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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «ОПТИМІЗАЦІЯ ПРОЦЕСІВ АВТОМАТИЗАЦІЇ У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ»

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

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

_____ Ілля БУЛАВІН
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Виконав: здобувач вищої освіти гр. ТСДМ-61
Ілля БУЛАВІН
Ім'я, ПРІЗВИЩЕ

Керівник: В'ячеслав ТРЕЙТЯК
к.т.н. *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

Булавіну Іллі Олександровичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Оптимізація процесів автоматизації у телекомунікаційних мережах
керівник кваліфікаційної роботи В'ячеслав ТРЕЙТЯК, к.т.н.
(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. Автоматизація у телекомунікаційних мережах.
2. Технології віртуалізації в автоматизованих мережах.
3. Hewlett packard enterprise server automation.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Планування мережі.
2. Технології віртуалізації в автоматизованих мережах.
3. Дизайн автоматизованої мережі.
4. Автоматизація роботи з серверами за допомогою Hewlett packard enterprise server automation.

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	22.10.2025	Викон.
3	Розробка другого розділу	02.11.2025	Викон.
4	Розробка третього розділу	12.11.2025	Викон.
5	Розробка четвертого розділу	22.11.2025	Викон.
6	Висновки, вступ, реферат	02.12.2025	Викон.
7	Розробка презентації	12.12.2025	Викон.

Здобувач вищої освіти _____ Ілля БУЛАВІН
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ В'ячеслав ТРЕЙТЯК
(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 Булавін І.О. 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: «Оптимізація процесів автоматизації у телекомунікаційних мережах»

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач Булавін Ілля Олександрович 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 Булавіна Іллі Олександровича на оцінку «відмінно» та присвоїти йому кваліфікацію магістр з електронних комунікацій та радіотехніки.

Керівник кваліфікаційної роботи _____ В'ячеслав ТРЕЙТЯК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Булавін І.О. 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 Булавіна Іллі Олександровича
(прізвище, ім'я, по батькові)
на тему «Оптимізація процесів автоматизації у телекомунікаційних мережах»

Актуальність.
У сучасних телекомунікаційних системах постійно зростають обсяги трафіку, кількість мережевих пристроїв та складність архітектури. Це вимагає переходу від ручного керування до повної автоматизації процесів конфігурації, моніторингу та самовідновлення мереж. Запропонована в роботі тематика є актуальною, оскільки відповідає світовим тенденціям розвитку SDN (Software Defined Networking), NFV (Network Function Virtualization), CI/CD-процесів та вендор-незалежних моделей управління мережею. Розробка комплексних методів автоматизації дозволяє зменшити людський фактор, підвищити надійність сервісів і забезпечити масштабованість телекомунікаційних інфраструктур, що є критично важливим для операторів зв'язку та корпоративних дата-центрів.
Позитивні сторони.
1. У роботі досліджено автоматизацію роботи з серверами за допомогою HPE Server Automation, що дозволяє централізовано керувати апаратними та програмними ресурсами, підвищуючи ефективність обслуговування серверної інфраструктури.
2. У роботі досліджено технологій віртуалізації, такі як GRE, IP-in-IP, MPLS, MPLS L2/L3VPN, VXLAN, GENEVE, MPLSoverUDP та MPLSoverGRE.
Недоліки.
1. У роботі було б доцільно провести порівняння між різними рішеннями (наприклад, VXLAN vs GENEVE, Ansible vs Nornir, SNMP vs NETCONF) для обґрунтування вибору конкретних підходів.
2. У роботі було б доцільно показати реальний сценарій автоматизації.

Відзначені зауваження не впливають на загальну позитивну оцінку магістерської кваліфікаційної роботи

Висновок: *кваліфікаційна робота на здобуття ступеня магістра заслуговує оцінку "відмінно", а здобувач Булавін Ілля Олександрович 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: 72 стор., 21 рис., 23 джерела.

Мета роботи – підвищення ефективності управління телекомунікаційними мережами шляхом впровадження методів автоматизації процесів конфігурації, моніторингу та самовідновлення сервісів на основі сучасних технологій віртуалізації, стандартизованих протоколів управління та концепцій CI/CD.

Об’єкт дослідження – телекомунікаційна мережа як складна розподілена система, що включає фізичну (underlay) та віртуальну (overlay) інфраструктури, а також системи керування, моніторингу та забезпечення надійності її функціонування.

Предмет дослідження – методи та засоби автоматизації управління телекомунікаційними мережами.

Короткий зміст роботи: у кваліфікаційній роботі проведено комплексне дослідження методів і засобів автоматизації управління сучасними телекомунікаційними мережами. Розглянуто підходи до оптимізації процесів конфігурації, моніторингу, самовідновлення сервісів та централізованого управління мережевими ресурсами. Встановлено, що впровадження систем IPAM, опису мережевих сервісів і вендор-агностичних моделей забезпечує узгодженість конфігурацій і скорочує операційні витрати. Досліджено технології віртуалізації (GRE, MPLS, VXLAN, GENEVE тощо) та концепції Underlay/Overlay, які підвищують гнучкість і масштабованість мереж. Проаналізовано архітектуру Edge-Leaf, протоколи маршрутизації BGP ASN та засоби централізованого управління серверами HPE Server Automation.

КЛЮЧОВІ СЛОВА: АВТОМАТИЗАЦІЯ МЕРЕЖ, МОНІТОРИНГ, САМОВІДНОВЛЕННЯ СЕРВІСІВ, IPAM, ВЕНДОР-АГНОСТИЧНА МОДЕЛЬ, КОНФІГУРАЦІЯ МЕРЕЖІ, CI/CD, ВІРТУАЛІЗАЦІЯ, UNDERLAY, OVERLAY, VXLAN, MPLS, GENEVE, ДАТА-ЦЕНТР, УПРАВЛІННЯ МЕРЕЖЕЮ

ABSTRACT

Text part of the master's qualification work: 72 pages, 21 figures, 23 sources.

The purpose of the work is to increase the efficiency of telecommunication network management by implementing methods for automating the configuration, monitoring, and self-healing processes of services based on modern virtualization technologies, standardized management protocols, and CI/CD concepts.

Object of the study is a telecommunication network as a complex distributed system that includes physical (underlay) and virtual (overlay) infrastructure, as well as control, monitoring, and reliability systems.

Subject of the study is methods and tools for automating the management of telecommunication networks.

Summary of the work: the qualification work conducted a comprehensive study of methods and tools for automating the management of modern telecommunication networks. Approaches to optimizing the configuration, monitoring, and self-healing processes of services, and centralized management of network resources were considered. It was found that the implementation of IPAM systems, network service descriptions, and vendor-agnostic models ensures the consistency of configurations and reduces operating costs. Virtualization technologies (GRE, MPLS, VXLAN, GENEVE, etc.) and Underlay/Overlay concepts that increase network flexibility and scalability are investigated. Edge-Leaf architecture, BGP ASN routing protocols, and HPE Server Automation centralized server management tools are analyzed.

KEYWORDS: NETWORK AUTOMATION, MONITORING, SELF-HEALING SERVICES, IPAM, VENDOR-AGNOSTIC MODEL, NETWORK CONFIGURATION, CI/CD, VIRTUALIZATION, UNDERLAY, OVERLAY, VXLAN, MPLS, GENEVE, DATA CENTER, NETWORK MANAGEMENT

ЗМІСТ

ВСТУП 9
РОЗДІЛ 1 ПЛАНУВАННЯ МЕРЕЖІ 11
1.1 Створення мережі 11
1.2 Основні компоненти 18
РОЗДІЛ 2 ТЕХНОЛОГІЇ ВІРТУАЛІЗАЦІЇ В АВТОМАТИЗОВАНИХ МЕРЕЖАХ33
2.1 Основні поняття 33
2.2 Класифікація мереж 37
2.3 Варіанти розгортання Overlay 42
РОЗДІЛ 3 ДИЗАЙН АВТОМАТИЗОВАНОЇ МЕРЕЖІ 46
3.1 Внутрішня топологія дата-центрів 46
3.2 DCI та маршрутизація 49
3.3 Використання BGP ASN 55
РОЗДІЛ 4 АВТОМАТИЗАЦІЯ РОБОТИ З СЕРВЕРАМИ ЗА ДОПОМОГОЮ HEWLETT PACKARD ENTERPRISE SERVER AUTOMATION 59
4.1 Основні дані 59
4.2 Конфігурація HPE Server Automation 61
4.3 Можливості Hewlett Packard Enterprise Server Automation 65
ВИСНОВКИ 71
ПЕРЕЛІК ПОСИЛАНЬ 73
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 75

ВСТУП

У сучасних телекомунікаційних мережах питання підвищення ефективності управління інфраструктурою та оптимізації процесів автоматизації набувають особливого значення. Збільшення обсягів трафіку, ускладнення архітектури дата-центрів та активне впровадження віртуалізованих мережевих сервісів створюють необхідність у комплексних підходах до моніторингу, управління та конфігурації мережевого обладнання.

Дипломна робота присвячена дослідженню методів автоматизації, що дозволяють підвищити надійність, масштабованість та гнучкість телекомунікаційних систем. Основна увага приділяється системам моніторингу та самовідновлення сервісів, управлінню IP-адресами (IPAM), опису мережевих сервісів, а також механізмам ініціалізації пристроїв та автоматизованої доставки конфігурацій на основі вендор-агностичних моделей.

Особливе значення у роботі приділено технологіям віртуалізації, зокрема GRE, IP-in-IP, MPLS, MPLS L2/L3VPN, VXLAN, GENEVE, MPLSoverUDP та MPLSoverGRE, які дозволяють формувати оверлейні мережі з високим рівнем ізоляції та масштабованості. Аналізуються концепції Underlay та Overlay, використання віртуальних мережевих функцій (VNF) та внутрішньої топології дата-центрів, включно зі структурою DCI, маршрутизацією та архітектурою Edge-Leaf.

Дослідження також охоплює автоматизацію роботи з серверами, зокрема за допомогою HPE Server Automation, що забезпечує централізоване управління апаратними та програмними ресурсами. Використання таких систем дозволяє підвищити ефективність адміністрування, скоротити час простою та знизити ризики виникнення помилок при ручному налаштуванні обладнання.

Метою дипломної роботи є комплексний аналіз існуючих підходів та розробка рекомендацій щодо оптимізації процесів автоматизації у телекомунікаційних мережах. Впровадження розглянутих методів і технологій дозволяє забезпечити надійну роботу мережі, підвищити її масштабованість та

ефективність управління, що є критично важливим для сучасних операторів та організацій, що експлуатують складні телекомунікаційні системи.

1 ПЛАНУВАННЯ МЕРЕЖІ

1.1 Створення мережі

Визначальна теза цього циклу досліджень полягає в тому, що у сучасних умовах ми налаштовуємо не окремі мережеві пристрої, а всю мережу як єдину інтегровану систему. На перший погляд ця ідея може здаватися не настільки значущою, проте саме вона відображає сутність сучасних тенденцій розвитку телекомунікацій. Протягом останніх років спостерігається стійкий зсув акцентів від роботи з індивідуальними конфігураціями пристроїв до сприйняття мережі як цілісного об’єкта управління. Це стало підґрунтям для появи та поширення таких концепцій, як Software Defined Networking (SDN), Intent Driven Networks (IDN) та Autonomous Networks (AN), які орієнтовані на автоматизацію, централізацію та підвищення ефективності керування мережевими ресурсами.

Якщо розглядати потреби прикладних сервісів у глобальному масштабі, то вони зводяться до двох ключових вимог: забезпечення гарантованої зв’язності між заданими точками (А і Б, іноді — +В-Я) та створення механізмів ізоляції від інших застосунків і користувачів. Іншими словами, мережева інфраструктура повинна одночасно гарантувати надійний обмін даними й захист від небажаних перетинів трафіку.

У цьому контексті завданням даного циклу є побудова системи, що підтримує актуальну конфігурацію всієї мережі. При цьому цілісна конфігурація автоматично декомпонується на набір конфігурацій для кожного окремого пристрою відповідно до його ролі та топологічного розташування. Система управління мережею виступає єдиним центром внесення змін: адміністратор визначає бажаний результат, а система самостійно розраховує необхідний стан для кожного вузла та здійснює його налаштування.

Такий підхід дозволяє звести до мінімуму ручну роботу з CLI, що традиційно була джерелом численних помилок і затримок. Усі зміни в параметрах мережі чи її архітектурі повинні бути попередньо формалізовані, описані та задокументовані, і

лише після цього вони впроваджуються у виробниче середовище. Наприклад, якщо ухвалюється рішення, що відтепер стоєчні комутатори в певному дата-центрі мають анонсувати дві мережі замість однієї, то процедура передбачає такі кроки:

1. Документування змін у відповідних системах управління.
2. Автоматичне генерування цільової конфігурації для всіх пристроїв мережі.
3. Запуск програми оновлення конфігурації, яка аналізує поточний стан кожного вузла, визначає необхідні зміни (видалення чи додавання параметрів) та приводить вузли до узгодженого стану.

При цьому безпосереднє ручне втручання адміністратора обмежується лише першим кроком — формалізацією змін. Усі наступні процеси відбуваються централізовано, автоматизовано та контрольовано, що відповідає сучасним принципам побудови корпоративних та глобальних телекомунікаційних систем.

Тестування конфігурації

Досвід експлуатації телекомунікаційних систем свідчить, що переважна більшість критичних інцидентів (приблизно 80%) виникає саме під час внесення змін у конфігурацію мережевого обладнання. Непрямим підтвердженням цього є спостереження за періодами святкових канікул, коли зміни практично не виконуються, і відповідно кількість збоїв різко зменшується. Це вказує на ключову проблему: людський фактор залишається одним із головних джерел ризику для стабільності мережевої інфраструктури.

Типовими прикладами помилок є: некоректно введена команда, виконання налаштувань у неправильній гілці конфігурації, відсутність важливого параметра (наприклад, community у маршрутизації), випадкове видалення глобальних MPLS-налаштувань на маршрутизаторі, непослідовне впровадження змін на групі пристроїв (коли перші кілька вузлів налаштовані правильно, а на наступному конфігурація виявляється з помилкою). Подібні ситуації призводили до численних глобальних відмов та простоїв, що супроводжувалися фінансовими втратами та зниженням рівня довіри користувачів.

Автоматизація процесів внесення змін покликана зменшити кількість людських помилок, проте варто враховувати, що вона одночасно збільшує масштаб

їх можливих наслідків. Якщо раніше через невірну команду страждав один маршрутизатор чи комутатор, то сьогодні некоректна автоматизована зміна здатна паралізувати всю мережу одночасно.

Традиційно правильність змін перевірялася вручну: адміністратори покладалися на власний досвід, уважність та спостереження за роботою мережі після застосування конфігурації. Проте такий підхід є вкрай ненадійним і суперечить сучасним принципам забезпечення безперервності сервісів. Еволюція методів управління мережею призвела до того, що все більше компаній впроваджують лабораторне тестування змін та попередню валідацію конфігурацій перед їх розгортанням у робочому середовищі.

На передовій сучасної практики знаходяться організації, які інтегрували автоматизоване тестування конфігурацій та процесів їх застосування у свою операційну діяльність. По суті, мова йде про адаптацію процедур CI/CD (Continuous Integration / Continuous Deployment), що традиційно використовуються у програмній розробці. У контексті телекомунікацій це означає, що зміни у конфігурації мають бути попередньо збережені у системі контролю версій (наприклад, GitHub), протестовані у віртуалізованому середовищі або на лабораторному стенді, а вже потім автоматично застосовані до робочої мережі. Такий підхід значно зменшує ризики відмов та дозволяє уникнути небезпечної практики безпосереднього застосування неперевірених змін у продуктивному середовищі.

Таким чином, метод негайного впровадження змін у робочу мережу без тестування можна розглядати як застарілий і ризикований — приблизно настільки ж небезпечний, як фізичний вплив на критичний елемент системи без попередньої перевірки його стабільності.

Версіонування конфігурацій

Органічним продовженням концепцій автоматизації та CI/CD у сфері управління телекомунікаційними мережами є впровадження повноцінного версіонування конфігурацій.

Згідно з цим підходом, будь-яка зміна в мережі, незалежно від її масштабу (навіть зміна параметра на одному малопомітному пристрої), розглядається як перехід всієї мережі з одного стану до іншого. Таким чином, адміністратор не виконує окремі команди на пристрої, а переводить мережу у нову версію стану.

Варто застосовувати концепцію семантичного версіонування, що добре зарекомендувала себе у розробці програмного забезпечення:

- Мажорна версія (X.0.0) — фіксує кардинальні зміни в архітектурі (наприклад, перехід з IGP на виключне використання BGP).
- Мінорна версія (X.Y.0) — відображає суттєві, але менш радикальні зміни (наприклад, зміна політик імпорту маршрутів у BGP).
- Патч-версія (X.Y.Z) — позначає незначні зміни (наприклад, оновлення IP-адреси Loopback-інтерфейсу на одному з ToR-комутаторів).

Наприклад, поточна версія мережі може мати номер 1.0.0. Зміна IP-адреси Loopback-інтерфейсу призведе до версії 1.0.1. Перегляд політик маршрутизації — до 1.1.0. Радикальний редизайн із відмовою від IGP — до 2.0.0.

Слід зазначити, що у великих мережах різні дата-центри можуть мати різні версії конфігурації, оскільки розвиток інфраструктури відбувається нерівномірно: десь встановлюється нове обладнання та додаються нові рівні комутаторів spine, а десь архітектура залишається незмінною.

Ключовим принципом є те, що будь-які зміни (окрім тимчасових відладних команд) повинні розглядатися як оновлення версії. Усі відхилення від поточної версії мають автоматично фіксуватися та супроводжуватися повідомленнями адміністраторам.

