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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «АНАЛІЗ ТА ВДОСКОНАЛЕННЯ СИСТЕМ МАРШРУТИЗАЦІЇ В ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖАХ (SDN)»

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.

_____ Ернест РОМАНОВСЬКИЙ
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Виконав: здобувач вищої освіти гр. ТСДМ-61
Ернест РОМАНОВСЬКИЙ
Ім'я, ПРІЗВИЩЕ

Керівник: Віталій ТЮРІН
д.т.н., доцент *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

Романовському Ернесту Руслановичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Аналіз та вдосконалення систем маршрутизації в програмно-конфігурованих мережах (SDN)
керівник кваліфікаційної роботи Віталій ТЮРІН, д.т.н., доцент
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» 10. 2025 р. № 467

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

3. Вихідні дані до кваліфікаційної роботи:
1. Системи маршрутизації.
2. Програмно-конфігуровані мережі.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Розвиток SDN.
2. NETSCALER SD-WAN в SDN мережах.
3. Однорангові мережі в SDN.
4. Мережа ADN як альтернатива SDN.

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 _____ Ернест РОМАНОВСЬКИЙ
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Віталій ТЮРІН
(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 Романовський Е.Р. 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: «Аналіз та вдосконалення систем маршрутизації в програмно-конфігурованих мережах (SDN)»

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач Романовський Ернест Русланович 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 Романовського Ернеста Руслановича на оцінку «відмінно» та присвоїти йому кваліфікацію магістр з електронних комунікацій та радіотехніки.

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

«____» _____ 20___ року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Романовський Е.Р. 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 Романовського Ернеста Руслановича
(прізвище, ім'я, по батькові)
на тему «Аналіз та вдосконалення систем маршрутизації в програмно-конфігурованих мережах (SDN)»

Актуальність.
Стрімкий розвиток хмарних сервісів, віртуалізації та розподілених корпоративних інфраструктур зумовлює зростання вимог до гнучкості, масштабованості та керованості комп'ютерних мереж. Традиційні WAN-рішення характеризуються складністю адміністрування, високою вартістю та обмеженою адаптивністю. У цих умовах програмно-конфігуровані мережі (SDN) і технологія SD-WAN забезпечують централізоване управління, автоматизацію маршрутизації та ефективне використання мережевих ресурсів. Для України актуальність теми посилюється потребою модернізації цифрової інфраструктури, підвищення її стійкості та економічної ефективності.
Позитивні сторони.
1. У роботі виконано детальний аналіз архітектурних підходів відкритих SDN-рішень і пропрієтарної платформи Cisco ACI.
2. У роботі обґрунтовано доцільність використання SD-WAN для побудови розподілених корпоративних мереж.
Недоліки.
1. У роботі не подано економічної оцінки впровадження SDN/SD-WAN у порівнянні з традиційними WAN-рішеннями.
2. У роботі недостатньо розглянуто питання інформаційної безпеки SDN-контролерів та SD-WAN-рішень.

Відзначені зауваження не впливають на загальну позитивну оцінку магістерської кваліфікаційної роботи

Висновок: *кваліфікаційна робота на здобуття ступеня магістра заслуговує оцінку "відмінно", а здобувач Романовський Ернест Русланович 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: 83 стор., 27 рис., 2 табл., 25 джерел.

Мета роботи – проаналізувати сучасні підходи до побудови програмно-конфігурованих мереж (SDN) та технології SD-WAN, визначити їхні переваги й обмеження порівняно з традиційними мережевими рішеннями.

Об’єкт дослідження – корпоративні та глобальні комп’ютерні мережі передачі даних, побудовані з використанням програмно-конфігурованих мережевих технологій.

Предмет дослідження – архітектурні принципи, методи маршрутизації та механізми централізованого управління трафіком у мережах SDN і SD-WAN, а також особливості їх реалізації у сучасних мережевих рішеннях.

Короткий зміст роботи: у кваліфікаційній роботі виконано комплексний аналіз підходів до маршрутизації в програмно-конфігурованих мережах (SDN) з урахуванням вимог до масштабованості, гнучкості, відмовостійкості та автоматизації. Розглянуто еволюцію мереж від традиційних архітектур до SDN, обґрунтовано переваги централізованого керування та програмної оптимізації маршрутів. Проаналізовано децентралізовані алгоритми Chord, Kademlia та CAN, проведено їх порівняння за ключовими характеристиками та показано доцільність вибору алгоритмів залежно від сценарію застосування. Окрему увагу приділено технології SD-WAN на прикладі NetScaler SD-WAN, що демонструє практичну ефективність SDN-підходу в глобальних і корпоративних мережах. Узагальнено сучасні тенденції розвитку SDN у напрямі автономних та intent-based мереж.

КЛЮЧОВІ СЛОВА: SDN, SD-WAN, МАРШРУТИЗАЦІЯ, ДЕЦЕНТРАЛІЗОВАНІ АЛГОРИТМИ, CHORD, KADEMLIA, CAN, ОВЕРЛЕЙНІ МЕРЕЖІ, ЦЕНТРАЛІЗОВАНЕ КЕРУВАННЯ, ЯКІСТЬ ОБСЛУГОВУВАННЯ QOS, ВІДМОВОСТІЙКІСТЬ, АВТОМАТИЗАЦІЯ МЕРЕЖ, КОРПОРАТИВНІ МЕРЕЖІ, АВТОНОМНІ МЕРЕЖІ

ABSTRACT

Text part of the master's qualification work: 83 pages, 27 figures, 2 table, 25 sources.

The purpose of the work is to analyze modern approaches to building software-defined networks (SDN) and SD-WAN technology, to determine their advantages and limitations compared to traditional network solutions.

Object of the study is corporate and global computer data transmission networks built using software-defined network technologies.

Subject of the study is architectural principles, routing methods and mechanisms for centralized traffic management in SDN and SD-WAN networks, as well as the features of their implementation in modern network solutions.

Summary of the work: the qualification work provides a comprehensive analysis of routing approaches in software-defined networks (SDN), taking into account the requirements for scalability, flexibility, fault tolerance and automation. The evolution of networks from traditional architectures to SDN is considered, the advantages of centralized management and software optimization of routes are substantiated. The decentralized algorithms Chord, Kademlia and CAN are analyzed, their comparison according to key characteristics is carried out and the expediency of choosing algorithms depending on the application scenario is shown. Special attention is paid to SD-WAN technology using the example of NetScaler SD-WAN, which demonstrates the practical effectiveness of the SDN approach in global and corporate networks. Current trends in SDN development in the direction of autonomous and intent-based networks are summarized.

KEYWORDS: SDN, SD-WAN, ROUTING, DECENTRALIZED ALGORITHMS, CHORD, KADEMLIA, CAN, OVERLAY NETWORKS, CENTRALIZED MANAGEMENT, QUALITY OF SERVICE QOS, FAILURE RESILIENCE, NETWORK AUTOMATION, CORPORATE NETWORKS, AUTONOMOUS NETWORKS

ЗМІСТ

ВСТУП 9
РОЗДІЛ 1 РОЗВИТОК SDN 11
1.1 Концепція та архітектура SDN 11
1.2 SDN від HP 17
1.3 Інтеграція, партнерська система та Cisco ACI 26
РОЗДІЛ 2 NETSCALER SD-WAN В SDN МЕРЕЖАХ 33
2.1 Роль SD-WAN 33
2.2 Побудова SD-WAN на NetScaler 39
2.3 Вдосконалення маршрутизації 42
РОЗДІЛ 3 ОДНОРАНГОВІ МЕРЕЖІ В SDN 50
3.1 Характеристики та проблематика 50
3.2 Рішення та створення топології 54
3.3 Основні алгоритми для модернізації 60
РОЗДІЛ 4 МЕРЕЖА ADN ЯК АЛЬТЕРНАТИВА SDN 74
4.1 Поняття та відмінності 74
4.2 Основні виклики та проблеми модернізації існуючої інфраструктури 79
ВИСНОВКИ 82
ПЕРЕЛІК ПОСИЛАНЬ 84
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 86

ВСТУП

Стрімкий розвиток інформаційних технологій, хмарних обчислень, віртуалізації, мобільних сервісів і розподілених систем суттєво підвищує вимоги до сучасних комп'ютерних мереж. Традиційні підходи до побудови та керування мережевою інфраструктурою дедалі частіше виявляються недостатньо гнучкими, складними в адмініструванні та погано пристосованими до швидких змін навантаження й бізнес-вимог. У таких умовах особливої актуальності набувають програмно-конфігуровані мережі (Software-Defined Networking, SDN), які пропонують принципово нову модель керування та оптимізації мережевих процесів.

Ключовою ідеєю SDN є відокремлення площини керування від площини передачі даних і централізація прийняття рішень щодо маршрутизації та політик обробки трафіка. Такий підхід відкриває можливості для програмної автоматизації, динамічної адаптації маршрутів, інтеграції мережі з прикладними сервісами та зменшення залежності від конкретних вендорів мережевого обладнання. Водночас ефективність SDN значною мірою визначається алгоритмами маршрутизації та механізмами поширення інформації, які використовуються як на рівні контролерів, так і всередині оверлейних та розподілених компонентів мережі.

Особливу роль у сучасних SDN-архітектурах відіграють децентралізовані підходи до маршрутизації, запозичені з однорангових (P2P) систем, блокчейн-платформ і розподілених сервісів. Алгоритми Chord, Kademlia, CAN та подібні до них демонструють різні властивості з точки зору масштабованості, стійкості до відмов, адаптивності та складності реалізації. Їх аналіз і порівняння є важливими для розуміння того, яким чином ці підходи можуть бути використані або вдосконалені в контексті програмно-конфігурованих мереж.

Окрему актуальність має питання маршрутизації у глобальних і корпоративних мережах, зокрема між дата-центрами, хмарними платформами та віддаленими філіями. Рішення класу SD-WAN на базі SDN-підходів демонструють, як програмне керування маршрутами дозволяє підвищити якість сервісів,

оптимізувати використання каналів зв’язку та забезпечити швидке відновлення після аварій. Подальшим етапом еволюції SDN стає перехід до intent-based networking і автономних мереж, здатних самостійно аналізувати свій стан, приймати рішення та відновлювати працездатність із мінімальною участю людини.

Метою даної кваліфікаційної роботи є аналіз існуючих підходів до маршрутизації в програмно-конфігурованих мережах та розгляд напрямів їх удосконалення з урахуванням сучасних тенденцій розвитку SDN, SD-WAN і автономних мереж. Для досягнення поставленої мети у роботі розглядаються теоретичні основи SDN, аналізуються децентралізовані алгоритми маршрутизації та широкомовної розсилки, проводиться їх порівняння за ключовими критеріями, а також оцінюється роль автоматизації й автономності в підвищенні ефективності мережевої інфраструктури.

Практичне значення роботи полягає в можливості використання отриманих результатів під час проєктування, модернізації та експлуатації сучасних програмно-конфігурованих мереж, а також у навчальному процесі при вивченні дисциплін, пов’язаних із комп’ютерними мережами, телекомунікаціями та мережевими технологіями.

1 РОЗВИТОК SDN

1.1 Концепція та архітектура SDN

Сучасний етап розвитку інформаційних технологій характеризується постійним зростанням вимог до гнучкості, масштабованості та адаптивності комп'ютерних мереж. Бізнес-процеси швидко змінюються, з'являються нові сервіси та цифрові платформи, що вимагає від мережевої інфраструктури здатності оперативно підлаштовуватися під нові умови. Очікується, що програмно-конфігуровані мережі зможуть вирішити цілу низку накопичених проблем, сприяючи створенню автоматизованих, програмованих, гнучких та економічно ефективних мережевих рішень. Водночас варто зазначити, що підходи до реалізації концепції SDN у провідних виробників мережевого обладнання суттєво відрізняються, яскравим прикладом чого є стратегії таких компаній, як Cisco та HP.

За оцінками дослідників, витрати на мережеву інфраструктуру становлять близько 17 % загального бюджету на інформаційно-телекомунікаційні технології. Незважаючи на значні фінансові вкладення, традиційні мережі часто виявляються недостатньо гнучкими й не завжди здатними ефективно реагувати на зміну бізнес-потреб. Сучасні тенденції, зокрема активний розвиток віртуалізації, хмарних обчислень, мобільності користувачів, а також стрімке зростання обсягів мережевого трафіку, докорінно змінюють вимоги до побудови та експлуатації мереж. У зв'язку з цим виникає закономірне питання: чи здатні мережеві продукти, що впроваджуються сьогодні, забезпечити підтримку майбутніх додатків і сервісів, а також наскільки розвиток мережі буде залежати від обладнання конкретного виробника комутаторів.

Пропрієтарний характер рішень і архітектурні особливості традиційного мережевого обладнання роблять таку залежність надзвичайно сильною. Це обмежує свободу вибору замовників і ускладнює модернізацію мережі без повної заміни апаратних компонентів. Саме тому деякі фахівці навіть називають поточну ситуацію в мережевій галузі революційною, адже накопичені проблеми потребують

принципово нових підходів. Як один із ключових шляхів їх подолання експерти розглядають перехід до архітектури програмно-конфігурованих або програмно-керованих мереж — Software-Defined Networking (SDN). Дана концепція передбачає відокремлення рівня керування від рівня передачі даних, що дозволяє централізовано управляти мережею та значно підвищувати її гнучкість.

У підсумку, впровадження SDN обіцяє істотно зменшити залежність замовників від технологій конкретного вендора, спростити управління мережею та створити умови для більш ефективного використання ресурсів. Це робить програмно-конфігуровані мережі перспективним напрямом розвитку сучасних телекомунікаційних систем і мережевих інфраструктур.

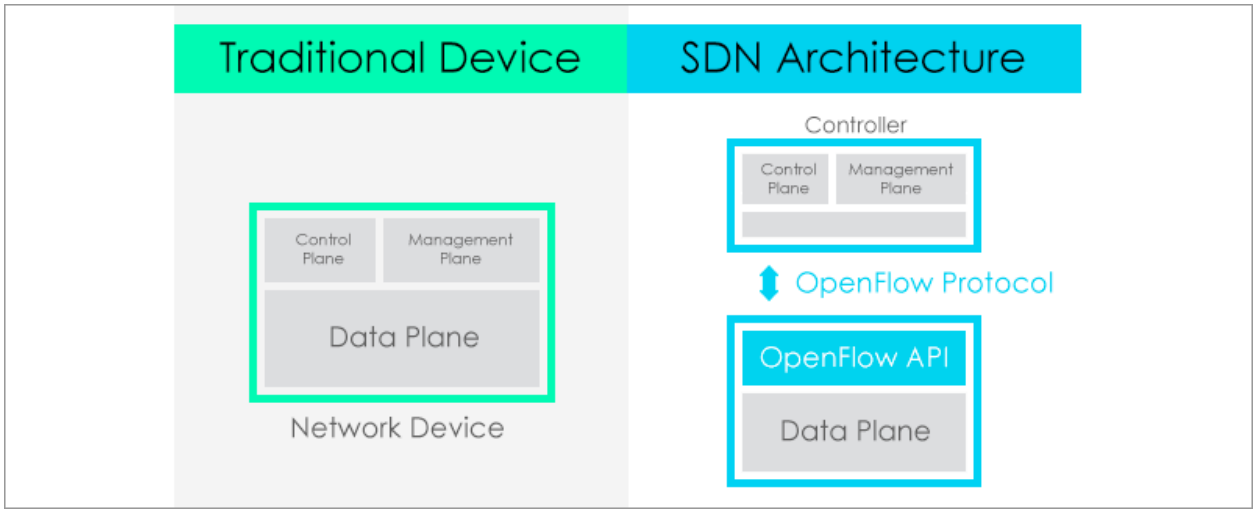


Рис. 1.1 У SDN вся логіка управління мережевими пристроями виноситься в так звану "площину управління", яка реалізується програмним чином. Конструктивно контролери можуть будуватися або з урахуванням фізичних, або віртуальних хостів. Управління мережевими пристроями, зазвичай, здійснюється за протоколом OpenFlow

Основна концепція програмно-визначених мереж (Software-Defined Networking, SDN) полягає в чіткому розділенні функцій передавання мережевого трафіка та функцій керування мережею. У традиційних мережевих пристроях, таких як комутатори та маршрутизатори, ці процеси тісно пов’язані між собою і реалізуються безпосередньо на одному й тому самому обладнанні. Кожен пристрій самостійно приймає рішення щодо маршрутизації та комутації пакетів, що ускладнює централізоване керування мережею та її масштабування. У моделі SDN,

навпаки, мережева інфраструктура, що може складатися з великої кількості пристроїв різних виробників, сприймається прикладними системами як єдиний логічний комутатор із централізованим керуванням.

Завдяки такому підходу адміністратори отримують можливість програмувати мережу як цілісну систему, а не налаштовувати кожен окремий комутатор чи маршрутизатор вручну. Мережеві пристрої в SDN виконують роль простих елементів передавання даних, які діють відповідно до інструкцій, отриманих від централізованого контролера. Це суттєво знижує складність управління мережею, зменшує ймовірність помилок конфігурації та спрощує процес адміністрування, особливо у великих і географічно розподілених мережах.

Реалізація концепції SDN істотно полегшує експлуатацію мережевої інфраструктури та її налаштування. Оскільки основна логіка керування переноситься на програмний рівень, комутатори можуть мати спрощену архітектуру, що робить їх дешевшими у виробництві та впровадженні. Адміністратори можуть оперативно змінювати параметри роботи мережі в режимі реального часу, швидко адаптуючи її до нових вимог бізнесу або навантажень. Це, у свою чергу, значно скорочує час впровадження нових додатків, сервісів і мережевих функцій, а також підвищує загальну ефективність використання мережевих ресурсів.

Важливою складовою SDN є наявність програмних інтерфейсів прикладного програмування (API), які надаються контролером. За допомогою цих інтерфейсів розробники можуть створювати спеціалізовані програмні додатки для керування мережею, автоматизації її роботи та реалізації складних політик обслуговування трафіка. Такі додатки здатні виконувати широкий спектр завдань — від балансування навантаження і забезпечення якості обслуговування до підвищення рівня безпеки та моніторингу стану мережі. При цьому розробникам не потрібно глибоко знати особливості внутрішньої реалізації конкретних мережевих пристроїв, оскільки взаємодія відбувається через уніфіковані та відкриті інтерфейси.

На перший погляд може здатися, що подібний підхід не повинен викликати зацікавленості у виробників мережевого обладнання. Протягом багатьох років вони інвестували значні ресурси в розробку унікальних апаратних і програмних функцій своїх комутаторів та маршрутизаторів, які й становили основну додану вартість їхніх продуктів. Можливість використання простих і відносно недорогих комутаторів, а також створення керуючих додатків сторонніми розробниками на основі відкритих API, потенційно підриває традиційні бізнес-моделі таких компаній і зменшує їхній вплив на ринок.

Однак реалії ринку свідчать про інше. Великі замовники, зокрема провідні оператори зв'язку та інтернет-провайдери, уже усвідомили переваги програмно-визначених мереж і активно підтримують ідеї SDN. Додатковим стимулом для розвитку цієї концепції стала підтримка протоколу OpenFlow з боку виробників мікросхем для мережевих комутаторів. У таких умовах вендори мережевого обладнання не можуть залишатися осторонь і змушені адаптувати свої стратегії, інтегруючи принципи SDN у власні продукти та рішення. У підсумку SDN стає не лише технологічним трендом, а й важливим елементом еволюції сучасних мережевих інфраструктур.

Сьогодні створення власного мережевого комутатора, що працює за протоколом OpenFlow, стало можливим навіть для компаній, які не мають багаторічного досвіду у сфері мережевих технологій. Це пояснюється тим, що логіка керування мережею в архітектурі SDN значною мірою виноситься на програмний рівень, а апаратна частина комутатора спрощується. У результаті знижується поріг входу на ринок мережевого обладнання, і до нього можуть долучатися нові гравці, зокрема стартапи та компанії з інших галузей інформаційних технологій.

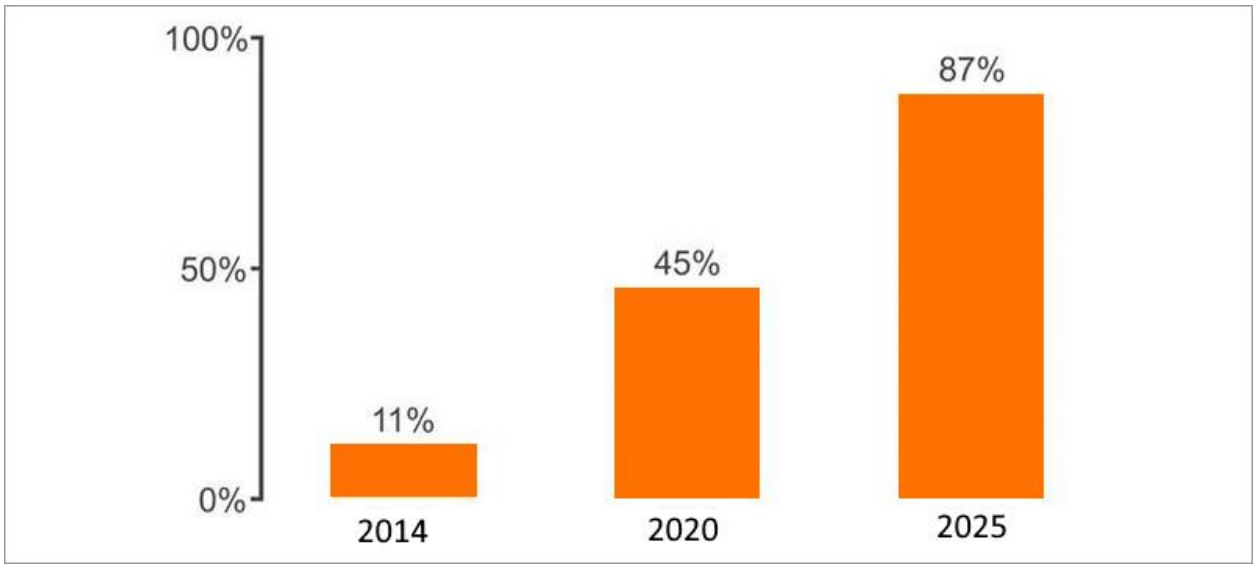


Рис. 1.2 За даними опитувань (липень, 2020 року), понад 87% середніх та великих підприємств планують до 2026 року запустити SDN у своїх ЦОД в експлуатацію

Важливу роль у розвитку цього підходу відіграє організація Open Network Foundation (ONF), яка об’єднує прихильників концепції «відкритих мереж», побудованих на основі протоколу OpenFlow. Кількість учасників ONF постійно зростає, і до її складу входять не лише виробники мережевого обладнання, а й оператори зв’язку, хмарні провайдери, розробники програмного забезпечення та наукові установи. Така широка підтримка сприяє формуванню відкритої екосистеми, у межах якої розробка, тестування та впровадження SDN-рішень відбуваються значно швидше й ефективніше, ніж у рамках традиційних закритих підходів.

У цих умовах бізнес-моделі Cisco та інших класичних виробників комутаторів і маршрутизаторів потенційно опиняються під загрозою. Аналітики відзначають, що у разі масового впровадження SDN обсяги продажів традиційного мережевого обладнання можуть істотно скоротитися. За оцінками експертів, повсюдне прийняття програмно-визначених мереж здатне більш ніж удвічі зменшити оборот одного з найбільших гравців ринку — компанії Cisco. Це зумовлено тим, що цінність поступово зміщується з унікальних апаратних рішень у бік програмного забезпечення, сервісів і відкритих стандартів.

У будь-якому разі SDN суттєво трансформує мережевий ринок, кардинально змінюючи підходи до проєктування, розгортання та управління мережами.

Традиційні методи побудови мереж, що базуються на жорстко прив’язаних до обладнання конфігураціях, поступаються місцем програмному керуванню, автоматизації та орієнтації на потреби прикладних сервісів. Це також впливає на механізми доставки додатків і сервісів, які стають більш гнучкими, динамічними та адаптованими до реальних умов експлуатації.

Водночас традиційні мережеві вендори по-різному сприймають ідеї SDN та по-своєму вибудовують стратегії розвитку. Такі великі гравці ринку, як Cisco та HP, почали формувати власні підходи до програмно-конфігурованих мереж ще кілька років тому, задовго до масового поширення цієї концепції. Їхні стратегії відображають різне бачення майбутнього мережевих технологій та ролі відкритих стандартів у цьому процесі.

Зокрема, у 2012 році з’явилася інформація про те, що компанія Cisco Systems може представити пропрієтарні мережеві продукти, які реалізують основні принципи SDN, але не обов’язково використовують протокол OpenFlow. Такий підхід передбачає збереження контролю над екосистемою власних рішень і мінімізацію залежності від відкритих стандартів. Водночас компанія HP оголосила про широку підтримку стандартного протоколу OpenFlow у багатьох своїх мережевих продуктах, наголосивши на важливості відкритості та сумісності.

У галузі швидко сформувалася думка, що в контексті SDN ці компанії пішли принципово різними шляхами розвитку: Cisco — у напрямі пропрієтарних рішень, а HP — у напрямі відкритих стандартів і міжвендорної взаємодії. Керівники HP неодноразово підкреслювали, що саме відкриті стандарти та сумісність з обладнанням інших виробників є основою довгострокового розвитку мережевих технологій і відповідають інтересам замовників. На їхню думку, пропрієтарний підхід обмежує свободу вибору та ускладнює еволюцію мереж, тоді як відкриті рішення створюють більш конкурентне, інноваційне та гнучке середовище для всіх учасників ринку.

1.2 SDN від HP

Насправді компанія HP почала рух у напрямі програмно-визначених мереж значно раніше, ніж SDN стала загальновизнаною та масово обговорюваною концепцією у професійному середовищі. Ще у 2008 році на одній з найавторитетніших міжнародних конференцій у галузі комп'ютерних мереж — ACM SIGCOMM — було продемонстровано комутатор HP із підтримкою протоколу OpenFlow. На той момент це був не просто технічний експеримент, а фактичне підтвердження працездатності ідеї відокремлення рівня керування від рівня передавання даних. Така демонстрація стала важливою віхою у розвитку SDN і засвідчила, що HP розглядає відкриті мережеві стандарти як стратегічний напрям розвитку своєї мережевої екосистеми.

Подальший практичний розвиток цієї концепції відбувся у 2012 році, коли підрозділ HP Networking представив дев'ять нових моделей комутаторів серії HP 3800, у яких була реалізована підтримка протоколу OpenFlow на рівні промислових рішень. Цей крок означав перехід від наукових і пілотних реалізацій до комерційно доступного обладнання, придатного для використання в корпоративних мережах, центрах обробки даних та операторських середовищах. Фактично HP запропонувала замовникам реальний інструмент для поступового впровадження SDN без необхідності повної відмови від існуючої мережевої інфраструктури.

Наступним етапом стала поява повноцінного програмного комплексу SDN від HP, який включав не лише апаратну підтримку OpenFlow, а й власний SDN-контролер, а також набір програмних інтерфейсів прикладного програмування (API). Завдяки цим інтерфейсам сторонні розробники отримали можливість створювати власні SDN-додатки для централізованого керування мережею, автоматизації конфігурації, реалізації політик безпеки, балансування навантаження та інтеграції мережі з бізнес-процесами. Таким чином, HP зробила акцент не лише на постачанні обладнання, а й на формуванні відкритої програмної платформи, здатної підтримувати інновації.

На сьогодні практично вся лінійка комутаторів і маршрутизаторів HP підтримує протокол OpenFlow. Важливою особливістю такого підходу є можливість подвійного режиму роботи: те саме обладнання може функціонувати як у традиційних мережах із локальним керуванням на кожному пристрої, так і в програмно-конфігурованих мережах під централізованим керуванням SDN-контролера HP. Це забезпечує плавний та контрольований перехід до SDN, дозволяє уникнути різких змін архітектури та мінімізує ризики для підприємств і операторів зв'язку.

