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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «МЕТОДИ УПРАВЛІННЯ ТРАФІКОМ У SDN-МЕРЕЖАХ»

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

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

_____ Павло МАКЕЛЬСЬКИЙ
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Виконав: здобувач вищої освіти гр. ТСДМ-62
Павло МАКЕЛЬСЬКИЙ
Ім'я, ПРІЗВИЩЕ

Керівник: Юрій МЕЛЬНИК
д.т.н., професор *Ім'я, ПРІЗВИЩЕ*

Рецензент: _____
Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Телекомунікацій

Кафедра ___Телекомунікаційних систем та мереж_____
Ступінь вищої освіти __магістр_____
Спеціальність ___172 Електронні комунікації та радіотехніка _____
Освітньо-професійна програма _____Телекомунікаційні системи та мережі_____

ЗАТВЕРДЖУЮ
Завідувач кафедри __ТСМ_____
_____ Віктор ЗАЇКА
«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Макельському Павлу Валерійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Методи управління трафіком у SDN-мережах
керівник кваліфікаційної роботи Юрій МЕЛЬНИК, д.т.н., професор
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від « » 2025 р. №

2. Строк подання кваліфікаційної роботи «___» _____ 2025 р.

3. Вихідні дані до кваліфікаційної роботи:
1. SDN-мережі.
2. Управління трафіком.
3. Контролер керування трафіку.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Поняття SDN мереж.
2. Контроль трафіку в SDN.
3. Контролер керування трафіку для T-SDN.
4. Створення керованого SDN простору.

5. Перелік ілюстративного матеріалу: ___презентація на____слайдах_____

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

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір та аналіз науково-технічної літератури	15.10.2025	Викон.
2	Розробка першого розділу	23.10.2025	Викон.
3	Розробка другого розділу	03.11.2025	Викон.
4	Розробка третього розділу	13.11.2025	Викон.
5	Розробка четвертого розділу	23.11.2025	Викон.
6	Висновки, вступ, реферат	03.12.2025	Викон.
7	Розробка презентації	13.12.2025	Викон.

Здобувач вищої освіти _____ Павло МАКЕЛЬСЬКИЙ
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Юрій МЕЛЬНИК
(підпис) *(Ім'я ПРІЗВИЩЕ)*

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

Направляється здобувач Макельський П.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)
на тему: «Методи управління трафіком у SDN-мережах»

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

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

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача Макельського Павла Валерійовича на оцінку «відмінно» та присвоїти йому кваліфікацію магістр з електронних комунікацій та радіотехніки.

Керівник кваліфікаційної роботи _____ Юрій МЕЛЬНИК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Макельський П.В. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри телекомунікаційних систем та мереж _____ Віктор ЗАЇКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу
на здобуття освітнього ступеня магістра

здобувача вищої освіти Макельського Павла Валерійовича
(прізвище, ім'я, по батькові)
на тему «Методи управління трафіком у SDN-мережах»

Актуальність.
Традиційні методи конфігурації мережевого обладнання вже не здатні забезпечити необхідну гнучкість, масштабованість та ефективність.
Технологія Software Defined Networking (SDN) вирішує ці проблеми, відокремлюючи контрольну та транспортну площини, що дає змогу централізовано управляти трафіком і швидко адаптувати мережу до змін навантаження. Тому дослідження методів управління трафіком у SDN безпосередньо відповідає потребам сучасної галузі телекомунікацій та є важливим для розвитку дата-центрів і операторських мереж.

Позитивні сторони.
1. У роботі детально розглянуто архітектуру SDN, принципи роботи контролера, механізми OpenFlow, віртуалізацію мережевих функцій (NFV), QoS, енергоефективність.
2. Особлива увага приділялася методам оптимізації пропускної здатності та енергозбереження.

Недоліки.
1. У роботі недостатньо розглянуто питання захисту контролера та уразливостей SDN-інфраструктури.
2. У роботі немає порівняльного аналізу методів управління трафіком.

Відзначені зауваження не впливають на загальну позитивну оцінку магістерської кваліфікаційної роботи

Висновок: *кваліфікаційна робота на здобуття ступеня магістра заслуговує оцінку "відмінно", а здобувач Макельський Павло Валерійович заслуговує присвоєння кваліфікації: магістр з електронних комунікацій та радіотехніки.*

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

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 84 стор., 22 рис., 23 джерела.

Мета роботи – аналіз, систематизація та вдосконалення методів управління трафіком у програмно-визначених мережах (SDN) з метою підвищення ефективності використання мережевих ресурсів, забезпечення стабільної якості обслуговування (QoS) та зниження енергоспоживання у центрах обробки даних.

Об’єкт дослідження – процеси управління трафіком у телекомунікаційних мережах із використанням архітектури програмно-визначених мереж (SDN), зокрема у середовищах центрів обробки даних (ЦОД) і хмарних інфраструктурах.

Предмет дослідження – методи, алгоритми та технологічні засоби оптимізації, моніторингу та балансування трафіку в SDN-мережах, а також механізми їх інтеграції з віртуалізацією мережевих функцій (NFV) і системами забезпечення якості обслуговування.

Короткий зміст роботи: у кваліфікаційній роботі досліджено принципи функціонування програмно-визначених мереж (SDN) та методи управління трафіком у таких системах. Показано, що традиційні підходи до конфігурації мережевого обладнання не забезпечують гнучкості й масштабованості сучасних дата-центрів. Визначено переваги SDN — централізоване управління потоками, автоматизація, інтеграція з NFV і підтримка QoS. Розглянуто проблеми оптимізації маршрутів, масштабування та енергоспоживання, запропоновано шляхи їх вирішення. Доведено, що SDN формує основу телекомунікаційних мереж нового покоління, здатних забезпечити високу ефективність, надійність і якість обслуговування.

КЛЮЧОВІ СЛОВА: SDN, УПРАВЛІННЯ ТРАФІКОМ, ПРОГРАМНО-ВИЗНАЧЕНІ МЕРЕЖІ, NFV, QOS, ДАТА-ЦЕНТР, ВІРТУАЛІЗАЦІЯ, ОПТИМІЗАЦІЯ, ЕНЕРГОЗБЕРЕЖЕННЯ, ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ

ABSTRACT

Text part of the master's qualification work: 84 pages, 22 figures, 23 sources.

The purpose of the work is to analyze, systematize and improve traffic management methods in software-defined networks (SDN) in order to increase the efficiency of network resource use, ensure stable quality of service (QoS) and reduce energy consumption in data centers.

Object of the study is traffic management processes in telecommunication networks using the software-defined network (SDN) architecture, in particular in data center environments (DCP) and cloud infrastructures.

Subject of the study is methods, algorithms and technological means of optimizing, monitoring and balancing traffic in SDN networks, as well as mechanisms for their integration with network function virtualization (NFV) and quality of service systems.

Summary of the work: the qualification work investigates the principles of operation of software-defined networks (SDN) and methods of traffic management in such systems. It is shown that traditional approaches to network equipment configuration do not provide flexibility and scalability of modern data centers. The advantages of SDN are determined - centralized flow management, automation, integration with NFV and QoS support. The problems of route optimization, scaling and energy consumption are considered, and ways to solve them are proposed. It is proved that SDN forms the basis of new generation telecommunication networks, capable of providing high efficiency, reliability and quality of service.

KEYWORDS: SDN, TRAFFIC MANAGEMENT, SOFTWARE-DEFINED NETWORKS, NFV, QOS, DATA CENTER, VIRTUALIZATION, OPTIMIZATION, ENERGY SAVING, TELECOMMUNICATION NETWORKS

ЗМІСТ

ВСТУП 9
РОЗДІЛ 1 ПОНЯТТЯ SDN МЕРЕЖ 11
1.1 Засади створення SDN 11
1.2 Налаштування та моніторинг мереж 15
1.3 Якість обслуговування, керування з’єднаннями та енергоефективність 24
РОЗДІЛ 2 КОНТРОЛЬ ТРАФІКУ В SDN 38
2.1 Віртуалізація мережевих функцій SDN 38
2.2 Технічні рішення для управління трафіком 45
2.3 Архітектура та розвиток NFV 52
РОЗДІЛ 3 КОНТРОЛЕР КЕРУВАННЯ ТРАФІКУ ДЛЯ T-SDN 59
3.1 Структура мережі 59
3.2 Структура контролера T-SDN 67
РОЗДІЛ 4 СТВОРЕННЯ КЕРОВАНОГО SDN ПРОСТОРУ 74
4.1 Традиційний підхід 74
4.2 Віртуальна мережа 77
ВИСНОВКИ 83
ПЕРЕЛІК ПОСИЛАНЬ 85
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 87

ВСТУП

Сучасні телекомунікаційні мережі переживають стрімку еволюцію, що зумовлена зростанням обсягів передавання даних, поширенням хмарних сервісів, віртуалізацією інфраструктури та підвищенням вимог до якості обслуговування. Традиційні підходи до управління мережами, засновані на статичній конфігурації обладнання, вже не відповідають динамічним умовам, у яких функціонують дата-центри та транспортні мережі. Їхня основна проблема полягає у складності масштабування, обмеженій гнучкості та високих експлуатаційних витратах, що істотно ускладнює підтримку стабільного рівня сервісів у багатокористувацьких середовищах.

У цих умовах усе більшого поширення набувають програмно-визначені мережі (SDN), які відокремлюють контрольну та транспортну площини та забезпечують централізоване управління. Завдяки цьому стає можливим оперативне реагування на зміни навантаження, гнучке виділення ресурсів, оптимізація маршрутів і впровадження нових сервісів без суттєвих затрат часу. SDN відкриває перспективи для інтеграції з технологіями віртуалізації мережевих функцій (NFV) та розширює можливості застосування QoS, дозволяючи досягати високих показників продуктивності, надійності й безпеки.

Особливу актуальність дослідження методів управління трафіком у SDN-мережах визначає зростання попиту на гнучкі й масштабовані рішення для обробки даних у дата-центрах та глобальних операторських інфраструктурах. Міграція віртуальних машин, балансування навантаження, підтримка багатокористувацького середовища, енергоефективність, а також автоматизація процесів управління — це ті завдання, які вимагають системного підходу та застосування новітніх технологій.

Метою дипломної роботи є аналіз і систематизація сучасних методів управління трафіком у SDN-мережах, виявлення їхніх переваг і недоліків, а також формування пропозицій щодо підвищення ефективності використання мережевих ресурсів. Для досягнення цієї мети у роботі розглянуто архітектуру SDN, її

інтеграцію з NFV, особливості впровадження QoS та перспективи використання у транспортних мережах (T-SDN).

Значущість роботи полягає у тому, що її результати можуть бути застосовані для розробки сучасних систем управління дата-центрами, оптимізації використання пропускної здатності каналів, впровадження механізмів адаптивної міграції віртуальних машин, а також для створення більш стійких і енергоефективних мереж наступних поколінь.

1 ПОНЯТТЯ SDN МЕРЕЖ

1.1 Засади створення SDN

Кількість і масштаби центрів обробки даних (ЦОД) продовжують невпинно зростати, а їхні мережеві інфраструктури розширюються у відповідь на постійне збільшення обсягів трафіку. Структура та профіль трафіку в таких мережах характеризуються високою динамічністю, що особливо яскраво проявляється у хмарних ЦОД. Це зумовлено тим, що орендарі постійно змінюються, а їхні потреби у ресурсах можуть переглядатися упродовж усього строку користування сервісами. За таких умов конфігурація мережі повинна бути здатною швидко адаптуватися до нових вимог. У сучасних дослідженнях та практичних впровадженнях ключова роль відводиться технології програмно-визначених мереж (Software Defined Networking, SDN), яка забезпечує програмне управління параметрами та архітектурою мережі. Саме ця технологія нині є одним із найважливіших інструментів у процесі керування мережами ЦОД, відповідаючи актуальним вимогам до їхньої ефективності, масштабованості та надійності. Дипломна робота зосереджується на аналізі ролі SDN у функціонуванні сучасних ЦОД та розглядає науково-дослідні здобутки у співпраці з провідними галузевими спеціалістами.

Згідно з прогнозами, наведеними в Глобальному індексі розвитку хмарних технологій (Cisco Global Cloud Index), опублікованому компанією Cisco у 2017 році, вже у 2021 році обсяг внутрішнього IP-трафіку ЦОД сягнув 14,7 зеттабайта, тоді як обсяги трафіку між ЦОД перевищили 2,8 зеттабайта. Водночас спостерігається тенденція зменшення ролі традиційних ЦОД, оскільки більшість обсягу інформаційних потоків — до 95 % — нині проходить саме через хмарні центри обробки даних. Такий стрімкий ріст трафіку призвів до появи нових великих хмарних ЦОД, у яких щільність розміщення обчислювальних потужностей постійно зростає, обсяг систем зберігання даних розширюється, а пропускна здатність мереж збільшується завдяки підключенню дедалі більшої кількості пристроїв з високими характеристиками швидкодії. У той самий час відбувається

масштабна міграція бізнес-додатків із приватних у публічні хмари, які часто будуються на основі віртуальних ЦОД. При цьому їхні ресурси можуть розподілятися між кількома фізичними центрами, що створює нові виклики для управління та забезпечення безперервної роботи.

Для адміністраторів ЦОД, а також для орендарів, які отримують можливість управляти власними віртуальними ЦОД, стає критично важливим мати у своєму розпорядженні універсальні та потужні інструменти. Вони повинні не лише абстрагуватися від ускладненої структури конфігурацій, але й дозволяти ефективно контролювати апаратні ресурси, здійснювати моніторинг систем, а також отримувати інформацію, необхідну для грамотного адміністрування. Як приклад, організація може виступати орендарем одночасно і фізичного, і віртуального ЦОД; оператор одного центру може бути користувачем іншого; інструменти управління, що застосовуються в різних ЦОД, можуть істотно відрізнятися і не завжди підлягати інтеграції в єдиний набір для централізованого керування.

У цій дипломній роботі центральне місце відведено аналізу ролі технології SDN у розвитку мережевої інфраструктури DCN. Сутність SDN полягає у використанні програмного керування ресурсами та функціями мережі, що забезпечує підвищення її гнучкості та здатності адаптуватися під потреби користувачів і програмних застосунків. Найчастіше впровадження SDN здійснюється на основі відкритого стандартного протоколу OpenFlow, однак існує велика кількість альтернативних підходів. Використання SDN розглядається як перспективна альтернатива традиційним методам статичної конфігурації мережевого обладнання. Запровадження SDN (і особливо протоколу OpenFlow, який був активно підтриманий виробниками комутаційного обладнання) дало потужний поштовх розвитку досліджень і розробок у сфері сучасних телекомунікаційних технологій, формуючи нові наукові та практичні напрями розвитку мереж майбутнього.

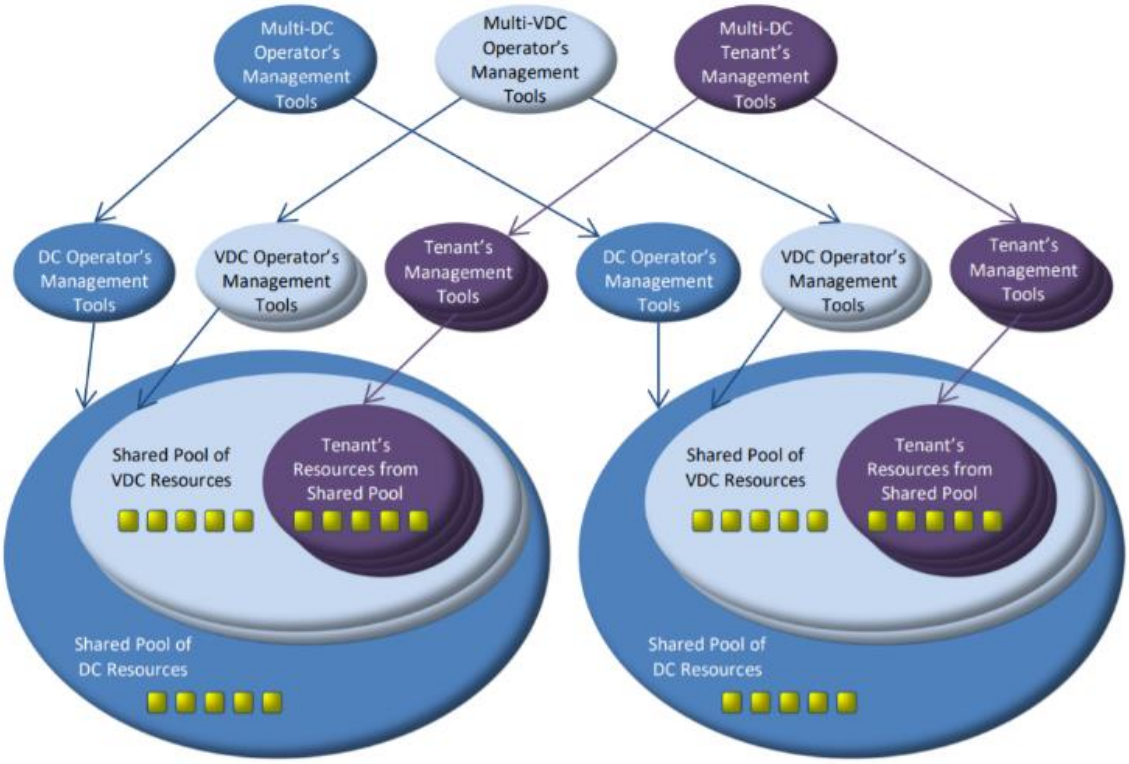


Рис. 1.1 Хмарний мульти-ЦОД із віртуальним мережним оператором

Центри обробки даних (ЦОД) відрізняються за своїми масштабами та архітектурою: від невеликих серверних кімнат, які обслуговують локальні завдання, до глобальних хмарних дата-центрів, що підтримують роботу міжнародних компаній і мільйонів користувачів по всьому світу. Найшвидше технологія програмно-визначених мереж (SDN) знайшла своє застосування саме у великих ЦОД. Це зумовлено тим, що у великих масштабах особливо важливим є ефективний розподіл і використання обмежених мережевих ресурсів. Такі центри постійно функціонують в умовах динамічних змін: профілі трафіку зазнають істотних коливань, користувачі постійно змінюються, з'являються нові програмні додатки та сервіси, а постачальники застосунків регулярно оновлюють свої рішення. Усе це створює потребу у високій адаптивності мережевої інфраструктури. Саме тому SDN стала ключовим інструментом для управління такими складними системами. У перспективі можна очікувати, що переваги SDN зумовлять її широке поширення не лише у масштабних хмарних ЦОД, а й у менших, менш динамічних центрах, які також потребуватимуть модернізації для підвищення ефективності та надійності.

Досить часто у професійній літературі та навіть у практичних впровадженнях SDN ототожнюють із віртуалізацією мереж, хоча насправді це два різних, хоча й взаємопов’язаних підходи. Віртуалізація мереж передбачає створення абстрактного рівня поверх фізичної інфраструктури, що дозволяє формувати одну або кілька віртуальних мереж незалежно від конкретної апаратної архітектури. Основною метою цього процесу є або спрощення уявлення про ресурси мережі для адміністраторів і користувачів, або організація механізмів безпечного спільного доступу до цих ресурсів різними клієнтами без необхідності взаємної довіри між ними. Водночас віртуалізація може будуватися на основі SDN, тоді як SDN, у свою чергу, може функціонувати на базі вже віртуалізованої інфраструктури. Таким чином, ці дві концепції не конкурують одна з одною, а швидше взаємодоповнюють, створюючи новий рівень гнучкості та керованості мереж.

У межах цієї дипломної роботи особлива увага приділяється ролі технології SDN у мережах центрів обробки даних (DCN). Акцент робиться на тих сценаріях застосування, що є найбільш актуальними для адміністраторів ЦОД, оскільки саме вони відповідають за підтримання стабільності, продуктивності й безпеки всієї інфраструктури. При цьому розглядаються як теоретичні основи SDN, так і практичні результати впровадження в сучасних ЦОД.

Для більш системного розуміння варіантів впровадження SDN у мережах дата-центрів у роботі буде застосовано класифікацію ключових категорій, що становлять інтерес для адміністраторів і операторів ЦОД (рис. 1.2). Саме ці напрями — від управління пропускною здатністю й балансування навантаження до забезпечення безпеки та автоматизації конфігурацій — стали головними об’єктами досліджень науковців та інженерів. У подальших розділах дипломної роботи наведено детальний аналіз цих аспектів, що дає можливість оцінити практичні переваги технології SDN у побудові й експлуатації сучасних високопродуктивних дата-центрів.

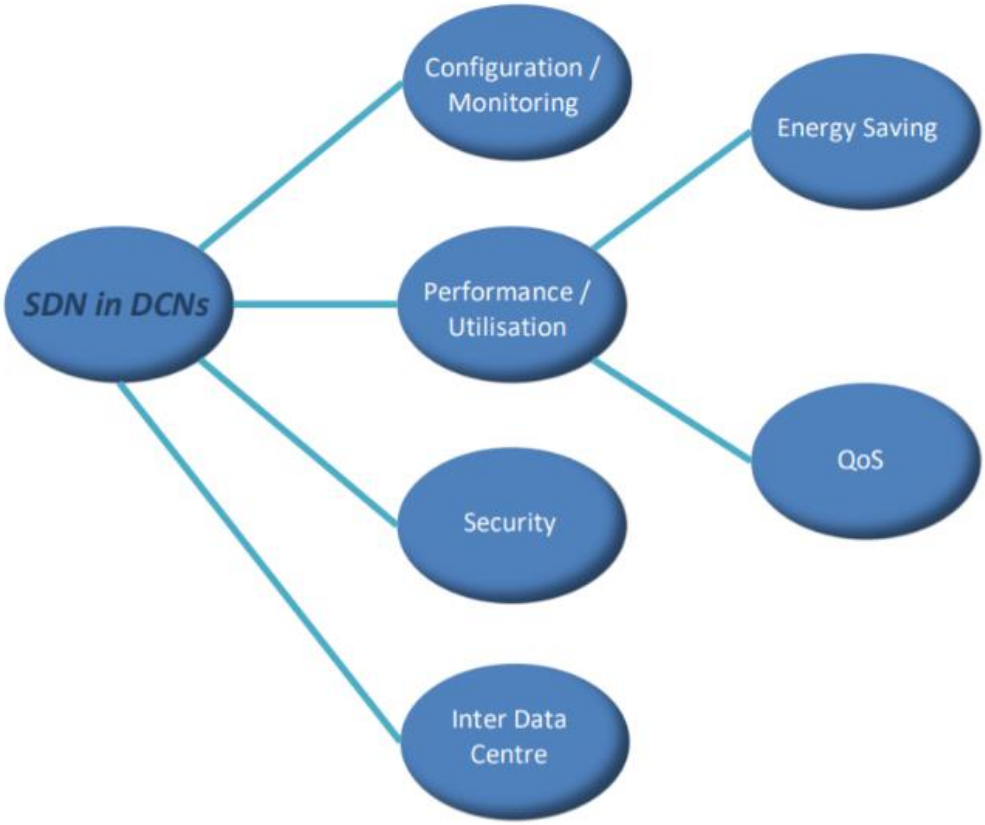


Рис. 1.2 Аспекти SDN, які становлять інтерес для адміністраторів ЦОД

1.2 Налаштування та моніторинг мереж

Під процесом налаштування у сучасних телекомунікаційних мережах розуміють не лише конфігурацію параметрів окремих пристроїв, а й повне управління всією інфраструктурою, що забезпечує їхню узгоджену роботу. У випадку мереж центрів обробки даних (Data Center Networks, DCN) до складу такої інфраструктури належать комутатори, маршрутизатори, проміжні блоки обробки, а також інші допоміжні елементи. Традиційно ці пристрої існували у фізичній формі, однак із розвитком віртуалізації дедалі більше компонентів переходять у програмне середовище, що відкриває нові можливості для їхнього керування. Сучасний хмарний центр обробки даних може містити понад тисячу фізичних комутаторів, які відрізняються між собою набором функцій, архітектурою, продуктивністю та підтримкою тих чи інших мережевих стандартів. Це створює складну багаторівневу

екосистему, управління якою без використання спеціалізованих технологій практично неможливе.

Інструменти управління мережею покликані забезпечити операторів абстрактним високорівневим представленням інфраструктури. Вони дозволяють перетворювати складні дії адміністратора, що виконуються на концептуальному рівні політик і правил, у конкретні інструкції для пристроїв нижчого рівня — фізичних або віртуальних. У цьому контексті програмно-визначені мережі (SDN) відіграють ключову роль, оскільки створюють уніфіковану картину всієї мережі, централізований механізм моніторингу та конфігурації. Завдяки SDN оператори отримують єдину точку управління всіма ресурсами, що значно спрощує процес оптимізації їхнього розподілу між застосунками, сервісами та кінцевими користувачами. Замість традиційної моделі, де кожен пристрій окремо налаштовується під умовні середні показники навантаження, сучасні ЦОД можуть функціонувати за принципом динамічного реагування на зміни трафіку, що забезпечує значно більшу гнучкість та ефективність.

Особливістю використання SDN є можливість створення та впровадження складних політик, які автоматично поширюються на всі елементи мережі та контролюються в режимі реального часу. Наприклад, у хмарному дата-центрі, де кількість орендарів постійно змінюється, необхідно регулярно оновлювати правила доступу та розподілу ресурсів. З’являються нові клієнти з новими вимогами до обчислювальних потужностей, частина орендарів залишає мережу, а інші змінюють свої параметри використання. Усі ці динамічні процеси можуть призводити до коливань у навантаженні на мережу та підвищення ризиків нестабільності. Використовуючи механізми SDN, адміністратор має змогу централізовано визначати політику розподілу ресурсів, яка автоматично коригується залежно від ситуації. Більш того, сучасні підходи дозволяють надавати орендарям контроль над їхньою часткою ресурсів на тому самому рівні, на якому оператор керує всією мережею. Це створює гнучку багаторівневу модель управління, де кожен учасник має доступ лише до релевантних йому сегментів, що підвищує прозорість і безпеку.

Важливо зазначити, що створення єдиного представлення ресурсів мережі не є простою задачею. Пристрої можуть мати різні характеристики навіть у межах однієї функціональної ролі. Наприклад, комутатори відрізняються обсягом пам’яті таблиць CAM, які використовуються для зберігання правил пересилання пакетів чи кешування даних, різним рівнем підтримки протоколу OpenFlow, а також наявністю або відсутністю механізмів для виконання користувацького коду безпосередньо на обладнанні. Усе це створює складність для управління та стандартизації. Програмно-визначений підхід дозволяє подолати цю проблему шляхом маскування апаратних відмінностей і подання всіх ресурсів у вигляді єдиної абстракції.

Не менш важливим є аспект моніторингу. Для забезпечення коректної роботи мережі необхідно постійно збирати й аналізувати дані про функціонування пристроїв. Технологія SDN дозволяє реалізувати динамічне керування виділеними під моніторинг ресурсами, такими як процесорні потужності чи обсяг пам’яті комутаторів. Це дозволяє балансувати між точністю вимірювань і рівнем використання ресурсів. Наприклад, у разі високого навантаження можна знизити деталізацію зібраної інформації, надавши пріоритет пересиланню пакетів, а у випадку необхідності виявлення потенційних атак або аномалій — навпаки, збільшити рівень деталізації та частоту збору даних. Таким чином, адміністратори отримують гнучкий інструмент, що адаптується до конкретних умов роботи мережі.

Окремо слід підкреслити значення сучасних напрямів розвитку моніторингових систем, зокрема мережевої телеметрії. Вона полягає у зборі даних про пакети безпосередньо в площині пересилання, що дає змогу оперативно виявляти несправності, аналізувати причини відмов та усувати проблеми ще до того, як вони призведуть до збоїв у роботі критично важливих застосунків. Використання телеметрії в поєднанні з SDN створює передумови для побудови інтелектуальних систем контролю, які здатні не лише фіксувати аномалії, але й прогнозувати їх виникнення на основі аналізу великих обсягів даних. Це принципово відрізняє новітні підходи від традиційної практики, коли для моніторингу виділявся фіксований набір ресурсів, а можливості їх адаптивного перерозподілу були відсутні.

Отже, технологія SDN забезпечує не просто централізоване управління та моніторинг, а й створює гнучке та інтелектуальне середовище, здатне адаптуватися до змінних умов функціонування центрів обробки даних. Це робить її одним із ключових напрямів розвитку сучасних інформаційно-телекомунікац

Контроль продуктивності та оптимізація використання ресурсів у ЦОД

У сучасних центрах обробки даних (ЦОД), особливо у великих інфраструктурах, що належать провайдерам публічних хмарних сервісів, питання продуктивності та ефективного використання ресурсів є одним із ключових. Навіть незначне зменшення затримок у мережі чи збільшення пропускної здатності каналів може надати компанії вагому конкурентну перевагу. Це пояснюється тим, що будь-які мілісекунди затримки чи втрата пакетів прямо впливають на роботу бізнес-додатків, швидкість обробки транзакцій і якість користувацького досвіду. Тому підхід до управління продуктивністю ЦОД має бути системним, комплексним і багаторівневим.

Розділення та регулювання трафіку

Одним із базових механізмів підвищення ефективності є розділення мережевого трафіку, яке дозволяє використовувати резервні маршрути, зазвичай закладені у проєкт ще на етапі побудови мережі для забезпечення відмовостійкості. Традиційно ці резерви активуються лише у випадках збоїв, проте завдяки SDN вони можуть застосовуватися й у штатному режимі. Це дає змогу суттєво підвищити коефіцієнт використання ресурсів і знизити непродуктивні витрати. У класичних рішеннях використовується технологія ECMP (Equal-Cost Multi-Path), що рівномірно розподіляє трафік між кількома маршрутами. Однак ECMP не здатна враховувати реальне завантаження каналів, тому балансування відбувається не завжди оптимально. На відміну від цього, SDN забезпечує інтелектуальне керування потоками, дозволяючи перенаправляти перевантажені з’єднання за лічені мілісекунди, що значно підвищує стабільність роботи.