Аналогічно, відкат конфігурації повинен розглядатися не як скасування останніх команд чи rollback силами операційної системи пристрою, а як повернення усієї мережі до визначеної попередньої версії. Такий підхід забезпечує цілісність управління, передбачуваність результатів і відповідає сучасним вимогам до надійності та масштабованості телекомунікаційних систем.

Моніторинг і самовідновлення сервісів

На перший погляд може здатися, що контроль стану сервісів у сучасних мережах — завдання цілком очевидне та давно відпрацьоване. Проте сьогодні воно набуває якісно нового змісту й масштабу. Якщо раніше головним було вчасно помітити несправність та залучити інженера для її усунення, то нині провідні сервіс-провайдери орієнтуються на принципи повної автоматизації. Суть полягає в тому, що несправний сервіс не намагаються вручну «лікувати» чи довго аналізувати причини його падіння. Натомість система швидко завершує роботу несправного процесу та запускає його заново, мінімізуючи час простою.

Ключовою умовою такого підходу є наявність потужної системи моніторингу, яка здатна за лічені секунди виявляти найменші відхилення від норми. Сьогодні вже недостатньо відслідковувати лише базові параметри — завантаженість інтерфейсів чи доступність вузлів. Також замало покладатися на чергового інженера, який вручну переглядає графіки та журнали подій. У сучасних телекомунікаційних системах дедалі частіше використовується принцип Self-Healing («самовідновлення»): як тільки моніторинг фіксує проблему, відповідні індикатори змінюють свій статус на «критичний», і система автоматично запускає механізми корекції для усунення збоїв.

Таким чином, йдеться не лише про контроль стану окремих пристроїв, а й про підтримку цілісного «здоров’я» всієї мережі. Цей контроль здійснюється у двох режимах:

- **white-box** — коли внутрішні параметри системи відомі, прозорі та легко відстежувані;
- **black-box** — коли аналіз здійснюється лише на основі зовнішніх результатів роботи, що є значно складнішим, але дозволяє оцінювати мережу навіть без детального доступу до її внутрішніх механізмів.

Необхідні передумови

Для впровадження такого комплексного підходу потрібна розвинена система управління мережею, яка включає:

- наявність актуального та детального інвентарного списку всіх пристроїв у мережі із зазначенням їх розташування, ролей, моделей і версій ПЗ (наприклад: leaf-комутатор у Києві, Juniper QFX 5120, версія R18.3);
- систему опису всіх мережевих сервісів (IGP, BGP, L2/3VPN, Policy, ACL, NTP, SSH та ін.);
- механізми первинної ініціалізації пристрою (hostname, Mgmt IP, Mgmt Route, Users, RSA-Keys, LLDP, NETCONF);
- інструменти для налаштування обладнання та приведення його конфігурацій до потрібного стану, включно з можливістю відкату на попередні версії;
- функції тестування цільової конфігурації перед її застосуванням;
- регулярну перевірку стану всіх пристроїв на предмет відхилень від актуальної версії з автоматичним інформуванням відповідальних осіб (наприклад, у разі несанкціонованого додавання нового правила в ACL уночі);
- механізми контролю загальної працездатності мережі та сервісів, що на ній функціонують.

Засоби реалізації

Оскільки завдання виглядає надзвичайно масштабним, його доцільно декомпозувати на окремі логічні компоненти. У результаті формується архітектура, що складається з десяти ключових елементів:

1. Інвентарна система.
2. Система управління IP-простором.
3. Система опису мережевих сервісів.
4. Механізм ініціалізації пристроїв.
5. Вендор-агностична конфігураційна модель.
6. Вендор-специфічний драйвер (інтерфейс).
7. Механізм доставки конфігурації на пристрій.
8. CI/CD-процеси для мережевих змін.
9. Механізм резервного копіювання та виявлення відхилень.
10. Система моніторингу.

Ці елементи формують сучасну модель побудови та підтримки мережевої інфраструктури, орієнтовану на автоматизацію та масштабованість. Варто підкреслити, що на початкових етапах розвитку даної концепції планувалося впровадження лише чотирьох базових компонентів. Проте зростання складності мереж, збільшення кількості сервісів і вимоги до їх безперервності призвели до суттєвого розширення архітектури, яка сьогодні включає цілу екосистему взаємопов'язаних рішень.

Таким чином, моніторинг і самовідновлення стають невід'ємними складовими сучасних телекомунікаційних мереж, дозволяючи зменшити час реакції на збої, забезпечити стабільність сервісів та підвищити рівень довіри користувачів до цифрової інфраструктури.

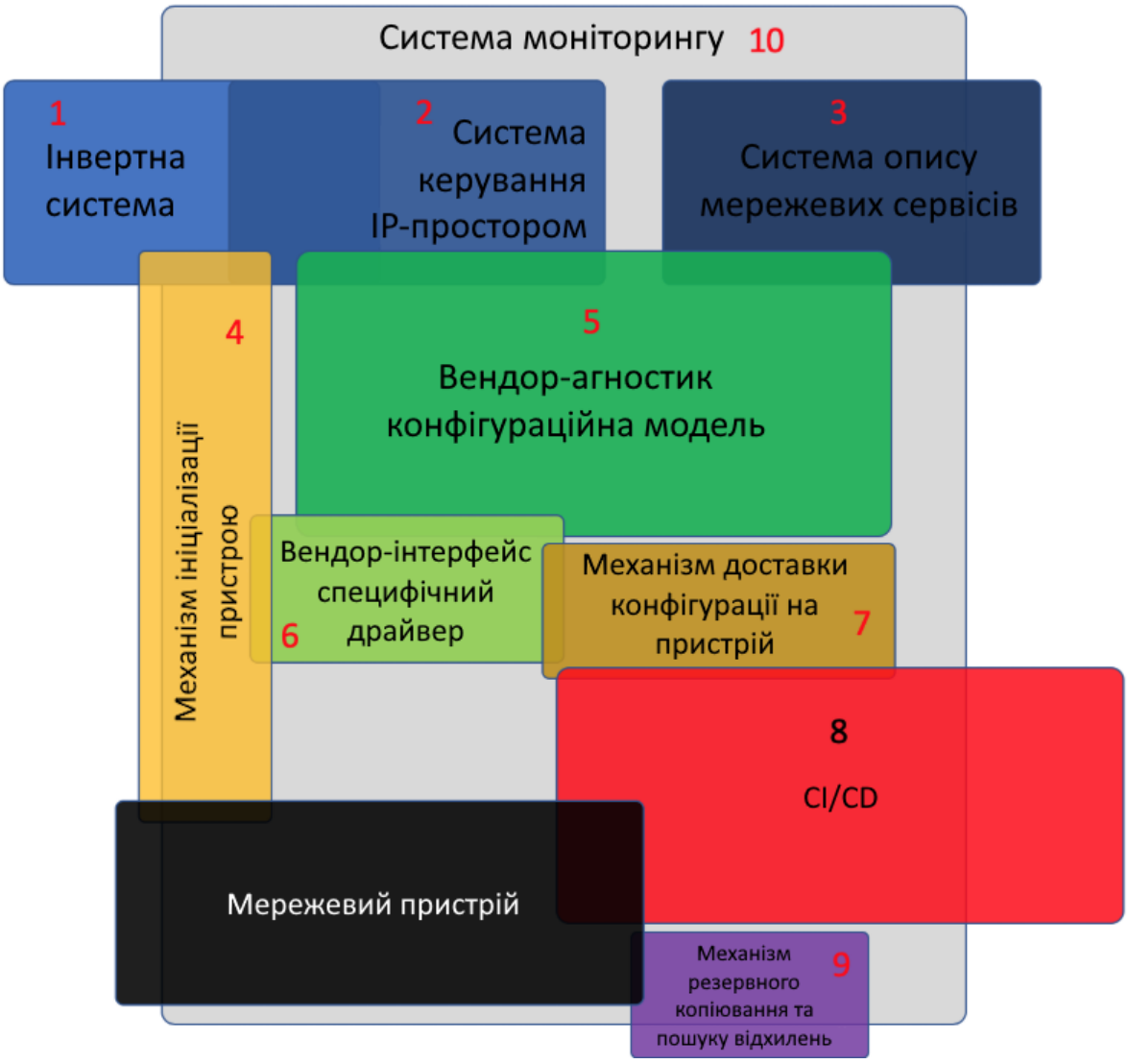


Рис. 1.1 На ілюстрації зображено усі компоненти та власне пристрій

Пересічні компоненти взаємодіють один з одним. Чим більше блок, тим більше уваги потрібно приділити цьому компоненту

1.2 Основні компоненти

Для ефективного управління сучасною телекомунікаційною інфраструктурою критично важливо мати повну та актуальну інформацію про всі мережеві пристрої, їхнє розташування та взаємозв’язки. Саме тут на допомогу приходить система інвентаризації, яка є невід’ємною складовою будь-якого підприємства, що прагне до високої надійності та керованості своєї мережі.

У корпоративному середовищі часто використовується окрема інвентаризаційна система для мережевих пристроїв. Вона вирішує специфічні завдання, які не покривають загальні системи обліку: від контролю наявності та стану обладнання до побудови детальної топології мережі. У рамках даного циклу статей ми будемо використовувати термін DCIM (Data Center Infrastructure Management). Варто зауважити, що у вузькому розумінні DCIM охоплює більше аспектів, ніж лише облік пристроїв — наприклад, управління енергоспоживанням, охолодженням, просторовим плануванням і навіть інтеграцію з системами моніторингу. Проте для наших цілей ми фокусуємося саме на інвентаризації як ключовому компоненті управління мережею.

У системі інвентаризації для кожного пристрою має зберігатися максимально детальна інформація, яка дозволяє не лише швидко ідентифікувати обладнання, а й інтегрувати його у процеси автоматизованого управління та моніторингу. Зокрема, це включає:

1. **Інвентарний номер** — унікальний ідентифікатор, який однозначно визначає пристрій у всій мережі;
2. **Назва або опис** — зрозуміле позначення, що відображає функцію або роль пристрою;
3. **Модель та виробник** — наприклад, *Huawei CE12800, Juniper QFX5120* та інші, включаючи точну модифікацію та версію апаратного забезпечення;

4. **Характерні параметри** — встановлені плати, типи та кількість інтерфейсів, пропускна здатність, специфічні апаратні функції;
5. **Роль у мережевій архітектурі** — Leaf, Spine, Border Router, Aggregation Router чи інші специфічні ролі залежно від топології та функцій мережі;
6. **Локація** — географічне положення, місто, дата-центр, стійка та юніт у стійці;
7. **Інтерконекти та підключення** — детальна інформація про фізичні та логічні зв'язки з іншими пристроями;
8. **Топологія мережі** — схема взаємодії всіх компонентів для швидкого аналізу та планування змін;
9. **Версія програмного забезпечення та конфігурації** — важлива для процесів оновлення, тестування та відновлення;
10. **Стан експлуатації** — поточний робочий стан, включно з останніми змінами та історією подій.

Завдяки такій системі можна не лише контролювати наявність і стан обладнання, а й інтегрувати її з автоматизованими процесами управління мережею, CI/CD-процесами, моніторингом і механізмами самовідновлення. Іншими словами, система інвентаризації стає основою для прозорого, керованого та безпечного функціонування сучасної телекомунікаційної інфраструктури, що дозволяє підприємствам ефективно масштабувати свої сервіси, швидко реагувати на збої та планувати розвиток мережі з високим рівнем передбачуваності.

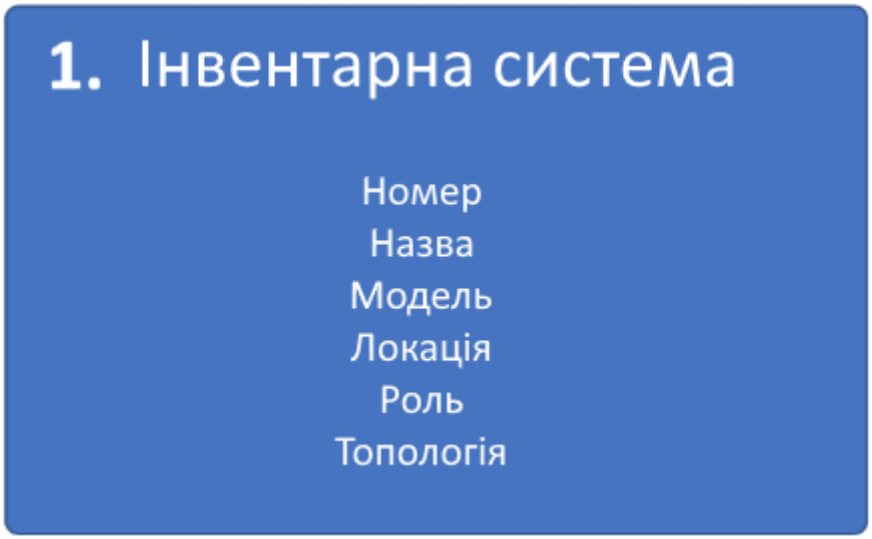


Рис. 1.2 Складові інфентарної системи

Звичайно, на перший погляд може здаватися, що система інвентаризації потрібна лише для ведення обліку обладнання та контролю його розташування. Проте її справжня цінність полягає в можливості автоматизувати управління мережею і забезпечити узгодженість усіх змін. Наявність детальної інформації про пристрої дозволяє швидко приймати рішення та застосовувати стандартні правила конфігурації без ризику помилок при ручному налаштуванні.

Наприклад, за допомогою системи інвентаризації можна точно знати, що в конкретному дата-центрі на Leaf-комутаторах різних виробників існують різні правила застосування ACL для фільтрації трафіку:

- на обладнанні Huawei ACL застосовуються на рівні VLAN,
- на обладнанні Juniper — на unit 0 фізичного інтерфейсу.

Це дозволяє автоматично формувати правильні конфігурації для різних пристроїв без ручного втручання.

Інший приклад — швидке розгортання нового Syslog-сервера на всіх Border-комутаторах певного регіону. Завдяки централізованому обліку інформації про пристрої та їх ролі система може автоматично визначити, на які елементи мережі необхідно встановити сервер, і виконати це розгортання у відповідності з правилами безпеки та внутрішньої політики компанії.

Крім фізичних пристроїв, система інвентаризації зберігає інформацію про віртуальні мережеві елементи, такі як віртуальні маршрутизатори, рут-рефлектори та інші сервіси. До цього також можна віднести DNS-сервери, NTP, Syslog та будь-які інші компоненти, які опосередковано впливають на роботу мережі. Таким чином, система стає не просто каталогом обладнання, а центральною платформою для управління всією інфраструктурою, що дозволяє:

- автоматично застосовувати конфігураційні зміни для різних типів пристроїв;
- швидко реагувати на зміни топології та додавати нові елементи без ризику конфліктів;
- інтегрувати віртуальні та фізичні компоненти мережі в єдину керовану систему;

- підтримувати актуальність та узгодженість конфігурацій у всіх сегментах мережі.

Таким чином, система інвентаризації перетворюється на ключовий елемент автоматизації та управління сучасною телекомунікаційною мережею, що забезпечує високу надійність, зменшує ризик помилок і скорочує час реагування на будь-які зміни або збої.

Система управління IP-адресами (IPAM)

Навіть у наш час деякі організації все ще ведуть облік IP-адрес і префіксів у Excel-файлах, що є досить обмеженим і трудомістким підходом. Проте сучасні телекомунікаційні та дата-центрові інфраструктури потребують більш надійних та масштабованих рішень. Сьогодні облік і управління IP-адресами здійснюється через бази даних, які мають веб-фронтенд на nginx або Apache, API для інтеграції з іншими системами та широкий функціонал для керування мережевими ресурсами з підтримкою VRF (Virtual Routing and Forwarding). Такі системи називають IPAM (IP Address Management).



Рис. 1.3 Складовы системи керування IPAM

Інформація, яка зберігається в IPAM

Для ефективної автоматизації та управління мережею IPAM зберігає наступні дані:

- VLAN — віртуальні локальні мережі, які використовуються для сегментації трафіку;

- VRF — віртуальні маршрутизовані сегменти для ізоляції маршрутів;
- Мережі та підмережі — з точними адресними діапазонами;
- IP-адреси — статичні та динамічно виділені адреси;
- Прив’язка IP-адрес до конкретних пристроїв, а мереж і VLAN — до конкретних локацій та стійок;
- Додаткові атрибути, які можуть знадобитися для інтеграції з автоматизованими процесами, такими як розгортання серверів чи налаштування мережевих сервісів.

Практичне значення для автоматизації

IPAM дозволяє уникнути класичних проблем управління IP-адресами:

- виділення вже зайнятих адрес;
- повторне використання одного і того ж префіксу у різних сегментах мережі;
- помилки при створенні конфігурацій на різних пристроях.

Наприклад:

- При виділенні Loopback-адреси для ToR-комутатора система автоматично перевіряє доступні адреси у префіксі з роллю Loopbacks. Якщо доступна адреса є — вона одразу виділяється, якщо ні — система ініціює створення нового префіксу.
- При генерації конфігурації пристрою можна визначити, в якому VRF має перебувати інтерфейс, автоматично підставивши правильне значення.
- Під час запуску нового сервера скрипт може звернутися до IPAM, дізнатися, в якому серверному комутаторі, на якому порту і яка підмережа призначена для інтерфейсу, та автоматично виділити серверу коректну IP-адресу.

Переваги інтеграції IPAM в автоматизацію

- Централізація управління IP-адресами — усі дані зберігаються в єдиній системі;
- Мінімізація людського фактору — зменшення ризику помилок при ручному призначенні адрес;
- Прозорість і контроль — будь-яка зміна адреси або префіксу фіксується, що забезпечує аудит та відстеження;

- Інтеграція з CI/CD та скриптами автоматизації — автоматичне виділення адрес для нових пристроїв та серверів;
- Масштабованість — легко керувати сотнями або тисячами IP-адрес у різних дата-центрах та регіонах.

