потреба у формуванні порівняльної оцінки різних класів алгоритмів, що дозволить визначити їх релевантність до конкретних сценаріїв застосування.

Таблиця 2.2

Порівняння характеристик оптимізації трафіку для SDN

Характеристика	Традиційні	Евристичні	AI/ML
Затримка	Середня/висока	Низька	Низька
QoS-орієнтація	Низька	Середня	Висока
Прогнозування стану	Відсутня	Частково	Так
Адаптивність	Низька	Середня	Висока
Обчисл. складність	Низька	Низька/середня	Висока
Стійкість	Висока	Середня	Залежить від моделі
Автономність	Ні	Частково	Так
Придатність до Real-Time	Низька	Висока	Висока

На основі порівняння можна зробити такі висновки:

1. Традиційні алгоритми забезпечують базову функціональність і масштабованість, але недостатньо гнучкі для змінного середовища 5G.

2. Евристичні алгоритми є оптимальними для оперативного управління та балансування навантаження, але не гарантують глобального оптимуму.

3. Алгоритми AI/ML пропонують найвищий рівень адаптивності, здатність до прогнозування та QoS-орієнтації, що робить їх найбільш перспективними для майбутніх 5G-мереж.

Ключовим є комбінований підхід, де:

- традиційні алгоритми забезпечують основу,
- евристичні — оперативну оптимізацію,
- AI/ML — довгострокову адаптацію.

Оптимальні рішення повинні бути розподіленими, контекстно-орієнтованими та здатними працювати у режимі реального часу

В наступному розділі буде більш розкрито використання LoxiLB, та попередню схему роботи продемонстровано на рисунку 2.5.

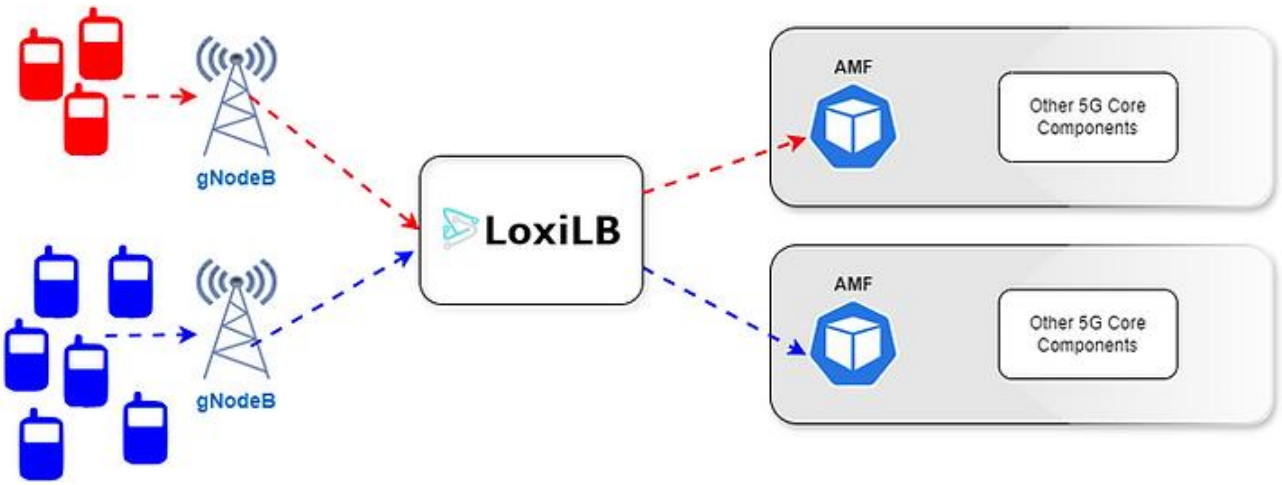


Рис. 2.5 Схема роботи LoxiLB

У межах класифікації підходів до балансування трафіку, що включає традиційні, евристичні та алгоритми на основі штучного інтелекту, LoxiLB використовує переважно евристичний підхід із опорою на традиційні механізми, не реалізуючи власних AI/ML-алгоритмів. Традиційна складова проявляється у використанні детермінованих правил балансування та статичних політик, які забезпечують базову стабільність, передбачуваність поведінки та коректне функціонування балансувальника у стандартних режимах експлуатації. Такі механізми формують фундамент роботи системи та гарантують мінімальні накладні витрати на прийняття рішень.

Ключовою ж особливістю LoxiLB є застосування реактивного евристичного підходу, за якого рішення щодо розподілу трафіку приймаються на основі поточного стану мережі та сервісів. Балансування здійснюється з урахуванням активних з’єднань, доступності вузлів, характеристик транспортного рівня та динамічних параметрів трафіку, що дозволяє оперативно адаптувати маршрути переспрямування без попереднього довгострокового прогнозування. Саме цей підхід є найбільш ефективним для середовищ із високою мінливістю навантаження, характерних для мереж 5G Core та контейнеризованих SDN/NFV-інфраструктур.

Алгоритми на основі штучного інтелекту та машинного навчання в LoxiLB безпосередньо не застосовуються. Функції довгострокової адаптації, прогнозування трафіку та стратегічної оптимізації мережевих ресурсів покладаються на зовнішні системи управління, зокрема SDN-контролери, NFV-оркестратори або аналітичні платформи. У такій архітектурі LoxiLB виконує роль високопродуктивного виконавчого компонента площини даних, який реалізує політики, сформовані на вищих рівнях управління.

Отже, з точки зору запропонованої триєдиної класифікації, LoxiLB доцільно віднести до евристичного підходу балансування навантаження з використанням традиційних алгоритмічних механізмів як бази, без інтеграції власних AI/ML-рішень. Така позиція є коректною з наукової точки зору та повністю узгоджується з архітектурою SDN-орієнтованих мереж п’ятого покоління [8].

3 ВПРОВАДЖЕННЯ SDN ДЛЯ УПРАВЛІННЯ ТРАФІКОМ У 5G

3.1 Огляд існуючих рішень та платформ SDN

Програмно-визначені мережі (SDN) відіграють ключову роль у сучасних інформаційно-телекомунікаційних системах, оскільки забезпечують необхідний рівень гнучкості, масштабованості та автоматизації для підтримки високодинамічних мережевих сервісів. На відміну від традиційних мережевих архітектур, де площина управління інтегрована безпосередньо у мережеві пристрої та функціонує ізольовано, SDN передбачає її централізацію в єдиному контролері, що координує маршрутизацію, обробку і трансформацію потоків даних. Такий підхід дозволяє операторам мобільного зв’язку швидко реагувати на зміну навантаження, впроваджувати складні політики управління трафіком і оптимізувати використання ресурсів у масштабах мережі. Особливо значущою ця концепція стає в епоху 5G, де кількість взаємодій між мережевими функціями значно зростає, а вимоги до часу реакції та пропускної здатності стають критичними.