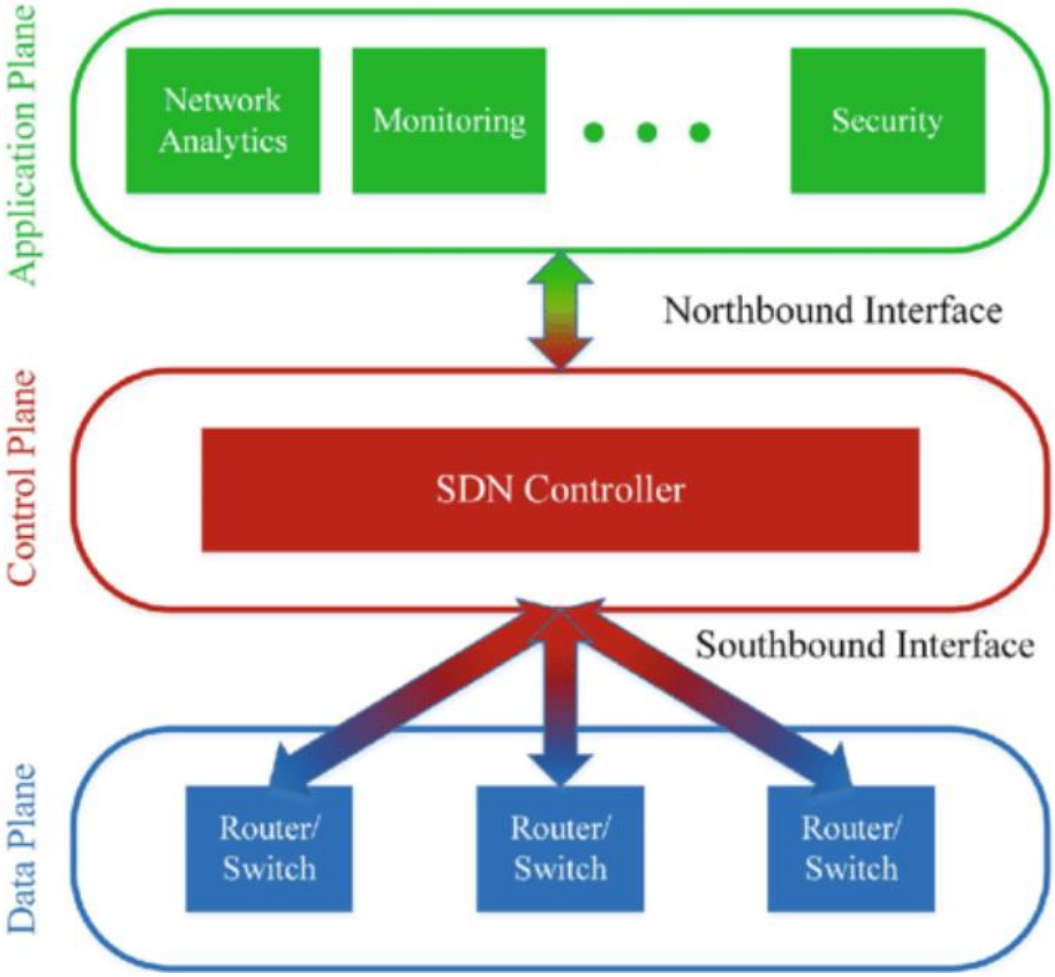


Рис. 1.3 Схема з API, застосунками, контроллером та пристроями — взаємодія між шарами, необхідно для опису балансування, DPI, динамічного керування потоками

Балансування навантаження як стратегія масштабування

Балансування навантаження у сучасних центрах обробки даних (ЦОД) розглядається не просто як допоміжний механізм, а як одна з ключових стратегій забезпечення ефективності, надійності та масштабованості інформаційної інфраструктури. Завдяки цьому підходу можливо одночасно досягати високої продуктивності систем, зменшувати ризики перевантажень і забезпечувати безперервність надання сервісів навіть у пікові моменти навантаження.

Балансування може здійснюватися на різних рівнях моделі OSI, що відкриває широкі можливості для оптимізації роботи мережі. На транспортному рівні (4-й рівень) воно базується на розподілі клієнтських потоків між кількома серверами, які забезпечують один і той самий сервіс. Це дозволяє уникнути залежності від

вертикального масштабування, коли продуктивність досягається шляхом заміни існуючого сервера на потужніший. Натомість реалізується горизонтальне масштабування: додаються нові сервери, які беруть на себе частину навантаження. Подібний підхід є набагато гнучкішим та економічно вигіднішим, адже дозволяє масштабувати інфраструктуру поступово, у відповідь на реальні потреби бізнесу чи зміни в поведінці користувачів. Крім того, у випадку відмови одного сервера інші здатні автоматично перебрати його функції, що значно підвищує відмовостійкість ЦОД.

Ще більш важливе значення балансування набуває на прикладному рівні (7-й рівень). Тут воно виходить за межі простого розподілу потоків і передбачає застосування механізмів глибокої перевірки пакетів (Deep Packet Inspection, DPI). Ця технологія дозволяє аналізувати не тільки заголовки, а й вміст трафіку, що відкриває можливості для набагато більш точного й гнучкого управління потоками. Трафік може перенаправлятися на певний сервер залежно від типу застосунку, характеру даних або навіть політик безпеки. Наприклад, потоки з високими вимогами до затримки можуть бути спрямовані на спеціалізовані високопродуктивні сервери, тоді як звичайний веб-трафік може оброблятися на стандартних вузлах.

Така логіка дозволяє інтегрувати балансування з іншими сервісами: системами віртуальних брандмауерів, засобами NAT, інструментами контент-фільтрації чи спеціалізованими аналітичними платформами. Завдяки цьому балансувальник стає не просто «розподілювачем» навантаження, а комплексним елементом інфраструктури безпеки й оптимізації.

Особливу роль у розвитку балансування відіграє технологія SDN (Software Defined Networking). Її інтеграція робить процес керування потоками динамічним і максимально гнучким. Адміністратори отримують можливість у реальному часі змінювати правила маршрутизації, адаптуючи їх до змін у рівні навантаження, появи нових загроз або необхідності виконання бізнес-політик. Більше того, SDN дозволяє позбутися надмірної кількості проміжних пристроїв, оскільки функції DPI, NAT чи навіть брандмауерів можуть бути вбудовані безпосередньо у

комутатори. Це зменшує затримки, підвищує продуктивність та знижує вартість експлуатації.

Міграція віртуальних машин як механізм оптимізації ЦОД

Одним із ключових інструментів підвищення ефективності роботи сучасних центрів обробки даних (ЦОД) є міграція віртуальних машин (ВМ). Це процес перенесення запущених віртуальних середовищ із одного фізичного хоста на інший без зупинки роботи сервісів або з мінімальними перервами. Його головною метою є оптимізація продуктивності, зниження затримок, підвищення відмовостійкості та ефективніше використання обчислювальних і мережевих ресурсів.

Найпоширеніший сценарій застосування міграції полягає у ситуації, коли дві або більше віртуальних машин активно обмінюються даними. Якщо вони розташовані на різних фізичних серверах, дані змушені проходити через кілька проміжних каналів і комутаторів, що збільшує затримки та створює додаткове навантаження на мережу. Переміщення таких ВМ на один хост або у найближчі сервери дозволяє мінімізувати кількість проміжних переходів, знизити мережеві затримки та зменшити ймовірність перевантаження каналів. Це особливо важливо для систем реального часу, фінансових транзакцій, аналітичних платформ та сервісів потокового передавання даних.

Управління процесом міграції значно спрощується завдяки впровадженню технології SDN (Software Defined Networking). Її основна функція у цьому випадку полягає у забезпеченні прозорості міграції: усі встановлені з’єднання мають залишатися стабільними навіть тоді, коли фізичне розташування віртуальної машини змінюється. Іншими словами, для користувача та прикладних сервісів процес переміщення ВМ має бути абсолютно непомітним. SDN забезпечує оновлення маршрутів у мережі в реальному часі, швидке перепідключення сесій і коректне перенесення політик безпеки, що дає змогу уникати збоїв.

Ще однією перевагою SDN є можливість резервування мережевих ресурсів для операцій міграції. Система може заздалегідь виділяти необхідну пропускну здатність каналів або обчислювальні ресурси, щоб процес відбувався максимально швидко й без впливу на якість обслуговування. У випадку високих навантажень це

особливо актуально, оскільки неконтрольована міграція здатна спричинити додаткові затримки або навіть тимчасові відмови сервісів.

Водночас слід враховувати й витрати, пов’язані з міграцією. Переміщення ВМ вимагає ресурсів процесора, пам’яті, дискових підсистем і мережевих каналів. Якщо міграції відбуваються занадто часто або виконуються без належного планування, то накладні витрати можуть перевищити очікуваний ефект. Наприклад, у випадках, коли навантаження на сервер не є критичним, а виграш від переміщення мінімальний, доцільніше залишити віртуальні машини на місці.

Проблеми швидкодії апаратних комутаторів у ЦОД

Однією з ключових технічних проблем, із якими стикаються адміністратори сучасних центрів обробки даних (ЦОД), є затримки у встановленні правил у таблицях потоків апаратних комутаторів. У середовищах із великою кількістю динамічних потоків навіть операція додавання одного нового правила може займати помітний час. Коли йдеться про сотні чи тисячі правил, ситуація стає критичною: система втрачає здатність оперативно реагувати на зміни у структурі трафіку. Це особливо небезпечно у багатокористувацьких середовищах (multi-tenant), де активність орендарів часто змінюється, і мережа повинна швидко перебудовуватися, щоб забезпечити належний рівень продуктивності та безпеки.

У випадках, коли швидке додавання правил у таблиці є неможливим, одним із дієвих рішень виступає використання попередньо налаштованих тунелів. Суть підходу полягає в тому, що нові потоки тимчасово спрямовуються через заздалегідь визначені маршрути, доки комутатори не завершать обробку й запис усіх необхідних правил. Це дозволяє уникнути небезпечних затримок та збоїв у роботі мережі. Завдяки такому методу забезпечується певний «буфер часу», необхідний для стабільного переходу системи від старого стану до нового без переривання сервісів. У результаті користувачі не помічають технічних труднощів, а адміністратори отримують змогу підтримувати стабільність роботи ЦОД навіть у моменти значних змін у навантаженні.

Ще однією важливою проблемою є нерівномірність характеристик обладнання, що експлуатується у великих інфраструктурах. Не всі комутатори

мають однакову потужність і функціональні можливості. Частина пристроїв підтримує великі таблиці потоків і здатна зберігати значні обсяги інформації для обробки пакетів. Інші відрізняються високою швидкістю обробки даних, мають сучасні процесори та інтерфейси, які дозволяють забезпечувати гігабітні чи терабітні швидкості. Є й ті, що відстають за характеристиками, стаючи слабкими ланками у загальній архітектурі. Це створює серйозну проблему — нерівномірність продуктивності у масштабах усього ЦОД.

Наслідки такої різнорідності досить суттєві. Навіть якщо у частині сегментів мережі комутатори забезпечують високу швидкодію, загальна продуктивність часто визначається найслабшою ланкою. Це призводить до вузьких місць у маршрутизації, збільшення затримок і втрат пакетів. У критичних випадках — до зниження якості обслуговування (QoS) та ризиків виникнення відмов. Традиційні методи адміністрування у таких умовах малоефективні, адже вимагають від спеціалістів ручної оптимізації ресурсів і складних налаштувань під конкретні сегменти мережі.

Технологія SDN (Software Defined Networking) пропонує вирішення цієї проблеми. Вона дозволяє абстрагувати різнорідність обладнання, перетворюючи усю мережеву інфраструктуру на єдиний віртуалізований ресурс. За допомогою централізованого контролера мережа розглядається як цілісна система, у якій кожен комутатор використовується оптимально відповідно до своїх характеристик. Потужні пристрої отримують більші навантаження, а менш продуктивні працюють у межах власних можливостей, не створюючи «вузьких місць». Це забезпечує баланс ресурсів, підвищує загальну ефективність роботи мережі й дозволяє масштабувати інфраструктуру без суттєвої перебудови.

Таким чином, проблеми швидкодії апаратних комутаторів і різнорідності їхніх характеристик є серйозними викликами для адміністраторів ЦОД. Проте завдяки інтеграції рішень на базі SDN стає можливим не лише мінімізувати негативні наслідки цих обмежень, а й перетворити їх на переваги, забезпечивши гнучке, динамічне та ефективне управління усією інфраструктурою.

1.3 Якість обслуговування, керування з’єднаннями та енергоефективність

Якість обслуговування в мережах центрів обробки даних: розширений аналіз

Якість обслуговування (Quality of Service, QoS) є одним із ключових механізмів, який забезпечує стабільну, передбачувану та надійну роботу сучасних інформаційно-телекомунікаційних систем, особливо у центрах обробки даних (ЦОД). У міру того як кількість користувачів, сервісів та обсягів передаваних даних постійно зростає, роль QoS стає ще більш значущою, адже саме цей механізм дозволяє підтримувати баланс між різними видами трафіку і гарантувати належний рівень якості обслуговування для критично важливих додатків.

Основна мета QoS полягає у тому, щоб забезпечити диференційований підхід до обробки трафіку. Це означає, що окремі класи даних отримують різні рівні пріоритету. Наприклад, сервіси реального часу, такі як відеоконференції чи VoIP-зв’язок, вимагають мінімальних затримок і втрат пакетів, тоді як звичайний веб-трафік або передача файлів можуть допускати певні коливання у швидкості. Завдяки механізмам QoS критично важливі потоки даних отримують гарантовані параметри обслуговування — низьку затримку, необхідну пропускну здатність, мінімальний рівень втрат пакетів і високу стабільність у часі.

У сучасних ЦОД без QoS неможливо уявити ефективну роботу бізнес-критичних застосунків. Наприклад, фінансові сервіси, аналітичні платформи чи системи інтернет-торгівлі повинні працювати без збоїв навіть у моменти пікових навантажень. Без пріоритезації трафіку такі сервіси могли б відчувати перебої через конкуренцію з менш критичними потоками, що у кінцевому результаті призводить до втрат для компаній та зниження довіри користувачів.

Ще одним важливим аспектом є здатність QoS мінімізувати вплив перевантажень. У середовищах, де тисячі клієнтів одночасно генерують запити, а обсяг переданих даних зростає у геометричній прогресії, навіть найпотужніше обладнання може стикнутися з проблемами перевищення ресурсів. Механізми QoS

дозволяють уникнути колапсу системи, адже вони забезпечують грамотний розподіл ресурсів між потоками відповідно до заданих політик. Це робить можливим стабільне функціонування навіть тоді, коли навантаження перевищує середні очікувані значення.

У контексті дата-центрів особливе значення має також гнучкість QoS. Системи мають справу з постійно змінюваним трафіком: одні сервіси зникають, інші з’являються, змінюються моделі використання клієнтами ресурсів. Традиційні методи управління трафіком не здатні ефективно адаптуватися до таких умов. Натомість QoS у поєднанні з технологіями SDN (Software Defined Networking) забезпечує можливість динамічного переналаштування політик у реальному часі. Це означає, що мережа може швидко реагувати на зміни у навантаженні, автоматично підвищуючи або знижуючи пріоритети для різних потоків, і тим самим підтримувати необхідний рівень обслуговування без втручання адміністратора.

Таким чином, QoS у мережах ЦОД — це не лише механізм розподілу ресурсів, а фундаментальний інструмент забезпечення надійності та гнучкості всієї інфраструктури. Він дозволяє підтримувати безперервну роботу критичних сервісів, оптимально використовувати апаратні та мережеві ресурси, мінімізувати ризики відмов і забезпечувати високу якість досвіду користувачів навіть в умовах інтенсивних перевантажень. У майбутньому роль QoS лише зростатиме, оскільки цифровізація бізнесу і зростання обсягів трафіку вимагатимуть ще більш тонкого управління мережею, а інтеграція із SDN і NFV зробить ці механізми ще більш потужними та адаптивними.

Ключові аспекти та проблематика QoS у ЦОД

У сучасних великих центрах обробки даних (ЦОД), особливо тих, що забезпечують роботу публічних хмарних сервісів, питання якості обслуговування (QoS) стає критично важливим. Причина полягає в тому, що навантаження на мережу розподіляється нерівномірно, постійно змінюється і залежить від десятків змінних факторів. У пікові моменти кількість користувачів і транзакцій може зростати у рази, і навіть найпотужніше обладнання стикається з перевантаженнями.

Це створює унікальні виклики, для вирішення яких недостатньо класичних методів управління трафіком.

Основні причини перевантаження в мережах ЦОД

1. **Обмежена пропускна здатність каналів.** Навіть при використанні сучасних оптичних технологій існують фізичні обмеження. Якщо обсяг переданих даних перевищує можливості інфраструктури, виникають черги і затримки, що критично для додатків у реальному часі.
2. **Недостатній обсяг буферної пам'яті.** Комутатори та маршрутизатори можуть тимчасово зберігати пакети, однак при надмірному навантаженні їхні буфери переповнюються. Це призводить до втрати даних, повторних передач і зростання затримок.
3. **Витрати обчислювальних ресурсів.** Обробка кожного пакета вимагає певної кількості операцій: перевірки контрольних сум, виконання шифрування, маршрутизації, застосування політик QoS. Коли кількість пакетів сягає мільйонів на секунду, навіть незначні додаткові витрати процесорного часу перетворюються на серйозну проблему.
4. **Динамічність хмарних середовищ.** У хмарних ЦОД орендарі можуть у будь-який момент запускати або зупиняти свої додатки, змінювати вимоги до ресурсів чи генерувати різко зростаючі навантаження. Це створює постійно змінюваний профіль трафіку, для якого статичні методи управління просто не підходять.

Таким чином, адміністратори стикаються з надзвичайно складними умовами, де традиційні методи планування і контролю виявляються малоефективними. Саме QoS стає тим механізмом, який дозволяє адаптивно реагувати на зміни у режимі реального часу і гарантувати належну якість обслуговування.

Розширені функціональні можливості QoS у ЦОД

Ізоляція критичного трафіку. QoS забезпечує відокремлення важливих потоків (VoIP-зв'язок, відеоконференції, банківські транзакції, медичні системи) від звичайного трафіку. Це унеможливлює ситуацію, коли, наприклад, масові

завантаження файлів або резервні копії заважають стабільній роботі критичних сервісів.

Пріоритезація потоків. Завдяки гнучким політикам QoS різні види трафіку можуть отримувати різні рівні доступу до ресурсів. Потоки, що обслуговують бази даних або критичні аналітичні застосунки, отримують вищий пріоритет порівняно зі звичайним трафіком користувачів. Це дозволяє уникати затримок там, де вони недопустимі.

Керування затримками. QoS формує умови для забезпечення стабільного часу доставки пакетів, що особливо важливо для мультимедійних сервісів та потокових застосунків. Для відео у високій якості навіть кількамілісекундні стрибки можуть призвести до втрати кадрів чи деградації картинки.

Гарантоване виділення ресурсів. Однією з ключових переваг QoS є можливість резервувати певний обсяг пропускної здатності для конкретних сервісів або користувачів. Це означає, що навіть під час перевантажень мережі необхідні ресурси будуть доступні, а критичні сервіси залишаться стабільними.

Адаптивність та динамічне налаштування. Сучасні системи QoS, особливо у поєднанні з SDN (Software Defined Networking), здатні автоматично змінювати політики залежно від часу доби, реального навантаження, поведінки користувачів чи вимог окремих орендарів. Це робить систему гнучкою та стійкою до непередбачуваних змін у профілі трафіку.

Таким чином, QoS у центрах обробки даних — це не лише набір технічних інструментів, а стратегічний механізм управління мережею, що забезпечує надійність, передбачуваність і безперервність роботи сервісів у середовищах із високою динамікою. У майбутньому роль QoS лише зростатиме, оскільки обсяги даних продовжують стрімко збільшуватися, а вимоги до якості бізнес-критичних застосунків стають дедалі жорсткішими.

Інтеграція SDN у систему QoS

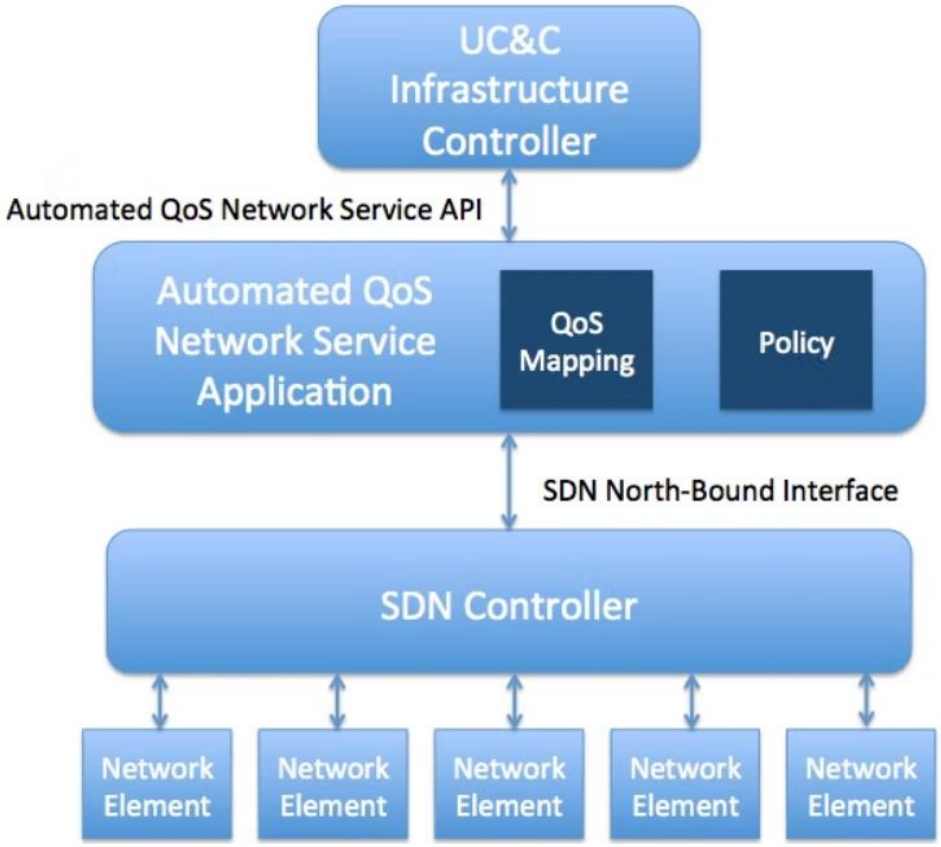


Рис. 1.4 Схема, де контролер SDN керує елементами мережі через політику QoS, відображено, як QoS-mapping та policy engine взаємодіють із пристроями мережі

Традиційні механізми QoS реалізовувалися переважно апаратно й вимагали складних конфігурацій на кожному пристрої окремо. Це робило систему негнучкою та повільною у реагуванні. Впровадження програмно-визначених мереж (SDN) докорінно змінює ситуацію.

SDN надає централізований контроль над мережею: адміністратор або контролер SDN може в реальному часі встановлювати правила для управління потоками. Якщо десь виникає перевантаження, система здатна миттєво перенаправити частину трафіку на інші маршрути, гарантуючи якість для пріоритетних сервісів. Це особливо важливо в хмарних середовищах, де профіль трафіку змінюється щосекунди.

Переваги поєднання QoS і SDN:

- Тонке налаштування рівня обслуговування на рівні окремих потоків.

- Швидке застосування нових політик без ручного втручання у кожен комутатор.
- Можливість формувати багаторівневі правила обслуговування (від критично важливих сервісів до другорядних).
- Динамічне перенаправлення потоків із перевантажених ділянок.

Практичні сценарії використання

Механізми QoS особливо актуальні для таких випадків:

- **Розподілені бази даних** — потребують стабільного каналу для синхронізації великих обсягів даних між вузлами.
- **Аналітичні системи типу MapReduce** — чутливі до затримок у мережі, адже будь-яке уповільнення збільшує час виконання обчислень.
- **Віртуальні приватні мережі (VPN)** — вимагають гарантій ізоляції між клієнтами та стабільного рівня захисту.
- **Відеоаналітика й потокове передавання** — сервіси, що не терплять затримок і потребують стабільної смуги пропускання.
- **Системи критичної інфраструктури** — управління енергетичними, транспортними або медичними ресурсами, де навіть короткочасна затримка може призвести до серйозних наслідків.

Перспективні напрями розвитку QoS у ЦОД

1. **Інтеграція із застосунками**. У майбутніх ЦОД додатки самі зможуть повідомляти мережу про свої потреби у пропускній здатності та затримках. Це дозволить автоматично формувати політики QoS під конкретні задачі.
2. **Явне управління маршрутами**. Застосунки отримають можливість обирати маршрути передачі даних, що дозволить уникати перевантажених ділянок і гарантовано підтримувати заданий рівень сервісу.
3. **Прогнозування на основі штучного інтелекту**. Використання алгоритмів машинного навчання для прогнозування пікових навантажень та проактивного перерозподілу ресурсів.

4. **Автоматизована сегментація трафіку**. Поєднання SDN і мережевої віртуалізації дозволить ізолювати трафік різних орендарів і надавати їм індивідуальні гарантії якості.
5. **Інтеграція з мережевою телеметрією**. Дані про затримки, втрати й завантаженість каналів будуть автоматично аналізуватися, а політики QoS — адаптуватися без участі людини.

QoS у поєднанні з технологіями SDN перетворюється з додаткової опції на ключовий елемент функціонування сучасних дата-центрів. Якщо раніше QoS була спрямована переважно на виділення ресурсів для певних сервісів, то сьогодні вона стала потужним інструментом динамічного керування всією мережею. Саме завдяки QoS стає можливим забезпечити стабільну роботу додатків у багатокористувацьких середовищах, знизити ризики перевантаження та підвищити загальну ефективність використання ресурсів.

Таким чином, якість обслуговування у ЦОД — це не лише технічна характеристика, а стратегічний фактор, що визначає конкурентоспроможність постачальників хмарних сервісів. У майбутньому роль QoS тільки зростатиме, оскільки саме вона дозволяє збалансувати інтереси мільйонів користувачів, бізнесу та інфраструктури в умовах стрімкого розвитку цифрової економіки.

Енергозбереження в сучасних центрах обробки даних

Збільшення кількості та масштабів центрів обробки даних (ЦОД) неминуче супроводжується різким зростанням енергоспоживання. Сьогодні витрати на електроенергію є однією з найбільших статей у структурі експлуатаційних витрат дата-центрів. Це змушує як науковців, так і інженерів-практиків шукати ефективні шляхи зниження рівня споживаної енергії без шкоди для продуктивності, надійності та безперервності роботи систем.

На початкових етапах основна увага приділялася саме обчислювальній складовій, зокрема консолідації віртуальних машин. Завдяки цій стратегії можна було відключати або переводити у «сплячий режим» сервери у години непікового навантаження, що давало відчутний ефект у скороченні витрат. Проте з часом стало очевидно, що значна частка енергоспоживання припадає не лише на сервери, а й на

мережеву інфраструктуру. Саме мережі всередині ЦОД часто є прихованими «споживачами енергії», адже вони спроєктовані з урахуванням пікових навантажень і тому завжди містять надлишкову кількість комутаторів, каналів та резервних пристроїв. У результаті у робочому режимі більшість таких елементів задіяна лише частково, але при цьому постійно споживає електроенергію. Це не лише підвищує операційні витрати, але й створює додаткове теплове навантаження на системи охолодження, які у свою чергу знову збільшують загальне енергоспоживання.

Виклики традиційної моделі

Традиційні мережі ЦОД завжди будувалися з надлишком пропускної здатності, що давало можливість уникати «вузьких місць» у разі стрибків трафіку чи відмов окремих пристроїв. Однак така стратегія мала суттєвий недолік: навіть у моменти низької активності мережа залишалася у стані підвищеного енергоспоживання. У середньому більшу частину часу ЦОД функціонує лише на невеликій частці своєї максимальної потужності, а решта ресурсів залишається «у резерві», продовжуючи витрачати енергію.

Роль SDN у зниженні енергоспоживання

Програмно-визначені мережі (SDN) стали важливим інструментом для розв’язання цієї проблеми. На відміну від традиційних підходів, де конфігурація кожного пристрою виконується окремо, SDN забезпечує централізоване керування та глобальне бачення всієї мережі. Це створює унікальні можливості для енергозбереження:

- Гнучке керування потоками даних. SDN дозволяє спрямовувати чи перенаправляти трафік через обмежену кількість активних комутаторів і каналів. Ті елементи, які тимчасово не використовуються, можуть бути вимкнені або переведені у режим низького енергоспоживання.
- Адаптивність до змін навантаження. Коли трафік зростає й наближається до пікових значень, система автоматично активує додаткові пристрої, забезпечуючи безперервність та стабільність роботи.

- Оптимізація використання обладнання. Завдяки знанню енергопрофілів різних комутаторів можна першочергово відключати найбільш енерговитратні пристрої, залишаючи активними ті, що працюють найбільш ефективно.

Динамічне регулювання параметрів. Навіть для активних комутаторів можливе налаштування робочої частоти процесора чи швидкості портів залежно від навантаження, що дозволяє зекономити додаткову частку енергії.

Переваги централізованого підходу

SDN має дві ключові властивості, які забезпечують її перевагу в реалізації енергозберігаючих стратегій:

- Повна видимість мережі. Контролер SDN у реальному часі отримує дані про всі активні потоки, що дозволяє прогнозувати навантаження та приймати проактивні рішення щодо оптимізації ресурсів.
- Централізоване керування. Перед тим як відключити пристрій чи канал, система може автоматично переналаштувати маршрути, щоб уникнути втрати пакетів чи різкого збільшення затримки. Це гарантує безпеку процесу та збереження якості обслуговування.

