ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
Кафедра Мобільних та відеоінформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Методи конвергенції програмно-конфігурованих мереж та технологій п'ятого покоління»

на здобуття освітнього ступеня магістра
зі спеціальності 172 Телекомунікації та радіотехніка
освітньо-професійної програми Апаратура радіозв'язку, радіомовлення і телебачення

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



(підпис) Владислав МЕДВЕДЄВ (Ім'я, ПРІЗВИЩЕ)

Виконав: здобувач вищої освіти
групи АРДМ-61
Владислав МЕДВЕДЄВ

Керівник: Віталій СТРЕЛЬНІКОВ

Рецензент: В. Мережко

Київ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

Кафедра	Мобільних та відеоінформаційних технологій
Ступінь вищої освіти	Магістр
Спеціальність	172 Телекомунікації та радіотехніка
Освітньо-професійна програма	Апаратура радіозв'язку, радіомовлення і телебачення

ЗАТВЕРДЖУЮ
Завідувачка кафедрою МВТ
_____ Наталія РУДЕНКО
« » _____ 2023 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Медведєву Владиславу Олександровичу

1. Тема кваліфікаційної роботи: «Методи конвергенції програмно-конфігурованих мереж та технологій п'ятого покоління»,
керівник кваліфікаційної роботи Віталій СТРЕЛЬНІКОВ, PhD,
затверджені наказом Державного університету інформаційно-комунікаційних технологій від 19.10.2023 р. №145.

2. Строк подання кваліфікаційної роботи 25.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
   1. Програмно-конфігуровані мережі.
   2. Технології п'ятого покоління.
   3. Науково-технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
   1. Дослідження технічних особливостей технології 5G;
   2. Механізми LTE, гарантія якості;
   3. Гарантування якості обслуговування.

5. Перелік ілюстративного матеріалу: презентація.

6. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Підбір науково-технічної літератури	19.10.23	Викон.
2.	Основні характеристики систем наземного цифрового телевізійного мовлення	31.10.23	Викон.
3.	Розробка телерадіомовної інфраструктури каналу з урахуванням хмарних технологій	15.11.23	Викон.
4.	Вибір обладнання телерадіомовної інфраструктури каналу	29.11.23	Викон.
5.	Висновки, вступ, реферат	11.12.23	Викон.
6.	Розробка презентації	18.12.23	Викон.

Здобувач вищої освіти _____ Владислав МЕДВЕДЄВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Віталій СТРЕЛЬНІКОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 84 стор., 27 рис., 4 табл., 27 дж.

Мета роботи – дослідження конвергенції програмно-конфігурованих мереж та технологій п'ятого покоління.

Об'єкт дослідження - мережі мобільного зв'язку п'ятого покоління.

Предмет дослідження – конвергенція програмно-конфігурованих мереж та технологій п'ятого покоління.

Короткий зміст роботи: В ході дослідження були вивчені і описані основні поняття і принципи 5G мереж. Концепція мереж п'ятого покоління передбачає розгортання надщільних мереж з високошвидкісним доступом поверх вже існуючих мереж, які будуть забезпечувати загальне покриття.

В першому розділі пройшло ознайомлення з такими технологіями як 5G, SDN, архітектурою та принципами SDN. Розроблені рекомендації що до розгортання мереж 5-го покоління та особливостей забезпечення якості обслуговування.

У другому розділі проаналізовано та описано механізм LTE, також проведено ознайомлення з перевагами та недоліками LTE. Зроблено висновок про те що поточні мережі 4G не витримують вимог, висунутих новими сценаріями застосування на даний час, тому технологія 5G на разі дуже актуальна.

В третьому розділі досліджувались процедури гарантування якості обслуговування, описувався принцип динамічного контролю. Було виявлено ряд проблем та описані методи їх подолання. Одна з них це: зниження показників ефективності обслуговування, яка вирішується одним з методів:

- реконфігурацією системи;
- обмеженням потоку заявок які направляються на обслуговування відповідного ядра.

Також в цьому розділі була описана інтеграція SDN в мобільних мережах.

КЛЮЧОВІ СЛОВА: SDN, 5G, ПРОГРАМНО – КОНФІГУРОВАНІ МЕРЕЖІ, НАДІЙНІСТЬ, РЕЗЕРВУВАННЯ, ПЕРЕМАРШРУТИЗАЦІЯ, ПОКАЗНИКИ НАДІЙНОСТІ

ABSTRACT

Text part of the master's qualification work: 84 pages, 27 pictures, 4 table, 27 sources.

The purpose of the work - research on the convergence of software-configured networks and technologies of the fifth generation.

Object of research – fifth generation mobile communication networks.

Subject of research – convergence of software-configured networks and technologies of the fifth generation.

Summary of the work: In the course of the study, the main concepts and principles of 5G networks were studied and described. The concept of fifth-generation networks involves the deployment of ultra-dense networks with high-speed access on top of already existing networks that will provide general coverage.

In the first section, an introduction to such technologies as 5G, SDN, architecture and principles of SDN took place. Recommendations have been developed for the deployment of 5th generation networks and the features of ensuring the quality of service.

The second chapter analyzes and describes the mechanism of LTE, and introduces the advantages and disadvantages of LTE. It was concluded that the current 4G networks cannot withstand the requirements set by the new application scenarios at the moment, therefore the 5G technology is currently very relevant.

In the third section, the procedures for guaranteeing the quality of service were studied, and the principle of dynamic control was described. A number of problems were identified and methods of overcoming them were described. One of them is: a decrease in service efficiency indicators, which is solved by one of the methods:

- system reconfiguration;
- by limiting the flow of applications that are sent to the service of the corresponding core.

This chapter also described the integration of SDN in mobile networks.

KEYWORDS: SDN, 5G, SOFTWARE-CONFIGURED NETWORKS, RELIABILITY, REDUCTION, ROUTING, RELIABILITY INDICATORS

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Медведєв В.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)

за спеціальністю 172 Телекомунікації та радіотехніка
освітньо-професійної програми Апаратура радіозв'язку, радіомовлення і телебачення

на тему: Методи конвергенції програмно-конфігурованих мереж та технологій п'ятого покоління

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач Медведєв Владислав Олександрович показав гарну теоретичну та інженерну підготовку, уміння володіти технологіями нового покоління, вміло працювати з програмно-апаратними засобами мобільного зв'язку, довідковою і науково-технічною літературою. Працюючи над завданнями, які доручались керівником, проявив ініціативність, сумлінність та хист до інженерної роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу Медведєва Владислава Олександровича на оцінку «відмінно» та присвоїти йому кваліфікацію «Магістр з телекомунікацій та радіотехніки».

Керівник кваліфікаційної роботи _____ Віталій СТРЕЛЬНІКОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

" " _____ 2023 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Медведєв В.О.
(прізвище та ініціали)

допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувачка кафедри
Мобільних та відеоінформаційних технологій _____ Наталія РУДЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

" " _____ 2023 року

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну магістерську роботу

здобувача вищої освіти Медведєва Владислава Олександровича

на тему: «Методи конвергенції програмно-конфігурованих мереж та технологій п'ятого покоління»

Актуальність:

Тема роботи є надзвичайно актуальною в сучасному світі телекомунікацій. Враховуючи, що 5G має принести значні поліпшення в швидкості, затримці та підтримці масового об'єднання пристроїв, використання SDN в цьому контексті може допомогти реалізувати ці можливості.

Однак, існують значні виклики, пов'язані з конвергенцією SDN та 5G, які вимагають подальших досліджень. Ці виклики включають питання безпеки, масштабованості, управління мережею, гарантії якості обслуговування (QoS) та ін. Отже, вивчення цієї теми важливе для того, щоб зрозуміти, як найкраще використовувати SDN для максимізації потенціалу 5G.

Позитивні сторони:

Робота дозволяє досить повно оцінити загальну характеристику, сутність та структуру поставленої проблеми. Дається чітке визначення мети роботи, об'єкту та предмету дослідження. Сформульовано наукові проблеми і представлено використані методи дослідження.

Недоліки:

1. З роботи не зрозуміло чи досліджувались питання недоліків технології SDN;
2. Інтеграція SDN в мобільних мережах розглянута в роботі не достатньо.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: кваліфікаційна робота заслуговує оцінку «відмінно», а здобувач Медведєв Владислав Олександрович заслуговує присвоєння кваліфікації: «Магістр з телекомунікацій та радіотехніки».

Рецензент: к.т.н., доцент каф. ТЕ (науковий ступінь, вчене звання) _____ (підпис) В.М. Черевик (Ім'я, ПРІЗВИЩЕ)

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 9
ВСТУП 11
1 ДОСЛІДЖЕННЯ ТЕХНІЧНИХ ОСОБЛДИВОСТЕЙ ТЕХНОЛОГІЇ 5G 13
1.1 Ознайомлення з технологією 5G 13
1.2 Опис сервісів які надаються 40
1.3 Вимоги до якості 43
Висновки 52
2 МЕХАНІЗМИ LTE, ГАРАНТІЯ ЯКОСТІ 53
2.1 Опис механізмів контроля LTE 53
2.2 Протоколи гарантії якості в мережах доступу і на рівні ядра мережі 60
Висновки 68
3 ГАРАНТУВАННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ 69
3.1 Процедура гарантування заданої якості обслуговування 69
3.2 Інтеграція SDN в мобільних мережах 75
Висновки 80
ВИСНОВКИ 81
ПЕРЕЛІК ПОСИЛАНЬ 83
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 86

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ATM	Asynchronous Transfer Mode (Мережева високопродуктивна технологія комутації)
ANI	Application network interface (Мережевий інтерфейс програми)
5G	5th Generation (П'яте покоління)
API	Application programming interface (набір готових функцій, що надаються додатком)
BYOD	Bring Your Own Device (принеси свій власний пристрій)
CDMA	Code Division Multiple Access(технологія зв'язку, при якій канали передачі мають загальну смугу частот)
CQMF	Cloud QoS management function (Функція керування хмарним QoS)
CQCF	Cloud QoS control function (Функція керування хмарним QoS)
CPE	Customer premises equipmen (Обладнання приміщень замовника)
CPU	Central processing unit (Центральний процесор)
GSM	Groupe Special Mobile (глобальний стандарт цифрового мобільного стільникового зв'язку)
IoT	Internet of Things (концепція обчислювальної мережі фізичних предметів, оснащених вбудованими технологіями для взаємодії один з одним або з зовнішнім середовищем)
IMT	International Mobile Telecommunication system (Міжнародна система мобільних телекомунікацій)
ISA	Industry Standard Architecture (Промислова стандартна архітектура)
ISDN	Integrated Services Digital Network (Цифрова Мережа з Інтегрованими Послугами)
LTE	Long-Term Evolution (стандарт бездротової високошвидкісної передачі даних для мобільних телефонів і інших терміналів, що працюють з даними)
MCE-T	Міжнародна спілка електрозв'язку (International Telecommunication Union, ITU)

MC-LAG	Multi-chassis link aggregation group (Група агрегації каналів із шасі)
MPLS	Multiprotocol Label Switching (багатопротокольна комутація за мітками
NAPT	Network Address and Port Translation (Трансляція мережевих адрес і портів)
NACFs	Network Attachment Control Functions, (Функції керування мережевими підключеннями)
NFV	Network Functions Virtualization (це концепція мережевої архітектури, що пропонує використовувати технології віртуалізації для віртуалізації цілих класів функцій мережевих вузлів у вигляді складових елементів)
NGN	Next Generation Network (Мережа наступного покоління)
OFDM	Orthogonal frequency-division multiplexing (цифрова схема модуляції, яка використовує велику кількість близько розташованих ортогональних піднесучих)
QoS	Quality of Service (ймовірність того, що мережа зв'язку відповідає заданій угоді про трафік)
PDP	Packet Data Protocol (Протокол пакетної передачі даних)
SLA	Service Level Agreement (угода про рівень надання послуги)
SDN	Software-defined Networking (Програмно-конфігурована мережа)
SGSN	Serving GPRS Support Node (Обслуговуючий вузол підтримки GPRS)
TLV	Tag, Length, Value (Тег, довжина, вартість)
RACF	Resource Access Control Facility (Засіб контролю доступу до ресурсів)
UMTS	Universal Mobile Telecommunications System (Універсальна Мобільна Телекомунікаційна Система)
UNI	User–network interface (мережевий інтерфейс користувача)
UPE	User Plane Entity (Об'єкт площини користувача)
VNF	Functions of a virtualized network (Функції віртуалізованої мережі)
VRRP	Virtual Router Redundancy Protocol (Протокол надлишковості віртуального маршрутизатора)

ВСТУП

Актуальність теми: В умовах сучасного світу дослідження технологій та мереж бездротового зв'язку являється надзвичайно важливим завданням, оскільки використання якісного та високошвидкісного зв'язку є важливим пріоритетом більшості розвинених держав. Провідні технологічні держави світу поставили за мету впровадити 5G до 2025 року. Цій технології визначена роль локомотива розвитку телекомунікаційна також лідера технологічного розвитку і технологій цифрової трансформації. Технологія 5G стане вирішальною інновацією, яка забезпечить високошвидкісним та більш надійним мобільним зв'язком, здатну справлятися з постійно зростаючими вимогами до передачі даних як з боку бізнесу, так і рядових користувачів. 5G надасть величезні можливості для підвищення продуктивності і зростання цифрової економіки. Наявність необхідних частот є одним з основних чинників для розвитку таких мереж, поряд з готовністю мережевої архітектури та інфраструктури, бізнес-моделей і абонентських пристроїв.

Програмно-настроєні мережі відносяться до програмованих мереж, якими можна керувати за допомогою програмних додатків. Ці мережі розроблені таким чином, щоб бути гнучкими, масштабованими та адаптуватися до мінливих потреб. Існує два типи програмно-настроєних мереж: програмно-визначені мережі (SDN) і мережеві функції віртуалізації (NFV). SDN відокремлює площину керування від площини даних, що дозволяє централізовано керувати мережею та контролювати її. NFV, з іншого боку, віртуалізує мережеві функції, такі як брандмауери, маршрутизатори та балансувальники навантаження, полегшуючи керування ними та розгортання. Переваги програмно-конфігурованих мереж включають покращену гнучкість мережі, зниження витрат і підвищення безпеки мережі. Відокремлюючи площину керування від площини даних, SDN забезпечує швидшу підготовку мережі та кращу оптимізацію мережі. З іншого боку, NFV дозволяє створювати віртуальні мережі, що зменшує потребу у фізичному обладнанні та знижує витрати.

Технології 5G відносяться до наступного покоління бездротових мереж зв'язку. Ці мережі розроблено для забезпечення вищої швидкості передачі даних, меншої затримки та збільшення пропускної здатності мережі. Очікується, що технології 5G матимуть значний вплив на різні галузі, включаючи охорону здоров'я, транспорт і виробництво. Однією з ключових особливостей технологій 5G є їхня здатність підтримувати зв'язок масового машинного типу (mMTC), що дозволяє підключати велику кількість пристроїв одночасно. Ця функція особливо корисна в індустрії Інтернету речей (IoT), де пристрої повинні спілкуватися один з одним у режимі реального часу. Крім того, технології 5G мають низьку затримку, що означає мінімальну затримку між надсиланням і отриманням даних.

Мета роботи: дослідження конвергенції програмно-конфігурованих мереж та технологій п'ятого покоління.

Об'єкт дослідження: мережі мобільного зв'язку п'ятого покоління.

Предмет дослідження: конвергенція програмно-конфігурованих мереж та технологій п'ятого покоління.

1 ДОСЛІДЖЕННЯ ТЕХНІЧНИХ ОСОБЛДИВОСТЕЙ ТЕХНОЛОГІЇ 5G

1.1 Ознайомлення з технологією 5G

За основу для технології 5G було взято мережі NGN

Згідно з визначенням, наведеним в Рекомендації MCE-T Y.2001, мережа наступного покоління (NGN) - це мережа з пакетною комутацією, здатна забезпечити користувачів різноманітними вузькосмуговими і широкосмуговими послугами, включаючи послуги телефонного зв'язку. Вона заснована на широкосмуговій мережі з пакетною технологією транспортування, що забезпечує необхідну якість послуг QoS, в якій функції, пов'язані з наданням послуг, не залежать від технологій транспортування інформації. Мережа NGN дає користувачам необмежений доступ до різноманітних послуг провайдерів і підтримує узагальнену мобільність, яка дозволяє користувачам отримати доступ до послуг у будь-якому місці і в будь-який час.

Мережа наступного покоління (NGN) — це термін, який використовується для опису нового покоління телекомунікаційних мереж, розроблених для задоволення зростаючого попиту на дані та мультимедійні послуги. NGN є еволюцією традиційних мереж, які в основному були розроблені для голосового зв'язку.

У рекомендації MCE-T Y.2012 перераховані основні принципи функціональної архітектури NGN:

Підтримка багатьох технологій доступу - функціональна архітектура NGN вимагає гнучкої конфігурації, необхідної для підтримки груп технологій доступу.

NGN – це мережа на основі пакетів, яка надає такі послуги, як голос, дані та мультимедіа через Інтернет-протокол (IP). Вона призначена для заміни традиційних мереж з комутацією каналів, які в основному використовувалися для голосовий зв'язок. NGN характеризується декількома особливостями, такими як гнучкість, масштабованість та інтелект. Ці функції дозволяють NGN підтримувати широкий спектр послуг і програм, включаючи відеоконференції,

онлайн-ігри та потокові послуги. NGN зазнав кілька оновлень і вдосконалення, що призвело до появи нових технологій NGN, таких як 5G. NGN важливий, оскільки він дозволяє мережевим операторам задовольняти зростаючий попит на дані та мультимедійні послуги. Із зростанням популярності потокових послуг, онлайн-ігор і соціальних медіа традиційних мереж уже недостатньо для задоволення потреб споживачів. NGN забезпечує більш ефективний і рентабельний спосіб надання цих послуг.

Архітектура NGN розділена на кілька рівнів, кожен з яких виконує певну функцію. Рівні включають транспортний рівень, рівень керування та рівень обслуговування. Транспортний рівень відповідає за фізичну передачу даних, тоді як рівень керування керує сигналізацією та маршрутизацією даних. Сервісний рівень надає програми та служби, які працюють поверх мережі.

Переваги та проблеми розгортання NGN пропонує кілька переваг, включаючи покращену якість обслуговування, збільшення пропускної здатності мережі та зниження експлуатаційних витрат. NGN забезпечує більш ефективний спосіб надання послуг, що призводить до зниження витрат для операторів мережі. Це також дозволяє надавати нові послуги та програми, які були недоступні в традиційних мережах. Однак існує також кілька проблем, пов'язаних із розгортанням NGN. Ці проблеми включають взаємодію, безпеку та нормативні питання.

Розподілене керування - використання принципу розподіленої обробки в пакетних мережах і підтримка прозорості розташування для розподілених обчислень.

Відкрите керування - мережеві інтерфейси керування мають бути відкритими для підтримки процесів створення нових, зміни існуючих послуг та підтримки засобів забезпечення логіки послуг сторонніх постачальників.

Незалежність надання послуг - процес надання послуг має бути розділений між функціями транспортної мережі, яка працює з використанням механізму розподіленого відкритого керування. Це підтримує конкурентне

оточення під час розвитку NGN, сприяє прискоренню процесів впровадження

нових послуг.

Для реалізації цих функцій в Рекомендації ITU-T Y.2011 [1] запропоновано базову еталонну модель NGN, яка включає два рівні: рівень послуг NGN (service stratum) і рівень транспорту NGN (transport stratum), кожен з яких містить по три площини: користувача, керування та менеджменту (Рис. 1.1).

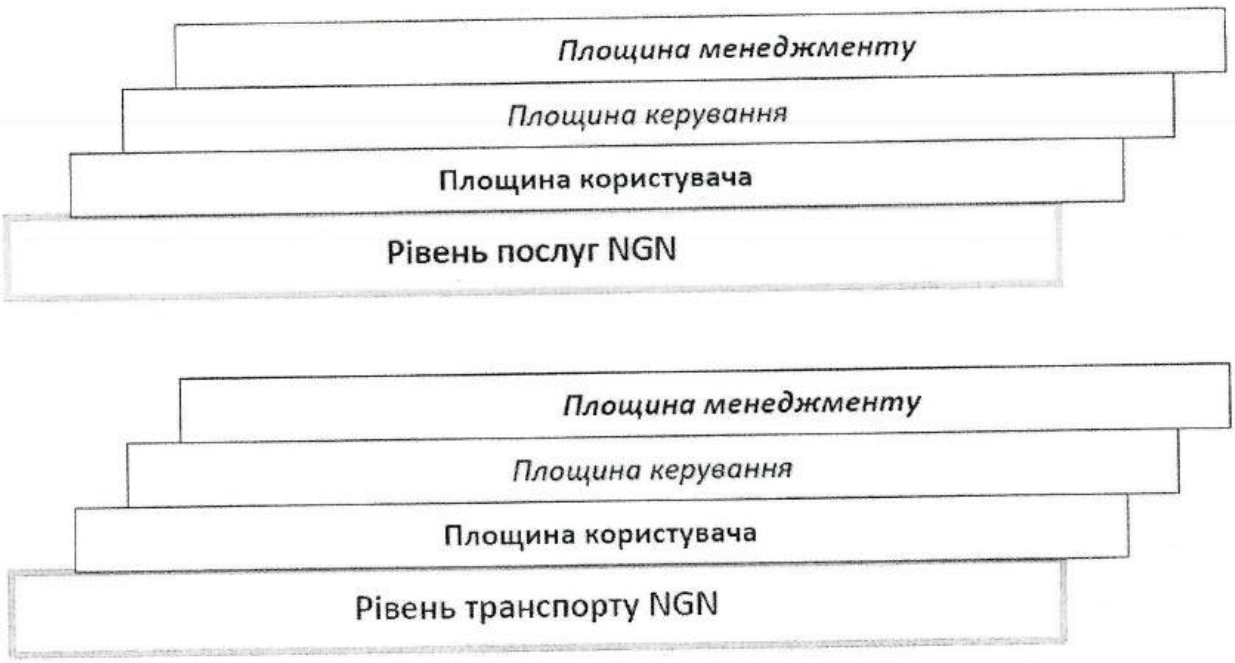


Рис. 1.1. Базова еталонна модель NGN (із рекомендації MCE-T Y.2011)

Функціональність рівнів базової еталонної моделі NGN наведено на Рис. (рекомендації ITU-T Y.2012). На кожному з рівнів використовують декілька функцій, так для надання послуг (прикладних сервісів кінцевим користувачам) застосовують функції підтримки прикладних сервісів і послуг, відповідні керуючі функції. NGN підтримує точку сполучення з функціональною групою прикладних сервісів, так званий інтерфейс прикладних сервісів мережі (application network interface-ANI), який реалізує канал взаємодії та обміну інформацією між прикладними сервісами і елементами мережі NGN. ANI забезпечує ресурси, необхідні для реалізації прикладних сервісів. Транспортний рівень забезпечує послуги IP-з'єднань для користувачів мережі NGN за допомогою функцій керування транспортом, включаючи функції керування мережевими підключеннями NACFs (Network Attachment Control Functions) і функції

керування ресурсами та доступом RACFs.

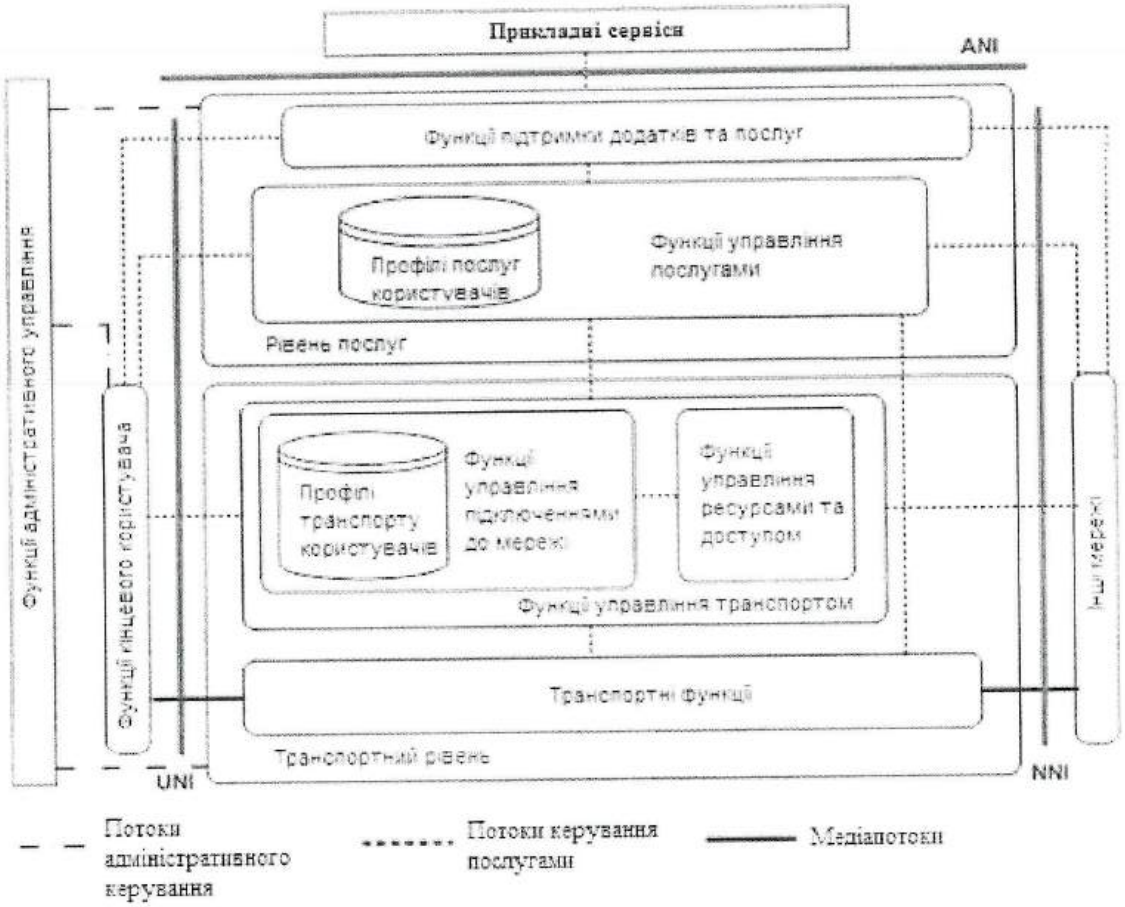


Рис. 1.2. Загальна функціональна архітектура NGN

Відповідно до Рекомендації MCE-T Y.2011 функції транспортного рівня включають безпосередньо транспортні функції і функції керування транспортом.