Першим кроком до реалізації повноцінних SDN-технологій стало впровадження протоколу OpenFlow, який запропонував революційну на той час можливість програмного керування таблицями потоків на мережевих пристроях. Хоча сьогодні OpenFlow поступово відходить на другий план через апаратні обмеження та складність масштабування, його концептуальний внесок у розвиток SDN є беззаперечним. Саме завдяки OpenFlow з’явилася можливість централізованого контролю за комутацією, яка згодом стала фундаментом для сучасних SDN-контролерів, таких як OpenDaylight та ONOS. Ці платформи забезпечили перехід від жорстких, статичних мереж до динамічних систем з програмним визначенням поведінки, здатних до самовідновлення та адаптації під змінні умови трафіку.

OpenDaylight, наприклад, став одним з перших масштабованих, модульних SDN-контролерів, орієнтованих на застосування у великих операторських

мережах. Його можливість інтегруватися з протоколами NETCONF, BGP-LS і PCEP забезпечила сумісність зі змішаними середовищами, де використовуються як традиційні, так і сучасні мережеві технології. ONOS, у свою чергу, був створений з урахуванням високих вимог до відмовостійкості та продуктивності. Завдяки розподіленій архітектурі та кластеризації ONOS демонструє здатність обробляти значні обсяги трафіку та виконувати складні обчислення, що робить його придатним для операторських мереж рівня Tier-1. У мобільних мережах ONOS і OpenDaylight реально використовуються для керування транспортними магістралями, SD-WAN-рішеннями та MEC-інфраструктурою [28].

Однак у міру розвитку хмарних технологій та контейнеризації з'явилась потреба у більш гнучких механізмах взаємодії з мережею, ніж ті, що надавали класичні SDN-контролери. З появою eBPF/XDP відбувся якісний стрибок у можливостях програмної обробки пакетів: відтепер користувацькі програми можуть виконувати низькорівневі операції у ядрі операційної системи з мінімальними затримками. Це дозволило реалізувати високопродуктивні балансувальники, проксі-сервери, системи контролю доступу та аналітики без втрати пропускної здатності. Фактично eBPF став «новим OpenFlow», але тепер не обмеженим спеціалізованим апаратним забезпеченням. На основі eBPF створено низку передових платформ, включаючи Cilium, LoxiLB та інструменти, оптимізовані для телеком-рішень 5G Standalone.

Паралельно з eBPF розвивалася концепція програмованих dataplane-рішень, представлена мовою P4. Вона відкрила можливість точного визначення способів обробки пакетів без потреби у модифікації обладнання. Для мобільних мереж таке програмування є особливо корисним, оскільки дозволяє створювати мережеві сервіси, адаптовані до нових вимог щодо сигналізації, QoS і сегментації трафіку у мережах 5G та майбутніх 6G.

Зі збільшенням масштабів віртуалізації логічним рішенням стало застосування Kubernetes як платформи для оркестрації контейнеризованих мережевих функцій (CNF). Kubernetes не є SDN-контролером у класичному розумінні, але він формує програмну площину управління для мережевих сервісів, реалізуючи розподілену

логіку керування, автоматичне оновлення, контроль станів і масштабування. CNI-плагіни виконують роль dataplane-шару, що уможливлює формування складних операторських топологій усередині кластерів. У такому середовищі Multus CNI забезпечує мультиінтерфейсність pod'ів, що є критично важливим для контейнеризованих AMF, SMF і UPF, оскільки вони мають працювати з декількома незалежними мережевими сегментами. Compatibility Multus із MACVLAN робить можливим наближення контейнеризованих топологій до реальних апаратних конфігурацій операторів мобільного зв'язку.

Особливе значення для побудови контейнеризованих телеком-середовищ має LoxiLB — SDN-орієнтований балансувальник нового покоління. Він побудований із використанням eBPF і орієнтований на роботу у Kubernetes, забезпечуючи мінімальні затримки, значну пропускну здатність та підтримку протоколів транспортного рівня, включно із SCTP. Остання властивість є ключовою для мобільних мереж п'ятого покоління, де протокол SCTP використовується у критично важливих процесах реєстрації та управління UE через NGAP. Завдяки LoxiLB стає можливим гнучке балансування навантаження між кількома AMF-екземплярами, що напряму підвищує масштабованість і надійність мережі. На відміну від комерційних апаратних балансувальників, які традиційно застосовуються у мобільних мережах, LoxiLB є відкритим програмним рішенням, здатним до інтеграції з контейнерними середовищами та адаптації до мінливих вимог оператора.

У контексті розвитку 5G SDN стає основою для реалізації інтелектуальних систем дистанційного управління мережевими параметрами. Завдяки централізованому керуванню оператор отримує змогу автоматизувати політики QoS, оптимізувати маршрутизацію, виконувати динамічне масштабування мережевих функцій і забезпечувати швидке реагування на зміни трафіку та відмови. Це особливо актуально у великих мережах, де AMF, SMF та інші функції розгортаються у кількох екземплярах, а їх взаємодія повинна відбуватися в режимі реального часу. У таких середовищах SDN-механізми не лише спрощують управління інфраструктурою, але й створюють підґрунтя для автоматизованого,

гнучкого та адаптивного керування мережею у рамках концепції self-organizing network (SON), що є важливим напрямом розвитку мобільних мереж.

Loxilb. Платформа loxilb була започаткована як проєкт, спрямований на спрощення розгортання хмарноорієнтованих та Kubernetes-навантажень у периферійних обчислювальних середовищах. У публічних хмарах на кшталт AWS чи GCP винесення сервісів у зовнішню мережу зазвичай не потребує значних зусиль: ці платформи типово забезпечують вбудовані зовнішні балансувальники навантаження, які гарантують ефективну маршрутизацію вхідного трафіку.