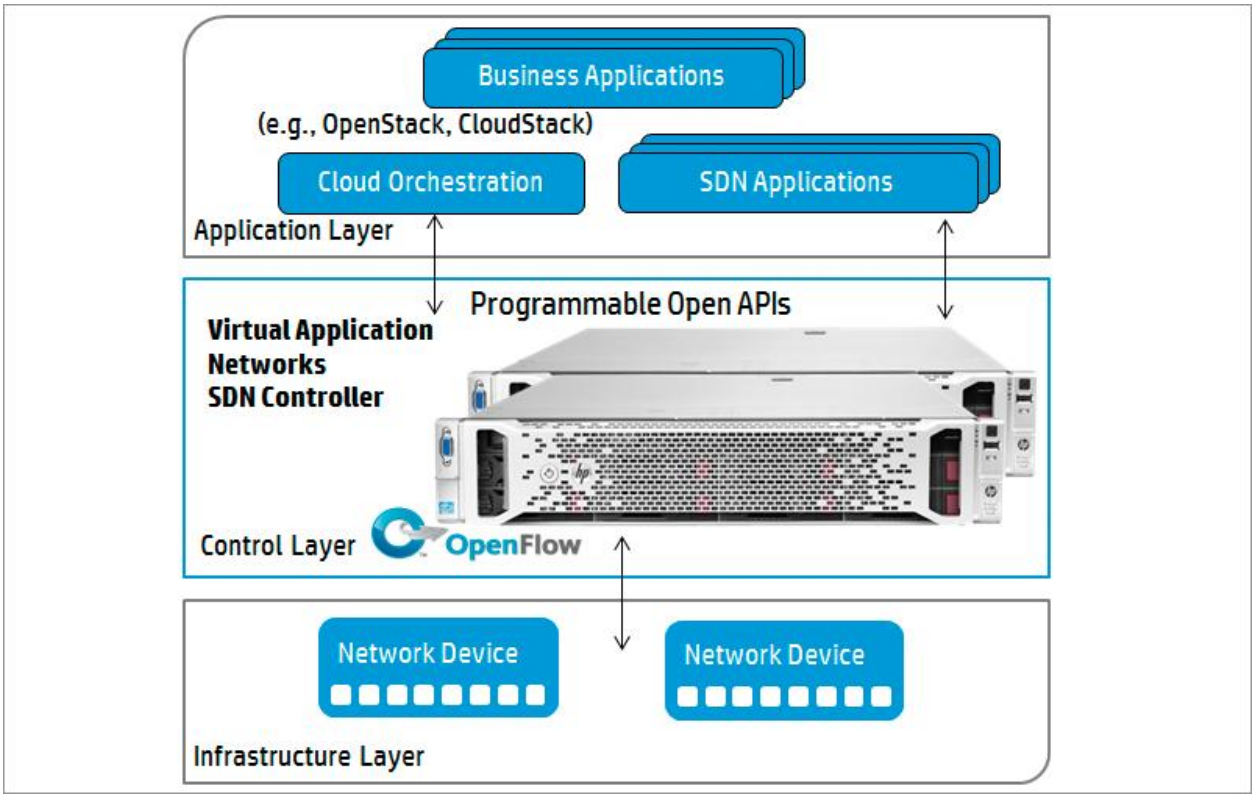


Рис. 1.3 HP Virtual Application Networks SDN Controller

У 2013 році компанія HP офіційно представила HP Virtual Application Networks SDN Controller. Це рішення було доступне як у вигляді програмного забезпечення, так і у формі готового апаратно-програмного комплексу на базі серверів HP ProLiant. Контролер може бути встановлений на фізичному сервері, у віртуальному середовищі або розгорнутий у вигляді кластерної конфігурації, що дозволяє досягти високої продуктивності, масштабованості та відмовостійкості. Така гнучкість архітектури робить контролер придатним як для невеликих

корпоративних мереж, так і для великих дата-центрів або операторських SDN-інфраструктур.

Функціонально SDN-контролер HP реалізує динамічне конфігурування мережевих пристроїв на основі правил і політик, заданих адміністраторами або прикладними системами. Взаємодія з комутаторами та іншими елементами інфраструктури здійснюється через протокол OpenFlow, що забезпечує централізоване управління потоками трафіка, швидку зміну маршрутів та оперативну реакцію на зміни мережевого навантаження або аварійні ситуації.

Окрім базових функцій керування потоками, контролер HP має широкий набір вбудованих сервісів. До них належать механізми мережевої віртуалізації, засоби керування та оптимізації трафіка, інструменти підвищення безпеки, а також функції моніторингу та аналізу стану мережі. Значну увагу приділено питанням контролю доступу: реалізовані механізми аутентифікації та авторизації, які дозволяють регламентувати доступ як до внутрішніх компонентів контролера, так і до зовнішніх SDN-додатків.

Для взаємодії з зовнішніми системами та прикладними рішеннями HP використовує RESTful-інтерфейс, побудований на принципах технології REpresentational State Transfer (REST). Завдяки цьому SDN-контролер може легко інтегруватися з системами оркестрації, платформами управління хмарною інфраструктурою, системами моніторингу та бізнес-додатками. Це забезпечує тісний зв’язок між мережею та IT-сервісами, перетворюючи мережеву інфраструктуру на активний елемент цифрових бізнес-процесів.

У компанії HP підкреслюють, що OpenFlow є важливим, але не єдиним компонентом SDN. Для побудови повнофункціональної програмно-визначеної мережі також використовуються інші механізми динамічного керування пристроями, зокрема NETCONF та OVSDB. Водночас особлива увага приділяється стандартизації взаємодії між рівнем керування та мережевою інфраструктурою (так званий «південний інтерфейс»), а також між контролером і прикладними системами («північний інтерфейс»), де ключову роль відіграють REST-API.

Окремою і все ще актуальною проблемою залишається взаємодія SDN-контролерів різних виробників. На практиці лише обмежена кількість вендорів активно працює над забезпеченням міжвендорної сумісності своїх рішень. Одним із показових прикладів у цьому напрямі є інтеграція SDN-контролера HP з платформою VMware NSX, що демонструє можливість створення гібридних та багатовендорних SDN-архітектур. Такий підхід відкриває шлях до побудови більш гнучких, масштабованих і відкритих мереж, здатних ефективно підтримувати сучасні та майбутні цифрові сервіси.

Застосунки SDN

На базі SDN-контролера компанії HP вже сформовано цілу екосистему прикладних рішень, орієнтованих на централізоване та програмне управління мережами. Ці застосунки є ключовим елементом концепції програмно-визначених мереж, оскільки саме вони перетворюють SDN із суто інфраструктурної технології на гнучку та інтелектуальну платформу для керування мережевими ресурсами відповідно до потреб бізнесу та прикладних сервісів.

Частина SDN-застосунків розроблена безпосередньо компанією HP. До таких рішень, зокрема, належать Net Optimizer та Net Protector. Застосунок Net Optimizer орієнтований на оптимізацію мережевого трафіка, підвищення ефективності використання пропускної здатності та покращення якості обслуговування (QoS) для критично важливих сервісів і додатків. Він дозволяє динамічно керувати потоками даних, адаптувати маршрутизацію до поточного навантаження та швидко реагувати на зміни в роботі мережі. У свою чергу, Net Protector зосереджений на питаннях мережевої безпеки, забезпечуючи централізоване впровадження політик захисту, контроль доступу та швидке виявлення потенційних загроз на рівні мережевих потоків.

Окрім власних рішень HP, значна кількість SDN-застосунків створюється партнерськими компаніями, а також відкритою спільнотою розробників. Такий підхід сприяє формуванню відкритої інноваційної екосистеми, у межах якої з’являються спеціалізовані додатки для різних галузей і сценаріїв використання — від корпоративних мереж і дата-центрів до операторських і хмарних інфраструктур.

Розробники можуть зосередитися на логіці керування та інтеграції з бізнес-додатками, не заглиблюючись у специфіку роботи конкретних мережевих пристроїв.

У сукупності ці застосунки дозволяють створити комплексне середовище SDN, яке включає кілька взаємопов’язаних рівнів: прикладні SDN-додатки, SDN-контролер як центральний елемент управління та мережеву інфраструктуру з підтримкою протоколу OpenFlow. У такій архітектурі саме контролер виступає посередником між додатками та фізичною мережею, забезпечуючи уніфікований доступ до мережевих ресурсів і їх централізоване керування.

Ключовою перевагою подібного підходу є можливість автоматизації процесів динамічного управління мережею в режимі реального часу. Застосунки можуть надсилати запити до SDN-контролера «на льоту», ініціюючи зміну мережевих параметрів відповідно до поточних потреб. Наприклад, при запуску нового сервісу мережа може автоматично виділити необхідні ресурси, налаштувати маршрутизацію та політики безпеки без участі адміністратора. Це значно скорочує час реакції мережі на зміни та зменшує залежність від ручного налаштування.

У результаті підвищується ефективність використання інфраструктурних ресурсів, оскільки мережа адаптується до реальних навантажень і вимог додатків. Одночасно зростає гнучкість мережевої інфраструктури, яка може швидко масштабуватися, змінювати конфігурацію та підтримувати нові сервіси без значних капітальних витрат. У довгостроковій перспективі це також сприяє зниженню сукупної вартості володіння (TCO), оскільки автоматизація, централізоване керування та використання відкритих стандартів зменшують витрати на експлуатацію, адміністрування та модернізацію мережі.

Стратегія SDN

У компанії HP послідовно наголошують на своїй відданості принципам відкритих мережевих рішень, які базуються на стандартах і забезпечують замовникам максимальну свободу вибору та інвестиційний захист. Такий підхід спрямований на те, щоб якнайповніше розкрити потенціал сучасних бізнес-додатків і водночас уже сьогодні підготувати мережеву інфраструктуру до

повномасштабного впровадження технологій Software-Defined Networking (SDN) з мінімальними фінансовими та організаційними витратами. HP розглядає SDN не як разову технологічну зміну, а як поетапну еволюцію мереж, що має бути інтегрована в довгострокову IT-стратегію підприємств.

Центральним елементом SDN-стратегії HP є комплексна (end-to-end) автоматизація мережевої інфраструктури — від центрів обробки даних (ЦОД) до кампусних мереж і віддалених філій компаній. Саме такий наскрізний підхід дозволяє усунути фрагментацію управління мережею та забезпечити єдині політики керування, безпеки й якості обслуговування на всіх рівнях. Тому рішення HP у сфері SDN не обмежуються лише мережами ЦОД, а охоплюють також філіальні, кампусні та глобальні мережі, де питання гнучкого та ефективного управління ресурсами є не менш актуальними.

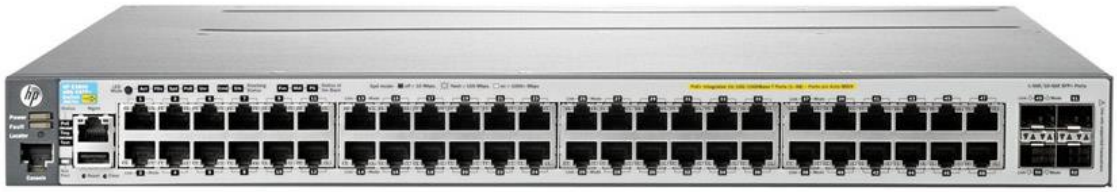


Рис. 1.4 HP 3800 Series — загальний вигляд обладнання серії 3800, яке включає моделі з різними конфігураціями портів та можливостями управління

У сучасних розподілених корпоративних середовищах мережі філій і глобальні мережі стикаються з такими ж складними завданнями, як і дата-центри: необхідністю швидкої адаптації до змін навантаження, підтримки мобільних користувачів, інтеграції з хмарними сервісами та забезпечення належного рівня

безпеки. У межах своєї SDN-стратегії HP прагне забезпечити єдину модель керування всією мережею підприємства, незалежно від її масштабу чи географічного розташування.

Компанія HP рекомендує замовникам уже на поточному етапі готуватися до впровадження SDN, навіть якщо повномасштабний перехід планується в середньостроковій перспективі. Зокрема, йдеться про доцільність придбання мережевого обладнання з підтримкою SDN-технологій, таких як OpenFlow та інші механізми програмного керування. Важливим кроком також є створення тестових або пілотних зон, у межах яких можна перевірити сумісність існуючої мережевої інфраструктури з SDN-додатками та оцінити потенційні переваги програмно-визначеного підходу.

Після успішної апробації окремі SDN-рішення можуть поступово впроваджуватися в промислову експлуатацію, не порушуючи стабільність роботи всієї мережі підприємства. Такий еволюційний підхід дозволяє знизити ризики, розподілити витрати в часі та накопичити практичний досвід роботи з SDN-технологіями. Якщо підприємство розпочне впровадження програмно-конфігурованих мереж уже сьогодні, то через кілька років воно зможе розгорнути повноцінну SDN-інфраструктуру, яка забезпечить високу гнучкість, масштабованість і помітне підвищення ефективності бізнес-процесів.

У довгостроковій перспективі зростання кількості доступних SDN-застосунків і розширення екосистеми партнерських рішень стане ключовим чинником масового впровадження SDN у корпоративних мережах. Чим більше прикладних сценаріїв і готових рішень з’являтиметься на ринку, тим швидше компанії будуть переходити від традиційних мереж до програмно-визначених архітектур. Аналітики IDC прогнозують, що ринок мережевих SDN-застосунків продовжить активно зростати і до 2027 року досягне обсягу близько 3,1 млрд доларів США, що додатково підтверджує стратегічну важливість SDN як одного з ключових напрямів розвитку сучасних мережевих технологій.

SDN App Store

У межах розвитку екосистеми програмно-визначених мереж компанія HP запустила проєкт HP SDN App Store — спеціалізовану електронну платформу для корпоративного сегмента, орієнтовану на поширення та впровадження SDN-застосунків. Метою створення цього майданчика стало формування централізованого середовища, у якому замовники, розробники та партнери можуть отримувати доступ до готових програмних рішень для керування мережею, а також до інструментів їх розробки та інтеграції.

Асортимент HP SDN App Store охоплює широкий спектр прикладних рішень, що вирішують різноманітні завдання сучасних корпоративних мереж. Серед них — застосунки для підвищення рівня мережевої безпеки, централізованого контролю доступу, управління та оптимізації трафіка, а також рішення для підтримки хмарних обчислень, мобільності користувачів і віртуалізованих середовищ. Такий підхід дозволяє організаціям підбирати SDN-функціональність відповідно до власних бізнес-потреб без необхідності глибокого втручання в апаратну частину мережі.

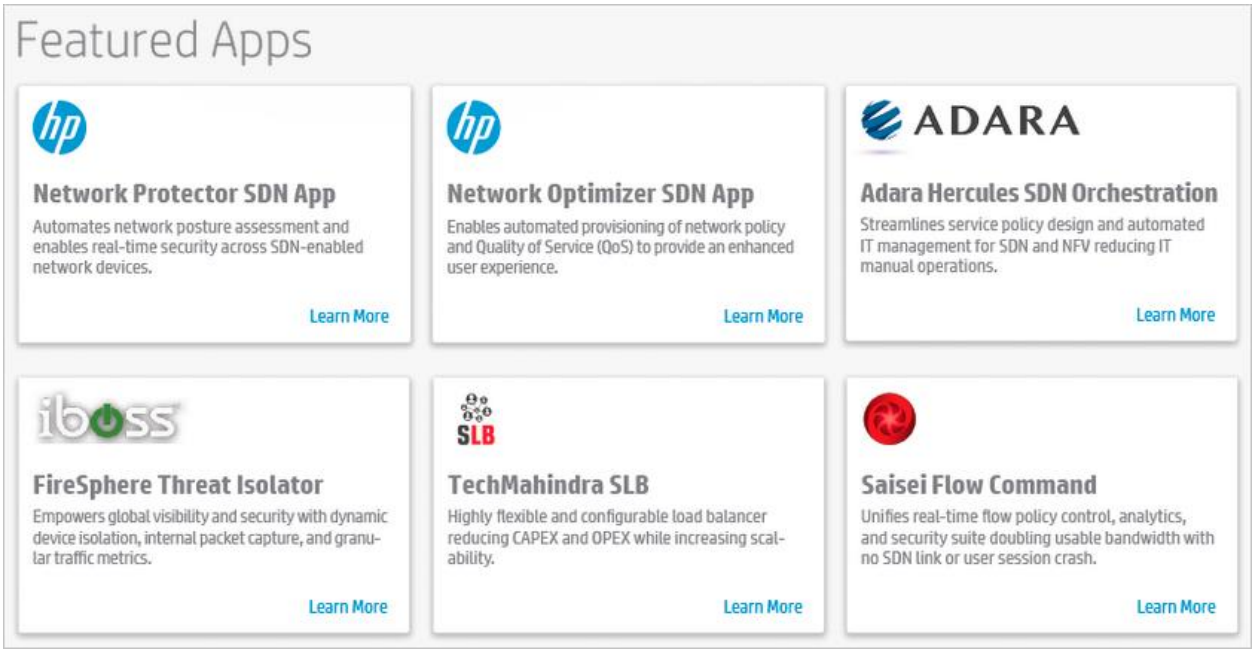


Рис. 1.5 Онлайн-супермаркет програм SDN. Розробники можуть представити там свої SDN-рішення, а замовники - підібрати для себе найбільш вигідну та зручну мережеву програму

Каталог застосунків HP SDN App Store постійно розширюється завдяки активній участі компаній-партнерів HP та інтернет-спільноти розробників. Відкрита модель платформи стимулює інновації та сприяє появі нових рішень, орієнтованих на конкретні галузеві або технологічні сценарії використання. У результаті SDN App Store перетворюється на динамічну екосистему, де мережеві функції реалізуються у вигляді програмних модулів, які можна швидко впроваджувати, оновлювати або замінювати.

Серед найбільш популярних рішень, представлених у SDN App Store, особливе місце посідають контролери віртуальних мереж, які забезпечують гнучке створення та керування ізольованими мережевими сегментами поверх фізичної інфраструктури. Також значним попитом користуються застосунки для оптимізації мережевого трафіка у середовищах уніфікованих комунікацій, зокрема при роботі сервісів на базі Microsoft Lync. Такі рішення дозволяють динамічно адаптувати мережу до вимог реального часу, забезпечуючи стабільну якість голосових і відеосервісів.

Окрему категорію складають набори для розробки програмного забезпечення (SDN SDK), які надають розробникам необхідні інструменти для створення власних SDN-застосунків. Використовуючи SDK, розробники можуть взаємодіяти з SDN-контролером через стандартні програмні інтерфейси, реалізовувати власну логіку керування мережею та інтегрувати мережеві функції з бізнес-додатками і системами оркестрації.

Крім надання програмних рішень, HP приділяє значну увагу навчанню та підготовці розробників SDN-застосунків. Компанія пропонує різні форми навчання, включаючи онлайн-курси, технічну документацію, навчальні матеріали, приклади коду та практичні лабораторні роботи. Такий підхід сприяє формуванню професійної спільноти розробників і пришвидшує впровадження SDN-технологій у корпоративних мережах.

У підсумку, HP SDN App Store відіграє важливу роль у розвитку програмно-визначених мереж, забезпечуючи зручний доступ до готових рішень, стимулюючи інновації та знижуючи бар’єр входу для впровадження SDN у бізнес-середовищі.

Це робить SDN не лише інфраструктурною технологією, а повноцінною програмною платформою для побудови гнучких, масштабованих і орієнтованих на потреби бізнесу мереж.

1.3 Інтеграція, партнерська система та Cisco ACI

Cisco ACI

У листопаді 2013 року керівництво компанії Cisco Systems представило власне бачення програмного керування складною мережевою інфраструктурою, яке було розроблене компанією Insieme, придбаною Cisco. Запропонована концепція була орієнтована насамперед на оптимізацію роботи прикладних сервісів і бізнес-додатків та мала подібні стратегічні цілі до програмно-визначених мереж (SDN). Дане рішення отримало назву Application Centric Infrastructure (ACI) і стало відповіддю Cisco на активне поширення SDN-технологій та відкритих стандартів у мережевій галузі.

Архітектура Cisco ACI складається з кількох ключових компонентів. До її складу входить контролер APIC (Application Policy Infrastructure Controller), комутатори серії Nexus 9000, а також розширена версія мережевої операційної системи NX-OS. Для роботи комутаторів Nexus 9000 у режимі ACI використовуються спеціалізовані ASIC-мікросхеми власної розробки Cisco, що забезпечують високу продуктивність і глибоку інтеграцію апаратного та програмного рівнів. Таким чином, ACI є комплексним апаратно-програмним рішенням, у якому всі компоненти тісно пов’язані між собою.

У професійному середовищі ACI часто розглядають як різновид SDN, але з чітко вираженою пропрієтарною спрямованістю. На відміну від класичної концепції SDN, яка робить акцент на використанні відкритих стандартів і відносно простих комутаторів, ACI базується на високофункціональних пристроях Cisco, зокрема комутаторах Nexus 9000. Розробка ACI демонструє прагнення Cisco скористатися своїми провідними позиціями на ринку мережевого обладнання та

запропонувати альтернативу стандартним SDN-підходам, зберігаючи контроль над екосистемою власних рішень.

Водночас повністю ігнорувати розвиток SDN та відкритих технологій сьогодні не може жоден великий вендор. Саме тому комутатори Cisco Nexus 9000 у так званому автономному режимі підтримують функціональність SDN і протокол OpenFlow, що дозволяє інтегрувати їх у гібридні мережеві архітектури та використовувати разом із зовнішніми SDN-контролерами. Це свідчить про прагматичний підхід Cisco, яка намагається поєднати власні пропрієтарні розробки з ринковими тенденціями.

Ключова відмінність підходу Cisco полягає у тому, що, подібно до SDN, ACI передбачає програмне управління мережею, проте керованими елементами залишаються не спрощені комутатори, а складні, багатофункціональні мережеві пристрої, які поєднують у собі логіку керування і передавання даних. Центральною ідеєю ACI є надання додаткам можливості “програмувати” мережу відповідно до власних вимог, а не підлаштовувати додатки під жорстко визначену мережеву конфігурацію.

Для реалізації цього підходу в ACI використовується концепція Application Network Profile (ANP) — профілю мережі додатка. У такому профілі описуються вимоги додатка до мережі, зокрема параметри якості обслуговування (QoS), політики безпеки, правила балансування навантаження, сегментації трафіка та взаємодії між компонентами додатка. Створені профілі ANP завантажуються у контролер APIC, який на їх основі автоматично програмує комутатори Cisco та застосовує відповідні політики в усій мережевій інфраструктурі.

Контролер APIC є центральним і найважливішим компонентом архітектури ACI. Він здійснює управління як фізичними, так і віртуальними мережевими пристроями, використовуючи політики, задані в ANP. APIC забезпечує централізоване застосування конфігурацій, контроль стану мережі, а також збір і передавання інформації про її роботу до систем вищого рівня. Завдяки цьому мережа стає більш передбачуваною, керованою та тісно інтегрованою з прикладними сервісами.

За задумом розробників Cisco, ACI має допомогти замовникам повністю розкрити потенціал бізнес-додатків, зменшити складність управління мережею та підвищити гнучкість IT-інфраструктури. Орієнтація на додатки дозволяє швидше впроваджувати нові сервіси, зменшувати час їх розгортання та забезпечувати стабільну роботу критично важливих систем.

Хоча ACI має багато спільних рис із SDN, у Cisco підкреслюють, що APIC формально не є SDN-контролером. На відміну від класичної SDN-моделі, APIC не реалізує жорсткого розділення між рівнем керування та рівнем передавання даних. Він працює незалежно від цих рівнів, виконуючи насамперед функції управління інфраструктурою, централізованого застосування політик та моніторингу стану мережі. Таким чином, Cisco ACI можна розглядати як альтернативну, прикладно-орієнтовану інтерпретацію ідей SDN, адаптовану до пропрієтарної екосистеми Cisco та потреб великих корпоративних і операторських мереж.

Можливості інтеграції та партнерська екосистема

На сучасному етапі розвитку мережевих технологій компанія Cisco Systems активно просуває архітектуру Application Centric Infrastructure (ACI) як альтернативу класичним підходам Software-Defined Networking (SDN). З цією метою кілька років тому Cisco представила так званий «орієнтований на стандарти» протокол OpFlex, який, за задумом розробників, має виконувати роль, подібну до протоколу OpenFlow у традиційних SDN-архітектурах. Компанія навіть декларувала намір просувати OpFlex через організацію IETF з метою надання йому статусу галузевого стандарту. Проте на практиці OpFlex залишається тісно пов’язаним з архітектурою ACI та екосистемою Cisco.

Станом на сьогодні для повноцінного розгортання ACI необхідне використання нового мережевого обладнання, зокрема комутаторів серії Cisco Nexus 9000, а також спеціалізованого програмного забезпечення — Application Policy Infrastructure Controller (APIC). Це означає, що перехід до ACI зазвичай супроводжується значними інвестиціями та оновленням інфраструктури. Водночас Cisco декларує можливість інтеграції ACI з різними системами оркестрації та

автоматизації, що дещо знижує бар'єр входу для великих корпоративних замовників.

Для забезпечення взаємодії ACI з платформами управління й оркестрації, такими як OpenStack, Puppet, CFEngine та іншими, Cisco використовує стандартні програмні інтерфейси на основі XML, JSON та RESTful API. Саме ці інтерфейси повинні забезпечувати інтеграцію ACI з зовнішніми IT-системами, а також із такими технологіями, як OpenDaylight, відкриті програмні віртуальні комутатори та мережеві механізми інкапсуляції, зокрема VXLAN. Таким чином, Cisco намагається позиціонувати ACI як рішення, здатне взаємодіяти з сучасними відкритими платформами, не ізолюючи його повністю від загальної SDN-екосистеми.

Для підтримки та розвитку власної архітектури Cisco активно формує партнерську екосистему ACI. До цієї ініціативи долучилися такі відомі компанії, як BMC, Computer Associates, Citrix, EMC, Emulex, F5, IBM, Microsoft, NetApp, VMware та низка інших гравців IT-ринку. Участь цих компаній сприяє створенню сумісних рішень, розширенню функціональності ACI та підвищенню привабливості платформи для корпоративних замовників, які вже використовують продукти зазначених вендорів.

Попри це, ACI залишається пропрієтарним рішенням, що фактично обмежує клієнтів рамками закритої екосистеми одного постачальника. Для окремих організацій, які цінують стабільність, підтримку «з одного вікна» та глибоку інтеграцію компонентів, такий підхід може бути прийнятним або навіть бажаним. Водночас він суперечить загальним тенденціям розвитку ринку, які орієнтовані на відкриті стандарти, міжвендорну сумісність і зменшення залежності від конкретного виробника обладнання.

Паралельно з розвитком ACI компанія Cisco прагне зберегти та зміцнити свої ринкові позиції, пропонуючи додаткові програмні надбудови для вже наявного обладнання та позиціонуючи їх як елементи SDN. Зокрема, підтримка SDN-функціональності, додана у 2013 році до таких рішень, як Cisco Open Network Environment (ONE) та Cisco OnePK (Platform Kit), дозволяє розглядати їх як

інструменти, покликані захистити позиції Cisco на ключових сегментах мережевого ринку.

Водночас ці інструменти з самого початку орієнтовані передусім на пристрої Cisco, забезпечуючи найкращі результати саме у зв’язці з власним обладнанням компанії. Такий підхід не передбачає повної відкритості та незалежності від вендора, які є базовими принципами класичної концепції SDN. У результаті рішення Cisco забезпечують еволюційний шлях розвитку для існуючих клієнтів компанії, але не реалізують у повному обсязі ідею відкритих програмно-визначених мереж.

Шлях до SDN

Згідно з оцінками сучасних аналітиків, найбільш перспективним напрямом розвитку мережевих технологій є відкриті SDN-рішення, побудовані на базі загальноприйнятих стандартів. Станом на 2025–2026 роки концепція SDN вже не є експериментальною — вона пропонує організаціям широкий вибір практичних інструментів і технологій. До них належать комутатори з підтримкою OpenFlow, NETCONF, OVSDB, розвинуті та стандартизовані API, а також корпоративне програмне забезпечення, яке ефективно використовує можливості програмно-керованих мереж. Усе це формує гнучку технологічну основу для побудови сучасної мережевої інфраструктури.