Таким чином, IPAM стає ключовим компонентом сучасної мережевої автоматизації, забезпечуючи надійне управління IP-адресами, оптимізацію конфігурацій і безперервність роботи інфраструктури.

Система опису мережевих сервісів

У сучасних мережах не достатньо просто зберігати дані про пристрої або адресний простір — необхідно точно описати, як кожен пристрій повинен бути налаштований для виконання своєї ролі. Саме цю функцію виконує система опису мережевих сервісів, яка визначає правила конфігурації для всіх типів обладнання та забезпечує стандартизацію налаштувань по всій мережі.



Рис. 1.4 Структура системи опису мережевих сервісів

Основні типи мережевих сервісів

Систему опису мережевих сервісів доцільно розділити на два основні типи:

1. Інфраструктурні сервіси — забезпечують базову роботу пристрою та мережевої інфраструктури.

   До них відносяться:

   - VTY (виртуальні термінальні сесії для адміністрування);
   - SNMP (моніторинг та управління пристроями);

- NTP (синхронізація часу);
- Syslog (збір та централізація логів);
- AAA (автентифікація, авторизація та облік);
- протоколи маршрутизації (IGP, BGP);
- CoPP (Control Plane Policing) та інші служби управління мережею.

2. Клієнтські сервіси — організовують безпосередньо послугу для кінцевого користувача або клієнта мережі.
   Сюди належать:
   - MPLS L2/L3VPN,
   - GRE, VXLAN, VLAN, L2TP,
   - різноманітні віртуальні мережі та тунелі, які забезпечують ізоляцію та транспорт даних для клієнтів.

Звичайно, існують і пограничні випадки, наприклад, MPLS LDP або BGP, які можуть одночасно виконувати функції інфраструктурних та клієнтських сервісів. Важливо розуміти, що суть системи полягає не у суворому розмежуванні, а у можливості уніфікувати правила конфігурації для будь-якого типу сервісу.

Конфігураційні примітиви

Обидва типи сервісів розкладаються на базові конфігураційні примітиви, які легко автоматизувати:

- Фізичні та логічні інтерфейси (tag/untag, MTU, trunk/port-mode);
- IP-адреси та VRF (IPv4, IPv6, VRF);
- ACL та політики обробки трафіку;
- Протоколи маршрутизації (IGP, BGP, MPLS);
- Політики маршрутизації (prefix-list, community, ASN-фільтри);
- Службові сервіси (SSH, NTP, LLDP, Syslog);
- інші допоміжні механізми, необхідні для стабільної роботи мережі.

Приклади застосування

Для прикладу, у реальних дата-центрах налаштування виглядає так:

- Leaf-комутатор повинен підтримувати BGP-сесії з усіма підключеними Spine-комутаторами, імпортувати лише підключені мережі, а від Spine

приймати маршрути тільки з певного префіксу. Додатково можуть застосовуватися обмеження для CoPP IPv6 ND (наприклад, до 10 пакетів на секунду) та інші політики контролю трафіку.

- Spine-комутатори у свою чергу виступають як рут-рефлектори, підтримують сесії з усіма підключеними Leaf-комутаторами та приймають лише маршрути певної довжини або з конкретним community.

Значення для автоматизації

Система опису мережевих сервісів дозволяє:

- Стандартизувати налаштування для всіх пристроїв відповідно до їх ролі;
- Зменшити ризик помилок, що виникають при ручному конфігуруванні;
- Інтегрувати фізичні та віртуальні сервіси в єдину автоматизовану систему;
- Прискорити розгортання нових сервісів та забезпечити узгодженість конфігурацій у всіх сегментах мережі;
- Підтримувати прозорість та контроль змін через централізоване управління політиками та примітивами.

Таким чином, ця система є ключовим елементом автоматизації та управління сучасними мережами, що дозволяє побудувати керовану, масштабовану та надійну інфраструктуру.

Механізм ініціалізації пристрою

Процес ініціалізації мережевого пристрою — це комплекс дій, необхідних для того, щоб новий пристрій став видимим для систем управління мережею та став доступним для віддаленого адміністрування. Саме від того, наскільки якісно і швидко виконується цей процес, залежить подальша ефективність автоматизації та управління мережею.



Рис. 1.5 Структура механізму ініціалізації пристрою

Основні кроки ініціалізації

1. Реєстрація пристрою в системі інвентаризації

   Кожен новий пристрій повинен бути внесений у систему DCIM або іншу інвентарну систему, де фіксуються: модель, серійний номер, роль у мережі, версія програмного забезпечення, фізичне розташування та інші ключові характеристики. Це дозволяє відстежувати кожен елемент мережі та планувати його подальшу інтеграцію.

2. Виділення IP-адреси управління

   Для забезпечення віддаленого доступу кожному пристрою призначається унікальна IP-адреса в мережі управління. Це необхідно для підключення через SSH, Telnet або NETCONF та для інтеграції з системами автоматизації.

3. Налаштування базового доступу

   На цьому етапі пристрій отримує мінімальний набір конфігурацій для забезпечення безпечного доступу та управління:

   - ім’я хоста (hostname),
   - IP-адреса управління та маршрут до мережі управління,
   - облікові записи користувачів і права доступу,
   - SSH-ключі для безпечного підключення,
   - включення необхідних протоколів управління (Telnet, SSH, NETCONF).

   Підходи до ініціалізації

Сьогодні існує кілька підходів до організації ініціалізації пристроїв:

1. Повністю ручна ініціалізація

Пристрій привозять у дата-центр або на тестовий стенд, де інженер вручну підключається до консолі, реєструє його в системах, налаштовує IP-адреси, користувачів і базові сервіси. Такий підхід підходить для невеликих мереж або статичних середовищ, але швидко стає непридатним при масштабуванні та автоматизації.

2. Zero Touch Provisioning (ZTP)

   У сучасних мережах широко застосовується ZTP — автоматична ініціалізація без ручного втручання. Пристрій після підключення отримує IP через DHCP, звертається до спеціального сервера конфігурацій і самостійно завантажує базову конфігурацію. Це дозволяє значно скоротити час розгортання і зменшити кількість помилок через людський фактор.

3. Інфраструктура консольних серверів

   Для великих дата-центрів та корпоративних мереж застосовуються консолі сервіси, які забезпечують автоматичну первинну настройку через консольний порт. Це поєднує контроль ручного підключення з можливостями автоматизації та дозволяє безпечно підготувати пристрій для інтеграції у мережу.

Переваги автоматизованої ініціалізації

- Прискорене розгортання пристроїв — нове обладнання стає доступним для управління та моніторингу у лічені хвилини;
- Зменшення людського фактору — мінімізується ризик помилок при первинному налаштуванні;
- Централізація та прозорість — всі нові пристрої автоматично з’являються у системах управління та моніторингу;
- Масштабованість — підходи ZTP та автоматичної ініціалізації через консолі дозволяють легко підключати десятки чи сотні нових пристроїв одночасно;
- Підготовка до автоматизованої конфігурації — після завершення ініціалізації пристрій готовий для інтеграції у CI/CD-процеси та подальшого управління конфігурацією.

Таким чином, механізм ініціалізації є ключовим етапом інтеграції пристроїв у сучасну мережеву інфраструктуру, що забезпечує швидке, безпечне та стандартизоване включення обладнання в автоматизовану систему управління.

Вендор-агностична конфігураційна модель

До цього моменту всі розглянуті системи були по суті набором окремих фрагментів, які забезпечували змінні та декларативний опис бажаного стану мережі. Проте в будь-який момент настає етап, коли доводиться працювати з конкретним обладнанням, яке має свої особливості, обмеження та інтерфейси управління.

Саме для цього створюється вендор-агностична конфігураційна модель — абстракція, яка поєднує примітиви, сервіси та змінні, і описує повну конфігурацію конкретного пристрою, при цьому залишаючись незалежною від виробника обладнання.

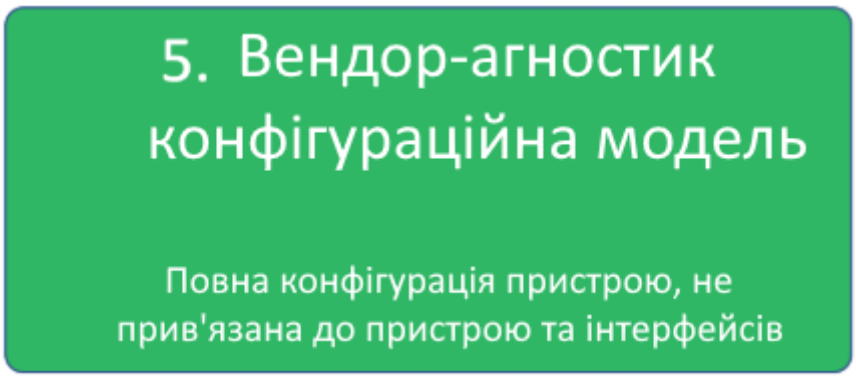


Рис. 1.6 Структура вендор-агностик конфігураційної моделі

Основні переваги та завдання цього підходу

1. Уніфікація взаємодії з пристроями

   Модель не залежить від конкретного способу доступу до обладнання. CLI, NETCONF, RESTCONF, SNMP — всі ці інтерфейси працюють з однією і тією ж абстрактною моделлю конфігурації. Це дозволяє централізовано управляти мережевими пристроями незалежно від їхнього виробника і спрощує автоматизацію.

2. Зменшення кількості шаблонів і скриптів

   Без вендор-агностичної моделі доводиться підтримувати окремі шаблони під кожного вендора у мережі. Будь-яка зміна дизайну або політик вимагала

редагування декількох місць одночасно, що створювало ризик помилок. Використання однієї абстрактної моделі дозволяє вносити зміни централізовано, після чого вони автоматично застосовуються до всіх пристроїв.

3. Контроль та порівняння конфігурацій

Модель дозволяє:

- завантажити поточну конфігурацію пристрою з резервної копії;
- привести її до абстрактного формату, сумісного з вендор-агностичною моделлю;
- порівняти з цільовою конфігурацією для обчислення дельти змін;
- автоматично сформувати патч, який змінює тільки необхідні елементи;
- або виявити відхилення для подальшого виправлення.

Додаткові переваги

- Масштабованість: одна модель працює для всіх пристроїв незалежно від виробника;
- Прозорість і контроль: централізована модель дозволяє бачити стан конфігурацій та зміни у всіх елементах мережі;
- Автоматизація процесів: спрощує інтеграцію з CI/CD та системами доставки конфігурації;
- Незалежність від вендора: дозволяє побудувати універсальний підхід до управління всією мережею, що особливо важливо для великих дата-центрів та корпоративних мереж із багатовендорною інфраструктурою.

Практичне застосування

Наприклад, завдяки вендор-агностичній моделі можна:

- швидко порівнювати конфігурації нового пристрою з існуючими стандартами;
- оновлювати конфігурацію всіх пристроїв певного типу одним патчем;
- забезпечити узгодженість налаштувань на всіх Leaf, Spine, Border-комутаторах, не прив’язуючись до конкретного вендора;

- інтегрувати процеси моніторингу та самовідновлення сервісів без додаткового ручного налаштування під кожен пристрій.

Таким чином, вендор-агностична конфігураційна модель є критичною складовою сучасної автоматизації мереж, яка забезпечує стандартизацію, масштабованість і надійність управління мережею незалежно від виробника обладнання.

Механізм доставки конфігурації на пристрій

Після того як конфігурація мережі згенерована та підготовлена у вигляді цільової моделі, наступним критично важливим кроком є її коректне та безпечне доставлення на мережеві пристрої. У великих корпоративних мережах або дата-центрах ручне завантаження конфігурації абсолютно неприпустиме через високий ризик помилок та масштабованість процесу.

Вибір транспортного протоколу

Перш ніж доставити конфігурацію, необхідно визначитися з транспортом. Сьогодні існує кілька варіантів:

- CLI (Telnet/SSH) — класичний метод, який використовувався десятиліттями, проте сьогодні його застосування обмежене і він вважається застарілим;
- SNMP — підходить більше для моніторингу і збору статистики, а не для повного завантаження конфігурацій;
- NETCONF — сучасний стандарт для управління мережевими пристроями, який дозволяє передавати конфігурацію декларативно та контролювати її стан;
- RESTCONF — ще новий протокол, який поступово набирає популярності, але поки недостатньо поширений;
- REST API — застосовується небагатьма виробниками, тому має обмежене використання;
- OpenFlow — більше орієнтований на доставку FIB (таблиць маршрутизації) і використовується у SDN, а не для повної конфігурації пристрою.

Якщо говорити простими словами, CLI сьогодні вважається легасі, SNMP не універсальний, а RESTCONF та REST API ще не набули масового застосування. У цьому циклі ми зосередимося на NETCONF, оскільки він надійний,

стандартизований та підтримується більшістю сучасних мережевих пристроїв. Важливо, що на цьому етапі інтерфейс доставки конфігурації вже визначений, і результат генерації конфігурації представлений у форматі, сумісному з обраним протоколом.

Вибір інструментів для доставки конфігурації

Після визначення протоколу необхідно обрати засоби автоматизації, які дозволять виконати доставку конфігурації ефективно та надійно. Основні варіанти:

1. Власні скрипти та рішення

   Можна використовувати Python разом з бібліотеками ncclient та asyncIO, створивши власну платформу автоматизації. Це дає максимальну гнучкість, дозволяє інтегрувати додаткові бізнес-логіки, проте вимагає значних витрат часу на розробку та підтримку.

2. Ansible

   Популярна система автоматизації, що має велику бібліотеку мережевих модулів для різних вендорів. Вона дозволяє швидко деплойнути конфігурації, інтегруватися з CI/CD процесами та забезпечує повторюваність налаштувань.

3. Salt

   Пропонує базові можливості роботи з мережею та може інтегруватися з Napalm для підтримки різних виробників. Підходить для організацій із обмеженим набором вендорів.

4. Napalm

   Спеціалізована бібліотека для роботи з конфігураціями мережевих пристроїв. Підтримує обмежену кількість вендорів, але дозволяє швидко застосовувати зміни та отримувати актуальний стан мережі.

5. Nornir

   Сучасний фреймворк для автоматизації мережевих процесів, який дозволяє інтегрувати різні джерела даних і протоколи доставки конфігурацій, забезпечуючи гнучкість та масштабованість. Його можливості будуть детально розглянуті у наступних частинах циклу.

Основні переваги автоматизованої доставки конфігурації

Впровадження автоматизованого механізму доставки конфігурацій забезпечує:

- Централізоване та безпечне оновлення пристроїв — конфігурації застосовуються стандартизовано, без людського втручання;
- Масштабованість процесу — одна процедура працює для десятків або сотень пристроїв одночасно;
- Стандартизацію мережі — всі зміни проходять через єдину модель, що забезпечує узгодженість конфігурацій;
- Інтеграцію з CI/CD — автоматизоване тестування та деплоймент конфігурацій у мережу;
- Зменшення ризику помилок — мінімізується людський фактор при налаштуванні обладнання.

Механізм доставки конфігурацій — це ключовий етап у побудові автоматизованої мережевої інфраструктури, який забезпечує швидку, надійну та стандартизовану роботу мережі. Правильний вибір протоколу та інструменту дозволяє не лише ефективно застосовувати конфігурації, а й підтримувати їхню відповідність цільовому стану, забезпечуючи контроль, повторюваність та інтеграцію з іншими автоматизованими процесами.

2 ТЕХНОЛОГІЇ ВІРТУАЛІЗАЦІЇ В АВТОМАТИЗОВАНИХ МЕРЕЖАХ

2.1 Основні поняття

Мережа — це основа, на якій тримається вся інфраструктура, і будь-які зміни тут потребують особливої обережності. Навіть короткочасне виведення одного вузла з експлуатації може паралізувати значну частину сервісів та вплинути на величезну кількість користувачів. Саме тому мережеві команди часто опираються будь-яким нововведенням: «Зараз усе працює (хоч ми й не до кінця розуміємо, як), а тепер треба щось нове налаштувати, і невідомо, які наслідки це матиме для всієї мережі».

Щоб зменшити залежність від ручного налаштування VLAN та інших мережевих сервісів на кожному вузлі, було запропоновано концепцію оверлейних мереж — накладених мереж, які працюють поверх фізичної інфраструктури. Серед популярних технологій: GRE, IP-in-IP, MPLS, MPLS L2/L3VPN, VXLAN, GENEVE, MPLSoverUDP, MPLSoverGRE та інші.

Їхня ефективність пояснюється двома ключовими моментами:

1. Налаштовуються лише кінцеві вузли, а транзитні пристрої залишаються недоторканими. Це значно прискорює процес розгортання нових сервісів і дозволяє автоматизувати більшість операцій без залучення всього відділу мережевої інфраструктури.
2. Вся логіка та інформація про мережу приховані всередині заголовків оверлею, і транзитні вузли не повинні знати про адресацію хостів або маршрути накладеної мережі. Це дозволяє зменшити обсяг даних у таблицях маршрутизації, що відкриває можливість використання більш простого та економічного обладнання.

Автоматизація оверлейних мереж

Сьогодні оверлейні мережі неможливо ефективно використовувати без автоматизації. Завдяки автоматичним системам:

- можна швидко створювати нові накладені сегменти мережі, не чіпаючи фізичні маршрутизатори та комутатори;
- усі кінцеві вузли конфігуруються централізовано, що мінімізує людський фактор та ймовірність помилок;
- автоматично контролюється стан оверлейної мережі, виявляються відхилення та несправності, а у разі потреби відбувається самовідновлення сервісів.