Натомість для локальних та edge-розгортань ситуація є суттєво іншою, оскільки в таких середовищах відсутні нативні механізми, аналогічні ServiceType=LoadBalancer. Протягом тривалого часу MetalLB залишався практично єдиним дієвим рішенням. Однак периферійні робочі навантаження висувають низку специфічних вимог: вони часто використовують спеціалізовані протоколи на кшталт QUIC, SCTP, SRv6, а також характеризуються жорсткими обмеженнями щодо затримки та ресурсів системи. Створення надійної та безшовної інфраструктури в таких умовах потребує глибокого розуміння особливостей мережевих протоколів і ретельного архітектурного опрацювання.

Зі зростанням кількості користувачів, які зверталися по вирішення подібних завдань, стало очевидно, що традиційний стек мережевої підсистеми Linux, попри свою зрілість і стабільність, не забезпечує достатньої гнучкості для оперативної підтримки широкого спектра протоколів та сценаріїв станового балансування навантаження, актуальних для edge-середовищ.

Ці виклики зумовили перехід до використання eBPF — потужної технології Linux, що дає змогу безпечно виконувати ізольовані програми безпосередньо в ядрі системи. eBPF дозволяє розширювати функційність ядра без модифікації його початкового коду та без суттєвих накладних витрат на продуктивність. Завдяки цьому eBPF забезпечує необхідну гнучкість і високу швидкодію для сучасних мережевих застосувань, не потребуючи виділених ядер CPU, що робить його оптимальною основою для легковагових та енергоефективних edge-архітектур.

loxilb — це відкритий хмарноорієнтований балансувальник навантаження,

реалізований мовою Go з використанням eBPF. Його спроєктовано для забезпечення уніфікованої роботи в середовищах «on-premise», публічних хмарах та гібридних інфраструктурах, побудованих на Kubernetes.

Основним призначенням loxilb є підтримка ефективного та гнучкого балансування навантаження для робочих навантажень нового покоління, зокрема в умовах складних архітектур. Rішення орієнтоване на потреби телекомунікаційних систем, мобільних мереж та edge-комп'ютингу, де активно впроваджуються хмарні технології та сучасні мережеві протоколи [30].

Використання eBPF забезпечує високопродуктивну комутацію трафіку з глибокою протокольною обізнаністю, мінімальними витратами системних ресурсів і модульною архітектурою. Завдяки цьому loxilb є придатним як для традиційних, так і для інноваційних інфраструктурних рішень.

У Kubernetes визначено кілька типів сервісів — ClusterIP, NodePort, LoadBalancer та Ingress, — кожен з яких забезпечує специфічні сценарії взаємодії: від комунікації між pod-ами до надання доступу до сервісів із зовнішньої мережі.

Усі ці механізми ґрунтуються на роботі балансувальників навантаження або проксі-рішень рівнів L4 чи L7. Завдяки модульності Kubernetes ці функції можуть реалізовувати різні програмні компоненти. Наприклад, kube-proxy зазвичай обслуговує ClusterIP та NodePort. Натомість для LoadBalancer та Ingress Kubernetes, як правило, не містить вбудованого провайдера.

У публічних хмарах типу AWS управління сервісами LoadBalancer виконується на рівні інфраструктури. Проте в локальних або самокерованих Kubernetes-кластерах вибір рішень суттєво обмежений. Навіть у керованих середовищах, таких як Amazon EKS, багато користувачів віддають перевагу власним балансувальникам через потребу в розширених можливостях, ширшому контролі чи підтримці специфічних протоколів.

Проблема стає ще суттєвішою у сферах 5G-телекомунікацій та edge-комп'ютингу, де застосовуються складні протоколи: QUIC, GTP, SCTP, SRv6, SEPP, DTLS тощо. Такі сценарії потребують високої продуктивності, протоколоорієнтованої обробки та гнучкої конфігурованості. loxilb створено саме

для задоволення цих вимог: він нативно підтримує тип сервісу LoadBalancer та може бути розгорнутий як у межах кластеру, так і поза ним.

За замовчуванням loxilb функціонує як L4-балансувальник навантаження та сервісний проксі. Хоча L4 забезпечує високу швидкодію та широкий спектр протоколів, Kubernetes також отримує значні переваги від L7-функціональності. Для цього loxilb підтримує балансування навантаження на L7-рівні в рамках своєї реалізації Ingress, підсиленої за допомогою eBPF-механізмів sockmap. Таким чином, loxilb виступає єдиним рішенням, що інтегрує можливості балансування на рівнях L4 та L7 для сучасних Kubernetes-середовищ [30].

eBPF. Фільтр пакетів Berkeley Packet Filter (BPF) був запропонований у 1992 році як високоефективний механізм фільтрації мережевих пакетів. Мережевий пакетний фільтр виконує функцію контролю трафіку, що надходить у мережу або виходить з неї, шляхом аналізу пакетів у процесі їх проходження крізь фільтр. Автори визначили BPF як рішення, що забезпечує продуктивність, приблизно у двадцять разів вищу порівняно з наявними на той час технологіями. Відмінністю BPF від попередніх систем була можливість виконання програм у віртуальній машині, орієнтованій на регістрову архітектуру, а також використання буферів на рівні застосунків, що усували необхідність копіювання всіх даних для прийняття рішення. Завдяки цьому BPF швидко став галузевим стандартом та був широко впроваджений як основна технологія мережевої фільтрації пакетів [27].

У 2014 році Олексій Старовойтов запропонував eBPF як модернізовану архітектуру BPF, адаптовану до вимог сучасного апаратного забезпечення. Віртуальна машина eBPF забезпечує значно вищу продуктивність, оскільки її модель обчислень наближена до принципів роботи сучасних процесорів, що дозволяє більш ефективно відображати інструкції eBPF на апаратний набір інструкцій (ISA). У представленому О. Старовойтовим коміті 2014 року eBPF був відкритий для використання з користувацького простору, і невдовзі його застосування перестало обмежуватися суто мережевим стеком. З часом eBPF перетворився на універсальний інструмент розширення функціональності ядра.

Ключовою перевагою eBPF є можливість модифікації поведінки ядра без його

перекомпіляції та перезавантаження системи, при цьому забезпечується безпечніший та простіший інтерфейс порівняно з програмуванням модулів ядра. Архітектура eBPF включає статичний верифікатор, який гарантує, що програма не спричинить аварійного завершення роботи ядра і матиме гарантоване завершення. Після компіляції eBPF-програма проходить перевірку верифікатором, який підтверджує її безпечність для виконання [27].