Перспективні підходи

Серед сучасних стратегій енергозбереження особливе місце займають:

- Енергетично-орієнтована інженерія трафіку (Energy-aware Traffic Engineering, ETE). Вона базується на аналізі закономірностей трафіку і дозволяє відключати міжкомутаторні з’єднання у моменти мінімального навантаження, наприклад, у нічний час.
- Інтелектуальні алгоритми управління. Використання машинного навчання для прогнозування піків трафіку та динамічного перемикання пристроїв у режим низького енергоспоживання.
- Ієрархічна оптимізація. Врахування індивідуальних енергопрофілів обладнання для пріоритетного вимкнення найвитратніших пристроїв.

- Гібридні моделі керування. Поєднання централізованого SDN-контролера з локальними алгоритмами економії енергії на рівні окремих комутаторів.

Енергозбереження у ЦОД уже давно перестало бути другорядним завданням — сьогодні це один із визначальних факторів їхньої ефективності та конкурентоспроможності. Використання програмно-визначених мереж дозволяє радикально змінити підхід до споживання енергії: від традиційної моделі постійної готовності до інтелектуальної моделі адаптивного управління. Завдяки SDN дата-центри отримують можливість витрачати енергію лише пропорційно до реальних потреб, знижувати експлуатаційні витрати, мінімізувати екологічний слід та підвищувати загальну стійкість інфраструктури. У перспективі саме поєднання SDN із енергоефективними алгоритмами прогнозування та автоматизації стане основою для побудови «зелених» ЦОД наступного покоління.

Управління з’єднаннями між центрами обробки даних

Сучасні власники великих дата-центрів дедалі частіше керують не одним, а одразу кількома об’єктами, розташованими у різних географічних регіонах. Це зумовлено низкою причин: необхідністю забезпечення надлишковості та відмовостійкості, створенням систем аварійного відновлення у випадку критичних збоїв, а також потребою у наближенні сервісів до кінцевих користувачів. Розміщення інфраструктури ближче до груп споживачів дає змогу суттєво знизити затримки у доставці даних, оптимізувати використання магістральної пропускної здатності Інтернету й покращити загальну якість обслуговування. Аналогічні мотиви мають і орендарі ЦОД, які все частіше використовують ресурси одразу кількох центрів, при цьому ці центри можуть належати різним операторам і функціонувати на основі різних технічних платформ.

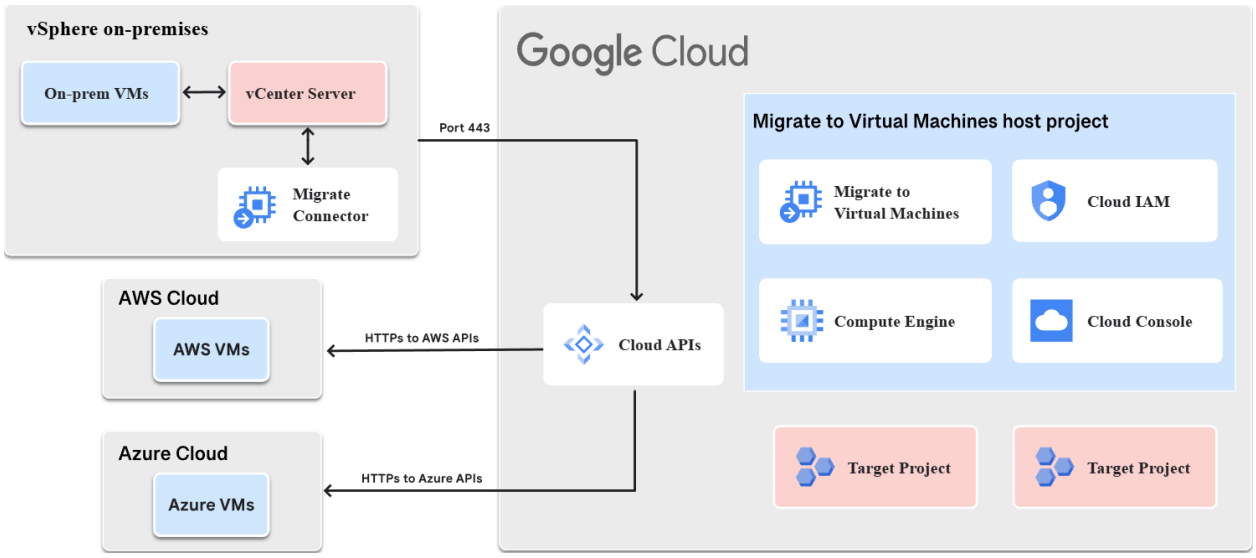


Рис. 1.5 Відображення процесу переміщення ВМ, зміни каналів, можливості масштабування, створення/видалення віртуальних з'єднань, на прикладі Google Cloud

Відмінності між внутрішніми та між-ЦОД з'єднаннями

З'єднання між ЦОД зазвичай реалізуються через глобальні мережі (WAN) та Інтернет-канали, які суттєво відрізняються від внутрішньої інфраструктури самого дата-центру. Якщо всередині ЦОД мережа проєктується із закладеним надлишком пропускної здатності для уникнення будь-яких «вузьких місць», то у випадку між-ЦОД з'єднань стратегія може змінюватися. Наприклад, оператори WAN-мереж часто підтримують низький рівень завантаження каналів, щоб клієнти мали відчуття високої надійності: у разі збою трафік миттєво перенаправляється альтернативними шляхами без помітного впливу для користувача.

Разом із тим, оператор ЦОД, який одночасно виступає і провайдером WAN-послуг, може балансувати між надійністю та вартістю. Замість дорогих надлишкових каналів він може використовувати менш пропускні, але більш завантажені канали, що знижує фінансові витрати. У такому разі особливо важливо забезпечити швидку реакцію системи у випадку відмови, щоб уникнути лавиноподібного перевантаження мережі. Саме технологія SDN забезпечує необхідну гнучкість: вона дозволяє в режимі реального часу переналаштовувати маршрути, мінімізуючи ризик збоїв, причому накладні витрати на таку перебудову є мінімальними.

Можливості для орендарів і роль SDN

У мульти-ЦОД архітектурах орендарям дедалі частіше надається можливість управляти віртуальними каналами, що з’єднують їхні мережі у різних дата-центрах. Ці віртуальні канали створюються поверх фізичних ресурсів оператора, однак завдяки віртуалізації стають повністю підконтрольними орендарю. Це означає, що клієнти можуть самостійно створювати нові канали, масштабувати їх пропускну здатність залежно від поточного навантаження або розривати з’єднання, якщо вони більше не потрібні.

SDN відіграє тут ключову роль: вона надає інтерфейси самообслуговування, за допомогою яких орендар може задавати не лише базові параметри каналу, а й визначати вимоги до пропускної здатності, рівня QoS та інших показників якості обслуговування. Це дозволяє клієнтам отримувати рівень гнучкості, який був недоступний у традиційних мережах, де будь-які зміни в інфраструктурі виконувалися вручну після подання заявки оператору.

Автоматизація процесів та сценарії використання у SDN

Однією з найбільших переваг програмно-визначених мереж (SDN) є можливість повної автоматизації процесів управління віртуальними каналами. Створення, зміна чи видалення таких каналів більше не потребують складних ручних операцій або залучення великої кількості інженерів. Натомість цей процес може виконуватися заздалегідь визначеними політиками та сценаріями, що запускаються автоматично у відповідь на зміни навантаження, вимоги користувачів чи інциденти в мережі. Це значно знижує ризик людських помилок, скорочує час реагування і забезпечує безперервність сервісів навіть у складних динамічних умовах.

Розширені сценарії використання SDN

Міграція віртуальних машин. Одним із ключових сценаріїв є підтримка безшовного переміщення ВМ між ЦОД. У традиційній архітектурі для цього потрібно було вручну резервувати пропускну здатність, налаштовувати нові маршрути та гарантувати відсутність розриву з’єднань. SDN робить цей процес автоматичним: контролер самостійно забезпечує стабільні канали, оновлює таблиці

маршрутизації у режимі реального часу та синхронізує політики безпеки. Завдяки цьому міграція стає прозорою як для користувачів, так і для застосунків.

Підтримка безперервних сервісів. У випадках, коли компанія переміщує свої робочі навантаження між різними дата-центрами (наприклад, для оптимізації витрат чи підвищення відмовостійкості), виникає необхідність у збереженні активних TCP-з'єднань. SDN забезпечує динамічне перепрокладання маршрутів і дозволяє уникати будь-яких перебоїв у роботі сервісів. Користувачі продовжують працювати із системою без збоїв, навіть якщо у цей момент відбувається масштабна міграція додатків у хмарі.

Багатокористувацьке середовище. Особливістю хмарних ЦОД є одночасна робота великої кількості орендарів, кожен із яких має власні вимоги до продуктивності, безпеки та ізоляції даних. SDN дозволяє ефективно розподіляти ресурси, динамічно адаптуючи пропускну здатність і параметри QoS під конкретні навантаження. У цьому випадку ізоляція досягається програмними засобами, а отже, немає необхідності у складній конфігурації VLAN або використанні дорогих апаратних рішень.

Переваги SDN у між-ЦОД взаємодії

Головним досягненням SDN у сфері взаємодії між дата-центрами є поєднання високого рівня автоматизації з можливістю жорсткого централізованого контролю. Це дозволяє досягти кількох стратегічних цілей:

- **Безперервність обслуговування.** Завдяки автоматичному перемиканню маршрутів і підтримці захисних каналів навіть у випадках аварій чи пікових навантажень робота сервісів залишається стабільною.
- **Оптимізація витрат.** SDN робить можливим гнучке використання каналів різної пропускної здатності залежно від потреб у конкретний момент часу, що значно скорочує експлуатаційні витрати провайдерів і підприємств.
- **Покращення клієнтського досвіду.** Завдяки впровадженню механізмів самообслуговування користувачі можуть самостійно змінювати параметри каналів, масштабувати сервіси або замовляти додаткові ресурси, що підвищує рівень задоволеності клієнтів.

- **Масштабованість та адаптивність.** У сучасному бізнес-середовищі вимоги до інфраструктури змінюються дуже швидко. SDN забезпечує можливість гнучкого нарощування ресурсів, швидкого підключення нових сервісів і автоматичного коригування конфігурацій без потреби у тривалих ручних налаштуваннях.

2 КОНТРОЛЬ ТРАФІКУ В SDN

2.1 Віртуалізація мережевих функцій SDN

Віртуалізація як основа сучасних мережевих технологій

Ідея відокремлення застосунку від фізичного обладнання й перенесення його роботи у програмне середовище є наріжним каменем сучасної IT-інфраструктури. Якщо необхідний нам сервіс замість «заліза» запускається в ізольованому контейнері або віртуальній машині, ми маємо справу з його віртуалізацією. Концепція віртуалізації з’явилася ще у 60-х роках XX століття, коли інженери працювали над поділом ресурсів великих мейнфреймів між кількома незалежними завданнями. На початку 2000-х проблема постала знову, проте вже в іншій площині: потрібно було навчитися ефективно розподіляти ресурси серверів між численними клієнтами та сервісами.

Віртуалізація апаратних ресурсів принесла значні переваги. Використання кількох застосунків на одному фізичному сервері виявилося вигіднішим, ніж підтримка великої кількості виділених пристроїв: витрачається менше енергії, зменшується кількість необхідних мережевих портів і кабельних з’єднань, зростає компактність інфраструктури. Застосування шаблонів віртуальних машин дозволило відмовитися від прив’язки до апаратних рішень і водночас зберегти всі переваги готових «коробкових» продуктів. Розвиток гіпервізорів та систем управління дав змогу підвищити відмовостійкість, спростити масштабування й оптимізувати витрати. Саме завдяки віртуалізації з’явилося поняття «хмарних сервісів» і моделей SaaS, IaaS, PaaS, які кардинально змінили IT-ринок.

Втім, правила, що добре працюють у сфері програмного забезпечення, не завжди напряму застосовні до мережевої інфраструктури. Тут виникає проблема, яку покликана вирішити **NFV (Network Function Virtualization)**.

Обмеження традиційних мереж та завдання NFV

Сучасні телекомунікаційні мережі складаються з великої кількості спеціалізованого обладнання, де кожен пристрій виконує вузьку функцію: NAT,

контроль швидкості доступу, підрахунок трафіку, батьківський контроль, фільтрація контенту чи міжмережевий екран. Це історично зумовлено спеціалізацією виробників на певних функціях та використанням унікальних апаратних рішень, що мало спільного з серверами загального призначення. У результаті оператор змушений підтримувати велику кількість різнорідних «коробок». Запуск нової послуги потребує закупівлі, доставки, інсталяції та налаштування нового обладнання, що тягне за собою витрати на площі, електроживлення й людські ресурси.

Така модель створює серйозні обмеження для розвитку. Вона інертна, потребує значних інвестицій та не дозволяє гнучко масштабувати портфель послуг. У сучасних умовах мережа повинна бути динамічною: мати змогу швидко запускати нові сервіси, активувати їх за запитом користувача і так само швидко вивільняти ресурси після відключення. Саме тут віртуалізація мережевих функцій і програмно-визначені мережі працюють разом, утворюючи нову парадигму.

NFV та SDN: взаємодоповнюючі технології

NFV робить можливим перенесення функцій, які раніше виконувалися апаратними пристроями, у програмне середовище. Завдяки цьому NAT, DPI, брандмауери чи VPN-шлюзи можуть працювати як віртуальні модулі, розгорнуті у хмарі або в дата-центрі. Проте сама по собі NFV не забезпечує достатньої керованості й координації. Саме тут свою роль відіграє **SDN (Software Defined Networking)**.

Якщо NFV відповідає за перетворення апаратних функцій у програмні сервіси, то SDN надає механізми централізованого управління мережею, абстрагуючи її від фізичної топології. У зв’язці NFV+SDN мережа перетворюється на гнучке, програмоване середовище, у якому нові сервіси можуть розгортатися автоматично, керовані політики застосовуються миттєво, а ресурси вивільняються після відключення послуги без ручного втручання.

Межі віртуалізації мережевих функцій

Важливо зазначити, що не всі мережеві функції однаково придатні до віртуалізації. Наприклад, передавання даних (forwarding, routing, switching)

залишається складним для повного перенесення у програмне середовище. Це пояснюється тим, що копіювання пакетів із порту на порт у реальному часі вимагає спеціалізованих чипів (ASIC чи NPU), здатних виконувати операції у троїчній пам’яті TCAM з високою швидкістю та мінімальними затримками. Такі рішення працюють швидше й ефективніше за процесори загального призначення, споживають менше енергії та забезпечують високу щільність портів.

Спроба реалізувати ті самі функції на CPU загального призначення неминуче призвела б до втрати продуктивності: складні стеки введення-виведення створюють затримки, а фізичний сервер не здатний забезпечити необхідну кількість портів. Тому базові функції пересилання залишаються за апаратними пристроями, тоді як більш «інтелектуальні» завдання (маршрутизація на основі політик, шифрування, балансування навантаження, аналітика) можуть бути перенесені у віртуальне середовище.

Поєднання NFV та SDN відкриває шлях до створення мереж нового покоління. NFV забезпечує перенесення функцій із «заліза» у програму, а SDN дає централізоване управління і контроль за трафіком. Разом вони формують динамічну, масштабовану та економічно ефективну інфраструктуру, здатну швидко реагувати на запити користувачів і бізнесу. Такий підхід поступово витісняє традиційну модель, у якій кожна «коробка» виконувала лише одну функцію, і створює основу для гнучких хмарних платформ та телекомунікаційних систем майбутнього.

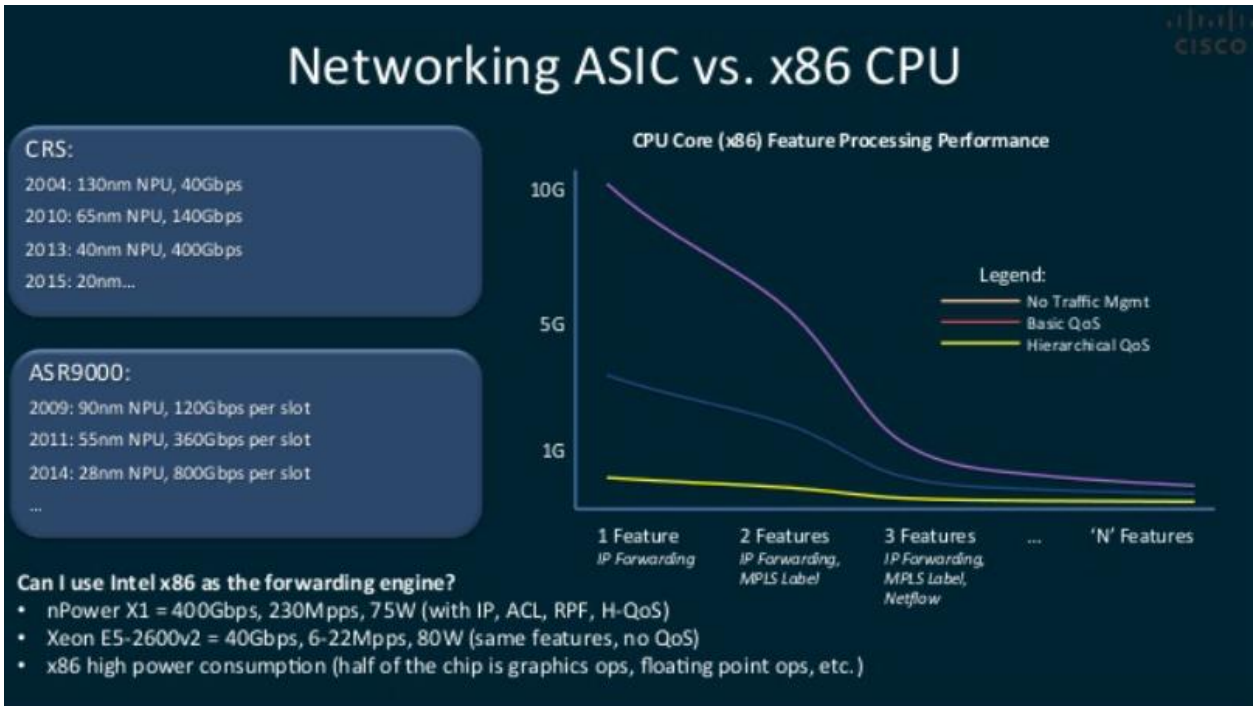


Рис. 2.1 Слайд Cisco про переваги NP, і про вплив фіч на продуктивність forwarding'a

У структурі сучасних телекомунікаційних мереж усі операції умовно поділяють на дві ключові площини — Data Plane та Control Plane. Data Plane охоплює всі процеси, пов’язані з безпосередньою передачею трафіку: пересилання пакетів, їх комутацію, маршрутизацію, фільтрацію та застосування базових правил обробки. Це рівень, де здійснюється найнижчий і найшвидший рівень взаємодії з даними, який забезпечує переміщення інформаційних потоків у режимі реального часу.

Натомість Control Plane відповідає за «інтелектуальну» складову мережі, тобто управління та координацію роботи Data Plane. До цієї площини належать протоколи виявлення сусідів, маршрутизаційні протоколи, алгоритми балансування навантаження, механізми запобігання петель, системи телеметрії, сервіси управління смугою пропускання, а також механізми аутентифікації, авторизації та обліку (AAA). Іншими словами, Control Plane формує правила та політики, за якими працює Data Plane, і надає мережі гнучкість та здатність адаптуватися до змін.

Віртуалізація мережевих функцій тісно пов’язана з цим поділом. Чим простіший функціонал Data Plane та чим складніший і насиченіший набір функцій Control Plane — тим легше й доцільніше переносити таку мережеву функцію у

програмне середовище. І навпаки: коли Data Plane є «важким» і потребує високої швидкодії, а Control Plane обмежується примітивними функціями, то віртуалізація такої задачі стає малоефективною, і краще залишати її виконання на спеціалізованому апаратному обладнанні.

Приклад віртуалізації на базі Customer Edge (CE) маршрутизаторів

Яскравим прикладом є маршрутизатори CE (Customer Edge), які встановлюються на межі мережі оператора та абонента. Вони виконують широкий спектр функцій у площині передачі даних. До основних завдань Data Plane у таких пристроях належать:

- базова маршрутизація та комутація пакетів;
- підтримка спеціальних методів маршрутизації, таких як **PBR (Policy-Based Routing)** чи **ABF (Access-Based Forwarding)**;
- робота зі списками контролю доступу (**ACL**) та підтримка складних сценаріїв безпеки, включаючи **Zone-Based Firewall**;
- підтримка різних стандартів інкапсуляції та тунелювання (**GRE, IPIP, MPLS, OTV**);
- реалізація трансляції адрес (**NAT, PAT**);
- застосування політик управління якістю обслуговування (**QoS**), серед яких policing, shaping, marking та scheduling.

У площині Control Plane CE-маршрутизатори також мають значний набір можливостей: від елементарних протоколів на кшталт ARP чи ND, до складних функцій рівня MPLS Traffic Engineering, які дозволяють гнучко управляти маршрутизацією та використанням ресурсів у масштабних мережах.

Навантаження таких пристроїв, які зазвичай обслуговують віддалені офіси або філії компаній, вимірюється десятками чи сотнями мегабіт за секунду. Цей рівень пропускної здатності робить їх надзвичайно зручними кандидатами для віртуалізації. На одному промисловому сервері можна розгорнути десятки віртуальних CE-маршрутизаторів, що дозволяє значно знизити витрати на обладнання, енергоспоживання та обслуговування, водночас забезпечивши гнучкість та централізоване управління.

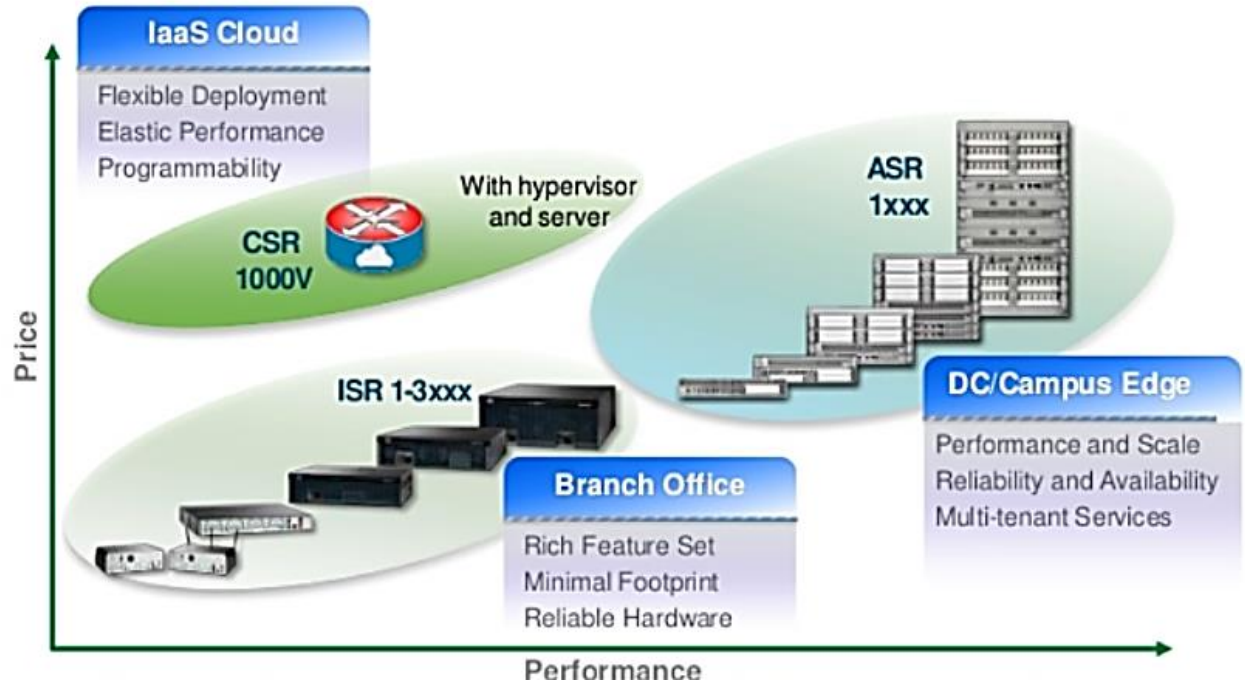


Рис. 2.2 Ніша для застосування віртуального CE-маршрутизатора Cisco CSR1000v щодо апаратних платформ

P/PE маршрутизатори та їхнє місце у віртуалізації мережевих функцій

Маршрутизатори рівня P (Provider) та PE (Provider Edge) є фундаментальними елементами операторських мереж. Вони мають схожий функціонал із CE-маршрутизаторами, проте відрізняються масштабом навантажень, які повинні опрацьовувати. Їхній Data Plane виконує обробку колосальних обсягів трафіку — від сотень гігабіт до десятків терабіт за секунду, забезпечуючи при цьому максимальну щільність портів. Такі пристрої будуються на базі високопродуктивних ASIC і NPU, здатних працювати в режимі максимальної продуктивності. Очевидно, що сервери традиційної архітектури не можуть впоратися з такими обсягами даних, тому віртуалізація Data Plane для маршрутизаторів операторського класу практично неможлива. Саме з цієї причини віртуалізація високопродуктивних комутаторів, які активно застосовуються у дата-центрах, також виглядає недоцільною — їхня роль залишається жорстко прив’язаною до фізичного обладнання.

Попри це, навіть такі «велетні» можуть частково інтегруватися у концепцію віртуалізації. Єдиним компонентом, який реально підлягає перенесенню у

програмне середовище, є Control Plane — або повністю, або частково. У цьому випадку вся обробка даних і пересилання пакетів залишаються за апаратною частиною, тоді як управління таблицями пересилання, маршрутизаційними політиками та сервісними функціями може здійснюватися зовнішніми системами. Це можуть бути як класичні SDN-контролери, що працюють за стандартом OpenFlow, так і оркестратори чи медіатори, які використовують інші інтерфейси взаємодії — CLI, NetConf, SNMP. Подібна архітектура поєднує продуктивність апаратного рівня з централізованим управлінням, яке робить мережу більш динамічною, контрольованою й придатною до автоматизації.

Яскравим прикладом є BGP Route Reflector, що відповідає за поширення таблиць маршрутизації у межах BGP-домену. Ця функція не потребує високопродуктивного Data Plane, а тому чудово підходить для віртуалізації. Проте навіть у великих операторських мережах таких елементів небагато, і вони не формують основу інфраструктури. Це ще раз підкреслює, що концепція NFV (Network Function Virtualization) більше стосується динамічних, абонентських сервісів масового використання — наприклад, NAT, VPN, Firewall чи DPI, — а не фундаментальних інфраструктурних вузлів, які відповідають за транзитні потоки терабітного масштабу.

У цьому контексті важливо розмежовувати ролі NFV та SDN. Якщо NFV орієнтована на перенесення мережевих функцій у програмне середовище, то SDN виконує роль інфраструктурної платформи, яка забезпечує централізоване управління і контроль. Винесений Control Plane у P/PE маршрутизаторах або комутаторах фактично виступає прикладом реалізації принципів SDN: зовнішня система програмує таблиці пересилання і задає політики, тоді як апаратний Data Plane забезпечує безпосередню обробку трафіку. У цьому випадку SDN та NFV не конкурують, а доповнюють одне одного: SDN забезпечує основу для координації, тоді як NFV відповідає за швидке розгортання та управління функціоналом, що не потребує надпотужної апаратної підтримки.

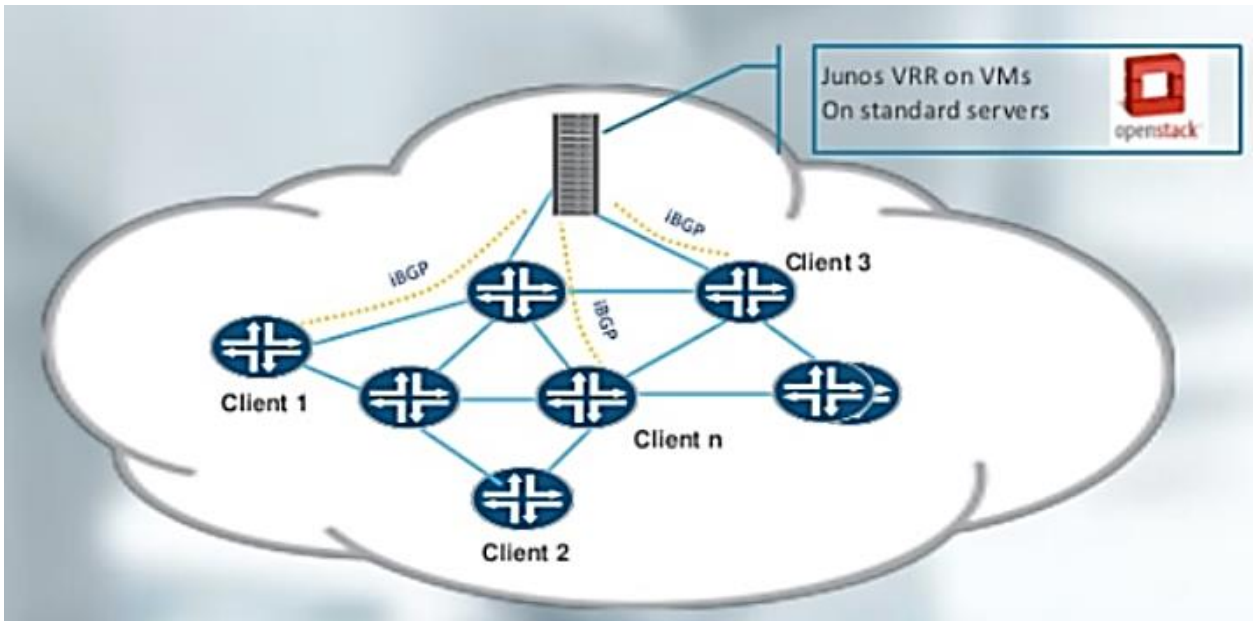


Рис. 2.3 Віртуалізований BGP Route-Reflector Juniper на стандартному сервері

Таким чином, маршрутизатори класу P/PE залишаються прикладом тієї категорії пристроїв, де віртуалізація Data Plane практично неможлива через масштаби навантажень, але віртуалізація Control Plane може надати значні переваги в управлінні й автоматизації. Це дозволяє інтегрувати операторські мережі у сучасну парадигму програмно-визначених мереж, поєднуючи високу продуктивність спеціалізованого обладнання з гнучкістю й адаптивністю програмного управління.