Як і будь-яка інша критично важлива IT-інфраструктура, SDN повинна базуватися на відкритих стандартах. Саме відкрита екосистема забезпечує конкуренцію між вендорами, знижує залежність від одного постачальника та суттєво прискорює впровадження інновацій у сфері мережевих технологій. У 2025–2026 роках цей підхід стає особливо актуальним у контексті хмарних обчислень, віртуалізації, edge-інфраструктур і зростаючої ролі автоматизації та оркестрації мереж.

Попри це, через інерцію мислення, обмежені бюджети та вплив економічних і безпекових викликів у багатьох організаціях досі домінує традиційний підхід до побудови мереж. Водночас SDN уже сьогодні демонструє здатність ефективно вирішувати завдання на стику фізичних і віртуальних середовищ, забезпечуючи централізоване управління, гнучку сегментацію трафіка та швидку адаптацію до

змін навантаження. Досвід великих інтернет-компаній і хмарних провайдерів переконливо показав, що масштабна мережева інфраструктура може динамічно змінюватися відповідно до вимог бізнесу та додатків.

Однак значна частина підприємств все ще не поспішає з реалізацією SDN-стратегії, помилково вважаючи, що перехід до SDN означає повну заміну наявного мережевого обладнання. Насправді такі побоювання ґрунтуються на поширеному хибному уявленні про SDN як про окремий продукт. У реальності SDN — це насамперед підхід до проєктування мереж, а також нова парадигма їх адміністрування, моніторингу та адаптації до бізнес-завдань, які формуються прикладними сервісами.

Перехід до SDN є поетапним і еволюційним процесом, що враховує конкретні бізнес-сценарії використання мережі. Навіть за наявності спеціалізованих продуктів, таких як SDN-комутатори з підтримкою OpenFlow, повна заміна мережевої інфраструктури не є обов’язковою. У більшості випадків SDN може впроваджуватися поступово — через пілотні зони, гібридні архітектури та інтеграцію з уже наявними мережевими рішеннями.

За оновленими прогнозами аналітичних компаній, зокрема IDC та Gartner, у 2025–2026 роках SDN переходить у фазу зрілості. Ринок програмно-визначених мереж продовжує стабільно зростати, а значну частку цього зростання формують SDN-застосунки, системи автоматизації та оркестрації. Паралельно розширюється набір інструментів, платформ і практичних сценаріїв використання SDN, що робить технологію доступною не лише для гіпермасштабних дата-центрів, а й для середніх та великих підприємств.

В Україні інтерес до програмно-визначених мереж у 2025–2026 роках також помітно зростає. Українські компанії, оператори зв’язку, державні організації та IT-інтегратори все активніше обговорюють пілотні SDN-проєкти, проводять дослідження та впроваджують елементи програмного керування мережами, особливо в хмарних і гібридних середовищах. Розвиток цифрової інфраструктури, потреба в гнучкості, безпеці та ефективному використанні ресурсів роблять SDN актуальним інструментом для післявоєнної відбудови та модернізації IT-систем.

Очікується, що SDN-рішення, засновані на відкритих стандартах, дозволять українським організаціям привести мережеву інфраструктуру у відповідність до реальних потреб бізнесу та доступних бюджетів. Важливою перевагою такого підходу є відсутність жорсткої прив’язки до конкретного вендора, що дає змогу комбінувати рішення різних виробників і поступово впроваджувати нові технології без кардинальних змін усієї інфраструктури. У підсумку SDN стає не просто технологічним трендом, а стратегічним інструментом підвищення гнучкості, стійкості та конкурентоспроможності сучасних мереж.

2 NETSCALER SD-WAN В SDN МЕРЕЖАХ

2.1 Роль SD-WAN

Розглянемо одне з рішень, призначених для побудови програмно-конфігурованих мереж (SDN) між підприємством і хмарним дата-центром, а також для організації ефективного мережевого з’єднання між центральним офісом і віддаленими філіями компанії. Подібні рішення набувають особливої актуальності в сучасних умовах цифрової трансформації бізнесу, коли організації дедалі активніше використовують хмарні сервіси, розподілені IT-ресурси та віддалені робочі місця.

Практика показує, що традиційні підходи до розширення WAN-інфраструктури часто не відповідають вимогам сучасного бізнесу. Збільшення пропускної здатності вже наявного WAN-каналу у багатьох випадках може тривати тижнями або навіть місяцями, оскільки залежить від оператора зв’язку, наявності технічної інфраструктури та складних погоджувальних процедур. Крім того, організація додаткового WAN-каналу нерідко пов’язана з суттєвими капітальними та операційними витратами, адже вартість операторських каналів залишається доволі високою, особливо для міжнародних або резервних з’єднань.

У таких умовах рішення на базі SDN стають реальною альтернативою традиційним WAN-технологіям. Вони дозволяють використовувати вже наявні канали зв’язку — зокрема інтернет-з’єднання різних провайдерів — та об’єднувати їх у єдину логічну мережу з централізованим програмним управлінням. Завдяки цьому підприємство отримує можливість динамічно розподіляти трафік, пріоритезувати критично важливі додатки, забезпечувати високу доступність сервісів і швидко адаптувати мережу до змін навантаження без фізичного розширення інфраструктури.

Особливо важливими такі рішення є для сценаріїв взаємодії корпоративної мережі з хмарним дата-центром, де затримки, нестабільність каналів або обмежена пропускна здатність можуть безпосередньо впливати на продуктивність бізнес-

додатків. Програмно-конфігурована мережа дозволяє автоматично оптимізувати маршрути передавання даних, враховуючи поточний стан каналів, вимоги сервісів та задані політики безпеки.

Крім того, SDN-підхід суттєво спрощує побудову мереж між центральним офісом і віддаленими підрозділами, що особливо актуально для компаній із географічно розподіленою структурою. Філії можуть швидко підключатися до корпоративної мережі з мінімальними витратами, а всі налаштування виконуються централізовано через програмний контролер. Це зменшує залежність від локальних IT-фахівців, скорочує час розгортання та знижує ризик помилок конфігурації.

Територіально розподілені корпоративні мережі WAN (Wide Area Network) є необхідною складовою інфраструктури компаній, які мають декілька дата-центрів, велику кількість філій, офісів і точок продажу як у межах одного міста, так і по всій країні або навіть у глобальному масштабі. Такі мережі забезпечують обмін даними між підрозділами, доступ до корпоративних ресурсів, централізованих сервісів і хмарних платформ. Водночас побудова та експлуатація WAN-інфраструктури пов’язана з низкою серйозних технічних і фінансових викликів.

Традиційно для організації корпоративних WAN використовуються фізичні виділені лінії зв’язку, які можуть належати самій компанії або орендуватися у операторів зв’язку. Проте такі канали вимагають постійно зростаючих витрат, а в окремих регіонах або між віддаленими локаціями їх прокладання може бути технічно складним або взагалі неможливим. Тому на практиці дедалі частіше застосовуються альтернативні рішення, зокрема віртуальні приватні мережі VPN (Virtual Private Network) поверх Інтернету, а також операторські канали з використанням технології MPLS (Multi-Protocol Label Switching).

Разом із тим мережі, побудовані на базі VPN та MPLS, мають суттєвий недолік — вони є статичними за своєю природою. Топологія таких мереж зазвичай жорстко зафіксована, її неможливо оперативно змінювати «на льоту» відповідно до поточних потреб бізнесу. Створення нових VPN-з’єднань або зміна маршрутів трафіка потребує значних зусиль з налаштування кожного мережевого елемента, що ускладнює масштабування та уповільнює впровадження нових сервісів.

Саме на цьому етапі на допомогу приходить технологія SDN (Software Defined Networking), яку нерідко називають концептуальним проривом у сфері мережевих технологій. Така характеристика пов’язана не зі складністю SDN, а з принципово іншим підходом до організації мережі. У класичних мережах кожен маршрутизатор, комутатор або міжмережевий екран самостійно приймає рішення щодо передавання пакетів, поєднуючи в собі площину керування (Control Plane) і площину передавання даних (Data Plane).

У SDN ці функції чітко розділяються. «Мозок» мережі, тобто Control Plane, виноситься на верхній рівень і реалізується у вигляді централізованого SDN-контролера. Саме він визначає, яким шляхом має пройти наступний пакет, формує правила маршрутизації та застосовує політики управління. Натомість мережеві пристрої виконують лише функцію швидкого передавання пакетів відповідно до отриманих інструкцій. Така архітектура дозволяє швидко змінювати топологію мережі, створювати нові VPN та адаптувати маршрути трафіка віддалено і централізовано, без необхідності вручну налаштовувати кожен окремий пристрій.

Початково концепція SDN розглядалася переважно в контексті одного дата-центру, де вона ефективно вирішувала завдання управління трафіком у віртуалізованих і хмарних середовищах. Однак для з’єднання між дата-центрами (DCI — Data Center Interconnect) або для підключення віддалених філій підприємства до центрального офісу виникла потреба у спеціалізованому підході. Таким підходом стала концепція Software Defined WAN (SD-WAN).

SD-WAN дозволяє значно ефективніше використовувати наявні WAN-канали за рахунок гнучкого й динамічного розподілу трафіка між різними типами з’єднань — виділеними каналами, MPLS, широкосмуговим Інтернетом або бездротовими мережами. Завдяки централізованому управлінню SD-WAN може автоматично обирати оптимальні маршрути, враховуючи затримки, пропускну здатність, втрати пакетів і пріоритети додатків.

Загалом SD-WAN — це не стільки окрема технологія, скільки новий підхід до проєктування, розгортання та експлуатації глобальних корпоративних мереж. У його основі лежить використання принципів SDN як найбільш ефективного

механізму керування трафіком і маршрутизації. Такий підхід забезпечує підприємствам підвищену гнучкість, кращу масштабованість, зниження витрат на мережеву інфраструктуру та можливість швидко адаптувати WAN до змін бізнес-вимог і цифрових сервісів.

Традиційно, WAN створювалися приблизно так:

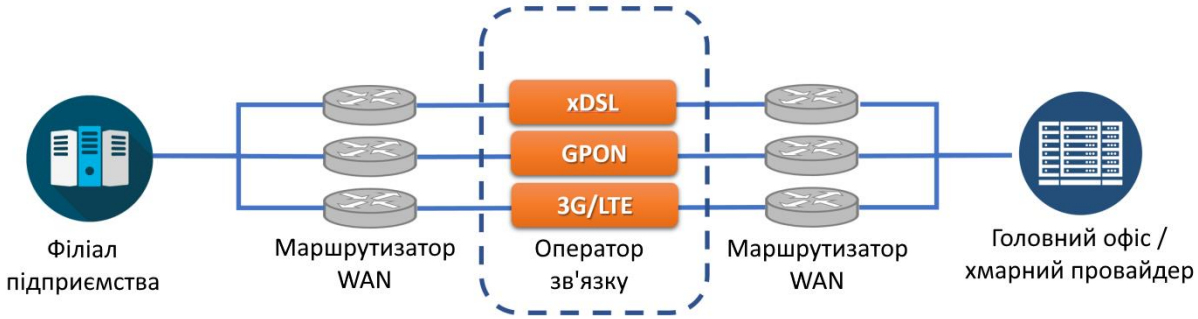


Рис. 2.1 Традиційна архітектура WAN

Подібна мережева інфраструктура зазвичай працює стабільно та без суттєвих збоїв, допоки не виникає якась позаштатна або аварійна ситуація. Це може бути як фізичне пошкодження кабелю оператора зв’язку під час будівельних чи ремонтних робіт, так і перевантаження мобільної мережі 3G/4G/LTE, особливо у години пікового навантаження або в умовах надзвичайних подій. Не можна виключати й інші непередбачувані фактори — від аварій у мережі провайдера до збоїв обладнання або проблем з електроживленням. У таких випадках нормальне функціонування корпоративної мережі може бути порушене на тривалий час.

Наслідки подібних інцидентів для підприємства часто є критичними. Відновлення працездатності мережі може займати години або навіть дні, протягом яких бізнес-процеси сповільнюються або повністю зупиняються. Користувачі втрачають доступ до корпоративних сервісів, хмарних додатків і централізованих систем, що призводить до фінансових втрат, зниження продуктивності та погіршення якості обслуговування клієнтів. Особливо чутливими до таких збоїв є компанії з розподіленою структурою та залежністю від онлайн-сервісів.

Саме для захисту від подібних непередбачуваних ситуацій і створювалися рішення класу SD-WAN. Вони дозволяють побудувати відмовостійку мережеву

інфраструктуру, здатну автоматично реагувати на аварії та деградацію каналів зв'язку. SD-WAN забезпечує динамічне перемикання трафіка між кількома доступними каналами, підтримує резервування та оптимізацію маршрутів, а також мінімізує час простою сервісів. Завдяки цьому підприємство може зберігати безперервність роботи навіть у разі виникнення серйозних проблем із окремими мережевими з'єднаннями.

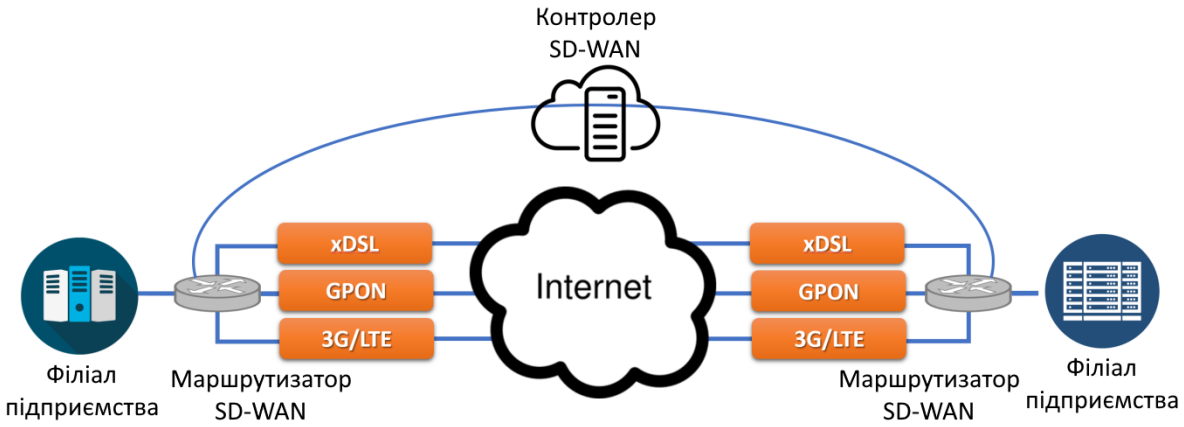


Рис. 2.2 Архітектура SD-WAN

У середовищі SD-WAN з'являється можливість централізованого керування мережевим трафіком за допомогою програмного забезпечення SDN-контролера. Це означає, що всі рішення щодо маршрутизації, пріоритезації та використання каналів зв'язку приймаються в єдиній точці керування, а не на кожному окремому маршрутизаторі чи комутаторі. У результаті VPN-мережі можна створювати дуже швидко, а їх конфігурування та масштабування відбувається гнучко, без складних і тривалих ручних налаштувань.

Раніше розрізнені мережеві з'єднання — наприклад, MPLS, широкосмуговий Інтернет або мобільні канали — у SD-WAN об'єднуються в єдину логічну «віртуальну мережу», якою керує централізований контролер. Для мережевого адміністратора головного офісу це означає суттєве спрощення експлуатації: більше немає потреби виїжджати до віддалених філій або залучати місцевих адміністраторів для первинного налаштування обладнання. Усі зміни виконуються віддалено з точки розміщення SD-WAN-контролера, що мінімізує або повністю усуває ручну конфігурацію пристроїв у філіях.

Крім зручності адміністрування, SD-WAN забезпечує раціональніше використання дорогих MPLS-каналів, орендованих у операторів зв’язку. Замість того щоб передавати через них увесь трафік, SD-WAN дозволяє спрямовувати низькопріоритетні потоки через значно дешевші канали публічного Інтернету. У результаті дорогі операторські канали використовуються лише там, де це дійсно необхідно, що суттєво знижує загальні витрати на мережеву інфраструктуру.

Саме тому можна виділити три основні переваги, які найчастіше стимулюють організації переходити на SD-WAN:

1. **Зручність побудови розподіленої філіальної мережі.**
   Рішення SD-WAN для з’єднання між дата-центрами та провайдерами хмарних послуг легко й швидко розгортаються та централізовано адмініструються. Відпадає необхідність відряджати IT-фахівців у філії для конфігурації кожного мережевого пристрою, що скорочує час запуску нових локацій і зменшує операційні витрати.
2. **Можливість використання гібридної мережі.**
   Багато філій уже підключені за допомогою MPLS-каналів, і SD-WAN не вимагає відмови від них. Такі канали можна залишити в роботі, доповнивши їх **недорогими інтернет-з’єднаннями**, і налаштувати політики трафіка так, щоб MPLS використовувався максимально економно — лише для пріоритетних сервісів, наприклад корпоративної **VoIP-телефонії (Voice over IP)** або інших критично важливих бізнес-додатків. За достатньої пропускної здатності та якості Інтернет-каналів можливе навіть передавання всього трафіка через широкосмугові мережі, включно з **3G/4G/LTE**.
3. **Автоматичне управління трафіком.**
   SD-WAN дозволяє заздалегідь визначити пріоритети для різних типів трафіка та каналів зв’язку, після чого система автоматично й у режимі реального часу перенаправляє потоки даних залежно від змін параметрів мережевих з’єднань. У разі погіршення якості каналу, зростання затримок або втрат пакетів трафік швидко перемикається на альтернативні маршрути без участі адміністратора.

У підсумку SD-WAN перетворює корпоративну WAN-інфраструктуру на гнучку, централізовано керовану та економічно ефективну систему, здатну оперативно адаптуватися до змін як у мережевих умовах, так і в бізнес-потребах організації.

2.2 Побудова SD-WAN на NetScaler

Компанії, які активно впроваджують централізацію IT-інфраструктури, зазвичай широко використовують низку сервісів, критично важливих для щоденної роботи бізнесу. До таких сервісів насамперед належать віртуалізація робочих місць VDI (Virtual Desktop Infrastructure) та/або термінальні сервіси, у середовищі яких функціонують ключові бізнес-додатки. Також важливу роль відіграють голосовий зв'язок по IP-мережі (VoIP, Voice over IP) та системи відеоконференцзв'язку, які забезпечують оперативну комунікацію між співробітниками, підрозділами та партнерами.

Будь-які збої в роботі цих сервісів або зниження їхньої якості — наприклад, затримки, втрати пакетів чи нестабільність з'єднання — безпосередньо впливають на швидкість і ефективність бізнес-процесів. Повільна робота VDI може ускладнити доступ співробітників до робочих середовищ, проблеми з VoIP призводять до погіршення якості голосового зв'язку, а перебої у відеоконференціях роблять неможливими повноцінні онлайн-наради. У результаті зростають простої, знижується продуктивність праці та підвищуються операційні ризики для підприємства.

У цьому контексті рішення SD-WAN NetScaler надає додаткові можливості для підвищення якості та продуктивності сервісів, які є чутливими до затримок або вимагають значної пропускної здатності. Зокрема, SD-WAN дозволяє оптимізувати роботу таких сервісів, як VoIP, де критичними є мінімальні затримки та стабільність каналу, а також відеоконференції та VDI, які потребують широкої смуги пропускання та прогнозованої якості з'єднання. Завдяки інтелектуальному управлінню трафіком SD-WAN може динамічно обирати оптимальні маршрути

передавання даних і забезпечувати пріоритетне обслуговування критично важливих потоків.

Розглянемо типову схему підключення корпоративної мережі віддаленого офісу до дата-центру підприємства. У класичному варіанті основний обсяг трафіка, включно з критичними бізнес-додатками, передається через високошвидкісний виділений MPLS-канал, який забезпечує гарантовану якість обслуговування та передбачувані характеристики з'єднання. Для підвищення надійності мережі додатково налаштовуються один або декілька резервних маршрутів через широкосмуговий доступ до Інтернету. Ці канали використовуються як резерв у разі відмови основного MPLS-з'єднання або для розвантаження мережі під час пікових навантажень.

Інтеграція такої схеми з SD-WAN дозволяє зробити її значно гнучкішою та ефективнішою. Система може автоматично визначати стан кожного каналу, перерозподіляти трафік між MPLS та Інтернет-з'єднаннями, забезпечувати безперервність роботи критичних сервісів і підтримувати стабільну якість користувацького досвіду навіть у разі деградації або відмови окремих мережевих шляхів. У підсумку підприємство отримує надійну, масштабовану та оптимізовану мережеву інфраструктуру, адаптовану до вимог сучасних централізованих IT-сервісів.

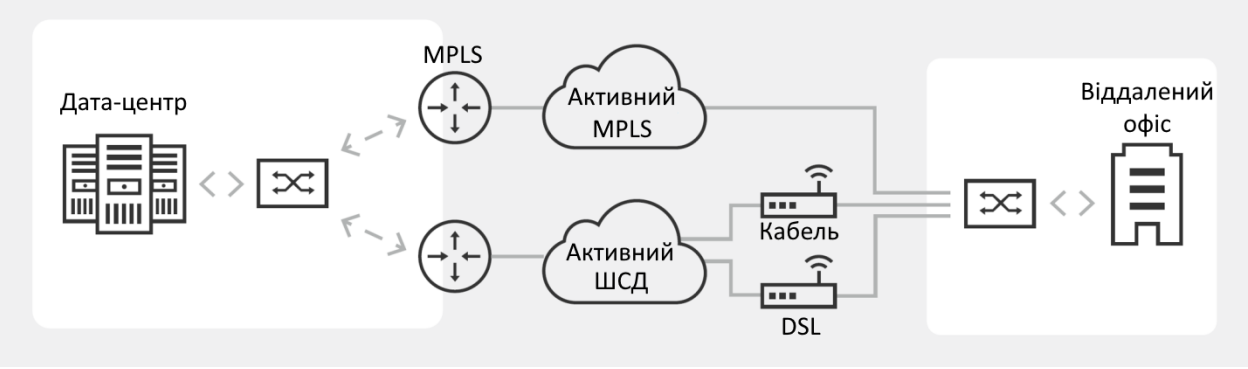


Рис. 2.3 Резервування каналів у традиційній WAN

На перший погляд описана схема виглядає логічною та працездатною, однак на практиці вона має низку суттєвих недоліків, які з часом починають серйозно впливати на стабільність мережі, продуктивність додатків і ефективність бізнес-процесів загалом.

По-перше, у мережах на базі MPLS майже завжди присутня значна частка невикористаної пропускної здатності. Це пояснюється тим, що з'єднання та маршрути трафіка задаються статично, а сам MPLS-канал є дорогим ресурсом, який резервується «із запасом». Водночас у моменти пікового навантаження виникає протилежна проблема: перенаправити частину трафіка з MPLS на широкосмуговий доступ (ШСД) оперативно неможливо. Для цього, як правило, потрібне ручне втручання мережевого адміністратора, що займає час і не гарантує миттєвого результату. Крім того, розширення вже існуючого виділеного каналу часто є технічно складним або взагалі недоступним через обмеження оператора зв'язку.

По-друге, у разі відмови основного каналу відновлення з'єднання може тривати від кількох секунд до кількох хвилин. За цей час прикладні сервіси перестають відповідати на запити користувачів, а поточні активні сесії можуть бути розірвані. У середовищах, де використовуються звичайні клієнт-серверні додатки (поза VDI або термінальними сервісами), це призводить до необхідності скасовувати або повторно виконувати непідтверджені транзакції. Очевидно, що в такій ситуації нормальний перебіг бізнес-процесів порушується, а підприємство зазнає фінансових і репутаційних втрат.

По-третє, після аварійного перемикання на резервні канали продуктивність критично важливих бізнес-додатків може істотно знизитися. Причина полягає в тому, що всі інші сервіси та прикладні системи також починають використовувати ці ж резервні канали. У результаті зростає рівень втрат пакетів у VoIP-трафіку, що безпосередньо погіршує якість голосового зв'язку, у системах відеоконференцій з'являються затримки та перешкоди, а VDI-середовища починають помітно «гальмувати», погіршуючи користувацький досвід.

По-четверте, підключення нових філій у межах такої архітектури часто виявляється фінансово та організаційно обтяжливим. Для цього необхідно закуповувати додаткове обладнання — маршрутизатори, міжмережеві екрани, інші мережеві пристрої. Це призводить до зростання сукупної вартості володіння мережею філії, збільшує навантаження на сервісний персонал і нерідко потребує

розширення штату IT-інженерів. Додатково зростають витрати на відрядження фахівців для інсталяції та налаштування обладнання на місцях.

По-п’яте, адміністрування такої мережі є складним і дуже трудомістким процесом. Для кожного додатка необхідно вручну налаштовувати власний маршрут трафіка. Якщо шлях до віддаленого офісу проходить через кілька мережевих «хопів» між маршрутизаторами, ще й через мережі різних типів, то підтримка якості обслуговування (QoS) стає надзвичайно складним завданням. Так само ускладнюється моніторинг і діагностика проблем, оскільки адміністратору доводиться аналізувати поведінку трафіка на великій кількості різнорідних ділянок мережі.

Усі перелічені проблеми мають тенденцію накопичуватися і посилюватися зі зростанням кількості філій, каналів зв’язку та дата-центрів. Ситуація ще більше ускладнюється з появою хмарних додатків і сервісів, які вимагають гнучкої маршрутизації, стабільної якості з’єднання та швидкої адаптації мережі до змін навантаження. У підсумку традиційна WAN-архітектура перестає відповідати сучасним вимогам бізнесу і стає стримувальним фактором розвитку підприємства.

2.3 Вдосконалення маршрутизації

Контролери NetScaler SD-WAN постійно здійснюють моніторинг ключових параметрів якості мережі, зокрема часу передавання пакетів (latency), джитеру та відсотка втрат пакетів. Зібрані показники аналізуються в режимі реального часу й використовуються як основа для автоматичного вибору найбільш оптимальних маршрутів для різних типів трафіка та окремих потоків даних. Такий підхід дозволяє системі не просто реагувати на аварії, а й проактивно адаптувати маршрутизацію до поточного стану WAN-каналів.

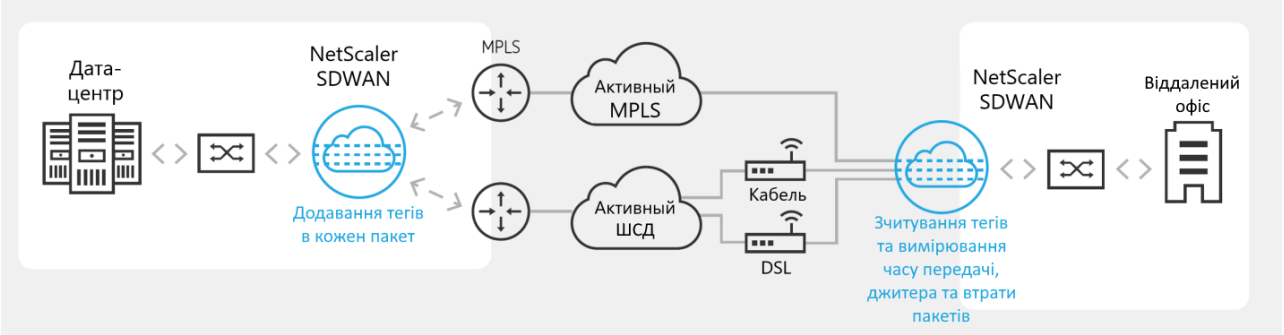


Рис. 2.4 Додавання тегів у трафік WAN для створення карти маршрутів у NetScaler SD-WAN

Рішення Citrix NetScaler SD-WAN здатне обирати оптимальні маршрути між майданчиками підприємства з використанням різних типів з'єднань — MPLS, широкосмугового Інтернету, бездротових каналів тощо. Мета такого вибору полягає у забезпеченні максимально можливої якості передавання даних через WAN для кожного конкретного типу трафіка. Система враховує специфіку сервісів, чутливих до затримок (наприклад, VoIP), а також додатків, що потребують великої пропускної здатності (VDI, відеоконференції).