У даному розділі не буде детального розгляду всіх існуючих технологій накладених мереж, натомість увагу буде зосереджено на загальному фреймворку роботи оверлеїв у дата-центрі, де можна побачити, як накладені мережі взаємодіють із фізичною інфраструктурою та системами автоматизації.

За приклад буде узято дата-центр, що складається з рядів однотипних стійок із стандартним серверним обладнанням, на якому працюють:

- віртуальні машини;
- контейнери;
- serverless-сервіси, що реалізують різноманітні бізнес- і мережеві сервіси.

І саме автоматизація конфігурацій оверлейних мереж дозволяє:

- швидко розгортати нові сервіси без ручного налаштування;
- централізовано управляти адресацією, політиками та сегментацією;
- контролювати продуктивність та стан мережі у режимі реального часу;
- інтегруватися з CI/CD процесами для безперервного оновлення та управління мережею.

Таким чином, накладені мережі у поєднанні з автоматизацією стають основою сучасних масштабованих дата-центрів, дозволяючи підвищити гнучкість, надійність та ефективність мережевих інфраструктур в Україні та світі.

У даному розділі сервером ми будемо називати програму, яка реалізує серверну частину клієнт-серверної взаємодії, тобто компонент, який обробляє запити клієнтів і надає необхідні сервіси або дані. Важливо розрізняти програмний сервер і фізичне обладнання — фізичні машини в стійках ми не будемо називати серверами, щоб уникати плутанини.

Фізична машина (хост) — це x86-комп’ютер, встановлений у стійку. У більшості випадків її будемо називати просто машина або хост. Саме на хості можуть запускатися гіпервізори, віртуальні машини та контейнери, які реалізують сервіси.

Гіпервізор — це спеціалізоване програмне забезпечення, що запускається на фізичному хості і емулює його ресурси для розміщення віртуальних машин (ВМ). У деяких джерелах слово «гіпервізор» використовується як синонім до «хост», проте для нас важливо розуміти, що це саме шар між фізичною машиною і віртуальними інстанціями.

Віртуальна машина (ВМ) — це ізольоване середовище з власною операційною системою, запущене на гіпервізорі. Для наших цілей не принципово, чи це повноцінна віртуальна машина, чи контейнер — ми будемо називати їх ВМ. Вони забезпечують ізоляцію сервісів і клієнтів, а також дозволяють легко масштабувати інфраструктуру.

Тенант — це широке поняття, яке ми визначаємо як окремий сервіс або окремого клієнта. Мульти-тенантність (або мультиорендність) означає використання одного й того самого додатка кількома клієнтами або сервісами з повною ізоляцією завдяки архітектурі програми, а не через окремі запущені екземпляри.

ToR (Top of the Rack switch) — комутатор, встановлений на верхній частині стійки, до якого підключені всі фізичні машини. Іноді в дата-центрах використовують інші топології, наприклад, End of Row (EoR) або Middle of Row (MoR), хоча остання зустрічається дуже рідко.

Underlay network або підлягаюча мережа — це фізична мережна інфраструктура: комутатори, маршрутизатори, міжмашинні кабелі, оптичні лінки. Вона забезпечує базову фізичну зв’язність між усіма пристроями.

Overlay network або наложена мережа (оверлей) — це логічна віртуальна мережа, побудована поверх фізичної, яка дозволяє організовувати сегментовані віртуальні мережі, тунелі та ізоляцію трафіку без втручання у фізичну топологію.

L3-фабрика (IP-фабрика) — концепція побудови мережі на основі виключно L3 маршрутизації, без VLAN та великих широкомовних доменів. Вона значно спрощує масштабування і забезпечує ефективне використання мережевих ресурсів. Назва «фабрика» символізує автоматизацію потоків трафіку та управління мережею.

SDN (Software Defined Network) — підхід до управління мережею, при якому всі зміни виконуються не вручну, а автоматично за допомогою програмного забезпечення. Зазвичай це передбачає винесення Control Plane на централізований контролер, що дозволяє керувати сотнями чи тисячами пристроїв одночасно.

NFV (Network Function Virtualization) — віртуалізація мережевих функцій, яка дозволяє запускати частину сервісів у вигляді ВМ або контейнерів, пришвидшувати впровадження нових послуг, організовувати Service Chaining та забезпечувати горизонтальне масштабування.

VNF (Virtual Network Function) — конкретний віртуальний мережевий компонент, наприклад: маршрутизатор, комутатор, фаєрвол, NAT, IPS/IDS тощо.

Уся ця структура разом із автоматизацією дозволяє:

- швидко розгортати сервіси та оновлювати мережеву конфігурацію;
- централізовано керувати адресацією, політиками та сегментацією;
- моніторити стан мережі та ВМ у реальному часі;
- інтегрувати мережу з CI/CD процесами, забезпечуючи безперервне оновлення і контроль версій конфігурацій.

Таким чином, правильне розмежування термінів та використання автоматизації дозволяє ефективно управляти сучасними дата-центрами та створювати масштабовану, надійну та гнучку інфраструктуру.

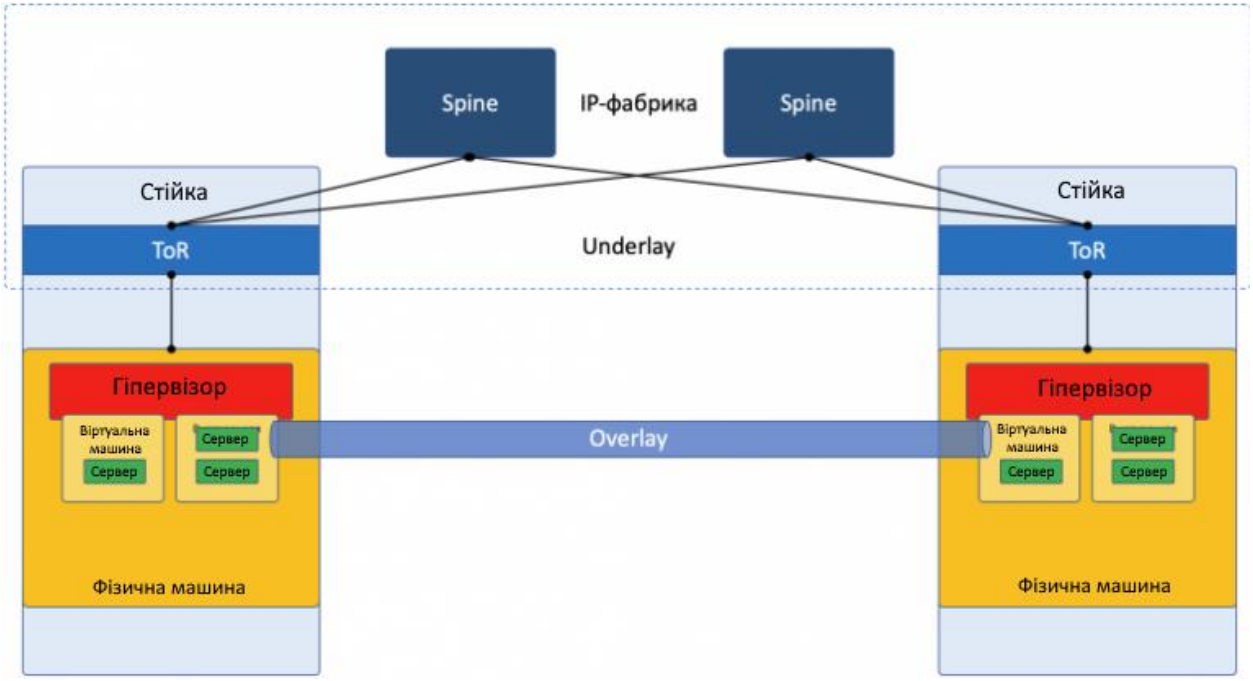


Рис. 2.1 Приклад віртуалізації мережі

2.2 Класифікація мереж

Сучасні мережі здебільшого можна чітко розділити на дві взаємопов'язані частини, кожна з яких виконує свою ключову роль у забезпеченні надійності, масштабованості та ізоляції:

1. Underlay — це фізична мережа, яка формує фундамент всієї інфраструктури. Вона включає комутатори, маршрутизатори, кабельні з'єднання та інші фізичні компоненти. Конфігурація цієї мережі, як правило, стабільна та мінімально змінюється з часом, оскільки саме на ній тримається вся логіка передачі даних. Основна роль Underlay полягає у забезпеченні базової зв'язності, стабільної маршрутизації та високої доступності для всіх пристроїв, що підключені до фізичної інфраструктури.

2. Overlay — це логічний шар або абстракція, який накладається на Underlay і дозволяє створювати ізольовані віртуальні мережі для різних тенантів або сервісів. Overlay забезпечує гнучкість і масштабованість: нові сервіси та клієнти можуть підключатися до мережі без необхідності змінювати фізичну топологію або задіювати додаткові ресурси Underlay. Цей шар особливо важливий у середовищах

з мульти-тенантністю, де ізоляція трафіку та сегментація ресурсів критично необхідні.

Таке розділення є справедливим як для дата-центрів, які ми розглядатимемо у цій серії статей, так і для інтернет-провайдерів (ISP). У випадку ISP Underlay забезпечує глобальну маршрутизацію та з'єднання між різними регіонами, а Overlay дозволяє організовувати приватні мережі для корпоративних клієнтів без порушення базової фізичної структури.

Що стосується корпоративних або етерпрайзних мереж, тут принцип розділення також зберігається, але структура Overlay може бути дещо менш формалізованою. Часто в таких мережах Overlay організовується на рівні окремих відділів або проектів, а Underlay може включати традиційні VLAN та L3-сегментацію для забезпечення внутрішньої стабільності.

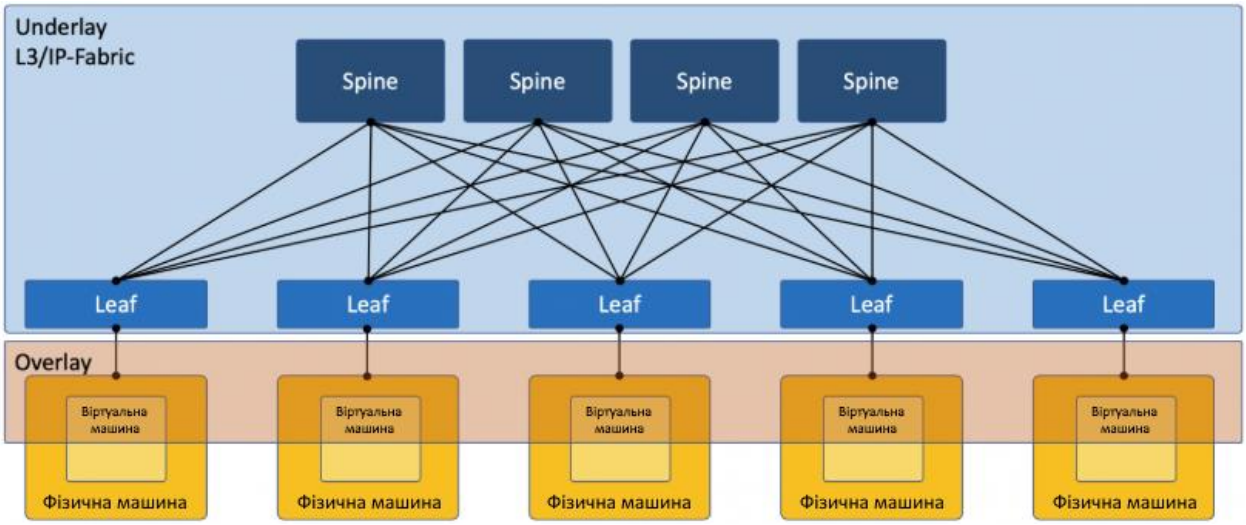


Рис. 2.2 Дві частини – Underlay та Overlay

Underlay — це фізична основа сучасної мережевої інфраструктури, що складається з апаратних комутаторів, маршрутизаторів, кабельних з'єднань і всіх необхідних фізичних компонентів. Саме цей шар відповідає за базову доставку пакетів між фізичними машинами, забезпечуючи фундаментальну зв'язність, без якої неможливо побудувати будь-яку більш складну віртуальну або логічну мережу.

Пристрої в Underlay "знають", як досягти кожної фізичної машини, і їхнє головне завдання — передавати дані на найнижчому рівні без урахування сервісів, які працюють поверх них. Цей шар не оперує поняттями тенантів, клієнтів чи

віртуальних мереж — йому важливо лише, щоб пакет коректно доставлявся від одного хоста до іншого.

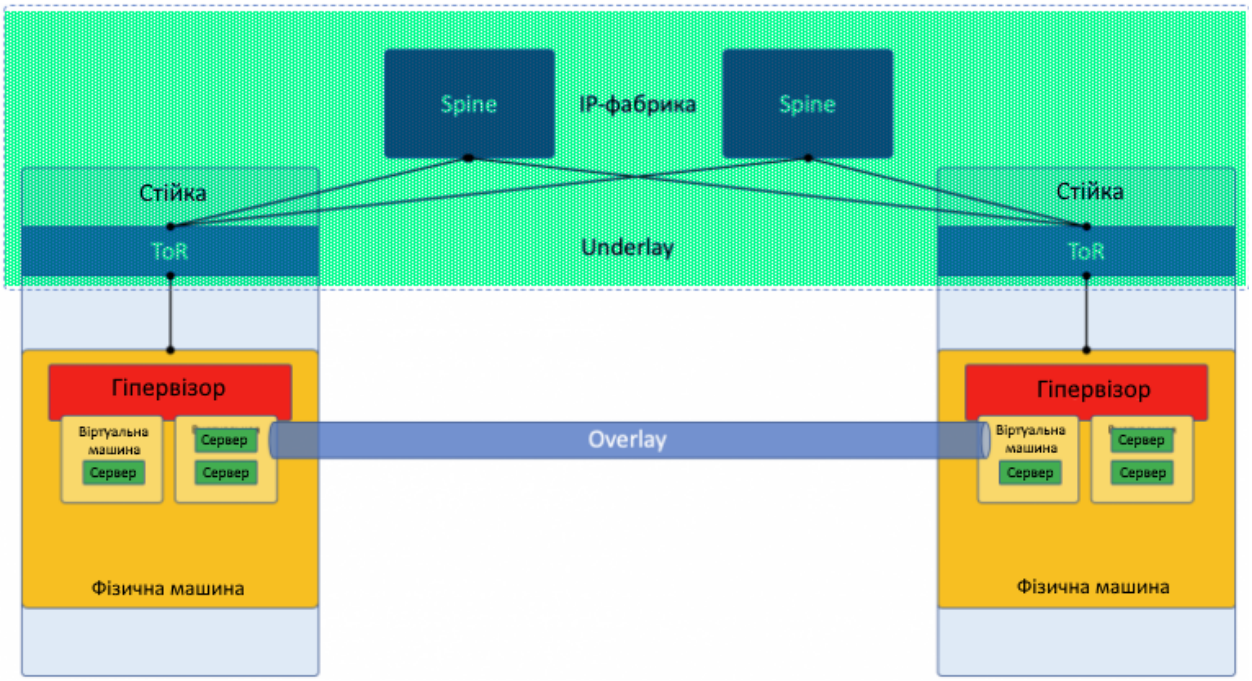


Рис. 2.3 Принцип роботи Underlay

Underlay базується на стандартних протоколах та технологіях, що забезпечує сумісність між різними вендорами і стандартизацію роботи мережі. Більшість апаратних пристроїв працює на пропрієтарному ПЗ, яке не дозволяє програмування чіпів або реалізацію власних протоколів, тому використання загальноприйнятих стандартів є критично важливим для стабільності та взаємодії різного обладнання. Лише великі компанії на кшталт Google можуть собі дозволити розробку власних комутаторів і відмову від стандартних протоколів, проте для більшості дата-центрів, корпоративних мереж або локальних провайдерів така можливість обмежена.

Конфігурація Underlay відносно стабільна і змінюється рідко. Його завдання — забезпечити базову IP-зв’язність між фізичними машинами, а всі зміни проводяться обдумано та планово, щоб не порушити роботу служб і не вплинути на клієнтів.

Приклади реалізацій Underlay включають:

- **IPv4 + OSPF** — класичний варіант маршрутизації в локальних мережах.

- **IPv6 + IS-IS + BGP + L3VPN** — для великих дата-центрів із підтримкою сучасних протоколів та мультипрефіксної маршрутизації.
- **L2 + TRILL** — для вирішення проблем масштабованості традиційного L2.
- **L2 + STP** — класичний варіант для простих або історично сформованих мереж.

Налаштування Underlay здійснюється за допомогою класичних методів: CLI, GUI або NETCONF, вручну, через скрипти або пропрієтарні інструменти. При цьому важливо розуміти, що зміни в Underlay потребують уважного планування та тестування, адже будь-яка помилка може відобразитися на всіх вищих шарах мережі.

Важливим аспектом сучасних дата-центрів і корпоративних мереж є автоматизація управління Underlay, яка дозволяє значно зменшити людський фактор і ризики помилок. Автоматизовані системи можуть моніторити стан мережі, виконувати планові зміни конфігурацій, перевіряти доступність та узгодженість IP-префіксів і маршрутизаційних таблиць, а також інтегруватися з Overlay для швидкого розгортання нових сервісів.

Overlay — це віртуальна мережа тунелів, яка накладається поверх фізичної мережі Underlay і виконує роль логічного середовища для взаємодії віртуальних машин (ВМ) одного клієнта або одного сервісу. Основна мета Overlay — забезпечити ізоляцію та безпеку між різними клієнтами або тенантами, при цьому дозволяючи ВМ одного клієнта обмінюватися даними так, ніби вони знаходяться в одній фізичній мережі, навіть якщо насправді їх пакети проходять через складну топологію фізичних пристроїв.