2.2 Технічні рішення для управління трафіком

CPE як основа абонентської мережі та перспективи його віртуалізації

Customer Premises Equipment (CPE), або абонентське обладнання, — це звична для кожного користувача невелика «коробочка», яку оператор встановлює вдома в абонента. Саме до цього пристрою підключається кабель провайдера, після чого він розподіляє інтернет на всі пристрої в помешканні, формуючи центральний вузол домашньої мережі. Зазвичай у складі такого обладнання функціонує DHCP-сервер для видачі локальних адрес, DNS-кешуючий сервер, а також клієнтські протоколи для взаємодії з мережею провайдера — PPPoE, L2TP, PPTP, DHCP,

802.1x. З боку Data Plane вирішальними залишаються такі функції, як NAT для трансляції адрес та Firewall для забезпечення базового рівня безпеки.

Традиційні вимоги до CPE незмінні вже багато років: пристрій має бути компактним, простим в експлуатації, надійним, привабливим за дизайном і водночас недорогим. Виробники давно уловили ці очікування ринку, тож сьогодні доступний широкий вибір пристроїв на будь-який смак і гаманець. До того ж, сучасні чипсети, що використовуються у CPE, мають досить високу обчислювальну потужність. Це дозволяє апаратно реалізовувати ресурсоємні функції, наприклад NAT чи комутацію, забезпечуючи високу продуктивність навіть у бюджетних моделях.

Обмеження сучасних CPE для операторів

Попри численні переваги, традиційні CPE дедалі частіше не відповідають вимогам операторів зв'язку. Це пояснюється низкою факторів:

- **Брак функціональності.** Провайдер часто не має доступу до інформації про стан пристрою чи рівень його завантаження. Це перетворює CPE на «чорну скриньку», яка може стати вузьким місцем у мережі.
- **Відсутність прозорості.** Оператор не бачить структури локальної мережі абонента й не може централізовано керувати налаштуваннями обладнання, що ускладнює підтримку та діагностику.
- **Гальмування інновацій.** Нестача необхідних функцій робить запуск нових послуг довготривалим і проблематичним.
- **Несвоєчасне оновлення ПЗ.** Прошивки CPE часто оновлюються із запізненням, що створює додаткові ризики з точки зору безпеки та стабільності роботи мережі.

Усе це означає, що традиційний підхід із локальним CPE у квартирі користувача стає дедалі менш ефективним і стримує розвиток нових сервісів.

Віртуалізація CPE: майбутнє абонентських сервісів

У найближчому майбутньому очікується переосмислення ролі CPE. З появою нових сервісів — таких як батьківський контроль, онлайн-кінотеатри, «розумний дім», резервне копіювання та реплікація даних, зберігання і перегляд відео з

домашніх камер спостереження, освітні сервіси на кшталт «шкільного робочого столу» — класичні CPE вже не здатні задовольнити всі потреби ринку.

Вирішальним кроком стане впровадження концепції віртуалізованого CPE (vCPE). У цій моделі фізичний пристрій, що залишається у квартирі абонента, матиме лише мінімальний набір функцій: базове підключення до мережі провайдера й пересилання трафіку у віртуальне середовище. Основні ж сервіси та мережеві функції оброблятимуться у vCPE-контейнері, розгорнутому на інфраструктурі оператора. Саме через цей контейнер проходитиме абонентський трафік, і саме там надаватимуться додаткові послуги.

Така архітектура відкриває нові можливості:

- оператор отримує повний контроль над усіма мережевими функціями та може централізовано керувати налаштуваннями;
- діагностика й усунення несправностей значно спрощуються;
- нові сервіси впроваджуються без фізичного втручання у мережу абонента;
- з’являється потенціал для нової моделі тарифікації, де об’єктом обліку виступатиме не лише обсяг трафіку, а й використані обчислювальні чи дискові ресурси.

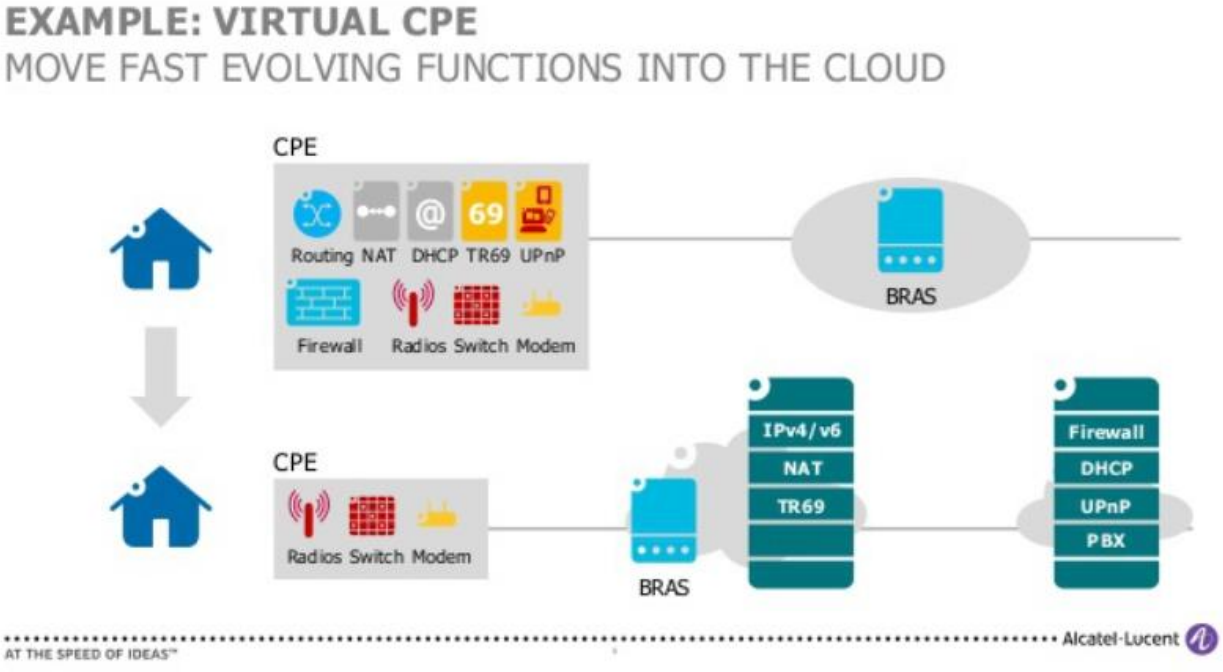


Рис. 2.4 Ілюстрація перенесення мережевих функцій із CPE-пристрою в хмару на прикладі Alcatel

BNG/BRAS, або широкосмугові шлюзи доступу, є ключовими елементами операторських мереж, адже саме через них абоненти отримують вихід в Інтернет. Ці пристрої виконують роль центральної точки контролю за наданням послуг, здійснюючи «дозування» трафіку та облік використання ресурсів згідно з тарифними планами. Вони відповідають за авторизацію кожного користувача через систему AAA за протоколом RADIUS, отримання індивідуальних атрибутів і правил для сесій та створення для кожного абонента унікального сервісу зі своїми політиками доступу, класами якості обслуговування, обмеженнями та правилами обліку. Це означає, що саме на рівні BNG формується персоналізований інтернет-доступ, де у кожної сесії є власні параметри адресації, ACL та QoS.

Такі маршрутизатори обробляють десятки й сотні тисяч одночасних підключень, тому мають витримувати колосальні обчислювальні навантаження. Вони працюють із протоколами ARP, ND, PPP, LCP, DHCP, керуючи сигналізацією великої кількості абонентських пристроїв, а також відстежують тривалість кожної сесії, кількість переданого трафіку та відповідність його тарифним умовам. BNG ухвалює рішення, кому надати доступ до Інтернету, кого перенаправити на портал авторизації, кому обмежити чи навпаки збільшити швидкість. Відповідно, контрольна площина таких пристроїв повинна бути надзвичайно продуктивною. У них використовуються мережеві процесори ще складніші, ніж у P/PE маршрутизаторів, оскільки вони виконують не лише пересилання пакетів, а й складну обробку даних у режимі реального часу.

Кожна абонентська сесія програмується у мережевий процесор, отримуючи власні лічильники, правила та класифікатори. Це потребує використання сотень тисяч апаратних лічильників, величезних обсягів спеціалізованої пам’яті, зокрема TCAM для зберігання класифікаторів і списків доступу, а також швидкісної пам’яті для організації черг. У випадках, коли застосовуються технології доступу з тунелюванням, такі як L2TP чи PPPoE, на BNG покладаються ще й завдання енкапсуляції та декапсуляції трафіку, що додатково збільшує складність роботи. Чим більше операцій виконується над пакетом, тим вагоміші переваги має спеціалізований ASIC перед універсальними процесорами архітектури x86.

Попри це, ідея віртуалізації BNG усе ж має перспективу у нішевих сценаріях. Якщо мова йде не про обробку терабітних потоків, а про роботу з меншими обсягами даних — на рівні кількох гігабіт на секунду, — то віртуалізований BNG може бути цілком ефективним. Це особливо актуально в умовах високої динаміки сервісів і великої кількості сесій із частими подіями підключення та відключення. Яскравим прикладом є мережі Wi-Fi у транспорті — літаках, поїздах чи автобусах. Тут обсяги трафіку невеликі, проте важлива швидкість і гнучкість обробки, а також можливість інтегрувати додаткові сервіси, такі як банерна реклама чи мультимедійні платформи. Такі рішення можна розгортати разом із vBNG на тому самому серверному кластері, зменшуючи витрати на обладнання та водночас розширюючи спектр послуг.

Таким чином, BNG/BRAS є одним із найбільш складних і навантажених елементів телекомунікаційної інфраструктури. Вони поєднують у собі функції маршрутизатора, контролера політик і системи обліку послуг, виконуючи одночасно обробку трафіку та управління абонентськими сесіями. Для магістральних мереж із величезними потоками даних їхня повна віртуалізація наразі малоймовірна, адже апаратні можливості залишаються критично важливими. Водночас у сегментах із відносно невеликими обсягами трафіку та високими вимогами до динамічності сервісів віртуалізований BNG здатен стати оптимальним рішенням, яке поєднує переваги NFV та SDN, надаючи операторам гнучкість і можливість швидко адаптуватися до потреб ринку.

NAT (Network Address Translation), або трансляція мережевих адрес, в останні десятиліття стала однією з найважливіших функцій у сучасних мережах. Причиною цього є гострий дефіцит публічних IP-адрес, якими можуть оперувати оператори зв’язку. Якщо ще десять років тому NAT здебільшого застосовувався у корпоративному (Enterprise) та сегменті SMB, то сьогодні ця функція стала звичною і для операторських мереж (SP-сегменту). NAT належить до найбільш ресурсоємних завдань площини передачі даних (Data Plane), оскільки для його виконання необхідно одночасно відстежувати й обробляти величезну кількість сесій. Наприклад, відкриття лише однієї сучасної вебсторінки з великою кількістю

медіаоб’єктів здатне створити та закрити сотні записів у таблицях NAT. У свою чергу, клієнти файлообмінних мереж, зокрема P2P-сервісів, можуть генерувати тисячі трансляцій на кожен мегабіт пропускної здатності, що значно збільшує навантаження на пристрій.

Для розв’язання цієї проблеми виробники впровадили так звані режими Carrier-Grade NAT (CGNAT), що дозволили значно підвищити масштабованість і продуктивність. Проте, навіть із такими оптимізаціями, виконання NAT на звичайних мережевих процесорах сьогодні залишається радше винятком. У більшості випадків для таких завдань використовуються спеціалізовані високопродуктивні серверні модулі, які встановлюються безпосередньо у центральні маршрутизатори. Завдяки інтеграції в backplane маршрутизатора вони сприймаються як звичайні лінійні карти й працюють із максимальною ефективністю. Яскравим прикладом може слугувати мультисервісний маршрутизатор Huawei ME-60 з модулем SFU, на якому реалізується функція CGNAT.

Важливою особливістю NAT є його так звана «товщина». Цю функцію можна теоретично поділити на дрібніші елементи шляхом сегментації пулу адрес, проте такий підхід робить її менш ефективною. Чим більш централізованим залишається NAT, тим раціональніше використовуються доступні адресні ресурси. Водночас саме ця «товщина» робить NAT цікавим прикладом для впровадження концепції розподіленої NFV (dNFV). У такій архітектурі логічна централізація (єдиний пул адрес, єдина точка управління) поєднується з фізичною розподіленістю, коли вузли з функціями NAT розташовуються топологічно ближче до трафіку, що обслуговується. Це дає змогу зменшити затримки, рівномірно розподіляти навантаження й одночасно зберігати централізований контроль.

Функціонал мережевої безпеки має багато спільного з NAT. До нього належать Stateful Firewall, NGFW, IDS, IPS, антивірусні та антиспам-системи. Вони також характеризуються високою динамікою станів, інтенсивним використанням пам’яті та значним навантаженням на процесори. Але на відміну від NAT, функції безпеки можна масштабувати набагато дрібніше — аж до рівня, коли на одного

абонента виділяється окремий контейнер. Це робить безпекові сервіси одним із найбільш очевидних прикладів для реалізації через NFV, оскільки вони добре поєднують вимоги до гнучкості, масштабованості та адаптивності.

Ще однією яскравою ілюстрацією потенціалу NFV є DPI (Deep Packet Inspection) — глибока інспекція пакетів, яка дозволяє операторові визначати або обмежувати рівень сервісу для конкретних додатків чи типів трафіку. DPI може використовуватися для реалізації таких послуг, як «батьківський контроль», коли весь абонентський трафік проходить через фільтри, що класифікують ресурси та ухвалюють рішення щодо доступу. На відміну від NAT, DPI здебільшого реалізується програмними засобами. Водночас продуктивність, цікава для оператора, може починатися вже з невеликих масштабів, що робить DPI одним із найбільш перспективних сценаріїв для NFV.

До важливих прикладів належить і IMS (IP Multimedia Subsystem), який використовується для надання голосових послуг, телебачення, потокового відео, сервісів миттєвих повідомлень і мультимедійних додатків, таких як відеоспостереження чи інтерактивні меню. IMS органічно вписується у портфоліо операторських послуг і може бути ефективно реалізований у рамках віртуалізованих рішень.

Окрему категорію складають інфраструктурні елементи мобільних мереж GSM/UMTS/LTE/WiFi: бездротові контролери, EPC, IMS, CSN, SMSC, PCC, GWc, GWu, PGW, SGW, HSS, PCRF. Для цих компонентів характерні високі вимоги до обчислювальних ресурсів, хоча обсяг трафіку, який вони обробляють, часто є відносно помірним. Лише деякі з них мають специфічні обмеження, пов’язані з параметрами QoS, проте загалом їх також можна успішно інтегрувати в середовище NFV.

Для повноти картини варто згадати і прикладні сервіси, такі як DHCP, DNS, HTTP-сервери, HTTP Proxy (з оптимізаторами, прискорювачами та URL-фільтрами), SIP Proxy тощо. Хоча їх іноді відносять до прикладного рівня моделі OSI, вони є важливою складовою мережевої інфраструктури. Ці сервіси легко

віртуалізуються, активно затребувані та здатні стати «будівельними блоками» для формування послуг нового покоління.

Таким чином, NAT, функції безпеки, DPI, IMS та інші прикладні й інфраструктурні сервіси утворюють широкий спектр завдань, які можна ефективно реалізувати за допомогою NFV. Вони демонструють, як поєднання гнучкості програмного забезпечення та масштабованості операторських рішень здатне радикально змінити підхід до побудови телекомунікаційних мереж.

2.3 Архітектура та розвиток NFV

На сьогодні вже достатньо чітко зрозуміло, які мережеві функції можна віртуалізувати та як вони можуть працювати окремо. Однак цього недостатньо для побудови повноцінної системи — головним завданням стає з’ясування того, яким чином усі ці функції можна комбінувати між собою у межах єдиного середовища, як гарантувати ізоляцію мережевих з’єднань між різними віртуальними елементами, забезпечити належний рівень безпеки, масштабованості та відмовостійкості. Не менш важливими є й практичні питання прозорості управління, вибору обчислювального та мережевого обладнання, його правильної конфігурації та інтеграції в існуючу інфраструктуру оператора. Саме пошук відповідей на ці проблеми у 2013 році став причиною створення робочої групи під егідою Європейського інституту зі стандартизації у сфері електрозв’язку (ETSI). Ініціаторами виступили сім провідних світових операторів — AT&T, BT, Deutsche Telekom, Orange, Telecom Italia, Telefonica та Verizon, які усвідомили, що лише спільними зусиллями можна виробити універсальні підходи та правила для побудови віртуалізованих мереж нового покоління.

Надалі до цієї ініціативи приєдналися десятки провідних виробників телекомунікаційного обладнання та програмного забезпечення. Так виникла спільнота NFV ISG, що сьогодні налічує вже кілька сотень учасників і стала центральним майданчиком для узгодження вимог, обміну досвідом та формування стандартів. На базі мереж операторів-учасників було організовано низку тестових

полігонів, де перевірялись практичні сценарії застосування NFV, розподілялися теми досліджень та аналізувались найбільш складні й перспективні напрямки. Результати таких експериментів ретельно фіксувались, обговорювались у відкритому середовищі, узагальнювались у вигляді звітів, після чого ставали основою для формування нових дослідницьких питань. Якщо на перших етапах концепція NFV виглядала доволі розмитою і бракувало конкретних механізмів реалізації, то вже через кілька років завдяки накопиченим матеріалам і публікаціям почала вимальовуватись більш чітка та структурована «мозаїка» майбутнього стандарту.

Варто зазначити, що практичний досвід пілотних упроваджень NFV часто одразу поширювався серед інших операторів і навіть копіювався «як є», без суттєвих змін. Це відбувалося попри пропрієтарність окремих рішень та відсутність єдиного відкритого стандарту. Виробники мережевого обладнання та програмних платформ, прагнучи завоювати частку цього нового ринку, почали пропонувати не лише окремі віртуалізовані елементи, а й комплексні рішення різного масштабу та ступеня готовності. Таким чином, NFV почала переходити з розряду експериментальних досліджень у практичну площину.

Справжнім поштовхом до розвитку стала поява у 2014 році відкритої ініціативи від Linux Foundation, яка започаткувала проєкт OPNFV (Open Platform for NFV). Його головною метою було стимулювати використання відкритих рішень та продуктів з відкритим кодом у сфері NFV, що дозволяло уникнути залежності від пропрієтарних систем. У рамках цієї платформи було запропоновано цілу низку базових компонентів: Open vSwitch та OpenDaylight як програмні мережеві рішення, OpenStack як система управління віртуалізацією, Ceph як децентралізоване сховище даних, KVM у ролі гіпервізора, а також операційні системи на базі Linux для хостового та гостьового середовища. Уже перший реліз платформи під назвою Arno став доказом життєздатності підходу і визначив курс на стандартизацію.

Активності у сфері стандартизації NFV вийшли далеко за межі ETSI. Вони охопили також інші відомі галузеві організації, серед яких MEF та TM Forum, які

зосереджуються на узгодженні моделей сервісів, методів управління та інтеграції віртуалізованих функцій у більш широкі бізнес-процеси. Усе це підкреслює, що NFV поступово перетворюється на глобальний стандарт галузі, який підтримується як провайдерами та вендорами, так і міжнародною open-source спільнотою.

Таким чином, еволюція NFV від перших дискусій до створення широких альянсів і практичних пілотів демонструє, що ця технологія вже вийшла за межі теорії. Вона формує основу нової парадигми розвитку телекомунікаційних мереж, де програмна гнучкість, відкрита архітектура та підтримка з боку індустрії забезпечують умови для масштабного переходу до віртуалізованої інфраструктури наступного покоління.

Архітектура та основні компоненти NFV

Концепція NFV (Network Functions Virtualization), запропонована та формалізована в рамках специфікацій ETSI, побудована на багаторівневій архітектурі, яка складається з трьох основних компонентів. Кожен із них виконує чітко визначену роль і водночас взаємодіє з іншими, утворюючи єдиний комплекс для реалізації сучасних телекомунікаційних сервісів. Така архітектура забезпечує не лише гнучкість і масштабованість мереж, а й їхню керованість, динамічність та економічну ефективність.

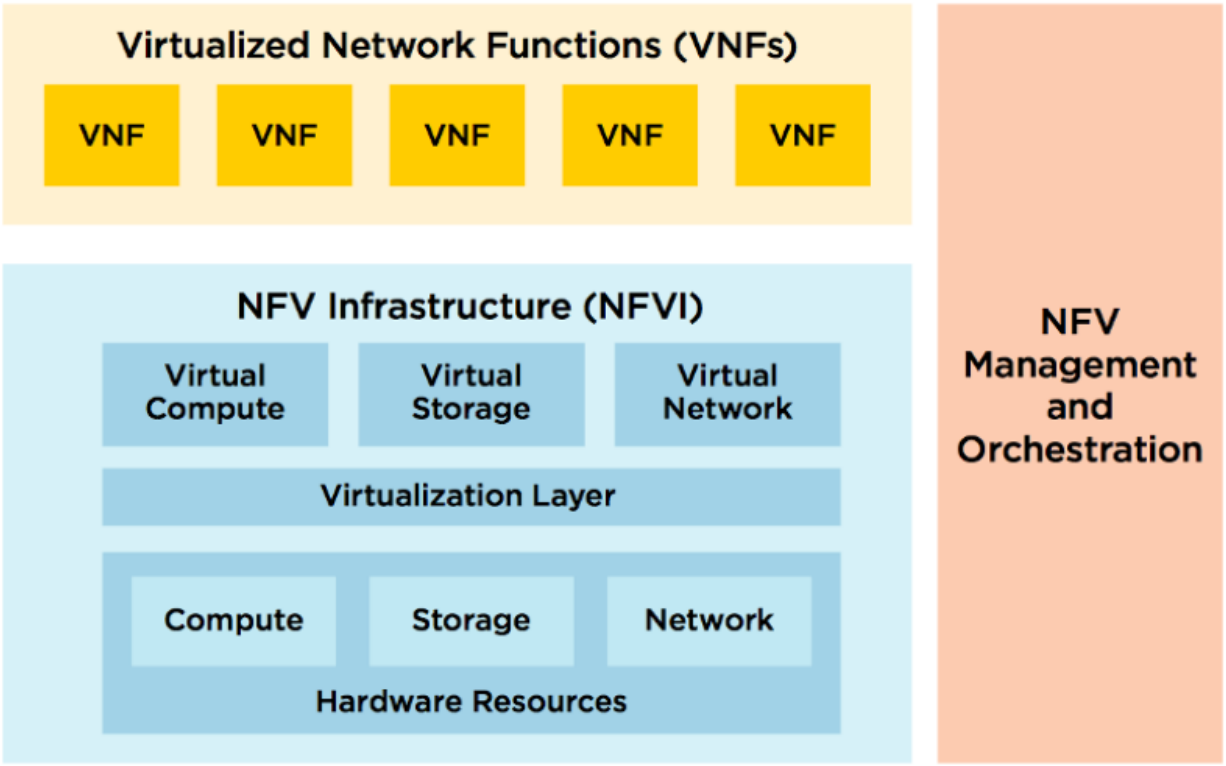


Рис. 2.5 Три основні компоненти NFV

1. Virtualized Network Functions (VNF).

На верхньому рівні розташовані віртуалізовані мережеві функції — VNF, які є центральним об’єктом усього підходу NFV. Це ті самі мережеві сервіси, які традиційно виконувались спеціалізованим апаратним обладнанням: маршрутизація, NAT, брандмауери, системи DPI, VPN-шлюзи, балансувальники навантаження тощо. У моделі NFV ці функції реалізуються у вигляді програмного забезпечення, що працює у віртуальному середовищі — зазвичай на базі віртуальних машин або контейнерів. VNF може складатися як із одного віртуального екземпляра, так і з цілого комплексу взаємопов’язаних машин, які спільно забезпечують виконання складнішої функції.

Для того щоб ці функції могли бути ефективно керовані, масштабовані та динамічно налаштовувані, у їхній структурі передбачений додатковий елемент — Element Management System (EMS). EMS відповідає за моніторинг роботи кожної функції, збір статистики, централізоване керування параметрами та автоматичну реакцію на події в мережі. Таким чином, EMS стає проміжною ланкою між операторськими системами управління та власне віртуалізованими функціями,

дозволяючи швидко змінювати політики чи параметри сервісів без необхідності втручання у фізичне обладнання.

2. NFV Infrastructure (NFVI).

На протилежному боці архітектури розташована інфраструктура NFV (NFVI). Це сукупність фізичних і віртуальних ресурсів, які забезпечують основу для виконання всіх VNF. До фізичних ресурсів належать сервери, системи зберігання даних, мережеві пристрої та комутатори. Віртуальні ресурси представлені гіпервізорами, системами віртуалізації, віртуальними комутаторами та програмними механізмами управління ресурсами.

Головною функцією NFVI є створення універсальної, масштабованої й гнучкої інфраструктури, здатної одночасно підтримувати десятки чи навіть сотні різних VNF. Вона повинна гарантувати виділення ресурсів у потрібному обсязі, забезпечувати балансування навантаження, ізоляцію середовищ, підтримку високої доступності й відмовостійкості. Таким чином, NFVI формує «фундамент» архітектури, на якому ґрунтується робота всієї системи.

3. NFV Management and Orchestration (MANO).

Над обома попередніми компонентами розташовується система MANO (Management and Orchestration). Вона є «керуючою обв’язкою», яка відповідає за управління життєвим циклом усіх віртуалізованих функцій, а також за конфігурацію й моніторинг інфраструктури. У структурі MANO виділяються окремі менеджери, які відповідають за управління VNF (VNF Manager) та NFVI (Virtualized Infrastructure Manager, VIM). Над ними знаходиться оркестратор, який виконує ключову роль: він узгоджує зміни між різними доменами системи, розподіляє ресурси відповідно до потреб сервісів, ініціює розгортання нових функцій, забезпечує їхнє масштабування та взаємодію.

Оркестратор MANO фактично є «мозковим центром» NFV-домену. Він забезпечує гнучкість у керуванні сервісами, дозволяє автоматично активувати чи деактивувати певні функції, інтегрує нові послуги та підтримує політики якості обслуговування (QoS). Його можливості критично важливі для того, щоб оператор міг швидко

реагувати на зміну попиту абонентів і одночасно оптимізувати використання своїх ресурсів.

Інтеграція з OSS/BSS.

Над усією архітектурою NFV знаходяться традиційні операторські системи OSS (Operations Support Systems) та BSS (Business Support Systems). До них належать системи моніторингу та управління мережею, білінгові платформи, інструменти провіжнінгу послуг, а також абонентські портали самообслуговування. NFV може інтегруватися з цими системами як через MANO — у вигляді єдиного комплексного рішення, так і безпосередньо через інтерфейси VNF та NFVI. Завдяки цьому оператори отримують можливість не лише управляти віртуалізованими функціями, але й органічно включати їх у власну бізнес-екосистему.

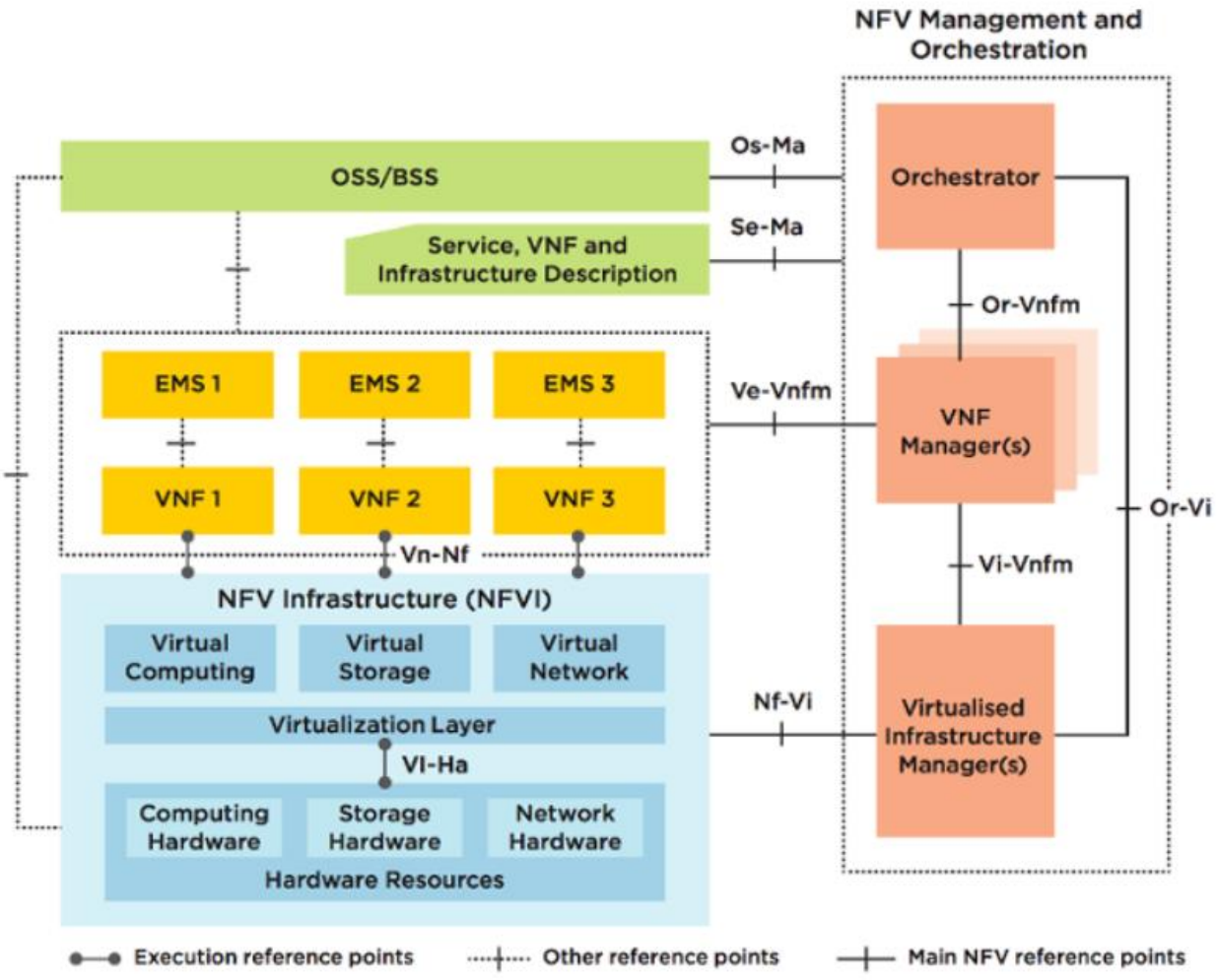


Рис. 2.6 Інтеграція з OSS/BSS

Завдяки такій архітектурі NFV стає ключовим інструментом для еволюції телекомунікаційних мереж. VNF забезпечує функціональність на рівні сервісів,

NFVI формує ресурсну базу, MANO виконує координацію та управління, а OSS/BSS дозволяють інтегрувати рішення в бізнес-процеси оператора. У комплексі це створює передумови для появи абсолютно нового покоління мереж — більш гнучких, керованих програмно, здатних швидко адаптуватися до потреб користувачів та відкривати шлях до впровадження сервісів, які раніше були технічно чи економічно недосяжними.