Транспортні функції (transport functions) забезпечують з'єднання всіх компонент і фізично розділених функцій всередині NGN. Ці функції підтримують передачу медіаінформації, а також інформації керування (сигналізації) та технічного обслуговування. Транспортні функції включають функції мережі доступу, прикордонні функції, функції транспортного ядра (магістралі) і функції шлюзів [5, 8].

Функції мережі доступу (access network functions) забезпечують підключення кінцевих користувачів до мережі, а також збір і агрегацію трафіку, що надходить з мережі доступу в транспортну магістраль (ядро). Ці функції також реалізують механізми керування якістю обслуговування QoS, пов'язані

безпосередньо з трафіком користувача, включаючи керування буферами, чергами і розкладами, пакетну фільтрацію, класифікацію трафіку, маркування трафіку, визначення політик обслуговування і формування профілю передачі трафіку.

Функції мережі доступу залежать від використовуваної технології доступу, наприклад, вони відрізняються для бездротової технології CDMA та провідної технології доступу xDSL. Залежно від технології, яка використовується для доступу до послуг NGN, мережа доступу включає функції, пов'язані з [6, 9]:

- кабельним доступом;
- доступом за технологіями xDSL;
- бездротовим доступом (наприклад, технології IEEE 802.11 (WiFi), 802.16 (WiMAX), доступ 3G RAN);
- оптичним доступом.

Прикордонні функції (edge functions) використовують для обробки трафіку, який виходить шляхом агрегування трафіку, що надходить з різних мереж доступу і передається в магістральну транспортну мережу. Вони включають функції, пов'язані з підтримкою якості обслуговування QoS і керування трафіком. Прикордонні функції використовують також між магістральними транспортними мережами.

Магістральні транспортні функції (core transport functions) відповідають за гарантовану передачу інформації через транспортну мережу з різним рівнем якості. Вони забезпечують механізми реалізації заданого рівня якості передачі QoS для користувача трафіку включаючи керування буферами, чергами і розкладом, фільтрацію пакетів, класифікацію, маркування і формування трафіку, контроль дотримання правил обслуговування, керування шлюзами і функції міжмережевих екранів.

Функції шлюзів (gateway functions) забезпечують можливості взаємодії з функціями кінцевих користувачів і/або іншими мережами, включаючи інші типи мереж NGN та ряд існуючих мереж, таких як ТфЗК/ISDN, публічний Інтернет та інші. Функції шлюзів можуть керуватися або безпосередньо функціями рівня керування або через функції керування транспортною мережею.

Функції обробки медіаінформації (media handling functions) забезпечують обробку медіаінформації при наданні послуг, таких як генерація тональних сигналів і перекодування. Ці функції реалізують спеціальними ресурсами обробки медіаінформації на транспортному рівні.

Функції керування транспортною мережею (transport control functions) включають функції керування ресурсами та доступом, функції керування приєднанням до мережі.

Функції керування ресурсами та доступом RACFs діють як арбітр між функціями керування послугами і транспортними функціями для підтримки QoS і пов'язані з керуванням транспортними ресурсами в мережі доступу і в магістральній транспортній мережі. Рішення з керування ґрунтується на інформації про необхідний транспорт, угодах про заданий рівень обслуговування SLA, правилах мережевої політики, пріоритетах послуг та інформації про стан і використання транспортних ресурсів. Функції RACF забезпечують абстрактний підхід до інфраструктури транспортної мережі для функцій керування послугами SCFs і надають сервіс-провайдерам можливість не залежати від мережевої топології, зв'язності, завантаження ресурсів, механізмів/технологій QoS та ін. Функції RACF взаємодіють з функціями SCF і транспортними функціями для різних прикладних програмних компонентів (наприклад, SIP-виклики, потокове відео й ін.), що вимагає керування транспортними ресурсами NGN, включаючи керування QoS, керування NAPT/Firewall і проходження трансляції мережевих адрес на рівні портів NAPT [10].

Функції керування підключенням до мережі NACFs забезпечують реєстрацію на рівні доступу та ініціалізацію функцій кінцевого користувача для послуг доступу NGN. Ці функції забезпечують транспортний рівень ідентифікацією/авторизацією, керуючи простором IP-адрес в мережі доступу і аутентифікації сесій доступу. Вони також повідомляють кінцевим користувачам про контактні точки до функцій NGN на рівні послуг. Функції NACF включають транспортний профіль користувача, який зберігатися у вигляді функціональної бази даних, що включає інформацію користувача, а також інші дані керування.

Рівень послуг (service stratum) включає:

– Функції керування послугами, включаючи функції профілів послуг користувачів;

– Функції підтримки прикладних програмних компонентів і функції підтримки послуг;

– Функції кінцевих користувачів;

– Функції адміністративного керування.

Функції керування послугами (service control functions) включають керування ресурсами, функції реєстрації, аутентифікації та авторизації для різних сервісів на рівні послуг. Вони також можуть включати функції керування медіаресурсами, такими як спеціалізовані пристрої та шлюзи на сигнальному рівні. Функції керування послугами підтримують профілі послуг користувачів, які є комбінацію інформації користувача та інших даних керування, індивідуальний профіль кожного користувача, такі дані зберігають у функціональних базах даних [7, 8].

Функції підтримки прикладних програмних компонентів і функції підтримки послуг (application support functions and service support functions) включають функції шлюзів, реєстрації, аутентифікації та авторизації на рівні прикладних програмних компонентів. Ці функції доступні в функціональних групах «прикладні сервіси» і «кінцеві користувачі». Вони працюють спільно з функціями керування послугами для забезпечення кінцевих користувачів і прикладних сервісів необхідними послугами NGN. Через інтерфейс

«користувач-мережа» UNI функції підтримки прикладних програмних компонентів і функції підтримки послуг забезпечують точку доступу до

функцій кінцевих користувачів. Взаємодія прикладних програмних компонентів з даними функціями здійснюється через точку доступу, реалізовану інтерфейсом «прикладна програма-мережа» ANI.

Функції кінцевих користувачів (end-user functions) не визначають ніяких обмежень на інтерфейси користувача і мережі доступу кінцевих користувачів, які можуть бути з'єднані з мережею доступу NGN. Термінальні пристрої користувачів послуг NGN є будь-якими мобільними або стаціонарними пристроями.

Функції адміністративного керування (management functions) забезпечують можливість керувати мережею NGN для надання послуг із заданим рівнем якості, безпеки та надійності. Ці функції розподіляються децентралізовано по всім функціональним блокам (FE) і вони взаємодіють з функціональними блоками керування мережевими елементами, керування мережею і керування послугами. Функції адміністративного керування використовують на транспортному рівні і рівні послуг і для кожного з рівнів вони реалізують такі завдання:

- Керування процесом усунення відмов (Fault Management);
- Керування конфігурацією мережі (Configuration Management);
- Керування розрахунками з користувачами і постачальниками послуг (Accounting Management);
- Контроль продуктивності мережі (Performance Management);
- Забезпечення безпеки роботи мережі (Security Management).

З метою більш простого розуміння принципів побудови мереж наступного покоління в більшості публікацій з NGN наводиться узагальнена 4-х рівнева архітектура NGN, в якій виділяються такі рівні (Рис. 1.3):



Рис. 1.3. Чотирьохшарова модель NGN

– рівень доступу, який містить мережу абонентського доступу до транспортної пакетної мережі;

– транспортний рівень, який включає магістральну пакетну мережу (мережу, побудовану на базі протоколів пакетної комутації IP або ATM, на сьогоднішній день найчастіше на базі технології MPLS та протоколу IP);

– рівень керування комутацією, включає сукупність функцій з керування усіма процесами обслуговування викликами в телекомунікаційній мережі;

– рівень послуг та експлуатаційного керування, який містить логіку виконання послуг та/або прикладних програмних компонентів, керує цими послугами, має відкриті інтерфейси для використання сторонніми організаціями (для розробки нових сервісів).

Термінальне обладнання рівня доступу не входить до складу мережі NGN. Безпосереднє підключення до мережі можливо тільки для пакетних абонентських терміналів, які працюють з використанням протоколів SIP та H.323.

Концепція NGN спричинила еволюцію систем керування в телекомунікаціях від спеціальних апаратних рішень до програмно-керованих мереж (SDN), які здійснюють контроль та керування відповідним обладнанням гетерогенних інформаційно-телекомунікаційних систем.

1.1.1 SDN

Система мережевої інфраструктури, що використовується в даний час, підтримується майже в тому ж вигляді протягом десятиліть, в той час як технології продовжують розвиватися. Управління ресурсами має найважливіше значення в мережевих сценаріях, давнє і досі відкрите питання. Більше того, у цьому сценарії головне питання для вирішення яким є роз'єднання логіки управління мережею від площини даних мережі, тобто фізичні маршрутизатори та комутатори, які передають трафік від джерела до пунктів призначення. Оскільки існує багато мережевих парадигм які намагаються знайти ефективну альтернативу класичній архітектурі Інтернету, лише деякі з них широко поширені та успішні. У

цьому конкурсі парадигма програмно-визначених мереж (SDN) є однією з найкращих і найбільш привабливими рішеннями для вдосконалення Інтернету з більшою гнучкістю та проблеми адаптивності. Ця нова мережева парадигма дозволяє централізуватись програмно для управління поведінкою всієї мережі шляхом відокремлення площини рішення маршрутизації від рівня переадресації. Парадигмі SDN потрібен механізм для здійснення зв'язку між керуванням і даними можливої площини. Ця функціональність отримується за допомогою нового протоколу OpenFlow. SDN спільно з OpenFlow дозволяє нам писати програми управління високого рівня, які задають поведінку мережевих компонентів. Ці програми можуть піклуватися про різні мережеві завдання, наприклад, безпеку, маршрутизацію та управління ресурсами. Ці завдання є одними з найважливіших аспектів у всіх мережевих сценаріях, оскільки основні Інтернет-сервіси, як правило, все ще базуються на класичній парадигмі BestEffort.

З одного боку, послуга Best-Effort проста, простота була найважливішим фактором, який визначив її світовий успіх. З іншого боку, на жаль, сервіс Best-Effort не може забезпечити будь-яку гарантію пропускної здатності, затримки в кінці та втрати пакету. Крім того, нині попит на якість, пов'язаний з транспортуванням даних ЗМІ зростає, як в наукових колах, так і в промисловості. Ця потреба являє собою дуже важкий виклик, і це вимагає значних зусиль для забезпечення якості, що підтримується QoS мережею [11-13].

Традиційно QoS визначається з точки зору доступності, тобто у відсотках часу, в який система відліку працює. Таким чином угоди про рівень обслуговування (SLAs) були визначені як функція відсотка доступності, наприклад, 99,999%, відомий як "п'ять дев'яток", що передбачає час простою 5,26 хвилин на рік. Простій - це час, необхідний для ідентифікації та усунення несправності у з'єднанні чи на обладнанні. Крім того, це дуже важливо розуміти, що кожен тип послуг має різні вимоги SLA, а не лише на основі доступності. Отже, вдосконалена угода про домовленість повинна прийняти / враховувати затримку пакету та параметри втрати пакету на додаток до доступністі. Звідси випливає, що якість деяких типів додатків залежить від затримки та / або втрати

пакету (наприклад, програми в режимі реального часу або мультимедійні передачі). З одного боку, послуги телефонії (наприклад, VoIP) мають сувору затримку вимоги до пакету та кодеку. У цих програмах, якщо пакет досягає призначення після заданого порогу затримки послуга стає марною. Для додатків в режимі реального часу також непридатні для повторної передачі втрачених пакетів. З іншого боку, у нас є інші типи застосувань, які називаються еластичними.

Гарантувати вимоги щодо якості в традиційному режимі Best-Effort непросто. З цього приводу працює спеціальна група Internet Engineering (IETF) За останні десятиліття запропоновано різні архітектури QoS, такі як IntServ та DiffServ. Однак ці пропозиції не були дуже успішними або реалізовані в широкому масштабі, оскільки вони вимагають певних кардинальних змін з веб-дизайну. У сучасній архітектурі Інтернету також існує суворий характер, брак інформації про доступні мережеві ресурси від кінця до кінця точки зору. Часткове рішення надійшло від методів мультипротокольної мітки (MPLS) та методу протоколу кордону шлюзу (BGP) [15], які є визначені для вирішення цих проблем. На жаль, цим рішенням не вистачає конфігурації та адаптивності в режимі реального часу. У цьому сценарії парадигма SDN може бути фундаментальним ключем для подолання існуючих пояснень обмежень найкращих зусиль вище.

Ця теза використовує поняття OpenFlow у SDN для управління диференціацією мережеві послуги з високим QoS. Зокрема, ми розглядаємо відеопотоки сервіс та послуга передачі даних. По-перше, ми визначаємо QoS Management і Оркестраційна архітектура, яка дозволяє нам керувати мережею в модульній формі шлях. По-друге, ми забезпечуємо чітку інтеграцію між архітектурою та стандартна парадигма SDN після розділення між контролем і площини даних. Потім ми надаємо формулу лінійного програмування (ІЛП) цілої лінійки проблема гарантування хорошого QoS з точки зору втрати та затримки пакетів, прийнято враховувати обмеження мережі, тобто максимально прийнятний пакет втрати та затримки для кожного типу послуги та наявної пропускної здатності на посиланнях. Зокрема, наша модель визначає найменший

товарний потік проблеми "Path" (MCFCSP) і використовує обидві відомі проблеми, отримані в результаті дослідження операцій: проблема багатотоварного потоку (MFP) та обмежений найкоротший шлях (CSP). З огляду на оптимальне рішення проблеми, ми інтегруємо результати за допомогою емульованої мережі за допомогою мінінет. Таким чином, можна відобразити різні мережеві потоки в реальній мережі, на основі оптимального рішення з моделі. Більше того, ми визначаємо різні рівні QoS, відповідно до системи MOS для служб, які ми розглядаємо. Нарешті, ми знайшли зв'язок між оптимальним рішенням забезпечення моделлю та рівнями MOS. Ми використали ці результати для надання свідчень про ефективність нашої моделі порівняно з традиційним рішенням, яке дає емулятор.

Тоді, змінюючи мережеві умови, легко знайти нові оптимальні маршрути між джерелом та пунктом призначення за допомогою модель.

Можливо також динамічне відображення маршрутів у мережі та, найголовніше - гарантувати необхідність забезпечення якості. Ця робота є першим кроком на шляху розгортання нашої пропозиції у Університеті Каліфорнії, Лос-Анджелес (UCLA), мережа містечка з диференційованими послугами та суворими вимогами щодо якості.

Масштабованість

Традиційні локальні мережі не дуже масштабуються, підтримуючи рух схід-захід оскільки щонайменше один пристрій рівня 3 і, швидше за все, декілька пристроїв 3 рівня, знаходяться на шляху від кінця до кінця. SDN дозволяє IT-організаціям перейти до масштабної моделі мереж, за допомогою якої вони додають мережеву функціональність при необхідності, а контролер SDN дозволяє їм керувати всіма функціональними можливостями мережі, як якщо б це був один пристрій. Ключовим фактором щодо масштабованості SDN є кількість комутаторів, які може підтримувати контролер SDC. У сучасних умовах IT-організації повинні сподіватися, що придбані ними контролери можуть підтримувати як мінімум 100 комутаторів, але вони також повинні розуміти, що кількість комутаторів, які може підтримувати контролер, буде залежати від

випадків використання SDN, які підтримуються.

IT-організації, які оцінюють SDN, повинні усвідомлювати той факт, що мережеві трансляції накладних витрат обмежать масштабованість рішень, які вони реалізують. Як результат, оцінюючи SDN-контролери, IT-організаціям слід переконатися, що контролер може пом'якшити вплив накладних передач мережі. Іншим фактором, що обмежує масштабованість SDN, є поширення записів таблиці потоків, яке відбувається, оскільки без певної форми оптимізації необхідний запис ход-за-ходом для кожного потоку. Як результат, оцінюючи SDN-контролери, IT-організаціям також необхідно переконатися, що контролер може мінімізувати розповсюдження записів таблиці потоків. Один із способів цього можна досягти, якщо контролер SDN використовує перезаписи заголовка в ядрі мережі. Якщо ця методика реалізована, єдиний унікальний запис таблиці даних знаходиться при вході та виході в мережу.

Інший аспект масштабованості - це здатність контролера SDN створювати SDN, який може охоплювати кілька сайтів. Ця можливість дозволяє переміщувати ВМ та віртуальне сховище між сайтами. Для отримання максимальної користі від цієї можливості контролер SDN повинен дозволяти мережевій політиці маршрутизації та переадресації автоматично застосовуватись до перенесених серверів та / або сховищ.

Продуктивність

Як було описано раніше, однією з ключових функцій контролера SDN є: встановлення потоків.

Таким чином, два ключові показники ефективності, пов'язані з контролер SDN - це час настройки потоку та кількість потоків в секунду що контролер може налаштувати. Ці показники продуктивності сильно впливають на розгортання додаткових контролерів SDN. Наприклад, якщо комутатори у виробничому SDN ініціюють більше потоків, ніж це може бути підтримано існуючими контролерами SDN, потрібно додати більше контролерів.

Потоки можна налаштувати одним із двох способів: проактивно або реактивно. Настроювання активного потоку відбувається до того, як пакет надійде

до комутатора OpenFlow, і тому коли перший пакет надходить на перемикач OpenFlow, комутатор вже знає, що робити з пакетом. Це призводить до незначної затримки настройки та відсутності реального обмеження кількості потоків в секунду, яке може підтримувати контролер. В ідеалі контролер SDN попередньо заповнює таблиці потоків максимально можливим ступенем.

Навпаки, налаштування реактивного потоку відбувається, коли перемикач OpenFlow отримує пакет, який не відповідає записам таблиці даних, і, отже, комутатор повинен відправити пакет на контролер для обробки. Після того як контролер вирішує, як обробляти потік, що інформація кешується за допомогою перемикача OpenFlow контролер SDN визначає, як довго зберігати кеш-пам'ять живою. Час, пов'язаний з налаштуванням реактивного потоку, - це сума часу, необхідного для передачі пакета від перемикача OpenFlow до контролера SDN; час обробки в контролері SDN та час, необхідний для відправлення повідомлення про зміну потоку назад до перемикача OpenFlow та заповнення таблиці потоків на комутаторі. Основні фактори, що впливають на час настройки потоку, включають потужність обробки перемикачів, які приєднані до контролера, обробку та продуктивність контролера вводу / виводу. На обробку та продуктивності контролера впливає ряд факторів. Наприклад, контролер, програмне забезпечення якого написано на C, буде швидше, ніж той, чиє програмне забезпечення написано на Java. У сучасних умовах IT-організації повинні очікувати, що контролери SDN не повинні бути вузьким місцем у створенні / видаленні записів потоку, керованих комутатором.

Мережа

У традиційному IT-середовищі конфігурація мережі здійснюється на основі пристрою. Такий підхід трудомісткий і схильний до помилок, і це призводить до невідповідностей. Цей підхід також є статичним, як і конфігурації не змінюються, оскільки змінюються умови мережі. Статичний характер традиційний підхід до програмованості мережі призводить до зниження потенційної продуктивності мережі. Як зазначалося, однією з ключових характеристик SDN є те, що в контролер є програмні інтерфейси. Одним із прикладів типу програмованості,

який слід шукати IT-організаціям у контролері SDN, є можливість перенаправлення трафіку. Наприклад, з міркувань безпеки IT-організація може вибрати, щоб трафік, який входить до сервера, проходив через брандмауер. Однак, щоб не споживати ресурси брандмауера з чистим трафіком, IT-організація може захотіти вибрати перенаправлення трафіку, який виходить з сервера, щоб не проходити через брандмауер. Це складно здійснити в традиційних мережевих умовах.

Інший приклад типу програмованості, який IT-організації повинні шукати в контролері SDN, - це можливість застосувати складних фільтрів до пакетів. Ці фільтри можна вважати динамічними, інтелектуальними ACL. Прості ACL можуть базуватися на прямій відповідності заголовків пакетів і можуть бути використані для визначення, чи потрібно скидати або передавати пакети. На відміну від цього, контролер SDN повинен мати можливість застосовувати фільтри, що складаються із складних комбінацій декількох полів заголовків пакетів. Фільтри повинні мати можливість динамічно розгортатися у віртуальних мережах, і роль контролера SDN полягає в тому, щоб відсунути пов'язані записи таблиці потоків до комутаторів. Контролер SDN також може підтримувати програмованість, надаючи шаблони, що дозволяють створювати CLI-коди, що проглядаються, які, на відміну від традиційного управління конфігурацією, дозволяють динамічно програмувати мережу.

Інший спосіб, за допомогою якого контролер SDN дозволяє програмуватись, - це реалізувати API на північному рівні, як показано на малюнку 1. Інформація про управління, яка є централізованою в контролері, доступна для потенційно необмеженого набору програм SDN, які здатні динамічно змінюватися базова мережа для виконання таких завдань, як переадресація пакетів по найменш дорогому шляху або зміна параметрів QoS на основі наявної пропускної здатності або інших факторів. Ці програми SDN включають традиційні мережеві послуги, такі як брандмауер та балансири навантаження, а також системи оркестрації, такі як OpenStack. Ці додатки можуть також включати інженерію трафіку або програми, які збирають дані, які використовуються для виконання завдань, таких

як управління мережею або включення чутливих до зворотного зв'язку використання.

Частина цінності, яку надає контролер SDN, - це інтелект в контролер виконує перевірку дизайну в рамках налаштування мережі і що перевірка дизайну усуває помилки вручну і, отже, збільшує мережу організації, які оцінюють контролери SDN, повинні розуміти функціональність, яку

пропонує контролер, що підвищує надійність мережі. Один з методів, який контролер SDN може використовувати для підвищення надійності мережі, вже обговорювався. Ця техніка - це можливість виявити декілька шляхів від початку походження до місця призначення. Якщо контролер SDN потім встановлює декілька шляхів між початком і пунктом призначення, на наявність рішення не впливає відключення єдиного зв'язку. Альтернативно, якщо контролер SDN встановлює лише один шлях від початку походження до місця призначення, коли стикається з відмовою посилання, контролер повинен мати можливість швидко перенаправляти трафік на активну лінію. Це вимагає, щоб контролер постійно моніторив топологію мережі.

Що стосується наявності зовнішніх з'єднань, важливо, щоб контролер підтримував технологію та альтернативи дизайну, такі як протокол надмірності віртуальної маршрутизатора (VRRP) та група агрегації з декількома шасі (MC-LAG), які призначені для підвищення надійності мережі.

Що стосується наявності самого контролера, важливо, щоб контролер був побудований з використанням як апаратних, так і програмних функцій надмірності. Також важливо, щоб контролер SDN включав кластеризацію. Наприклад, кластеризація двох контролерів SDN в режимі активного / гарячого режиму очікування підвищує надійність і кластеризацію трьох або більше контролерів SDN, при цьому один знаходиться в гарячому режимі очікування, збільшує доступність, масштабованість та продуктивність контролера SDN. Однак для того, щоб кластеризація забезпечила дуже швидкий час відмови, важливо, щоб рішення було здатне підтримувати синхронізацію пам'яті між активними та резервними контролерами.

Щоб забезпечити безпеку в мережі, контролер SDN повинен мати можливість підтримувати автентифікацію корпоративного класу та авторизацію адміністраторів мережі. Крім того, адміністратори мережі повинні мати можливість блокувати доступ до трафіку управління SDN,
дотримуючись того ж типу процедур, які вони використовують для блокування інших ключових форм трафіку, таких як трафік управління.

Деякі додаткові функції, пов'язані з безпекою, які повинен надавати контролер SDN, вже обговорювалися. Одним із прикладів такої функціональності є можливість застосувати складні фільтри до пакетів, що можна альтернативно називати здатністю реалізовувати динамічні, інтелектуальні ACL. Іншим прикладом такої функціональності є здатність контролера забезпечити, щоб кожен орендар, який обмінюється інфраструктурою, мав повну ізоляцію від усіх інших орендарів. Крім того, оскільки контролер SDN є кандидатом на зловмисну атаку, контролерам SDN потрібна можливість як обмежувати швидкість комунікацій управління, так і бути в змозі попередити мережевих адміністраторів, коли в мережі спостерігається підозра на атаку.

1.1.2 SDN Архітектура

Програмно-визначена мережева архітектура SDN — це нова парадигма для проектування мережі, яка обіцяє покращити гнучкість мережі, її масштабованість і безпеку.

Архітектура SDN — це підхід до проектування мережі, який відокремлює площину керування від площини даних, щоб забезпечити централізоване уявлення про мережу. У традиційній мережевій архітектурі мережеві пристрої, такі як комутатори та маршрутизатори, виконують функції рівня керування та даних. Навпаки, архітектура SDN відокремлює площину керування, яка керує потоком мережевого трафіку, від площини даних, яка пересилає пакети даних. Площина керування централізована, і мережеві адміністратори можуть запрограмувати її для керування потоком мережевого трафіку на основі політик і правил. Ключові поняття, компоненти та принципи архітектури SDN

включають централізований контролер, програмовані мережеві пристрої та відкритий API для мережевого програмування. Централізований контролер забезпечує єдину точку керування мережею, а програмовані мережеві пристрої дозволяють адміністраторам мережі налаштовувати та керувати потоком мережевого трафіку. Відкритий API дозволяє адміністраторам мережі програмувати мережу за допомогою стандартних мов програмування, таких як Python і Java.