Дані клієнта інкапсулюються в спеціальні тунельні заголовки, що дозволяє передавати їх через загальну фізичну інфраструктуру без порушення логічного розділення мереж. Це означає, що ВМ можуть спілкуватися між собою без знання реального маршруту пакета, який може проходити через десятки або сотні комутаторів і маршрутизаторів. Overlay забезпечує абстракцію фізичної мережі та дозволяє програмно керувати маршрутизацією, ізоляцією і політиками безпеки.

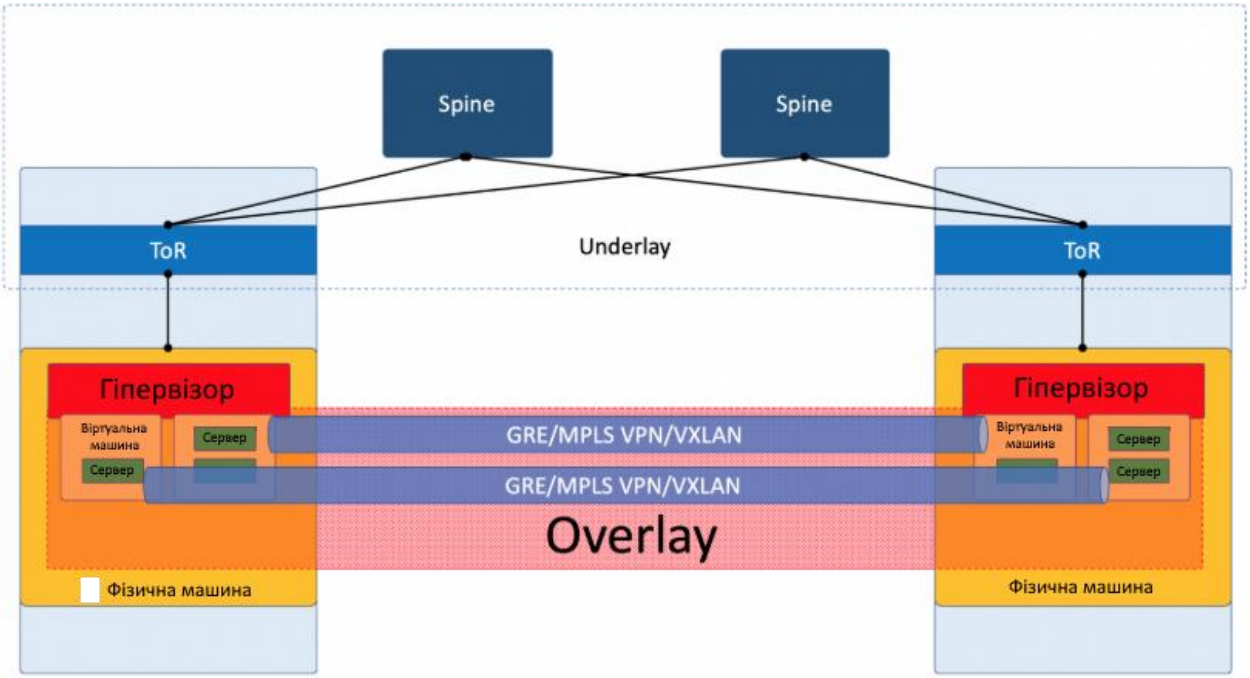


Рис. 2.4 Принцип роборти Overlay

Приклади технологій Overlay, які найчастіше використовуються в сучасних дата-центрах:

- GRE-тунелі — простий і надійний спосіб інкапсуляції пакетів для організації ізольованих сегментів.
- VXLAN — дозволяє масштабувати L2-сегменти поверх L3-мережі, забезпечує мульти-тенантність та інтеграцію з автоматизованими платформами управління.
- EVPN — підтримує гнучке маршрутизування та інтеграцію L2/L3 через IP-фабрики, що дозволяє ефективно керувати великою кількістю тенантів.
- L3VPN — створює ізольовані маршрутизовані мережі для різних клієнтів або сервісів, що забезпечує логічну сегментацію.
- GENEVE — сучасний протокол тунелювання з підтримкою розширюваних метаданих, що дає змогу інтегрувати нові сервіси без зміни базової фізичної мережі.

Налаштування Overlay зазвичай здійснюється через центральний контролер, який відповідає за управління Control Plane та доставку налаштувань на пристрої, що маршрутизують і інкапсулюють трафік клієнтів. Контролер дозволяє централізовано керувати всією Overlay-мережею, автоматизувати додавання нових

ВМ, масштабування сервісів та зміни політик без необхідності ручного втручання в кожен вузол.

Автоматизація є ключовим елементом Overlay: вона дозволяє швидко масштабувати мережу, додавати нових тенантів, організовувати service chaining і забезпечувати узгодженість та безпеку всіх віртуальних мереж. За допомогою автоматизованих скриптів і платформ, таких як Ansible, Nornir або власних контролерів SDN, можна забезпечити швидке і безпомилкове розгортання Overlay-мережі, мінімізуючи людський фактор та ризики помилок.

2.3 Варіанти розгортання Overlay

Overlay, що починається з ToR-комутатора

У цьому підході точка ініціації Overlay розташована на комутаторі доступу (Top of Rack, ToR), встановленому у стійці. Така конфігурація часто застосовується у випадку VXLAN-фабрик у сучасних дата-центрах.

Цей метод є тестованим і перевіреним часом, особливо в мережах великих провайдерів послуг (ISP), і підтримується практично всіма виробниками мережевого обладнання.

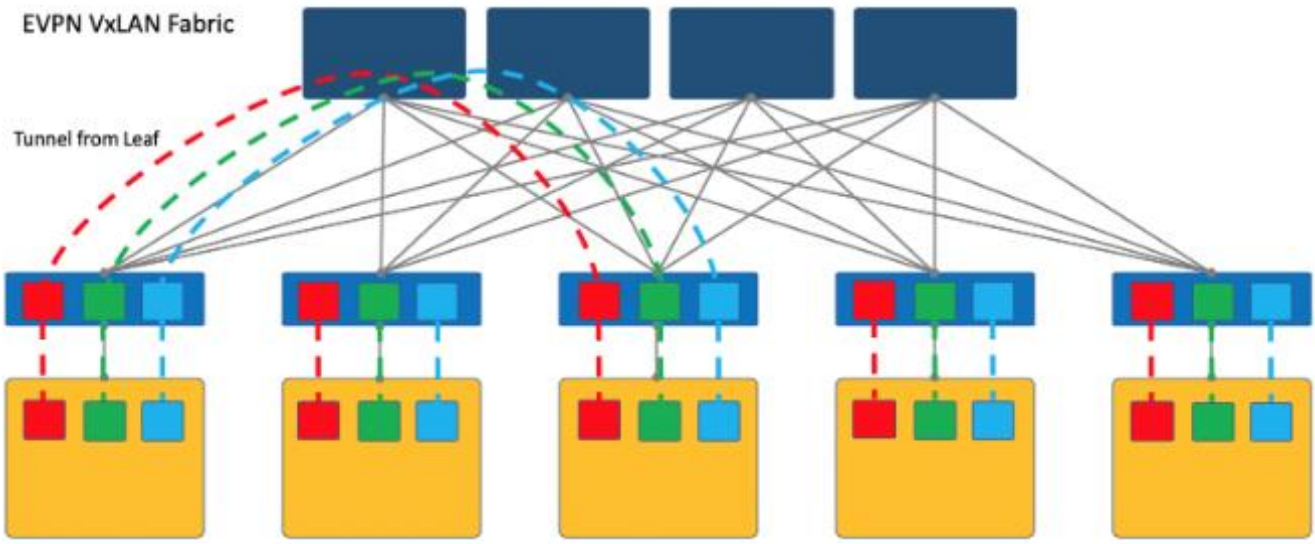


Рис. 2.5 Overlay на ToR-комутаторі

Основні характеристики та вимоги:

- **Розділення сервісів**: ToR-комутатор повинен вміти ізолювати трафік різних сервісів та тенантів, тобто забезпечувати інкапсуляцію і маршрутизацію клієнтських даних у межах Overlay.
- **Взаємодія з адміністраторами ВМ**: мережевий адміністратор повинен координувати зміни конфігурацій з адміністраторами віртуальних машин або автоматизованими системами управління, оскільки внесення нових сервісів і політик часто потребує інтеграції обох систем.
- **Автоматизація**: хоч зміни в конфігурації можуть виконуватися автоматично (через SDN-контролери чи платформи управління конфігураціями), адміністратор все одно повинен контролювати процес для уникнення конфліктів і забезпечення коректної роботи мережі.
- **Централізований контроль**: цей підхід дозволяє централізовано управляти трафіком, політиками безпеки та ізоляцією клієнтів, що спрощує масштабування і забезпечує високу узгодженість мережевих сервісів.

Переваги:

- Потужна інтеграція з фізичною інфраструктурою.
- Підтримка масштабованих багатотенантних мереж.
- Централізоване управління трафіком і політиками безпеки.

Недоліки:

- Вимагає сумісності обладнання та правильного налаштування ToR-комутаторів.
- Потребує співпраці мережевих адміністраторів з адміністраторами ВМ та автоматизованими системами.
- Висока складність при розгортанні нових сервісів без автоматизації.

Цей підхід особливо ефективний для великих дата-центрів та корпоративних мереж України, де є стабільна фізична інфраструктура, а розгортання багатотенантних Overlay-мереж має відбуватися швидко, без шкоди для існуючих сервісів.

Overlay, що ініціюється та термінується на хості

Другий підхід до організації Overlay-мережі передбачає, що всі тунелі створюються і закінчуються безпосередньо на кінцевих хостах. Це означає, що фізична мережа (Underlay) залишається максимально статичною, простою та стабільною, а хости беруть на себе всю роботу з інкапсуляції, маршрутизації та управління трафіком Overlay.

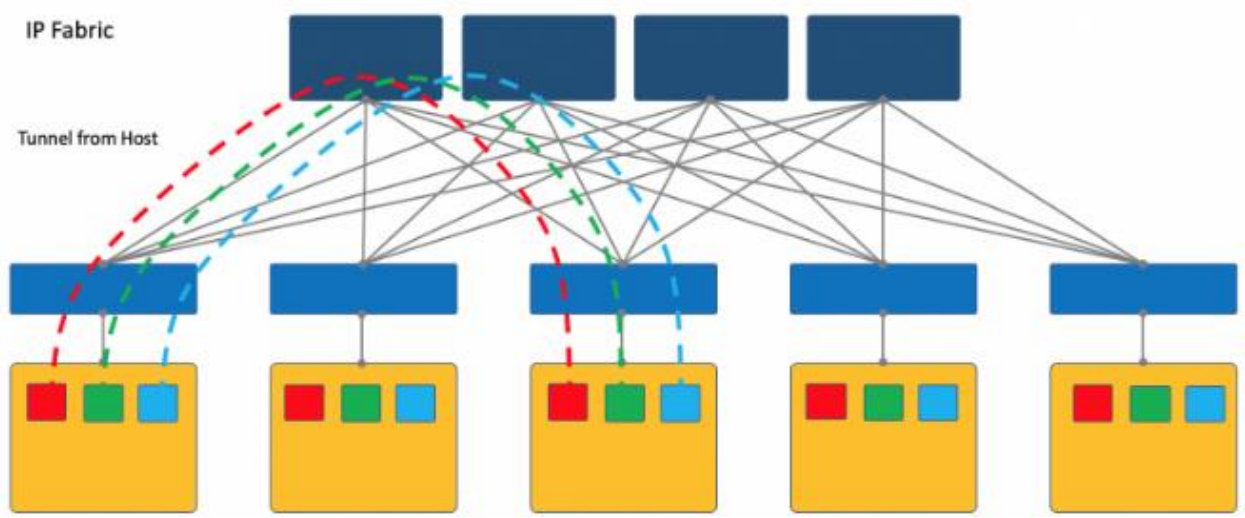


Рис. 2.6 Overlay з хоста

Для реалізації цього підходу на кожному хості необхідно запускати спеціальний програмний агент або клієнтську програму, яка відповідає за роботу з Overlay:

- інкапсуляцію пакетів у відповідні тунельні заголовки;
- декодування і маршрутизацію отриманого трафіку;
- підтримку політик безпеки і ізоляції між різними тенантами.

Хоч це й додає певну складність на рівні хостів, такий підхід має значні переваги:

1. **Простота запуску на хостах**
    - На Linux-серверах або інших стандартних платформах налаштувати клієнтський додаток набагато легше, ніж на мережевих комутаторах, де часто доводиться використовувати пропрієтарні SDN-рішення.

- Це забезпечує мультивендорну сумісність, оскільки Overlay-клієнт може працювати однаково на будь-якому хості, незалежно від виробника мережевого обладнання.

2. **Спрощення комутаторів ToR**
   - Комутатори доступу залишаються максимально простими і не потребують складної логіки для маршрутизації Overlay-трафіку.
   - Вони не зберігають ARP-таблиці або інформацію про всі віртуальні мережі та клієнтів, а лише фізичні IP-адреси підключених хостів.
   - Це значно зменшує навантаження на таблиці комутації та маршрутизації, роблячи мережу більш стабільною та легко масштабованою.
3. **Гнучкість і масштабованість Overlay**
   - Оскільки логіка Overlay переміщена на хости, нові сервіси або клієнтські сегменти можна швидко додавати або змінювати без необхідності перепрошивки або переналаштування фізичних комутаторів.
   - Такий підхід ідеально підходить для дата-центрів і корпоративних мереж, де фізична інфраструктура повинна залишатися стабільною, а логіка мережевих сервісів — динамічною.
4. **Потенціал для автоматизації**
   - Використання клієнтських агентів дозволяє централізовано керувати Overlay через автоматизовані системи, скрипти та оркестратори.
   - Можна реалізувати автоматичне налаштування тунелів, розподіл IP-адрес, оновлення політик безпеки та моніторинг здоров’я Overlay у режимі реального часу.

Отже, підхід Overlay з хоста значно спрощує підтримку фізичної мережі, дозволяє швидко масштабувати послуги та реалізувати високий рівень автоматизації, одночасно зберігаючи простоту і стабільність Underlay.

3 ДИЗАЙН АВТОМАТИЗОВАНОЇ МЕРЕЖІ

3.1 Внутрішня топологія дата-центрів

У сучасних дата-центрах мережеву інфраструктуру зазвичай проектують за єдиною схемою внутрішньої зв’язності, побудованою на основі топології Клоза. Такі мережі дозволяють забезпечити високу доступність, передбачувану масштабованість і рівномірний розподіл навантаження між комутаторами.

Структура дата-центру

У кожному дата-центрі зазвичай присутні близько 10 стійок, в яких розміщене серверне обладнання. Для зручності нумерації і посилань у схемах ці стійки будемо позначати літерами A, B, C….

Кожна стійка містить приблизно 30 фізичних машин (x86-комп’ютери, які ми будемо називати «хостами» або «машинами»). Ці машини для загальної мережевої архітектури цікавлять нас менше, бо основна увага зосереджена на мережевих пристроях і зв’язках між ними.

У кожній стійці також встановлено комутатор верхнього рівня стояка — Top of the Rack (ToR), або в термінах топології Клоза — Leaf. Leaf-комутатор виконує роль точки агрегування трафіку для всіх підключених фізичних машин у стійці та забезпечує їх взаємодію з більш високими рівнями мережі.

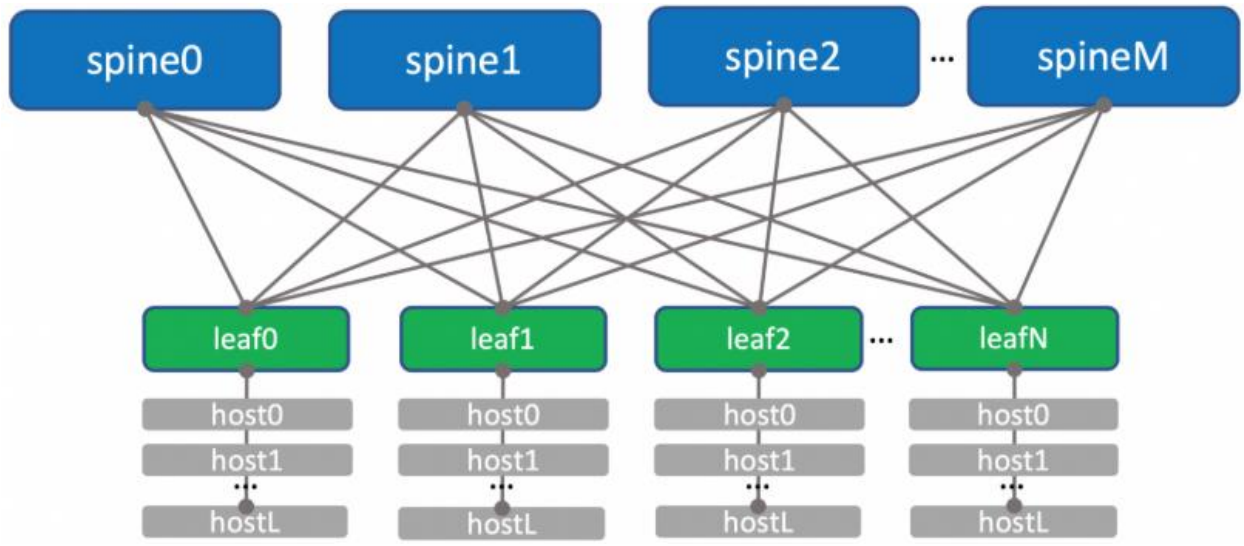


Рис. 3.1 Структура мережі

Іменування та роль пристроїв

Для уніфікованого іменування мережевих елементів використовуємо формат: **XXX-leafY**, де:

- **XXX** — трьохбуквене скорочення дата-центру,
- **Y** — порядковий номер комутатора у межах дата-центру.