3 КОНТРОЛЕР КЕРУВАННЯ ТРАФІКУ ДЛЯ T-SDN

3.1 Структура мережі

Сьогодні вже складно здивувати когось стартапами чи інноваційними проєктами у сфері software-defined networks (SDN). Цей напрям активно розвивається як зусиллями найбільших світових корпорацій, так і завдяки ентузіазму відкритих спільнот open source, які формують величезний масив знань, бібліотек і готових інструментів.

Втім, ще донедавна практично всі дослідження та впровадження зосереджувалися на інфраструктурі дата-центрів. Саме там SDN першочергово проявила свій потенціал: централізоване управління, швидке масштабування, ізоляція трафіку та автоматизація стали критично важливими у середовищі, де постійно змінюється профіль навантажень. Разом із тим, для транспортних мереж (transport networks), які характеризуються значно більшою протяжністю, складнішою структурою та жорсткішими вимогами до відмовостійкості, можливість застосування концепції SDN ще кілька років тому викликала великі сумніви.

Ситуація почала змінюватися у жовтні 2015 року, коли компанія NetCracker здійснила розгортання контролера T-SDN (Transport Software-Defined Network) у мережі одного з провідних європейських операторів. Це стало важливим підтвердженням того, що принципи, апробовані в дата-центрах, можуть ефективно працювати й у масштабах магістральних транспортних систем. Контролер дозволив автоматизувати значну частину рутинних операцій, які раніше виконувалися вручну інженерами. В результаті оператор зміг зекономити сотні людино-годин, які раніше витрачалися на налаштування обладнання, маршрутизацію потоків та виділення сервісів для клієнтів. Ефект від цього виявився не лише у скороченні витрат часу та ресурсів, а й у підвищенні стабільності та прогнозованості роботи всієї мережі.

Архітектура та структура тестової мережі

В основі інфраструктури були використані ключові елементи сучасних оптичних систем. Усередині доменів функціонували плати ROADM/WSS (Reconfigurable Optical Add-Drop Multiplexer / Wavelength Selective Switch). Ці пристрої виступають гнучкими оптичними мультиплексорами введення-виведення, які дозволяють у режимі реального часу змінювати маршрути проходження сигналів між вузлами. Їх застосування забезпечує можливість перебудови топології без фізичного втручання, створюючи умови для гнучкого управління трафіком, швидкої реакції на аварійні події та динамічного балансування навантаження.

Міждоманні з'єднання формувалися за допомогою клієнтських портів, інтегрованих у спеціалізовані плати — транспондери. Оптичний транспондер виступає своєрідним мостом між обладнанням абонентського або прикладного рівня та мультиплексованою лінією WDM (Wavelength Division Multiplexing). У випробуваннях застосовувалися транспондери з десятьма клієнтськими інтерфейсами зі швидкістю 10 Гбіт/с кожен (відповідно до стандарту IEEE 802.3ae), а також з агрегуючим каналом ODU4.

ODU (Optical Data Unit) — це стандартизований контейнер, який транспортує дані у межах OTN (Optical Transport Network). Він забезпечує контроль якості передачі, синхронізацію, виправлення помилок та відстеження параметрів на всьому маршруті. Саме завдяки контейнеризації OTN вдалося забезпечити універсальність і сумісність для різних типів сервісів та протоколів.

Тестова мережа продемонструвала значний потенціал: одне фізичне оптичне волокно могло одночасно транспортувати до 80 ODU-контейнерів, кожен зі швидкістю 100 Гбіт/с. Загальна пропускна здатність у такій конфігурації сягала 8 Тбіт/с на одне волокно. Це яскраво демонструє можливості масштабування, які відкриває інтеграція технологій OTN і SDN, роблячи транспортні мережі здатними відповідати на виклики майбутнього зростання трафіку.

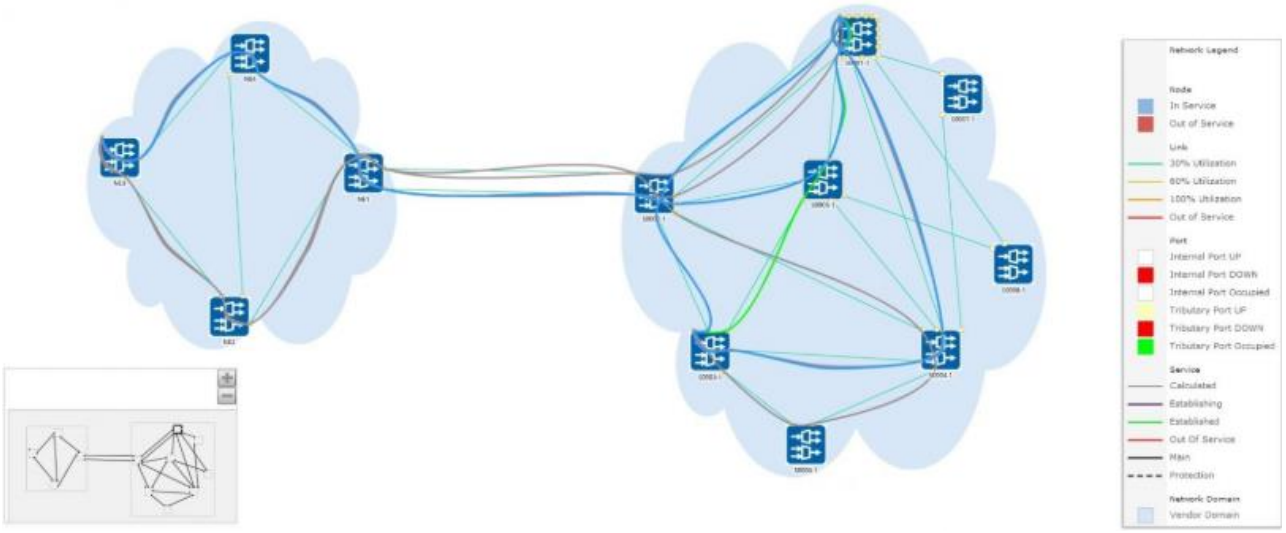


Рис. 3.1 Тестова мережа

Таким чином, впровадження T-SDN стало підтвердженням зрілості підходу SDN для магістральних оптичних систем. Поєднання ROADM/WSS, транспондерів та контейнерів ODU забезпечило не лише високі швидкості передавання, а й гнучке керування топологією та ресурсами. Це дає змогу операторам оптимізувати роботу мережі, прискорювати розгортання нових сервісів, а також зменшувати витрати на експлуатацію. У перспективі подібні рішення стануть основою для розвитку глобальних транспортних мереж наступного покоління.

Контролер на основі T-SDN відкрив нові можливості для управління транспортними мережами, реалізувавши функціонал, який раніше вимагав значних витрат часу та зусиль з боку інженерів. Серед ключових можливостей, які він підтримує, варто відзначити:

- **автоматичне прокладання сервісу** за запитом клієнта, що дозволяє у найкоротші терміни створювати необхідні з’єднання без ручного втручання;
- **автоматичне перемикання на захисний маршрут** у випадку відмови порту чи вузла, або ж динамічний перерахунок шляху, якщо обладнання не підтримує стандартні механізми резервування;
- **постійну систему моніторингу** стану мережі, включно з відстеженням помилок та оперативним інформуванням адміністраторів.

Концепція та архітектура T-SDN

Щоб зрозуміти сутність T-SDN, необхідно підкреслити, що вона базується на ключових принципах SDN, відпрацьованих у дата-центрах, але перенесених у масштаб транспортних мереж. Головна ідея полягає у розділенні площини передачі даних (Data Plane) та площини управління (Control Plane). Це розділення дає змогу створювати єдиний централізований контролер, який координує роботу всіх пристроїв у межах певного домену мережі.

Над контролером функціонує рівень застосунків (SDN Application Layer), який взаємодіє з ним через стандартизовані інтерфейси. Завдяки цьому користувачі та оператори отримують можливість керувати транспортною мережею на вищому рівні абстракції: формулювати політики, задавати правила та отримувати необхідні послуги без складних операцій налаштування обладнання.

Контролер, володіючи повною інформацією про структуру та ресурси мережі, здатний виконувати низку завдань значно ефективніше, ніж класичні протоколи управління. Деякі з цих функцій вже частково реалізовані традиційними технологіями, проте T-SDN надає змогу підняти їх на якісно новий рівень, зробивши процес управління динамічним, автоматизованим і більш надійним.

Переваги та нові можливості T-SDN

1. **Спрощення взаємодії з транспортною мережею.**

   Уявімо ситуацію, коли замовлення мережевого сервісу стає для клієнта настільки ж простим, як купівля товару в інтернет-магазині. Користувач формує запит, а контролер у автоматичному режимі переналаштовує всю інфраструктуру: визначає маршрут, виділяє необхідні ресурси, налаштовує пристрої. В результаті клієнт отримує сервіс за лічені хвилини, а не дні чи тижні, як це часто відбувається у класичних моделях.

2. **Оптимальне використання пропускної здатності.**

   Ефективна утилизація каналів — завдання, над яким працюють інженери десятиліттями. У транспортних мережах, де пропускна здатність є надзвичайно дорогоцінним ресурсом, воно набуває особливого значення. Проте універсального механізму для динамічного розподілу ресурсів між клієнтами досі не існує. T-SDN здатна вирішити цю проблему: контролер у

режимі реального часу аналізує завантаженість каналів, визначає резерви та перенаправляє трафік, мінімізуючи ризик перевантаження та простоїв.

Розглянемо випадок, коли трафік між двома оптичними пристроями, умовно позначеними як A та B, може передаватися кількома шляхами. Контролер відстежує, яка частина каналу вже використана (відображена червоним кольором на графіку), а яка залишається вільною (зелений колір). На схемі це можна зобразити так: блакитний пунктир — оптичне волокно, чорні лінії — клієнтський канал. Завдяки такому моніторингу контролер здатний балансувати навантаження, перемикаючи трафік у вільні сегменти й забезпечуючи рівномірний розподіл ресурсів.

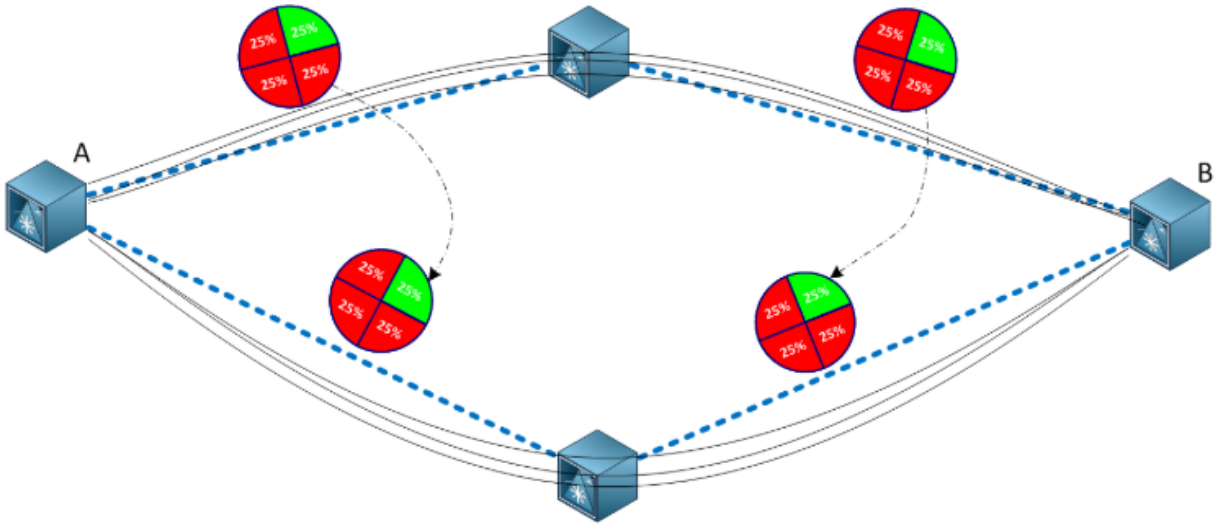


Рис. 3.2 Передача трафіку між двома оптичними пристроями

Уявімо ситуацію, коли оператору транспортної мережі необхідно організувати новий клієнтський канал, який за своєю ємністю значно перевищує вже наявні з’єднання й потребує не менше ніж 50% пропускної здатності магістралі. У класичній архітектурі це могло б стати серйозним викликом, адже для виділення таких ресурсів довелося б або додавати нові фізичні канали, або проводити складні переналаштування всієї мережевої інфраструктури.

Однак у випадку використання T-SDN можливий більш гнучкий підхід. Контролер, маючи повну картину завантаження мережі в режимі реального часу, здатний перебудувати маршрути існуючих потоків так, щоб вивільнити потрібний обсяг ресурсів. Наприклад, один із вже активних клієнтських каналів, який раніше

проходив по верхньому маршруту, може бути автоматично перенаправлений на альтернативний, нижній шлях. Це дозволяє вивільнити приблизно половину смуги пропускання на початковому сегменті й створити простір для розміщення нового, більш ємного каналу.

Такий підхід забезпечує одразу кілька переваг:

- уникається потреба у фізичному розширенні мережі;
- зберігається баланс навантаження між різними сегментами транспортної інфраструктури;
- мінімізуються затримки під час надання нового сервісу клієнту — ресурс виділяється фактично миттєво;
- оператор отримує можливість значно підвищити ефективність використання наявних каналів.

У підсумку приклад із новим каналом, що займає 50% пропускної здатності, демонструє практичну цінність T-SDN: завдяки інтелектуальному контролеру і гнучкому управлінню топологією транспортна мережа перетворюється на адаптивне середовище, здатне швидко реагувати на зростаючі потреби користувачів без додаткових капіталовкладень у обладнання.

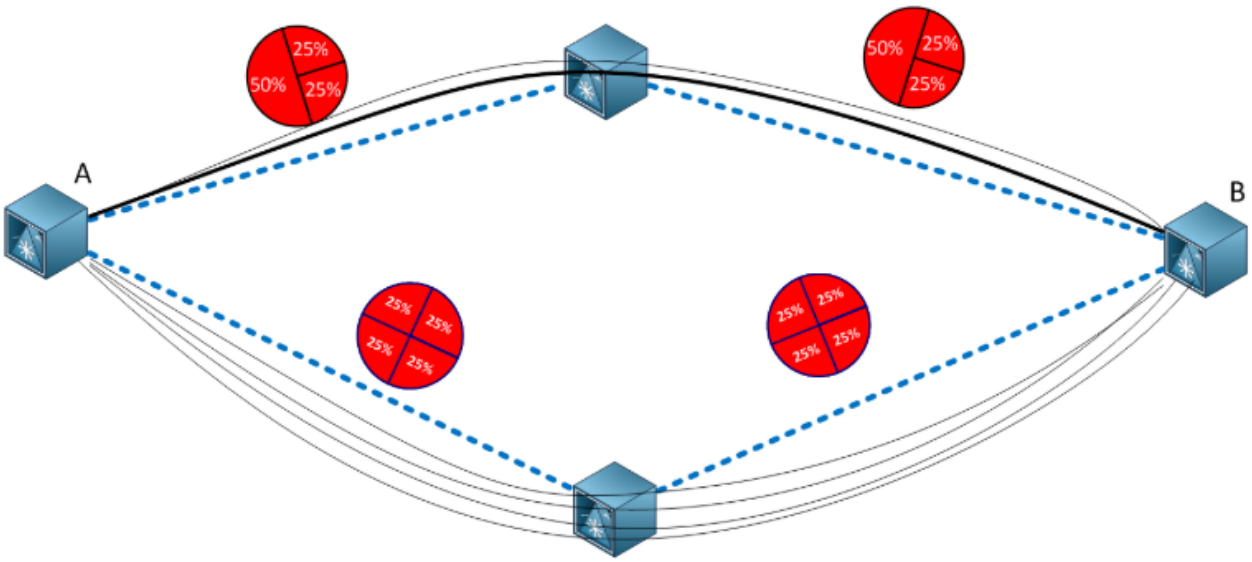


Рис. 3.3 Перенаправлення по альтернативному шляху одного із вже активних клієнтських каналів

У процесі модернізації транспортних мереж постає завдання виконання операцій так, щоб для кінцевого користувача вони залишалися абсолютно непомітними. Перерозподіл каналів чи зміна маршруту передавання даних повинні відбуватися без навіть короткочасних перебоїв, а також без зниження параметрів якості обслуговування (QoS). Для операторів зв'язку це критично важливо, адже клієнти не готові миритися навіть із секундними затримками або втратами пакетів. На практиці таке динамічне переналаштування можливе, проте воно здебільшого виконується вручну інженерами мережі. Це означає, що процес займає значний час, залежить від людського фактора та потенційно схильний до помилок. Використання ж централізованого T-SDN контролера здатне змінити ситуацію докорінно: операції з перенаправлення трафіку можуть виконуватися автоматично, із заданими параметрами надійності, що гарантує безперервність сервісів.

Варто зауважити, що використання каналу на рівні 100% пропускної здатності практично недосяжне. Ця цифра наводиться у технічній літературі як приклад для демонстрації проблеми. Реальні показники утилизації зазвичай складають близько 80–90%, що пов'язано як з особливостями протоколів, так і з необхідністю залишати резерв для підтримання стабільності мережі.

Однією з найбільш перспективних можливостей T-SDN є концепція «пропускна здатність на запит» (bandwidth on demand). Вона полягає у тому, що якщо обсяг трафіку клієнта перевищує ємність заздалегідь придбаного ним каналу, система може тимчасово збільшити пропускну здатність саме для цього користувача. Це забезпечує передачу даних із вищою швидкістю у періоди пікових навантажень і водночас захищає від втрат пакетів. Для клієнта такий підхід є економічно вигідним: оплачувати потрібно лише фактичний час додаткового використання ресурсу, а не постійне резервування дорогих високошвидкісних каналів.

Ще одна сильна сторона T-SDN — це можливість централізованого та оптимального вибору маршрутів. Традиційно прокладання нового сервісу в транспортній мережі вимагає врахування багатьох метрик: затримки, втрат, пропускної здатності, вартості використання ресурсів тощо. Автоматизований

контролер здатен виконувати цю задачу набагато швидше та точніше, аналізуючи всі доступні параметри та обираючи оптимальний шлях. Це не лише прискорює надання послуг клієнтам, а й дозволяє операторам більш ефективно використовувати власну інфраструктуру.

Не менш важливим є забезпечення високої надійності та доступності сервісів (High Availability). Контролер здатний у реальному часі реагувати на збої в мережі: виконувати перемикання на резервні маршрути, швидко відновлювати роботу сервісів навіть у разі серйозних аварій. Підтримуються різноманітні схеми резервування — від класичних «1+1» та «1:1» до складніших динамічних алгоритмів. Усе це знижує час відновлення сервісів і мінімізує ризики тривалих простоїв.

Ще одна перевага T-SDN — безпечне конфігурування мережі. У традиційних системах зміни в конфігурації пристроїв часто виконуються вручну й можуть призводити до серйозних інцидентів. Історія телекомунікацій знає чимало прикладів, коли людські помилки викликали глобальні збої. Достатньо згадати витік маршрутів (route leak) від 12 червня 2015 року, який торкнувся значної частини Інтернету. Використання високорівневих візуальних застосунків у рамках T-SDN суттєво знижує ризик неправильних налаштувань, адже більшість складної роботи бере на себе автоматизована система, тоді як адміністратор оперує лише логічними сутностями та політиками.

Крім того, архітектура T-SDN від самого початку орієнтована на масштабованість. Збільшення кількості мережевих пристроїв чи додавання нових застосунків для управління не вимагає додаткових налаштувань контролера. Це дозволяє гнучко нарощувати інфраструктуру та підтримувати її актуальність без ризику втратити стабільність або сумісність.

Зрозуміло, що такі інноваційні можливості викликають неоднозначну реакцію серед фахівців: від захоплення перспективами до жорсткої критики та недовіри. Адже на даному етапі багато заявлених функцій потребують практичного підтвердження. Реально оцінити ефективність T-SDN зможуть лише масштабні

дослідження, створення прототипів і пілотні впровадження у реальних операторських мережах.

На сьогодні інженери компанії NetCracker спільно з фахівцями NEC активно працюють над розширенням функціональності контролера T-SDN, тестують нові алгоритми та розробляють прототипи, що мають стати фундаментом для повноцінних комерційних рішень у майбутньому. Усе це свідчить про те, що T-SDN поступово переходить зі стадії концепції у стадію практичної реалізації, відкриваючи шлях до побудови нової генерації інтелектуальних транспортних мереж.

3.2 Структура контролера T-SDN

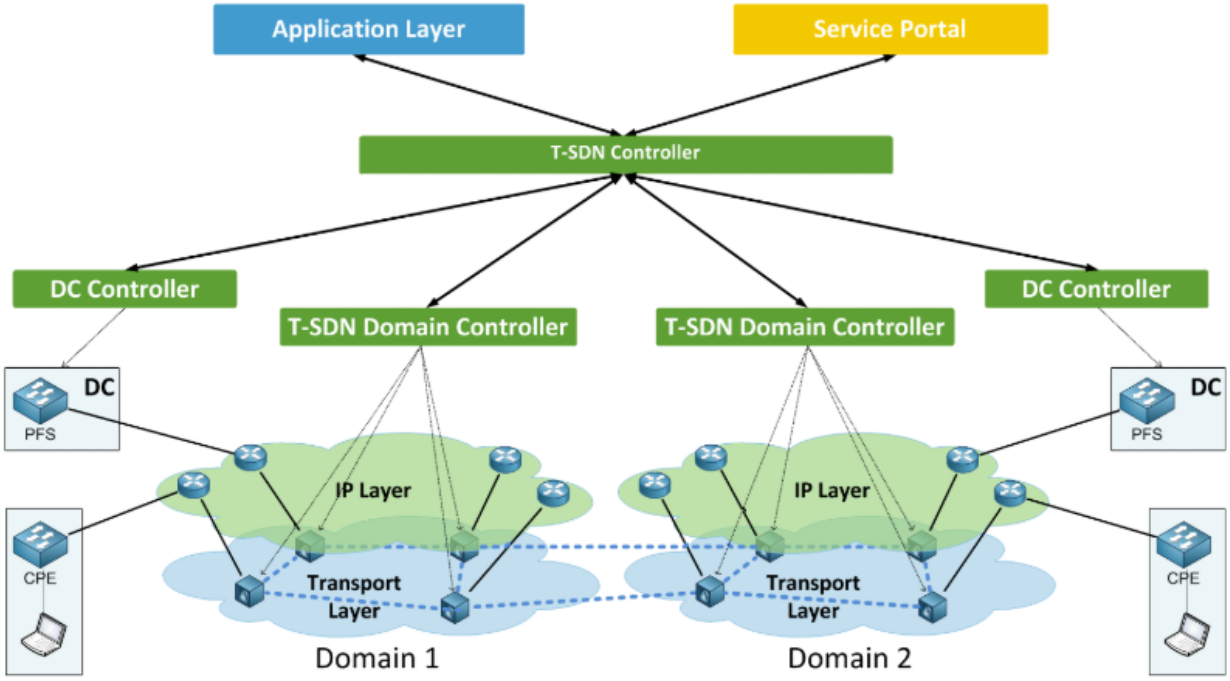


Рис. 3.4 Топологія алгоритмів дії контролера T-SDN

Під час розробки сучасного контролера транспортних мереж ключовим завданням визначається підтримка широкого спектру вимог, що відповідають потребам провайдерів різного масштабу. Йдеться не лише про базові можливості управління інфраструктурою, а й про створення гнучкої, масштабованої та високопродуктивної системи, здатної працювати в умовах стрімкого зростання обсягів трафіку та різноманіття сервісів.

Серед основних вимог, на які орієнтовано розробку контролера, можна виділити такі:

- забезпечення повного управління великою, розподіленою у просторі транспортною мережею провайдера;
- прокладання маршрутів по всій інфраструктурі з урахуванням політик та специфічних сценаріїв використання;
- оптимізація маршрутів відповідно до технічних метрик, вимог користувачів і пріоритетів сервісів;
- підтримка мультивендорного середовища, що дозволяє інтегрувати обладнання різних виробників у єдину систему;
- реалізація концепції «пропускна здатність на запит» (bandwidth on demand), яка забезпечує динамічне виділення додаткових ресурсів для клієнта у моменти пікових навантажень;
- гарантування високої надійності та доступності сервісів (high availability) навіть за умови аварій чи збоїв;
- можливість масштабування системи без суттєвих змін у її архітектурі;
- максимальна ефективність використання наявної пропускної здатності, що особливо актуально в умовах обмежених ресурсів.

Розроблюваний контролер береться за зразком рішень компанії NetCracker, яка є резидентом Дія.City та вже має значний досвід у створенні систем управління мережами для провайдерів світового рівня. Це дозволяє орієнтуватися на перевірені архітектурні підходи, адаптуючи їх до сучасних реалій українського та глобального телекомунікаційного ринку.

Архітектура контролера має ієрархічну структуру, яка складається з двох рівнів. Доменний контролер T-SDN (нижній рівень) відповідає за управління окремим сегментом транспортної мережі, виконуючи безпосередню взаємодію з обладнанням. Він контролює транспортні пристрої, виконує завдання моніторингу та локальної оптимізації. Над ним функціонує центральний контролер T-SDN (верхній рівень), який працює вже не з конкретними пристроями, а з доменними

контролерами. Завдяки цьому досягається абстрагування від низькорівневих операцій, а управління мережею здійснюється на глобальному рівні.

Завдання управління мережею декомпозуються та делегуються нижчим контролерам, що дозволяє знизити навантаження на центральний рівень і підвищити продуктивність системи. Центральний контролер агрегує дані про роботу доменів, аналізує їх та ухвалює рішення, які визначають подальшу стратегію управління мережею. Такий підхід створює баланс між локальною деталізацією та централізованим контролем, що забезпечує одночасно і масштабованість, і стабільність.

На схемі нижче зображено принцип розподілу управління між двома рівнями контролерів T-SDN: доменним контролером, який відповідає за керування одним окремим доменом, та контролером верхнього рівня, який здійснює управління всією мережею в цілому.

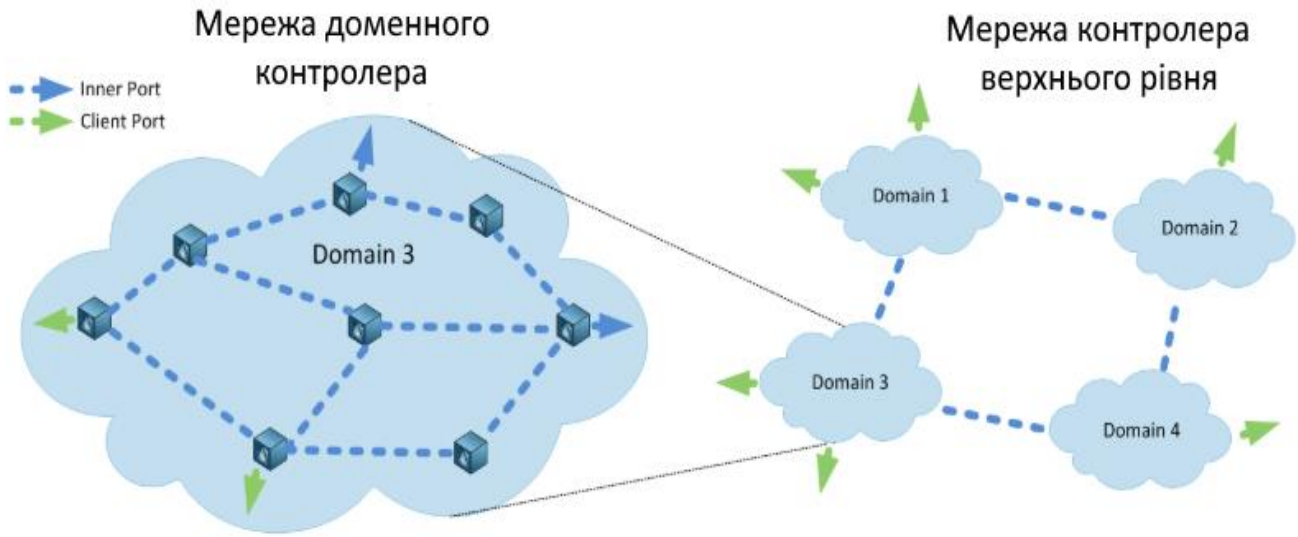


Рис. 3.5 Мережі, керовані доменним контролером T-SDN (управління одним доменом) та контролером T-SDN верхнього рівня (управління всіма доменами

Іншими словами, контролер верхнього рівня сприймає цілу групу пристроїв як одне логічне ціле. Такий підхід, з одного боку, дозволяє уникнути значних накладних витрат і підвищити продуктивність управління мережею, а з іншого — забезпечує глобальне бачення інфраструктури. Це особливо важливо у випадку крос-доменних з’єднань, які неможливо повноцінно контролювати на рівні

окремого домену, оскільки вони не перебувають у зоні видимості доменного контролера T-SDN.