Однією з значних переваг архітектури SDN є її гнучкість в управлінні та налаштуванні мережі. Мережні адміністратори можуть запрограмувати мережу реагувати на зміну умов мережі та шаблонів трафіку. Ця гнучкість дозволяє мережевим адміністраторам швидко й ефективно розгортати нові програми та служби. Ще однією перевагою архітектури SDN є її підвищена масштабованість і економічна ефективність. Архітектура SDN дозволяє мережевим адміністраторам легко додавати або видаляти мережеві пристрої, що зменшує витрати на розширення та обслуговування мережі. Крім того, архітектура SDN скорочує час простою мережі, дозволяючи мережевим адміністраторам вносити зміни в мережу, не перериваючи мережевий трафік. Архітектура SDN також покращує безпеку та продуктивність мережі. Централізований контролер забезпечує єдину точку контролю безпеки мережі, дозволяючи адміністраторам більш ефективно контролювати та керувати потоком мережевого трафіку. Крім того, архітектура SDN дозволяє мережевим адміністраторам програмувати мережу для визначення пріоритетів критичних програм і послуг, що покращує продуктивність мережі.

Незважаючи на свої переваги, архітектура SDN також має деякі проблеми та обмеження. Однією з найбільш важливих проблем є інтеграція із застарілими системами та протоколами. Багато організацій досі використовують застарілі системи та протоколи, несумісні з архітектурою SDN. Ця несумісність ускладнює реалізацію архітектури SDN у цих організаціях. Ще одним викликом є питання стандартизації та сумісності. Архітектура SDN все ще є відносно новою технологією, і немає стандартизації з точки зору інтерфейсів програмування,

протоколів і моделей даних. Ця відсутність стандартизації ускладнює інтеграцію архітектури SDN з іншими мережевими технологіями. Архітектура SDN представляє складність у мережевому програмуванні та управлінні. Адміністратори мережі повинні мати навички програмування, щоб ефективно програмувати мережу. Крім того, архітектура SDN вимагає значних інвестицій у навчання та освіту, щоб гарантувати, що адміністратори мережі мають необхідні навички для ефективного керування мережею.

Архітектура SDN може бути представлена трьома різними логічними шарами, як показано на Рис. 1.4.

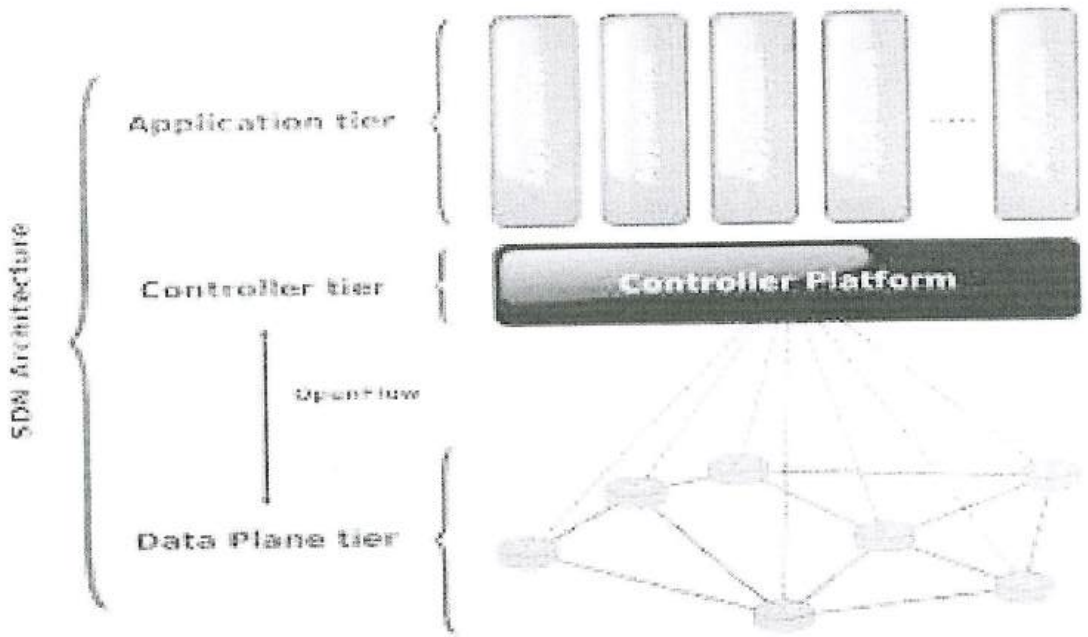


Рис.1.4. Архітектура SDN

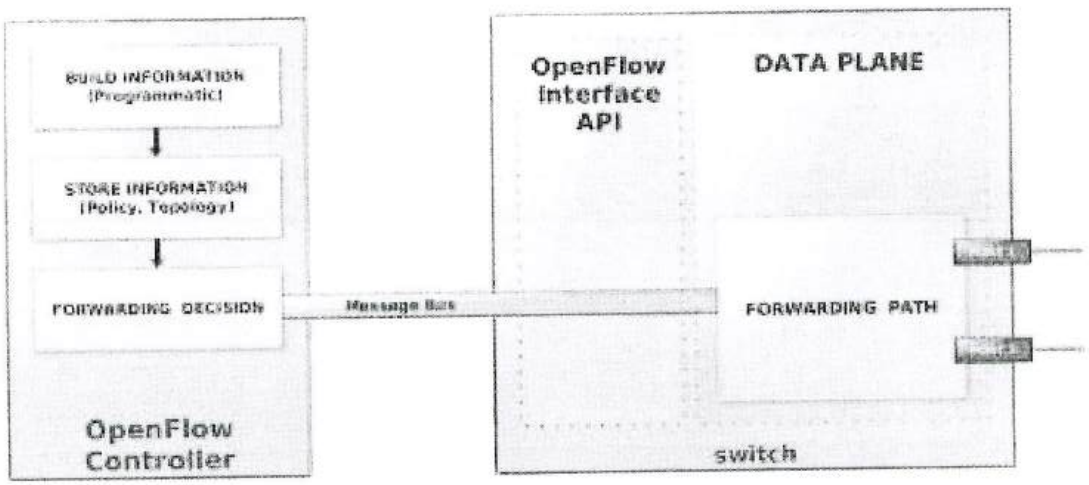
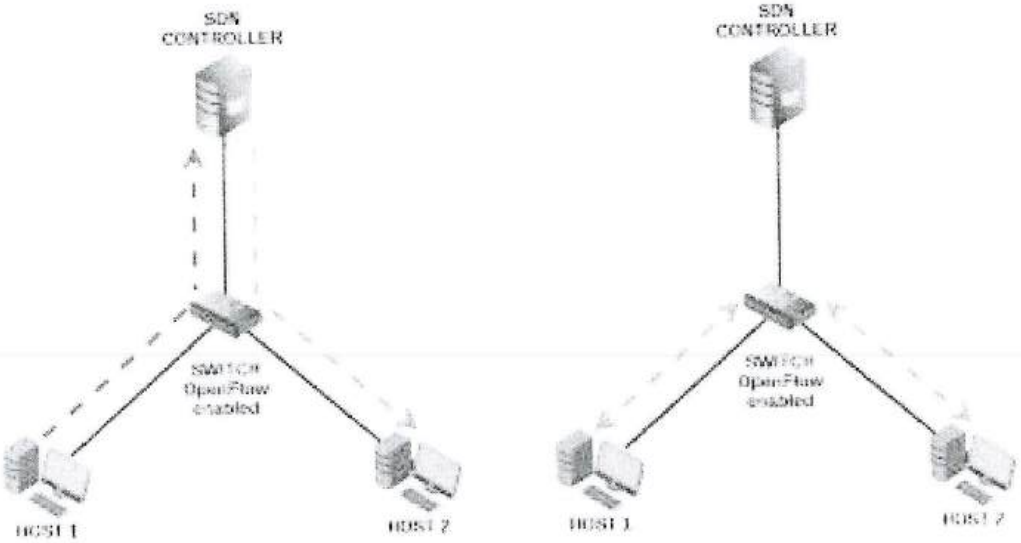


Рис. 1.5. Компоненти комутаторів SDN

SDN, відокремлюючи площину управління від площини даних, може запропонувати гнучку рамку автоматизації та управління мережею. Ця рамка робить розробку інструментів для автоматизації завдань (які виконуються вручну сьогодні) можливою. Ці засоби автоматизації можуть зменшити експлуатаційні накладні витрати нестабільність мережі, введена помилкою оператора. На жаль, програмні середовища постачальників, як правило, є власними та закритими, а їх відсутність полегшує управління та налаштування мережі. Однак SDN архітектура може полегшити інновації та забезпечити простий програмний контроль мережевого тракту даних, що породжує ідею програмованих мереж. Це важливий аспект, який дозволяє знизити бар'єр до входу для нові ідеї.

1.1.3 Принцип роботи

Коли OpenFlow Switch отримує пакет, якого він ніколи не бачив і для якого він не відповідає записів потоку, він надсилає цей пакет, який називається пакетним входом до контролера. Потім контролер приймає рішення про те, як обробляти цей пакет. Це може опустити пакет або додати запис потоку, що прямує до комутатора. У разі течії введення запису, перемикач дізнається, як передавати подібні пакети в майбутньому, як показано на Рис. 1.6. Хоча додаткові деталі цих взаємодій далі описані нижче, на даний момент цікавим є з'ясування паралелізму між описаними кроками вище та взаємодія з кешем центрального процесора (CPU). Зокрема, коли виникає помилка кешу, дії, які зазвичай здійснює процесор, порівнянні з взаємодіями протоколу OpenFlow у разі невідповідності потоку записи. Насправді, коли ЦП потребує конкретних даних, першим кроком є пошук його в кеш (починаючи з найближчого, наприклад, кеша шару L1), як фаза пошуку в комутаторі. Якщо дані є в кеш-пам'яті, виникає звернення кешу і процесор може продовжувати наступну інструкцію. В іншому випадку процесор має для кешування пропустіть отримання даних десь в іншому місці.



(a) Former the switch sends the first unknown coming packet up to the controller.

(b) Later the next packets are forwarded directly to the host by the switch.

Рис. 1.6. Обробка пакетів за допомогою перемикачів, включених OpenFlow

Цей підхід схожий на кроки, зроблені в комутаторі, якщо не відповідає рівномірний потік записів. Подальше цікаве порівняння можна зробити між протоколом OpenFlow та функціональними можливостями (тобто, Інструкційним набором) ЦП.

Набір інструкцій

Функції, пропоновані протоколом OpenFlow, можуть бути прирівняні до Архітектура набору інструкцій (ISA) процесора, як показано на Рис. 1.7.Починаючи з набір інструкцій дозволяє отримати доступ до внутрішньої архітектури процесора (пам'яті, протокол OpenFlow надає зовнішньому програмному застосуванню примітиви, які можуть бути використані для програмування площини переадресації мережеві пристрої. Основні дії, які може здійснити протокол, засновані на потоках даних встановлення всередині вимикачів, як пояснено нижче.

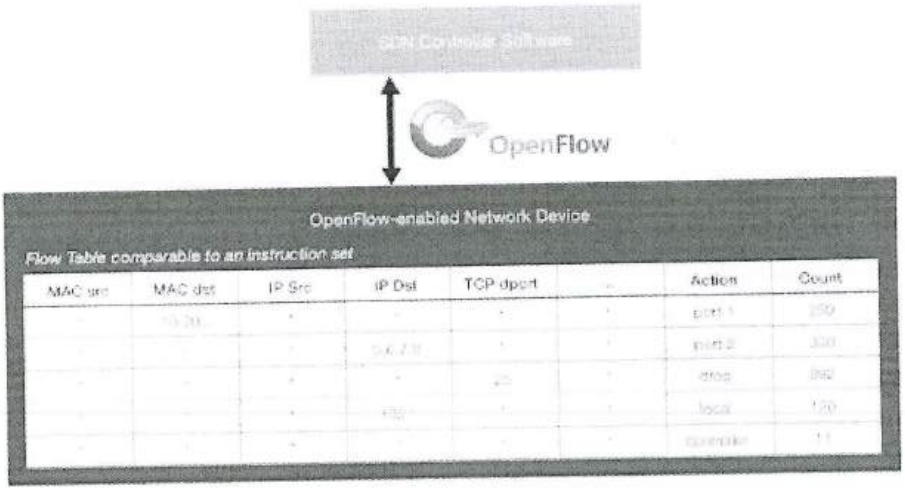


Рис. 1.7. Набір інструкцій OpenFlow

Операція на основі потоків

Протокол OpenFlow широко використовує концепцію «потоків» для ідентифікації мережевого трафіку на основі заздалегідь визначених правил узгодження, які можуть статично або динамічно запрограмовані програмним забезпеченням SDN управління. OpenFlow не тільки дозволяє мережеве програмування на основі потоку, але й забезпечує детальний контроль над потоками даних, що дозволяє мережі динамічно адаптувати ресурси за потребою. Однак це управління потоком, як правило, неможливо поточні схеми маршрутизації на основі IP. Насправді в цьому випадку все протікає між дві кінцеві точки повинні йти тим самим шляхом через мережу, незалежно відрізні їх вимоги. Перш ніж глибоко ознайомитися з останніми специфікаціями OpenFlow, подивившись на підсумок еволюції протоколу може дати нам уявлення про вдосконалення.

Підсумок еволюції

Перший випуск протоколу OpenFlow, версія 1.0, був задуманий 2009 р. Тоді, пройшовши еволюцію проміжного протоколу, OpenFlow дійшов до останньої та стабільної версії 1.4, узагальненої у Рис. 1.8.

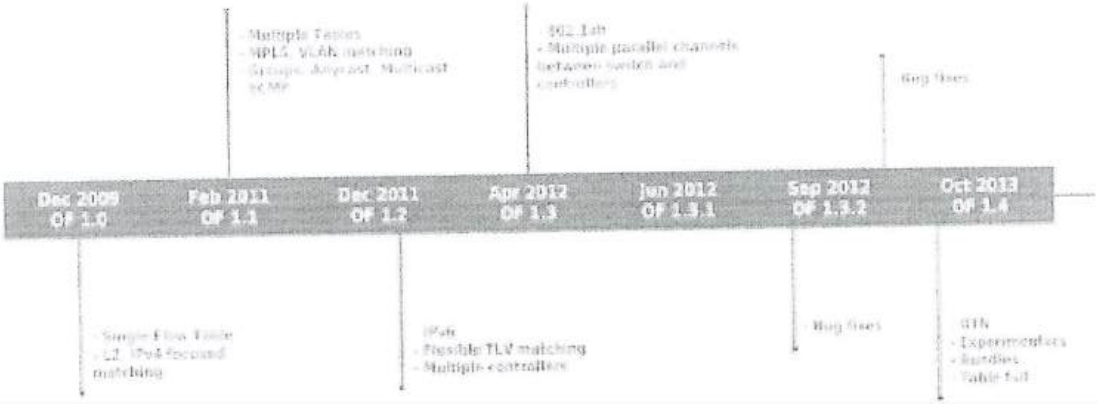


Рис. 1.8. Підсумок розвитку OpenFlow

Зокрема, основні функції першої версії OpenFlow 1.0:

1. Єдина логічна таблиця для виконання правил потоку. Більше того, цей аспект обмежує повне використання апаратних можливостей ASIC.

2. Групи для створення групових портів, аналогічні агрегації зв'язків у застарілі мережі. Це підходить для багатопоточності або надмірності.

3. Віртуальна локальна мережа (VLAN), яка підходить для грубої підтримки тегів.

4. Віртуальні порти, що розширюють OpenFlow за межами фізичних портів OpenFlow використовуватиметься для впровадження віртуалізації мережі для багатосторонніх масштабів.

5. Управління перериванням з'єднання, корисне у випадку з'єднання втрати.

Як правило, коли підключення контролера виходить з ладу або припиняється, і не вдається підключитися до резервного контролера, перемикач переходить у «аварійний стан режим "та негайно скидає поточне з'єднання TCP. У такому стані процес узгодження диктується записами таблиці аварійних потоків (позначені бітом аварійних ситуацій), тоді як будь- які інші записи видаляються. Перемикач продовжує працювати в режимі OpenFlow, поки не відновиться до контролера. Однак в останній специфікації

OpenFlow 1.4.0 було вбудовано кілька нових функцій [14]. Найважливіші

удосконалення протоколу:

1. Удосконалення формату типу довжини-значення (TLV) для підвищення розширюваності протоколу. Структура TLV підходить для підтримки додаткових майбутніх експериментів.

2. Підтримка мультиконтролера робить можливою примусову взаємодію та синхронізацію між контролерами. Зокрема, моніторинг потоку дозволяє контролеру ідентифікувати в комутаторі зміни, внесені іншими контролерами. Крім того, коли оновлюється таблиця групової таблиці або лічильник таблиці, контролери, пов'язані з цим пристроєм, отримують сповіщення.

3. Атомне виконання пучка інструкцій, щоб уникнути проміжних держав. Зокрема, контролер не повинен отримувати будь-яке повідомлення, що виникає внаслідок часткового застосування пакету (збій не вдається).

4. Дрібнозерниста здатність правила допомагати контролеру керувати обмеженням можливостей для зберігання правил. Зокрема, у випадку, якщо таблиця повна, комутатори можуть проактивно вимикати правила відповідно до важливості записів. Якщо таблиці правил заповнюються, можуть бути і деякі "події вакансії" використовуються як система раннього виявлення для попередження контролера.

5. Підтримка оптичного порту дозволяє нам працювати з волоконно-оптичними мережами, керуючи частотою та потужністю, що беруть участь в оптичному зв'язку.

Наступний розділ поглиблює основні характеристики протоколу відповідно до специфікації OpenFlow 1.4.0.

Перемикання компонентів

Перемикач OpenFlow є основоположною частиною SDN. Кожен комутатор, який представлений як базове обладнання для переадресації, доступне через відкритий інтерфейс, має два різновиди:

1. "чисті" перемикачі OpenFlow не мають застарілих функцій або бортового управління, і повністю покладаються на контролер для переадресації рішень.

2. "Гібридні" комутатори підтримують OpenFlow на додаток до традиційних

операції та протоколи, що робить можливою зворотну сумісність (більшість комерційні комутатори, доступні сьогодні, - це гібриди). Крім того, кожен перемикач складається із внутрішніх компонентів із трьох різних компонентів. Як показано на Рис. 1.9, основними частинами вимикача є такі:

1. OpenFlow канал, який дозволяє спілкуватися та керувати між зовнішнім контролером і комутатором через протокол OpenFlow.

2. Одна або кілька таблиць потоків, які зберігають записи потоку для виконання пакету пошук і переадресація.

3. Груповий стіл, особливий вид таблиці, призначений для виконання операцій, які є загальними для безлічі потоків.

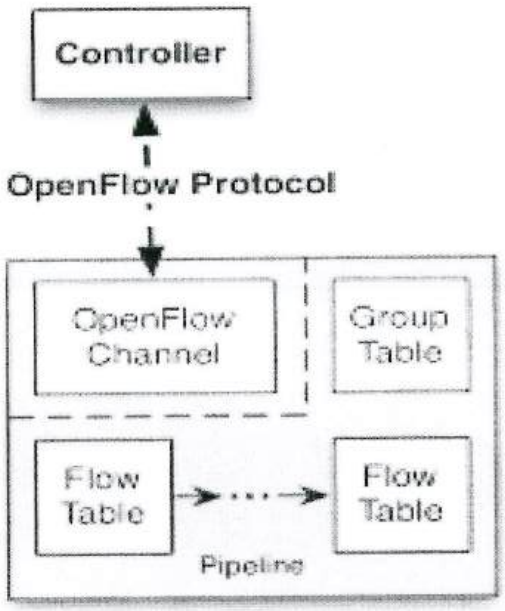


Рис. 1.9. Компоненти перемикача OpenFlow

Такий підхід дозволяє складно дії переадресації, такі як багатошаровість та агрегація ліній. Канал OpenFlow - це інтерфейс, який з'єднує кожен перемикач OpenFlow до контролера. За допомогою цього інтерфейсу контролер може управляти декількома перемикає надсилання та отримання повідомлень від них відповідно до протоколу OpenFlow. Канал OpenFlow також дозволяє забезпечити безпечне спілкування серед комутаторів і контролерів, що використовують безпеку транспортного шару (TLS) криптографічний протокол (до речі, зв'язок

може здійснюватися безпосередньо через TCP). Оскільки таблиці OpenFlow вважаються ядром OpenFlow, детальною аналіз потрібен. Зокрема, таблиці OpenFlow складаються з деяких основи механізмів. Як описано в наступному розділі, найбільш важливими є: відповідність пакету, яка витягує заголовок пакета і виконує пов'язані з ним дії, і обробка конвеєра, що дозволяє комутаторам переслати та обробити пакет через ланцюг таблиці.

Кожен перемикач OpenFlow може містити кілька таблиць потоків, які, як правило, складаються з декількох записів потоку. Механізм обробки визначає, як пакети повинні взаємодіяти з кожною таблицею потоків, як зображено на Рис. 1.10.

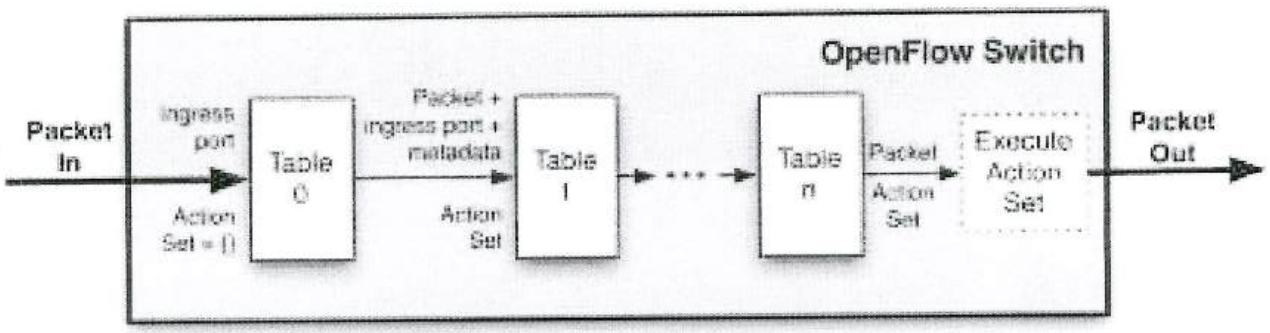


Рис.1.10. Взаємодія пакетів з таблицями потоків

Як показано на Рис. 1.10 кожен пакет узгоджується з записами потоку, починаючи з першої таблиці потоків, званої потоковою таблицею 0. Потім, залежно від За результатами попереднього матчу обробка трубопроводу може продовжуватися і тривати перейти до наступної таблиці подання для подальшої обробки. Для кожної таблиці може відбуватися відповідність пакетів, і, отже, деякі конкретні дії можуть здійснюватися комутатором. Оскільки відповідність пакетів є першою точка входу, яка консультувалася щодо процедури пошуку, більш детальна інформація щодо цього механізм необхідний.

Слабкі місця та проблеми SDN

Основна увага в цьому розділі стосується слабких сторін та проблем вирішення проблем за допомогою мереж SDN та протоколу OpenFlow. Пропозиція SDN та OpenFlow спосіб спростити прототипування, розгортання та

управління мережеві елементи. Однак ми також повинні враховувати деякі цікаві аспекти, які можуть призвести мережу до небезпечного або недоступного стану наступним чином:

1. Наявність контролера - головний аспект, який необхідно зробити розглянути. Жорстка залежність між вимикачами та контролером всякий раз, коли необхідна модифікація правил, може стати проблемою. Більше того, якщо дизайн мережі враховує лише один централізований контролер, це може стати "єдиною точкою відмови". Розподілений підхід може бути реалізований для гарантування доступності та уникнення потенційний небажаний збій. Крім того, деяка надмірність або резервне копіювання розчин може бути використаний для забезпечення надійності.

2. Важлива також безпека. У SDN контролер є компонентом критичні знання мережі та цей аспект піддає контролеру до можливих атак та погроз. Крім того, канали серед контролера та комутаторів можуть бути вразливими. За даними OpenFlow специфікації, можна використовувати захищений зв'язок за допомогою протоколу TLS, але його використання залежить від дизайну мережі з його моменту, тому він не потрібен.

3. Послідовність таблиць потоків також є потенційною проблемою. З кількох контролери можуть керувати однаковими таблицями потоків, наприклад, виробництвом з цього випливає апаратний контролер та деякі інші експериментальні контролери що останній буде «найслабшою ланкою в ланцюжку». Отже, вони може бути застосовано до нижчого контролю безпеки, що веде таблиці потоків у непослідовний стан. Реалізація датчика потоку може бути придатною уникнення цих потенційних загроз.

4. Масштабованість мережі також залежить від контролера, який потенційно може стати «вузьким місцем». У випадку, якщо занадто багатопакетів потрапить до контролер, проблеми з продуктивністю можуть виникати в мережі. З цього випливає, що важливо враховувати розподіл площини управління, для уникнення цих небажаних проблем.

5. Продуктивність мережі також може бути пов'язана з моделлю управління

прийнято. Оскільки розмір таблиці потоку обмежений, управління дуже велика кількість потоків все ще залишається сильним викликом. Однак добре розроблена мережа може знизити проблеми з продуктивністю за допомогою ініціативи підхід. Насправді, як раніше було проаналізовано, ініціатива підхід досягає кращих показників, ніж реактивний режим, оскільки він обмежує кількість повідомлень, що обмінюються між контролером та вимикачі. Описані вище аспекти були прийняті до уваги дослідники спільноти та представляють майбутні проблеми для SDN. В останньому розділі цієї глави представлений один з найпоширеніших контролерів, Floodlight, придатний для роботи зі SDN.

1.2 Опис сервісів які надаються

Телекомунікаційні сервіси (службові) – це послуги, які надаються у гетерогенному телекомунікаційному середовищі *в процесі організації взаємодії* між абонентами або машинами.