3.2 Розгортання та налаштування контейнеризованого середовища для дослідження 5G Core і SDN-балансування

У цьому підрозділі детально описується процес розгортання експериментального середовища, призначеного для дослідження механізмів балансування навантаження протоколу SCTP у ядрі мережі п’ятого покоління за допомогою SDN-орієнтованої платформи LoxiLB. Проєкт реалізовано на основі контейнеризованої інфраструктури Kubernetes, доповненої мультиінтерфейсною мережею Multus CNI, мережевими плагінами MACVLAN та стеком Open5GS як реалізацією компонентів 5G Core. Для моделювання радіодоступу використовувався симулятор my5G-RANTester. Схема роботи та логічна архітектура продемонстрована на рисунку 3.1.

Підготовка архітектури та середовища виконання. Експериментальний стенд формувався як багатовузловий кластер Kubernetes, розгорнутий за допомогою Kind (Kubernetes-in-Docker) [29]. Такий підхід забезпечив ізоляцію, повторюваність та можливість швидкого відтворення інфраструктури. Використання Docker як базового середовища дозволило створити віртуалізовані вузли (1 вузол керування та 2 робочі вузли), що емулюють розподілену мережу оператора.

Перед початком конфігурації користувача було додано до групи Docker для забезпечення роботи без привілейованих прав. Після цього перевірено функціонування демонів контейнеризації, що підтверджується виводом активних контейнерів. З цим можна ознайомитися на рисунку 3.2.

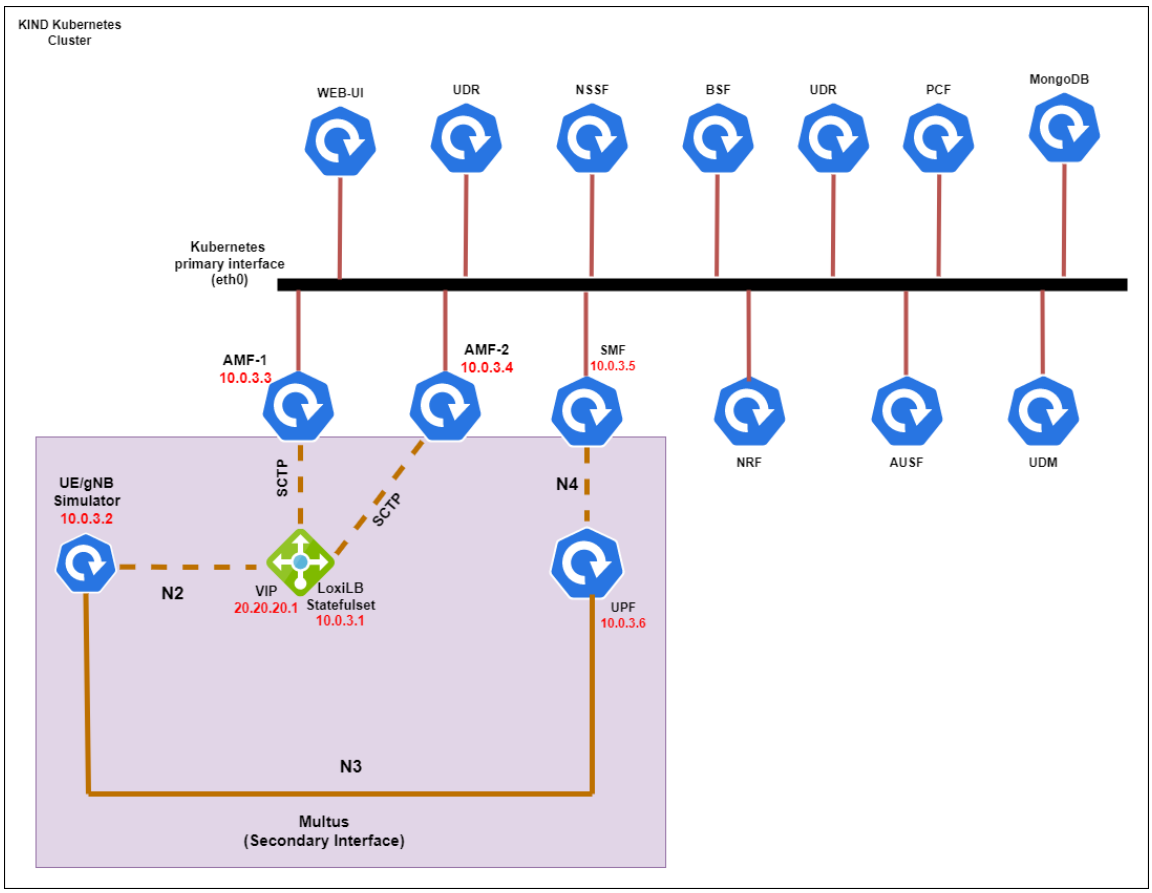


Рис. 3.1 Архітектура дослідження 5G Core і SDN-балансування

Створення Kubernetes-кластера за допомогою Kind. Кластер формувався відповідно до YAML-конфігурації *config-3node.yml*, яка визначає один master-вузол та два worker-вузли. Процес розгортання включав підготовку базових образів, активацію CNI-плагіна та об'єднання робочих вузлів у єдине кероване середовище. Результат успішного створення кластера наведено на рисунку 3.3.

```
chornob@mankotest3:~/5gcore-sctp-loadbalancer$ sudo usermod -aG docker $USER
chornob@mankotest3:~/5gcore-sctp-loadbalancer$ newgrp docker
chornob@mankotest3:~/5gcore-sctp-loadbalancer$ docker ps
CONTAINER ID   IMAGE                  COMMAND                  CREATED         STATUS         PORTS                       NAMES
c005f7c240f0   kindest/node:v1.30.0   "/usr/local/bin/entr…"   13 minutes ago   Up 13 minutes                              kind-worker2
1dff7c43bd61   kindest/node:v1.30.0   "/usr/local/bin/entr…"   13 minutes ago   Up 13 minutes                              kind-worker
c37baab19662   kindest/node:v1.30.0   "/usr/local/bin/entr…"   13 minutes ago   Up 13 minutes   127.0.0.1:40779->6443/tcp   kind-control-plane
chornob@mankotest3:~/5gcore-sctp-loadbalancer$ kind export kubeconfig --name kind
Set kubectl context to "kind-kind"
chornob@mankotest3:~/5gcore-sctp-loadbalancer$ kubectl get nodes
NAME                 STATUS   ROLES           AGE   VERSION
kind-control-plane   Ready    control-plane   13m   v1.30.0
kind-worker          Ready    <none>          13m   v1.30.0
kind-worker2         Ready    <none>          13m   v1.30.0
chornob@mankotest3:~/5gcore-sctp-loadbalancer$ kubectl create -f multus-daemonset.yml
customresourcedefinition.apiextensions.k8s.io/network-attachment-definitions.k8s.cni.cncf.io created
clusterrole.rbac.authorization.k8s.io/multus created
clusterrolebinding.rbac.authorization.k8s.io/multus created
serviceaccount/multus created
configmap/multus-cni-config created
daemonset.apps/kube-multus-ds created
```