Завдяки такій архітектурі стає можливим прокладати клієнтський сервіс через усю транспортну мережу: від точки входу до точки виходу із мережі провайдера. У результаті забезпечується ефективне управління утилизацією каналів, оптимізація маршрутів, підвищення надійності та стабільна доступність сервісів, що є критично важливими параметрами для сучасних операторських мереж.

Архітектура контролера T-SDN, створена компанією NetCracker у партнерстві з корпорацією NEC, демонструє сучасний підхід до управління транспортними мережами нового покоління. Вона має багаторівневу ієрархічну структуру, яка дозволяє не лише централізовано контролювати всю інфраструктуру, але й адаптуватися до мультивендорного середовища, де застосовуються пристрої різних виробників.

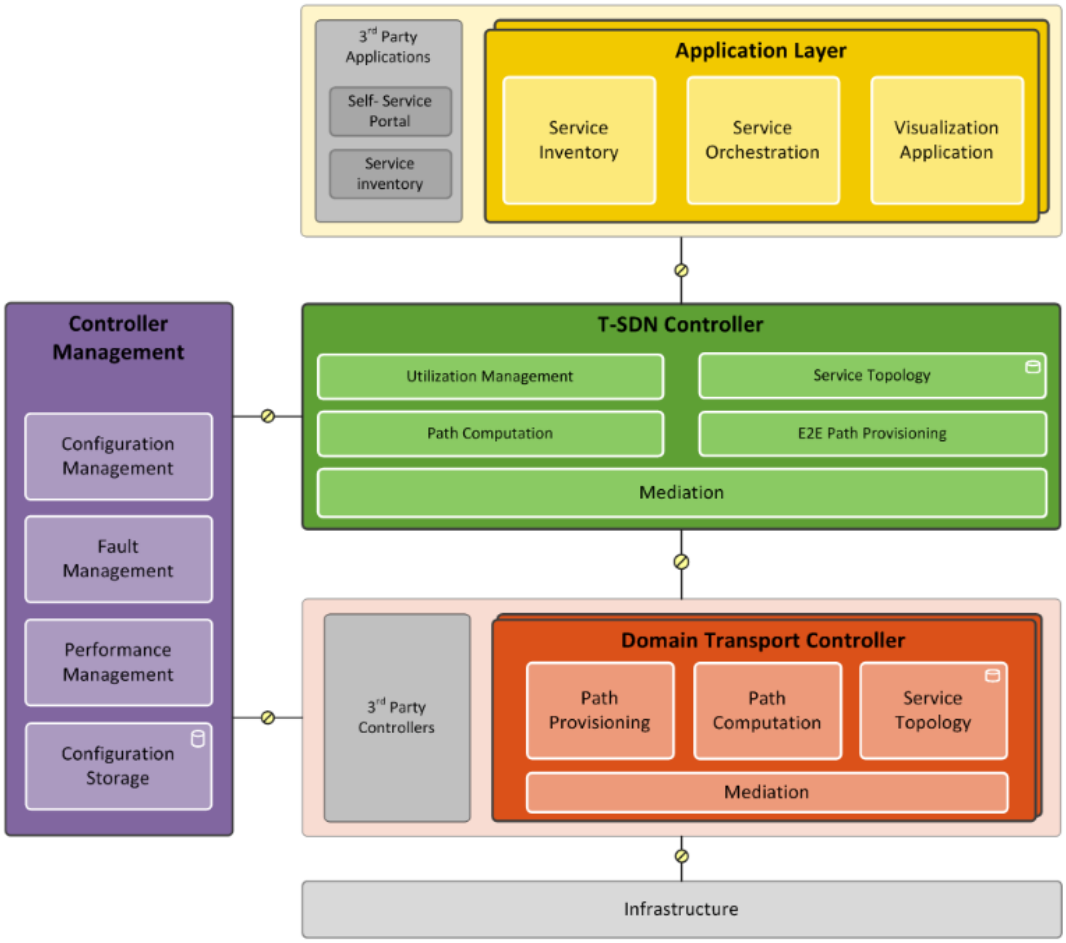


Рис. 3.5 Архітектура контролера T-SDN

На нижньому рівні архітектури розташовується мережева інфраструктура, що включає комутатори, маршрутизатори, транспондери та інші транспортні пристрої. Вони взаємодіють із доменними SDN-контролерами через набір протоколів та інтерфейсів API, серед яких можуть бути як стандартизовані (наприклад, OpenFlow чи NETCONF), так і пропрієтарні механізми управління. Це забезпечує базовий рівень сумісності та дає можливість інтегрувати обладнання від різних виробників в єдину систему управління.

Наступний рівень становлять доменні контролери, які виконують завдання управління певними сегментами мережі. Вони збирають дані з обладнання, контролюють роботу окремих доменів і передають агреговану інформацію до центрального контролера верхнього рівня. Саме доменні контролери знімають основне навантаження з центральної системи, адже на них покладається детальне управління транспортними елементами.

На верхньому рівні розташовується головний T-SDN-контролер, який абстрагується від низькорівневої взаємодії з обладнанням і керує виключно доменними контролерами. Завдяки цьому підходу досягається висока масштабованість: мережа з десятками чи навіть сотнями доменів може управлятися з єдиного центру без перевантаження системи. На найвищому рівні знаходяться також прикладні сервіси та інтерфейси, що забезпечують адміністрування, моніторинг, журналювання та візуалізацію мережі. Це можуть бути високорівневі додатки, які взаємодіють із контролером за допомогою стандартних API та дозволяють користувачам і адміністраторам формувати політики, відслідковувати якість обслуговування та керувати конфігураціями.

Особливо важливим є те, що архітектура T-SDN від NetCracker повністю відповідає еталонній моделі SDN-контролера, запропонованій Open Networking Foundation (ONF) у 2014 році. Це підтверджує сумісність із глобальними стандартами та гарантує можливість масштабування рішення у напрямі індустріальних практик. Життєздатність такої моделі підтверджується численними тестуваннями у лабораторіях NetCracker на обладнанні різних виробників, де

перевірялася не лише продуктивність, а й сумісність з мультивендорними середовищами.

Основні функціональні модулі контролера T-SDN:

- **Прокладання маршрутів (Path Provisioning)** — відповідає за побудову маршрутів на логічному рівні та їх узгодження із даними від доменних контролерів через модуль медіації.
- **Обчислення маршруту (Path Computation, PCE)** — визначає оптимальний шлях для клієнтського сервісу у мережевому графі з урахуванням великої кількості критеріїв.
- **Управління утилизацією (Utilization Management)** — оптимізує використання пропускної здатності каналів, балансуючи навантаження.
- **Сервісна топологія (Service Topology)** — зберігає інформацію про актуальні та заплановані сервіси, їхні параметри та стан.
- **Медіатор (Mediation)** — здійснює інтеграцію з мережевими пристроями та підтримує протоколи RESTCONF, NETCONF, SNMP, SSH, OpenFlow, HTTP/HTTPS.
- **Управління контролером (Controller Management)** — відповідає за конфігурацію, управління відмовами, продуктивністю, безпекою та інші аспекти відповідно до моделі **FCAPS** стандарту ISO.

Модуль PCE — інноваційний елемент системи

Модуль обчислення маршруту (PCE) є одним із найскладніших елементів. На перший погляд може здатися, що задача пошуку шляху вже вирішена алгоритмами Дейкстри або протоколами OSPF, IS-IS чи HWMP (802.11s). Проте вимоги операторських мереж значно складніші: потрібно враховувати бажані та небажані вузли, обов’язкові точки проходження, заборонені вершини та специфіку обладнання різних виробників. Така задача належить до NP-повних, тому NetCracker реалізовує її за допомогою комбінації евристичних підходів і класичних алгоритмів, адаптованих для багаторівневого графа (фізичний, фізико-логічний та абстрактний рівні). Це дозволяє досягати високої ефективності пошуку маршруту незалежно від особливостей конкретного обладнання.

Подальший розвиток технології

Після успішного запуску пілотних версій контролера T-SDN компанія NetCracker активно долучається до розвитку Open Source-проектів, таких як ONOS та ODENOS, а також бере участь у стандартизації SDN-рішень у рамках діяльності ONF та інших міжнародних організацій. Важливу роль у цьому відіграє партнерство з NEC, виробником сучасного мережевого обладнання, що дозволяє відразу тестувати нові алгоритми та функціонал у лабораторних умовах на новітніх пристроях.

Попит з боку великих телекомунікаційних операторів стимулює подальший розвиток системи. Провайдери формують нові, більш складні вимоги, змушуючи вдосконалювати як низькорівневі інтерфейси медіації, так і високорівневі прикладні додатки для управління та моніторингу. Команда NetCracker, що має багаторічний досвід у впровадженні рішень OSS/BSS, заклала міцний фундамент для формування нового покоління інтелектуальних контролерів, які поєднують автоматизацію, масштабованість, мультивендорну сумісність і відповідність міжнародним стандартам.

4 СТВОРЕННЯ КЕРОВАНОГО SDN ПРОСТОРУ

4.1 Традиційний підхід

Приклад побудови віртуалізованої мережі

Щоб краще зрозуміти принципи роботи віртуалізованих мереж, почнемо з базового прикладу. Багатьом користувачам знайоме завдання — створити віртуальну машину, підключити її до мережі та налаштувати для неї IP-адресацію. З боку адміністратора чи користувача все виглядає досить просто: у віртуалізованому середовищі є «віртуальна машина-1» (VM1), «віртуальна машина-2» (VM2) та певна «мережа» (Network), у межах якої вони можуть взаємодіяти. Але внутрішня реалізація цієї схеми набагато складніша й багаторівнева.

У сучасних інфраструктурах практично ніколи не використовується лише один фізичний сервер. Для розгортання робочого середовища застосовується декілька серверів — хостів віртуалізації, які виконують роль гіпервізорів. Віртуальні машини, що працюють на різних серверах, повинні мати можливість обмінюватися даними так, ніби вони знаходяться в одній фізичній мережі. Для цього кожну віртуальну машину підключають до спеціального мережевого моста (bridge). Міст, своєю чергою, прив’язаний до фізичного мережевого інтерфейсу сервера, а через нього — до корпоративної мережі підприємства чи дата-центру. Таким чином, створюється ілюзія єдиного мережевого середовища, у якому віртуальні машини можуть взаємодіяти незалежно від того, на якому саме сервері вони працюють.

Однак у реальних сценаріях на цьому все не закінчується. Зазвичай виникає потреба у сегментації трафіку, коли дані певних віртуальних машин мають передаватися лише у межах визначеного сегмента мережі. Це робиться для підвищення безпеки, ефективності та керованості. Наприклад, можна виділити окремий сегмент для середовища розробки, де програмісти тестують новий функціонал, і ще один — для тестового середовища, де відбувається імітація робочих навантажень. Таким чином, трафік із середовища розробки не зможе

потрапити в сегмент тестування або в продуктивне середовище, що знижує ризики та забезпечує чіткий розподіл ресурсів.

Кількість таких сегментів може бути великою, і кожен із них потребує індивідуальних налаштувань: виділення підмереж, налаштування правил доступу, визначення політик безпеки тощо. Зі зростанням кількості сегментів значно ускладнюється управління всією інфраструктурою. Тому дедалі більшої ваги набувають автоматизовані підходи та використання програмно-визначених мереж (SDN), які дозволяють централізовано керувати цими процесами.

У результаті навіть просте завдання зі створення кількох віртуальних машин у межах однієї мережі на практиці перетворюється на складну багаторівневу архітектуру, де враховуються питання маршрутизації, сегментації, безпеки, балансування навантаження й масштабованості. Саме цей приклад демонструє, наскільки важливою є грамотна організація віртуалізованих мереж для ефективної роботи сучасних дата-центрів і корпоративних IT-інфраструктур.

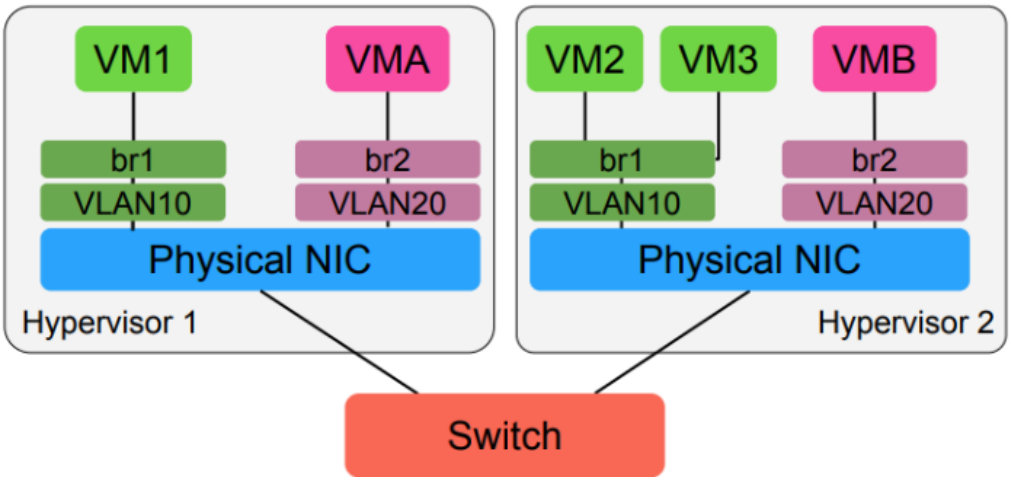


Рис. 4.1 Приклад простої віртуалізації мережі

Першою істотною складністю, з якою стикається адміністратор у процесі побудови віртуалізованих мереж, є необхідність налаштовувати мережеві мости (bridges) на кожному окремому гіпервізорі. З технічного боку це можливо частково автоматизувати, застосувавши спеціальні скрипти чи системи централізованого управління конфігураціями. Проте навіть у такому випадку залишається потреба у ручному втручанні на рівні кожного вузла, що у великих інфраструктурах з десятками або сотнями серверів стає складним і трудомістким завданням.

Ситуація ускладнюється ще більше, коли постає потреба в налаштуванні фізичних комутаторів. Це завдання часто виходить за межі компетенцій фахівців із віртуалізації і потребує залучення профільних мережевих інженерів. Наприклад, щоб дозволити передавання трафіку з певними VLAN-тегами, необхідно налаштувати транкові з'єднання на фізичних комутаторах. Такий підхід призводить до затримок, оскільки процес узгодження та впровадження змін може займати тривалий час, а також знижує гнучкість і швидкість реакції інфраструктури на нові вимоги бізнесу.

Окремо варто відзначити обмеження масштабованості класичних VLAN. Ідентифікатор VLAN має довжину всього 12 біт, що обмежує їх максимальну кількість значенням у 4096 сегментів. У масштабах невеликої мережі цього достатньо, але у великих корпоративних чи хмарних інфраструктурах цього ресурсу критично бракує. Великі дата-центри можуть одночасно підтримувати десятки тисяч ізольованих сегментів для різних клієнтів і застосунків, що неможливо реалізувати у рамках стандартної VLAN-архітектури.

Крім того, VLAN має ще одне фундаментальне обмеження: взаємодія між різними сегментами можлива лише на мережевому рівні (через маршрутизатори або L3-комутатори). Це означає, що політики безпеки, які діють на канальному рівні, залишаються примітивними й негнучкими. Адміністратор не може вбудувати глибокий контроль доступу або, наприклад, встановити міжмережевий екран безпосередньо між віртуальними машинами в межах одного VLAN. Як наслідок, увесь трафік усередині сегмента передається без будь-якої додаткової перевірки чи обмежень, а контроль можливий лише «на виході» з VLAN.

Це створює значні ризики. Якщо один із пристроїв у сегменті виявиться скомпрометованим, він матиме можливість безперешкодно поширювати шкідливий трафік усім іншим учасникам сегмента. У критичних випадках це може призвести до внутрішніх DoS-атак або до масового зараження всієї інфраструктури. Таким чином, навіть добре організована VLAN-сегментація не гарантує достатнього рівня безпеки у великих та складних середовищах.

У сукупності всі ці фактори демонструють, що традиційний підхід до побудови віртуальних мереж має низку суттєвих недоліків: він незручний в управлінні, погано масштабується і не забезпечує належного рівня захисту. Саме це підштовхнуло індустрію до розвитку нових підходів — віртуалізації самої мережі.

Завдяки таким рішенням, як програмно-визначені мережі (SDN) та мережеві функції у вигляді програмного забезпечення (NFV), з’явилася можливість будувати віртуальні мережеві інфраструктури, що не прив’язані до фізичної топології та здатні гнучко змінюватися відповідно до вимог бізнесу. Віртуалізація мереж дозволяє створювати тисячі ізольованих сегментів поверх однієї фізичної інфраструктури, застосовувати гнучкі політики безпеки на будь-якому рівні, динамічно масштабувати ресурси й автоматизувати управління конфігураціями. У результаті IT-служби отримують інструмент, який не лише усуває недоліки VLAN, але й відкриває принципово нові можливості для розвитку корпоративних і хмарних систем.

4.2 Віртуальна мережа

Користувачі та адміністратори швидко звикають до зручних і ефективних інструментів. Коли з’являється можливість працювати з новими технологіями, що спрощують щоденні процеси, повертатися до старих методів стає небажаним і часто навіть неможливим. Так само, як електричні шуруповерти витіснили ручні викрутки, а сенсорні смартфони замінили кнопкові телефони, сучасні замовники, одного разу випробувавши мережеву віртуалізацію на основі SDN-рішень на зразок VMware NSX, більше не погоджуються будувати інфраструктуру на традиційних VLAN. У таких умовах інтеграція SDN у системи віртуалізації стала не опцією, а необхідністю, продиктованою ринком і очікуваннями користувачів.

Чому саме SDN?

Запровадження SDN дало змогу створити єдину точку управління віртуальною мережею. Це дозволило абстрагуватися від фізичної топології корпоративної інфраструктури та працювати з логічними сутностями, що

відображають бізнес-процеси замовників. Замість ручного налаштування фізичних комутаторів з'явилася можливість керувати віртуальними об'єктами через централізовану панель управління чи API. Саме це забезпечило гнучкість, швидку адаптацію до змін, масштабованість і високий рівень автоматизації.

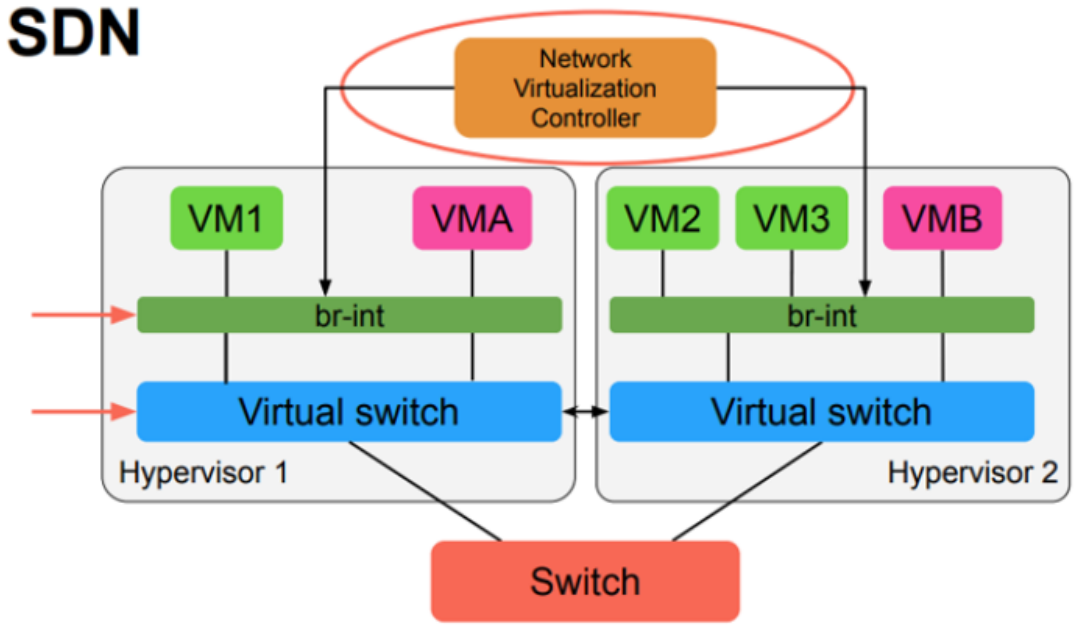


Рис. 4.2 Зразок мережі з єдиною точкою управління

Вимоги до нового рішення

При переході на нову модель було висунуто вимогу зберегти всі функції, доступні у традиційних мережах, щоб користувачі не втратили у можливостях і могли працювати з інструментами, до яких звикли. Серед основних вимог:

- **Аналоги VLAN** — логічні та широкомовні домени зі збереженням функціональних характеристик.
- **Система управління IP-адресами (IPAM)** — для автоматизації роботи з адресним простором у віртуальних мережах.
- **Механізми інтеграції з зовнішніми мережами**, адже оверлейні рішення за замовчуванням ізольовані, і необхідно створювати шлюзи для виходу трафіку за межі віртуального середовища.
- **Інструменти моніторингу та управління** — засоби відстеження стану мережі, журналювання операцій, а також зрозумілий графічний інтерфейс.
- **Сумісність із протоколами маршрутизації корпоративного рівня** (OSPF, BGP).

- **Відкритий API** для автоматизації та зовнішнього управління інфраструктурою.

Вибір технологічного стека

Після детального аналізу було обрано стек OVN/OVS. Хоча вона перебувала радше на концептуальному рівні й не відзначалася високою стабільністю, саме це стало фундаментом для початку перших тестів та експериментів.

Тестування OVN/OVS

Було проведено низку випробувань поза межами основної системи віртуалізації:

- перевірено роботу dataplane та ефективність пересилання пакетів;
- здійснено навантажувальні тести з високою інтенсивністю трафіку;
- зафіксовано ключові метрики продуктивності (пропускна здатність, затримки, споживання ресурсів).

Результати виявилися позитивними: OVN/OVS підтвердив стабільність і здатність витримувати суттєві навантаження без втрати продуктивності.

Висновки з тестування

Тестування довело, що OVN/OVS відповідає ключовим вимогам:

- забезпечує масштабованість,
- є достатньо гнучким,
- має підтримку з боку активної спільноти,
- використовується у масштабних інсталяціях OpenStack, що підтверджує його зрілість.

Ці фактори дозволили зробити висновок про можливість швидкого впровадження рішення у продуктивне середовище без втрати стабільності платформи. Звісно, були виявлені й певні недоліки, проте для їх глибшого аналізу необхідно детальніше розглянути архітектуру OVN та її ключові відмінності від традиційної VLAN-моделі.

У традиційній моделі віртуалізації мереж кожна віртуальна машина підключається на гіпервізорі до окремого мережевого моста (bridge). Цей міст зв’язаний із фізичним мережевим адаптером сервера, а через нього — з

корпоративним комутатором. Такий підхід технічно працездатний, але має суттєві обмеження. При зростанні кількості серверів і сегментів адміністрування ускладнюється, масштабування потребує значних зусиль, а рівень гнучкості та безпеки залишається недостатнім для сучасних вимог.

На зміну цьому прийшла концепція програмно-визначених мереж (SDN), де ключову роль відіграє інтеграційний віртуальний програмований комутатор Open vSwitch (OVS). На відміну від фізичних або окремих програмних мостів, саме він стає універсальною точкою підключення віртуальних машин. Між собою екземпляри Open vSwitch з'єднуються за допомогою Geneve-тунелів, що дозволяє створити єдину логічну мережу поверх фізичної інфраструктури. Завдяки цьому віртуальні машини можуть вільно обмінюватися даними незалежно від того, на якому фізичному сервері вони розміщені, тоді як для користувача мережа виглядає цілісною і прозорою.

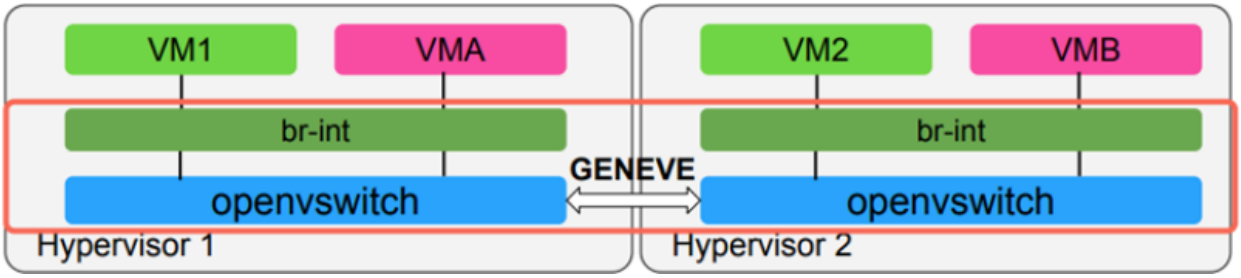


Рис. 4.3 Open vSwitch з'єднуються за допомогою Geneve-тунелів

Архітектура Open vSwitch складається з трьох основних компонентів. Модуль ядра (Kernel Module) забезпечує обробку мережевого трафіку у площині пересилання: комутацію, маршрутизацію, фільтрацію та виконання базових правил. База даних правил (Flow Database) містить усі інструкції у форматі OpenFlow, які визначають, як саме слід обробляти пакети — від пересилання до блокування чи маркування. Демон управління (ovs-vswitchd) синхронізує політики та забезпечує своєчасне застосування правил у Data Plane, гарантуючи актуальність конфігурації на всіх вузлах.

Завдяки поєднанню цих елементів OVN та OVS забезпечують масштабовану й керовану інфраструктуру, у якій адміністратор працює з логічними об'єктами, а не з фізичними портами чи мостами. Це дозволяє централізовано формувати

правила доступу, застосовувати їх одночасно на багатьох гіпервізорах, створювати тисячі ізольованих віртуальних сегментів поверх однієї фізичної інфраструктури та контролювати трафік на більш глибокому рівні, включно з міжмашинною взаємодією у межах одного сегмента.

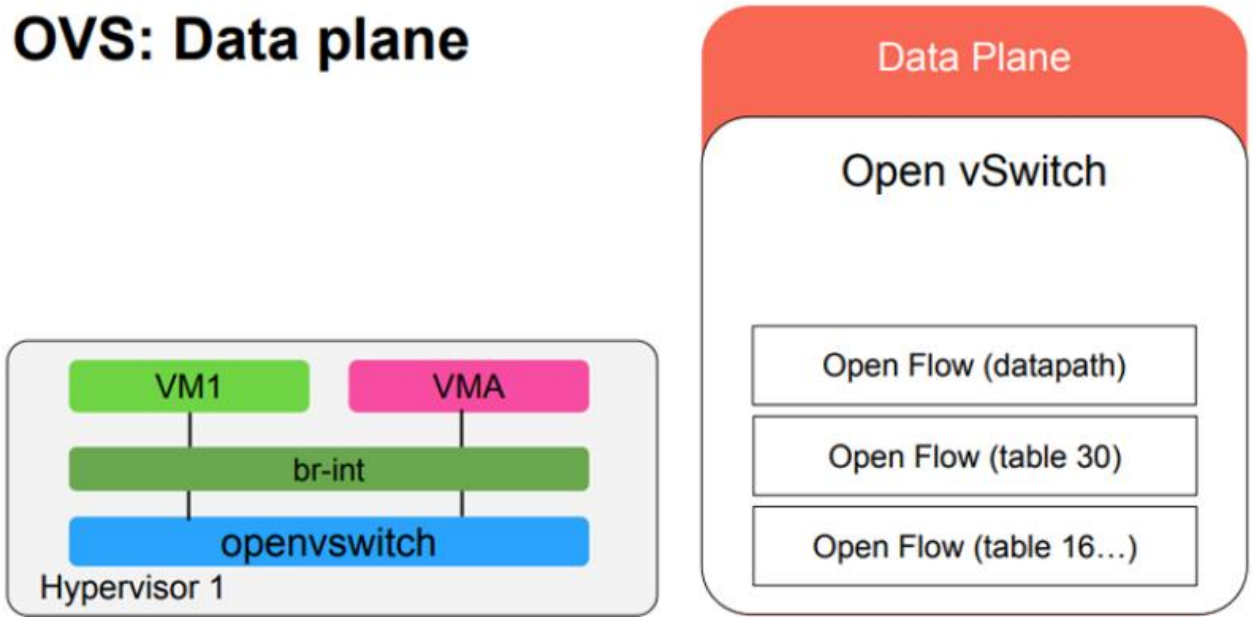


Рис. 4.4 Конфігурація для Data plane надходить із вищого рівня - з Control plane

У системі Open Virtual Network (OVN) конфігурація Data Plane надходить із вищого рівня — Control Plane. Тут ключову роль відіграють розподілені контролери OVN, які запускаються на кожному гіпервізорі, а також централізована Southbound DB (південна база даних). Саме в ній зберігається актуальна інформація про стан усієї мережі: логічні топології, правила маршрутизації, політики доступу та параметри взаємодії між віртуальними машинами.