Важливою особливістю рішення є здатність автоматично ідентифікувати понад 4000 різних прикладних сервісів за їхнім унікальним «відбитком» (application fingerprint). Це дозволяє SD-WAN-контролеру точно визначати, який саме додаток ініціює сесію, та застосовувати до нього відповідні політики пріоритезації, маршрутизації й використання каналів. Таким чином, мережа стає не просто транспортним середовищем, а додатко-орієнтованою інфраструктурою.

Пристрої NetScaler, розташовані в центральному дата-центрі та на віддалених майданчиках, спільно формують динамічну «карту» доступних WAN-маршрутів між локаціями. Така карта містить детальну інформацію про продуктивність кожного маршруту, показники якості з'єднання, а також умовну «вартість» каналу. Під вартістю може розумітися як фінансова складова (наприклад, дорогий MPLS або дешевший Інтернет), так і технологічні обмеження чи політики використання каналу.

Коли певний додаток ініціює мережеву сесію, NetScaler SD-WAN-контролер на стороні відправлення обирає маршрут на основі сукупності кількох метрик. При

цьому враховується критичність і важливість додатка для бізнесу, поточний стан каналів, а також їхня вартість. У разі, якщо одного маршруту недостатньо для забезпечення потрібної пропускної здатності або надійності, система може одночасно використовувати кілька маршрутів, розподіляючи трафік між ними.

Разом із тим якість будь-якого WAN-маршруту не є сталою величиною і може змінюватися з часом. Саме тому контролер NetScaler SD-WAN на вихідній стороні додає до кожного пакета спеціальні мітки (tag). Ці мітки дозволяють ідентифікувати шлях проходження пакета мережею та здійснювати точні вимірювання параметрів з’єднання.

Контролер на стороні приймання зчитує ці мітки та фіксує реальний час доставки пакетів, аналізує їхню послідовність і на основі цього обчислює втрати пакетів, рівень джитеру та інші показники якості маршруту. Отримана інформація не залишається локальною — вона поширюється серед інших SD-WAN-пристроїв у межах мережі підприємства.

У результаті всі контролери NetScaler SD-WAN постійно оновлюють свої карти маршрутів, використовуючи найсвіжіші дані про стан WAN-каналів. Це дозволяє системі динамічно та без участі адміністратора змінювати маршрути передавання трафіка, обираючи найкращі доступні шляхи в кожний конкретний момент часу. Такий механізм забезпечує високу стабільність роботи критичних бізнес-додатків, оптимальне використання мережевих ресурсів і стійкість корпоративної WAN-інфраструктури до деградації або відмов окремих каналів.

Відновлення після аварій

Рішення NetScaler SD-WAN забезпечує надзвичайно швидке та безперервне відновлення з’єднання у разі аварійних ситуацій в мережі. Наприклад, якщо MPLS-канал перевантажений, починає працювати нестабільно або взагалі перестає відповідати на запити, приймальний SD-WAN-пристрій майже миттєво визначає проблему за ознаками втрати пакетів, зростання затримок або джитеру. У такій ситуації система протягом кількох мілісекунд автоматично переносить поточні активні сесії на найкращі з доступних альтернативних WAN-маршрутів.

Ключовою перевагою цього механізму є те, що користувачі не помічають жодних розривів або переривань у роботі сервісів. Поточні голосові виклики, відеоконференції або сесії VDI продовжують працювати без обриву, повторного підключення чи втрати даних. Таким чином, NetScaler SD-WAN забезпечує високу відмовостійкість і підтримує безперервність бізнес-процесів навіть у разі серйозних проблем із окремими каналами зв'язку.

Альтернатива традиційному використанню WAN і DCI

NetScaler SD-WAN виступає економічно вигідною альтернативою традиційним підходам до побудови WAN та DCI (Data Center Interconnect). Хоча канали широкосмугового доступу до Інтернету або мобільні мережі також можуть зазнавати деградації якості, ймовірність одночасного погіршення всіх доступних каналів є вкрай низькою. Саме цю особливість ефективно використовує SD-WAN.

Система здатна динамічно та "попакетно" переміщувати трафік між доступними каналами, обираючи у кожний момент часу той шлях, який має найкращі характеристики. Завдяки цьому сумарна якість передавання даних часто виявляється не гіршою, а іноді й кращою, ніж при статичному використанні одного дорогого операторського MPLS-каналу.

Цей підхід набуває особливої актуальності, якщо врахувати, що розширення пропускної здатності традиційної WAN-інфраструктури зазвичай займає тижні або навіть місяці, потребує узгоджень з оператором та супроводжується значними витратами. У випадку SD-WAN підприємство може значно швидше підвищити ефективність мережі, використовуючи вже наявні канали без істотних капітальних інвестицій.

Пріоритезація трафіку та управління QoS

Ще однією важливою перевагою NetScaler SD-WAN є гнучке призначення пріоритетів трафіку та гранулярне управління якістю обслуговування (QoS) залежно від конкретного додатка або типу сервісу. У базовій конфігурації всі додатки в NetScaler можуть бути розподілені на три основні категорії:

- **real-time (у реальному часі)** — додатки, чутливі до затримок і джитеру (VoIP, відеоконференції);

- **interactive (інтерактивні)** — сервіси, що потребують швидкої реакції, але менш критичні до мілісекундних затримок (VDI, веб-додатки);
- **bulk (пакетні або фонові)** — трафік, для якого не критична ані затримка, ані миттєва доставка (резервне копіювання, оновлення, передавання великих файлів).

У разі необхідності система дозволяє налаштувати більш точні відносні пріоритети, використовуючи додаткові критерії, такі як IP-адреса, DSCP-мітки, порт джерела або призначення, а також інші параметри мережевого трафіку. Це дає змогу будувати складні політики QoS, адаптовані до реальних бізнес-потреб.

Наприклад, голосовому трафіку у бізнес-сесіях може бути призначений найвищий пріоритет порівняно з іншими додатками. Або ж для нього можна задати той самий рівень якості, що й для інших сервісів реального часу — таких як відеоконференції чи VDI. Аналогічно можуть бути пріоритезовані критично важливі бізнес-додатки, від стабільності яких залежить робота підприємства.

Дублювання пакетів

Для сценаріїв, у яких необхідно забезпечити максимально можливу доступність і стабільність сервісів, у NetScaler SD-WAN використовується спеціальна функція дублювання пакетів (Packet Duplication) для бізнес-критичних додатків. Суть цього механізму полягає в тому, що кожен пакет даних надсилається одночасно двома незалежними маршрутами WAN, які не залежать один від одного за фізичною або логічною інфраструктурою.

Якість сервісу значною мірою визначається відсотком втрат пакетів, а при використанні дублювання цей показник практично зводиться до нуля. Контролер NetScaler SD-WAN на стороні приймання аналізує потоки даних і використовує перший отриманий пакет, автоматично ігноруючи його дубль. Таким чином, система завжди обирає найшвидший і найякісніший шлях, навіть якщо інший маршрут має більші затримки або тимчасові втрати.

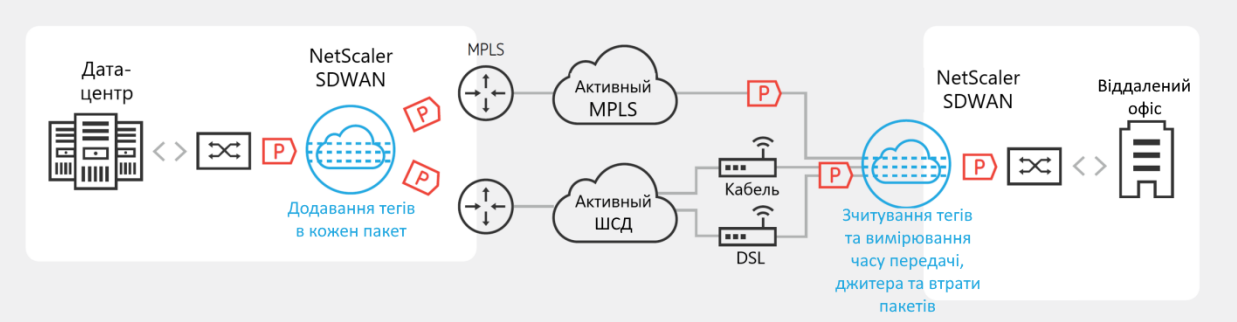


Рис. 2.5 Дублювання пакетів у NetScaler SDWAN

Безумовно, дублювання пакетів потребує додаткової пропускної здатності, оскільки обсяг передаваних даних збільшується. Однак у випадку критично важливих сервісів, таких як голосовий зв'язок VoIP, відеоконференції або віртуалізовані робочі середовища, це виправдано. У результаті досягається виняткова якість передавання мовлення та відео, а також висока надійність мережевої складової бізнес-додатків. Імовірність того, що обидві копії пакета будуть втрачені одночасно, є вкрай низькою.

Окрім дублювання пакетів, NetScaler SD-WAN містить цілу низку додаткових функцій, спрямованих на підвищення якості та продуктивності додатків, чутливих до затримок, зокрема VoIP, відеоконференцій і систем віртуалізації.

Динамічний вибір маршрутів

Інтелектуальний механізм маршрутизації дозволяє призначати прямі маршрути між офісами компанії, минаючи головний дата-центр, якщо це доцільно. Такий підхід суттєво зменшує затримки передавання даних між майданчиками та знижує навантаження на центральну інфраструктуру і WAN-канали дата-центру.

Traffic Shaping і динамічне резервування смуги пропускання Функції Traffic Shaping та динамічного резервування пропускної здатності надають розширені можливості керування якістю обслуговування для різних класів додатків. Система може гарантувати мінімальну смугу для критичних сервісів і водночас обмежувати фоновий або низькопріоритетний трафік.

Packet Reordering

Функція перевпорядкування пакетів (Packet Reordering) усуває проблеми, пов'язані з доставкою пакетів у неправильній послідовності. Це запобігає

помилковому сприйняттю втрат пакетів на рівні додатків і звільняє їх від необхідності повторних запитів на передавання даних, що позитивно впливає на продуктивність.

Stateful Firewall

Вбудований Stateful Firewall відстежує стан і характеристики кожного мережевого з'єднання. Він здатен відрізняти дозволені пакети від несанкціонованих або невідомих і пропускає через граничний маршрутизатор лише ті пакети, які відповідають встановленим політикам безпеки. Це підвищує загальний рівень захисту WAN-інфраструктури.

DPI (глибокий аналіз пакетів)

Механізм Deep Packet Inspection (DPI) дозволяє здійснювати глибокий аналіз трафіку та блокувати типи протоколів або робочих навантажень, які не дозволені політиками контролера. Це дає змогу точно контролювати, які додатки і сервіси можуть використовувати WAN-канали.

Зручне управління політиками WAN

Налаштування політик WAN не становить складності завдяки системі управління NetScaler SD-WAN Center, яка має інтуїтивно зрозумілий інтерфейс та гнучкі інформаційні панелі. Адміністратор може в режимі реального часу моніторити параметри WAN-маршрутів через різні зовнішні мережі та швидко виявляти потенційні проблеми.

Компресія та кешування трафіку

Залежно від редакції NetScaler SD-WAN підтримує компресію передаваних даних (усунення зайвих або повторюваних фрагментів) і бітове кешування. Кешування здійснюється як на стороні відправника, так і на стороні приймача, що усуває необхідність повторної передачі однакового трафіку через WAN-канали та зменшує загальне навантаження на мережу.

Отже, узагальнюючи, ключові переваги NetScaler SD-WAN можна подати у вигляді такого списку:

- зменшення обсягу трафіку у WAN-мережі;
- маршрутизація даних найшвидшими та найякіснішими маршрутами;

- забезпечення найкращого рівня QoS для високопріоритетних додатків;
- високий рівень мережевої безпеки;
- простота адміністрування каналів між дата-центрами, офісами та філіями;
- використання недорогих інтернет-каналів (фіксованих і мобільних) замість дорогих виділених ліній;
- більш ефективне використання дорогих операторських каналів;
- можливість детального моніторингу WAN-маршрутів для швидкого пошуку та усунення несправностей.

Наприклад, для застосування NetScaler SD-WAN у сценарії Xen Desktop VDI був отриманий результат зниження в кілька разів необхідної смуги між офісом і дата-центром, де розміщуються віртуальні машини користувачів:

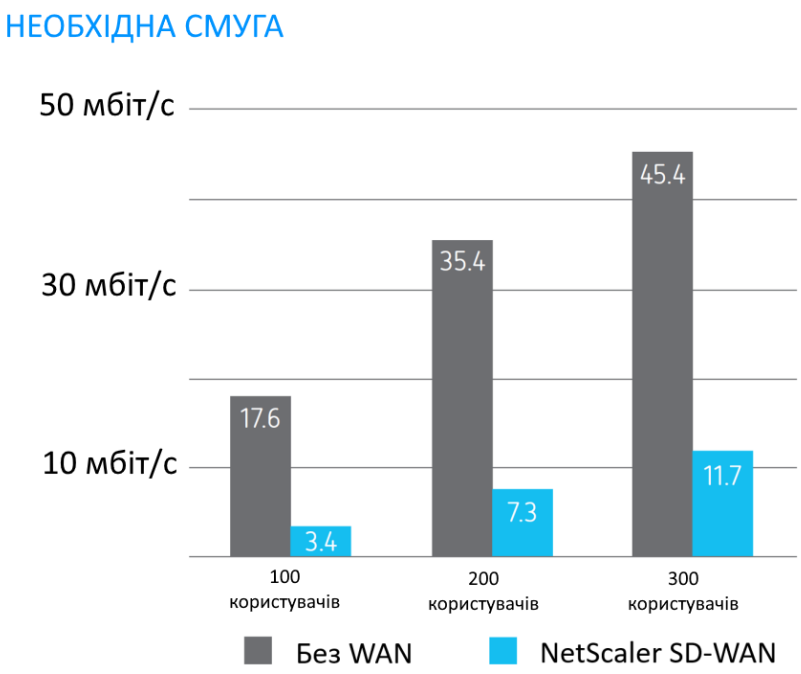


Рис. 2.6 Зниження необхідної смуги між офісом та дата-центром з NetScaler SD-WAN

3 ОДНОРАНГОВІ МЕРЕЖІ В SDN

3.1 Характеристики та проблематика

Із розвитком глобальної мережі Інтернет та зростанням вимог до гнучкості, масштабованості й автономності інформаційних систем дедалі більшої популярності набувають децентралізовані системи, побудовані на основі однорангових мереж (P2P, peer-to-peer). На відміну від традиційних клієнт-серверних моделей, де центральний сервер виступає ключовим елементом і є потенційною точкою відмови, в однорангових мережах відсутній виділений центр керування, а всі учасники є рівноправними. Кожен вузол може безпосередньо обмінюватися даними з будь-яким іншим, дотримуючись узгоджених протоколів і правил взаємодії.

Однорангові мережі лежать в основі багатьох сучасних технологій і сервісів, зокрема файлообмінних систем, блокчейн-платформ, багатокористувацьких ігор, мультимедійних сервісів і розподілених обчислень. Їхня популярність зумовлена низкою характерних переваг, які можна чітко виокремити.

Основні властивості та переваги однорангових (P2P) мереж:

- **Відмовостійкість.**

  У централізованих мережах існують критичні компоненти (сервери), відмова яких призводить до втрати працездатності системи. В однорангових мережах такі компоненти відсутні, тому вихід з ладу одного або навіть кількох вузлів **не порушує функціонування всієї мережі**.

- **Саморегулювання.**

  У P2P-мережах немає централізованого керуючого елемента. Стабільність і цілісність системи забезпечуються **домовленостями між учасниками**. Типовим прикладом є блокчейн-системи, де коректність роботи гарантується дотриманням правил консенсусу всіма вузлами.

- **Масштабованість.**

  У клієнт-серверних архітектурах продуктивність системи обмежується

можливостями сервера. У децентралізованих мережах обробка запитів і зберігання даних **розподіляються між вузлами**, тому відсутній єдиний елемент, який стримує зростання продуктивності.

- **Розподіл навантаження.**

  У централізованих системах кожен новий клієнт збільшує навантаження на сервер. В однорангових мережах кожен вузол може одночасно бути і споживачем, і джерелом даних, завдяки чому **ресурси мережі зростають разом із кількістю учасників**.

- **Економічність.**

  P2P-мережі зазвичай будуються на базі **недорогих програмно-апаратних компонентів загального призначення**. Вони не потребують потужних централізованих серверів, що знижує загальну вартість впровадження та експлуатації.

- **Простота розгортання.**

  Приєднання нового учасника до мережі, як правило, не потребує складних процедур налаштування. Достатньо виконати базові операції конфігурації, що сприяє швидкому зростанню мережі.

- **Стійкість до цензури.**

  Оскільки контент розподілений між великою кількістю вузлів, **блокування доступу до даних стає надзвичайно складним**. Історичним прикладом є закриття централізованого сервісу Napster і подальший успіх розподілених файлообмінних систем, які функціонують і сьогодні.

Ключовим елементом, що об’єднує різнорідних учасників у єдину систему, є організація мережевої взаємодії. У клієнт-серверних системах вона реалізується відносно просто — всі з’єднання проходять через центральний вузол. У децентралізованих мережах єдиного комунікаційного центру не існує, і саме тому маршрутизація та керування потоками даних стають значно складнішими завданнями.

Розвиток таких складних розподілених архітектур тісно пов’язаний із вдосконаленням концепції програмно-визначених мереж (SDN). Сучасні SDN-

підходи виходять за межі класичного централізованого керування та дедалі більше орієнтуються на програмну, адаптивну і політико-орієнтовану маршрутизацію в розподілених середовищах. Принципи SDN дозволяють гнучко керувати потоками трафіку, балансувати навантаження та оптимізувати маршрути навіть у мережах без жорстко визначеного центру, що робить їх надзвичайно актуальними для P2P- і блокчейн-систем.

Практичний досвід розроблення блокчейн-платформ показує, що саме організація мережевої взаємодії є однією з найскладніших частин таких систем. Завдання, які на перший погляд здаються простими, на практиці потребують глибокого розуміння алгоритмів маршрутизації, моделей саморегуляції та сучасних SDN-підходів. Узагальнення цього досвіду дозволяє швидше зануритися в предметну область, зрозуміти принципи побудови однорангових мереж і усвідомити, як ідеї SDN сприяють їх подальшому розвитку та вдосконаленню.

Постановка задачі в межах SDN-мережі

Розглядається однорангова мережа, що функціонує всередині програмно-визначеної мережі (SDN). Така мережа складається з великої кількості вузлів, які безпосередньо обмінюються повідомленнями між собою, а логіка керування передаванням даних, маршрутизацією та політиками трафіку реалізується на рівні SDN-контролера. У межах цієї SDN-інфраструктури необхідно розв’язати такі задачі:

1. **Реалізувати адресну (унікасну) розсилку**, тобто забезпечити надійну доставку повідомлення від вузла-відправника до конкретного вузла-отримувача;
2. **Реалізувати широкомовну розсилку**, тобто забезпечити доставку повідомлення від вузла-відправника до всіх вузлів однорангової мережі, що працює поверх SDN.

Для коректної роботи механізмів обміну даними кожному вузлу призначається унікальний ідентифікатор, який є неповторним у межах конкретної мережі. У загальному випадку такий ідентифікатор являє собою набір байтів, що однозначно визначає вузол, подібно до того, як ім’я ідентифікує людину. Як

ідентифікатор можуть використовуватися різні структури даних, наприклад хеш від інформації, що зберігається у вузлі.

У блокчейн-системах, які часто інтегруються або функціонують у середовищі SDN, у ролі ідентифікаторів зазвичай застосовуються публічні криптографічні ключі. Вони виконують не лише функцію ідентифікації, а й дозволяють реалізувати аутентифікацію, електронний цифровий підпис, шифрування та інші криптографічні операції, що підвищує рівень безпеки обміну даними в мережі.

У межах даного опису для спрощення сприйняття ідентифікатори вузлів розглядаються у вигляді чисел. Такий підхід полегшує пояснення алгоритмів маршрутизації та доставки повідомлень, не змінюючи при цьому їхньої суті, оскільки при переході від числового представлення до бітових або байтових структур логіка роботи алгоритмів залишається незмінною.

Ще одним важливим початковим припущенням є те, що IP-адреси вузлів відомі. У реальних SDN-системах способи отримання цієї інформації можуть бути різними. Наприклад, у мережі можуть використовуватися спеціалізовані служби або сервери, які зберігають та актуалізують інформацію про склад учасників, їхні ідентифікатори та IP-адреси. Іншим підходом є отримання цих даних від одного з уже підключених вузлів. Також можливий механізм широкомовного запиту, у відповідь на який вузли надсилають свої параметри.

Досить поширеним є й механізм bootstrap, коли вузол спочатку отримує інформацію лише про обмежену кількість «найближчих» учасників мережі, після чого запити рекурсивно поширюються далі за отриманими адресами. Детальний розгляд цих механізмів виходить за межі даного матеріалу, оскільки є об’ємною темою та потребує окремого аналізу. У подальшому викладі будемо виходити з припущення, що кожен вузол уже має всю необхідну інформацію для участі в обміні повідомленнями.

Вузли разом зі своїми ідентифікаторами формують оверлейну мережу, яка працює поверх фізичної мережі на основі IP-адрес, керованої SDN-контролером. Коли вузол з ідентифікатором 1 надсилає повідомлення вузлу з ідентифікатором 2, фактичне передавання здійснюється шляхом відправлення даних на IP-адресу, що

відповідає вузлу з ідентифікатором 2. При цьому SDN-контролер може впливати на вибір маршрутів, політики трафіку та пріоритети передавання.

Таким чином, кожен вузол однорангової мережі повинен зберігати актуальний перелік активних ідентифікаторів вузлів та відповідних їм IP-адрес. Саме на основі цієї інформації, у поєднанні з можливостями SDN, реалізуються ефективні механізми адресної та широкомовної доставки повідомлень у межах сучасної програмно-визначеної мережі.

Таблиця 3.1

Параметри мережі

Ідентифікатор вузла	**IP-адреса**
1	10.10.3.1
2	63.63.12.1
3	100.1.1.1
4	71.44.18.99
5	44.10.0.1
6	152.1.35.1

3.2 Рішення та створення топології

Найпростішим підходом є організація прямого з’єднання кожного вузла з усіма іншими. У такій схемі вузол-відправник, знаючи ідентифікатор вузла-отримувача, знаходить відповідну IP-адресу та безпосередньо передає повідомлення за цією адресою.

Для невеликих мереж подібне рішення є цілком працездатним і простим у реалізації. Проте зі зростанням масштабів мережі цей підхід швидко втрачає практичну доцільність. У такому випадку всі з’єднання між вузлами утворюють повний граф, у якому кожен вузол має прямий зв’язок з кожним іншим. Кількість ребер такого графа, тобто кількість необхідних з’єднань, визначається за формулою:

$$C = N(N-1)/2 \tag{3.1}$$

де N — загальна кількість вузлів у мережі.

За збільшення числа вузлів кількість з’єднань зростає надзвичайно швидко, фактично за квадратичною залежністю. Наприклад, для мережі зі 100 вузлів необхідно 4950 з’єднань, тоді як для 1000 вузлів їхня кількість зростає вже до 499 500. Такий вибуховий ріст кількості зв’язків робить повнозв’язну топологію непридатною для великих і масштабованих мереж, особливо в контексті сучасних розподілених та SDN-орієнтованих систем.

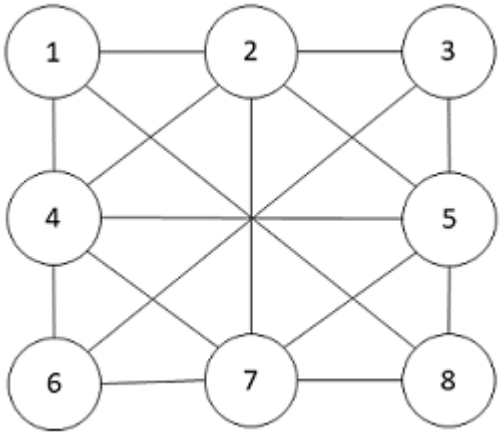


Рис. 3.1 Кожен вузол здійснює підключення до всіх вузлів у мережі

Створення топології

Очевидно, що описаний раніше підхід із повним з’єднанням усіх вузлів між собою є непридатним для практичного використання. Тому виникає потреба в упорядкуванні вузлів, тобто у формуванні певної топології мережі, яка забезпечувала б прийнятний баланс між кількістю з’єднань, масштабованістю та ефективністю маршрутизації.

Одним із найбільш інтуїтивних варіантів є побудова топології на основі відстані між вузлами. У такому випадку кожен вузол встановлює з’єднання лише з обмеженою кількістю найближчих до нього сусідів. Нехай це число позначається як C — максимальна кількість сусідніх вузлів, з якими підтримується прямий зв’язок. Під час побудови маршруту передавання повідомлення можна послідовно переходити від одного вузла до іншого, кожного разу обираючи той вузол, який є найближчим до поточного в контексті заданої метрики.

На перший погляд, такий алгоритм виглядає простим і логічним. Проте на практиці його реалізація породжує цілу низку складних питань і неоднозначностей.

1. Як обрати значення C, тобто максимальну кількість з’єднань для кожного вузла?

   З одного боку, зі збільшенням C покращується зв’язність мережі та зменшується довжина маршрутів. З іншого боку, зростає загальна кількість встановлених з’єднань, що ускладнює масштабування та збільшує накладні витрати. Виникає питання: як визначити оптимальне значення C, яке забезпечувало б ефективну маршрутизацію без надмірного ускладнення топології?

2. Як змінювати конфігурацію мережі у разі додавання або видалення вузлів?

   У глобальних і розподілених мережах такі події відбуваються постійно: одні вузли припиняють роботу, інші — з’являються в мережі. У разі жорсткого дотримання правила підключення лише до найближчих вузлів це може призводити до формування неоптимальної топології. Наприклад, якщо певний вузол виходить з мережі, інші вузли можуть автоматично перебудувати з’єднання не найкращим чином. У такій ситуації деякі маршрути стають довшими або менш збалансованими, хоча існують альтернативні варіанти з кращими характеристиками. У ідеальному випадку всі маршрути між вузлами мали б однакову або близьку довжину, що забезпечувало б рівномірний розподіл навантаження та передбачувану затримку.

Таким чином, навіть порівняно простий підхід до побудови топології на основі локальних відстаней між вузлами виявляється недостатнім для динамічних і масштабованих мереж. Це вимагає використання більш складних моделей організації топології, які здатні адаптуватися до змін складу мережі та забезпечувати стабільні характеристики маршрутизації, особливо в умовах сучасних SDN-орієнтованих середовищ.

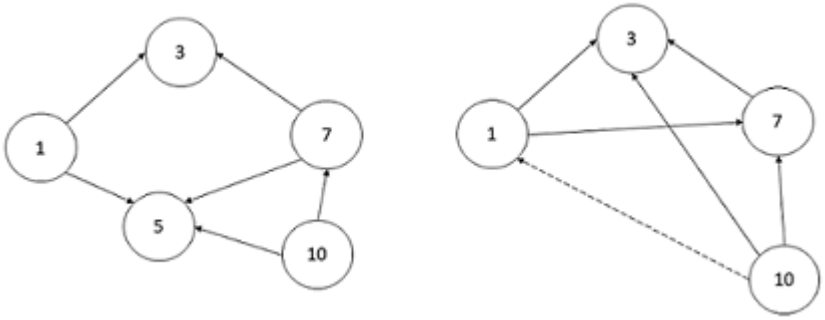


Рис. 3.2 Мережа з C = 3. У разі зникнення вузла 5 вузол 10 підключається до найближчого вузла 3, хоча доцільніше було б підключитися до вузла 1

Організація широкомовної розсилки

Описані раніше проблеми не є критичними, і за допомогою найпростішого алгоритму все ж можливо реалізувати адресну розсилку — нехай не оптимальну, але цілком працездатну. Проте у випадку широкомовної розсилки ситуація суттєво ускладнюється.