Рисунок 3.2 Перевірка роботи Docker-середовища

```
chornob@mankotest3:~/5gcore-sctp-loadbalancer$ sudo kind create cluster --config config-3node.yml
Creating cluster "kind" ...
 ✓ Ensuring node image (kindest/node:v1.30.0) 🖼
 ✓ Preparing nodes 📦 📦 📦
 ✓ Writing configuration 📜
 ✓ Starting control-plane 🕹️
 ✓ Installing CNI 🔌
 ✓ Installing StorageClass 💾
 ✓ Joining worker nodes 🚜
Set kubectl context to "kind-kind"
You can now use your cluster with:

kubectl cluster-info --context kind-kind

Thanks for using kind! 😊
```

Рисунку 3.3 Створення тривузлового кластера Kind

Після ініціалізації було виконано верифікацію стану вузлів за допомогою команди *kubectl get nodes*. Усі вузли перейшли у стан *Ready*, що свідчить про коректність конфігурації. Наведено на рисунку 3.4.

```
chornob@mankotest3:~/5gcore-sctp-loadbalancer$ sudo -s
root@mankotest3:/home/chornob/5gcore-sctp-loadbalancer# kubectl -n kube-system get po
NAME                                         READY   STATUS    RESTARTS   AGE
coredns-7db6d8ff4d-pt72r                     1/1     Running   0          16m
coredns-7db6d8ff4d-ztw8k                     1/1     Running   0          16m
etcd-kind-control-plane                      1/1     Running   0          16m
kindnet-4pnrs                                1/1     Running   0          16m
kindnet-hq2qf                                1/1     Running   0          16m
kindnet-ttkl5                                1/1     Running   0          16m
kube-apiserver-kind-control-plane            1/1     Running   0          16m
kube-controller-manager-kind-control-plane   1/1     Running   0          16m
kube-multus-ds-58xwd                         1/1     Running   0          2m21s
kube-multus-ds-pzllr                         1/1     Running   0          2m21s
kube-multus-ds-xv654                         1/1     Running   0          2m21s
kube-proxy-crhvp                             1/1     Running   0          16m
kube-proxy-hhv2m                             1/1     Running   0          16m
kube-proxy-khpk2                             1/1     Running   0          16m
kube-scheduler-kind-control-plane            1/1     Running   0          16m
```

Рис. 3.4 Верифікація стану вузлів

Оскільки реалізація компонентів 5G Core вимагає підтримки багатьох мережевих інтерфейсів, до кластера було інтегровано Multus CNI, що надає можливість створення множинних мережевих інтерфейсів на pod-рівні. Розгортання Multus здійснювалося шляхом застосування відповідного манифеста daemonset , продемонстровано на рисунку 3.5.

Для забезпечення сумісності з MACVLAN та іншими плагінами було додатково встановлено набір стандартних CNI-плагінів за допомогою *cni-*

install.yml.

```
chornob@mankotest3:~/5gcore-sctp-loadbalancer$ kubectl create -f cni-install.yml
 created
daemonset.apps/install-cni-plugins createdconfigmap/cni-install-sh created
daemonset.apps/install-cni-plugins created
```

Рис. 3.5 Інсталяція Multus CNI

Повторна перевірка системних pod'ів підтвердила успішне завантаження сервісів Multus у кластер, продемонстрована на рисунку 3.6.

```
Every 2.0s: kubectl -n kube-system get po

NAME                                         READY   STATUS    RESTARTS      AGE
coredns-7db6d8ff4d-pt72r                     1/1     Running   1 (10h ago)   12h
coredns-7db6d8ff4d-ztw8k                     1/1     Running   1 (10h ago)   12h
etcd-kind-control-plane                      1/1     Running   0             10h
install-cni-plugins-6pwm8                    1/1     Running   0             10h
install-cni-plugins-7lp96                    1/1     Running   0             10h
install-cni-plugins-vr4jp                    1/1     Running   0             10h
kindnet-4pnrs                                1/1     Running   2             12h
kindnet-hq2qf                                1/1     Running   2             12h
kindnet-ttkl5                                1/1     Running   2             12h
kube-apiserver-kind-control-plane            1/1     Running   0             10h
kube-controller-manager-kind-control-plane   1/1     Running   2 (10h ago)   12h
kube-multus-ds-2fbxr                         1/1     Running   2             11h
kube-multus-ds-bkwb2                         1/1     Running   1 (10h ago)   11h
kube-multus-ds-vx9fz                         1/1     Running   1 (10h ago)   11h
kube-proxy-crhvp                             1/1     Running   2 (10h ago)   12h
kube-proxy-hhv2m                             1/1     Running   2 (10h ago)   12h
kube-proxy-khpk2                             1/1     Running   2 (10h ago)   12h
kube-scheduler-kind-control-plane            1/1     Running   2 (10h ago)   12h
```

Рис. 3.6 Перевірка pod'ів сервісів Multus

Для логічного відокремлення компонентів мережевої інфраструктури створено три незалежні namespace:

- open5gs - для компонентів ядра 5G;
- loadbalancer - для балансувальника LoxiLB;
- ran-simulator - для симулятора радіомережі.

Процес створення namespace показано на Рисунку 3.7 - Створення ізольованих просторів імен.

```
chornob@mankotest3:~/5gcore-sctp-loadbalancer$ kubectl create -f core-5g-macvlan.yml
networkattachmentdefinition.k8s.cni.cncf.io/core5g-def created
networkattachmentdefinition.k8s.cni.cncf.io/core5g-def created
networkattachmentdefinition.k8s.cni.cncf.io/core5g-def created
```

Рис.3.7 Створення ізольованих просторів імен

MACVLAN забезпечує прямий доступ контейнерів до L2-мережі, що необхідно для коректного функціонування SCTP-сесій між AMF та gNB.