Для забезпечення безперервної роботи Southbound DB може бути реплікована на кілька вузлів. Це дозволяє досягти відмовостійкості, адже у випадку збою одного сервера система продовжує функціонувати без втрати даних. Контролери, розміщені на гіпервізорах, постійно синхронізуються з базою та оперативно реагують на будь-які зміни в інфраструктурі. Наприклад, якщо один із серверів виходить з ладу, інформація про це миттєво фіксується у Southbound DB, а контролери автоматично оновлюють правила в Data Plane, перебудовуючи маршрути й переналаштовуючи трафік.

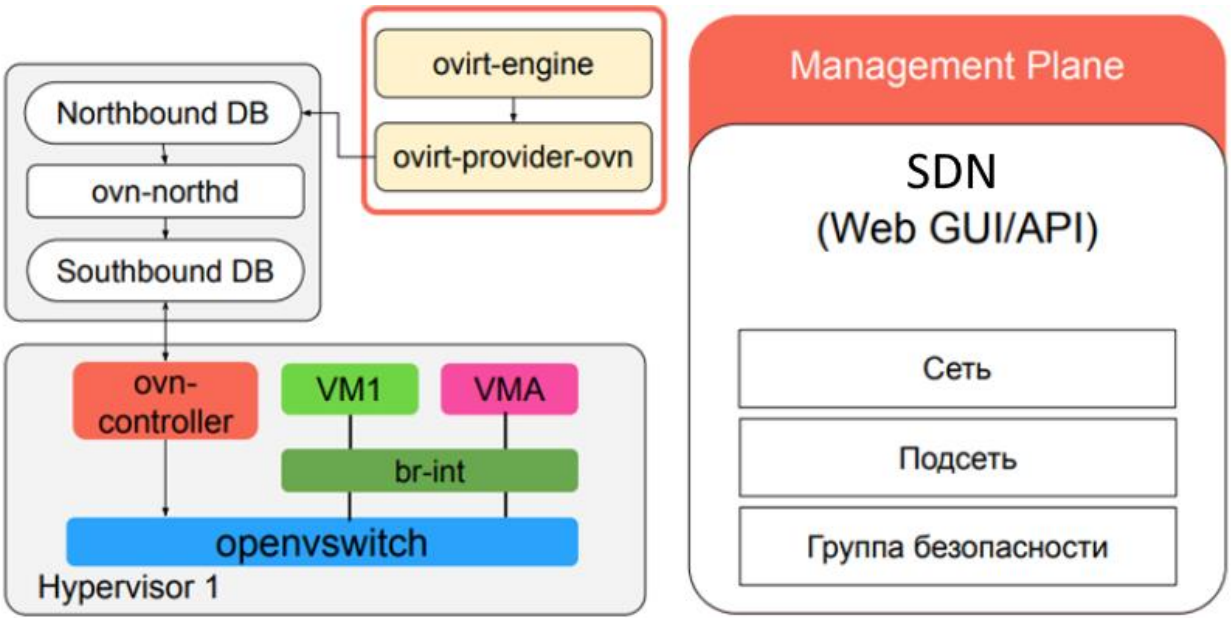


Рис. 4.5 Рівень Management plane

Над рівнем Control Plane розташовується Management Plane — шар управління, у межах якого адміністратор працює з логічними об’єктами, зрозумілими з точки зору мережевої організації: логічними комутаторами, групами портів, політиками безпеки та іншими параметрами. Саме тут формується опис бажаного стану мережі, який передається у Northbound DB (північну базу даних). Далі ці дані спеціальні сервіси перетворюють і синхронізують із Southbound DB, що безпосередньо взаємодіє з площиною пересилання (Data Plane).

ВИСНОВКИ

У результаті проведеного дослідження було розглянуто широке коло теоретичних і практичних аспектів, пов’язаних із функціонуванням програмно-визначених мереж та методами управління трафіком у таких середовищах. Дослідження довело, що традиційні підходи, засновані на статичній конфігурації мережевого обладнання та використанні VLAN-сегментації, в умовах сучасних дата-центрів і транспортних мереж стають неефективними. Це пояснюється різнорідністю обладнання, обмеженою масштабованістю та складністю оперативного реагування на динамічні зміни трафіку.

Використання технології SDN дозволяє реалізувати якісно новий рівень управління мережею: централізоване керування потоками, гнучке розподілення ресурсів, автоматизацію процесів конфігурації, а також інтеграцію з іншими сучасними підходами, такими як віртуалізація мережевих функцій (NFV). Ключовими перевагами SDN є здатність адаптуватися до швидких змін у навантаженнях, забезпечувати пріоритезацію критичного трафіку, підтримувати безшовну міграцію віртуальних машин, балансувати навантаження та динамічно формувати політики QoS.

У ході дослідження було встановлено, що проблематика управління трафіком у SDN-мережах пов’язана з низкою викликів: повільним встановленням правил у таблицях потоків апаратних комутаторів, нерівномірністю продуктивності мережевого обладнання, складністю оптимізації маршрутів з урахуванням QoS і SLA, а також потребою у масштабуванні в багатокористувацьких середовищах. Разом із тим, завдяки централізованим контролерам і програмним методам абстрагування ці проблеми можуть бути ефективно вирішені.

Особлива увага приділялася методам оптимізації пропускної здатності та енергозбереження: SDN надає можливість динамічного вимкнення або переведення в енергозберігаючий режим неактивних комутаторів і каналів, що дозволяє знизити операційні витрати. Також було показано, що QoS у поєднанні з SDN дає змогу

забезпечувати гнучкий розподіл ресурсів, ізоляцію критичного трафіку, контроль затримок і мінімізацію втрат пакетів у реальному часі.

Розвиток SDN у транспортних мережах (T-SDN) підтверджує універсальність підходу: завдяки поділу на контрольну та транспортну площини стає можливим централізоване керування маршрутами, реалізація пропускної здатності «на вимогу», забезпечення високої доступності сервісів та побудова міждоменних з’єднань. Поєднання цих рішень із NFV дає можливість переносити мережеві функції, такі як NAT, Firewall, DPI чи BNG, у віртуальне середовище, що зменшує капітальні та операційні витрати та прискорює впровадження нових послуг.

Таким чином, у дипломній роботі було доведено, що методи управління трафіком у SDN-мережах формують основу для створення нових поколінь телекомунікаційних інфраструктур, здатних забезпечити високу гнучкість, масштабованість, надійність і ефективність. Вони дозволяють ефективно використовувати ресурси, підвищують якість обслуговування, мінімізують ризики відмов і відкривають шлях до подальшої інтеграції з хмарними сервісами, інтелектуальними системами аналізу та мережами наступних поколінь.

ПЕРЕЛІК ПОСИЛАНЬ

1. Traffic Management in SDN – A Roadmap to Research. 2018. – книга про виклики й моделі управління трафіком в SDN.
2. Goransson, P.; Black, C. Software Defined Networking. O'Reilly, 2016. – загальні концепції SDN, включно з управлінням трафіком.
3. Hodaei, A. A Survey on Traffic Management in Software-Defined Networks: Challenges, Effective Approaches, and Potential Measures. 2021. – огляд методів управління трафіком в SDN.
4. SJ Rajan, S. N., et al. Efficient Traffic Management with Adaptive SDN in Vehicular Networks. Scientific Reports, 2025. – управління трафіком у VANET + SDN.
5. Salau, A. O., et al. Software Defined Networking Based Network Traffic … PMC, 2024. – огляд ML-підходів до маршрутизації та управління трафіком у SDN.
6. Prasanth, L. L., et al. A Computationally Intelligent Framework for Traffic Engineering … IEEE / Springer, 2024. – алгоритми маршрутизації, прогнозування трафіку, оптимізація.
7. Priyadarsini, M., et al. Software Defined Networking Architecture, Traffic Management Including Load Balancing and Energy … 2021. – про балансування навантаження й енергоефективність.
8. Isravel, D. P., et al. Traffic Management of SDN/NFV-Based Smart 5G Networks Using Time Series Analysis. 2023. – часорядні методи аналізу для управління трафіком.
9. A Survey and Comparison of SDN Based Traffic Management Techniques. Asian Journal of Applied Science and Technology, 2025. – порівняльний огляд технік управління трафіком.
10. Prabu, U. An Insight into Traffic Engineering in Software-Defined Networks. 2022. – техніки Traffic Engineering, вимірювання матриць трафіку.
11. Islam, MDS; Hossain, M.; AlMukhtar, M. A Survey on SDN & SDCN Traffic Measurement: Existing Approaches and Research Challenge. 2022. – огляд методів вимірювання і моніторингу трафіку.

12. Phan, T. V.; Islam, S. T.; Nguyen, T. G.; Bauschert, T. Q-DATA: Enhanced Traffic Flow Monitoring in SDN Applying Q-learning. 2019. – підходи з Q-learning для моніторингу потоків трафіку.
13. Phan, T. V.; Hajizadeh, M.; Nguyen, T. K.; Bauschert, T. Destination-Aware Adaptive Traffic Flow Rule Aggregation in SDN. 2019. – агрегування правил потоків для контролю таблиць потоків.
14. Kreutz, D.; Ramos, F. M. V.; Verissimo, P.; Rothenberg, C. E.; Azodolmolky, S.; Uhlig, S. Software-Defined Networking: A Comprehensive Survey. 2014. – фундаментальний огляд SDN, проблем масштабованості, продуктивності.
15. Traffic Engineering and QoS Optimization of Integrated Networking. – книга про TE та QoS в об’єднаних мережах.
16. Prabu, U.; Prabu, L. L., et al. An Insight into Traffic Engineering in Software-Defined … – стаття-глава про TE в SDN.
17. Goransson, P.; Black, C. SDN: Software Defined Networks. – книга-огляд про SDN, включаючи управління трафіком.
18. Prasanth, L. L.; Uma, E. A Computationally Intelligent Framework for Traffic Engineering and Congestion Management in Software-Defined Network (SDN). – стаття про ML-підхід до TE і керування навантаженням.
19. Belzarena, P., et al. SDN-Based Overlay Networks for QoS-Aware Routing. – про мережі-оверлеї в SDN для маршрутизації з QoS.
20. Zhang, J.; Ye, M.; Guo, Z., et al. CFR-RL: Traffic Engineering with Reinforcement Learning in SDN. – використання RL для керування критичними потоками.
21. Liaskos, C.; Dimitropoulos, X., et al. Backpressure on the Backbone: A Lightweight, Non-Intrusive Traffic Engineering Approach. – підхід пропускної здатності, маршрутизація за навантаженням.
22. Sanvito, D.; Filippini, I., et al. Adaptive Robust Traffic Engineering in Software Defined Networks. – про адаптивний TE в SDN, мінімізація змін.
23. Rusek, K.; Suárez-Varela, J., et al. RouteNet: Leveraging Graph Neural Networks for Network Modeling and Optimization in SDN. – GNN-моделювання для прогнозу латентності, втрат і оптимізації маршрутів.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ

КВАЛІФІКАЦІЙНА РОБОТА

МЕТОДИ УПРАВЛІННЯ ТРАФІКОМ У SDN-МЕРЕЖАХ

Виконав:
студент групи ТСДМ-62
Павло МАКЕЛЬСЬКИЙ

МЕТА РОБОТИ ТА АКТУАЛЬНІСТЬ

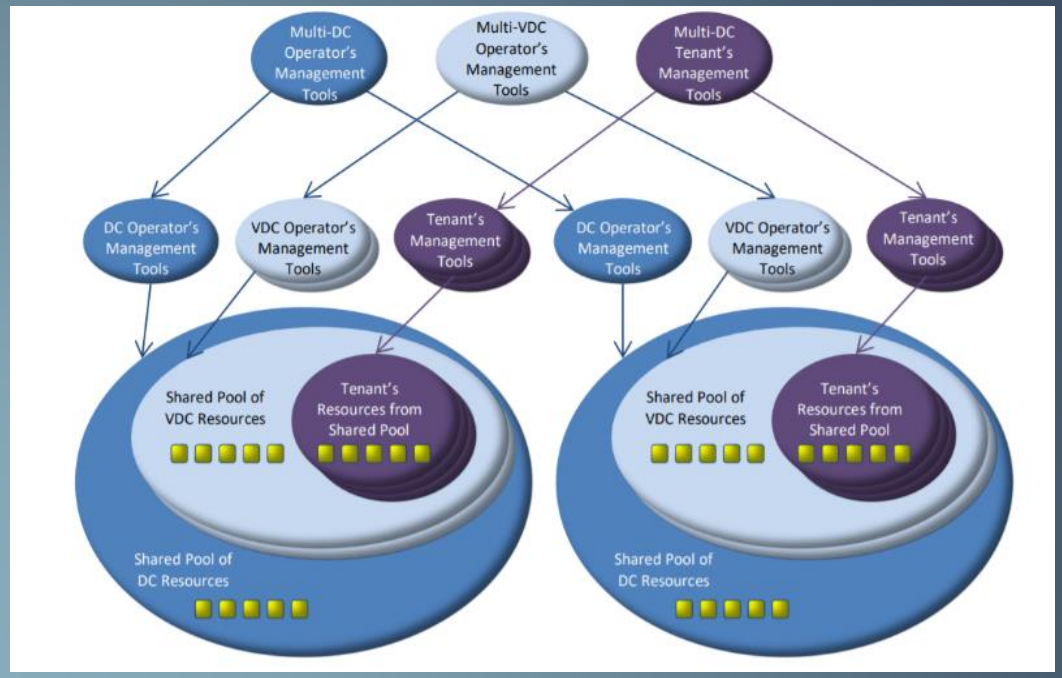
- Мета роботи – аналіз, систематизація та вдосконалення методів управління трафіком у програмно-визначених мережах (SDN) з метою підвищення ефективності використання мережевих ресурсів, забезпечення стабільної якості обслуговування (QoS) та зниження енергоспоживання у центрах обробки даних.
- Об’єкт дослідження – процеси управління трафіком у телекомунікаційних мережах із використанням архітектури програмно-визначених мереж (SDN), зокрема у середовищах центрів обробки даних (ЦОД) і хмарних інфраструктурах.
- Предмет дослідження – методи, алгоритми та технологічні засоби оптимізації, моніторингу та балансування трафіку в SDN-мережах, а також механізми їх інтеграції з віртуалізацією мережевих функцій (NFV) і системами забезпечення якості обслуговування.

Актуальність.

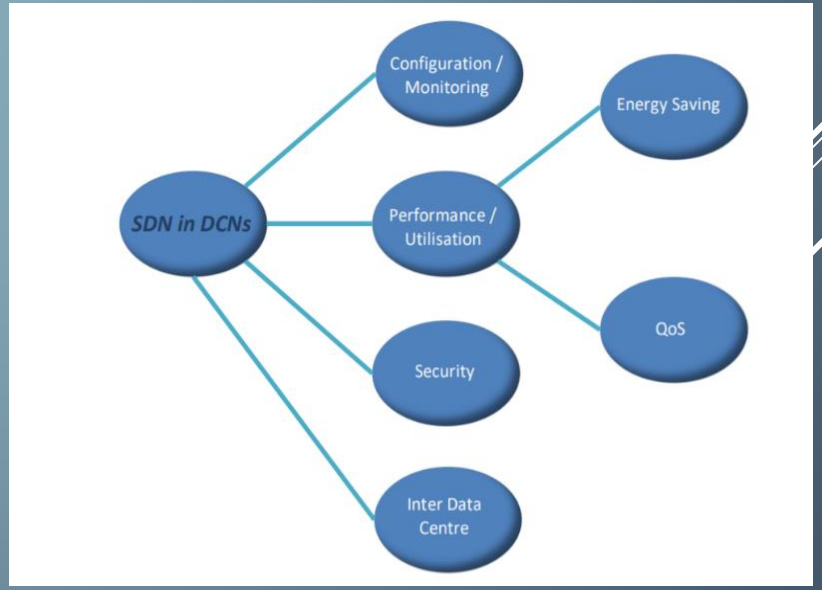
- Традиційні методи конфігурації мережевого обладнання вже не здатні забезпечити необхідну гнучкість, масштабованість та ефективність.
- Технологія Software Defined Networking (SDN) вирішує ці проблеми, відокремлюючи контрольну та транспортну площини, що дає змогу централізовано управляти трафіком і швидко адаптувати мережу до змін навантаження. Тому дослідження методів управління трафіком у SDN безпосередньо відповідає потребам сучасної галузі телекомунікацій та є важливим для розвитку дата-центрів і операторських мереж.

ПОНЯТТЯ SDN МЕРЕЖ

- Кількість і масштаби центрів обробки даних (ЦОД) постійно зростають у відповідь на збільшення обсягів цифрового трафіку. Сучасні ЦОДи мають складну архітектуру, що включає численні сервери, комутатори, маршрутизатори та системи зберігання даних. Зростання кількості користувачів і сервісів призводить до підвищення динамічності мережевого трафіку та ускладнює управління інфраструктурою. Для забезпечення стабільної роботи таких систем необхідно застосовувати ефективні методи моніторингу, балансування навантаження та оптимізації ресурсів. Важливу роль відіграють інтелектуальні алгоритми, здатні автоматично реагувати на зміни стану мережі. Крім того, зростає значення енергоефективності, безпеки передачі даних і масштабованості.



Хмарний мульти-ЦОД із віртуальним мережним оператором



Аспекти SDN, які становлять інтерес для адміністраторів ЦОД

НАЛАШТУВАННЯ ТА МОНІТОРИНГ МЕРЕЖ

- У сучасних центрах обробки даних управління мережею виходить за межі налаштування окремих пристроїв і охоплює централізований контроль усієї інфраструктури. Програмно-визначені мережі (SDN) забезпечують єдину точку керування, автоматизацію процесів і адаптацію до змін трафіку. Вони дозволяють створювати політики, що динамічно розподіляють ресурси між сервісами та користувачами, підвищуючи гнучкість і безпеку. SDN також забезпечує розширений моніторинг і телеметрію в реальному часі, що дозволяє швидко виявляти проблеми й оптимізувати роботу мережі. Завдяки цьому ЦОД стають ефективнішими, масштабованішими та більш надійними.

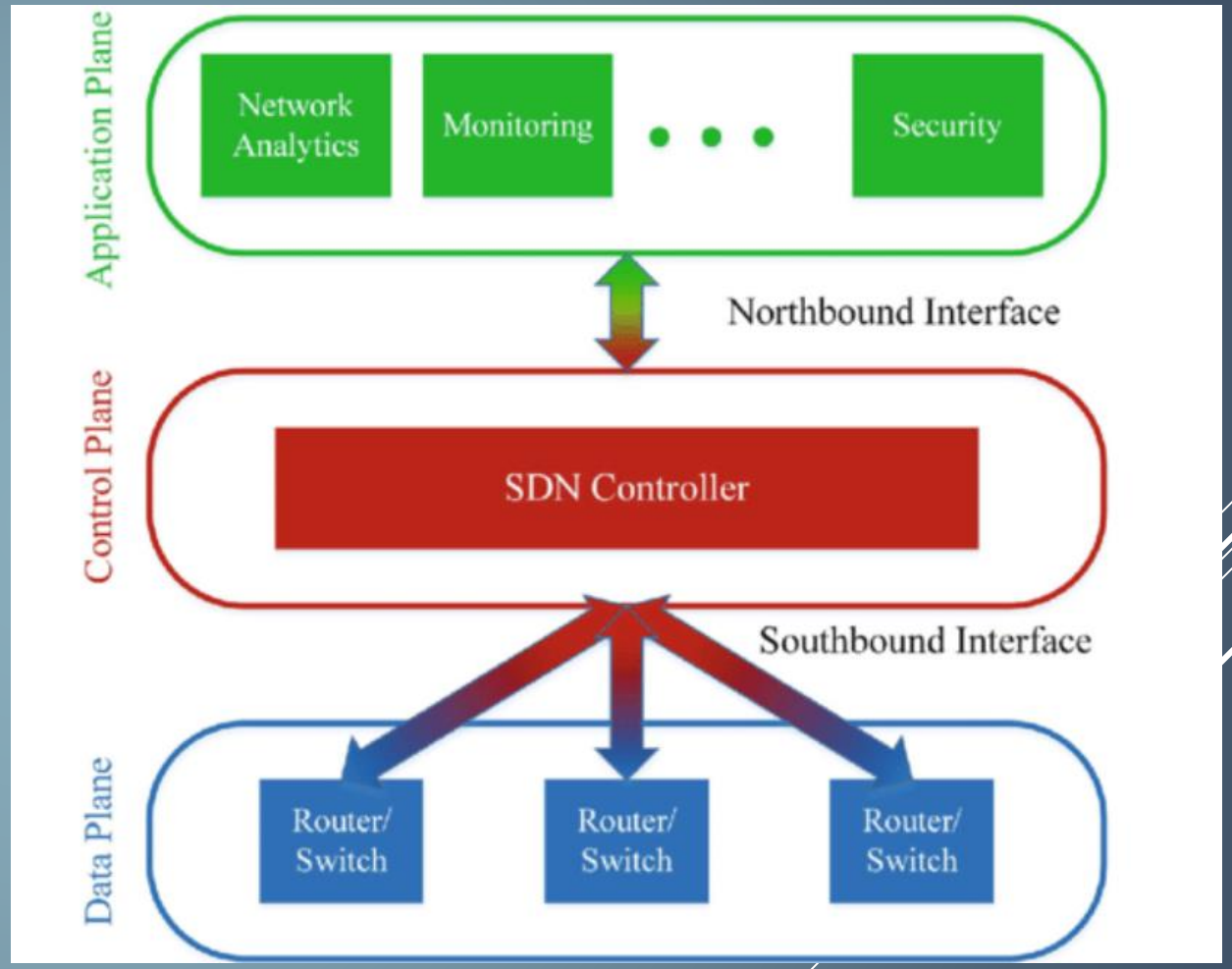
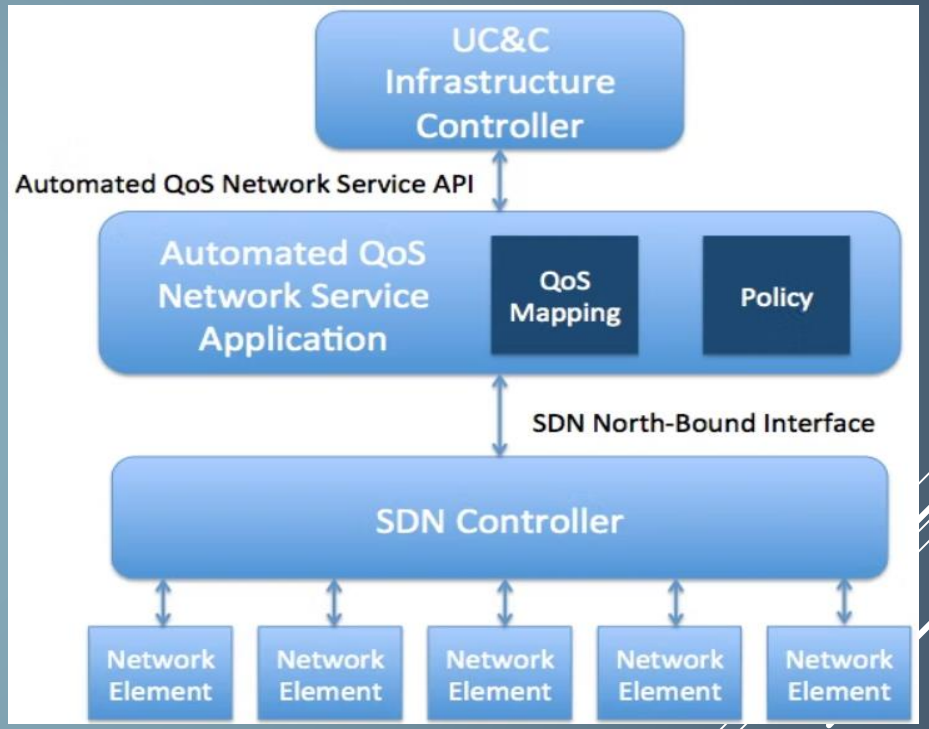


Схема з API, застосунками, контроллером та пристроями — взаємодія між шарами, необхідно для опису балансування, DPI, динамічного керування потоками

ЯКІСТЬ ОБСЛУГОВУВАННЯ, КЕРУВАННЯ З'ЄДНАННЯМИ ТА ЕНЕРГОЕФЕКТИВНІСТЬ

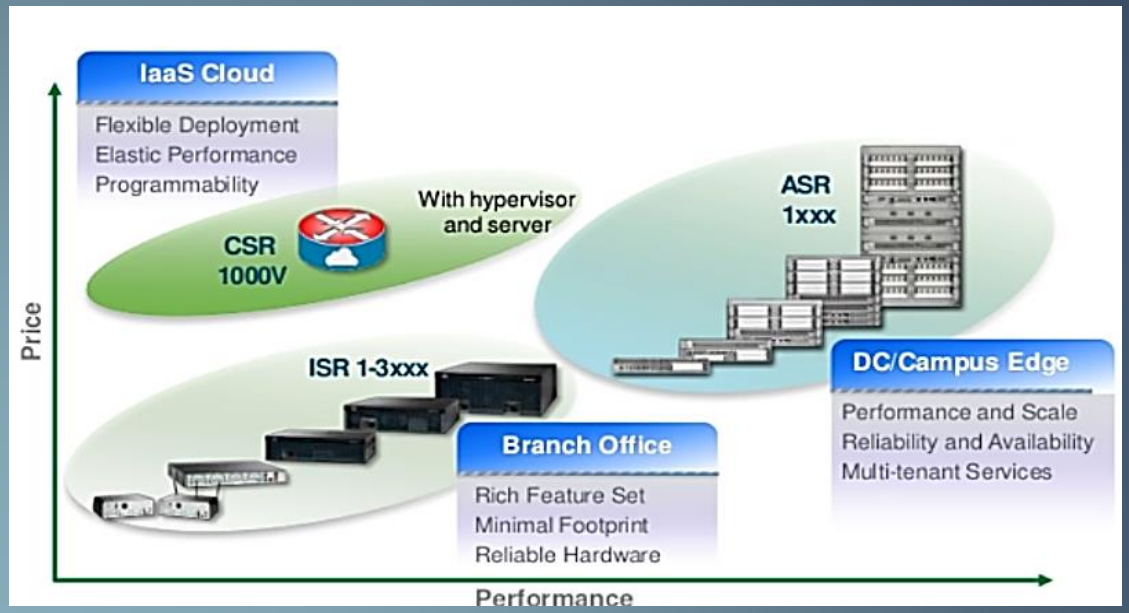
- Якість обслуговування (QoS) є ключовим механізмом, що забезпечує стабільну роботу дата-центрів, дозволяючи ефективно розподіляти ресурси між різними потоками трафіку. Завдяки QoS критично важливі сервіси, як-от VoIP, відеоконференції чи фінансові системи, отримують пріоритет і гарантовану пропускну здатність. Поєднання QoS із технологією SDN забезпечує динамічне керування мережею в реальному часі, адаптацію до змін навантаження й уникнення перевантажень. У сучасних ЦОД QoS не лише підвищує ефективність роботи сервісів, а й мінімізує затримки, втрати пакетів і забезпечує високу якість користувацького досвіду навіть у пікові періоди.



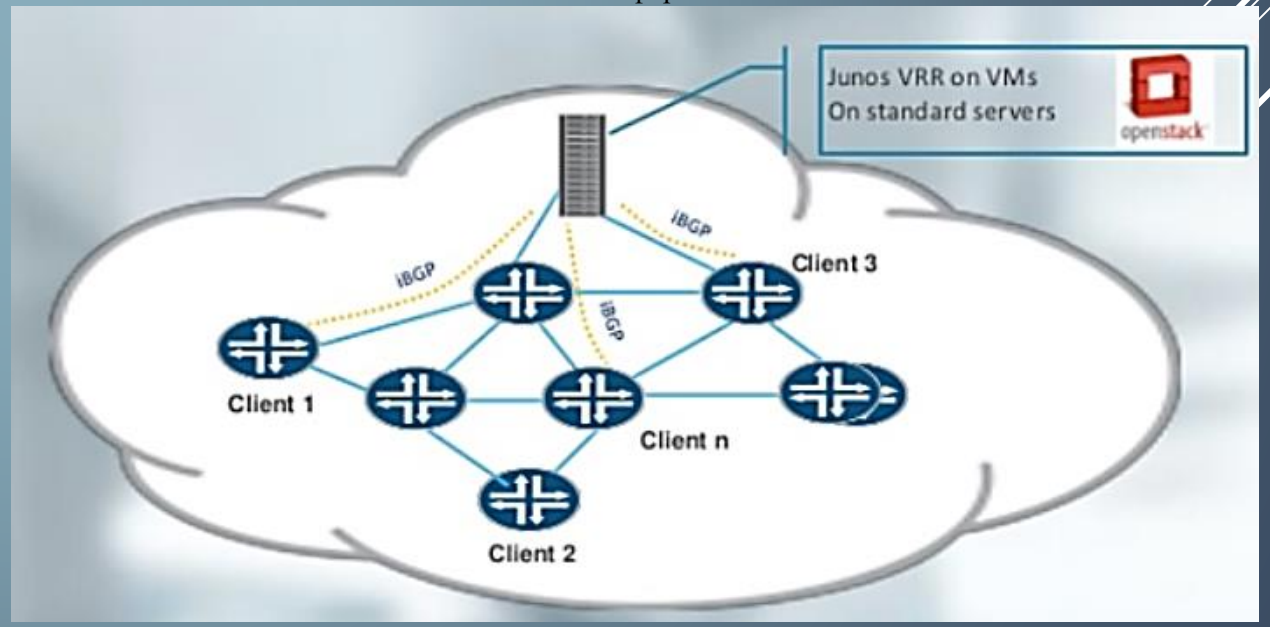
Схема, де контролер SDN керує елементами мережі через політику QoS, відображено, як QoS-mapping та policy engine взаємодіють із пристроями мережі

ВІРТУАЛІЗАЦІЯ МЕРЕЖЕВИХ ФУНКЦІЙ SDN

- Віртуалізація стала основою сучасних мережевих технологій, дозволяючи відокремити програмні функції від апаратного забезпечення. NFV (Network Function Virtualization) переносить мережеві функції — NAT, Firewall, VPN — у віртуальне середовище, зменшуючи витрати й підвищуючи гнучкість. У поєднанні з SDN (Software Defined Networking), що забезпечує централізоване керування, створюється програмно-керована інфраструктура нового покоління. Data Plane відповідає за пересилання даних, а Control Plane — за управління. Саме другий рівень найкраще піддається віртуалізації, що дозволяє оптимізувати CE-маршрутизатори та частково перенести керування P/PE-вузлами у хмару без втрати продуктивності.