Сьогоднішні підприємства розгортають у своїх філіалах по декілька сервісів одночасно. Для багатьох із них підтримка виділеного автономного пристрою є надто затратною та негнучкою. В інших реалізаціях, функціональність може бути забезпечена інтегрованим маршрутизатором доступу, який може бути обмеженим у наборі функцій. По мірі того, як підприємство розвивається, все більше послуг та прикладних програмних компонентів мігрують до корпорації дата-центрів або загальнодоступних хмар, що приводить до змін в побудові корпоративних мереж. Крім того, мобільність і принцип BYOD (Bring Your Own Device – принеси свій власний пристрій) стають все більш затребуваними, в результаті чого стають актуальними послуги запобігання витоку даних.

Зіткнувшись із необхідністю великих інвестицій, багато підприємств починають шукати альтернативні варіанти. Ці альтернативи можуть включати в себе віртуалізацію Enterprise CPE (маршрутизатора доступу) в мережу оператора.

Такі тенденції віртуалізації в поєднанні з перевагами які надає NFV

забезпечують значні бізнес-можливості для постачальників послуг, які намагаються відповідати зростаючим потребам клієнтів. Традиційні IP-маршрутизатори, засновані на власному апаратному та програмному забезпеченні, є одними з найбільш капіталомістких частин інфраструктури постачальників послуг. Маршрутизатори оператора (Provider Edge routers) вичерпують ресурси платформи керування, перш ніж закінчуються ресурси платформи даних, таким чином віртуалізація функцій платформи керування покращує масштабованість.

Зберегти ресурси можна також переміщаючи функціональність маршрутизації від цільових маршрутизаторів до еквівалентних функцій, реалізованих в апаратних середовищах COTS, що забезпечують можливості хмарних обчислень, такі як NFVI.

Замість того, щоб інвестувати власний капітал у розгортання мережевої інфраструктури, постачальник послуг може надавати розширені мережеві функції. Постачальник може використовувати об'єкт VNF за допомогою інтерфейсу NFVI, який забезпечує функціональність, необхідну для впровадження клієнтського обладнання CPE та інший об'єктів VNF для платформи керування маршрутизатором оператора, покращуючи його масштабованість. Створення функціональності VNF для підприємства в якості служби можна порівняти з поняттям хмарного обчислення – «Програмне забезпечення як сервіс».

Інститут стандартизації NIST SP 800-146 [13] визначає програмне забезпечення як сервіс (SaaS) як можливість споживачів використовувати

прикладні програмні компоненти, що працюють у хмарній інфраструктурі. Споживач може керувати програмою лише з точки зору конфігурації та не може контролювати базову інфраструктуру.

У цьому прикладі віртуалізованих корпоративних служб VNF є прикладним програмним компонентом постачальника послуг. Підприємство є споживачем послуги. Підприємство не керує та не контролює NFVI або VNF. Підприємство як споживач VNFaaS не має інвестувати додатковий капітал у розширені мережеві функції, надані за допомогою платформи керування, а може отримати їх за певні кошти від постачальника послуг, якщо це необхідно. Постачальник послуг може

масштабувати ресурси NFVI, виділені на екземпляр VNF у відповідь на збільшення використання VNF.

NIST SP 800-146 [1, 3] визначили наступні переваги моделі SaaS, які також повинні застосовуватися у випадку з VNFaaS:

– Незначна роль програмного забезпечення підприємства для доступу до сервісу;

– Ефективне використання ліцензій на програмне забезпечення;

– Централізоване керування;

– Економія на попередніх витратах.

Мережі постачальників послуг Pre-NFV містять пороговий маршрутизатор PE на межі ядра перед пристроєм клієнтського обладнання (CPE), як показано на Рис. 1.11. При цьому є дві бізнес-моделі; як постачальник послуг так і підприємство можуть володіти та керувати CPE.



Рис. 1.11. Постачальник послуг без віртуалізації інфраструктури підприємства

Віртуалізація інфраструктури підприємства може включати:

– Віртуалізацію функцій обладнання користувача CPE (vE-CPE) у хмарі постачальника послуг.

– Віртуалізацію функцій порогового маршрутизатора оператора PE (vPE), де функції віртуальних сервісів мережі та функцій ядра PE можуть виконуватись в хмарі постачальника послуг.

Ці два етапи є незалежними і можуть розгортатись окремо. PE маршрутизатори, як правило, надаються великій кількості клієнтів, тоді як

маршрутизатор CPE використовується виключно одним клієнтом. Таким чином, економія масштабу, яку можна отримати від віртуалізації CPE є значно більшою, ніж при віртуалізації PE. Отже, віртуалізація CPE є корисною як для користувачів підприємства, так і для постачальників послуг. Віртуалізація PE може відбутись на більш пізньому етапі, щоб завершити перехід до повністю віртуалізованого рішення NFV.

У деяких архітектурах vE-CPE та vPE можуть контролюватися централізованим контролером, який виконує принципи та стандарти SDN (наприклад, OpenFlow).

Постачальник послуг несе відповідальність за розгортання, налаштування, оновлення та керування роботою екземпляру VNF для забезпечення очікуваного рівня обслуговування (SLA) для абонентів VNFaaS.

1.3 Вимоги до якості

Незважаючи на успіхи, досягнуті в області розробки мереж мобільного зв'язку четвертого покоління, з'являються нові вимоги, викликані зростаючими потребами в комунікаціях, що в свою чергу вимагає розвитку нового покоління мобільних мереж (5G). Нові можливості використання, такі як потокове відео високої роздільної здатності, віддалений моніторинг, управління в реальному часі створюють вимоги, пов'язані з пропускною здатністю, затримкою передачі, надійністю і стійкістю мережі.

Очікується, що мережі забезпечать високу безпеку, мінімальну затримку (нижче 5 мс.), надійність передачі 99,999% і стовідсоткову доступність.

Розробка мережі 5G повинна бути спрямована на подолання вищевказаних обмежень, з метою надання ультра-надійних, безпечних сервісів з мінімальною затримкою великій кількості інтелектуальних об'єктів і систем, а також новим мобільних терміналів.

Порівняння технологій 3G/4G/5G представлено на Рис.1.12 Технології IMT-2000 (3G) IMT-Advanced (4G) покращують пропускну здатність мережі, швидкість передачі даних користувачів, використання спектра і зменшують затримки. Впровадження технології IMT (5G) планується для "потужної і критично важливої машинної взаємодії", зменшення затримки, спектральної ефективності, швидкості, мобільності і надійності.

Мережева архітектура 5G складається з двох шарів: радіомережі та хмарної мережі. Різні типи базових станцій, що виконують мінімальний набір функцій, утворюють радіомережу. Хмарна мережа складається з площини користувача (User Plane Entity - UPE) і площині управління (Control Plane Entity - CPE), які виконують функції площини користувача і площини управління відповідно. Як показано на Рис. 1.13, фізична реалізація хмари може бути адаптована для задоволення різних цільових показників. Наприклад, UPE і CPE можуть бути розташовані близько до базових станцій для зменшення затримки критичних послуг. Також може бути виконано підключення БС до невеликого прилеглого центру обробки даних (ЦОД-3), а не до центрального ЦОД-2. З іншого боку, БС може бути з'єднана з ЦОД-2, якщо затримка не критична. Така гнучкість дозволяє оператору розгорнути великі і малі центри обробки даних для підтримки конкретних потреб у послугах. Така архітектура спрощує мережу і забезпечує швидке і гнучке розгортання і управління.

Різні технології, такі як Network Functions Virtualization (NFV) і Software Defined Networking (SDN) призначені для створення і впровадження таких мереж. Проте, майбутні сервіси, такі як потокове відео та інші послуги мають різні вимоги, які підкреслюють необхідність динамічного масштабування функціональності мережі.

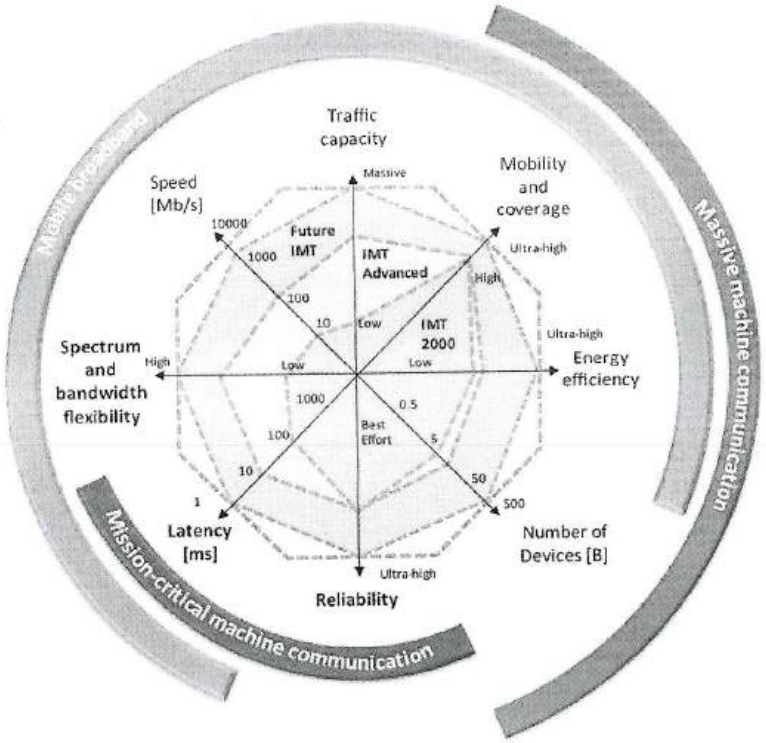


Рис. 1.12. Порівняння технологій 3G/4G/5G

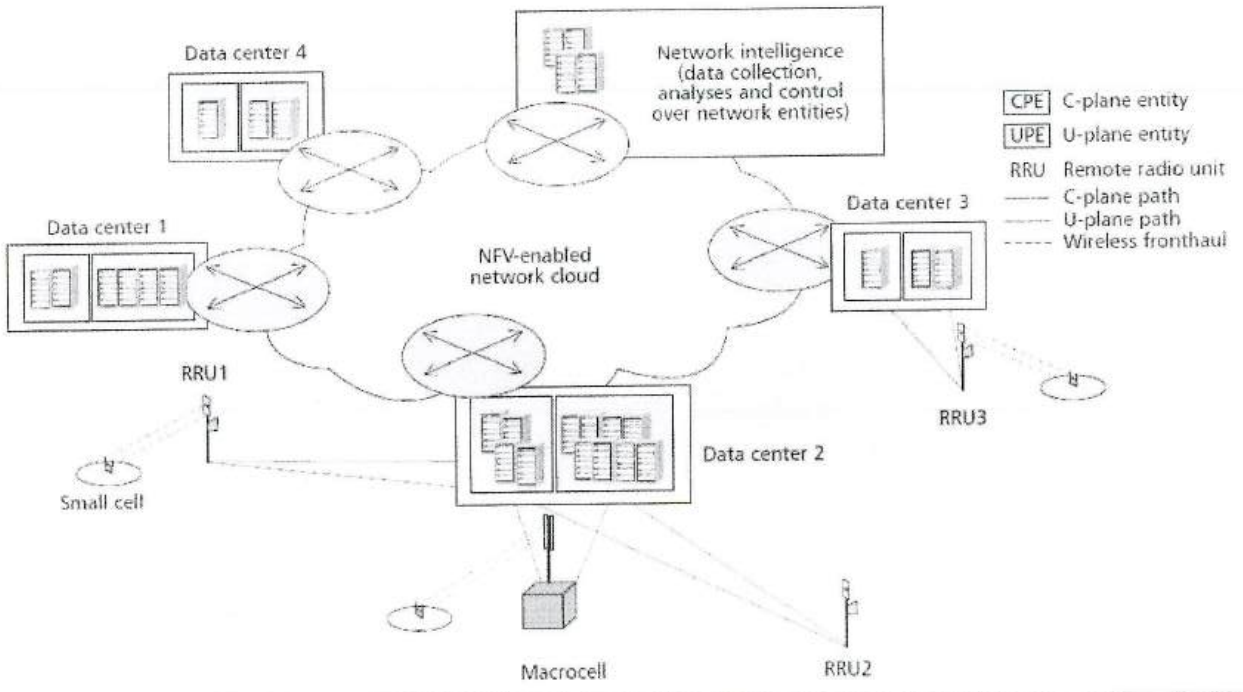


Рис. 1.13. Мережева архітектура 5G

Гетерогенні мережі відрізняються підвищеною пропускною здатністю, великим покриттям і надійністю, більш високою ефективністю використання радіочастотного спектру і низьким енергоспоживанням з боку як мережевої

інфраструктури, так і термінального обладнання.

Мобільні оператори мережі стикаються з наростаючою проблемою зростання трафіку передачі даних, в зв'язку з поширеністю смартфонів і транслюванням аудіо і відео послуг. У новій парадигмі оператори повинні управляти навантаженням, задовольняючи зростаючі споживчі і корпоративні очікування продуктивності, забезпечуючи повсюдний широкосмуговий доступ, а також швидко впроваджувати нові послуги, щоб зберегти конкурентну перевагу. Існуючі мобільні мережі постійно стикаються з такими обмеженнями, як стаціонарне і дороге устаткування, складні протоколи управління і гетерогенні інтерфейси конфігурації. З метою вирішення поточних обмежень, необхідно вивчати і застосовувати принципи SDN в мобільних мережах, а саме SDMN (Software Define Mobile Networks). SDN розділяє рівні управління і передачі даних, використовуючи стандартні протоколи, що дозволяють віддаленим пристроям здійснювати управління і експлуатацію рівнів даних. Протокол синхронізації потрібен для комунікації обох рівнів, одним з таких протоколів є OpenFlow. Переваги SDN в області хмарних обчислень є очевидними, однак застосування даної концепції в мобільних мережах вимагає подальшого вивчення.

В процесі еволюції механізму управління QoS в GSM/UMTS/LTE мережах сталася міграція управління QoS з рівня користувацького обладнання до керування на рівні мережі. Цей підхід також збережеться в мережах 5G.

Механізми керування QoS в мережах 5G повинні забезпечити пріоритет відео і VoIP трафіку над іншими сервісами. Сервіс потокового відео без буферизації дуже чутливий до затримок в мережі, тому одним з найбільш важливих параметрів, який визначає вимоги до QoS є загальний час затримки пакетів (packet delay budget - PDB). У Таблиця 1.1 наведені вимоги до затримки в 3G/4G/5G мережах.

Таблиця 1.1

Вимоги до затримки в 3G/4G/5G мережах

Терміни QoS	Запланована затримка пакетів (мс)		
	3G	4G	5G
Без гарантування якості	Не визначено	100-300	Не визначено
З гарантованою якістю	100-280	50-300	1

Ці дані показують, що з ростом покоління мобільної мережі, вимоги до нижньої межі затримки даних збільшуються. Також аналіз вимог до загальної мережевої затримки 5G показав, що вона повинна бути менше 1 мс.

На Рис. 1.14 представлено порівняння вимог до затримки на рівні управління/рівні користувача для сигнального/абонентського трафіків відповідно.

На Рис 1.14 видно, що вимоги до мережі 5G будуть в два рази жорсткішими для сигнального трафіку і в 10 разів жорсткішими для абонентського трафіку.

Іншим параметром є частка втрачених пакетів через помилки при отриманні пакетів даних (IP-packet Error Rate).

Значення цього параметра, що визначає вимоги максимального числа втрат IP пакетів для широкомовного відео за допомогою мобільних мереж 3G/4G/5G, наведені в Таблиця 1.2.

Таблиця 1.2

Вимоги до кількості втрачених пакетів для широкомовного відео в 3G/4G/5G мережах

Терміни QoS	Запланована затримка пакетів (мс)		
	3G	4G	5G
Без гарантування якості	10^{-2}	10^{-3}	10^{-4}
З гарантованою якістю	10^{-2}	10^{-6}	10^{-7}

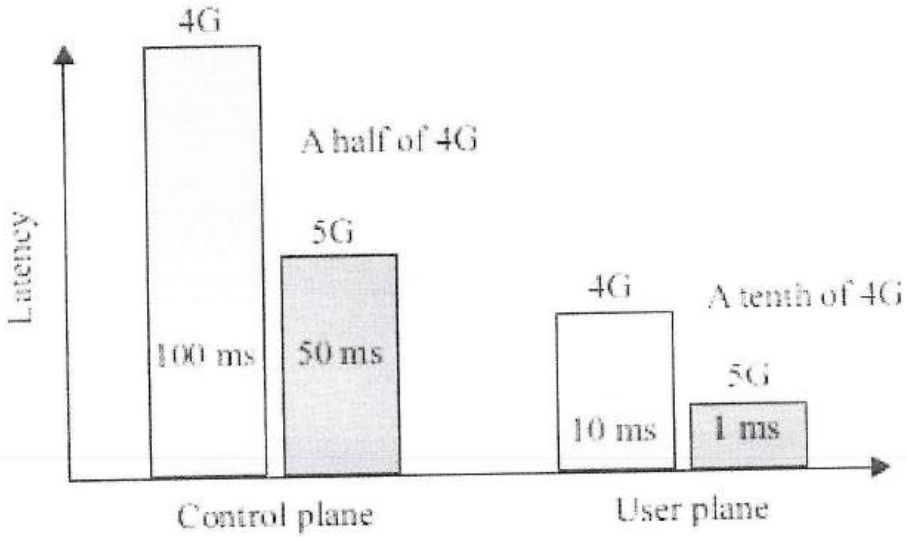


Рис. 1.14. Порівняння вимог до затримки на рівні управління та рівні користувача

Для інших сервісів якість також буде визначатися часткою втрачених пакетів в мережах 3G/4G/5G. Умови обслуговування абонентських пристроїв будуть визначатися в обох випадках: з гарантованою якістю обслуговування і без гарантованої якості. Вимоги до коефіцієнта втрат пакетів для інших послуг наведені в Таблиця 1.3.

Розвиток концепції NFV призведе до віртуалізації функцій управління якістю, які можуть бути розділені на 2 складові: управління (Cloud QoS management function - CQMF) і контролю (Cloud QoS control function - CQCF), які показані на Рис 1.15.

Таблиця 1.3

Вимоги до частки втрачених пакетів для інших сервісів в 3G/4G/5G мережах

Терміни QoS	Коефіцієнт втрат пакетів (Packet Error Loss Rate)			
	SDTV	HDTV	4k UHD	8k UHD
Покоління мобільних мереж	3G/4G	4G	4G	5G
Широкомовне відео з гарантованою якістю	10−6	10−7	10−8	10−9

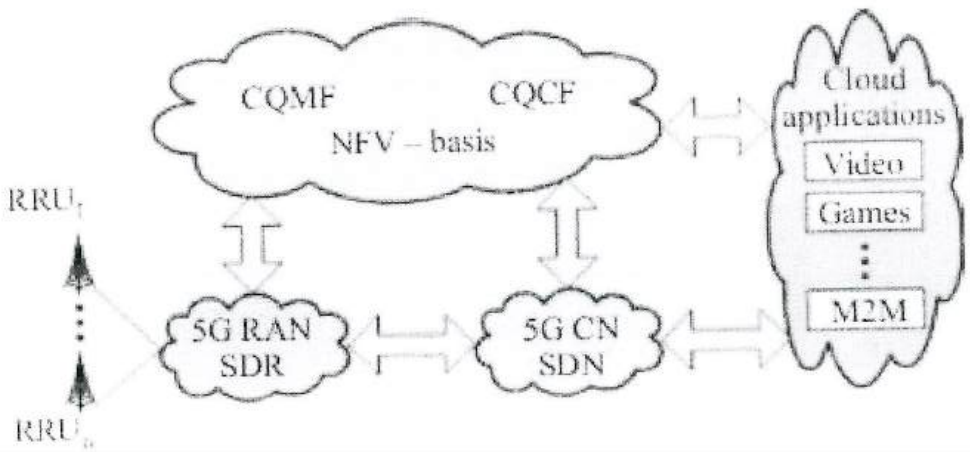


Рис. 1.15. Основні складові функцій управління якістю

Функція CQCF забезпечує контроль потоків трафіку в режимі реального часу на основі QoS, встановленого під час з'єднання. Основні механізми управління QoS включають управління профілями трафіку, планування і управління потоками даних.

Функція CQMF забезпечує підтримку QoS в мережі 5G відповідно до SLA, а також забезпечує моніторинг, технічне обслуговування, аналіз і масштабування QoS.

Реалізація алгоритмів пріоритетності трафіку в мережах 5G буде ґрунтуватися на процедурах класифікації трафіку з акцентом на пріоритети відео-трафіку і M2M трафіку. Класифікація процедур трафіку повинна бути проведена з урахуванням можливостей адаптації: характеристики трафіку будуть динамічно змінюватися з появою нових додатків, як в M2M області, так і в області відео.

1.3.1 Показники якості послуг передачі даних

Якість послуг передачі даних має вирішальне значення в галузі телекомунікацій, оскільки вона впливає на досвід і задоволення користувачів. Двома ключовими компонентами служб передачі даних є обслуговуючий вузол підтримки GPRS (SGSN) і вузол підтримки шлюзу GPRS (GGSN).

Якість послуг передачі даних SGSN можна виміряти трьома ключовими показниками: затримкою пакетів і джиттером, швидкістю втрат пакетів і пропускною здатністю. Затримка пакетів і тремтіння стосуються часу,

необхідного пакетам даних для проходження від джерела до пункту призначення, і варіації цього часу. Коефіцієнт втрати пакетів вимірює відсоток пакетів даних, втрачених під час передачі. Пропускна здатність вимірює кількість даних, які можна передати за певний період. Наприклад, у дослідженні, проведеному компанією Ericsson, якість послуг передачі даних SGSN оцінювалася на основі затримки пакетів, рівня втрат пакетів і пропускної здатності. Дослідження показало, що середня затримка пакетів становила 150 мс, коефіцієнт втрати пакетів – 0,5%, а пропускна здатність – 1,5 Мбіт/с.

Подібним чином якість послуг передачі даних GGSN можна виміряти за трьома ключовими показниками: частота втрат пакетів, затримка пакетів і тремтіння, а також пропускна здатність. Коефіцієнт втрати пакетів вимірює відсоток пакетів даних, втрачених під час передачі. Затримка пакетів і тремтіння стосуються часу, необхідного пакетам даних для проходження від джерела до пункту призначення, і варіації цього часу. Пропускна здатність вимірює кількість даних, які можна передати за певний період. Наприклад, у дослідженні, проведеному Huawei, якість послуг передачі даних GGSN оцінювалася на основі рівня втрати пакетів, затримки пакетів і пропускної здатності. Дослідження показало, що рівень втрати пакетів становив 0,7%, середня затримка пакетів – 120 мс, а пропускна здатність – 2,5 Мбіт/с.

На якість послуг передачі даних SGSN і GGSN можуть впливати різні фактори, включаючи топологію мережі, мережевий трафік і конфігурацію обладнання. З точки зору топології мережі, послуги передачі даних SGSN більше підходять для плоских мережевих топологій, тоді як служби передачі даних GGSN більше підходять для ієрархічних мережевих топологій. Крім того, апаратні конфігурації, такі як кількість процесорів і розмір пам'яті, можуть впливати на якість послуг передачі даних. Стратегії для покращення якості послуг передачі даних SGSN і GGSN включають оновлення апаратного забезпечення, оптимізацію топології мережі та впровадження політики якості обслуговування (QoS).

Отже, якість послуг передачі даних SGSN і GGSN можна виміряти

затримкою пакетів і тремтінням, швидкістю втрат пакетів і пропускною здатністю. Порівняльний аналіз служб передачі даних SGSN і GGSN показує, що обидва мають сильні та слабкі сторони, які можна вирішити за допомогою різних стратегій. Підвищення якості послуг передачі даних має важливе значення для забезпечення задовільного досвіду користувача та підтримки конкурентної переваги в галузі телекомунікацій.

В системах мобільного зв'язку третього покоління функції контролю параметрів доступності сервісів виконувала підсистема SGSN, в ядрі EPC ці функції виконує підсистема PCRF.

На Рис. 1.16 зображена архітектура мережі передачі даних 2G/3G. Основним мережевим вузлом в цій архітектурі є вузол підтримки послуг GPRS (Serving GPRS Support Node, SGSN), який відстежує розташування абонентських терміналів передачі пакетних даних, забезпечує захисні функції і контроль доступу. SGSN з'єднується з контролером базових станцій BSC, використовуючи Frame Relay - мережу комутації фреймів (пакетів другого, канального рівня). Вузол шлюзовий підтримки GPRS (Gateway GPRS Support Node, GGSN) взаємодіє з зовнішніми мережами пакетної передачі даних (Packet Data Networks, PDNs), забезпечуючи передачу даних до/від мобільних терміналів. GGSN пов'язаний із зовнішніми мережами з пакетним перемиканням і з'єднується з вузлами SGSN через мережі, які використовують протокол IP. Керуючий блок пакетної комутації (Packet Controller Unit, PCU) забезпечує послуги пакетної радіопередачі на область охоплення BSC. Для з'єднання вузлів SGSN і GGSN з іншими елементами мережі, що забезпечують глобальну пакетну передачу даних, може додаватися кілька нових інтерфейсів (з позначенням G*, де * - символ, що визначає конкретний інтерфейс).

Розглянемо основні причини збою в роботі системи передачі даних. Однією з найбільш поширених причин є помилка, яка відправляється з боку GGSN на Gn інтерфейс. Ця помилка широко поширена в GTP повідомленнях інформаційного елемента.

PDP Context - набір даних про абонента, що здійснив процедуру GPRS

Attach (процедуру аутентифікації і надання доступу в інтернет), який зберігається як на стороні SGSN, так і на стороні терміналу абонента, зокрема в цей набір даних входить профіль, що забезпечує певний рівень якості обслуговування абонента - QoS, призначена абоненту адреса в мережі, деякі дані про тарифікацію абонента.