На перший погляд, логічним виглядає підхід, за якого вузол-відправник передає повідомлення своїм сусіднім вузлам, ті — своїм сусідам, і так далі, тобто використовується так звана лавиноподібна маршрутизація. Однак при такій схемі в мережі неминуче виникають замкнені контури, що призводить до багаторазової передачі одного й того самого повідомлення.

Розглянемо приклад топології, наведений на рисунку 3.3. Вузол 1 надсилає повідомлення своїм найближчим сусідам — вузлам 3 і 5. Вузол 3 пересилає це повідомлення своєму найближчому сусіду — вузлу 7. Далі вузол 7 передає повідомлення вузлам 5 і 10, унаслідок чого вузол 5 отримує те саме повідомлення також від вузла 10. Після цього вузол 5 пересилає отримані повідомлення вузлу 1, оскільки саме він є для нього найближчим сусідом. У результаті вузол 5 отримує одне й те саме повідомлення двічі та повторно надсилає його вузлу-відправнику, що ілюструє проблему циклів при широкомовній розсилці.

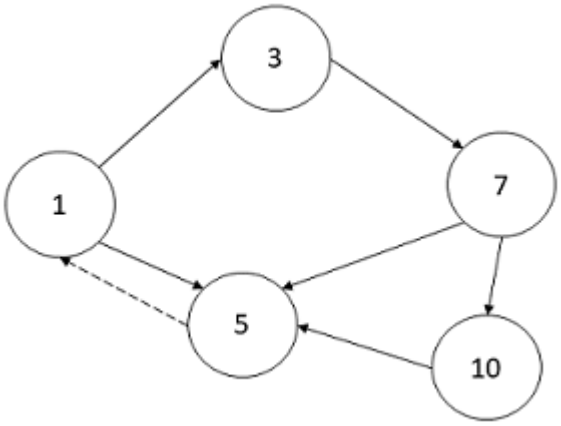


Рис. 3.3 Виникнення замкнутого контуру

Як видно, вузли мережі повинні вміти розпізнавати дубльовані повідомлення і припиняти їх подальше пересилання, інакше одні й ті самі дані будуть нескінченно циркулювати по замкнених контурах. У наведеному прикладі вузол 1 не повинен повторно передавати отримане повідомлення вузлу 3, оскільки це призводить до утворення циклу.

Для виявлення дублікатів повідомлення мають містити ознаки, що дозволяють однозначно їх ідентифікувати. Вузол, який отримує повідомлення, зберігає ці ознаки, а при повторному надходженні того самого повідомлення може визначити, що воно вже було оброблене, і зупинити його подальше поширення.

Унікальні ідентифікатори повідомлень можуть формуватися різними способами. Наприклад, кожному повідомленню можна призначати унікальний порядковий номер, який разом з ідентифікатором вузла-відправника утворює унікальний ідентифікатор повідомлення. Іншим варіантом є використання хеш-суми вмісту повідомлення або ж спеціальних атрибутів, характерних для конкретної мережі.

У теорії такий підхід виглядає цілком прийнятним, проте на практиці він супроводжується значною кількістю проблем. Мережа швидко перевантажується дублікатами повідомлень; лічильники ідентифікаторів можуть переповнюватися; хеш-функції не гарантують повної відсутності колізій; зберігання списку вже отриманих ідентифікаторів потребує додаткової пам’яті; пошук відповідного ідентифікатора під час обробки кожного повідомлення займає значний час. Крім того, відсутні чіткі критерії, коли саме можна безпечно видаляти записи з бази

оброблених повідомлень. У сукупності всі ці чинники роблять такий алгоритм малопридатним для практичного використання.

Які ж існують альтернативні підходи до розв’язання цієї проблеми? Один із варіантів полягає в тому, щоб додавати до повідомлення список уже відвіданих вузлів. У цьому випадку кожен вузол, отримавши повідомлення, пересилає його лише тим сусідам, яким воно ще не надсилалося. Така схема є працездатною, але її застосування обмежується невеликими мережами. У великих мережах список відвіданих вузлів швидко зростає і може багаторазово перевищувати обсяг корисних даних. Крім того, через те, що повідомлення змінюється на кожному кроці маршруту, використання електронного цифрового підпису стає неможливим, оскільки будь-яка модифікація робить підпис недійсним. Для деяких систем, зокрема блокчейн-платформ, ця проблема є критичною.

Іншим підходом до організації широкомовної розсилки є так звана «розсилка за запитом». У цьому випадку вузол-ініціатор спочатку надсилає своїм сусідам короткі повідомлення-сповіщення, які містять унікальні ознаки даних, що плануються до передачі. Отримавши таке сповіщення, вузли перевіряють, чи отримували вони ці дані раніше. Якщо ні, вони надсилають запит ініціатору для отримання відповідної інформації. Після отримання даних вузли, у свою чергу, сповіщають своїх сусідів про наявність нових відомостей. Процес повторюється доти, доки всі учасники мережі не отримають потрібні дані. Оскільки сповіщення мають невеликий розмір, їх дублювання не створює суттєвих накладних витрат.

Описаний механізм довів свою працездатність і застосовувався в ранніх реалізаціях однорангових мереж, проте він також має низку істотних недоліків:

- складний протокол взаємодії між вузлами;
- низька швидкість поширення інформації через велику кількість операцій типу «запит – відповідь»;
- неможливість повністю усунути дублювання даних, оскільки ті самі повідомлення можуть багаторазово передаватися одними й тими ж маршрутами;

- додаткові обчислювальні витрати, пов’язані з перевіркою наявності даних при кожному новому сповіщенні.

Таким чином, організація широкомовної розсилки в однорангових мережах є складною і нетривіальною задачею, що потребує ретельного теоретичного обґрунтування та продуманих алгоритмічних рішень.

3.3 Основні алгоритми для модернізації

Chord

Ідея, покладена в основу алгоритму Chord (його академічний опис відомий у науковій літературі), є доволі простою за своєю суттю. Усі вузли мережі впорядковуються за зростанням їхніх ідентифікаторів. Кожен вузол встановлює з’єднання з наступним у цьому впорядкованому списку, а останній вузол замикає ланцюг, з’єднуючись із першим. У результаті формується кільцева топологія, у якій ідентифікатор кожного наступного вузла є більшим за ідентифікатор попереднього.

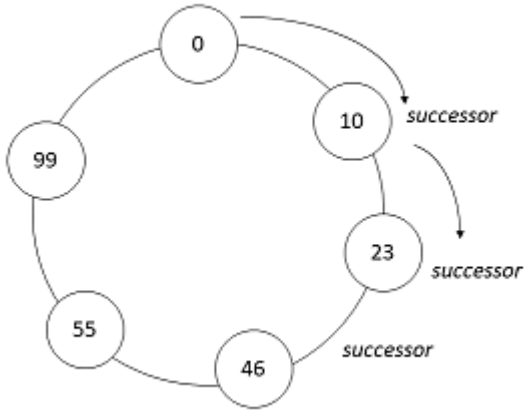


Рис. 3.4 Кільцева топологія Chord

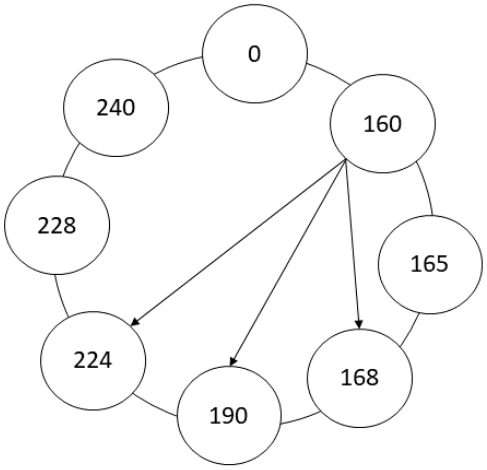
Маршрутизація в такій структурі в найпростішому варіанті здійснюється шляхом послідовної передачі повідомлення від вузла до вузла по кільцю, доки воно не досягне адресата. У разі додавання нового вузла або виходу одного з наявних його безпосередній попередник переналаштовує з’єднання на найближчого наступника, завдяки чому кільцева структура автоматично відновлюється.

Очевидно, що за такого підходу маршрутизація є неефективною. У найгіршому випадку кількість кроків передавання повідомлення становить O(N), де N — кількість вузлів у мережі. Щоб зменшити число проміжних вузлів на маршруті, у Chord використовується спеціальний механізм оптимізації — finger table, яку можна перекласти як таблицю вказівників або таблицю посилань.

Таблиця вказівників формується таким чином. Нехай m — кількість бітів, що використовуються для представлення ідентифікатора вузла. Тоді кожен вузол з ідентифікатором n створює таблицю з m записів, де кожен елемент визначається за формулою:

$$entry(i) = (n + 2^{\mathrm{i}}) mod 2^{\mathrm{m}} \qquad (3.2)$$

Кожен запис таблиці вказує на вузол, який знаходиться на відстані, що вдвічі перевищує попередню. Якщо вузол із таким ідентифікатором у мережі відсутній, у таблицю заноситься найближчий доступний вузол, що відповідає цій позиції в кільці.



m = 8, n = 160

m — Кількість біт в ідентифікаторі
n — Номер вузла

$$i^{th} = successor\left(n + 2^{i}\right) mod\ 2^{m},\ i = 1 \ldots \mathrm{m}$$

Комірка	Вирахувано	Фактично
0	160	160
1	162	165
2	164	165
3	168	168
4	176	190
5	192	224
6	224	224
7	32	160

Рис. 3.5 Таблиця вказівників у Chord для вузла з номером 160

Завдяки цьому під час маршрутизації повідомлення передаються не послідовно через усі вузли кільця, а стрибками на значні відстані. Кожен наступний вузол, отримавши повідомлення, використовує власну таблицю вказівників і пересилає його вузлу, який розташований приблизно вдвічі ближче до цільового. У

результаті довжина маршруту істотно скорочується, а середня кількість кроків наближається до log(N).

Розглянемо, як у Chord організовується широкомовна розсилка. Вузол-ініціатор надсилає повідомлення всім вузлам, зазначеним у його таблиці вказівників. Кожен із цих вузлів, отримавши повідомлення, повторює аналогічну процедуру відповідно до власної таблиці. У підсумку повідомлення поширюється по всій мережі за m кроків, де m — кількість бітів ідентифікатора вузла.

Разом із тим виникає проблема дублювання, оскільки таблиці вказівників різних вузлів можуть містити посилання на ті самі вузли. Для усунення надлишкових пересилань у Chord застосовується спеціальний механізм обмеження. Кожне повідомлення містить додаткове поле limit, яке визначає, яким вузлам дозволено його подальше поширення. Значення limit для конкретного пересилання дорівнює наступному елементу таблиці вказівників відправника.

Пояснимо це на прикладі. Нехай ідентифікатор вузла має розмірність 3 біти, отже максимальна кількість вузлів у системі дорівнює 8. Припустімо, що вузол 1 ініціює широкомовну розсилку. У його таблиці вказівників містяться вузли 2, 3 і 5, яким він надсилає повідомлення. Під час пересилання повідомлення вузлу 2 наступним записом у таблиці є вузол 3, і саме це значення передається як limit. Вузол 2, отримавши повідомлення з обмеженням 3, аналізує свою таблицю та не знаходить у ній вузлів із ідентифікаторами меншими за limit, тому далі повідомлення не поширює.

Аналогічно вузол 1 надсилає повідомлення вузлу 3, передаючи як limit значення 5. Вузол 3 бачить, що у його таблиці є вузол 4, ідентифікатор якого менший за отримане обмеження, тому пересилає повідомлення цьому вузлу. У випадку пересилання повідомлення вузлу 5 наступного запису в таблиці вже немає, тож за правилами кільцевої топології наступником вважається вузол 1, і це значення також передається як limit.

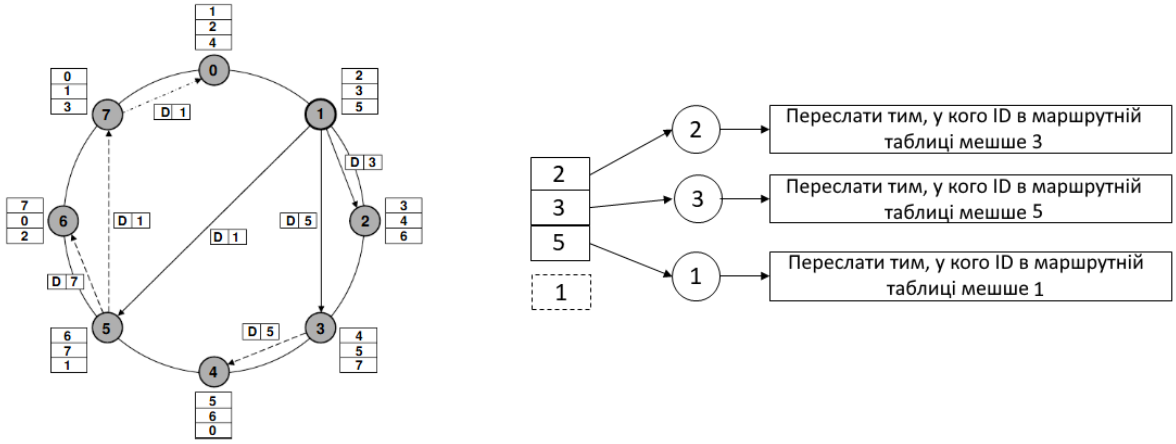


Рис. 3.6 Широкомовне розсилання в Chord

Описаний механізм повторюється ітеративно на всіх вузлах мережі. У результаті широкомовна розсилка завершується в середньому за log(N) кроків, причому точна кількість залежить від того, наскільки число вузлів у мережі наближене до степеня двійки.

Kademlia

Розглянемо ще один поширений алгоритм маршрутизації — Kademlia, який ґрунтується на використанні деревоподібної топології. Як і в алгоритмі Chord, у Kademlia вузли впорядковуються за певною метрикою відстані між ними. Проте на відміну від Chord, де використовується арифметична різниця між ідентифікаторами, у Kademlia відстань визначається ступенем близькості ідентифікаторів, яка обчислюється за допомогою операції виключного АБО (XOR) між значеннями ідентифікаторів вузлів.

Увесь простір ключів поділяється на групи, що називаються бакетами. Кожен бакет охоплює діапазон ключів із відстанями від 2^i до 2^{i+1}, причому місткість кожного наступного бакета вдвічі перевищує місткість попереднього. У результаті формується ієрархічна структура ключів, яку зручно уявляти у вигляді дерева. Вузол, який приєднується до мережі, повинен встановити з’єднання щонайменше з одним довільним вузлом із кожного непорожнього бакета.

Під час передавання повідомлення вузол-відправник спочатку визначає, у якому бакеті знаходиться ідентифікатор вузла-отримувача, після чого надсилає повідомлення одному з вузлів цього бакета, з якими він має активні з’єднання.

Отримавши повідомлення, проміжний вузол повторює аналогічну процедуру у межах власної структури бакетів. Такий ітеративний процес триває доти, доки повідомлення не досягне цільового вузла. Теоретично довжина маршруту в Kademlia також наближається до log(N), де N — кількість вузлів у мережі.

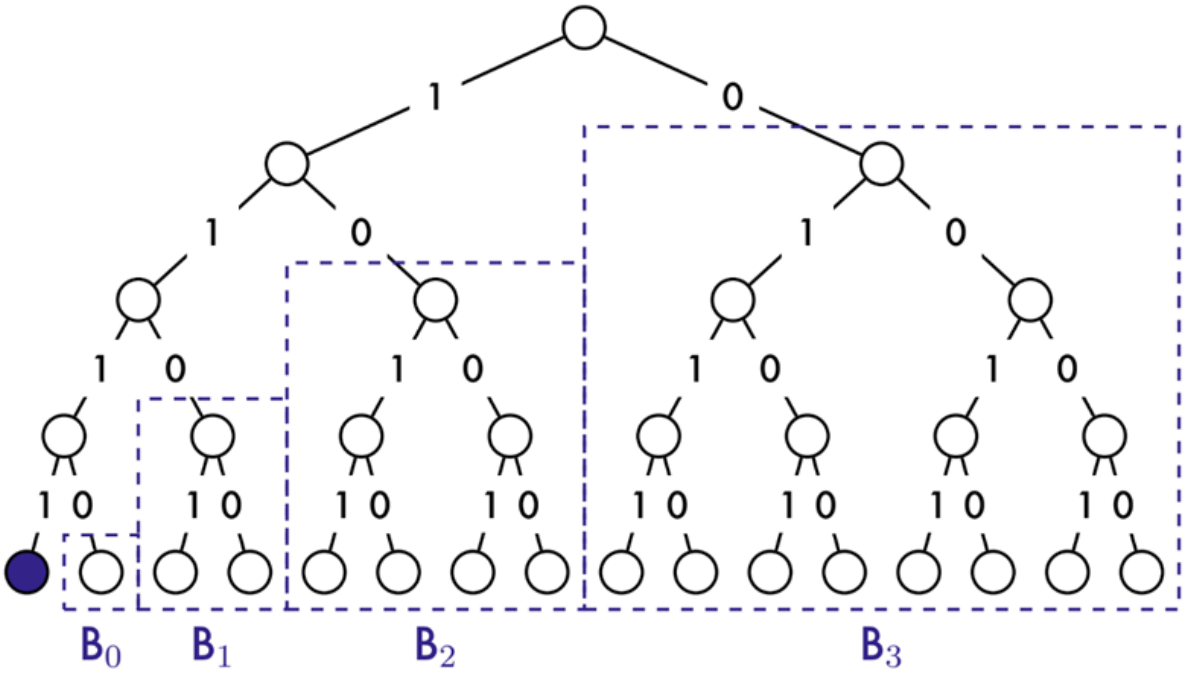


Рис. 3.7 Дерево ключів Kademlia

Варто зауважити, що дерево в Kademlia є лише логічною моделлю. На практиці немає потреби явно будувати всю деревоподібну структуру — достатньо визначити відповідний бакет і обрати з нього вузол для наступного кроку маршрутизації.

Розглянемо, як у Kademlia організовується широкомовна розсилка. Вузол-ініціатор обирає по одному вузлу з кожного бакета та надсилає їм повідомлення. При цьому повідомленню присвоюється спеціальний параметр — «висота», значення якого дорівнює поточній кількості бакетів у дереві. Вузли, що отримали повідомлення, виконують аналогічні дії для своїх бакетів, зменшуючи значення висоти на одиницю. Процес триває доти, доки значення висоти не стане рівним нулю, після чого розсилка завершується.

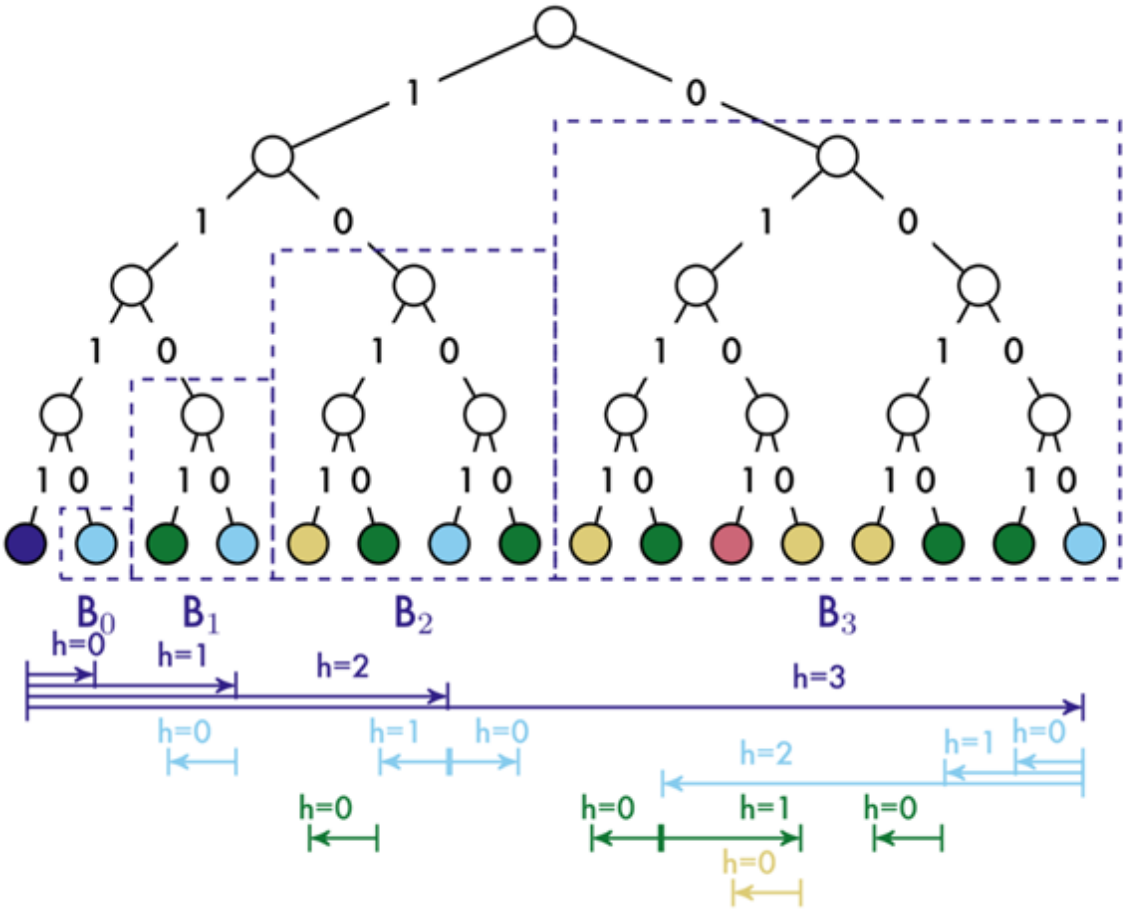


Рис. 3.8 Широкомовне розсилання Kademlia

Однією з ключових особливостей Kademlia є те, що маршрут повідомлення не є детермінованим. На кожному кроці вузол обирає наступного отримувача випадковим чином із відповідного бакета. Такий підхід спеціально застосовується для підвищення стійкості мережі до атак типу «відмова в обслуговуванні» (DoS).

Якщо в мережі присутній зловмисний вузол, який навмисно припиняє пересилання повідомлень, потрапляння повідомлення до такого вузла призводить до його втрати. Проте завдяки випадковому вибору маршруту цей вузол не здатен повністю заблокувати роботу всієї мережі. Частина повідомлень може втрачатися, але мережа загалом залишається працездатною. Більше того, у разі реалізації механізмів контролю добросовісності (наприклад, підтвердження отримання повідомлень) зловмисний вузол може бути виключений із маршрутів без необхідності перебудови всієї топології.

Такий підхід підвищує надійність і адаптивність мережі, однак має й побічний ефект — порядок доставки повідомлень не гарантується. Наприклад, декілька повідомлень, надісланих одним і тим самим вузлом, можуть досягти адресата у довільній послідовності. Для деяких систем це не є критичним, але для інших має принципове значення. Зокрема, у блокчейн-системах порядок надходження блоків є ключовим: якщо отриманий блок посилається на попередній блок, який ще відсутній у вузла-отримувача, такий блок вважається невалідним. У подібних випадках застосовуються спеціальні механізми обробки, наприклад тимчасове накопичення блоків перед їх включенням до основного ланцюга.

CAN

Розглянемо ще один алгоритм маршрутизації, який вирізняється своєю оригінальністю, — Content-Addressable Network (CAN). Цей підхід базується на побудові мережі у вигляді багатовимірної декартової системи координат, яка проєктується на тор відповідної розмірності. Важливо підкреслити, що така координатна система є віртуальною і жодним чином не пов’язана з реальним фізичним простором або географічним розташуванням вузлів.

Процес формування цієї системи можна уявити наступним чином. У випадку двовимірного простору мережа подається у вигляді площини, де кожному виміру відповідає окрема координатна вісь. Якщо уявно «згорнути» ці площини так, щоб кожна з них утворила коло, а отримані кола з’єднати вздовж центральної осі, формується тор відповідної розмірності. Саме така геометрична модель лежить в основі топології CAN. Для наочності часто розглядають тор у розрізі, що дозволяє краще зрозуміти принципи організації зв’язків між вузлами.

Надалі, з метою спрощення пояснення та кращої візуалізації, зазвичай використовується двовимірна система координат. Водночас слід пам’ятати, що описана топологія легко масштабується і може бути застосована до згорнутого простору довільної розмірності d, що забезпечує гнучкість і адаптивність алгоритму при збільшенні кількості вузлів у мережі.

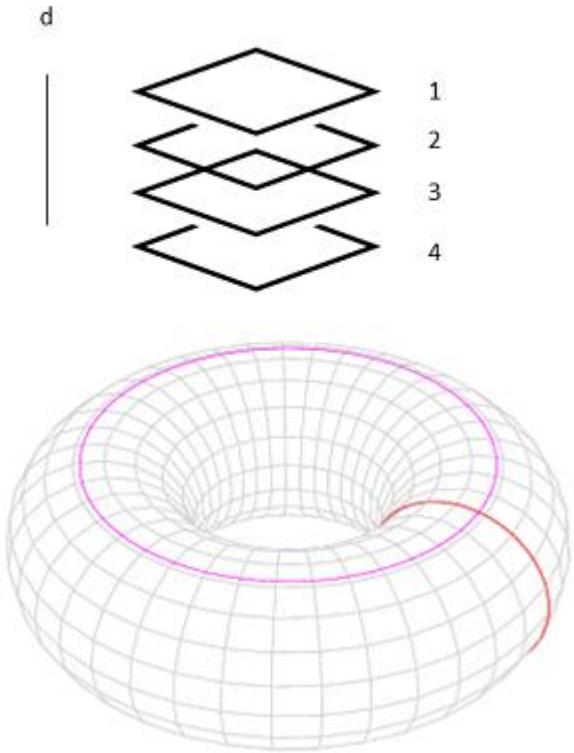


Рис. 3.9 Побудова тора розмірності d = 4. Кожна площина і-ї розмірності поєднана з площинами сусідніх розмірностей, утворюючи безперервний простір координат

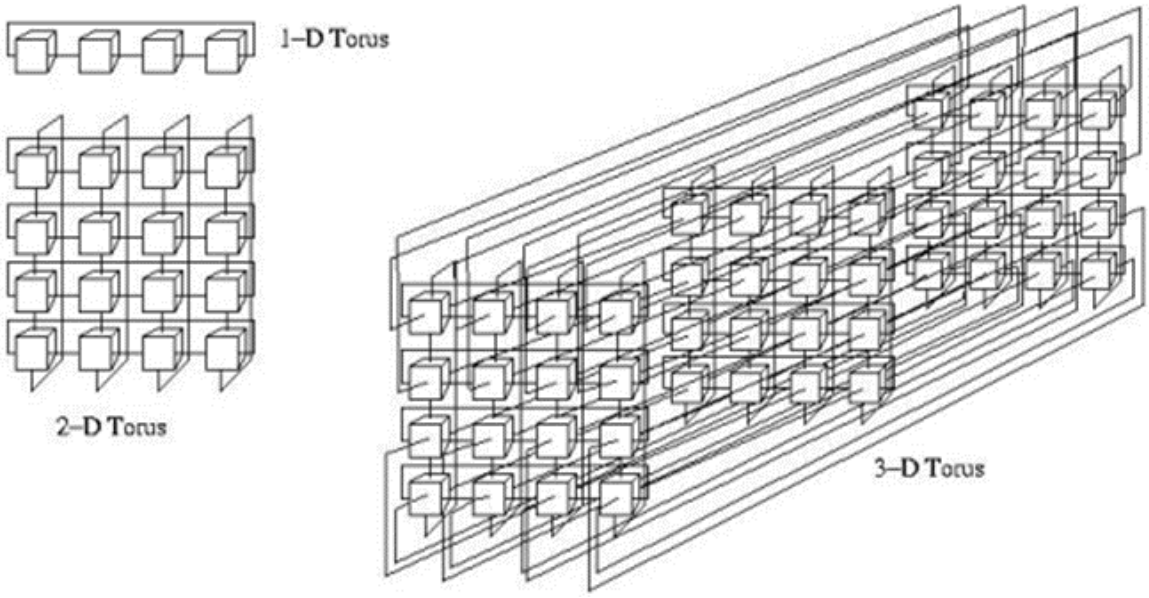


Рис. 3.10 Перетин двовимірного та тривимірного тора

Ідентифікатори вузлів у мережі CAN відображаються у вигляді точок у координатному просторі. Кожен вузол відповідає за окрему зону цього простору та

в межах своєї зони володіє інформацією про сусідні вузли, які розташовані в суміжних зонах.