Наприклад: kiev-leaf03.

У статтях ми часто будемо вживати терміни **Leaf** і **ToR** як синоніми, проте важливо пам’ятати різницю:

- **ToR** — фізичний комутатор у стійці, до якого підключаються всі хости;
- **Leaf** — логічна роль пристрою в мережі першого рівня у топології Клоза.

Іншими словами, Leaf ≠ ToR, хоча на практиці один і той самий пристрій може виконувати обидві функції. Наприклад, Leaf може бути End-of-Row комутатором у великому дата-центрі. Для спрощення викладу, в цій серії статей будемо іноді вживати їх як синоніми.

Агрегуючий рівень — Spine

Кожен Leaf-комутатор підключений до чотирьох комутаторів вищого рівня — Spine, які агрегують трафік і забезпечують зв’язність між різними Leaf. Для Spine у дата-центрі виділяється окрема стійка, і іменування аналогічне: XXX-spineY.

Підключення до зовнішніх мереж

У тій же стійці, що і Spine, встановлюється мережеве обладнання для зв’язності між дата-центрами, зазвичай два маршрутизатори з MPLS. За своєю функціональністю вони аналогічні ToR: Spine не відрізняє звичайний ToR із підключеними хостами від маршрутизатора для DCI — для нього всі пристрої просто форвардять пакети.

Спеціальні ToR-комутатори, що відповідають за підключення до зовнішніх мереж або між дата-центрами, називаються Edge-leaf, і іменуються XXX-edgeY.

Висновки по структурі

Отже, базова фізична мережа дата-центру виглядає наступним чином:

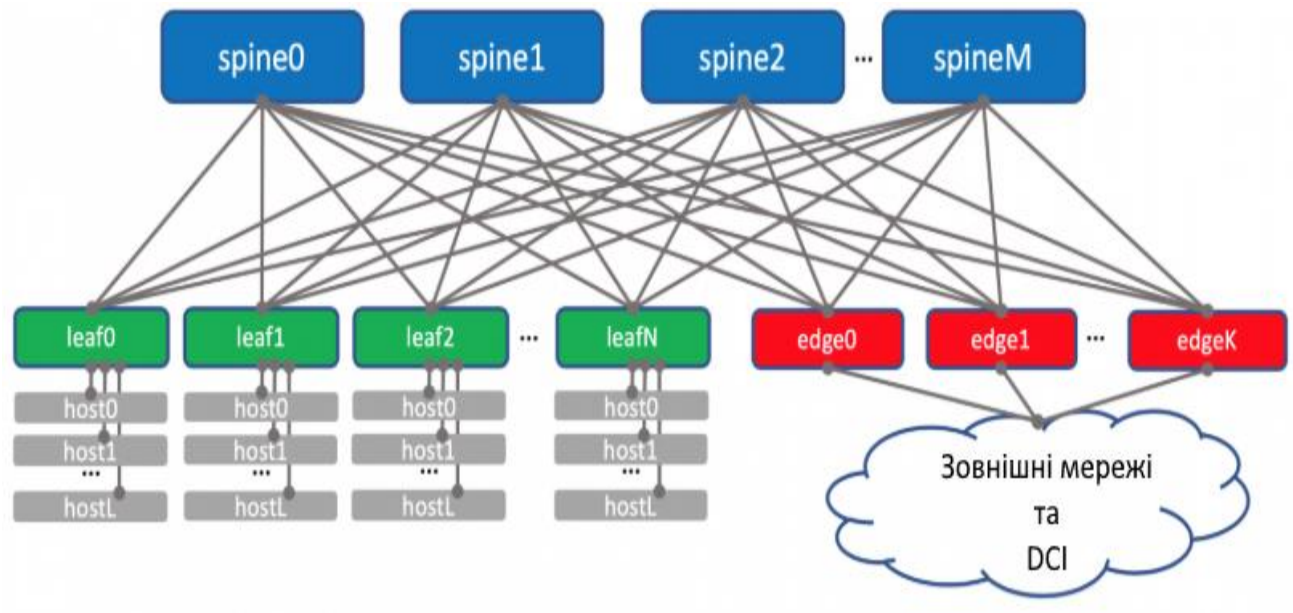


Рис. 3.2 Базова фізична мережа дата-центру

- **Leaf (ToR)** — комутатор у кожній стійці для підключення хостів;
- **Spine** — агрегуючий рівень для зв'язності між Leaf та оптимального маршрутизаційного розподілу;
- **Edge-leaf** — точки виходу для з'єднання з іншими дата-центрами та зовнішніми мережами.

Автоматизація та управління

Таке структурування мережі дозволяє ефективно впроваджувати автоматизацію:

- Налаштування Leaf і Edge-leaf можна централізовано керувати через контролер SDN;
- Spine-комутатори обробляють маршрутизацію без необхідності ручного налаштування кожного Leaf;
- Масштабування нових стоєк або хостів не потребує перебудови всього підключення, достатньо автоматично додати нові Leaf у топологію і оновити таблиці маршрутизації.

На представленій схемі Edge та Leaf дійсно розташовані на одному фізичному рівні. У класичних трирівневих мережах ми звикли, що аплінк (uplink) означає канал вгору, тобто підключення до вищого рівня ієрархії. У випадку з DCI (Data Center Interconnect) ситуація дещо інша: вихідний трафік йде «назад униз», що

порушує звичну логіку і трохи збиває з пантелику тих, хто працював з традиційними мережами.

У великих дата-центрах, які поділяються на менші логічні одиниці — POD'и (Point Of Delivery), створюють окремі Edge-POD для DCI та підключення до зовнішніх мереж. Це дозволяє ефективно розділяти внутрішню структуру дата-центру від точок виходу назовні, забезпечує більшу гнучкість у масштабуванні та спрощує автоматизацію управління мережею.

Функціонально Edge і Leaf виконують різні завдання, навіть якщо фізично вони можуть знаходитися на одному рівні. Leaf-комутатори відповідають за підключення серверних машин у стойці, керування локальним трафіком і взаємодію з нижнім рівнем хостів. Edge-комутатори або Edge-POD забезпечують маршрутизацію між дата-центрами та зовнішніми мережами, інтегруючись у централізовану систему SDN або інші платформи автоматизованого управління.

Такий підхід дозволяє не лише спростити роботу адміністратора мережі, але й автоматизувати більшість процесів управління трафіком: від конфігурації тунелів і VLAN до моніторингу та самовідновлення сервісів. Крім того, він забезпечує чітку ізоляцію між внутрішньою інфраструктурою та зовнішніми потоками, що критично для безпеки та масштабованості великих дата-центрів.

3.2 DCI та маршрутизація

Організація DCI через Edge-Leaf

Для забезпечення міждатацентрового зв'язку (DCI) ми використовуємо Edge-Leaf, які виступають як основні точки виходу в магістральну мережу. Саме через них трафік між дата-центрами потрапляє у глобальну мережу та повертається назад.

Для спрощення моделі припустимо, що дата-центри з'єднані прямими лінками, що дозволяє обмежитися розглядом лише внутрішньої зв'язності без врахування зовнішньої мережі. Я усвідомлюю, що кожне спрощення моделі — виключення компонентів, лінків чи сервісів — робить мережу менш складною для

навчальних і тестових цілей. В реальних умовах такі спрощення створюють додаткові складнощі та потребують «костилів» для підтримки стабільної роботи. Проте головна мета цього циклу — не вирішувати всі проблеми реальної мережі, а опрацювати та продемонструвати підходи до автоматизації, управління і проєктування масштабованих дата-центрів.

На Edge-Leaf реалізується шар underlay, який поміщається в VPN і транспортується через MPLS-магістраль. Це дозволяє надійно ізолювати внутрішній трафік дата-центру від зовнішнього, забезпечуючи безпеку та контроль над потоками даних. VPN-шари забезпечують окремі канали для кожного клієнта чи сервісу, що гарантує відсутність перетину даних різних користувачів.

В результаті отримуємо високорівневу логічну схему мережі: фізичні комутатори та маршрутизатори взаємодіють із віртуальними шарами, забезпечуючи ізоляцію клієнтських сервісів, централізоване управління та автоматизацію процесів.

Цей підхід не тільки спрощує адміністрування мережі, але й створює основу для масштабованої та гнучкої архітектури, здатної адаптуватися під різні сценарії навантаження, підключення нових дата-центрів і впровадження нових сервісів без необхідності перебудовувати всю фізичну мережу.

Автоматизація тут відіграє ключову роль: завдяки централізованому контролю можна швидко змінювати конфігурацію, оновлювати маршрутизацію та налаштовувати VPN-шари, не втручаючись вручну в кожен комутатор чи маршрутизатор. Це значно прискорює процеси розгортання нових сервісів і мінімізує людські помилки.

Маршрутизація

Для організації маршрутизації всередині дата-центру було обрано BGP як основний протокол обміну маршрутами. Це дозволяє ефективно керувати потоками даних між комутаторами Leaf і Spine, а також забезпечує гнучке масштабування мережі при додаванні нових стійок або серверних хостів. Використання BGP усередині ДЦ дозволяє централізовано управляти маршрутами, встановлювати політики фільтрації та пріоритизації трафіку, а також інтегруватися з

автоматизованими системами управління конфігураціями, що особливо важливо для великих мульти-тенантних середовищ.

Для магістральної мережі MPLS застосовується поєднання OSPF + LDP. OSPF відповідає за поширення інформації про топологію, тоді як LDP призначений для розподілу міток MPLS, необхідних для тунелювання трафіку між різними сегментами дата-центру. Таке рішення забезпечує надійне та передбачуване пересилання пакетів у магістральній частині мережі, дозволяє реалізувати балансування навантаження та підвищує відмовостійкість мережі.

Для організації DCI (Data Center Interconnect), тобто з'єднання між різними дата-центрами, використовується BGP L3VPN поверх MPLS. Це дозволяє створювати ізольовані маршрути для різних клієнтів і сервісів, зберігаючи при цьому прозору маршрутизацію між ДЦ. Такий підхід спрощує масштабування, підтримку мульти-тенантних середовищ і впровадження автоматизованих процесів управління мережею, включаючи перевірку та застосування конфігурацій через CI/CD-процеси.

Загальна схема маршрутизації та особливості

У L3-фабриці використання OSPF або ISIS обмежене, що пов'язано з концепцією централізованого управління і уникненням складних широкомасштабних протоколів, які автоматично обчислюють найкоротші маршрути. Це означає, що автоматичне виявлення сусідів (auto-discovery) та динамічне обчислення маршрутів відсутні. Всі маршрути, сусідства та політики маршрутизації налаштовуються централізовано, проте сам процес їх застосування автоматизований за допомогою скриптів, систем управління конфігурацією та контролерів SDN.

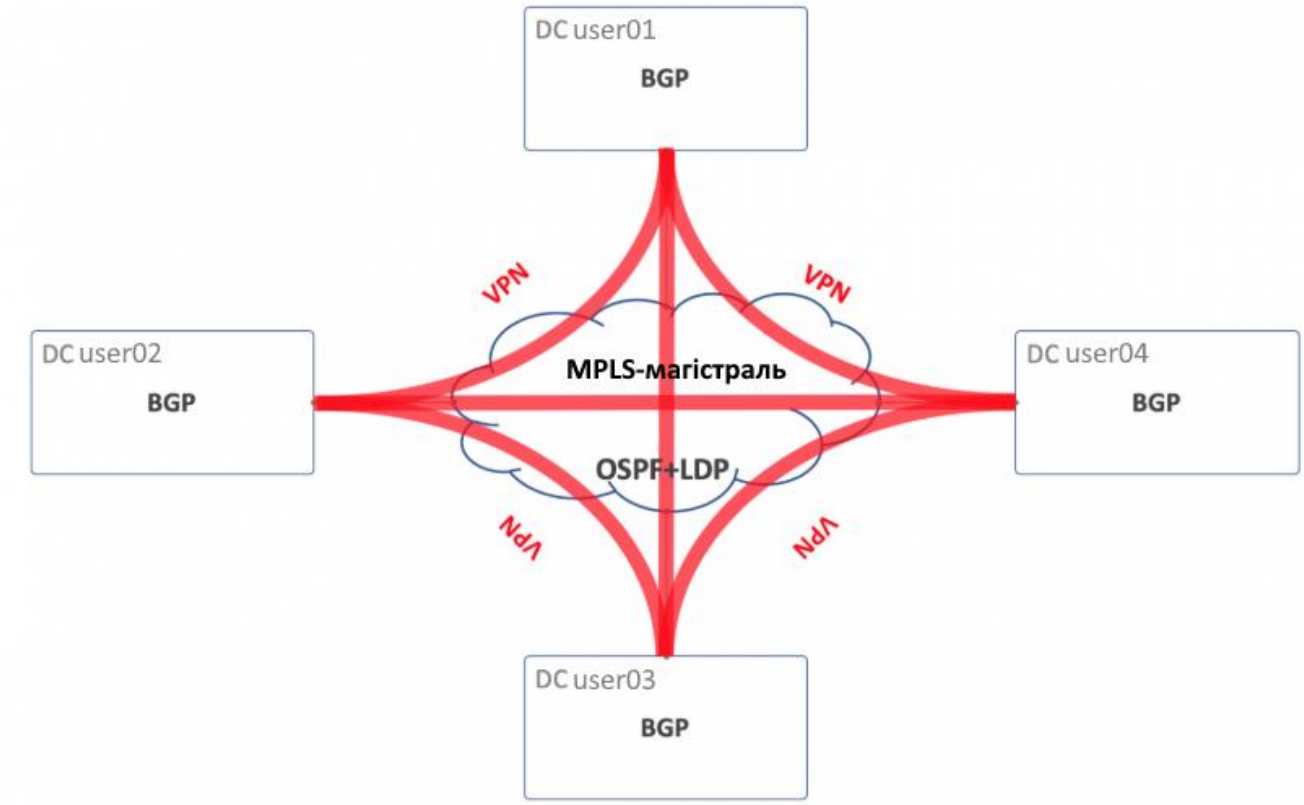


Рис. 3.3 Загальна схема маршрутизації

Таким чином, мережа залишається стабільною та передбачуваною, одночасно отримуючи гнучкість у керуванні конфігураціями. Кожна зміна — від додавання нових маршрутів до зміни політик трафіку — проходить через автоматизовані процеси тестування та деплойменту, що мінімізує ризик помилок і забезпечує безперебійну роботу сервісів.

Політики маршрутизації

На Leaf-комутаторах відбувається імпорт префіксів з фізичних інтерфейсів Underlay до протоколу BGP. Це дозволяє кожному Leaf-комутатору мати повну інформацію про підмережі в дата-центрі та маршрутизувати трафік ефективно і безпомилково. Кожна пара Leaf–Spine утворює BGP-сесію, в якій префікси Underlay анонсуються в обох напрямках, що забезпечує динамічну видимість топології і автоматичне перенаправлення трафіку у разі збоїв або змін мережі. Така архітектура також дозволяє рівномірно балансувати навантаження між маршрутами та забезпечує високу відмовостійкість.

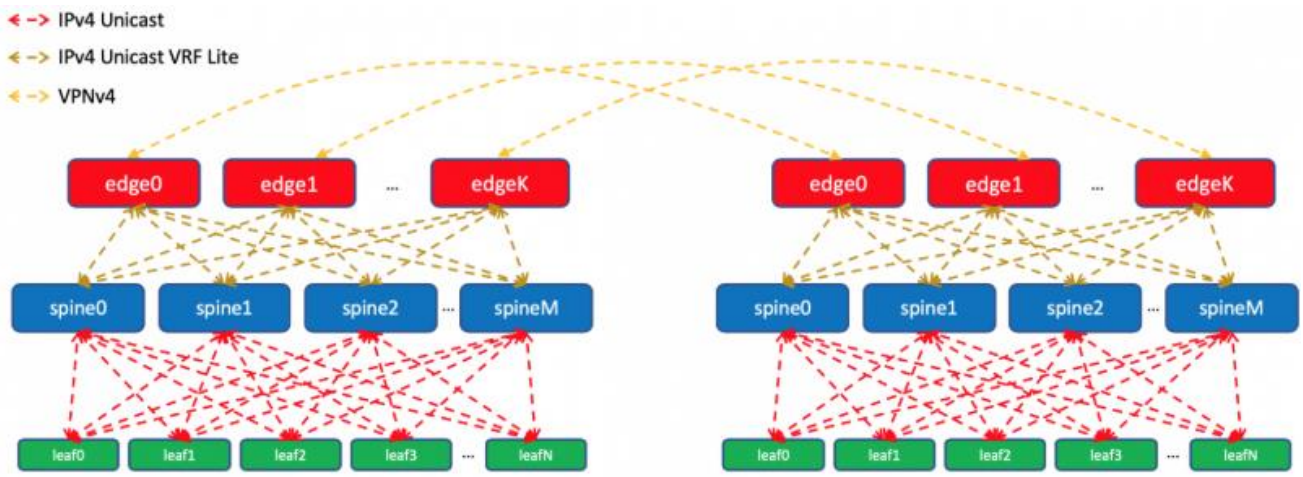


Рис. 3.4 Імпортовані префікси

Всередині одного дата-центру специфічні маршрути, імпортовані на ToR/Leaf, поширюються між усіма Leaf-комутаторами. На Edge-Leaf маршрути агрегуються та анонсуються в інші дата-центри, після чого спускаються до ToR-комутаторів віддалених ДЦ. Це забезпечує, що кожен ToR-комутатор точно знає, як дістатися до будь-якого іншого ToR у своєму дата-центрі, а також де знаходиться точка входу для маршрутизації до віддалених дата-центрів.