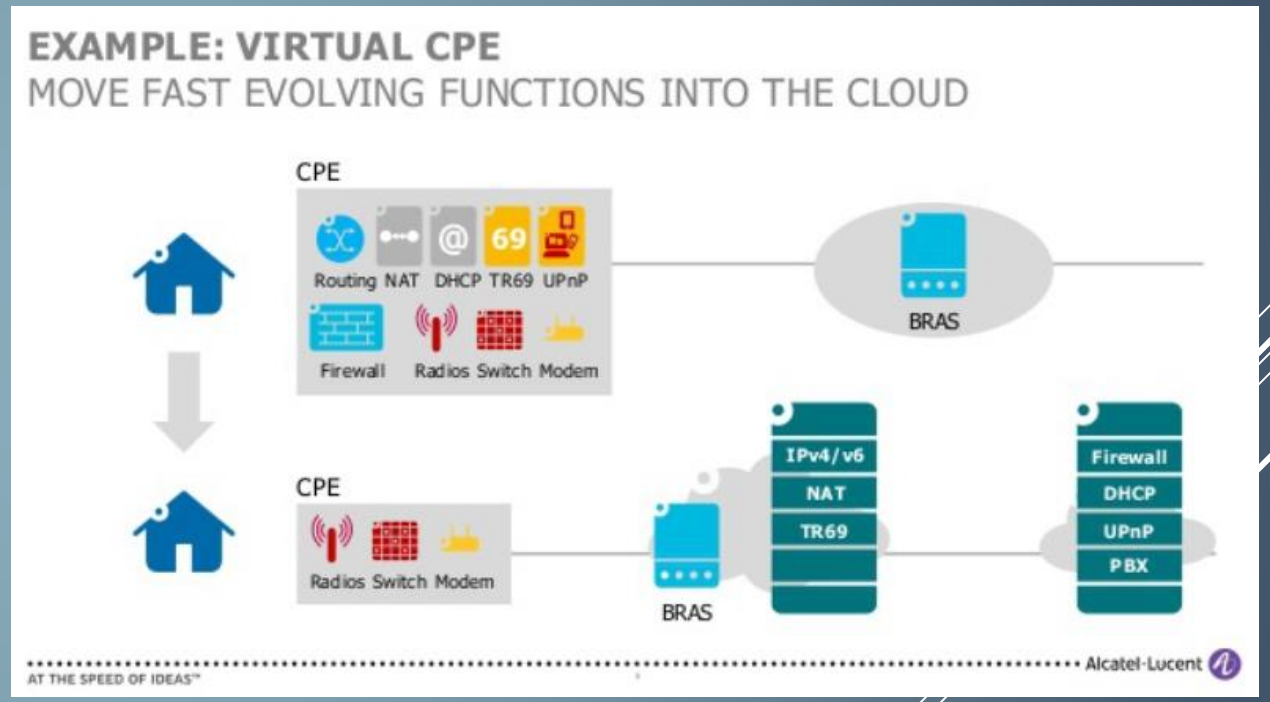
Ніша для застосування віртуального CE-маршрутизатора Cisco CSR1000v щодо апаратних платформ



Віртуалізований BGP Route-Reflector Juniper на стандартному сервері

ТЕХНІЧНІ РІШЕННЯ ДЛЯ УПРАВЛІННЯ ТРАФІКОМ

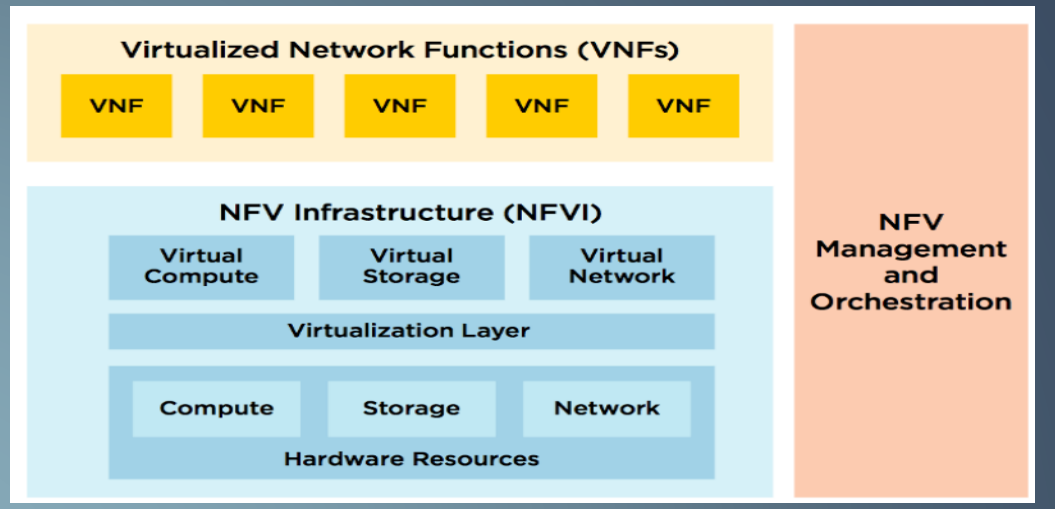
- CPE (Customer Premises Equipment) — це абонентське обладнання, яке забезпечує підключення користувача до мережі провайдера. Воно виконує базові функції, як-от DHCP, NAT, Firewall, проте має обмеження — відсутність прозорості, складність керування й оновлень. Майбутнє CPE — у його віртуалізації (vCPE), коли більшість функцій переноситься у хмару оператора. Це забезпечує централізоване управління, швидке впровадження сервісів і зниження витрат. Аналогічно, часткова віртуалізація BNG, NAT, DPI та систем безпеки дозволяє підвищити гнучкість, масштабованість і автоматизацію.



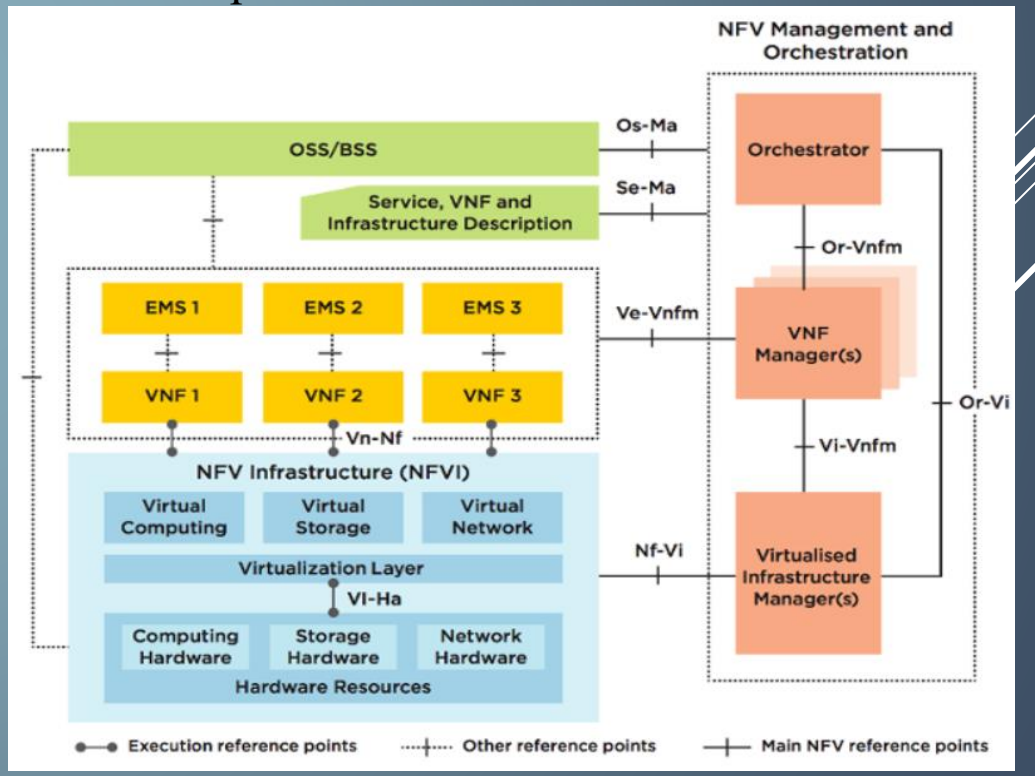
Ілюстрація перенесення мережевих функцій із CPE-пристрою в хмару на прикладі Alcatel

АРХІТЕКТУРА ТА РОЗВИТОК NFV

- Концепція **NFV (Network Functions Virtualization)** виникла у 2013 році за ініціативи **ETSI** та провідних операторів (AT&T, Deutsche Telekom, Verizon тощо) для створення єдиних стандартів віртуалізації мережевих функцій. Згодом сформувалась спільнота **NFV ISG**, а у 2014 році Linux Foundation започаткувала проєкт **OPNFV**, який об’єднав відкриті рішення — OpenStack, Open vSwitch, KVM, Ceph. Архітектура NFV складається з трьох рівнів: **VNF** — віртуалізовані функції; **NFVI** — інфраструктура; **MANO** — система управління та оркестрації. Разом вони забезпечують масштабованість, автоматизацію та інтеграцію з OSS/BSS, формуючи основу мереж нового покоління.



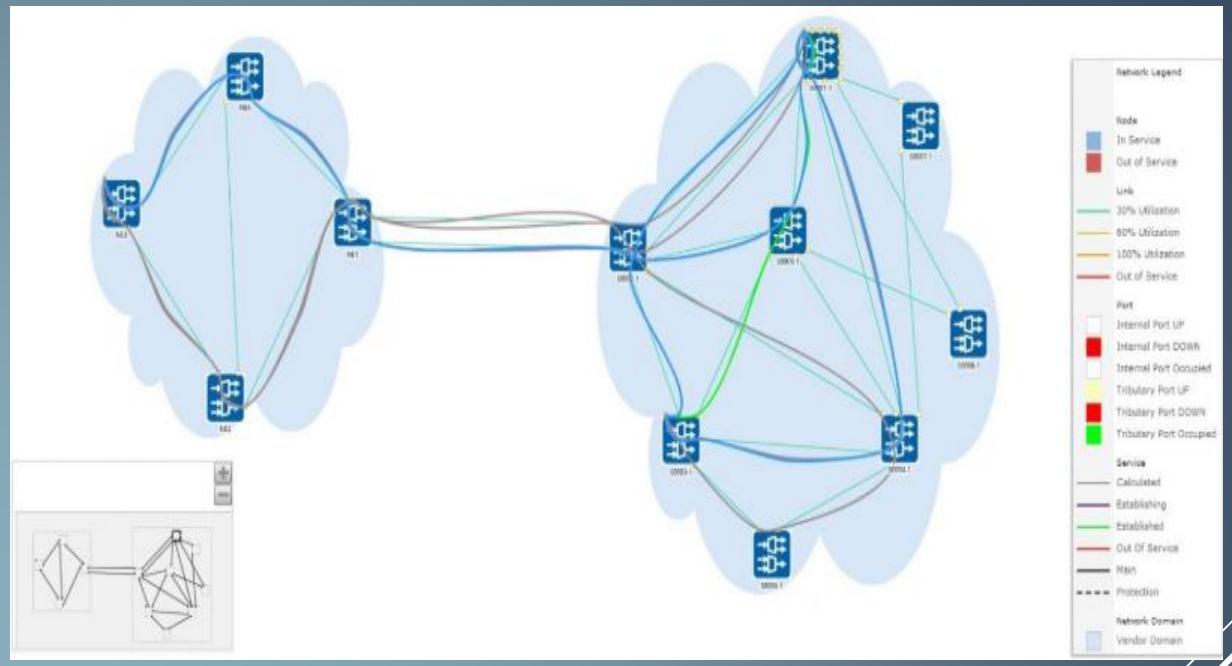
Три основні компоненти NFV



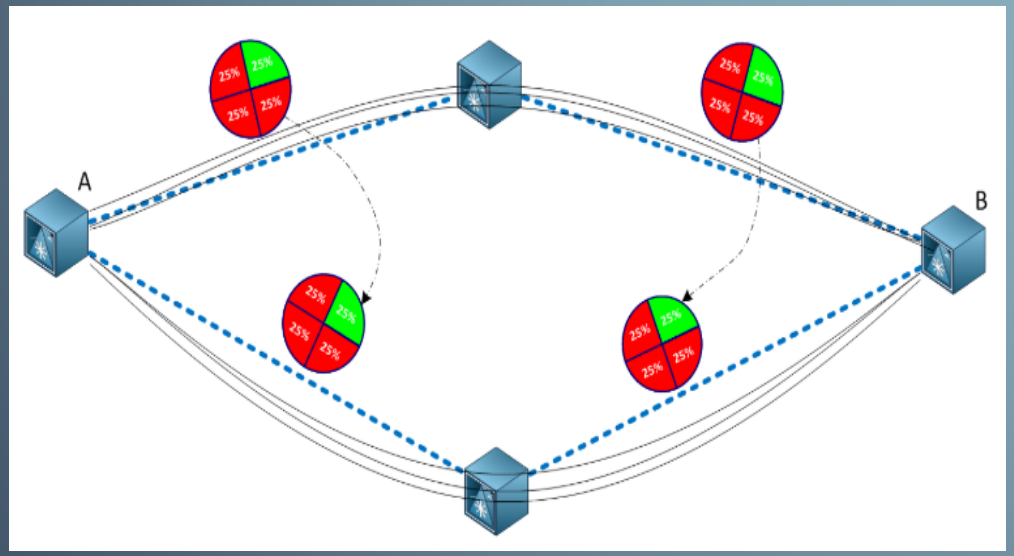
Інтеграція з OSS/BSS

СТРУКТУРА МЕРЕЖІ

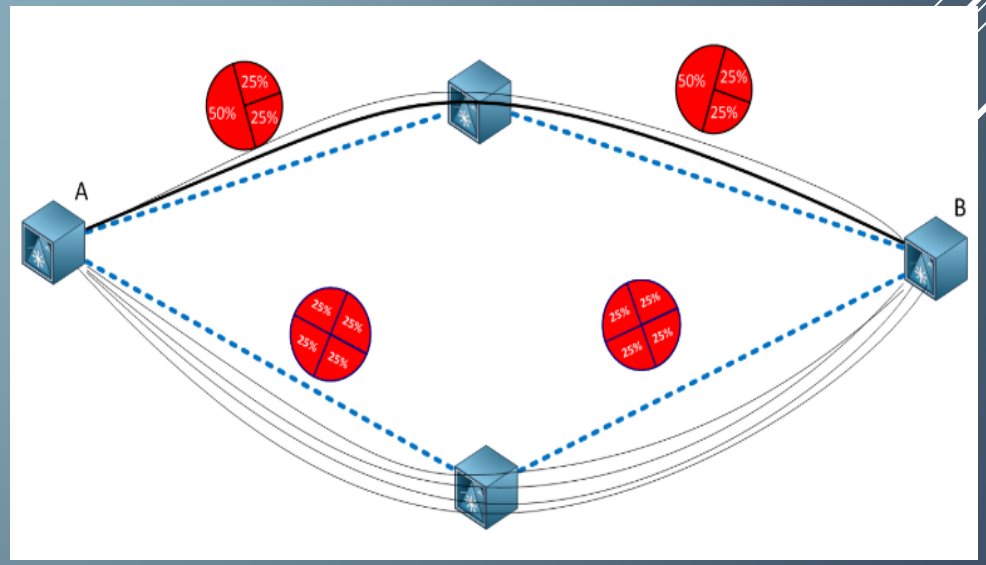
- Технологія **SDN** активно розвивається і виходить за межі дата-центрів, де вона вперше довела ефективність централізованого управління та автоматизації. У 2015 році компанія **NetCracker** впровадила контролер **T-SDN** у транспортній мережі європейського оператора, довівши, що принципи SDN придатні для магістральних систем. Інтеграція з оптичними технологіями **ROADM/WSS**, транспондерами та контейнерами **ODU** забезпечила високу пропускну здатність (до 8 Тбіт/с) і гнучке керування топологією. **T-SDN** підвищує ефективність використання ресурсів, надійність, швидкість надання сервісів і формує основу для інтелектуальних транспортних мереж нового покоління.



Тестова мережа

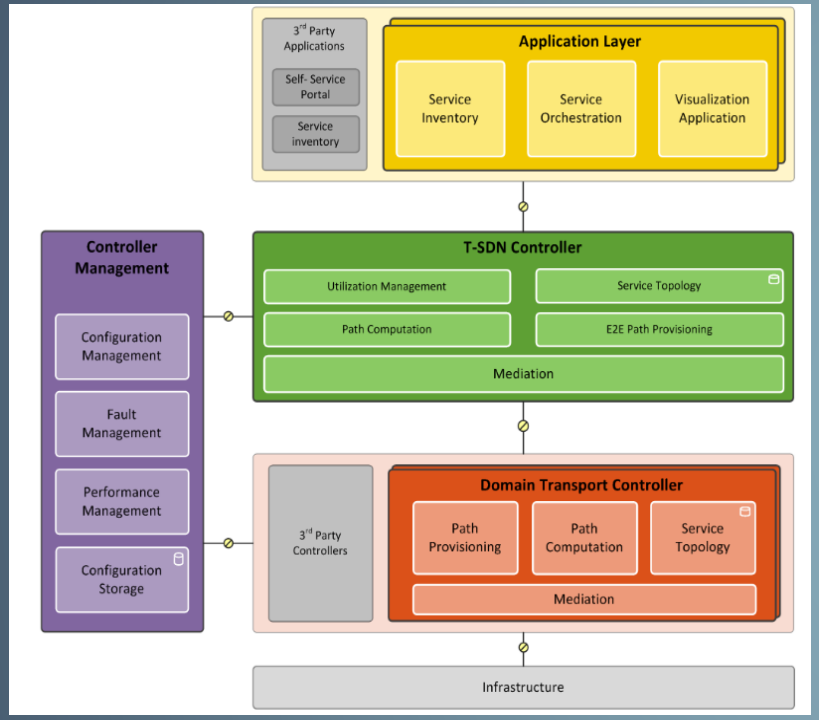


Передача трафіку між двома оптичними пристроями

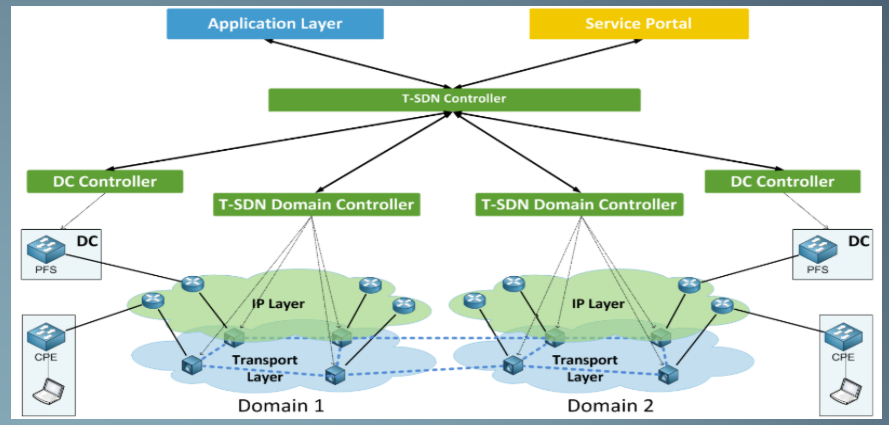


Перенаправлення по альтернативному шляху одного із вже активних клієнтських каналів

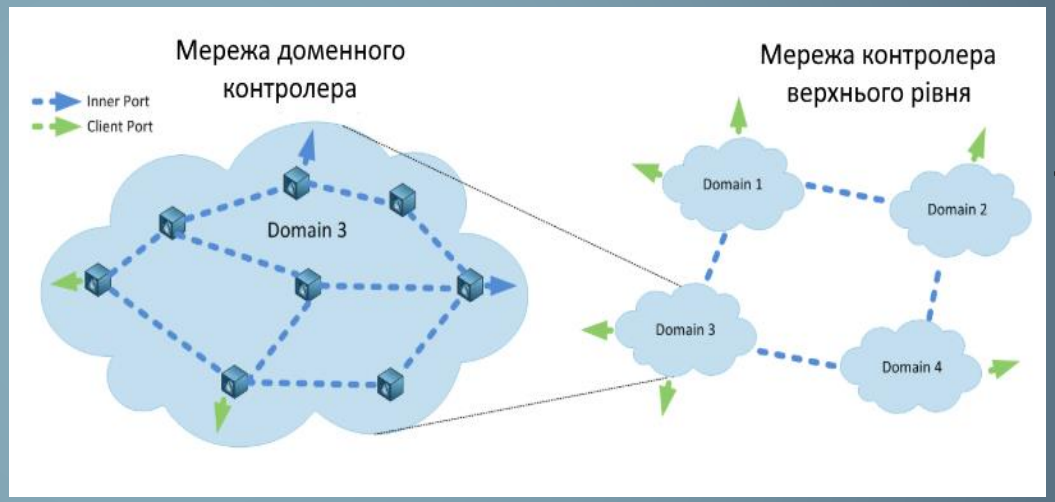
СТРУКТУРА КОНТРОЛЕРА T-SDN



Архітектура контролера T-SDN



Топологія алгоритмів дії контролера T-SDN

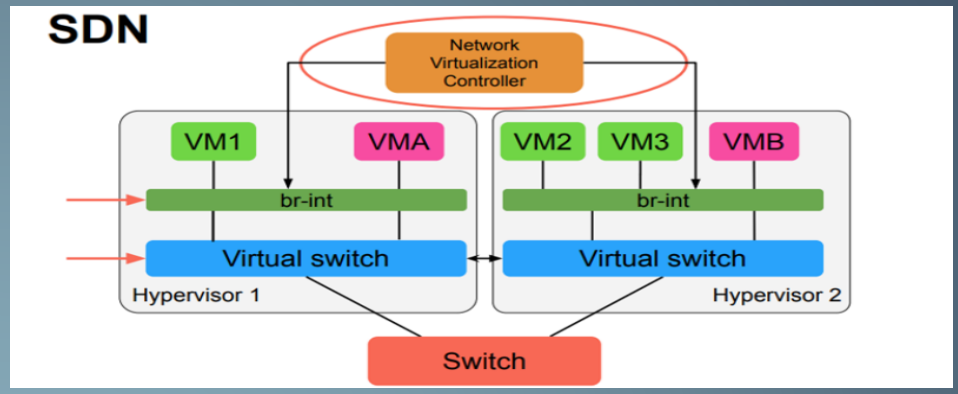


Мережі, керовані доменним контролером T-SDN (управління одним доменом) та контролером T-SDN верхнього рівня (управління всіма доменами

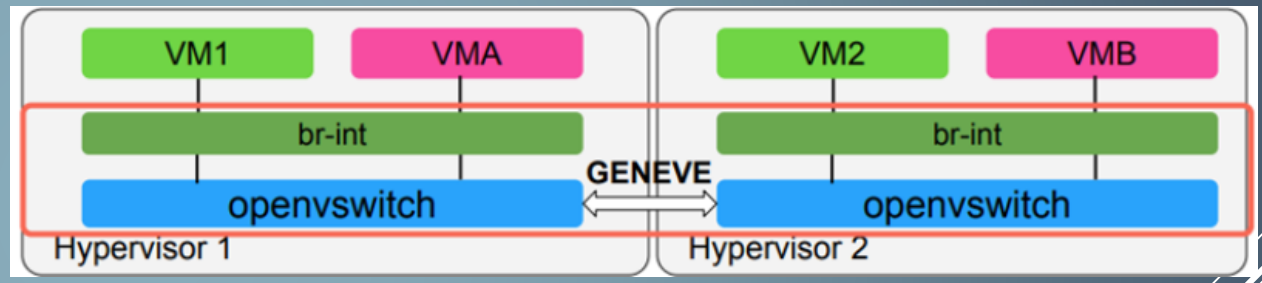
- Під час розробки контролера транспортних мереж головною метою є створення гнучкої, масштабованої та надійної системи, здатної керувати великими інфраструктурами провайдерів. Архітектура **T-SDN** має два рівні: доменний контролер керує окремими сегментами, а центральний — усією мережею, забезпечуючи глобальний контроль і баланс навантаження. Рішення компанії **NetCracker** підтримує мультивендорне середовище, автоматичне прокладання маршрутів, оптимізацію трафіку та концепцію «пропускна здатність на запит». Завдяки модульній структурі та сумісності зі стандартами **ONF**, контролер T-SDN гарантує масштабованість, стабільність і ефективне управління мережами нового покоління.

ВІРТУАЛЬНА МЕРЕЖА

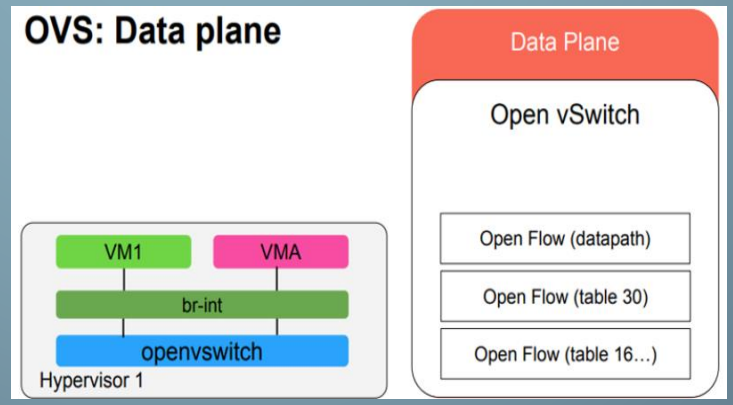
- Інтеграція SDN у системи віртуалізації стала необхідною для забезпечення централізованого управління, масштабованості та автоматизації мереж. Обраний стек **OVN/OVS** довів свою стабільність і високу продуктивність під час тестування. Його архітектура на базі **Open vSwitch** дозволяє створювати єдину логічну мережу поверх фізичної інфраструктури за допомогою Geneve-тунелів. У системі **OVN** реалізовано три рівні: **Data Plane**, **Control Plane** і **Management Plane**, що забезпечують синхронізацію, гнучке керування політиками та масштабовану, відмовостійку віртуальну інфраструктуру з підтримкою тисяч ізольованих сегментів.



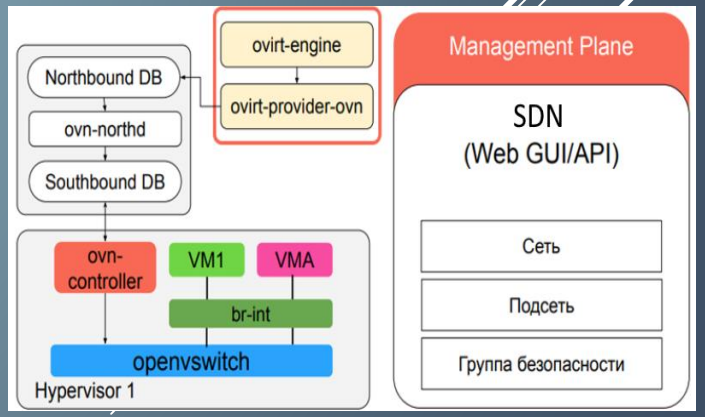
Зразок мережі з єдиною точкою управління



Open vSwitch з’єднуються за допомогою Geneve-тунелів



Конфігурація для Data plane надходить із вищого рівня - з Control plane



Рівень Management plane

ВИСНОВКИ

- У дипломній роботі розглянуто теоретичні та практичні аспекти функціонування програмно-визначених мереж (SDN) і методи управління трафіком у таких системах. Показано, що традиційні підходи до конфігурації мережевого обладнання не забезпечують необхідної гнучкості й масштабованості в умовах сучасних дата-центрів.
- Доведено, що використання SDN дає змогу централізовано керувати потоками даних, автоматизувати конфігурацію, оптимізувати маршрути та впроваджувати політики QoS. Особливу увагу приділено інтеграції SDN з технологією NFV, що забезпечує віртуалізацію мережевих функцій і зниження витрат.
- У роботі проаналізовано ключові проблеми SDN — затримки при оновленні таблиць потоків, різнорідність комутаторів, складність масштабування та енергоспоживання. Запропоновано шляхи їх вирішення за допомогою централізованого управління та інтелектуальної оптимізації ресурсів.
- Показано, що поєднання SDN, NFV і QoS формує основу для побудови гнучких, енергоефективних і надійних телекомунікаційних інфраструктур нового покоління, здатних забезпечити високу якість обслуговування та адаптивність до динамічних навантажень.

ДЯКУЮ ЗА УВАГУ!

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: Павло МАКЕЛЬСЬКИЙ

Назва: МЕТОДИ УПРАВЛІННЯ ТРАФІКОМ У SDN-МЕРЕЖАХ

Координатор: Юрій МЕЛЬНИК

Підрозділ: ННІТ

Коефіцієнт подібності 1:0.17

Коефіцієнт подібності 2:0

Тривога: 0

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*