Розгортання компонентів 5G Core виконувалося через Helm-чарт open5gs-helm-charts. Під час ініціалізації було інстальовано ключові мережеві функції, зокрема: AMF, SMF, UPF, NRF, AUSF, PCF, UDM, UDR тощо. Процес створення namespace показано на Рисунку 3.8

```
chornob@mankotest3:~/5gcore-sctp-loadbalancer$ helm -n open5gs upgrade --install core5g open5gs-helm-charts/
Release "core5g" does not exist. Installing it now.
NAME: core5g
LAST DEPLOYED: Thu Dec 11 09:52:29 2025
NAMESPACE: open5gs
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
Status after deployment:

$(kubectl --namespace open5gs get all)
```

Рис. 3.8 Розгортання Open5GS через Helm

Після інсталяції виконано перевірку стану pod’ів у namespace *open5gs*. На ранніх етапах деякі компоненти перебувають у стані *Init*, що є типовим результатом очікування мережевих залежностей, , продемонстровано на рисунку 3.9.

```
NAME                                    READY   STATUS              RESTARTS   AGE
core5g-amf-1-deployment-64bbd8ccc4-6q75f   0/1     Init:0/1            0          82s
core5g-amf-2-deployment-8547897847-2vtlf   0/1     Init:0/1            0          84s
core5g-ausf-deployment-79df64f66-qmfj7     0/1     Init:0/1            0          84s
core5g-bsf-deployment-558ffdf654-qv4gx     0/1     Init:0/1            0          84s
core5g-mongo-ue-import-bvr98               0/1     Completed           0          84s
core5g-mongodb-5f6bc94fc8-pktxl            1/1     Running             0          84s
core5g-nrf-deployment-7d6bf587b-gj6n7      0/1     ContainerCreating   0          84s
core5g-nssf-deployment-78fd88db99-2fqtv    0/1     Init:0/1            0          84s
core5g-nssf-deployment-78fd88db99-2fqtv    0/1     Init:0/1            0          84s
core5g-pcf-deployment-55b66d9754-slks6     0/1     Init:0/2            0          84s
core5g-smf-deployment-76dcfd78bd-bsn95     0/1     Init:0/2            0          84s
core5g-udm-deployment-6b9479b65-k5f5d      0/1     Init:0/1            0          84s
core5g-udr-deployment-c7fc6c5f4-xwfl27     0/1     Init:0/2rCreating   0          84s
core5g-upf-deployment-5698b7dbd9-zdpw7     0/2     ContainerCreating   0          84s
core5g-webui-ddf48cb7f-b8f8m               0/1     Init:0/1            0          84s
```

Рис. 3.9 Стан pod’ів Open5GS під час ініціалізації

Балансувальник LoxiLB інтегрується як Kubernetes-ресурс, розгорнутий через власний Helm-чарт. Його завдання — здійснювати розподіл SCTP-з’єднань від RAN-компонентів до AMF-вузлів, забезпечуючи відмовостійкість та ефективне балансування сигналізаційного навантаження. Процес розгортання наведено на Рисунку 3.10.

```
chornob@mankotest3:~/5gcore-sctp-loadbalancer$ helm -n loadbalancer upgrade --install lb5g loxilb-helm-chart/
Release "lb5g" does not exist. Installing it now.
NAME: lb5g
LAST DEPLOYED: Thu Dec 11 10:13:49 2025
NAMESPACE: loadbalancer
STATUS: deployed
REVISION: 1
TEST SUITE: None
chornob@mankotest3:~/5gcore-sctp-loadbalancer$ kubectl -n loadbalancer get po
NAME     READY   STATUS    RESTARTS   AGE
lb5g-0   1/1     Running   0          38s
```

Рис. 3.10 Інсталяція LoxiLB

Для моделювання поведінки gNB та UE застосовувався симулятор *my5G-RANTester*. Його встановлення за допомогою Helm показано на **Рисунку 3.11.** Після завершення контейнер переходить у стан *Running*.

```
chornob@mankotest3:~/5gcore-sctp-loadbalancer$ helm -n ran-simulator upgrade --install sim5g my5GRanTester-helm-chart/
Release "sim5g" does not exist. Installing it now.
NAME: sim5g
LAST DEPLOYED: Thu Dec 11 10:17:24 2025
NAMESPACE: ran-simulator
STATUS: deployed
REVISION: 1
TEST SUITE: None
chornob@mankotest3:~/5gcore-sctp-loadbalancer$ kubectl -n ran-simulator get po
NAME                              READY   STATUS              RESTARTS   AGE
sim5g-simulator-fd8bd7876-lpc9m   0/1     ContainerCreating   0          36s
chornob@mankotest3:~/5gcore-sctp-loadbalancer$ kubectl -n ran-simulator get po
NAME                              READY   STATUS    RESTARTS   AGE
sim5g-simulator-fd8bd7876-lpc9m   1/1     Running   0          61s
```

Рис. 3.11 Розгортання симулятора радіодоступу my5G-RANTester

Для перевірки мережевої конфігурації було виконано команду *ip a* всередині pod’а симулятора, що дозволяє переконатися у правильному формуванні інтерфейсів, у тому числі *uetun0* - віртуального тунелю UE. Процес перевірки мережевої конфігурації наведено на Рисунку 3.12.

```
chornob@mankotest3:~/5gcore-sctp-loadbalancer$ kubectl -n open5gs exec -ti core5g-amf-1-deployment-64bbd8ccc4-6q75f -- bash
Defaulted container "amf" out of: amf, wait-for-nrf (init)
root@core5g-amf-1-deployment-64bbd8ccc4-6q75f:/# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0@if4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether f2:87:70:76:40:71 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.244.2.4/24 brd 10.244.2.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::f087:70ff:fe76:4071/64 scope link
       valid_lft forever preferred_lft forever
3: net1@if39: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 06:72:3e:ab:cf:e1 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.0.3.3/24 brd 10.0.3.255 scope global net1
       valid_lft forever preferred_lft forever
    inet6 fe80::472:3eff:feab:cfe1/64 scope link
       valid_lft forever preferred_lft forever
```