Для організації DCI (Data Center Interconnect) маршрути передаються як VPNv4. На Edge-Leaf інтерфейс у бік внутрішньої фабрики поміщається у VRF, який ми назвемо UNDERLAY, а BGP-сусідство зі Spine піднімається всередині цього VRF. Маршрути між Edge-Leaf комутаторами передаються в сімействі VPNv4. Така конфігурація дозволяє ізолювати внутрішні маршрути від зовнішніх, контролювати доступ і підтримувати безпечну маршрутизацію між дата-центрами.

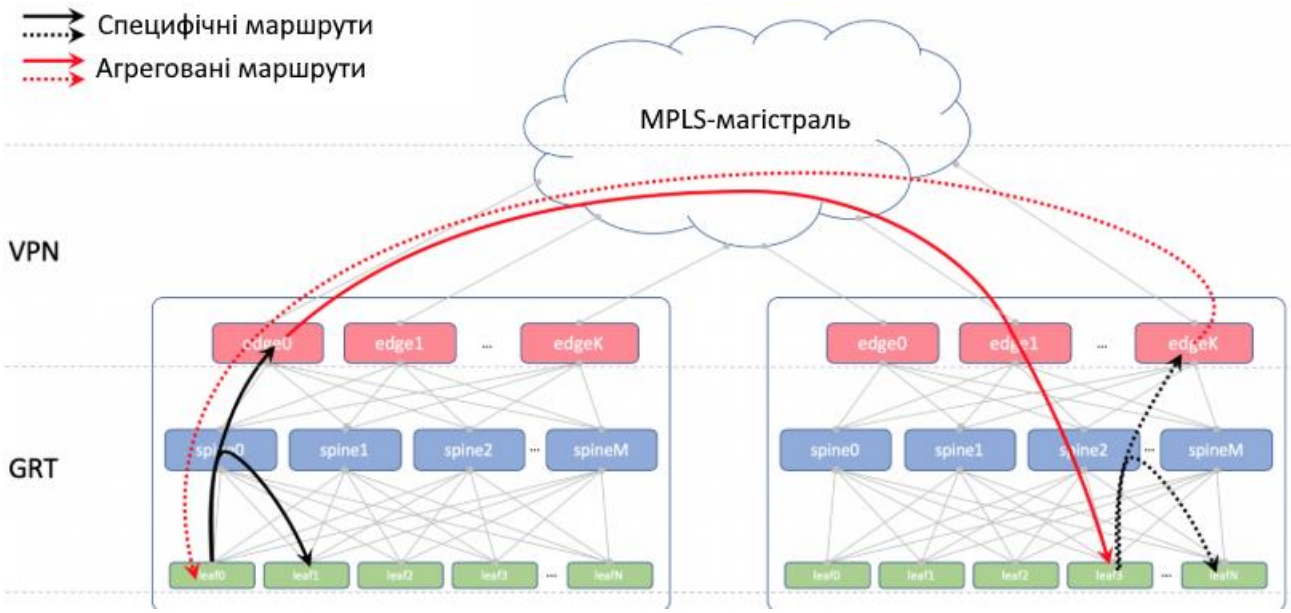


Рис. 3.5 Передача маршрутів як VPNv4 для організації DCI

Ця система політик маршрутизації дає ряд ключових переваг:

- **Ізоляція маршрутів**: внутрішні та зовнішні префікси відокремлені, що запобігає небажаному доступу і конфліктам адрес;
- **Агрегація маршрутів**: Edge-Leaf комутатори зменшують кількість префіксів у глобальній таблиці маршрутизації, оптимізуючи продуктивність мережі;
- **Автоматизація та контроль**: зміни в мережі можна легко інтегрувати в процеси CI/CD, що дозволяє швидко вносити конфігураційні правки і підтримувати актуальність топології;
- **Висока відмовостійкість**: у разі збою будь-якого маршруту або вузла, трафік автоматично перенаправляється по альтернативних шляхах без втрати доступності сервісів;
- **Простота управління**: централізоване управління маршрутизацією через Edge-Leaf дозволяє мінімізувати ручне втручання і помилки адміністраторів.

Крім того, такі політики дозволяють гнучко керувати трафіком клієнтів, вводити пріоритети для критичних сервісів і масштабувати мережу без порушення існуючих підключень.

3.3 Використання BGP ASN

Edge-Leaf ASN

У всіх комутаторах Edge-Leaf усіх дата-центрів використовується один і той самий ASN. Це робиться для того, щоб між Edge-Leaf-комутаторами можна було організувати iBGP-сесію, що дозволяє обмінюватися маршрутами всередині одного автономного системного простору без проблем, характерних для eBGP між різними ASN. У нашому прикладі для демонстрації використовується номер 65535. У реальних умовах це міг би бути публічний ASN, зареєстрований у відповідному регістрі.

Spine ASN

На рівні Spine у кожному дата-центрі використовується свій окремий ASN. Для прикладу ми починаємо з першого номера приватного діапазону ASN: 64512, 64513 і так далі. Такий підхід дозволяє зберегти чітке розмежування між маршрутизацією всередині окремого ДЦ та між ДЦ.

Причини використання ASN на рівні ДЦ

Це питання можна розділити на два аспекти:

1. Чому всі Spine одного ДЦ мають однаковий ASN?
2. Чому різні ДЦ мають різні ASN?

Однакові ASN на всіх Spine одного ДЦ

Розглянемо приклад AS-Path маршруту Underlay на Edge-Leaf

Якщо спробувати анонсувати цей маршрут назад на Spine, комутатор відкине його, адже ASN Spine вже присутній у шляху. Це дозволяє уникнути петель маршрутизації і забезпечує, що маршрути Underlay, підняті до Edge-Leaf, не повернуться вниз. Всі комунікації між хостами всередині ДЦ здійснюються на рівні Spine, що забезпечує контрольовану та безпечну маршрутизацію.

Різні ASN для різних ДЦ

Використання різних ASN у різних ДЦ дозволяє:

- ізолювати маршрути між дата-центрами;
- уникати конфліктів AS-Path при передачі маршрутів у DCI;

- забезпечити більш прозору та керовану політику маршрутизації між ДЦ;
- спростити інтеграцію з зовнішніми мережами та провайдерами.

Такий підхід дозволяє мережі залишатися стабільною та передбачуваною навіть при масштабуванні кількох дата-центрів, де одночасно працюють сотні або тисячі комутаторів і серверів.

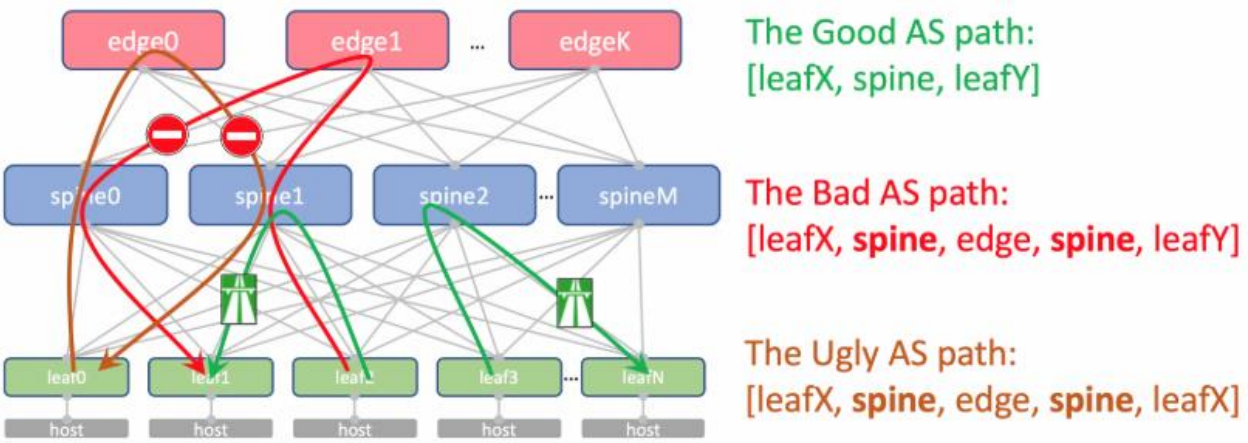


Рис. 3.6 Комунікація між хостами всередині ДЦ відбувається в межах спайнів

У контексті автоматизації мережі, чітке визначення ASN дозволяє програмним контролерам:

- автоматично конфігурувати BGP-сесії між Edge-Leaf та Spine;
- розподіляти маршрути з урахуванням ієрархії мережі;
- уникати ручної корекції конфігурацій, що значно зменшує ризик людських помилок;
- забезпечувати швидке масштабування мережі без порушення існуючих маршрутів.

Чому ASN повинні відрізнятися у різних дата-центрах

Іноді виникає потреба, щоб loopback'и сервісних віртуальних пристроїв були доступні з усіх дата-центрів. Наприклад, на одному з хостів у ДЦ може запускатися route-reflector або VNGW (Virtual Network Gateway), який анонсує свій loopback через BGP на локальний ToR/Leaf. Цей loopback має бути досяжний і в інших дата-центрах, отже маршрут проходить через всю інфраструктуру DCI.

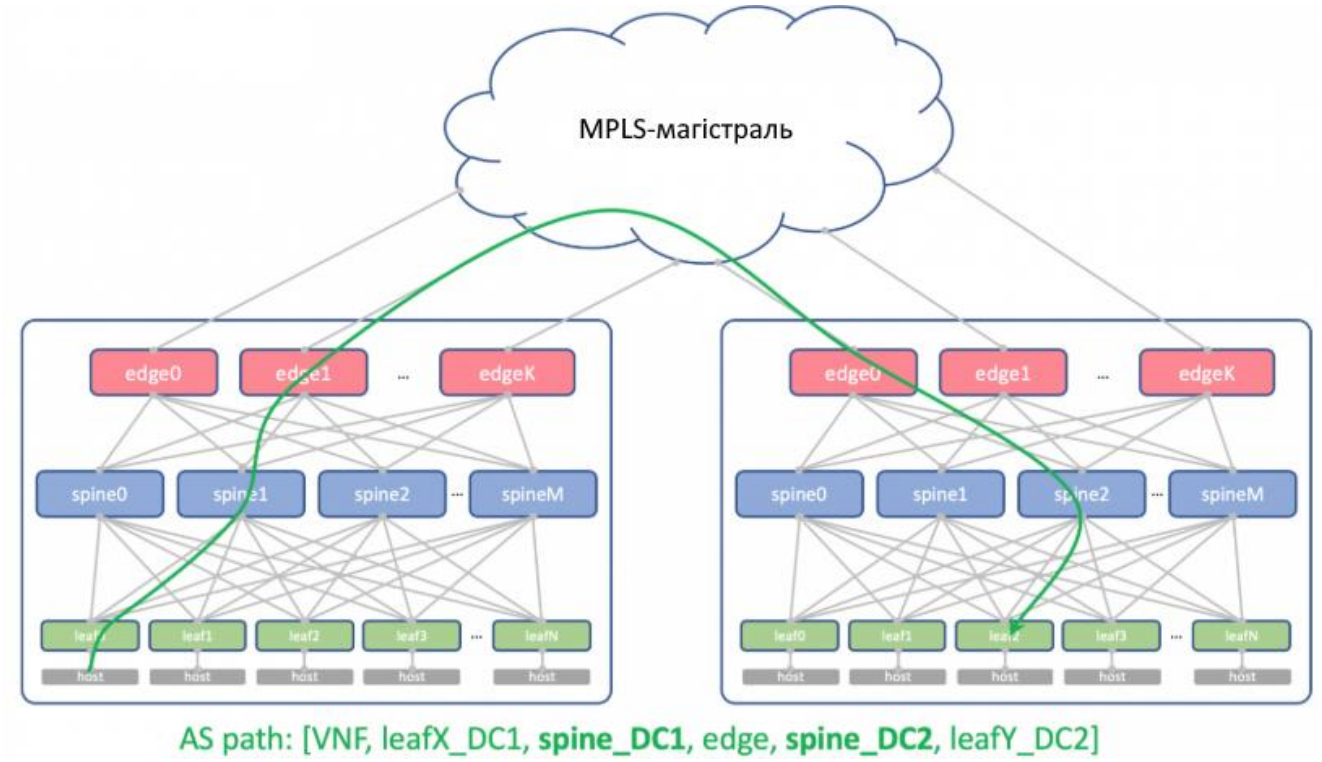


Рис. 3.7 Virtual Network Gateway

Нехай умовний AS-шлях для такого маршруту виглядає так:

[VNF_ASN, leafX_DC1_ASN, spine_DC1_ASN, edge_ASN, spine_DC2_ASN, leafY_DC2_ASN]

Щоб уникнути проблем із петлями в BGP, жоден ASN у цьому AS-Path не повинен повторюватися. В іншому випадку маршрут може бути відхилений або створювати складнощі в роботі протоколу.

Отже, отримуємо такі правила:

- Spine_DC1 і Spine_DC2 мають мати різні ASN;
- leafX_DC1 і leafY_DC2 також повинні належати до різних ASN.

Саме тому Spine у різних ДЦ отримують унікальні ASN, а для Edge-Leaf обирають один спільний ASN, щоб забезпечити коректне iBGP-сусідство між ними без складних налаштувань eBGP.

Чому не варто використовувати повторювані ASN

Інженери іноді вдаються до прийомів на кшталт allowas-in, які дозволяють маршрутам із повторюваними ASN проходити крізь BGP, всупереч стандартному механізму запобігання петлям. Такі рішення можуть застосовуватися у специфічних випадках, але вони:

- порушують стандартну логіку BGP та механізм запобігання петлям;
- ускладнюють трасування маршрутів та відстеження проблем;
- підвищують ризик некоректної маршрутизації та несподіваних відмов.

Особистий досвід показує, що використання подібних «хаків» часто призводить до складних і непередбачуваних наслідків у мережі.

Переваги підходу з різними ASN у різних ДЦ

1. **Запобігання петлям.**

   Різні ASN забезпечують унікальний AS-Path, і BGP автоматично відкидає потенційні петлі.

2. **Чіткість політик маршрутизації.**

   Різні ASN дозволяють однозначно визначати, з якого ДЦ прийшов маршрут і куди його направляти, без плутанини.

3. **Прозорість AS-Path.**

   Маршрути мають логічну структуру, легко простежити їх походження та призначення.

4. **Спрощення взаємодії між дата-центрами.**

   Різні ASN на Spine та Leaf забезпечують коректну агрегацію маршрутів і ефективну передачу трафіку між ДЦ.

Таким чином, призначення унікальних ASN для різних дата-центрів є ключовою практикою для забезпечення стабільності, надійності та коректності маршрутизації в масштабних мережах. Це дозволяє уникнути конфліктів і гарантує, що маршрути між хостами та сервісами у різних ДЦ передаватимуться безпечно та передбачувано.

4 АВТОМАТИЗАЦІЯ РОБОТИ З СЕРВЕРАМИ ЗА ДОПОМОГОЮ HEWLETT PACKARD ENTERPRISE SERVER AUTOMATION

4.1 Основні дані

HPE Server Automation — це потужне програмне рішення для централізованого управління серверною інфраструктурою, яке дозволяє виявляти, контролювати та налаштовувати фізичні та віртуальні сервери у корпоративній мережі. Система автоматично сканує мережу на наявність серверів, що ще не перебувають під управлінням, і формує спеціальний список таких пристроїв. Після цього адміністратор підключає сервери до системи, встановлюючи необхідні програмні модулі, що дозволяє вводити їх у керований пул і надавати повний спектр управлінських функцій.

Розгортання операційних систем та управління ресурсами

Система дозволяє виділяти фізичні ресурси на сервері або створювати віртуальні машини з попередньо налаштованими операційними системами, які одразу вводяться у керований пул серверів. Це означає, що нові ресурси стають готовими до використання та підпадають під централізоване управління. Такий підхід дозволяє стандартизувати середовище, зменшити ризики конфліктів у конфігураціях і прискорити підготовку нових серверних ресурсів.

Централізоване оновлення операційних систем

HPE Server Automation підтримує автоматизоване оновлення серверів, включно з встановленням патчів і нових версій ОС для Windows, Linux та Solaris. Адміністратор може вибирати патчі, які пропонує постачальник ОС, налаштовувати порядок їх встановлення, виключати несумісні оновлення, і таким чином забезпечувати стабільну роботу серверів без ризику збоїв.

Ініціалізація програмного забезпечення та шаблони конфігурацій

Після додавання серверів у керований пул можна встановлювати та налаштовувати додатки за допомогою Software Policies — спеціальних шаблонів, що визначають, яке ПЗ слід встановити, які конфігурації застосовувати і які скрипти

виконувати під час інсталяції. Це дозволяє стандартизувати базові конфігурації серверів і забезпечити єдину політику розгортання додатків на всіх керованих одиницях. Наприклад, можна автоматично встановлювати однакову версію Apache на всіх серверах або на визначеній групі серверів.

Аудит та відповідність політикам

Функція Audit and Remediation дає змогу перевіряти, чи відповідають сервери встановленим політикам конфігурації, і в разі виявлення невідповідностей автоматично їх виправляти. Це дозволяє підтримувати єдиний стандарт налаштувань на всіх серверах, уникати помилок ручного адміністрування та забезпечує стабільність і передбачуваність роботи інфраструктури.

Управління конфігураціями та стандартізація

Можна створювати шаблони конфігурацій додатків і розгортати їх на всіх керованих серверах. Крім того, HPE Server Automation дозволяє перевіряти відповідність конфігураційних файлів встановленим стандартам на всіх серверах у пулі, що значно підвищує узгодженість середовища та знижує ризики помилок при масштабуванні.