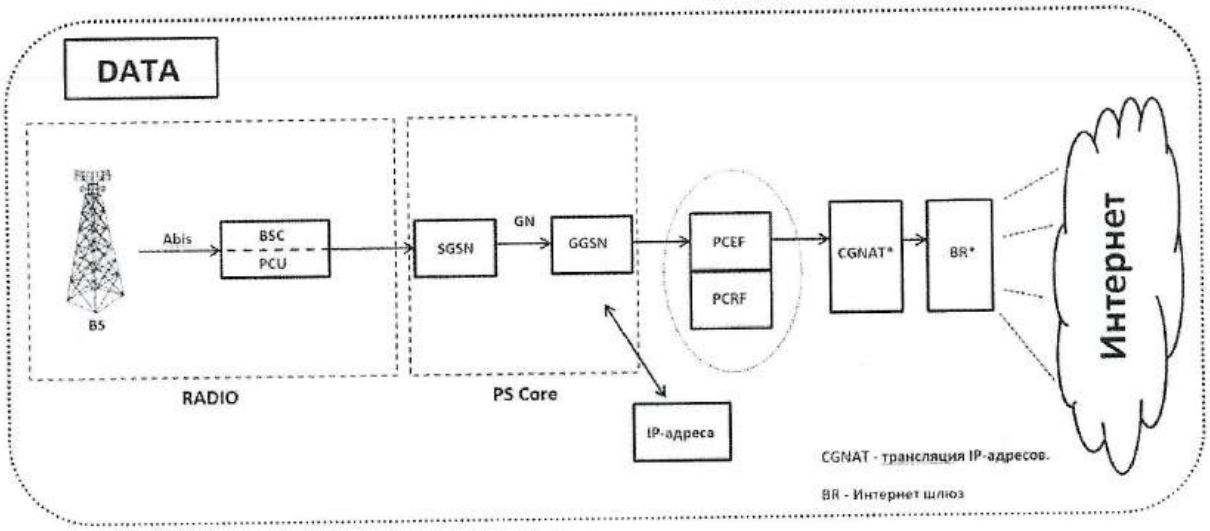


Рис. 1.16. Архітектура мережі передачі даних 2G/3G

Висновки

Якщо подивитись на нові вимоги суспільства то стає зрозуміло, що мереж четвертого покоління вже не вистачає для деяких задач, тому їх оновлення до 5G наразі є дуже актуальнім і в деяких країнах дана технологія вже в прямому доступі.

В даному розділі пройшло ознайомлення з такими технологіями як 5G, SDN, архітектурою та принципами SDN. Були описані Вимоги до якості та сервіси які надаються (SaaS, VNFaaS та інші). Проаналізувавши технології 5G було виявлено певні недоліки, була проведена оцінка та ознайомлення з рішеннями що до їх вирішення. Розроблені рекомендації що до розгортання мереж 5-го покоління та особливостей забезпечення якості обслуговування.

2 МЕХАНІЗМИ LTE, ГАРАНТІЯ ЯКОСТІ

2.1 Опис механізмів контроля LTE

Мережа оператору мобільного зв'язку – це складна технологічна система, яка складається як з спеціалізованого телекомунікаційного обладнання.

Long-Term Evolution (LTE) — це стандарт бездротового широкосмугового зв'язку, який забезпечує високу швидкість передачі даних і низьку затримку. Щоб досягти цього, LTE використовує різні механізми керування, які керують передачею даних між обладнанням користувача та мережею. Три основних механізмів керування в LTE: протокол керування радіоресурсами (RRC), протокол конвергенції пакетних даних (PDCP) і протокол керування радіоканалом (RLC).

Протокол RRC відповідає за встановлення, підтримку та розблокування радіозв'язку між обладнанням користувача та мережею LTE. Він керує сигнальними повідомленнями, якими обмінюються обладнання користувача та мережа, щоб встановити з'єднання, розподілити радіоресурси та розірвати з'єднання, коли воно більше не потрібне. Протокол RRC також реалізує процедури безпеки, такі як автентифікація та шифрування для забезпечення конфіденційності та цілісності даних, що передаються через радіоінтерфейс. Крім того, він керує передачею з'єднань між базовими станціями, щоб забезпечити безперебійне підключення під час переміщення обладнання користувача.

PDCP відповідає за стиснення та розпакування пакетів даних, щоб зменшити накладні витрати на передачу малих пакетів через радіоінтерфейс. Він реалізує стиснення заголовків для видалення зайвої інформації із заголовків пакетів, що зменшує розмір пакетів і покращує ефективність передачі. PDCP також керує процедурами повторної передачі та відновлення помилок, щоб забезпечити надійну передачу даних через радіоінтерфейс. Він виявляє помилки в отриманих пакетах і запитує повторну передачу втрачених пакетів, щоб

переконатися, що дані доставлені правильно.

Протокол RLC відповідає за забезпечення ефективної передачі пакетів даних через радіоінтерфейс. Він реалізує сегментацію та повторне збирання пакетів даних, щоб розбити їх на менші одиниці, які можуть передаватися ефективніше. Протокол RLC також реалізує механізми керування потоком і перевантаженням, щоб керувати швидкістю передачі даних і гарантувати, що мережа не буде перевантажена занадто великим трафіком. Він виявляє перевантаження в мережі та відповідно регулює швидкість передачі даних. Крім того, протокол RLC реалізує процедури виявлення та виправлення помилок, щоб забезпечити безпомилкову передачу даних.

Отже, три основні механізми керування в LTE - протокол RRC, PDCP і протокол RLC - відіграють вирішальну роль в управлінні передачею даних між обладнанням користувача та мережею. Кожен протокол має власний набір обов'язків і функцій, і разом вони забезпечують надійну та ефективну передачу даних через радіоінтерфейс. Розуміння цих механізмів контролю має важливе значення для мережевих інженерів і техніків, які відповідають за проектування, розгортання та підтримку мереж LTE.

Швидкість передачі по LTE в низхідному напрямку (до користувача) досягає 100 Мбіт/с, у висхідному - 50 Мбіт/с. Затримка на рівні користувача не перевищує 5 мс за рахунок високої ефективності використання спектра. Такі високі характеристики забезпечуються за рахунок використання декількох антен (принцип MIMO) і мультиплексування з ортогональним поділом частот OFDM на фізичному рівні.

Мережа E-UTRAN - це найперший вузол у вдосконаленій пакетній системі EPS. Вона забезпечує високу швидкість передачі даних, малу затримку на обох площинах керування і користувача, безшовне перемикання і більше покриття комірки. Розглянемо задачі, функції та процедури рівня доступу в стеку протоколів радіодоступу.

Структура E-UTRAN показана на Рис. 2.1. Мережа складається з вузлів eNodeB (eNB), які забезпечують протоколи площини користувача (PDCP/

RLC/MAC/PHY) і керування (RRC). Вузли eNB взаємодіють між собою через інтерфейс X2. Для зв'язку з удосконаленим пакетним ядром (EPC) використовується протокол S1. Обмін з вузлом керування мобільністю (MME) відбувається по інтерфейсу S1-MME, а с обслуговуючим шлюзом (SGW) - по інтерфейсу S1-U. Інтерфейс S1 підтримує зв'язки типу безліч- безліч між MME, SGW і eNB.

Інформацію, яку пропускає через себе UTRAN, прийнято розділяти на два шари. До шару доступу (AS) відносяться дані, необхідні для взаємодії терміналу користувача (UE) і мережі UTRAN. Шар без доступу (NAS) містить інформацію, переноситься між базової мережею оператора (CN) і UE через UTRAN.

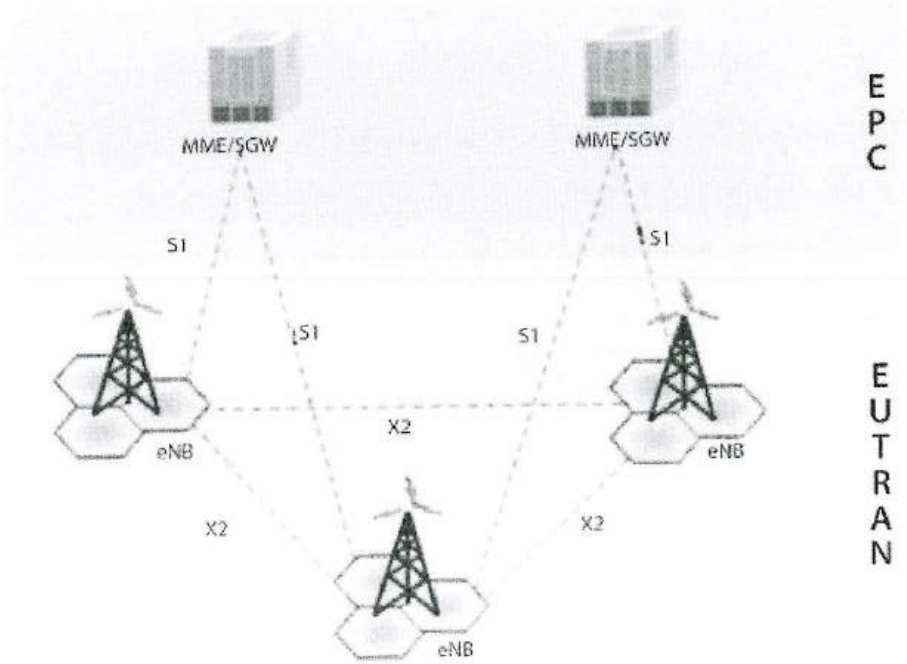


Рис. 2.1. Архітектура мережі E-UTRAN

Рівень доступу об'єднує протоколи радіодоступу. Це протоколи, що забезпечують спільне використання радіоресурсів обладнання користувача і мережі доступу. Крім того, AS відповідає за з'єднання з каналом радіодоступу (RAB), за допомогою яких забезпечується взаємодія між UE і CN (сервіс NAS).

Рівень доступу надає обладнанню користувача можливість отримання доступу до ресурсів і сервісів мережі, а також всю необхідну інфраструктуру.

Протоколи радіодоступу виконують такі функції:

- керування ресурсами радіоканалу (RRM). Це керування радіоканалом і радіоприйомом, контроль мобільності з'єднання і динамічний розподіл ресурсів обладнання користувача в обох напрямках передачі.

- керування трафіком:

- передача даних, в т.ч. в режимі реального часу, між інфраструктурою (рівень NAS) і обладнанням користувача;

- обробка всіх типів даних при різних параметрах каналу (рівень активності, пропускна здатність, затримка передачі і ймовірність появи помилкових бітів);

- ефективне перетворення атрибутів трафіку, які використовують не-LTE прикладними програмними компонентами, в атрибути каналу радіодоступу (RAB) на рівні доступу;

- стиснення IP-заголовка і шифрування потоків даних користувача;

- самостійний вибір MME на обладнанні користувача, коли мережа не надає відповідної інформації;

- передача даних з площини користувача на SGW;

- керування розташуванням: розподіл і передача пошукових повідомлень;

- розподіл і передача широкомовної інформації;

- задання конфігурації вимірюваних параметрів і форми виведення результатів для розподілу ресурсів і забезпечення мобільності;

- розподіл і передача повідомлень про землетруси і цунамі;

- надання первинного доступу до мережі, реєстрація та приєднання до мережі або вихід з неї;

- керування передачею на різних рівнях: між eNodeB, всередині eNodeB, між eNodeB зі зміною MME, між eNodeB зі збереженням MME, але зміною SGW, між RAT;

- функціональна різноманітність і шифрування;

- кодування радіоканалу.

SAE – це архітектура ядра мережі, розроблена консорціумом 3GPP для стандарту бездротового зв'язку LTE (Рис. 2.2).

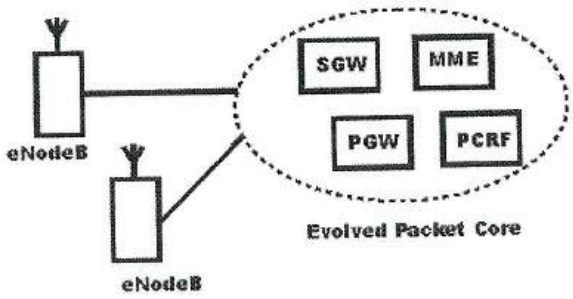


Рис. 2.2. Архітектура ядра мережі SAE

Розвиток системної архітектури (SAE) — це базова мережева архітектура для мобільних мереж 4G і 5G. SAE — це комплексна мережева архітектура, яка забезпечує надання високоякісних мобільних широкосмугових послуг. Архітектура складається з кількох ключових компонентів, включаючи Evolved Packet Core (EPC) і базову мережу 5G. EPC відповідає за керування трафіком даних між мобільними пристроями та Інтернетом, тоді як базова мережа 5G надає розширені функції, такі як нарізка мережі, периферійні обчислення та автоматизація мережі. Архітектура SAE розроблена для підтримки широкого діапазону мобільних пристроїв, включаючи смартфони, планшети та пристрої IoT.

Переваги SAE надають кілька переваг мережевим операторам і кінцевим користувачам. По-перше, SAE покращує продуктивність і надійність мережі шляхом зменшення затримки та збільшення пропускної здатності даних. Це забезпечує доставку програм із високою пропускною здатністю, таких як потокове відео та онлайн-ігри. По-друге, SAE забезпечує розширену підтримку програм із низькою затримкою, таких як автономні транспортні засоби, віртуальна реальність і доповнена реальність. По-третє, SAE забезпечує більшу масштабованість і гнучкість для операторів мереж, дозволяючи їм адаптуватися до мінливих вимог мережі та швидко розгортати нові послуги.

Незважаючи на свої переваги, SAE також має ряд проблем і обмежень. По-перше, інтеграція SAE із застарілими мережевими системами може бути складною та трудомісткою. Це може призвести до затримок у оновленні та

розгортанні мережі. По-друге, перехід від застарілих мереж до SAE може бути складним, особливо для мережевих операторів із великими та складними мережами. По-третє, існують проблеми безпеки та конфіденційності, пов'язані з обробкою конфіденційних даних користувача. Оператори мереж повинні забезпечити захист даних користувачів і дотримання правил конфіденційності.

SAE є основною мережевою архітектурою для сучасних мобільних мереж, що забезпечує покращену продуктивність мережі, надійність і гнучкість для мережевих операторів. У той час як SAE має кілька переваг, він також представляє кілька проблем і обмежень, пов'язаних із інтеграцією із застарілими мережами, міграцією, а також проблемами безпеки та конфіденційності. Незважаючи на ці проблеми, SAE залишається критично важливим компонентом сучасних мобільних мереж, забезпечуючи надання високоякісних мобільних широкосмугових послуг мільйонам користувачів у всьому світі.

SAE є еволюційним продовженням ядра мережі GPRS, з деякими відмінностями:

- спрощена архітектура - архітектура SAE знижує експлуатаційні та капітальні витрати. Нова плоска модель означає, що потрібно підвищити пропускну здатність вузлів тільки двох типів (базових станцій і шлюзів), щоб вони впоралися з трафіком в разі його значного зростання.

- цілком побудована на IP (AIPN) – перші концепції 3G було розроблено для того, щоб голос, як і раніше передавався по системі з комутацією каналів. З тих пір спостерігався перехід до IP-мереж. Відповідно архітектура SAE побудована на базі IP-мережі.

- забезпечує більшу пропускну здатність мережі радіодоступу (RAN) – передбачається, що низхідний канал (Down Link) буде мати швидкість понад 100 Мбіт/с, і основна увага системи буде зосереджена на мобільності смуги пропускання, мережа повинна буде підтримувати набагато більше рівнів даних.

- забезпечує меншу затримку RAN - зі збільшенням необхідних рівнів взаємодії і більш швидких відповідей, SAE концепція забезпечить рівень затримки в районі 10 мс.

- підтримує мобільність між декількома гетерогенними RAN, що включає підтримку, як систем типу GPRS, так і не-3GPP систем (наприклад WiMAX) [1].

Основним компонентом архітектури SAE є Evolved Packet Core (EPC). EPC служить еквівалентом мережі GPRS. Архітектура EPC показана на Рис. 2.3.

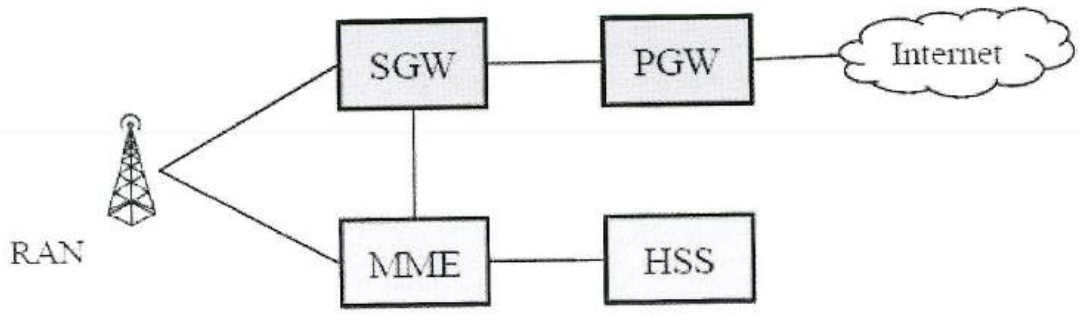


Рис. 2.3. Типова архітектура EPC/LTE

Архітектура EPC є мережею All-IP з комутацією пакетів, який вміщує різні схеми бездротового доступу, такі як Long Term Evolution (LTE). Мережа EPC складається з різних вузлів: Evolved NodeB (eNB) вузла для радіодоступу LTE, об'єкта керування мобільністю (MME) – вузол для керування мобільності терміналу, вузла домашньої абонентської системи (HSS), вузла бази даних інформації про користувачів, вузла облслуговуючого шлюза (SGW), вузла якірної точки мобільності для керування терміналами, а також вузла шлюза пакетної мережі передачі даних (PGW), який служить шлюзом між терміналами і зовнішніми мережами, такими як Інтернет. [2]

MME – це ключовий контролюючий модуль для мережі доступу LTE. Він відповідає за процедури забезпечення мобільності, хендовера, стеження і пейджінга UE. Він бере участь в процесах активації/дезактивації мережевих ресурсів і так само відповідає за вибір SGW для UE при початковому підключенні і при хендовері всередині LTE зі зміною вузла ядра мережі (CN). Він відповідає за аутентифікацію користувача (при взаємодії з HSS).

SGW – призначений для обробки і маршрутизації пакетних даних, що надходять в підсистему базових станцій. SGW маршрутизує і направляє пакети з одними даними, в той же час виконуючи роль вузла керування мобільністю для

даних користувача при хендовері між базовими станціями (eNodeB), а також вузла керування мобільністю між мережею LTE і мережами з іншими технологіями 3GPP. Коли UE вільний і не зайнятий викликом, SGW відключає низхідний канал даних (DL) і створює пейджинг, якщо потрібно передати дані по DL в UE напрямку. Він керує і зберігає стани UE (наприклад вимоги до пропускної здатності для IP-сервісів, внутрішню інформацію мережевої маршрутизації). Він також надає копію даних користувача при узаконеному перехопленні.

PGW – забезпечує з'єднання від UE до зовнішніх пакетних мереж даних, будучи точкою входу і виходу трафіку для UE. UE може мати одночасно з'єднання з більш ніж одним PGW для підключення до декількох мереж. PGW виконує функції захисту, фільтрації пакетів для кожного користувача, підтримку білінгу, узаконеного перехоплення і сортування пакетів. Інша важлива роль PGW - бути вузлом керування мобільністю між 3GPP і не-3GPP технологіями, такими як WiMAX і 3GPP2 (CDMA 1X і EVDO).

HSS – це центральна база даних, яка містить інформацію про користувача. Функції HSS включають мобільність, керування викликами і підтримкою встановлення сеансу, аутентифікацію і авторизацію користувачів. HSS базується на pre-Rel-4 Home Location Register (HLR) і центрі аутентифікації (AuC) [3].

2.2 Протоколи гарантії якості в мережах доступу і на рівні ядра мережі

Протоколи забезпечення якості відіграють вирішальну роль у забезпеченні оптимальної роботи мереж і відповідності очікуванням клієнтів.

Мережі доступу є першою точкою контакту для користувачів, які підключаються до Інтернету. Таким чином, вони відіграють вирішальну роль у забезпеченні надійного з'єднання. Існує кілька типів мереж доступу, включаючи цифрові абонентські лінії (DSL), кабельні, оптоволоконні та бездротові. Кожен тип мережі доступу має власні унікальні протоколи забезпечення якості.

Наприклад, DSL-мережі покладаються на ослаблення сигналу та запас шуму для забезпечення надійного з'єднання. З іншого боку, кабельні мережі використовують співвідношення сигнал/шум і методи виправлення помилок для підтримки якості. Оптоволоконні мережі використовують рівні оптичної потужності та вимірювання дисперсії, щоб гарантувати безпомилкову передачу сигналів. Бездротові мережі використовують такі методи, як вимірювання потужності сигналу та перешкод для підтримки якості. Однак забезпечення якості в мережах доступу може бути складним завданням. Перешкоди сигналу, збій обладнання та обмежена пропускна здатність – це лише деякі з проблем, які можуть вплинути на роботу мережі. Щоб подолати ці проблеми, мережеві оператори повинні запровадити протоколи забезпечення якості, адаптовані до конкретного типу мережі та її унікальних проблем.

Ядро мережі відповідає за керування трафіком, маршрутизацію та безпеку мережі. Таким чином, дуже важливо підтримувати гарантію якості на цьому рівні. Протоколи забезпечення якості для основних компонентів мережі, таких як маршрутизатори, комутатори та брандмауери, необхідні для забезпечення оптимальної роботи мережі. Одним із ключових протоколів забезпечення якості основних компонентів мережі є резервування. Резервування гарантує наявність резервних компонентів на випадок збою. Механізми відновлення після відмови також мають вирішальне значення для того, щоб мережа могла продовжувати працювати у разі збою. Окрім механізмів резервування та відновлення після збоїв, мережеві оператори також повинні запровадити протоколи забезпечення якості для безпеки мережі. Брандмауери, системи виявлення вторгнень та інші заходи безпеки необхідні для захисту мережі від кіберзагроз.

Щоб забезпечити оптимальну роботу мереж, мережеві оператори повинні впроваджувати найкращі практики та бути в курсі нових тенденцій у протоколах забезпечення якості. Однією з найкращих практик є впровадження угод про рівень обслуговування (угоди про рівень обслуговування гарантують, що продуктивність мережі відповідає очікуванням клієнтів, і забезпечують основу для вирішення проблем, коли вони виникають. Ще одна найкраща практика – це

використання автоматизованих засобів моніторингу та тестування. Ці інструменти проактивно визначають і вирішують мережу проблеми, перш ніж вони вплинуть на продуктивність мережі. Вони також можуть скоротити час і зусилля, необхідні для діагностики та вирішення проблем, коли вони виникають. Нарешті, інтеграція штучного інтелекту та машинного навчання є новою тенденцією в протоколах забезпечення якості. Ці технології можуть оптимізувати мережу: алгоритми машинного навчання можуть аналізувати моделі мережевого трафіку, щоб виявити потенційні проблеми, перш ніж вони вплинуть на продуктивність мережі.

Протокол: NBAP (Node B Application Part).

Оркестрація та менеджмент (O&M) базової станції UMTS (Node B) Node B розділена на дві частини: O&M, пов'язана з фактичною реалізацією базової станції, позначена як конкретна реалізація (Implementation Specific) O&M, та O&M, що впливає на ресурси передачі трафіку в базовій станції, яка управляється контролером радіомережі, позначена як логічна O&M. Архітектура контролера мережі (RNC) з інтерфейсами O&M показана на Рис.2.4.

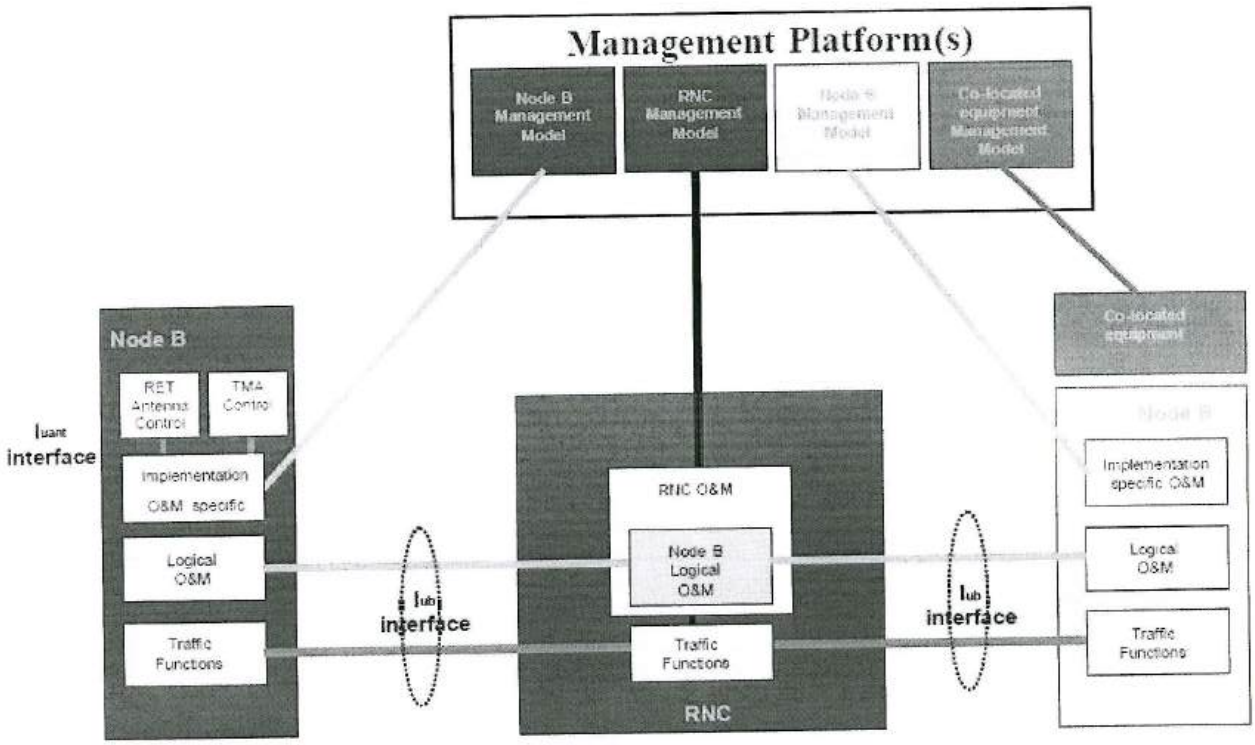


Рис. 2.4. Архітектура контролера мережі з інтерфейсами O&M

На функції конкретної реалізації O&M значною мірою впливає реалізація базової станції (NodeB), як з точки зору її апаратних компонентів, так і з точки зору управління компонентами програмного забезпечення. Тому функції є залежними від реалізації та виконуватися між базовою станцією та системою управління.