Рис. 3.12 Процес перевірки мережевої конфігурації

Запуск тесту реєстрації користувацького обладнання здійснювався через: *./app load-test -n 1*. У процесі тестування симулюється повний цикл NGAP/NAS взаємодії: ініціалізація радіоз'єднання, передача сигналізаційних повідомлень, автентифікація, створення безпечного контексту та завершення процедури реєстрації. Виконання процедури наведено на **Рисунку 3.13** У виводі видно формування SCTP-сесій, обмін NGAP-повідомленнями та підтвердження успішної автентифікації UE.

```
chornob@mankotest3:~/5gcore-sctp-loadbalancer$ kubectl -n ran-simulator exec -ti deploy/sim5g-simulator -- bash
root@sim5g-simulator-fd8bd7876-lpc9m:/workspace/my5G-RANTester/cmd# ./app load-test -n 1
INFO[0000] my5G-RANTester version 1.0.1
INFO[0000] ----------------------------------------
INFO[0000] [TESTER] Starting test function: Testing registration of multiple UEs
INFO[0000] [TESTER][UE] Number of UEs: 1
INFO[0000] [TESTER][GNB] gNodeB control interface IP/Port: 10.0.3.2/9487
INFO[0000] [TESTER][GNB] gNodeB data interface IP/Port: 10.0.3.2/2152
INFO[0000] [TESTER][AMF] AMF IP/Port: 20.20.20.1/38412
INFO[0000] ----------------------------------------
INFO[0000] [GNB] SCTP/NGAP service is running
INFO[0000] [GNB] UNIX/NAS service is running
encoding/hex: odd length hex string
INFO[0000] [GNB][SCTP] Receive message in 0 stream
INFO[0000] [GNB][NGAP] Receive Ng Setup Response
INFO[0000] [GNB][AMF] AMF Name: open5gs-amf1
INFO[0000] [GNB][AMF] State of AMF: Active
INFO[0000] [GNB][AMF] Capacity of AMF: 255
INFO[0000] [GNB][AMF] PLMNs Identities Supported by AMF -- mcc: 208 mnc:93
INFO[0000] [GNB][AMF] List of AMF slices Supported by AMF -- sst:01 sd:000001
INFO[0001] [TESTER] TESTING REGISTRATION USING IMSI 0000000031 UE
INFO[0001] [UE] UNIX/NAS service is running
INFO[0001] [GNB][SCTP] Receive message in 1 stream
INFO[0001] [GNB][NGAP] Receive Downlink NAS Transport
INFO[0001] [UE][NAS] Message without security header
INFO[0001] [UE][NAS] Receive Authentication Request
INFO[0001] [UE][NAS][MAC] Authenticity of the authentication request message: OK
INFO[0001] [UE][NAS][SQN] SQN of the authentication request message: VALID
INFO[0001] [UE][NAS] Send authentication response
INFO[0001] [GNB][SCTP] Receive message in 1 stream
INFO[0001] [GNB][NGAP] Receive Downlink NAS Transport
INFO[0001] [UE][NAS] Message with security header
INFO[0001] [UE][NAS] Message with integrity and with NEW 5G NAS SECURITY CONTEXT
INFO[0001] [UE][NAS] successful NAS MAC verification
INFO[0001] [UE][NAS] Receive Security Mode Command
INFO[0001] [UE][NAS] Type of ciphering algorithm is 5G-EA0
INFO[0001] [UE][NAS] Type of integrity protection algorithm is 128-5G-IA2
```

Рис. 3.12 Процес реєстрації UE через симулятор my5G-RANTester

Після встановлення сеансу з боку UE було перевірено таблиці з'єднань LoxiLB. Команда: *loxicmd get ct* демонструє, що SCTP-трафік рівномірно маршрутизовано між AMF-вузлами. Відповідний результат показано на Рисунку 3.13.

```
chornob@mankotest3:~$ kubectl -n loadbalancer exec -ti lb5g-0 -- bash
root@lb5g-0:/# loxicmd get ct
| SERVICE NAME | DESTIP | SRCIP | DPORT | SPORT | PROTO | IDENT | STATE | ACT | PACKETS | BYTES |
|--------------|--------|-------|-------|-------|-------|-------|-------|-----|---------|-------|
root@lb5g-0:/# loxicmd get ct
| SERVICE NAME |   DESTIP   |  SRCIP   | DPORT | SPORT | PROTO | IDENT | STATE |                ACT                | PACKETS | BYTES |
|--------------|------------|----------|-------|-------|-------|-------|-------|-----------------------------------|---------|-------|
|              | 10.0.3.1   | 10.0.3.3 |  9487 | 38412 | sctp  | 0:0   | est   | fsnat-20.20.20.1,10.0.3.2:38412:w0 |      22 |  1996 |
|              | 20.20.20.1 | 10.0.3.2 | 38412 |  9487 | sctp  | 0:0   | est   | fdnat-10.0.3.1,10.0.3.3:38412:w0   |      22 |  1956 |
root@lb5g-0:/#
```

Рис. 3.13 Таблиця активних SCTP-з'єднань у LoxiLB

У таблиці видно:

1. DESTIP (адреса AMF).
2. SRCIP (адреса gNB).
3. SPORT/DPORT (порти SCTP).
4. STATE (established).
5. тип NAT-операції.

Це прямо підтверджує, що балансувальник виконує коректне розподілення NGAP/SCTP-сесій між backend-вузлами.

Для додаткової перевірки коректності тунелювання користувацької площини було виконано ICMP-тести з UE-інтерфейсу uetun1. Спочатку проведено пінг внутрішньої адреси UPF (10.45.0.1), після чого - зовнішнього ресурсу 4.2.2.2. Результати наведено на Рисунку 3.14 та 3.15.

```
root@sim5g-simulator-fd8bd7876-lpc9m:/workspace/my5G-RANTester/cmd# ping -I uetun1 4.2.2.2
PING 4.2.2.2 (4.2.2.2) from 10.45.0.2 uetun1: 56(84) bytes of data.
64 bytes from 4.2.2.2: icmp_seq=1 ttl=52 time=26.7 ms
64 bytes from 4.2.2.2: icmp_seq=2 ttl=52 time=27.6 ms
64 bytes from 4.2.2.2: icmp_seq=3 ttl=52 time=29.5 ms
64 bytes from 4.2.2.2: icmp_seq=4 ttl=52 time=26.3 ms
^C
--- 4.2.2.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 26.385/27.579/29.583/1.251 ms
```