У d-вимірному координатному просторі зони вважаються сусідніми за умови, що вони мають спільну координатну межу вздовж одного виміру та є суміжними за всіма іншими вимірами. Іншими словами, сусідство визначається наявністю спільної сторони між зонами.

Так, у двовимірній системі координат, показаній на рисунку 11, зона 4 має сусідні зони 3, 1, 5 та 7. Це пояснюється тим, що відповідні вузли мають спільну сторону вздовж осі X або осі Y, а також межують між собою за іншими координатами. Натомість зона 8 не вважається сусідньою до зони 4, оскільки між ними відсутня спільна межа, а отже пряме сусідство не формується.

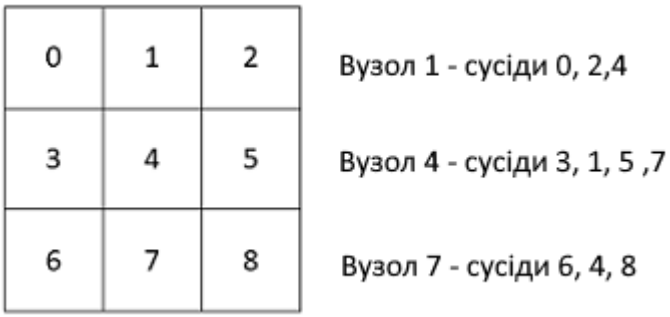


Рис. 3.11 Двовимірна координатна площина

Постає закономірне питання: яким чином відобразити ідентифікатор вузла у вигляді точки в d-вимірному просторі? У загальному випадку для цього застосовується спеціальна хеш-функція, яка для заданого ідентифікатора вузла формує унікальний набір координат у багатовимірному просторі.

На практиці часто використовується простий, але достатньо ефективний метод розбиття. Бітове представлення ідентифікатора вузла довжиною n біт ділиться на рівні за розміром сегменти, кількість яких дорівнює d. Кожен із цих сегментів інтерпретується як окрема координата відповідного виміру. Таким чином формується повний набір координат вузла у d-вимірному просторі, що наочно ілюструється на рисунку.

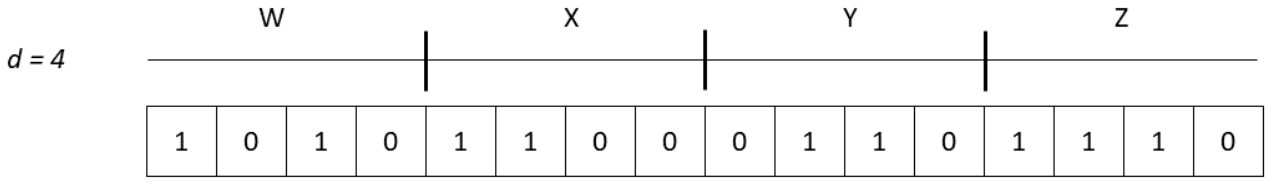


Рис. 3.12 Поділ 16-бітного ідентифікатора вузла на 4 координатні розмірності

Маршрутизація в мережі CAN виконується за допомогою алгоритму. На кожному кроці передавання вибирається така сусідня зона, координати якої є найближчими до координат вузла-отримувача, після чого повідомлення пересилається саме в цю зону.

Оскільки для кожної зони зазвичай існує декілька суміжних сусідів, у мережі CAN можливий вибір різних альтернативних маршрутів. Наявність таких альтернатив підвищує надійність і відмовостійкість мережі, оскільки у разі недоступності одного з шляхів може бути використаний інший.

З теоретичної точки зору швидкість маршрутизації в CAN оцінюється як N^(1/d), де N — кількість вузлів у мережі, а d — розмірність координатного простору.

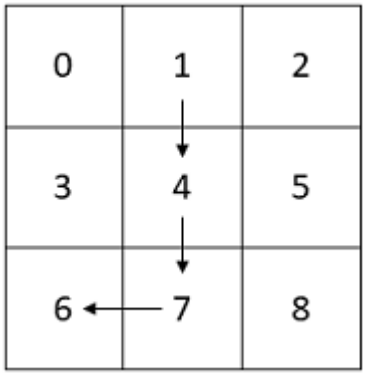


Рис. 3.13 Маршрутизація в мережі CAN

Потрібно окремо розглянути механізми приєднання та виходу вузлів із мережі CAN, оскільки саме на цьому етапі проявляються характерні особливості даного підходу. Теоретично, якби кожній точці координатного простору відповідав окремий активний вузол, поділ простору на зони був би зайвим — у такому разі кожен вузол представляв би власну зону, що містить рівно одну точку.

Проте в реальних умовах кількість функціонуючих вузлів значно менша за кількість можливих точок у координатному просторі. Саме тому в мережі CAN кожен вузол обслуговує не одну точку, а цілу множину точок, які разом утворюють певну зону. У межах цієї зони вузол взаємодіє з вузлами сусідніх зон, підтримуючи цілісність і зв’язність мережі.

Під час підключення нового вузла відповідна зона ділиться на дві частини, і новий вузол бере на себе керування однією з них. Навпаки, у разі відключення вузла його зона об’єднується з сусідньою, а керування розширеною зоною переходить до вузла, що залишився активним. Важливо, що така реконфігурація має локальний характер: зміни стосуються лише тих зон, де відбувається поділ або об’єднання, оскільки саме там змінюється склад сусідів. Усі інші зони мережі залишаються без змін, що забезпечує ефективну масштабованість і мінімізує накладні витрати на перебудову мережі.

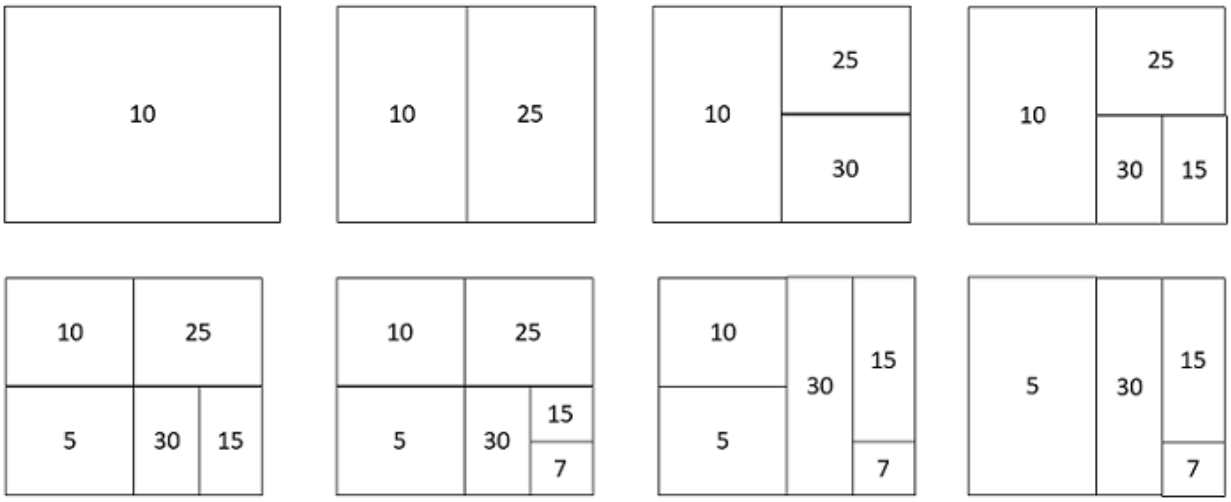


Рис. 3.14 Реконфігурація зон при додаванні/видаленні нових вузлів

Порівняльний аналіз

Який саме підхід до проєктування децентралізованої системи слід обрати — питання відкрите, і єдиної правильної відповіді на нього не існує. Розглянуті алгоритми базуються на принципово різних концепціях і по-різному поводяться залежно від характеристик мережі, типу навантажень та умов експлуатації. Дана проблематика детально досліджується у численних фундаментальних наукових

працях, де виконуються як теоретичні, так і експериментальні порівняння різних підходів.

У межах цієї роботи не ставиться за мету проведення вичерпного кількісного аналізу. Натомість ми зосередимося на якісному порівнянні, намагаючись виділити основні переваги та недоліки кожного алгоритму, а також окреслити сценарії, у яких той чи інший підхід є найбільш доцільним.

Основні критерії оцінювання алгоритмів наведено в таблиці нижче.

Таблиця 3.2

Порівняння алгоритмів

Критерій	**Chord**	**Kademlia**	**CAN**
Складність реалізації	Низька	Середня	Висока
Детермінованість маршруту	Висока	Низька	Середня
Стійкість до churn	Низька	Висока	Середня
Стійкість до атак типу «відмова в обслуговуванні»	Низька	Висока	Середня
Обсяг пам’яті	Низький	Високий	Середній
Адаптивність	Низька	Середня	Висока

Складність реалізації.

Ідейна простота алгоритму Chord є очевидною — його базова концепція легко сприймається і не потребує складних механізмів. Водночас CAN значно складніший з точки зору практичної реалізації через багатовимірну координатну модель і керування зонами. Алгоритм Kademlia займає проміжне місце: його принципи загалом інтуїтивні, однак реалізація потребує ретельнішого опрацювання, ніж у випадку з Chord.

Детермінованість маршруту.

Цей критерій відображає ступінь передбачуваності шляху, яким передаються повідомлення мережею. У Chord маршрут є повністю детермінованим і однозначно визначається позиціями вузлів у кільці. У Kademlia маршрут не є строго фіксованим: вибір наступного вузла залежить від поточного стану таблиць маршрутів і може змінюватися з часом. У CAN детермінованість залежить від конкретної реалізації: за наявності кількох можливих напрямків можна задати правило вибору найближчої зони, що зробить маршрут передбачуваним.

Стійкість до churn.

Під churn розуміють здатність мережі стабільно функціонувати за умов частого приєднання та виходу вузлів. Chord у цьому аспекті є найменш стійким, оскільки кожна зміна складу мережі потребує перебудови кільцевої топології та оновлення finger table. Kademlia, навпаки, демонструє високу стійкість: її таблиці оновлюються лише в тих вузлах, які безпосередньо взаємодіють із вузлом, що підключається або відключається. CAN займає проміжну позицію — при виході вузла необхідна локальна перебудова зон у сусідів, а при додаванні нового вузла може знадобитися інформація про загальну топологію для коректного визначення зони.

Стійкість до атак типу «відмова в обслуговуванні».

Такі атаки виникають у випадку, коли вузол на маршруті навмисно припиняє пересилання повідомлень. Chord є найбільш уразливим, адже порушення цілісності кільця змушує систему шукати наступний вузол і виконувати переналаштування. Kademlia має найвищу стійкість завдяки наявності багатьох альтернативних маршрутів, що дозволяє обходити зловмисні вузли. У CAN кількість альтернативних шляхів обмежена, тому його стійкість до таких атак оцінюється як середня.

Обсяг пам’яті.

У Chord розмір маршрутної таблиці є фіксованим, а кожен запис містить лише ідентифікатор відповідного вузла. У Kademlia вузли зберігають ідентифікатори у k-бакетах, що покривають різні діапазони XOR-відстаней, тому загальна кількість записів може бути досить значною. У CAN зберігається інформація лише про

сусідні зони та відповідні вузли, що забезпечує помірні вимоги до використання пам’яті.

Адаптивність.

Під адаптивністю розуміють можливість налаштування алгоритму під конкретні вимоги системи. Chord у цьому відношенні є найменш гнучким, оскільки майже не має параметрів для тонкого налаштування. У Kademlia адаптація можлива шляхом зміни розміру бакетів, параметрів запитів або стратегій вибору сусідів. CAN пропонує значно ширші можливості: можна змінювати розмірність координатного простору, правила вибору напрямків маршрутизації, механізми локального оновлення зон та інші параметри, що робить його найбільш гнучким серед розглянутих алгоритмів.

Наведені критерії не охоплюють усіх можливих аспектів, які можуть впливати на вибір архітектури. Проте вони є надійною відправною точкою для аналізу та проєктування децентралізованих систем з урахуванням вимог до масштабованості, надійності та керованості.

4 МЕРЕЖА ADN ЯК АЛЬТЕРНАТИВА SDN

4.1 Поняття та відмінності

Автономно керована мережа та її відмінність від SDN

Поняття автономно керованої мережі тісно пов’язане з еволюцією програмно-визначених мереж (SDN), однак не є їх прямим синонімом. Якщо SDN зосереджується на централізованому програмному керуванні мережевою інфраструктурою, то автономна мережа робить наступний крок — вона здатна самостійно аналізувати свій стан, приймати рішення та виконувати дії без постійного втручання адміністратора.

Для формування чітких критеріїв оцінювання такого підходу компанія Huawei спільно з консалтинговою компанією IDC провела дослідження, метою якого стало визначення рівнів автономності мережевої інфраструктури та її здатності до самостійного функціонування.

Очікування замовників від мережі ЦОД

Сучасні замовники очікують, що мережева інфраструктура центру обробки даних буде:

- ефективною з точки зору використання ресурсів;
- надійною та відмовостійкою;
- простою в адмініструванні та супроводі;
- масштабованою без складних ручних операцій;
- здатною швидко адаптуватися до змін навантаження.

Ідеальним варіантом вважається мережа, яка:

- самостійно налаштовується;
- автоматично оптимізує параметри роботи;
- виявляє та локалізує проблеми;
- виконує відновлення після збоїв без участі інженера

Обмеження традиційного SDN-підходу

Хоча сучасні SDN-контролери значно розширили можливості автоматизації, вони:

- переважно виконують заздалегідь визначені політики;
- залежать від ручного проєктування логіки керування;
- не завжди здатні самостійно адаптуватися до нетипових ситуацій.

Це породжує ключове питання: як виміряти рівень автоматизації та зрозуміти, наскільки мережа справді є автономною?

Підхід IDC до оцінювання автономності мереж

У межах дослідження IDC було запропоновано:

- розглядати автономність як **багаторівневу характеристику**, а не як двійкову ознаку;
- оцінювати мережу за здатністю:
    - спостерігати (monitoring),
    - аналізувати (analytics),
    - приймати рішення (decision making),
    - виконувати дії (automation).

Таким чином, автономна мережа — це не просто SDN з контролером, а інтелектуальна система, яка поступово переходить від реактивного до проактивного керування

Цифровізація як рушій автономних мереж

Розвиток автономно керованих мереж відбувається на тлі глобальних процесів:

- масової цифровізації бізнесу;
- переходу до хмарних моделей обчислень;
- зростання складності IT-інфраструктур;
- дефіциту кваліфікованих IT-спеціалістів.

Хмарні технології в цьому контексті — це не лише середовище виконання навантажень, а й парадигма автоматизованої експлуатації.

Епоха множинних інновацій

За оцінками IDC, сучасний IT-ринок входить в період, що характеризується одночасним розвитком:

- штучного інтелекту;
- Інтернету речей (IoT);

- блокчейн-технологій;
- інтерфейсів природної взаємодії.

Спільною метою всіх цих напрямів є:

- зменшення ролі людини в операційному керуванні;
- підвищення самостійності систем;
- перехід до автономних інфраструктур.

Місце автономних мереж у розвитку SDN

У цьому контексті автономно керовані мережі можна розглядати як:

- логічне продовження SDN;
- поєднання SDN, аналітики, машинного навчання та автоматизації;
- основу для майбутніх мереж ЦОД і хмарних платформ.

Таким чином, автономність стає ключовим критерієм зрілості мережі, а SDN — технологічним фундаментом, на якому ця автономність вибудовується.

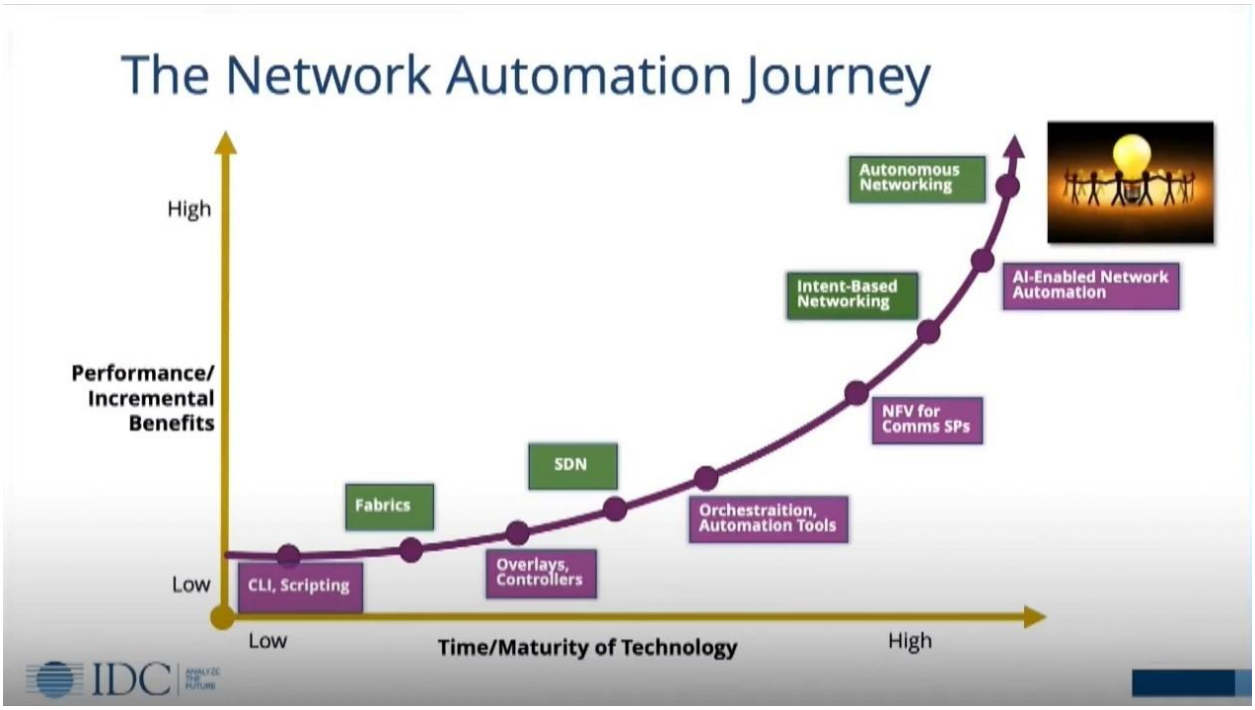


Рис. 4.1 Шлях розвитку автоматизації мережевої інфраструктури: від CLI та SDN до intent-based та автономних мереж

На поданій схемі показано еволюційний шлях автоматизації мережевої інфраструктури, який проходить через низку послідовних етапів розвитку. Початковою точкою цього процесу є використання інтерфейсу командного рядка (CLI) та створення окремих скриптів для виконання типових операцій. Такий підхід

дозволяє частково зменшити обсяг ручної роботи, проте він залишається трудомістким, залежним від досвіду адміністратора і погано масштабується.

Наступним кроком стає поява мережевих фабрик, які забезпечують більш уніфікований підхід до побудови мереж і дають змогу підвищити швидкість розгортання, продуктивність та керованість інфраструктури. Після цього розвиток автоматизації переходить на рівень SDN-контролерів і технологій віртуалізації, де керування мережею відокремлюється від апаратного рівня, а логіка управління централізується. Саме на цьому етапі активно впроваджуються інструменти оркестрації та автоматизації для мереж центрів обробки даних, що дозволяє швидше запускати сервіси та ефективніше використовувати ресурси.

Якісно новим рівнем розвитку є перехід до мереж, що керуються на основі намірів (intent-based networking). У таких мережах адміністратор описує бажаний результат або політику, а система самостійно визначає, яким чином її реалізувати на рівні конфігурацій і маршрутів. Однак кінцевою метою цього прогресу є створення повністю автономної мережі, у якій ключові процеси керування, оптимізації та відновлення виконуються автоматично з використанням штучного інтелекту. Саме до цього рівня прагнуть провідні виробники та аналітичні компанії, розглядаючи автономність як стратегічний напрям розвитку мережевих технологій.

Виникає закономірне питання: що саме слід розуміти під автономністю мережі та як об’єктивно оцінити її рівень? Для відповіді на це питання компанія IDC запропонувала шестирівневу модель автономності, яка дозволяє чітко класифікувати мережеві рішення залежно від ступеня автоматизації та самостійності їхньої роботи.

На **рівні 0** керування мережею повністю здійснюється вручну на всіх етапах її життєвого циклу. Автоматизація відсутня, а всі налаштування, зміни та відновлення виконуються оператором.

Рівень 1 також передбачає переважно ручне керування мережею, хоча можуть застосовуватися окремі інструменти для спрощення рутинних операцій. Проте загальний підхід до експлуатації залишається традиційним і сильно залежить від людини.

На **рівні 2** з’являється часткова автоматизація окремих сценаріїв. Вона поєднується зі стандартними засобами моніторингу, аналізу та керування політиками, але не охоплює всі аспекти роботи мережі.

Рівень 3 характеризується так званою умовною автоматизацією. Система вже здатна аналізувати стан мережі, формувати рекомендації та пропонувати варіанти дій, однак остаточне рішення щодо їх застосування залишається за оператором.

На **рівні 4** мережа стає значною мірою автоматизованою та автономною. Керування здійснюється декларативними методами на основі намірів, а роль адміністратора зводиться переважно до спостереження за подіями та підтвердження або відхилення рішень, запропонованих системою.

Нарешті, **рівень 5** відповідає повністю автономній мережі, яка протягом усього життєвого циклу здатна самостійно застосовувати політики, виявляти та усувати несправності, оптимізувати роботу і відновлювати сервіси без участі людини. Саме цей рівень розглядається як кінцева мета розвитку сучасних мережевих технологій.

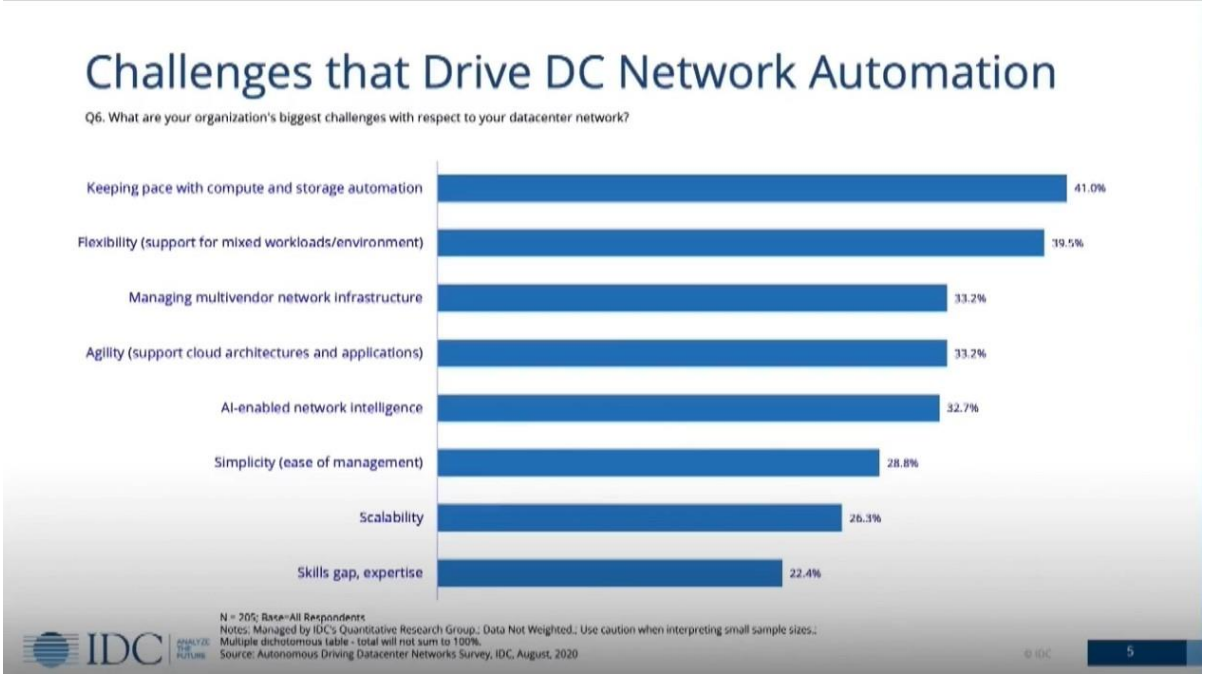


Рис. 4.2 Ключові проблеми керування мережами ЦОД, які зумовлюють перехід до SDN та автономної автоматизації

4.2 Основні виклики та проблеми модернізації існуючої інфраструктури

Компанії, які впроваджують інноваційні підходи в мережах центрів обробки даних, стикаються з низкою системних і взаємопов'язаних викликів. За результатами досліджень IDC, виконаних на основі опитувань IT-експертів, основні проблеми пов'язані не лише з технологіями як такими, а з необхідністю узгодженого розвитку всієї IT-інфраструктури.

Насамперед, на перше та друге місця виходять питання узгодження рівнів автоматизації. Мережа ЦОД повинна розвиватися синхронно з обчислювальними ресурсами та системами зберігання даних. Окрім цього, критично важливою є гнучкість мережі, тобто її здатність підтримувати змішані робочі навантаження й різні середовища — від традиційних корпоративних застосунків до хмарних сервісів, контейнерних платформ і мікросервісних архітектур.

До ключових викликів автоматизації мереж ЦОД, за даними IDC, належать:

- необхідність синхронізації автоматизації мережі з автоматизацією обчислень і сховищ;
- підтримка гібридних і мультихмарних середовищ;
- забезпечення гнучкої роботи з різнорідними робочими навантаженнями;
- скорочення часу розгортання нових сервісів без ризику порушення стабільності.

На третьому місці серед проблем перебуває багатовендорність мережевої інфраструктури. У більшості сучасних дата-центрів мережа формується з обладнання та програмних рішень різних виробників. Це створює потребу в універсальному інструменті керування, здатному об'єднати всі компоненти в єдину систему та забезпечити їх узгоджену роботу відповідно до заданого рівня автономності. Показово, що близько 90 % опитаних IDC вважають досягнення автономності мережі стратегічною ціллю своїх організацій.

Загалом дослідження IDC демонструє, що автономне керування мережею вже стало актуальним трендом. До половини компаній, які активно розвивають власну IT-інфраструктуру, так чи інакше інвестують у технології автоматизації та

автономності. Особливо яскраво цей процес проявляється на прикладі цифрової трансформації фінансового сектору.

За останні роки фінансові організації швидко перенесли значну частину своєї діяльності в цифрові канали, організувавши онлайн-продажі та дистанційні сервіси. Це дозволило компенсувати скорочення офлайн-активності, зберегти прибутковість і паралельно автоматизувати низку внутрішніх процесів. Автоматизація сприяла зменшенню кількості помилок персоналу та прискоренню бізнес-процесів, але водночас призвела до різкого ускладнення IT-інфраструктури.

Серед негативних наслідків цього процесу можна виділити такі:

- зростання кількості змін у мережевій інфраструктурі;
- підвищення складності взаємодії між сервісами;
- обмеженість ресурсів як мережі, так і команди адміністраторів;
- зростання кількості інцидентів, пов’язаних не з «залізом», а з логікою роботи мережі.

За оцінками, до 50 % складних проблем у ЦОДах прямо або опосередковано зумовлені саме цими факторами. Значну частину часу фахівці змушені витрачати на рутинні операції, тоді як навантаження, пов’язане з впровадженням нових сервісів, постійно зростає. Кожна нова імплементація потребує тестування, перевірки взаємного впливу з іншими сервісами та додаткового контролю, що збільшує ризик помилок.

Саме тому до 40 % серйозних інцидентів у ЦОДах виникають через людський фактор. Будь-які зміни — запуск нових застосунків, розгортання сервісів, зміни конфігурацій — потребують великої кількості перевірок, на які часто бракує часу. Наслідком може стати масштабна аварія.