Як варіант транспортного рішення для конкретної реалізації O&M - це маршрут від базової станції до системи управління через контролер мережі RNC. У цьому випадку інтерфейс конкретної реалізації O&M для та інтерфейс Iub мають одного і того ж фізичного каналу, а TS 25.442 [4] визначає функцію маршрутизації та транспортного каналу для цього сценарію. Розгортання маршрутизації через RNC в UTRAN є необов'язковим. Там, де потрібна сигналізація між спільно розміщеним обладнанням та його системою управління, вона може бути перенесена на той самий канал, що і конкретна реалізація O&M.

Логічна O&M - сигналізація, пов'язана з контролем логічних ресурсів (каналів, сот, ...), що належать контролеру мережі RNC, але фізично реалізовані у базовій станції. Контролер радіомережі контролює ці логічні ресурси. Ряд процедур O&M, фізично реалізованих у Node B, впливають на логічні ресурси, і тому вимагають обміну інформацією між RNC та Node B. Усі повідомлення, необхідні для підтримки цього інформаційного обміну, класифікуються як логічні O&M, які є невід'ємною частиною сигнального протоколу NBAP (Node B Application Part).

QoS протоколи

Протоколи якості обслуговування QoS — це набір правил, які визначають пріоритет мережевого трафіку, щоб гарантувати доставку критичних даних із мінімальними затримками та втратами. Протоколи QoS мають важливе значення для передачі даних, оскільки вони допомагають керувати перевантаженнями мережі, зменшують затримку та забезпечують ефективне використання мережевих ресурсів. Існує три типи протоколів QoS: Integrated Services (IntServ), Differentiated Services (DiffServ) і Best Effort. Integrated Services (IntServ) — це протокол QoS, який забезпечує наскрізну якість обслуговування для окремих

програм. IntServ використовує протокол резервування ресурсів (RSVP) для резервування мережевих ресурсів і забезпечення наявності необхідної пропускної здатності для певних програм. IntServ також використовує угоди про рівень обслуговування (SLA), щоб переконатися, що мережевий провайдер відповідає узгодженим вимогам щодо якості обслуговування.

IntServ — це протокол QoS, який пропонує високий рівень обслуговування для окремих програм. IntServ забезпечує основу для наскрізної якості обслуговування, резервуючи мережеві ресурси для конкретних програм. IntServ використовує RSVP для резервування пропускної здатності та забезпечення наявності необхідних ресурсів для певних програм. RSVP — це протокол сигналізації, який дозволяє мережі резервувати ресурси для певних програм. IntServ також використовує угоди про рівень обслуговування (SLA), щоб переконатися, що мережевий провайдер відповідає узгодженим вимогам щодо якості обслуговування. Угоди про рівень обслуговування — це контракти між мережевим провайдером і клієнтом, які визначають рівень обслуговування, який буде надаватися. Угоди про рівень обслуговування визначають такі параметри якості обслуговування, як пропускна здатність, затримка та втрата пакетів, яких повинен дотримуватися постачальник мережі.

Диференційовані послуги (DiffServ) — це протокол QoS, який забезпечує масштабований і гнучкий підхід до якості обслуговування. DiffServ використовує Differentiated Service Code Point (DSCP) для позначення пакетів і пріоритезації трафіку. Значення DSCP використовуються для класифікації трафіку на різні класи та призначення різних рівнів обслуговування кожному класу. DiffServ також використовує Per Hop Behavior (PHB) для визначення поведінки мережі на кожному стрибку. PHB визначає алгоритми постановки в чергу та планування, які використовуються для визначення пріоритетів трафіку. PHB забезпечує пріоритетність трафіку на основі його важливості та доставку критичних даних із мінімальними затримками та втратами.

Враховуючи вищесказане, протоколи QoS мають важливе значення для передачі даних, щоб забезпечити ефективне та ефективне використання

мережевих ресурсів. Існує три типи протоколів QoS: Integrated Services (IntServ), Differentiated Services (DiffServ) і Best Effort. IntServ і DiffServ є найбільш часто використовуваними протоколами QoS. IntServ забезпечує наскрізну якість обслуговування для окремих програм, тоді як DiffServ забезпечує масштабований і гнучкий підхід до якості обслуговування.

Функція (TF, Translation Function) *трансляції* перетворює внутрішні примітиви послуг мережі LTE в модулі різних протоколів взаємодіючих зовнішніх мереж, включаючи перетворення атрибутів послуг мережі LTE в параметри QoS протоколів зовнішніх мереж[19, 21].

Функція управління можливостями (A/CCF, Admission / Capability Control Function) забезпечує інформацією про усі можливі ресурси мережевих вузлів, визначаючи при кожному запиті (чи модифікуванні) послуги, чи можуть мережеві вузли забезпечити необхідні ресурси. Ця функція також контролює можливість надання самої послуги, тобто чи реалізована в мережі запитана послуга.

Функція керування підпискою (SCF, Subscription Control Function) забезпечує контроль доступності абонентам певних послуг з необхідними параметрами QoS.

Відповідно до рекомендації 3GPP TS 23.402 V15.1.0 (2017-09), модель QoS, яка застосовується в поєднанні з опорними точками на основі протоколу PMIP, не використовує ідентифікатори каналів у пакетах площини користувача. Вона базується на фільтрах пакетів та пов'язаних з ними параметрах QoS (QCI, ARP, MBR, GBR), що надаються системі доступу через позамаршрутну (off-path) сигналізацію.

PCRF сигналізує ті ж фільтри пакетів та пов'язані з ними параметри QoS через Gxa, Gxb та Gxc, що і через Gx; інакше кажучи, деталізація інформації QoS, яка передається через Gxa, Gxb та Gxc, така ж, як і через Gx.

Канал EPS з S5/S8 на основі протоколу PMIP і протоколу доступу E-UTRAN показано на Рис. 2.5.

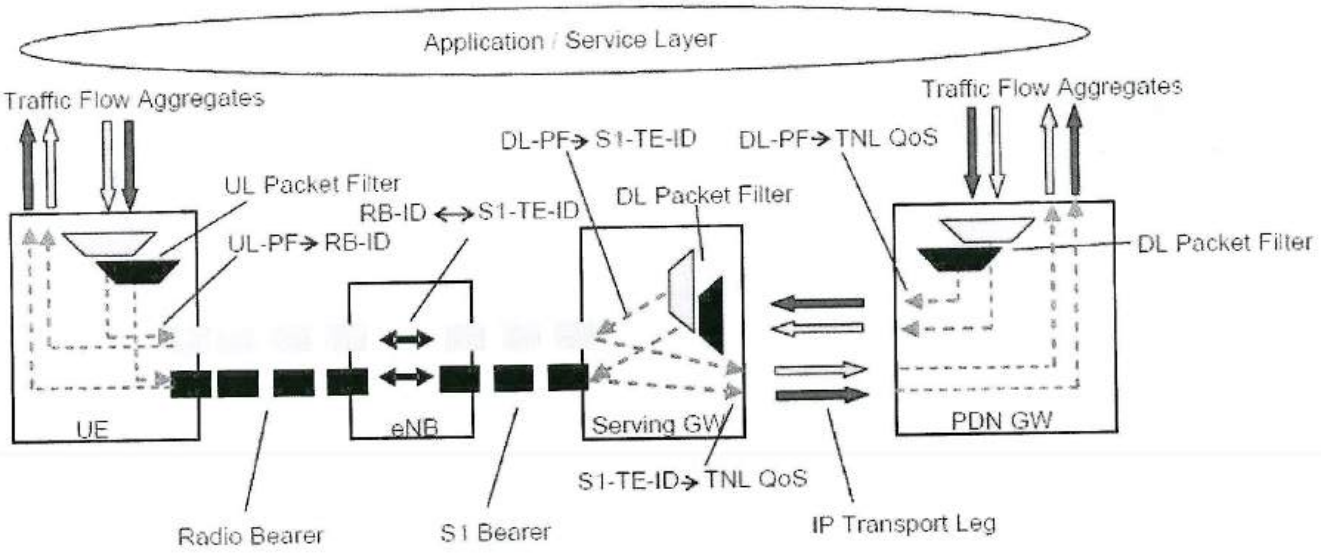


Рис. 2.5. Два канали Unicast EPS (S5/S8 на основі PMIP та протокол доступу E-UTRAN)

Для S5/S8 на основі протоколу PMIP та протоколу доступу E-UTRAN, канал EPS містить конкатенацію одного радіоканалу та одного каналу S1. Служба підключення PDN між обладнанням користувача (UE) і зовнішньою мережею пакетної передачі даних підтримується шляхом об'єднання каналу EPS та IP-з'єднання між шлюзом обслуговування і шлюзом PDN. Контроль QoS між Serving GW і PDN GW забезпечується на рівні транспортної мережі (TNL).

Канал EPS реалізується наступними елементами:

- В обладнанні користувача UFT TFT відображає агрегат потоку трафіка до каналу EPS у напрямку висхідної лінії зв'язку.

- У шлюзі обслуговування (Serving GW) DL TFT відображає агрегат потоку трафіку до каналу EPS у напрямку низхідної лінії зв'язку.

- радіоканал передає пакети каналу EPS між UE та eNodeB. Існує одноразове відображення між каналом EPS та радіоканалом.

- Канал S1 переносить пакети каналу EPS між eNodeB і шлюзом обслуговування. Існує одноразове відображення між каналом EPS та каналом S1.

- Для кожного обладнання користувача в туннелі PDN транспортуються пакети каналу EPS між шлюзом обслуговування та шлюзом PDN. Між каналом EPS та цим тунелем реалізується відображення «багато до одного».

- UE зберігає відображення між фільтром пакетної передачі висхідної лінії зв'язку та радіоканалом для створення зв'язків між агрегатом потоку трафіку та радіоканалом у висхідній лінії зв'язку.

- eNodeB зберігає відображення «один до одного» між радіоканалом та каналом S1, щоб створити зв'язок між радіоканалом та каналом S1 як у напрямку висхідної лінії зв'язку, так і в напрямку низхідної лінії зв'язку[16].

- Шлюз обслуговування зберігає відображення «один до одного» між фільтром пакетної передачі по низхідній лінії зв'язку та каналом S1, щоб створити відображення між агрегатом потоку трафіку та каналом S1 у низхідній лінії зв'язку.

- Шлюз доступу до інших мереж (PDN SW) забезпечує APN-AMBR для всіх SDF тих самих APN, які пов'язані з QCI без GBR.

Параметри QoS мають першочергове значення для технології SDN. При цьому важливо враховувати зв'язок між типом прикладних програм (передача даних в реальному часі чи передача файлів) та параметрами мережі, такими як доступна смуга пропускання, втрати пакетів, затримки або джиттер.

В таблиці наведено вимоги до параметрів якості обслуговування SDN для різного типу трафіку.

Таблиця 2.1

Вимоги до параметрів якості обслуговування SDN

Тип трафіку	Затримка	Втрати пакетів	Джиттер	Смуга пропускання
Голосова телефонія (VoIP)	≤ 20 мс	≤ 1%	< 30 мс	21-320 кбіт/с
Відео	≤ 150 мс	≤ 1%	≤ 30 мс	10-20 Мбіт/с
Потокове відео	≤ 4-5 мс	≤ 1%	–	40-100 Мбіт/с

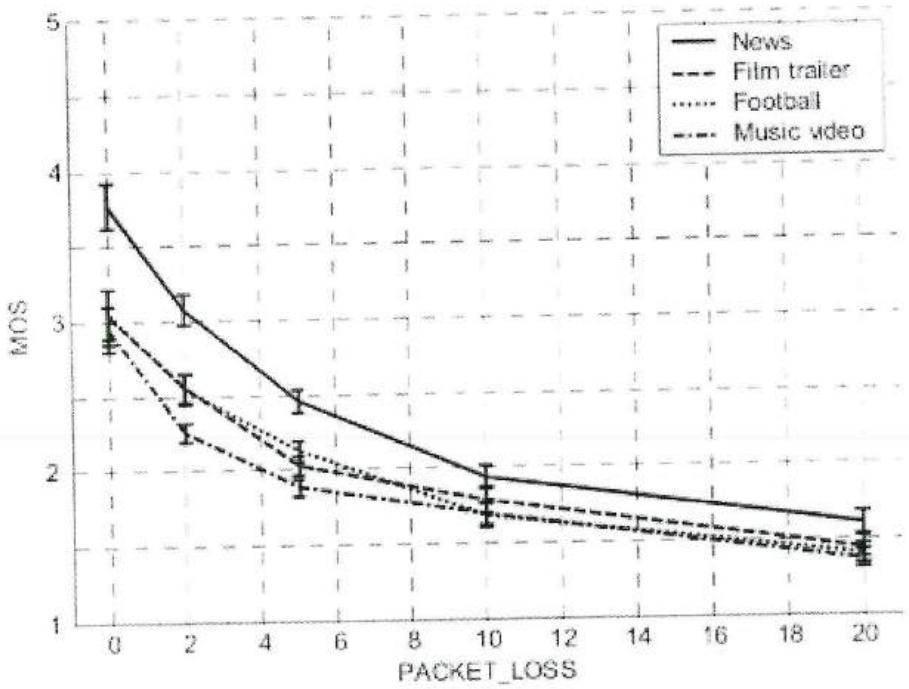


Рис. 2.6. Графік втрати пакету

Голосова телефонія не терпить втрат пакетів (в ідеалі, їх взагалі не повинно бути), особливо якщо використовується стиснутий кодек.

Максимальна затримка потокового відео залежить від буферизації відео-додатків, тому вона може бути меншою за вказане значення.

Допустиме значення джиттера не є основним параметром для прикладних програм, що використовують потокове відео, тому для нього немає визначених вимог. Вимоги до пропускної здатності потокового відео пов'язані з форматом кодування і швидкістю відеопотоку, тому вони не мають фіксованого значення.

Висновки

У другому розділі проаналізовано та описано механізм LTE, також проведено ознайомлення з перевагами та недоліками LTE. При аналізі вже відомих механізмів також пройшло ознайомлення з архітектурою мережі SAE, EPC/LTE. Були досліджені наступні протоколи гарантії якості в мережах доступу: NBAP (Node B Application Part), QoS протоколи. Ми підходимо до висновку про те що поточні мережі 4G не витримують вимог, висунутих новими сценаріями застосування на данний час, тому технологія 5G на разі дуже актуальна.

3 ГАРАНТУВАННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ

3.1 Процедура гарантування заданої якості обслуговування

Надання високоякісних послуг має вирішальне значення для будь-якої організації, яка хоче досягти успіху на сучасному конкурентному ринку. Однак забезпечення незмінної якості може бути складним завданням, особливо коли ви маєте справу з різними постачальниками послуг і очікуваннями клієнтів. Гарантування даної якості обслуговування як процес передбачає встановлення стандартів якості, впровадження заходів контролю якості та постійне покращення якості послуг.

Першим кроком у гарантуванні заданої якості послуг є встановлення стандартів якості. Це передбачає визначення ключових показників ефективності (KPI), які визначають високоякісну послугу, встановлення контрольних показників для кожного KPI на основі галузевих стандартів і очікувань клієнтів, а також документування стандартів якості в угоді про рівень обслуговування (SLA). Наприклад, KPI готелю можуть включати чистоту в номерах, чуйність персоналу та задоволеність гостей. Контрольні показники для кожного KPI можна встановити на основі галузевих стандартів і відгуків клієнтів. SLA окреслить очікування щодо кожного KPI та наслідки їх недотримання.

Після встановлення стандартів якості наступним кроком є впровадження заходів контролю якості. Це передбачає розробку контрольного списку контролю якості, який охоплює всі ключові показники ефективності в SLA, навчання постачальників послуг дотримуватися контрольного списку та надання узгоджених послуг, а також проведення періодичних аудитів для забезпечення відповідності стандартам якості. Наприклад, контрольний список контролю якості ресторану може включати такі пункти, як температура їжі, презентація та обслуговування клієнтів. Персонал буде навчено дотримуватися контрольного списку та надаватиме постійне обслуговування. Будуть проводитися періодичні перевірки, щоб переконатися, що ресторан відповідає

стандартам якості, викладеним у SLA.

Останнім кроком у гарантуванні заданої якості обслуговування є постійне покращення якості обслуговування. Це передбачає збір відгуків від клієнтів за допомогою опитувань, оглядів і скарг, використання відгуків для визначення областей для покращення послуги, впровадження змін до послуги на основі відгуків і моніторинг впливу на KPI. Наприклад, компанія з прокату автомобілів може збирати відгуки клієнтів за допомогою опитувань і оглядів. Якщо клієнти постійно скаржаться на тривалий час очікування, щоб отримати взятий напрокат автомобіль, компанія може запровадити новий процес, щоб оптимізувати процес реєстрації та контролювати вплив на KPI.

Гарантування заданої якості послуг вимагає системного підходу, який передбачає встановлення стандартів якості, впровадження заходів контролю якості та постійне покращення якості послуг. Дотримуючись цієї процедури, організації можуть гарантувати, що їхні послуги відповідають очікуванням клієнтів і залишаються конкурентоспроможними на ринку.

Принцип динамічного контролю якості полягає у наступному: значення затримки у обслуговуванні заявки на встановлення з'єднання (роз'єднання, відновлення) порівнюється із політикою якості обслуговування відповідного абонента. Якщо показник не відповідає, тоді послідовно порівнюються показники якості у віртуальних вузлах та каналах зв'язку віртуальної мережі із пороговими значенням відповідних політик збережених у підсистемі PCRF. Даний принцип аналізує такі кількісні показники ефективної роботи системи, як: час затримки заявки службового потоку у віртуальному вузлі та ймовірність втрати запитів у вузлі обслуговування. Вузол обслуговування - це віртуальна машина яка виконує функції керування мережевого вузла [20-22].

Після того, як було виявлено де саме є проблема зниження показників ефективності обслуговування приймаються міри: Якщо проблема у часі передачі між вузлами обслуговування, то рекомендується зробити реконфігурацію системи, а саме змінити розміщення віртуальних вузлів у фізичних вузлах гетерогенної структури датацентрів. Якщо проблема ідентифікована у одному

вузлі обслуговування, тоді рекомендовано збільшити кількість ресурсів обслуговування. Якщо спостерігається зниження показників якості обслуговування у групі вузлів зв'язаних інтерфейсів, наприклад які утворюють єдине ядро мережі EPC, тоді рекомендовано обмежити потік заявок які направляються на обслуговування відповідного ядра. Для цього рекомендовано розрахувати інтенсивність навантаження на групу вузлів. Алгоритм процедури наведений на Рис. 3.1.

Для реалізації принципу динамічного контролю якості потрібна модифікація підсистем системи PCRF. Підсистема «Єдине сховище політик» розширюється, додаються наступні політики відносно показників якості обслуговування потоків керування:

1. Допустимий час затримки заявки службового потоку у віртуальному вузлі.

2. Допустимі втрати запитів у віртуальному вузлі

3. Допустимий час обслуговування запитів у групах віртуальних вузлів які забезпечують заданий сервіс.

4. Допустимі затримки при передачі між вузлами обслуговування Значення допустимих затримок доставки керівного впливу на мережеві вузли.

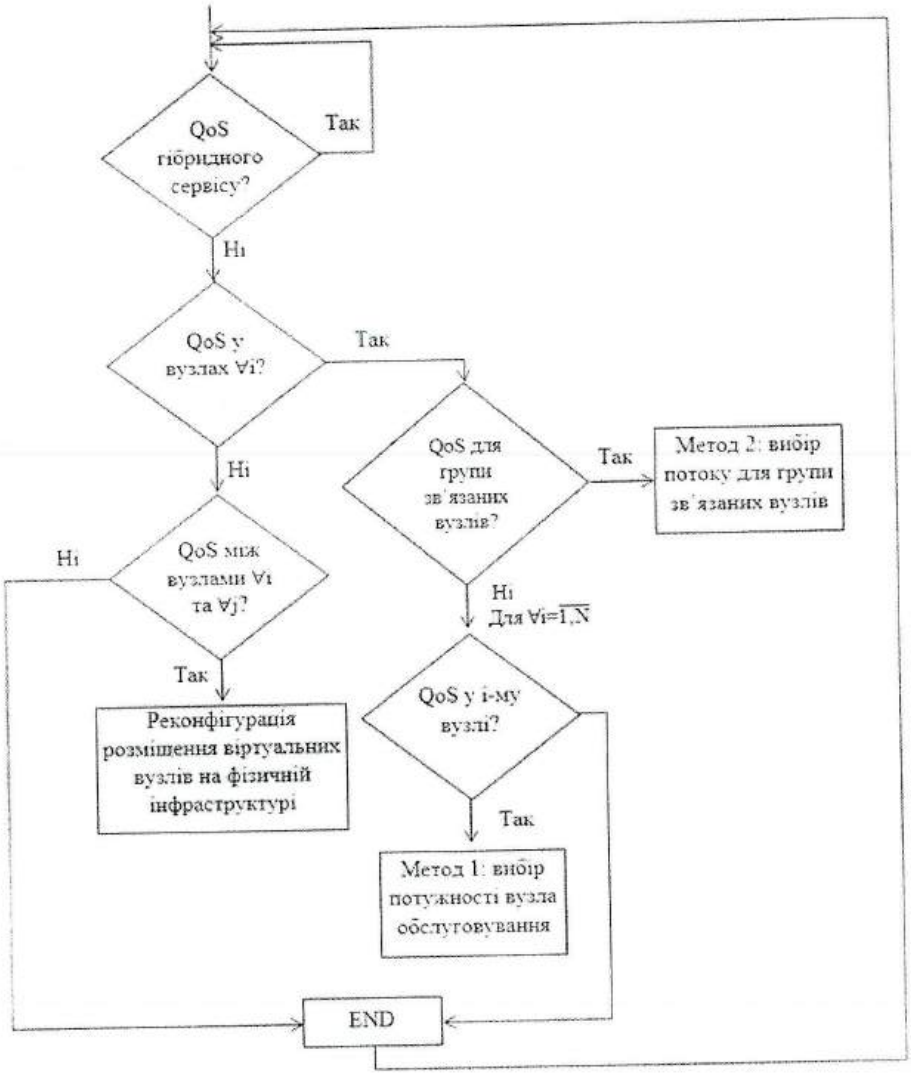


Рис. 3.1. Процедура гарантування заданої якості обслуговування

Розширена підсистема зображена на 3.2.



Рис. 3.2. Модифікація підсистеми PCRF

– Підсистема «Керування політикою» формує групу вимог до виконання набору політик по відношенню до різних потоків керування.

– Підсистема «Сервер політики» виявляє проблему невідповідності поточних показників якості заявленим політикам обслуговування відповідного абонента.

– У підсистемі «Сервер прикладних програм» реалізовані програмні модулі в яких виконуються обчислення відповідно до запропонованих методів. Вихідним даними для методів є статистичні дані отримані від системи моніторингу та дані про політики, які забезпечуються для відповідних абонентів.

– Підсистема «Сховище даних про абонента» доповнюється інформацією про віртуальні вузли, або створюється окрема база даних інформації про статистику функціонування віртуальної мережі обслуговування, де збирається інформація про потоки заявок на обслуговування, статистика відносної залежності інтенсивності обслуговування від ресурсів обслуговування диференційовано для кожного типу запитів [17].

Принцип динамічного контролю якості обслуговування потребує нових процедур: необхідно організувати взаємодію системи керування мобільного зв'язку із системою керування віртуалізованими ресурсами (Рис. 3.3).

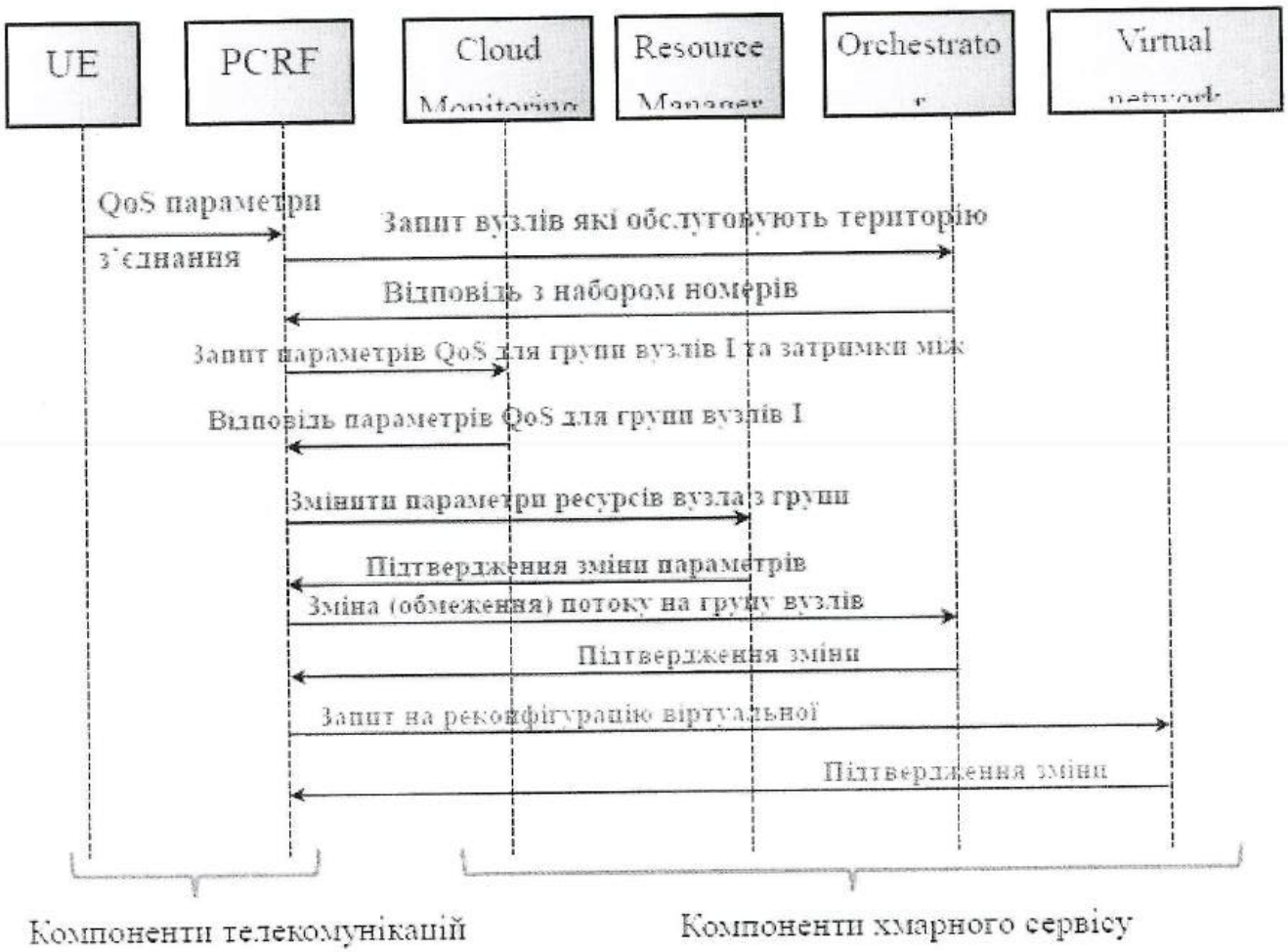


Рис. 3.3. Взаємодія системи керування мобільного зв'язку та системи керування віртуалізованим середовищем

Контроль якості виконання керівних процедур оцінюється на рівні абонентського пристрою:

Абонентський пристрій фіксує час затримки у виконанні службових процедур, а саме час від моменту ініціалізації з'єднання до моменту початку передачі даних, та передає підсистемі PCRF.