Рис.3.14 Перевірка UE-трафіку через тунель

```
root@sim5g-simulator-fd8bd7876-lpc9m:/workspace/my5G-RANTester/cmd# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0@if11: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 8e:67:54:21:32:0e brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.244.2.10/24 brd 10.244.2.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::8c67:54ff:fe21:320e/64 scope link
       valid_lft forever preferred_lft forever
3: net1@if39: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 4a:42:5e:a6:48:99 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.0.3.2/24 brd 10.0.3.255 scope global net1
       valid_lft forever preferred_lft forever
    inet6 fe80::4842:5eff:fea6:4899/64 scope link
       valid_lft forever preferred_lft forever
4: tunl0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/ipip 0.0.0.0 brd 0.0.0.0
5: uetun1@NONE: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 65515 qdisc noqueue state UNKNOWN group default
    link/ipip 127.0.0.3 peer 127.0.0.2
    inet 10.45.0.2/32 scope global uetun1
       valid_lft forever preferred_lft forever
    inet6 fe80::5efe:7f00:3/64 scope link
       valid_lft forever preferred_lft forever
root@sim5g-simulator-fd8bd7876-lpc9m:/workspace/my5G-RANTester/cmd# ip link set dev tun10 up
Cannot find device "tun10"
root@sim5g-simulator-fd8bd7876-lpc9m:/workspace/my5G-RANTester/cmd# ip link set dev tunl0 up
root@sim5g-simulator-fd8bd7876-lpc9m:/workspace/my5G-RANTester/cmd# ping -I uetun1 10.45.0.1
PING 10.45.0.1 (10.45.0.1) from 10.45.0.2 uetun1: 56(84) bytes of data.
64 bytes from 10.45.0.1: icmp_seq=1 ttl=64 time=0.515 ms
64 bytes from 10.45.0.1: icmp_seq=2 ttl=64 time=0.435 ms
64 bytes from 10.45.0.1: icmp_seq=3 ttl=64 time=0.592 ms
64 bytes from 10.45.0.1: icmp_seq=4 ttl=64 time=0.547 ms
64 bytes from 10.45.0.1: icmp_seq=5 ttl=64 time=0.598 ms
64 bytes from 10.45.0.1: icmp_seq=6 ttl=64 time=0.524 ms
^C
--- 10.45.0.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5129ms
```

Рис.3.15 Перевірка UE-трафіку через тунель

Аналіз результатів проекту. Виконаний проект демонструє, що використання SDN-підходу до балансування сигналізаційного трафіку в ядрах мобільних мереж дозволяє значно підвищити масштабованість і надійність інфраструктури. LoxiLB успішно розподіляє SCTP-потоки між AMF-екземплярами без порушення процедур реєстрації та подальшого обслуговування UE. Це свідчить про можливість інтеграції подібних рішень у системи віддаленого керування мережевими параметрами, що розглядається в рамках дипломної роботи.

Наявність стабільних UE-тунелів та успішне проходження ICMP-тестів підтверджує відсутність деградації користувацького трафіку в умовах роботи балансувальника. Водночас сам механізм контейнеризації та мультипідключення через Multus забезпечив необхідну гнучкість розгортання складних мережевих

топологій.

Загалом отримані результати демонструють практичну можливість застосування SDN-балансування SCTP для підвищення ефективності управління розподіленими компонентами 4G/5G Core, що є важливим елементом систем віддаленого моніторингу та конфігурації мереж оператора мобільного зв’язку.

ВИСНОВКИ

У магістерській роботі проведено комплексне дослідження впровадження програмно-визначених мереж (SDN) у мобільних мережах п’ятого покоління з метою забезпечення гнучкого та ефективного управління мережевим трафіком. Основну увагу приділено аналізу сучасних архітектур 5G та практичним підходам до оптимізації управління трафіком із використанням SDN у контейнеризованому середовищі.

У результаті виконання роботи проаналізовано сучасний стан розвитку мереж 5G, визначено вимоги до управління трафіком у високонавантажених мережах та обґрунтовано доцільність застосування SDN і NFV для забезпечення масштабованості, гнучкості й автоматизації. Показано, що впровадження SDN дозволяє підвищити ефективність використання мережевих ресурсів, реалізувати динамічне балансування навантаження та покращити якість обслуговування користувачів.

У першому розділі роботи здійснено аналіз еволюції мобільних систем зв’язку та сучасних технологій побудови мереж 5G. Розглянуто архітектури NSA та SA, ключові функції ядра 5G (AMF, SMF, UPF), а також механізми QoS, network slicing і технології радіодоступу. Встановлено, що складність та динамічність мереж 5G потребують використання нових підходів до управління трафіком.

У другому розділі досліджено принципи функціонування SDN і NFV у мережах 5G, проаналізовано можливості SDN-контролерів ONOS та OpenDaylight. Зроблено висновок, що поєднання SDN і NFV є ключовим чинником побудови гнучких та масштабованих мереж 5G, які підтримують централізоване управління, QoS та network slicing.

У третьому розділі розгорнуто контейнеризоване експериментальне середовище Kubernetes з використанням Multus CNI, MACVLAN та компонентів 5G Core (Open5GS). Реалізовано SDN-орієнтоване балансування трафіку SCTP на основі платформи LoxiLB. Проведений аналіз підтвердив ефективність запропонованого підходу та його придатність для використання в розподілених

архітектурах 5G Core.

Отримані результати підтверджують доцільність впровадження SDN для управління трафіком у мережах 5G та можуть бути використані під час проєктування і модернізації операторських телекомунікаційних мереж, а також у подальших наукових дослідженнях у сфері інтелектуального управління мережами.

Основні результати кваліфікаційної магістерської роботи викладено у тезах на науково-практичних конференціях, що забезпечило апробацію отриманих результатів і підтвердило їх наукову новизну та практичну значущість. У межах роботи проаналізовано сучасні підходи до інтеграції алгоритмів ШІ у системи передачі даних, визначено їх переваги та недоліки, а також розроблено рекомендації щодо підвищення ефективності та надійності таких систем. Отримані результати становлять цінну основу для подальших досліджень і можуть бути використані при створенні інтелектуальних інфокомунікаційних рішень нового покоління. "Захист інфокомунікаційних мереж за допомогою штучного інтелекту" та "Інтеграція штучного інтелекту в інформаційно комунікаційних системах та мережах", за авторством Магась С.В. та Манько А.М., що подані до друку в збірник тез до IX Всеукраїнської студентської науково-практичної конференції від Міжнародного науково-технічного університету імені академіка Юрія Бугая.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