Додатково ускладнює ситуацію час реагування на інциденти. У середньому лише виявлення проблеми займає близько 80 хвилин, і при цьому несправності часто виникають не на фізичному рівні, а на рівні протоколів, сервісної доступності чи взаємодії компонентів. У результаті служби підтримки працюють цілодобово, але все одно залишаються об’єктом постійних скарг.

У цьому контексті особливо актуальною стає класифікація рівнів автономності, запропонована IDC. Відповідно до неї, мережа повинна демонструвати певний набір можливостей на кожному рівні. Рішення Huawei Autonomous Driving Network (ADN) уже відповідає вимогам третього рівня автономності, забезпечуючи автоматичну підтримку роботи мережі, включно з запуском і зупинкою процесів, налаштуванням обладнання та постійним збором телеметрії в реальному часі.

У частково автоматичному режимі ADN здатна:

- аналізувати події в мережі;
- визначати першопричини інцидентів;
- формувати рекомендації щодо їх усунення;
- надавати оператору готові сценарії дій.

Подальший розвиток платформи передбачає впровадження механізмів зворотного зв’язку та самонавчання. Згідно з дорожньою картою, до 2028 року Huawei планує досягти п’ятого рівня автономності, тобто повністю самокерованої мережі.

Ефект від впровадження автономного керування проявляється вже на етапі проєктування мережі. Замовнику достатньо задати базові параметри — кількість пристроїв і пропускну здатність каналів, після чого система автоматично формує готову мережеву фабрику ЦОД. Надалі автономна мережа аналізує навантаження, оптимізує інформаційні потоки та в режимі реального часу усуває вузькі місця.

Таким чином, Huawei Autonomous Driving Network є логічним розвитком ідей SDN. Вона усуває ключові обмеження програмно-визначених мереж, зменшує залежність від людського фактора та дозволяє зосередити зусилля IT-персоналу на стратегічних, а не рутинних завданнях.

ВИСНОВКИ

У кваліфікаційній роботі було виконано комплексний аналіз підходів до маршрутизації в програмно-конфігурованих мережах (SDN) та напрямів їх подальшого вдосконалення з урахуванням сучасних вимог до масштабованості, гнучкості, відмовостійкості й автоматизації мережевої інфраструктури. Актуальність дослідження зумовлена стрімким зростанням обсягів трафіка, поширенням хмарних сервісів, віртуалізації, розподілених обчислень і необхідністю швидкої адаптації мереж до змін бізнес-процесів.

У роботі було розглянуто еволюцію мережевих підходів від традиційних статичних архітектур до SDN, де ключовою ідеєю є відокремлення площини керування від площини передачі даних та централізація прийняття рішень. Показано, що SDN створює передумови для програмної оптимізації маршрутів, впровадження політик QoS, автоматичного реагування на деградацію каналів і тісної інтеграції мережі з прикладними сервісами та системами оркестрації.

Значну увагу приділено аналізу децентралізованих алгоритмів маршрутизації та поширення повідомлень, зокрема Chord, Kademlia та CAN, які можуть бути використані як логічна основа для побудови оверлейних механізмів усередині SDN-мереж. Проведено їх порівняння за такими критеріями, як складність реалізації, детермінованість маршрутів, стійкість до churn, захищеність від атак типу «відмова в обслуговуванні», вимоги до пам’яті та адаптивність. Показано, що не існує універсального алгоритму, оптимального для всіх сценаріїв, а вибір рішення має залежати від характеру навантаження, динаміки мережі та вимог до надійності.

У роботі також проаналізовано механізми широкомовної розсилки в децентралізованих середовищах і показано, що ця задача є значно складнішою за адресну маршрутизацію. Розглянуті підходи Chord, Kademlia та CAN демонструють різні компроміси між швидкістю поширення, кількістю дублювань і складністю реалізації, що є важливим при проєктуванні SDN-рішень для розподілених сервісів, зокрема блокчейн-платформ і P2P-систем.

Окремим напрямом дослідження стало вдосконалення маршрутизації в глобальних і корпоративних мережах на основі SD-WAN. На прикладі рішень класу NetScaler SD-WAN показано, як SDN-підхід дозволяє реалізувати динамічний вибір маршрутів на основі затримок, джитеру та втрат пакетів, забезпечити швидке відновлення після аварій, пріоритизацію трафіка, пакетну реплікацію для бізнес-критичних сервісів і ефективне використання як дорогих MPLS-каналів, так і публічного Інтернету. Це безпосередньо демонструє практичну цінність програмно-керованої маршрутизації.

Важливим результатом роботи є узагальнення сучасних тенденцій розвитку SDN у напрямі intent-based networking та автономних мереж. На основі моделі IDC проаналізовано рівні автономності мереж — від повністю ручного керування до самокерованих систем із використанням штучного інтелекту. Показано, що автономні мережі, зокрема підходи на кшталт Huawei Autonomous Driving Network, є логічним продовженням SDN і спрямовані на зменшення впливу людського фактора, скорочення часу виявлення та усунення несправностей і підвищення загальної надійності ЦОД.

Отже, результати дослідження підтверджують, що SDN є не окремою технологією, а універсальною парадигмою побудови сучасних мереж, у межах якої можливе поєднання централізованого керування з децентралізованими алгоритмами маршрутизації та автоматизованими механізмами адаптації. Вдосконалення систем маршрутизації в SDN-мережах має відбуватися з урахуванням як теоретичних моделей, так і практичних сценаріїв експлуатації, що відкриває широкі перспективи для подальших досліджень і впроваджень у галузі телекомунікацій та інформаційних технологій.

ПЕРЕЛІК ПОСИЛАНЬ

1. Беркман Л. Н. Програмно-конфігуровані мережі: принципи побудови та керування // Зв’язок. – 2015. – № 4. – С. 12–18.
2. Кільменінов О. А., Лещенко О. О., Похабова І. Е. Програмно-конфігуровані мережі: методи побудови та керування : навч. посіб. – Київ : Державний університет телекомунікацій, 2018. – 146 с.
3. Програмно-конфігуровані мережі SDN : навчально-методичні матеріали. – Київ : ДУІКТ, 2020. – 98 с.
4. Коломоєць М. С. Аналіз функціонування програмно-конфігурованої мережі на базі протоколу OpenFlow // Інформаційні технології та комп’ютерна інженерія. – 2024. – № 1. – С. 45–52.
5. Дуравкін Ю. В. Моделювання програмно-конфігурованих мереж на основі теорії мережевого обчислення // Системи управління, навігації та зв’язку. – 2017. – № 3. – С. 76–82.
6. Митник О. М. Дослідження ефективності балансування трафіку в програмно-конфігурованих мережах SDN : кваліфікаційна робота. – Тернопіль : ТНТУ, 2019. – 82 с.
7. Бешлей М. І. Методи побудови інтенційно-орієнтованих мереж передачі даних : автореф. дис. … д-ра техн. наук. – Львів : НУ «Львівська політехніка», 2021. – 36 с.
8. Прислупський А. І. Програмно-конфігуровані телекомунікаційні мережі : дис. … канд. техн. наук. – Львів : НУ «Львівська політехніка», 2020. – 184 с.
9. SDN та OpenFlow : сучасні підходи до керування мережами // Вісник НТУУ «КПІ». – 2021. – № 2. – С. 33–41.
10. Архітектура SDN у мережах дата-центрів : навчальний курс. – Харків : ХНУРЕ, 2022. – 112 с.
11. Kreutz D., Ramos F. M. V., Verissimo P., Rothenberg C. E., Azodolmolky S., Uhlig S. Software-Defined Networking: A Comprehensive Survey // Proceedings of the IEEE. – 2015. – Vol. 103, No. 1. – P. 14–76.

12. Feamster N., Rexford J., Zegura E. The Road to SDN: An Intellectual History of Programmable Networks // ACM SIGCOMM Computer Communication Review. – 2014. – Vol. 44, No. 2. – P. 87–98.
13. Open Networking Foundation. OpenFlow Switch Specification. Version 1.5.1. – ONF, 2015. – 178 p.
14. IETF. RFC 6241: Network Configuration Protocol (NETCONF). – 2011.
15. IETF. RFC 7047: The Open vSwitch Database Management Protocol (OVSDB). – 2013.
16. IETF. RFC 8040: RESTCONF Protocol. – 2017.
17. IETF. RFC 7348: Virtual eXtensible Local Area Network (VXLAN). – 2014.
18. Stoica I., Morris R., Karger D., Kaashoek M., Balakrishnan H. Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications // ACM SIGCOMM. – 2001. – P. 149–160.
19. Maymounkov P., Mazières D. Kademlia: A Peer-to-Peer Information System Based on the XOR Metric // Lecture Notes in Computer Science. – 2002. – Vol. 2429. – P. 53–65.
20. Ratnasamy S., Francis P., Handley M., Karp R., Shenker S. A Scalable Content-Addressable Network // ACM SIGCOMM. – 2001. – P. 161–172.
21. OpenDaylight Project. OpenDaylight Controller Documentation. – 2024.
22. Cisco Systems. Application Centric Infrastructure (ACI) Design Guide. – Cisco Press, 2024.
23. IETF. OpFlex Control Protocol (Internet-Draft). – 2015.
24. MEF Forum. MEF 70.1: SD-WAN Service Attributes and Framework. – 2021.
25. Huawei, IDC. Autonomous Driving Network: White Paper. – 2020.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ

КВАЛІФІКАЦІЙНА РОБОТА

АНАЛІЗ ТА ВДОСКОНАЛЕННЯ СИСТЕМ МАРШРУТИЗАЦІЇ В ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖАХ (SDN)»

Виконав:
студент групи ТСДМ-61
Ернест РОМАНОВСЬКИЙ

МЕТА РОБОТИ ТА АКТУАЛЬНІСТЬ

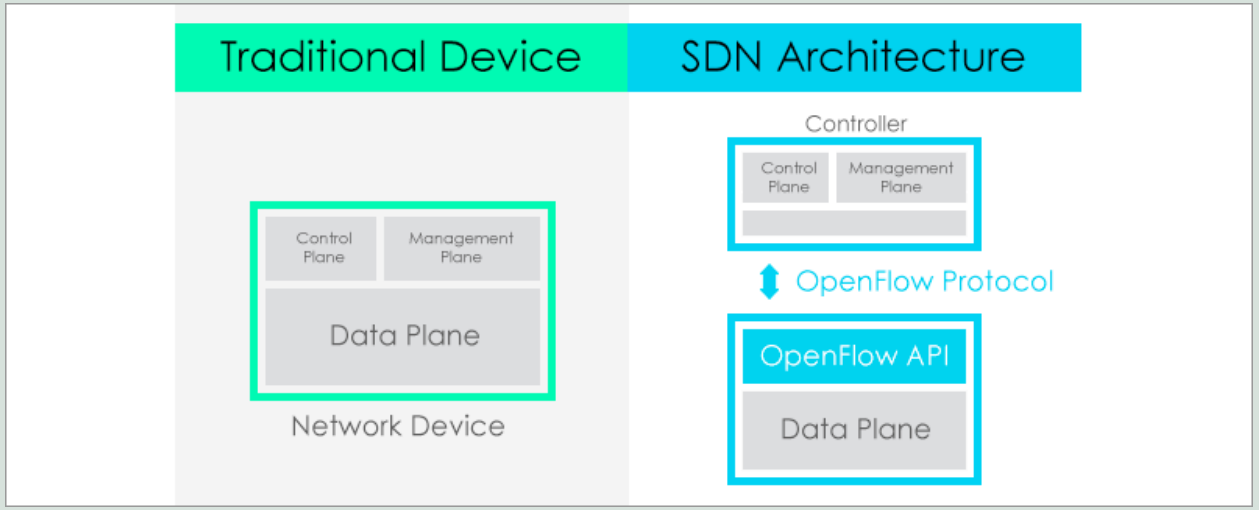
- Мета роботи – проаналізувати сучасні підходи до побудови програмно-конфігурованих мереж (SDN) та технології SD-WAN, визначити їхні переваги й обмеження порівняно з традиційними мережевими рішеннями.
- Об’єкт дослідження – корпоративні та глобальні комп’ютерні мережі передачі даних, побудовані з використанням програмно-конфігурованих мережевих технологій.
- Предмет дослідження – архітектурні принципи, методи маршрутизації та механізми централізованого управління трафіком у мережах SDN і SD-WAN, а також особливості їх реалізації у сучасних мережевих рішеннях.

Актуальність.

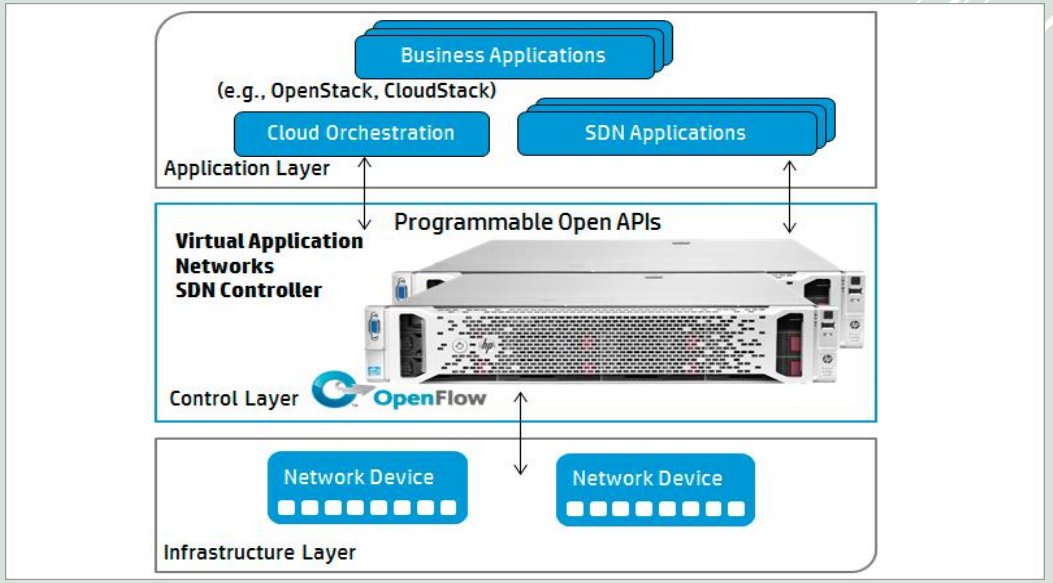
- Стрімкий розвиток хмарних сервісів, віртуалізації та розподілених корпоративних інфраструктур зумовлює зростання вимог до гнучкості, масштабованості та керованості комп’ютерних мереж. Традиційні WAN-рішення характеризуються складністю адміністрування, високою вартістю та обмеженою адаптивністю. У цих умовах програмно-конфігуровані мережі (SDN) і технологія SD-WAN забезпечують централізоване управління, автоматизацію маршрутизації та ефективне використання мережевих ресурсів. Для України актуальність теми посилюється потребою модернізації цифрової інфраструктури, підвищення її стійкості та економічної ефективності.

РОЗВИТОК SDN

- Програмно-визначені мережі (SDN) виникли як відповідь на зростання вимог до гнучкості, масштабованості та автоматизації мережевої інфраструктури. Основна ідея SDN полягає у відокремленні площини керування від площини передавання даних, що дозволяє централізовано програмувати мережу, зменшити залежність від конкретного вендора та ефективніше використовувати ресурси.
- Компанія HP зробила ставку на відкриті стандарти, насамперед OpenFlow, розробивши SDN-контролер і відкриту екосистему застосунків, що забезпечує еволюційний перехід до SDN. Cisco, у свою чергу, запропонувала пропрієтарну архітектуру ACI, орієнтовану на прикладні політики та глибоку інтеграцію апаратного й програмного рівнів.
- Попри різні підходи вендорів, загальною тенденцією є перехід від жорстко прив'язаних до обладнання мереж до програмного, політико-орієнтованого керування.



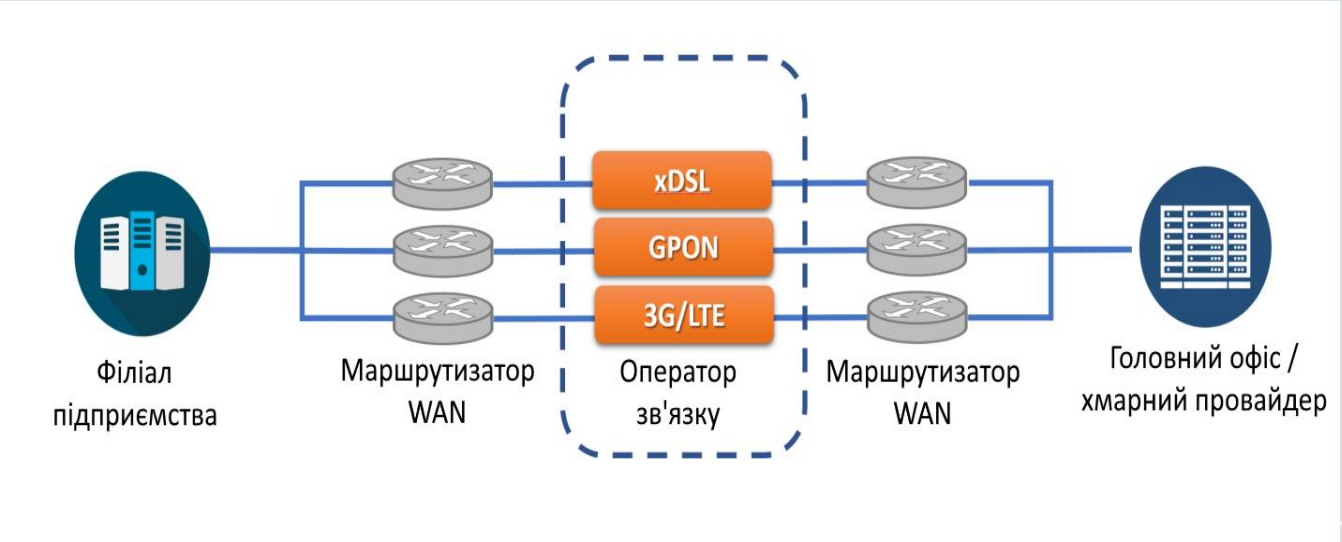
У SDN вся логіка управління мережевими пристроями виноситься в так звану "площину управління", яка реалізується програмним чином. Конструктивно контролери можуть будуватися або з урахуванням фізичних, або віртуальних хостів. Управління мережевими пристроями, зазвичай, здійснюється за протоколом OpenFlow



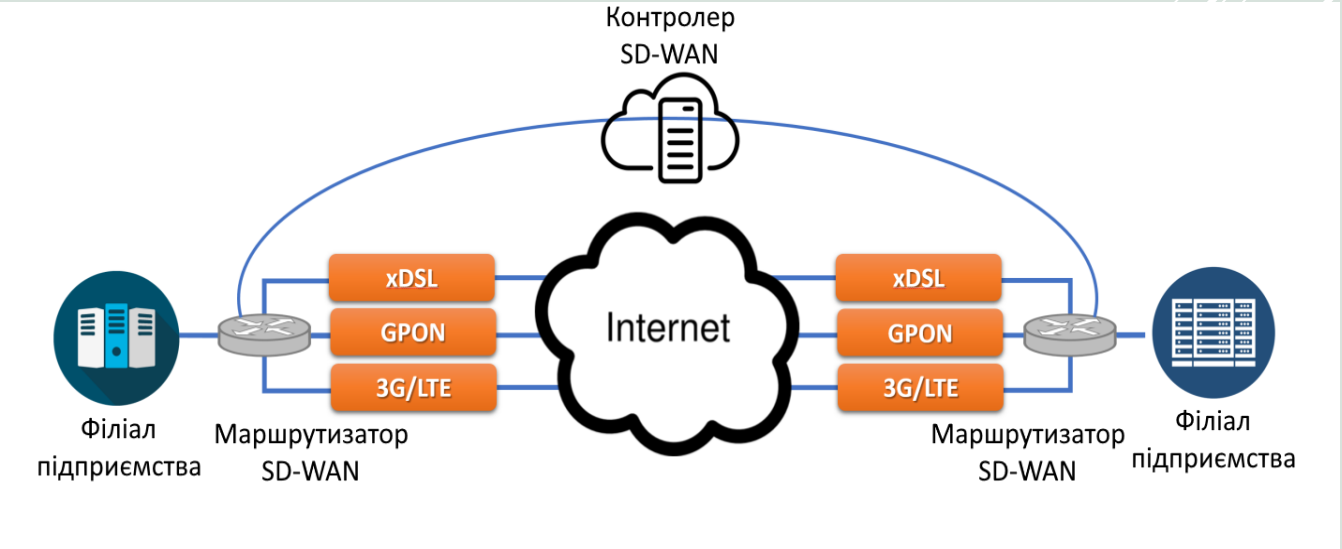
HP Virtual Application Networks SDN Controller

РОЛЬ SD-WAN

- Традиційні WAN-мережі не відповідають сучасним вимогам бізнесу через високу вартість, статичну маршрутизацію та складність масштабування.
- Технологія SDN, а зокрема її розвиток у вигляді SD-WAN, пропонує принципово інший підхід до побудови корпоративних WAN. Вона забезпечує централізоване програмне керування, динамічний вибір маршрутів, гнучке використання різних типів каналів (MPLS, Інтернет, мобільні мережі) та автоматичне реагування на деградацію з'єднань.
- SD-WAN дозволяє підвищити відмовостійкість, знизити витрати на інфраструктуру, спростити підключення філій і забезпечити стабільну роботу критичних сервісів (VoIP, VDI, відеоконференції). У результаті корпоративна WAN перетворюється на гнучку, масштабовану й економічно ефективну мережу, адаптовану до сучасних бізнес-вимог.



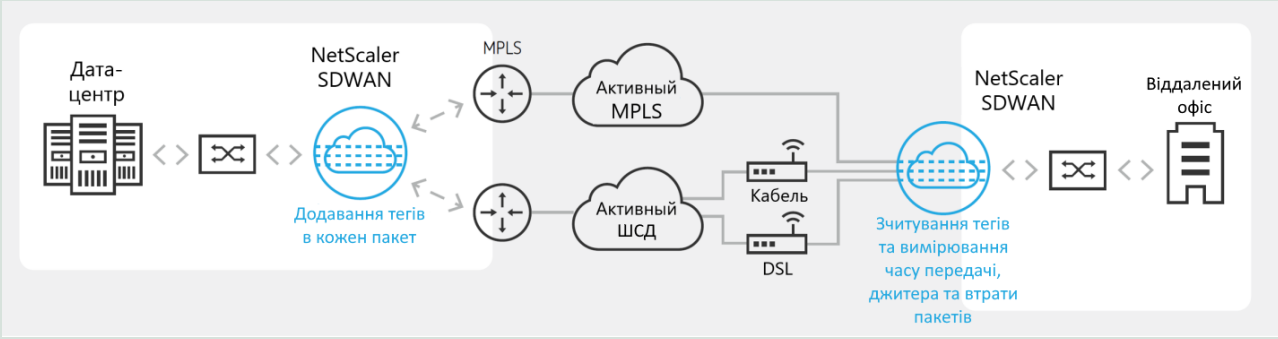
Традиційна архітектура WAN



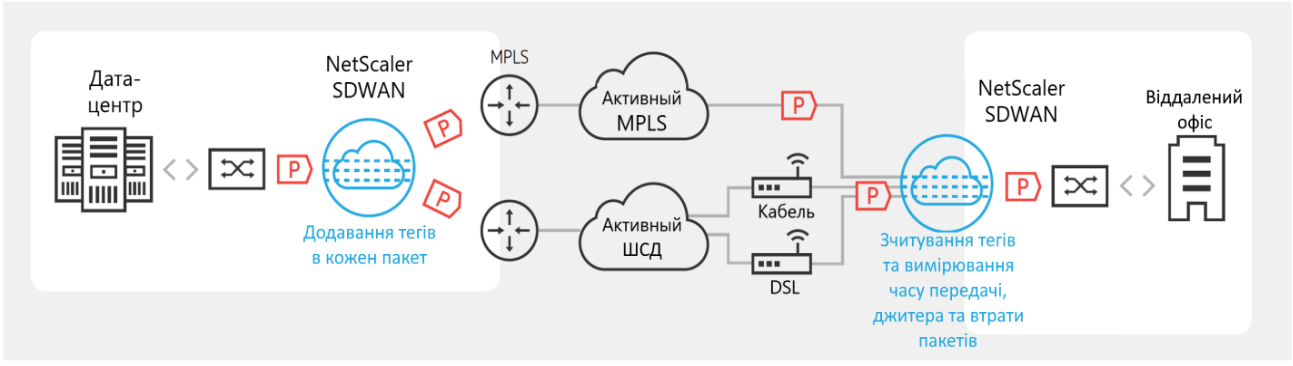
Архітектура SD-WAN

ВДОСКОНАЛЕННЯ МАРШРУТИЗАЦІЇ

- NetScaler SD-WAN постійно моніторить параметри якості мережі (затримку, джитер, втрати пакетів) і в реальному часі динамічно обирає оптимальні WAN-маршрути для різних типів трафіку. Система автоматично розпізнає тисячі додатків і застосовує до них відповідні політики маршрутизації та QoS, формуючи додатко-орієнтовану мережу.
- Рішення підтримує використання кількох каналів (MPLS, Інтернет, бездротові), швидке безшовне відновлення після аварій, пріоритезацію трафіку та дублювання пакетів для бізнес-критичних сервісів. Це забезпечує високу відмовостійкість, стабільну роботу VoIP, відео та VDI без розривів сесій.
- NetScaler SD-WAN є економічною альтернативою традиційним WAN і DCI, дозволяючи ефективно використовувати недорогі інтернет-канали. Додаткові механізми (traffic shaping, packet reordering, DPI, firewall, компресія та кешування) підвищують продуктивність, безпеку й спрощують адміністрування корпоративної WAN-інфраструктури.