PCRF отримує цю інформацію від абонента та аналізує на сервері політик; у підсистемі виконання рішень політики порівнює отримані дані на відповідність обраної політики, яка відповідає абоненту та зберігається у «Сховищі даних про абонента».

Якщо значення параметрів затримок не відповідають політиці, PCRF робить запит до підсистеми «Оркестратор» для визначення групи вузлів *i*, які

обслуговують відповідного абонента.

Підсистема «Оркестратор» надсилає номери вузлів, які обслуговують абонента, розташованого у заданій місцевості. PCRF відправляє підсистемі «Моніторинг хмарних прикладних програм» запит для отримання інформації про час затримки та показники втрат у вузлах *i*, а також інформацію про затримки між вузлами обслуговування. Система моніторингу хмарних прикладних програм збирає інформацію відносно показників затримки та втрат гібридних сервісів, які обслуговуються у вузлах віртуальної мережі. Дані відносно групи вузлів обслуговування і передають у PCRF, де реалізовано принцип динамічного контролю якості обслуговування гібридних сервісів. Відповідно до керівних рішень, підсистема PCRF направляє запити:

- на реконфігурацію віртуальної мережі, до «Менеджера віртуальної мережі»;
- на реконфігурацію ресурсів до «Менеджера ресурсів»;
- на зміну потоків обслуговування до «Оркестратора» потоків по віртуальній мережі.

При реалізації принципу динамічного контролю якості обслуговування задіяно більшість підсистем системи PCRF.

3.2 Інтеграція SDN в мобільних мережах

Інтеграція програмно-визначених мереж SDN — це мережева архітектура, яка відокремлює площину керування від площини даних, що забезпечує централізоване керування мережею та можливість програмування.

Огляд інтеграції SDN у мобільні мережі обіцяє забезпечити значні переваги, такі як покращена гнучкість мережі, масштабованість і економічна ефективність. Відокремлюючи площину керування від площини даних, SDN забезпечує централізоване керування мережею та можливість програмування, що може спростити мережеві операції та зменшити експлуатаційні витрати.

Крім того, SDN дає змогу динамічно конфігурувати мережу та керувати трафіком, що може підвищити продуктивність мережі та досвід користувача. Однак інтеграція SDN у мобільні мережі також створює кілька проблем.

Однією з головних проблем є потреба в новій архітектурі мережі, яка може підтримувати площину керування SDN. Це вимагає значних змін в існуючій інфраструктурі мобільної мережі, що може бути дорогим і трудомістким. Крім того, інтеграція SDN у мобільні мережі вимагає високого рівня координації та співпраці між різними зацікавленими сторонами, включаючи операторів мобільних мереж, постачальників обладнання та розробників програмного забезпечення. Незважаючи на ці проблеми, потреба в інтеграції SDN у мобільні мережі стає все більш важливою. Із зростаючим попитом на послуги мобільного передавання даних і появою нових технологій, таких як 5G, мобільні мережі мають бути більш гнучкими, масштабованими та ефективними, ніж будь-коли раніше. Інтеграція SDN може допомогти операторам мобільних мереж задовольнити ці вимоги, забезпечуючи більш гнучку та програмовану мережеву архітектуру.

Існує кілька підходів до інтеграції SDN у мобільні мережі, кожен із яких має свої переваги та недоліки. Одним із підходів є використання централізованого контролера SDN, який керує всією мобільною мережею, включаючи мережу радіодоступу (RAN) і базову мережу. Цей підхід забезпечує високий ступінь програмованості та гнучкості мережі, але він також вимагає значних змін в інфраструктурі мобільної мережі та може бути складним для впровадження. Інший підхід полягає у використанні розподіленого контролера SDN, який керує певними мережевими доменами, такими як RAN або базова мережа. Цей підхід забезпечує більш локалізований контроль і може бути легшим у реалізації, ніж централізований контролер. Однак це також може призвести до більш складної архітектури мережі та може вимагати додаткової координації між різними контролерами SDN. Для інтеграції SDN у мобільні мережі необхідно виконати кілька технічних вимог. Вони включають підтримку відкритих стандартів та інтерфейсів, можливість динамічно керувати

мережевими ресурсами та здатність обробляти великі обсяги мережевого трафіку. Крім того, інтеграція SDN вимагає високого рівня безпеки та надійності мережі, оскільки будь-які збої в площині керування SDN можуть мати значний вплив на продуктивність мережі та взаємодію з користувачем.

Інтеграція SDN у мобільні мережі може мати значний вплив на продуктивність мережі, її ефективність і фінансові наслідки.

Методи конвергенції стосуються методів, які використовуються для поєднання двох або більше різних технологій або систем в одне інтегроване рішення. У випадку програмно-конфігурованих мереж і технології 5G досліджується кілька методів конвергенції, включаючи нарізку мережі, віртуалізацію та периферійні обчислення. Розрізання мережі дозволяє створювати кілька віртуальних мереж в одній фізичній мережевій інфраструктурі, кожну з яких адаптовано до конкретних випадків використання. Віртуалізація дозволяє створювати віртуальні мережеві функції (VNF), які можна розгортати та керувати ними незалежно від основного обладнання. Граничні обчислення передбачають розгортання обчислювальних ресурсів ближче до кінцевого користувача, зменшуючи затримку та покращуючи продуктивність. Ці методи конвергенції пропонують кілька переваг, включаючи підвищену гнучкість, масштабованість і ефективність.

Є кілька робіт, які описують інтеграцію SDN в мобільних мережах [18, 20-22]. Вони пропонують додавати SDN-агенти в елементи мобільної мережі. SoftRAN [5] пропонує централізовану архітектуру в якості альтернативи розподіленому рівню керування, який реалізується в даний час в LTE мережах. Це абстрагує всі базові станції, розгорнуті в географічній зоні в якості великої віртуальної базової станції. Всі фізичні базові станції виглядають як радіоелементи з мінімальною логікою керування. Ці радіо елементи потім керуються централізованим елементом. CellSDN [6] надає детальну класифікацію пакетів комутаторам доступу, яка може бути реалізована в програмному забезпеченні (наприклад, з використанням відкритого VSWITCH). Інші роботи [22-25] визначають, що кожна базова станція має комутатор доступу, який

виконує детальну класифікацію пакетів на шляху від мобільного терміналу. Комутатори доступу можуть бути програмними (наприклад, Open vSwitch). Сервер також може мати локального агента, який кешує політики обслуговування для мобільних терміналів, щоб звести до мінімуму взаємодію з центральним контролером.

Інша частина ядра мережі складається з комутаторів, в тому числі кількох шлюзів, підключених до Інтернету. Ці основні комутатори виконують багатовимірну класифікацію пакетів на високій швидкості для кількох тисяч або десятків тисяч правил.

В даний час існують лише кілька поглиблених наукових доповідей, що стосуються мобільних мережевих архітектур, які поєднують в собі поняття хмарних обчислень, SDN та NFV. Перші архітектурні пропозиції - особливо в контексті хмарних-RAN - включають відображення мережевих функцій, необхідних для інтеграції мобільних мереж з технологією SDN. Це лише функції контролю мобільного зв'язку, тобто MME, HSS, PCRF і рівня керування S/P-GW. Додаткові функції включають в себе транспорт, балансування навантаження, безпеку, політики, білінг, моніторинг, QoE або оптимізацію ресурсів. Ці функції працюють в мобільній Cloud мережі як SDN-прикладні програмні компоненти. При такому підході, призначений для користувача рівень складається тільки із стратегічно розташованих SDN сумісних комутаторів і звичайних комутаторів. SDN комутатори замінять повністю або частково поточний транспорт мобільної мережі [24-27]. Це консолідована архітектура показана на Рис. 3.4.

Необхідні елементи мережі EPC працюють в хмарі. Затримка може вплинути на розташування розгортання деяких обчислювальних вузлів, що працюють віртуально. Деякі стратегічні функції можуть бути розміщені близько до важливих вузлів, створюючи таким чином децентралізовану хмару.

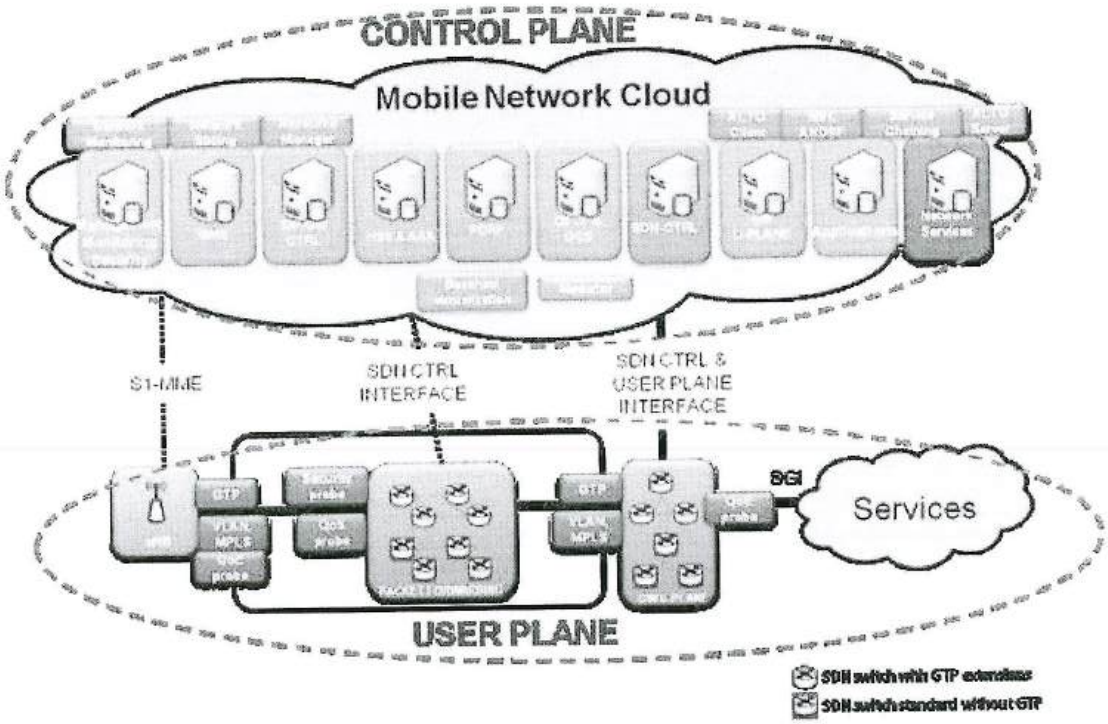


Рис. 3.4. Консолідована архітектура мобільної мережі

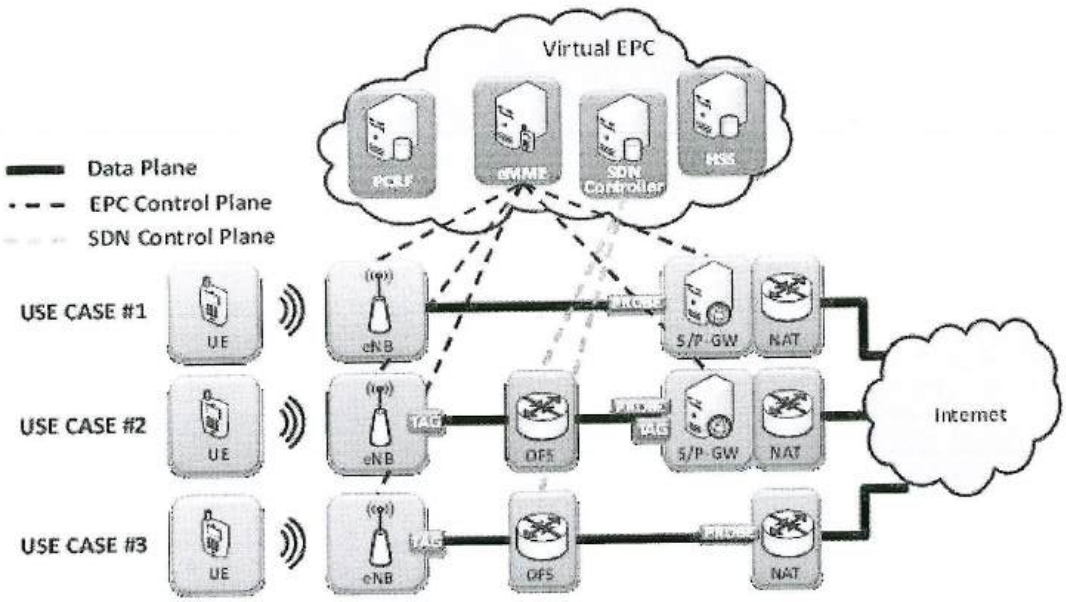


Рис. 3.5. Сценарій міграції з використанням OpenFlow

Рис. 3.5 являє собою 3-крововий сценарій міграції з використанням OpenFlow як протоколу зв'язку з SDN. Перший випадок використання (тобто UC1) відповідає традиційній LTE архітектурі, зі старими вузлами. Другий випадок використання (тобто UC2) вводить технологію SDN для керування 2-м рівнем маршрутизації на ядрі мобільної мережі, зберігаючи старі вузли. Цей

сценарій є гібридним підходом. І, нарешті, третій випадок використання (тобто UC3) зображує повністю сумісну мережу SDN.

Висновки

В третьому розділі досліджувались процедури гарантування якості обслуговування, описувався принцип динамічного контролю. Було виявлено ряд проблем та описані методи їх подолання. Одна з них це: зниження показників ефективності обслуговування, яка вирішується одним з методів:

1) реконфігурацією системи;

2) обмеженням потоку заявок які направляються на обслуговування відповідного ядра.

Також в цьому розділі була описана інтеграція SDN в мобільних мережах.

ВИСНОВКИ

В ході дослідження були вивчені і описані основні поняття і принципи 5G мереж. Концепція мереж п'ятого покоління передбачає розгортання надщільних мереж з високошвидкісним доступом поверх вже існуючих мереж, які будуть забезпечувати загальне покриття.

В першому розділі пройшло ознайомлення з такими технологіями як 5G, SDN, архітектурою та принципами SDN. Були описані Вимоги до якості та сервіси які надаються (SaaS, VNFaaSта інші). Проаналізувавши технології 5G було виявлено певні недоліки, була проведена оцінка та ознайомлення з рішеннями що до їх вирішення. Розроблені рекомендації що до розгортання мереж 5-го покоління та особливостей забезпечення якості обслуговування.

У другому розділі проаналізовано та описано механізм LTE, також проведено ознайомлення з перевагами та недоліками LTE. При аналізі вже відомих механізмів також пройшло ознайомлення з архітектурою мережі SAE, EPC/LTE. Були досліджені наступні протоколи гарантії якості в мережах доступу: NBAP (Node B Application Part), QoS протоколи. Ми підходимо до висновку про те що поточні мережі 4G не витримують вимог, висунутих новими сценаріями застосування на даний час, тому технологія 5G на разі дуже актуальна.

В третьому розділі досліджувались процедури гарантування якості обслуговування, описувався принцип динамічного контролю. Було виявлено ряд проблем та описані методи їх подолання. Одна з них це: зниження показників ефективності обслуговування, яка вирішується одним з методів:

1) реконфігурацією системи;

2) обмеженням потоку заявок які направляються на обслуговування відповідного ядра.

Мережі, налаштовані програмним забезпеченням, і технологією 5G відкривають захоплюючі можливості для майбутнього мереж. Використовуючи переваги обох технологій і використовуючи методи конвергенції для їх інтеграції, мережеві оператори можуть створювати дуже гнучкі, масштабовані та ефективні

рішення, які відповідають вимогам сучасних програм і послуг. Оскільки ці технології продовжують розвиватися, цілком імовірно, що ми побачимо ще більше інноваційних рішень, які ще більше розширять можливості наших мереж і сервісів, які вони підтримують.

Традиційні мобільні мережі характеризуються складною і негнучкою ієрархічною архітектурою. Інтеграція SDN у мобільні мережі пропонує кілька переваг, зокрема покращену продуктивність мережі, підвищену гнучкість мережі та зменшення її складності. SDN також може включати нові послуги та програми, які раніше були неможливі в традиційних мобільних мережах. Існують також потенційні проблеми та обмеження щодо інтеграції SDN у мобільні мережі, включаючи потребу в нових мережевих архітектурах і потенційну можливість збільшення складності мережі. Крім того, можуть виникнути проблеми з регулюванням і безпекою, які необхідно вирішити, перш ніж SDN можна буде повністю інтегрувати в мобільні мережі.

Інтеграція SDN у мобільні мережі пропонує кілька переваг, включаючи покращену продуктивність мережі, підвищену гнучкість мережі та зменшення її складності. Потенційний вплив SDN на розвиток мобільних мереж є значним, а поточні дослідження та розробки SDN для мобільних мереж є перспективними. Однак існують також потенційні проблеми та обмеження щодо інтеграції SDN у мобільні мережі, які необхідно вирішити. Загалом SDN має потенціал кардинально змінити спосіб взаємодії з нашими мобільними пристроями та мережами, які їх підтримують.

ПЕРЕЛІК ПОСИЛАНЬ

1. 3GPP (2022). "5G". [Електронний ресурс] – Режим доступу: https://www.3gpp.org/5G. (дата звернення 19.10.2023)

2. 3GPP (2021). "LTE (Long-Term Evolution) technology". [Електронний ресурс] – Режим доступу: https://www.3gpp.org/LTE. (дата звернення 19.10.2023)

3. ITU (2015). "Next Generation Networks (NGN)". [Електронний ресурс] – Режим доступу: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/ngn/201503/Pages/default.aspx. (дата звернення 19.10.2023)

4. ITU-T (2007). "Y.1540: Internet protocol data communication service - IP packet transfer and availability performance parameters". [Електронний ресурс] – Режим доступу: https://www.itu.int/rec/T-REC-Y.1540/en. (дата звернення 21.10.2023)

5. ITU-T (2015). "Y.1541: Network performance objectives for IP-based services". [Електронний ресурс] – Режим доступу: https://www.itu.int/rec/T-REC-Y.1541/en. (дата звернення 22.10.2023)

6. Open Networking Foundation (2022). "Software-Defined Networking (SDN)". [Електронний ресурс] – Режим доступу: https://www.opennetworking.org/sdn-resources/sdn-definition/.(дата звернення 25.10.2023)

7. Andrews, J.G., Ghosh, A., & Muhamed, R. (2014). Fundamentals of LTE. Prentice Hall.

8. Chen, H., Zhang, Y., & Xiong, N. (2013). "A Survey of QoS Management in Cloud Computing: Challenges and Opportunities". IEEE Network, 27(5), 38-43. doi: 10.1109/MNET.2013.6642655

9. Hu, Y.C., Patel, M., Sabella, D., Sprecher, N., & Young, V. (2014). "Mobile Edge Computing—A Key Technology towards 5G". ETSI White Paper, 11(11), 1-16.

10. Kaur, S., Singh, P., & Ahuja, R. (2019). "A Study on Quality of Service in SDN: Review and Research Directions". Computer Networks, 159, 1-26. doi: 10.1016/j.comnet.2019.04.008

11. Liu, H., & Li, X. (2016). "A Survey of 5G Network: Architecture and

Emerging Technologies". IEEE Access, 4, 1142-1153. doi: 10.1109/ACCESS.2016.2523026

12. National Instruments (2016). "5G Wireless: High-Frequency Design and Test - 5G New Radio". [Електронний ресурс] – Режим доступу: https://www.ni.com/en-us/innovations/white-papers/19/5g-wireless-high-frequency-design-and-test.html. (дата звернення 30.10.2023)

13. Network World (2022). "What is 5G?". [Електронний ресурс] – Режим доступу: https://www.networkworld.com/article/3203489/what-is-5g-how-is-it-better-than-4g-and-what-will-it-mean-for-businesses.html. (дата звернення 30.10.2023)

14. Niyato, D., Wang, P., & Hong, X. (2018). "Machine-to-Machine Communications for Home Energy Management System in Smart Grid". IEEE Wireless Communications, 20(1), 108-115. doi: 10.1109/MWC.2016.6476849

15. Open Networking Foundation (2022). "SDN Use Cases". [Електронний ресурс] – Режим доступу: https://www.opennetworking.org/sdn-resources/sdn-use-cases/. (дата звернення 05.11.2023)

16. R. Jain, "The Art of Computer Systems Performance Analysis Techniques for Experimental Design, Measurement, Simulation, and Modeling," New York: Wiley-Interscience, 1991.

17. F. Wang, Y. Zhang, N. Zhang, X. Zhou, Q. Wu and Z. Zhang, "A Deep Reinforcement Learning Based Resource Allocation Scheme for 5G Network," in IEEE Transactions on Vehicular Technology, vol. 70, no. 3, pp. 2223-2235, March 2021. doi: 10.1109/TVT.2021.3051914 (https://ieeexplore.ieee.org/document/9318339)

18. L. Chen, J. Xu, D. Zhang and Y. Sun, "Achieving QoS-Aware Service Function Chain Provisioning Through SDN and NFV," in IEEE Transactions on Network and Service Management, vol. 17, no. 3, pp. 1429-1443, Sept. 2020. doi: 10.1109/TNSM.2020.3014656 (https://ieeexplore.ieee.org/document/9174563)

19. S. S. Ahmed, H. Zhang, M. Chen, M. Alazab and A. Hussain, "A Secure, Intelligent, and Scalable 5G Network: Challenges and Opportunities," in IEEE Network, vol. 35, no. 5, pp. 204-211, Sept.-Oct. 2021. doi: 10.1109/MNET.011.2000378 (https://ieeexplore.ieee.org/document/9484568) (дата звернення 11.11.2023)

20. T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta and D. Sabella, "On Multi-access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration," in IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1657-1681, thirdquarter 2017. doi: 10.1109/COMST.2017.2699318 (https://ieeexplore.ieee.org/document/7974999) (дата звернення 12.11.2023)

21. S. Suyama, J. Shen, H. Suzuki, K. Fukawa and Y. Okumura, "Evaluation of 30 Gbps super high bit rate mobile communications using channel data in 11 GHz band 24x24 MIMO experiment", IEEE ICC2017, June 2017.

22. R. Venkatesha Prasad, F. Granelli, G. Tuna and M. Lalam, "SDN and NFV Integration in Generalized Mobile Network Architecture," in IEEE Network, vol. 32, no. 2, pp. 140-145, March-April 2018. doi: 10.1109/MNET.2018.1700222 (https://ieeexplore.ieee.org/document/8323151) (дата звернення 12.11.2023)

23. X. Zhang, Z. Zhang, J. Wu and Y. Xie, "A Network Slicing-Based Resource Allocation Scheme for 5G Wireless Networks," in IEEE Transactions on Network and Service Management, vol. 17, no. 1, pp. 407-420, March 2020. doi: 10.1109/TNSM.2019.2962141 (https://ieeexplore.ieee.org/document/8826026) (дата звернення 15.11.2023)

24. "Sharing and compatibility studies of the fixed-satellite service and IMT operating in the frequency band 3 600-3 800 MHz", Document 5D/1348, 2022.

25. Y. Sun, L. Zhong, D. Zhou and D. Li, "Coexistence of Airborne radar and IMT systems in the 3GHz Band", 2022 International Wireless Communications and Mobile Computing (IWCMC), pp. 196-200, 2022.

26. L. Zhong, D. Zhou, R. Liu, X. Wang and X. Meng, "The Feasibility of Coexistence between IMT-2020 and Inter-Satellite Service in 26GHz band", 2020 International Wireless Communications and Mobile Computing (IWCMC), pp. 1006-1011, 2020.

27. Y. Takahashi, T. Okuyama, K. Muraoka, S. Satoshi, J. Mashino and Y. Okumura, "Field trial of 28 GHz-band 5G downlink massive MIMO employing beam tracking in railway environment", IEICE Trans. Commun., vol. E102-B, no. 8, pp. 1411-1417, Aug. 2019.

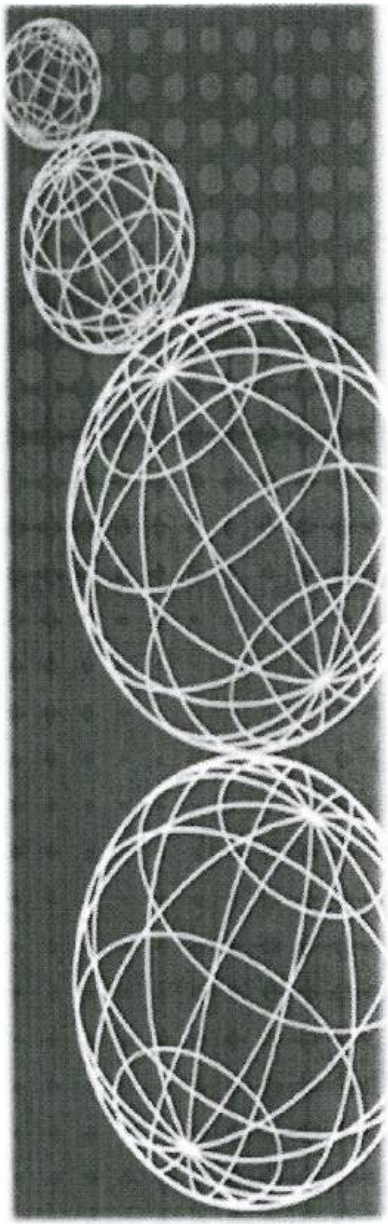
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Презентація по магістерській роботі на тему:

Методи конвергенції програмно-конфігурованих мереж та технологій п'ятого покоління

Виконав: студент
Медведєв Владислав Олександрович

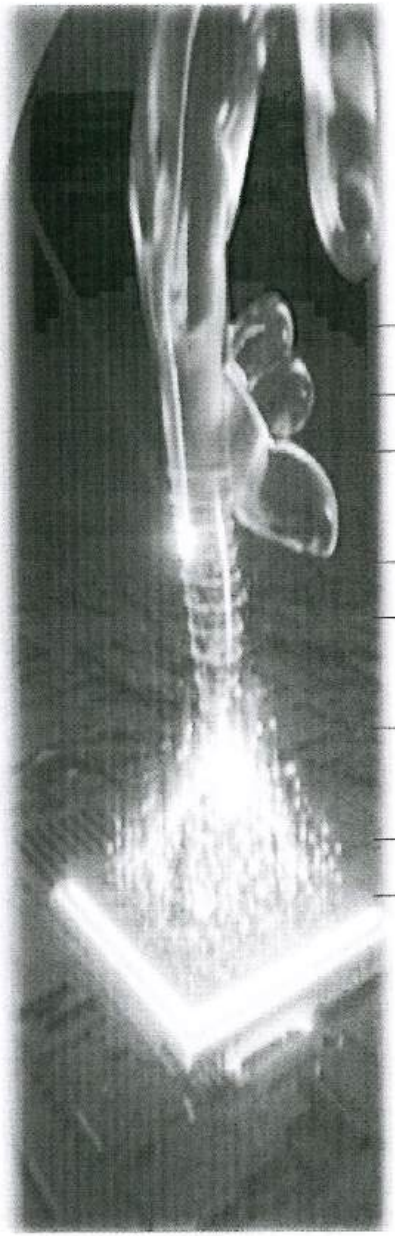


МЕТА РОБОТИ

ОБ'ЄКТ дослідження:
мережі мобільного зв'язку п'ятого покоління.

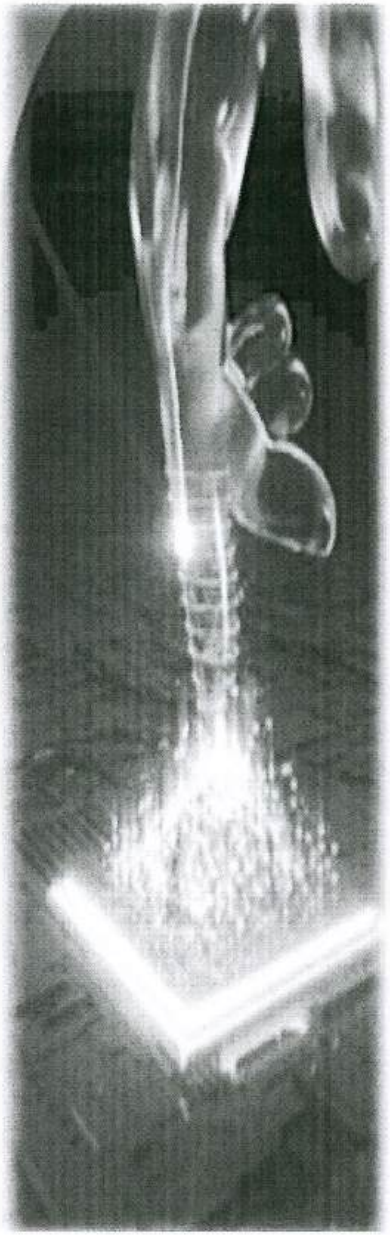
ПРЕДМЕТ дослідження:
конвергенція програмно-конфігурованих мереж та технологій п'ятого покоління.

МЕТА РОБОТИ:
дослідження конвергенції програмно-конфігурованих мереж та технологій п'ятого покоління.

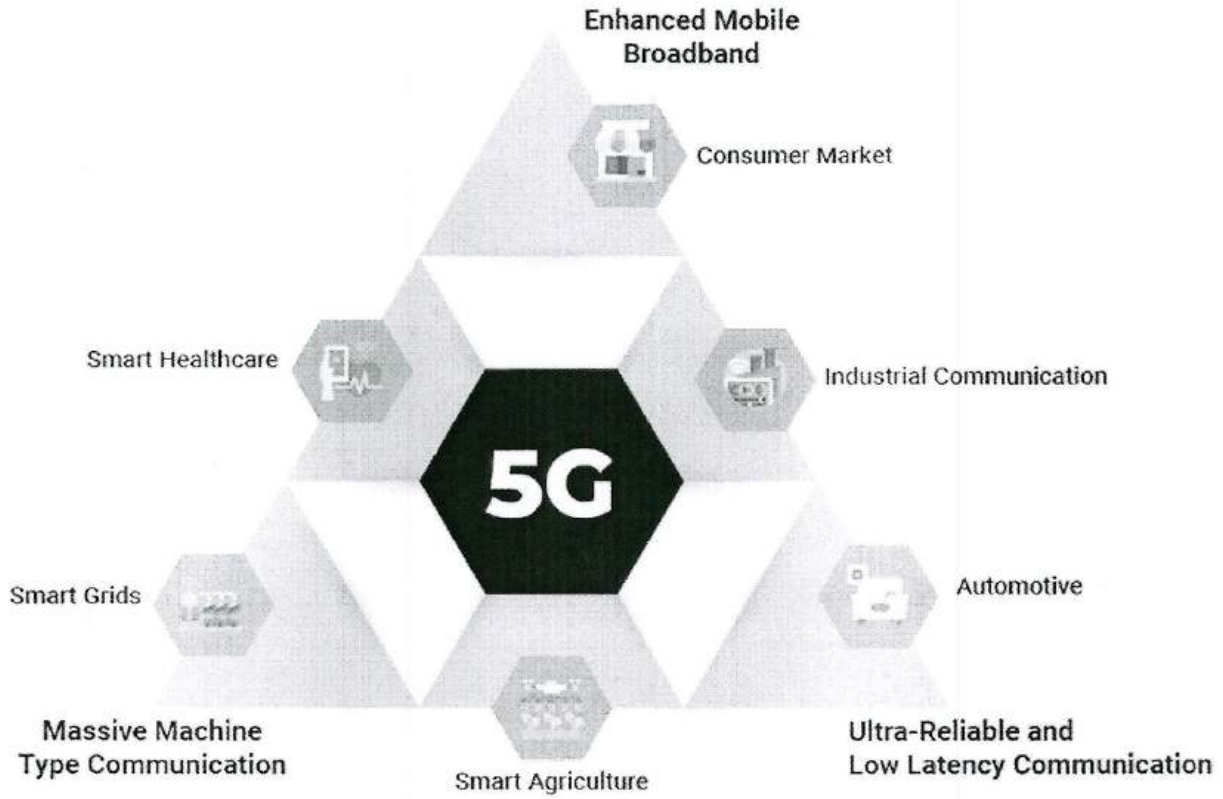


Ключові вимоги до 5G в порівнянні з 4G

Параметри	4G	5G
Пікова швидкість завантаження	1 Гбіт/с	20 Гбіт/с
Швидкість завантаження для користувачів	10 Мбіт/с	100 Мбіт/с
Затримка	10 мс	1-2 мс
Максимальна швидкість переміщення без втрати сигналу	350 км/год	500 км/год
Щільність підключення	100 тис. пристроїв/кв.км	1 млн. пристроїв/кв.км
Трафік на одиницю площі	0.1 Мбіт/с/кв.м	10 Мбіт/с/кв.м

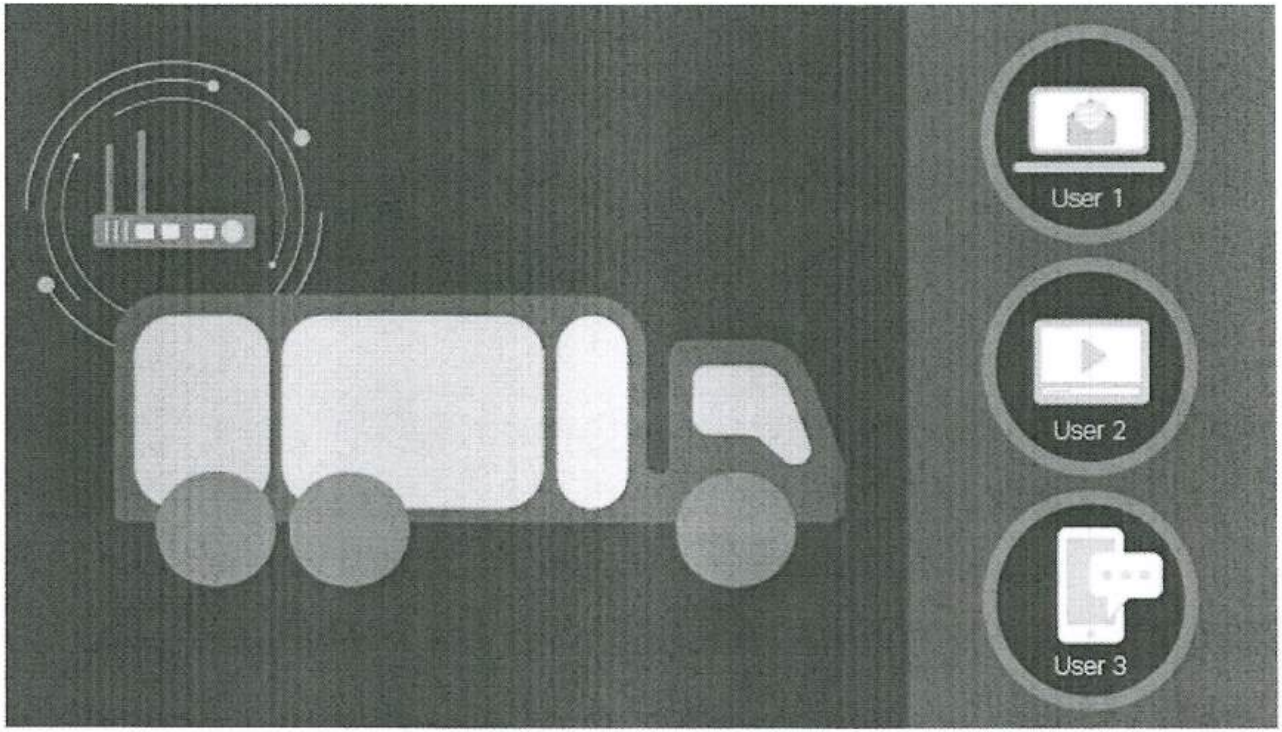


Особливості технології 5G



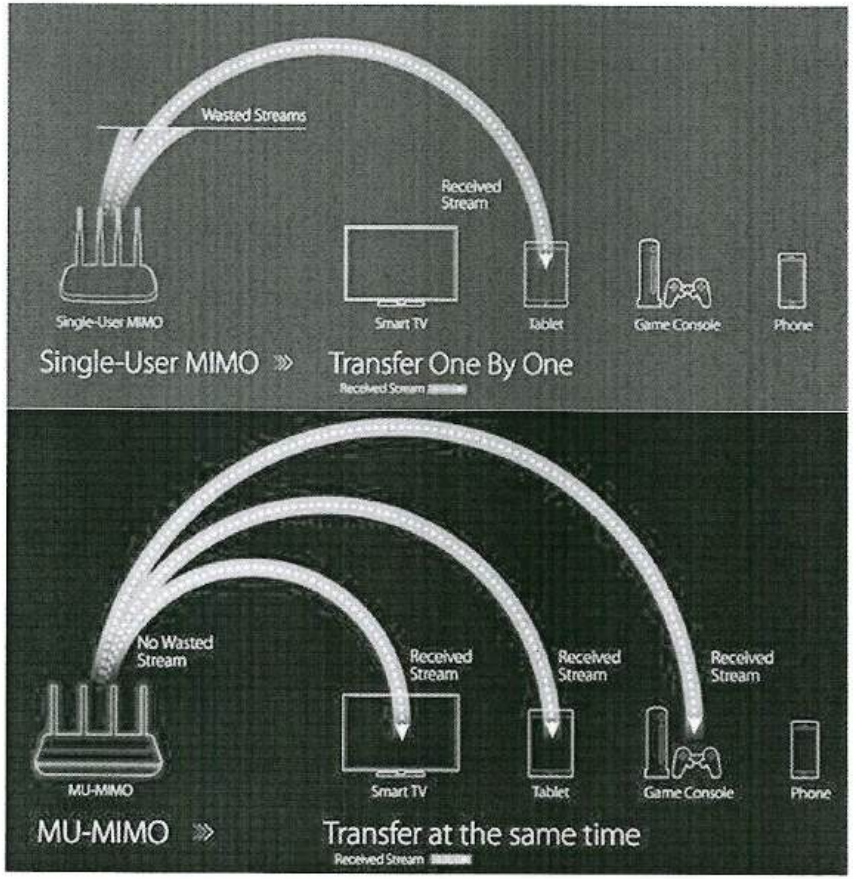
5 Generation

Множинний доступ з ортогональним частотним поділом



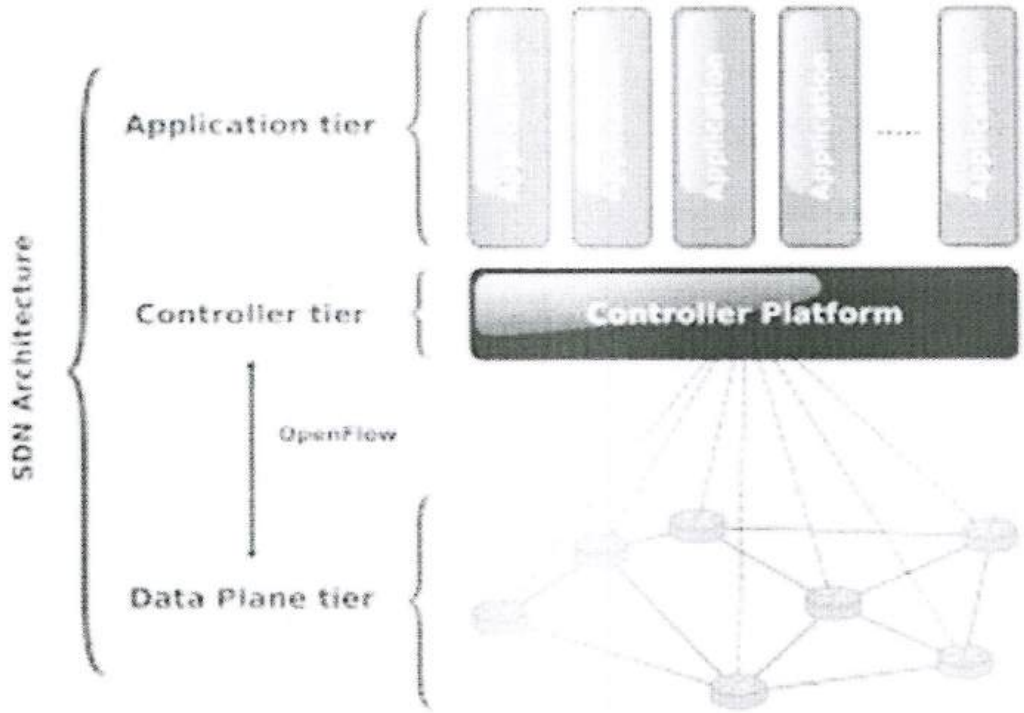
5G

Масиви антен MIMO (Multiple-Input Multiple-Output)



5G

Архітектура SDN мереж



SDN дає велику кількість плюсів:

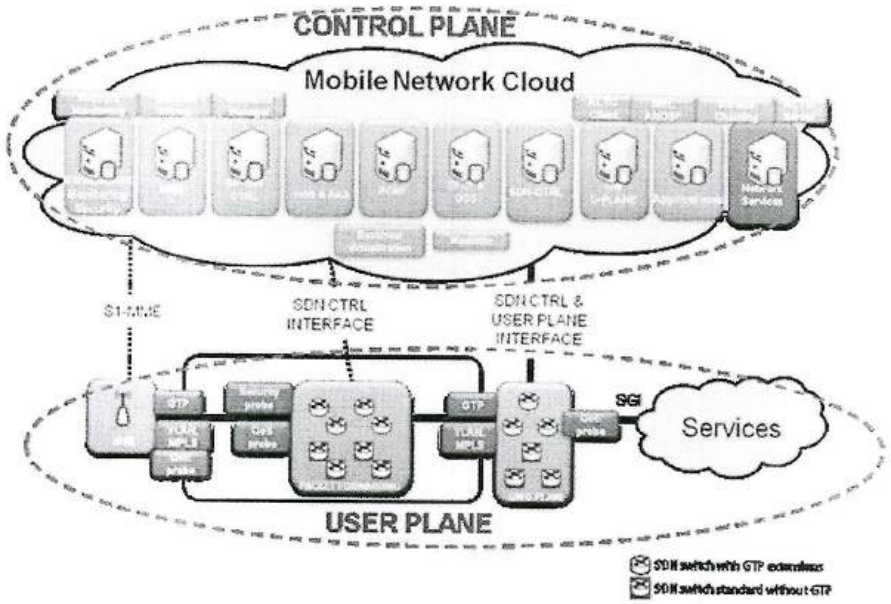
Можливість бачити топологію всієї мережі;

Можливість зміни всієї мережі в цілому, а не окремих одиниць обладнання;

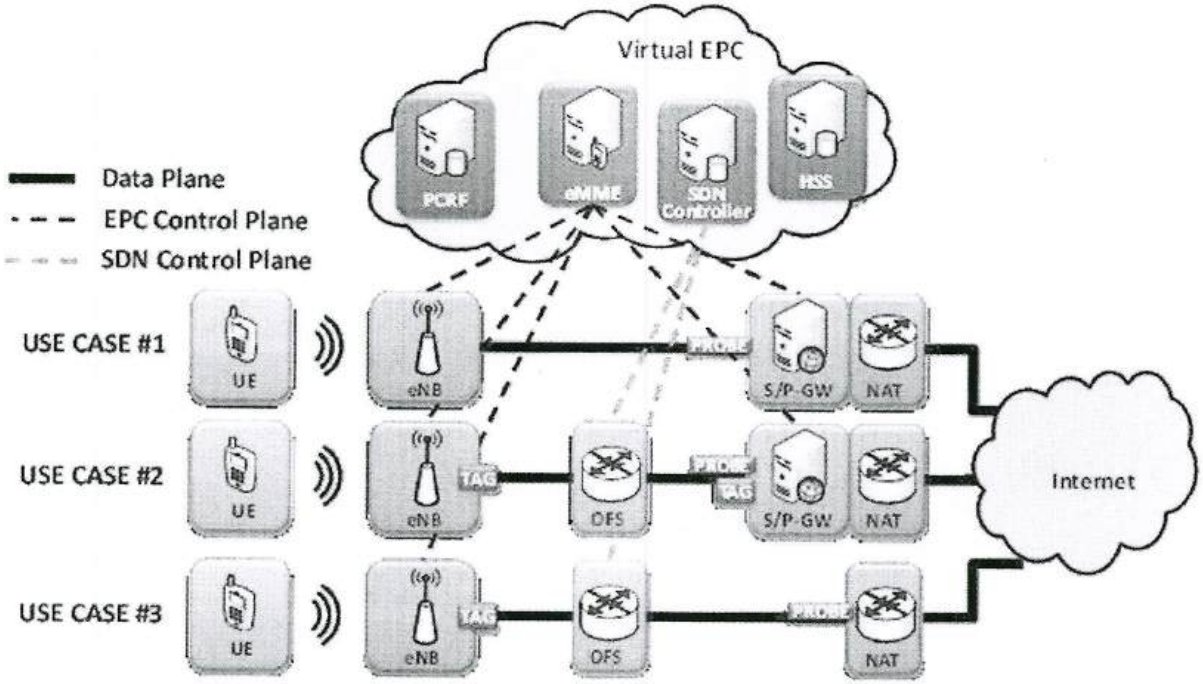
Можливість робити незалежне оновлення обладнання в мережі;

Можливість контролювати всю мережу.

Інтеграція SDN в мобільних мережах

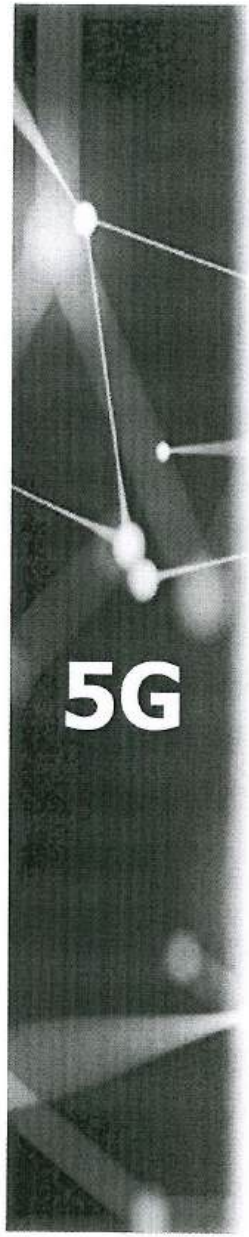


Аріхітектура що створена на обладання (1G-4G)



Програмна 5G архітектура на основі хмарних технологій та SDN

Програмна 5G архітектура являє собою 3-кроковий сценарій міграції з використанням OpenFlow як протоколу зв'язку з SDN. Перший кейс відповідає традиційній LTE архітектурі, зі старими вузлами. Другий кейс вводить технологію SDN для керування 2-м рівнем маршрутизації на ядрі мобільної мережі, зберігаючи старі вузли. Цей сценарій є гібридним підходом. І, нарешті, третій кейс зображує повністю сумісну мережу SDN.



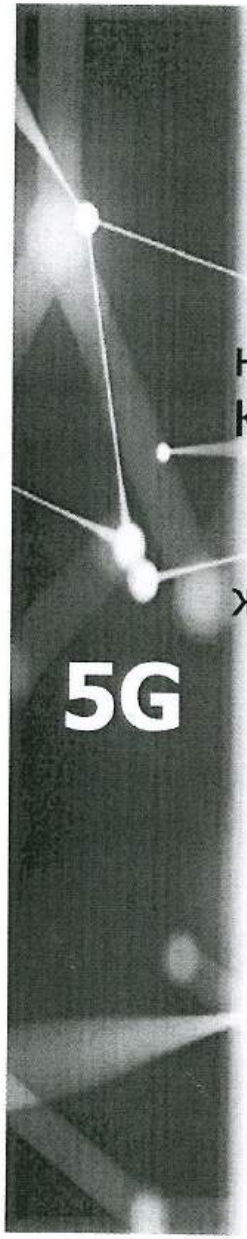
ВИСНОВКИ

В ході дослідження були вивчені і описані основні поняття і принципи 5G мереж. Концепція мереж п'ятого покоління передбачає розгортання надщільних мереж з високошвидкісним доступом поверх вже існуючих мереж, які будуть забезпечувати загальне покриття.

В першому розділі пройшло ознайомлення з такими технологіями як 5G, SDN, архітектурою та принципами SDN. Розроблені рекомендації що до розгортання мереж 5-го покоління та особливостей забезпечення якості обслуговування.

У другому розділі проаналізовано та описано механізм LTE, також проведено ознайомлення з перевагами та недоліками LTE. Зроблено висновок про те що поточні мережі 4G не витримують вимог, висунутих новими сценаріями застосування на даний час, тому технологія 5G на разі дуже актуальна.

В третьому розділі описана інтеграція SDN в мобільних мережах. Інтеграція SDN у мобільні мережі пропонує кілька переваг, включаючи покращену продуктивність мережі, підвищену гнучкість мережі та зменшення її складності.



Апробація результатів магістерської роботи

Основні результати магістерської роботи доповідалися на Всеукраїнській науково-практичній конференції «Telecommunication: problems and innovation», Київ: ДУІКТ, 20 грудня 2023 р.

Основні наукові результати магістерської роботи опубліковано в науковому журналі "Наукові записки ДУІКТ, – 2023, – №2".

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Владислав МЕДВЕДЄВ

Назва: Методи конвергенції програмно-конфігурованих мереж та технологій п'ятого покоління

Координатор: Віталій СТРЕЛЬНІКОВ

Підрозділ: ННІТ

Коефіцієнт подібності 1 :5.5

Коефіцієнт подібності 2 :1.1

Тривога: 1

Після аналізу Звіту подібності констатую наступне:

☑ виявлені в роботі запозичення є сумлінними і не мають ознак плагіату. Тому робота визнається самостійною і допускається до захисту;

☐ виявлені в роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і самостійності її автора. Роботу направити на доопрацювання;

☐ виявлені в роботі запозичення є недобросовісними і мають ознаки плагіату або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень. У зв'язку з чим, робота не допускається до захисту.

....

Дата *Підпис Наукового керівника*