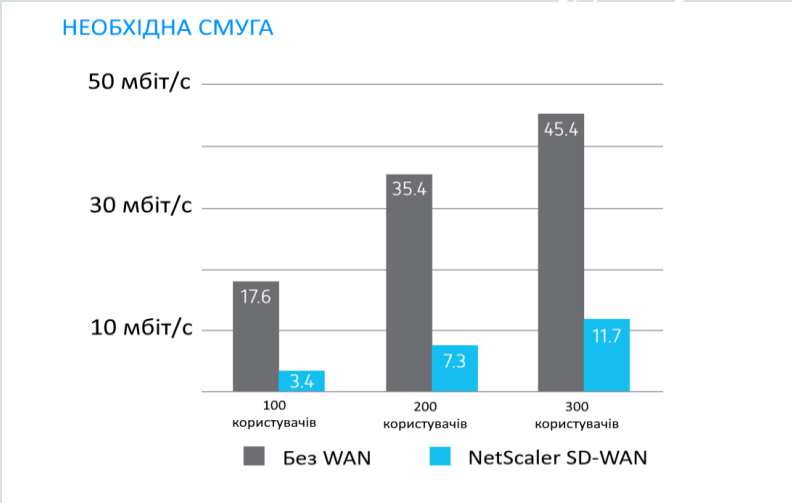


Додавання тегів у трафік WAN для створення карти маршрутів у NetScaler SD-WAN



Дублювання пакетів у NetScaler SDWAN

Зниження необхідної смуги між офісом та дата-центром з NetScaler SD-WAN



ОДНОРАНГОВІ МЕРЕЖІ В SDN

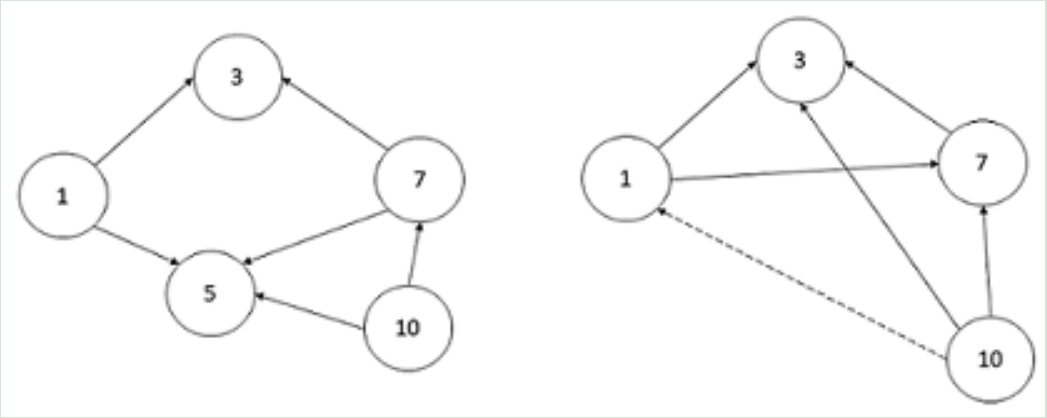
Параметри мережі

Ідентифікатор вузла	IP-адреса
1	10.10.3.1
2	63.63.12.1
3	100.1.1.1
4	71.44.18.99
5	44.10.0.1
6	152.1.35.1

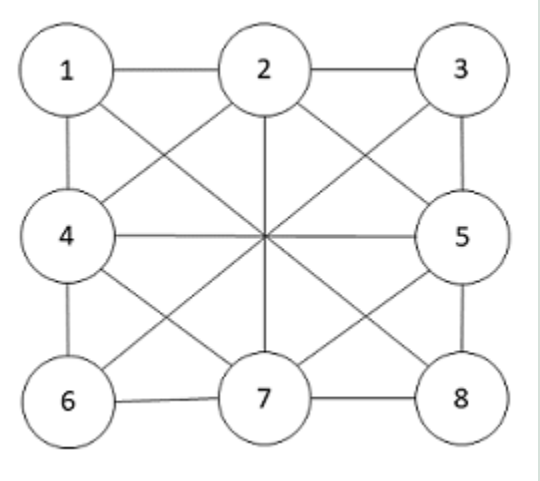
- Однорангові мережі (P2P) широко застосовуються в сучасних розподілених системах завдяки відмовостійкості, масштабованості та відсутності централізованого керування. Вони використовуються у файлообмінних сервісах, блокчейн-платформах і розподілених обчисленнях, але ускладнюють задачі маршрутизації та керування трафіком.
- Інтеграція P2P-мереж із програмно-визначеними мережами (SDN) дозволяє реалізувати гнучке керування потоками даних і політиками маршрутизації. У межах SDN вузли утворюють оверлейну мережу з унікальними ідентифікаторами, що відповідають IP-адресам, забезпечуючи ефективну адресну та широкомовну доставку повідомлень.

РІШЕННЯ ТА СТВОРЕННЯ ТОПОЛОГІЇ

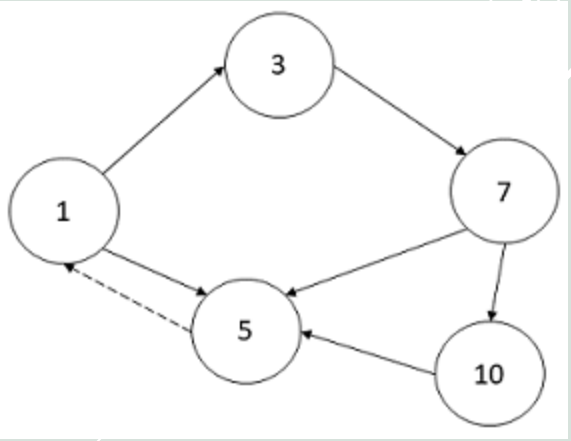
- Найпростіший варіант — пряме з’єднання кожного вузла з усіма іншими, але для великих мереж він непридатний через квадратичне зростання кількості з’єднань: $C = N(N-1)/2$. Тому мережу потрібно впорядковувати, формуючи топологію з обмеженою кількістю сусідів для кожного вузла. Однак виникають проблеми вибору оптимального числа сусідів ССС та перебудови зв’язків при додаванні/виході вузлів, що може погіршувати маршрути й баланс навантаження.
- Ще складнішою є широкомовна розсилка: лавиноподібне пересилання спричиняє цикли та дублювання повідомлень. Використання унікальних ідентифікаторів або списків відвіданих вузлів зменшує дублювання, але потребує додаткової пам’яті й обчислень та погано масштабується; до того ж змінність повідомлення унеможливлює цифровий підпис. Підхід «розсилка за запитом» знижує накладні витрати, але має складний протокол і меншу швидкість поширення.



Мережа з С = 3. У разі зникнення вузла 5 вузол 10 підключається до найближчого вузла 3, хоча доцільніше було б підключитися до вузла 1



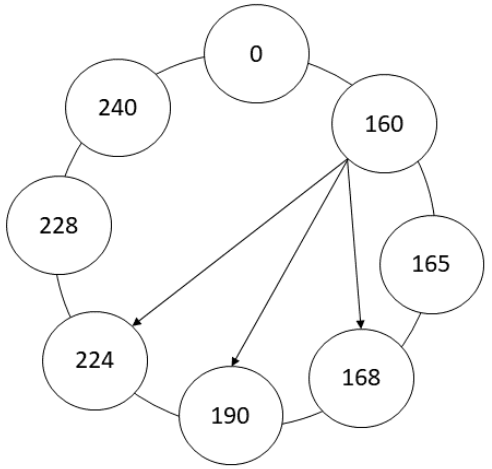
Кожен вузол здійснює підключення до всіх вузлів у мережі



Виникнення замкнутого контуру

CHORD

- Повнозв’язна топологія з прямим з’єднанням усіх вузлів є простою, але непридатною для масштабованих мереж через квадратичне зростання кількості з’єднань. Тому застосовуються впорядковані топології з обмеженою кількістю сусідів, однак їх перебудова в динамічних мережах є складною і може призводити до неоптимальної маршрутизації.
- Особливою проблемою є широкомовна розсилка, оскільки лавиноподібне поширення повідомлень викликає цикли та дублювання даних. Прості механізми їх усунення мають значні накладні витрати. Для вирішення цих проблем використовуються структуровані алгоритми, зокрема Chord, у якому кільцева топологія та таблиці вказівників забезпечують маршрутизацію і широкомовну розсилку за log(N) кроків.



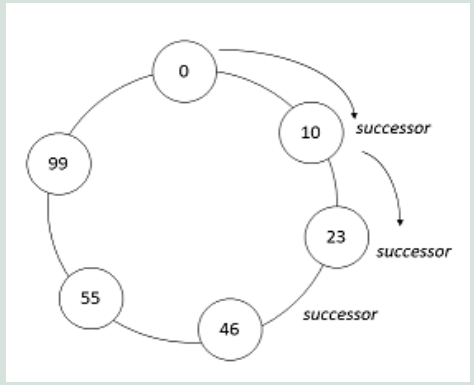
m — Кількість біт в ідентифікаторі
n — Номер вузла

$$i^{th} = successor(n + 2^i) \ mod \ 2^m, \ i = 1 \ldots m$$

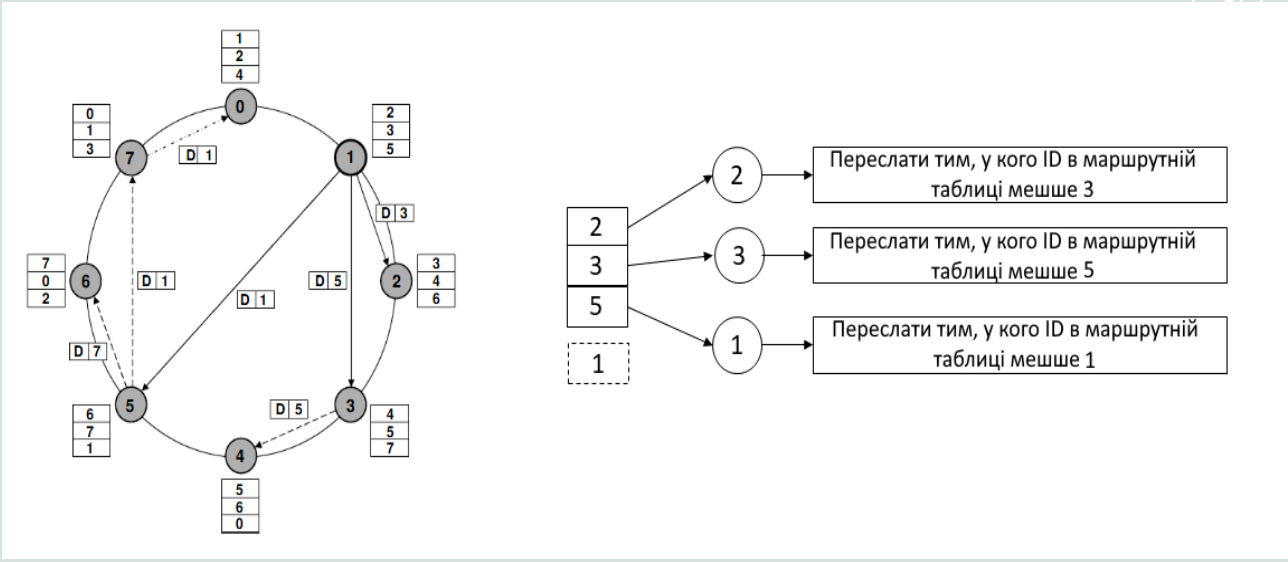
m = 8, n = 160

Комірка	Вирахувано	Фактично
0	160	160
1	162	165
2	164	165
3	168	168
4	176	190
5	192	224
6	224	224
7	32	160

Таблиця вказівників у Chord для вузла з номером 160



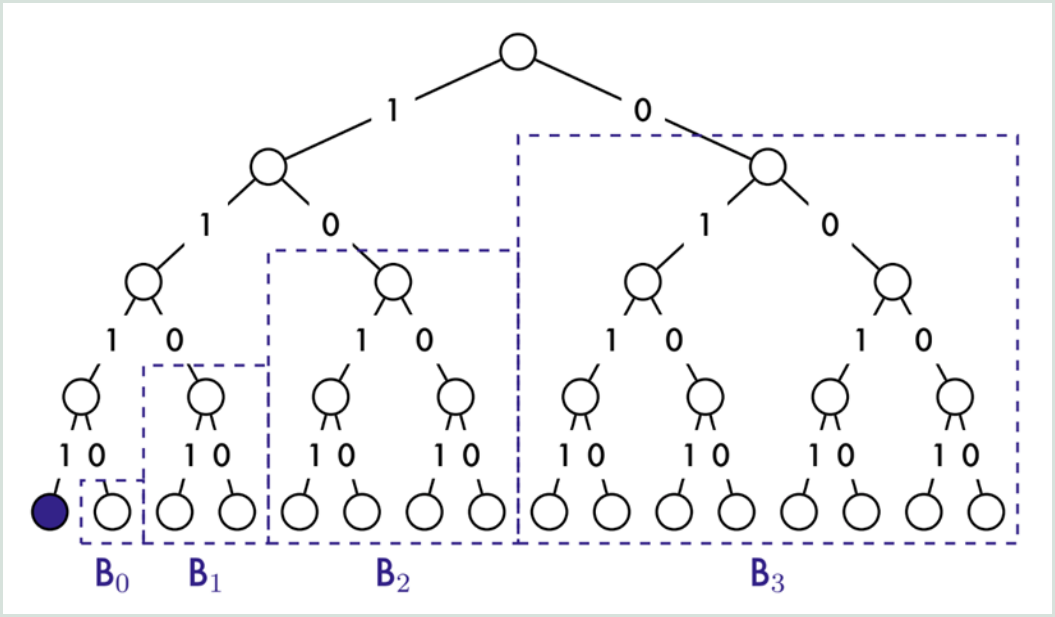
Кільцева топологія Chord



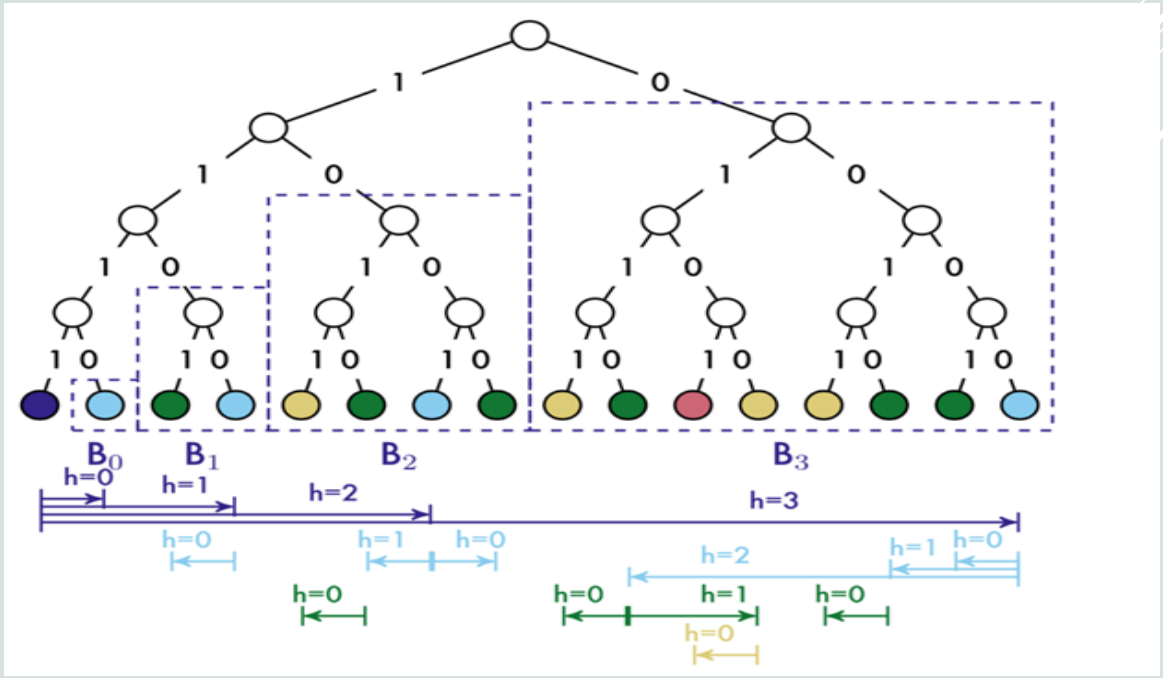
Широкомовне розсилання в Chord

KADEMLIA

- **Kademlia** — алгоритм маршрутизації з деревоподібною логічною топологією, у якому відстань між вузлами визначається за XOR-метрикою їх ідентифікаторів. Простір ключів поділяється на бакети з діапазонами відстаней, що формують ієрархічну структуру. Кожен вузол підтримує з'єднання з вузлами з різних бакетів.
- Маршрутизація здійснюється ітеративно: на кожному кроці повідомлення передається вузлу, який є ближчим до адресата за XOR-відстанню, що забезпечує середню довжину маршруту порядку log(N). Широкомовна розсилка реалізується шляхом передавання повідомлень вузлам з різних бакетів із використанням параметра «висота», який обмежує глибину поширення та запобігає надмірному дублюванню.



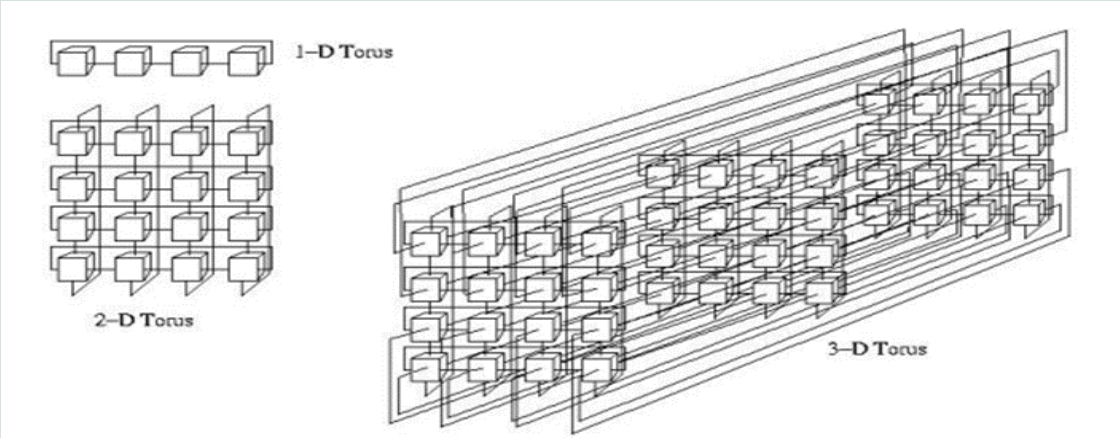
Дерево ключів Kademlia



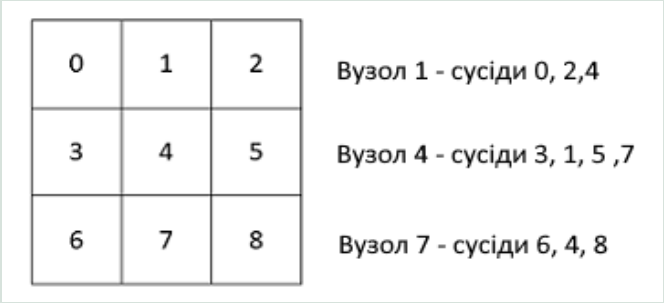
Широкомовне розсилання Kademlia

CAN

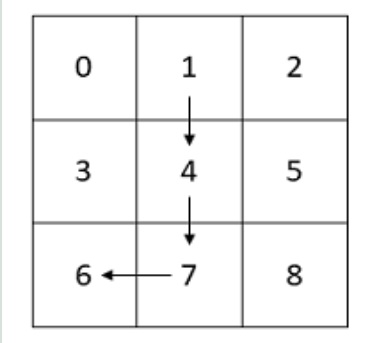
- **Content-Addressable Network (CAN)** — алгоритм маршрутизації, у якому мережа організовується у вигляді віртуального d-вимірного координатного простору, згорнутого в тор. Кожен вузол відповідає за окрему зону цього простору та підтримує зв’язок із вузлами суміжних зон. Ідентифікатори вузлів відображаються у координати за допомогою хешування або поділу бітового ідентифікатора на d сегментів.
- Маршрутизація здійснюється алгоритмом шляхом вибору сусідньої зони, найближчої до цільових координат, що забезпечує середню складність N^(1/d), де N — кількість вузлів у мережі, а d — розмірність координатного простору. Під час додавання або видалення вузлів відбувається локальний поділ або об’єднання зон, що мінімізує перебудову мережі та забезпечує масштабованість і відмовостійкість CAN.



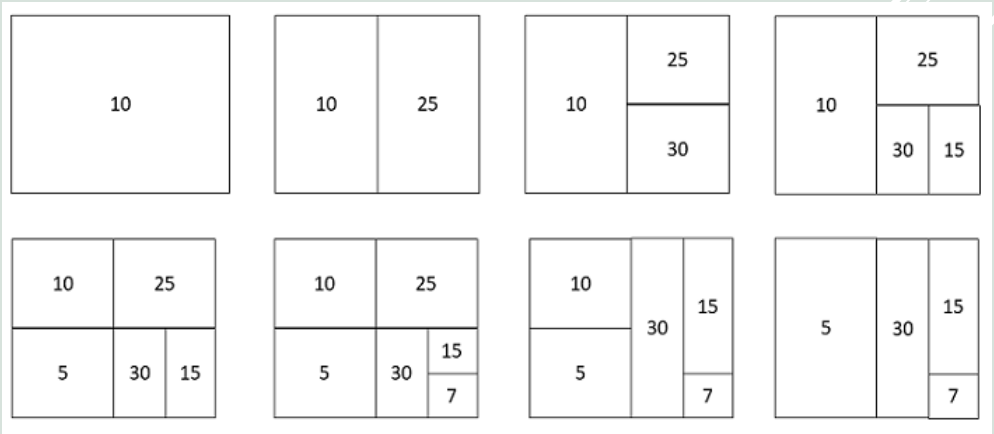
Перетин двовимірного та тривимірного тора



Двовимірна координатна площина



Маршрутизація в мережі CAN



Реконфігурація зон при додаванні/видаленні нових вузлів

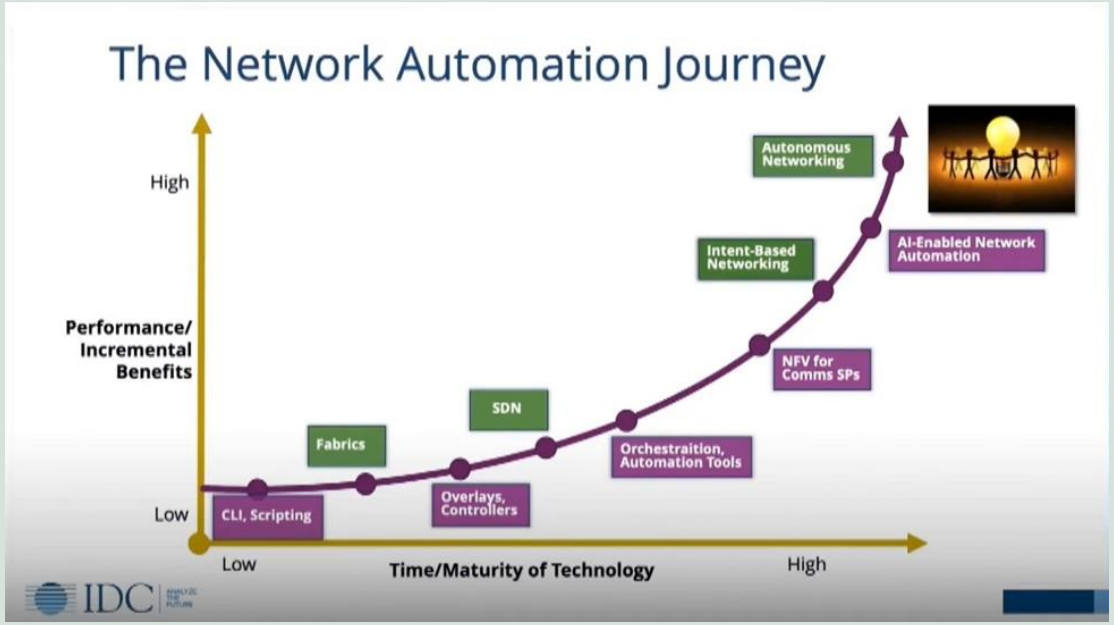
ПОРІВНЯЛЬНИЙ АНАЛІЗ

Критерій	Chord	Kademlia	CAN
Складність реалізації	Низька	Середня	Висока
Детермінованість маршруту	Висока	Низька	Середня
Стійкість до churn	Низька	Висока	Середня
Стійкість до атак типу «відмова в обслуговуванні»	Низька	Висока	Середня
Обсяг пам'яті	Низький	Високий	Середній
Адаптивність	Низька	Середня	Висока

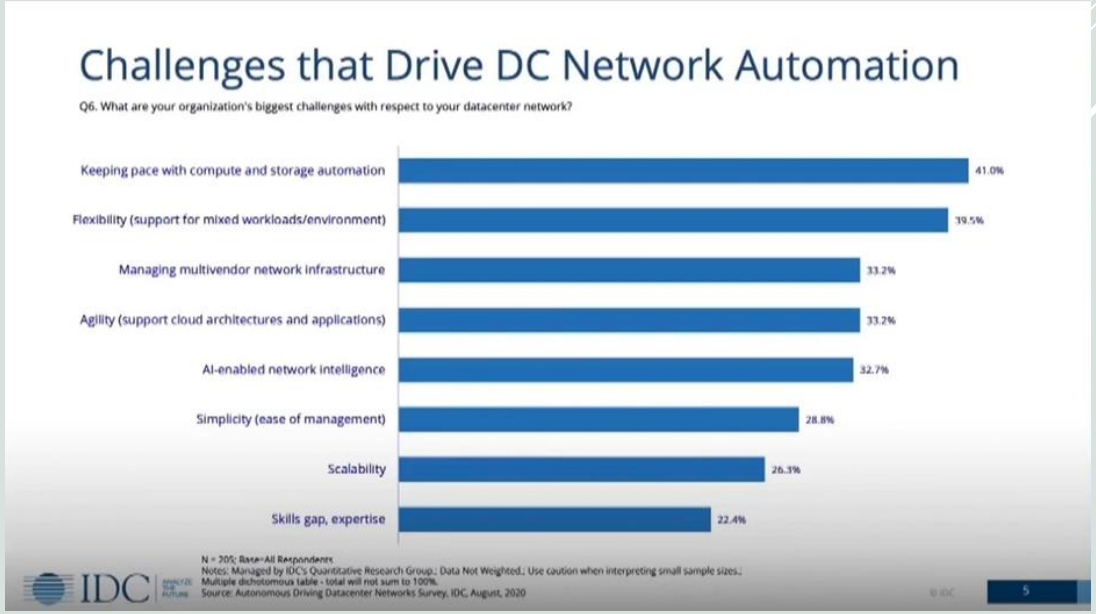
- Єдиного універсального підходу до проєктування децентралізованих систем не існує, оскільки різні алгоритми демонструють різну ефективність залежно від умов експлуатації, типу навантажень і динаміки мережі. У роботі виконано якісне порівняння алгоритмів Chord, Kademlia та CAN з метою визначення їхніх переваг, недоліків і доцільних сценаріїв застосування.
- Порівняльний аналіз показує, що Chord є простим у реалізації та детермінованим, але має низьку адаптивність і стійкість до churn та атак. Kademlia характеризується високою стійкістю, відмовостійкістю та гнучкістю, проте потребує більших ресурсів пам'яті й має недетерміновані маршрути. CAN є найбільш гнучким і масштабованим алгоритмом, але складним у реалізації та з помірною стійкістю до динамічних змін.
- Наведені критерії дозволяють обґрунтовано обирати алгоритм маршрутизації відповідно до вимог масштабованості, надійності та керованості децентралізованих мереж.

МЕРЕЖА ADN ЯК АЛЬТЕРНАТИВА SDN

- **Автономно керована мережа** є наступним етапом розвитку SDN і відрізняється здатністю самостійно аналізувати стан мережі, приймати рішення та виконувати дії без постійного втручання адміністратора. На відміну від традиційного SDN, яке працює за заздалегідь визначеними політиками, автономні мережі поєднують централізоване керування з аналітикою, автоматизацією та елементами штучного інтелекту.
- За моделлю IDC автономність мережі розглядається як багаторівнева характеристика — від повністю ручного керування до повністю самокерованих систем. Розвиток автономних мереж зумовлений цифровізацією, ускладненням IT-інфраструктур і дефіцитом фахівців, а самі автономні мережі розглядаються як логічне продовження SDN та основа майбутніх мереж центрів обробки даних.



Шлях розвитку автоматизації мережевої інфраструктури: від CLI та SDN до intent-based та автономних мереж



Ключові проблеми керування мережами ЦОД, які зумовлюють перехід до SDN та автономної автоматизації

ВИСНОВКИ

- У кваліфікаційній роботі виконано комплексний аналіз підходів до маршрутизації в програмно-конфігурованих мережах (SDN) з урахуванням вимог до масштабованості, гнучкості, відмовостійкості та автоматизації.
- Розглянуто еволюцію мереж від традиційних архітектур до SDN, обґрунтовано переваги централізованого керування та програмної оптимізації маршрутів.
- Проаналізовано децентралізовані алгоритми Chord, Kademlia та CAN, проведено їх порівняння за ключовими характеристиками та показано доцільність вибору алгоритмів залежно від сценарію застосування.
- Окрему увагу приділено технології SD-WAN на прикладі NetScaler SD-WAN, що демонструє практичну ефективність SDN-підходу в глобальних і корпоративних мережах.
- Узагальнено сучасні тенденції розвитку SDN у напрямі автономних та intent-based мереж.

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: Ернест РОМАНОВСЬКИЙ

Назва: АНАЛІЗ ТА ВДОСКОНАЛЕННЯ СИСТЕМ МАРШРУТИЗАЦІЇ В ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖАХ (SDN)

Координатор: Віталій ТЮРІН

Підрозділ: ННІТ

Коефіцієнт подібності 1:1.2

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*