Розгортання комплексних додатків

Система забезпечує швидке та безпечне переміщення додатків від розробників до тестувальників і далі до експлуатаційного середовища, що дозволяє організаціям скоротити час впровадження нових сервісів і забезпечити їх стабільну роботу на всіх середовищах.

Перевірка відповідності програмного забезпечення

Інструмент Policy Compliance Scan дозволяє перевіряти, чи відповідає встановлене програмне забезпечення політикам конфігурації серверів. Це допомагає виявляти відхилення і підтримувати контроль за станом серверів у реальному часі.

Формування звітності

HPE Server Automation надає широкий спектр звітів про стан керованих серверів. Звіти можна гнучко налаштовувати та адаптувати для різних категорій

користувачів, що дозволяє адміністраторам і менеджерам отримувати точну та актуальну інформацію про стан інфраструктури.

Переваги системи

HPE Server Automation дозволяє безпечно та ефективно управляти змінами на серверах, моделювати та перевіряти зміни перед їх реальним застосуванням, зменшуючи час простою і ризик помилок. Це забезпечує стандартизацію, контроль та повний огляд стану серверної інфраструктури, що значно спрощує управління великими датацентрами та складними середовищами з великою кількістю фізичних і віртуальних серверів.

У результаті HPE Server Automation не тільки підвищує ефективність адміністративних операцій, але й забезпечує надійність, прогнозованість та контроль у керуванні серверною інфраструктурою будь-якого масштабу.

4.2 Конфігурація HPE Server Automation

HPE Server Automation (HPE SA) є потужним інструментом для централізованого управління серверною інфраструктурою підприємства, що охоплює фізичні та віртуальні сервери, а також складні мульти-оточення. Ця система дозволяє адмініструвати сервери на всіх етапах їхнього життєвого циклу, забезпечує контроль конфігурацій, безпечне оновлення операційних систем і додатків, аудит та відповідність корпоративним стандартам. Розглянемо детально ключові аспекти її функціонування.

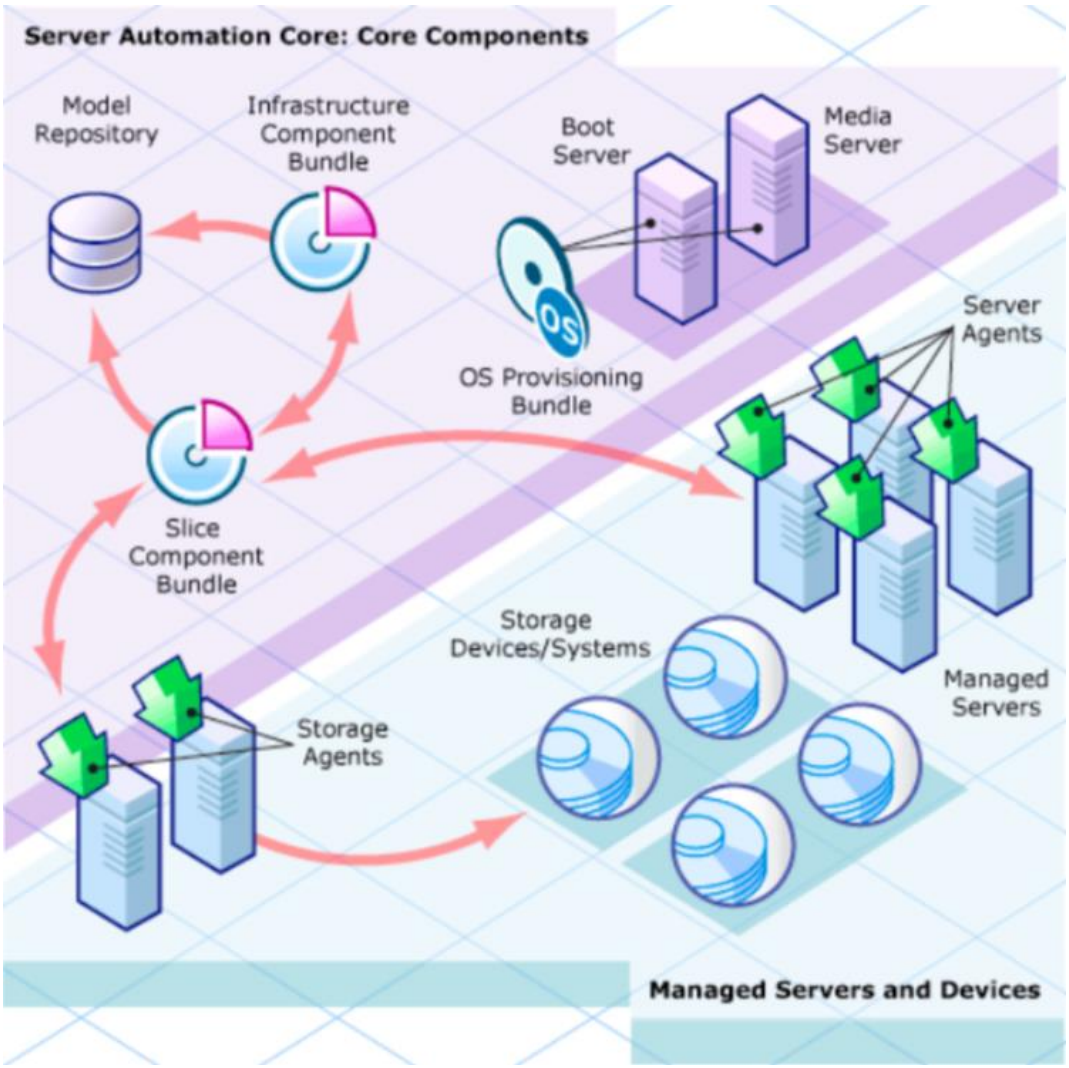


Рис. 4.1 Іллюстрація концептуальної структури можливостей конфігурованих параметрів

1. Виявлення та підключення серверів

Першим кроком у роботі HPE SA є сканування мережі для виявлення серверів, які ще не перебувають під управлінням системи. Система формує спеціальний список таких серверів, дозволяючи адміністраторам швидко визначати, які машини потребують інтеграції.

Після виявлення сервери підключаються до системи за допомогою встановлення програмних агентів, які дозволяють HPE SA виконувати управлінські завдання. Ці агенти забезпечують:

- управління фізичними ресурсами сервера;
- створення та управління віртуальними машинами;
- моніторинг стану операційних систем та встановлених додатків;

- автоматизоване застосування конфігурацій та патчів.

Цей процес дозволяє централізовано керувати великою кількістю серверів у датацентрах будь-якого масштабу.

2. Розгортання операційних систем та ресурсів

HPE SA надає можливість розгортання операційних систем на виділених ресурсах. Це може бути як фізичний сервер, так і віртуальна машина, створена поверх гіпервізора. Система дозволяє:

- виділяти фізичний простір на сервері для нових ОС;
- автоматично створювати ВМ з попередньо налаштованою ОС;
- інтегрувати нові сервери у керований пул, забезпечуючи їхню централізовану підтримку.

Крім того, HPE SA дозволяє проводити автоматичне оновлення операційних систем. Це стосується серверів під управлінням Windows, Linux та Solaris. Адміністратор може обирати, які патчі застосовувати, а система забезпечує їх централізоване, безпечне та гнучке встановлення, уникаючи несумісних оновлень.

3. Ініціалізація та управління програмним забезпеченням

Після включення сервера у керований пул можна виконувати установку та конфігурацію програмного забезпечення. Для цього використовуються спеціальні шаблони — Software Policies, які визначають:

- які програми будуть встановлені на сервері;
- конфігурації та параметри налаштування;
- скрипти, що застосовуються під час встановлення.

Ці політики дозволяють забезпечити уніфіковану базову конфігурацію серверів, яка застосовується до всіх керованих одиниць. Наприклад, можна встановити базову версію веб-сервера Apache або іншого корпоративного додатку на всі сервери одночасно, або на певну їх групу відповідно до ролі.

4. Аудит та відповідність стандартам

HPE SA включає модуль Audit and Remediation, що дозволяє перевіряти сервери на відповідність заданим політикам конфігурації та корпоративним

стандартам безпеки. Система може автоматично виявляти невідповідності та застосовувати необхідні зміни, щоб сервери відповідали встановленим критеріям.

Основні можливості цього модуля:

- аудит файлів, каталогів, конфігураційних параметрів;
- перевірка окремих серверів або цілих груп;
- створення розкладу для планових перевірок;
- автоматичне виправлення помилок та відновлення стандартного стану серверів.

За допомогою цих інструментів можна порівнювати конфігурації серверів з еталонними образами або іншими серверами у керованому пулі, оцінювати їх відповідність політикам і забезпечувати стандартизовану конфігурацію в усій інфраструктурі.

5. Управління додатками та версіями

Модуль Application Deployment дозволяє ефективно керувати всіма етапами життєвого циклу програмних продуктів:

- створення та тестування додатків;
- переміщення додатків від розробників до тестувальників та подальше розгортання;
- моделювання компонентів додатків, включно з кодом, скриптами та конфігураційними файлами;
- керування кількома паралельними версіями і релізами;
- розгортання та відкат версій на цільових серверах у разі виявлення помилок.

Це забезпечує контроль якості та стабільність роботи додатків на всіх серверах компанії.

6. Архітектура розгортання HPE SA

Простий пакет включає ядро системи та базу даних Oracle на одному сервері. Більш складні розгортання можуть мати:

- додаткові ядра, що підвищують продуктивність системи;
- сателіти, що дозволяють підключати віддалені датацентри або обмежені серверні середовища;

- Multi-master з’єднання, яке забезпечує синхронізацію даних між незалежними інстансами системи.

База даних Oracle використовується для зберігання повної інформації про сервери, операційні системи, додатки та конфігурації. Можна використовувати як базу з пакета інсталяції, так і вже існуючу Oracle-базу, налаштовану під HPE SA.

7. Комплексний аудит та відновлення

Функціонал Audit and Remediation дозволяє:

- порівнювати сервери та їхні образи з еталонними;
- виконувати планові та одноразові перевірки;
- встановлювати політики сумісності та безпеки;
- створювати спеціальні перевірки для окремих серверів чи груп;
- виправляти помилки на різних рівнях: файли, каталоги, патчі, ключі реєстру, пакети та інші компоненти.

Це гарантує, що всі сервери відповідають внутрішнім стандартам та корпоративним нормам.

4.3 Можливості Hewlett Packard Enterprise Server Automation

1. Візуалізація та моніторинг архітектури (Service Automation Visualizer, SAV)

Service Automation Visualizer (SAV) забезпечує глибоке та наочне уявлення про всю архітектуру IT-середовища, включно з фізичними та віртуальними серверами, мережевими пристроями, системами зберігання даних та розподіленими бізнес-додатками. Завдяки цій функціональності адміністратори можуть детально аналізувати взаємодію компонентів інфраструктури, що значно підвищує прозорість і контроль над IT-середовищем.

У контексті мережевої автоматизації SAV дозволяє:

- **Відстежувати взаємодію серверів через мережу**, визначати, які фізичні та віртуальні машини обмінюються даними, та як ці процеси впливають на пропускну здатність і затримки;

- **Візуалізувати маршрути та тунелі передачі даних** між ВМ та фізичними серверами, включно з конфігураціями VPN, VLAN, GRE- або VXLAN-тунелями, що дозволяє зрозуміти, які канали використовуються для внутрішньої та міждатацентрової комунікації;
- **Оцінювати вплив змін конфігурації на продуктивність і доступність мережевих ресурсів**, наприклад, при оновленні ОС, змінах мережевих політик або розгортанні нових сервісів;
- **Прогнозувати наслідки впровадження змін у мережевій інфраструктурі**, що дає змогу приймати більш обґрунтовані рішення та уникати непередбачуваних збоїв;
- **Оптимізувати планування автоматизації мережевих процесів**, включно з розподілом ресурсів, балансуванням навантаження та налаштуванням правил маршрутизації.

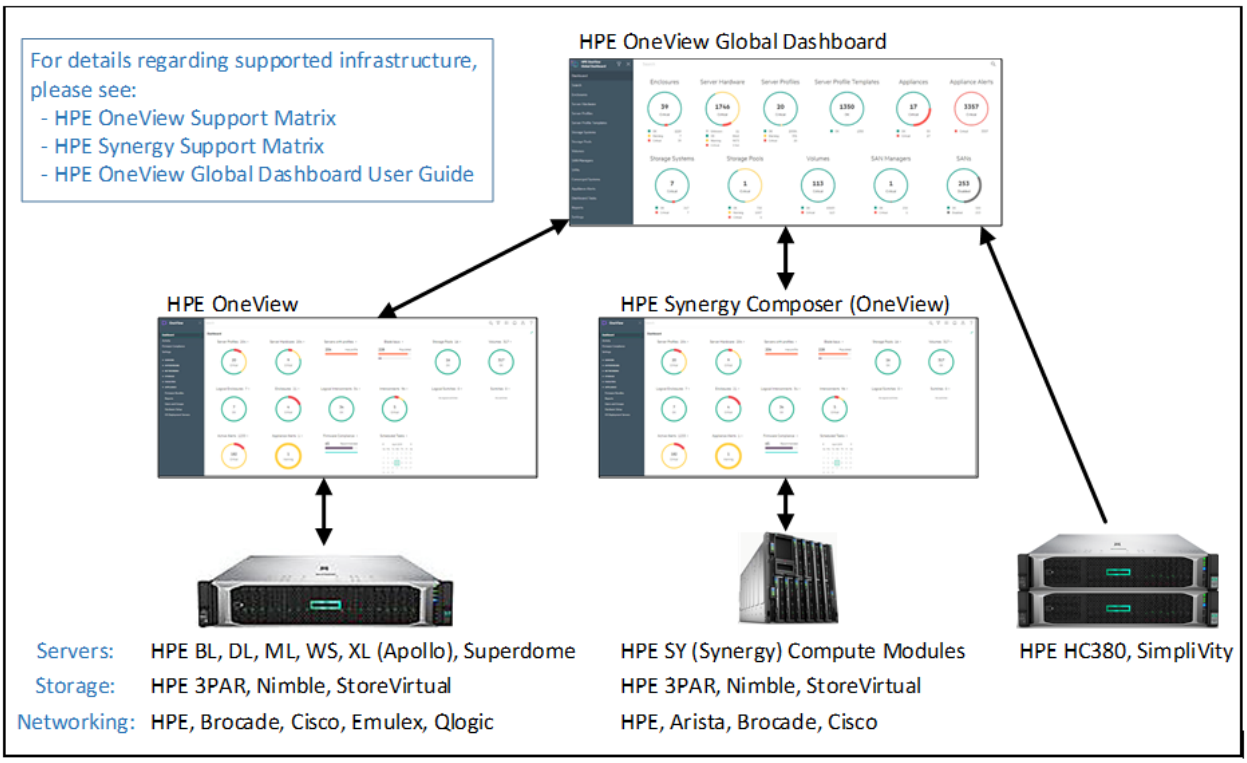


Рис. 4.2 Централізоване управління серверами та інтеграція з IT-інфраструктурою для ефективної автоматизації процесів

Таким чином, SAV не лише спрощує розуміння складної IT-інфраструктури, але й забезпечує ключовий інструмент для інтеграції автоматизації мережевих

процесів, дозволяючи системним адміністраторам ефективно контролювати взаємодію серверів, мережевих пристроїв і додатків у масштабних середовищах.

2. Автоматизація управління сховищами та видимість даних (Storage Visibility and Automation)

Цей інструмент надає можливість комплексного контролю за всім життєвим циклом даних: від моменту їх надходження в сховища до передачі через мережеву інфраструктуру. Для організацій, що прагнуть підвищити рівень автоматизації мережевих процесів, такі можливості є критично важливими, адже вони дозволяють:

- Отримувати детальну інформацію про завантаження мережевих каналів, що використовуються для передачі даних між серверами та сховищами, а також про їхню ефективність і можливі вузькі місця.
- Прогнозувати навантаження на мережу та оптимізувати пропускну здатність між сховищами та серверами, що дозволяє уникати перевантажень і забезпечує стабільність роботи систем.
- Автоматизувати численні рутинні операції, серед яких аудит використання ресурсів, резервне копіювання даних, контроль прав доступу, а також моніторинг і виявлення потенційних проблем у мережевому трафіку.
- Забезпечувати ефективне управління ресурсами та зменшувати навантаження на IT-персонал, дозволяючи йому зосередитися на більш стратегічних завданнях.
- Підвищувати прозорість та керованість IT-інфраструктури, оскільки адміністратори мають повну картину того, як дані переміщуються і обробляються у системі.
- Підтримувати безперервність роботи серверів та мережевих каналів, скорочувати час простою та зменшувати ризики втрати даних.
- Забезпечувати гнучкість та масштабованість, дозволяючи легко інтегрувати нові ресурси та модернізувати існуючі компоненти мережевої та серверної інфраструктури.

Таким чином, використання Storage Visibility and Automation не лише підвищує ефективність роботи сховищ і мережевих ресурсів, але й є ключовим фактором у процесі планування, оптимізації та автоматизації IT-процесів у сучасних організаціях.

3. Система звітності (Reports)

HPE SA надає вичерпні звіти щодо:

- стану серверів, мережевих пристроїв та додатків;
- використання патчів, ОС та мережевих політик;
- дій користувачів та дотримання стандартів безпеки.

У мережевій автоматизації це дозволяє:

- відслідковувати, які маршрути або мережеві політики застосовуються на конкретних серверах;
- виявляти вузькі місця у пропускній здатності та продуктивності;
- оцінювати ефективність автоматичних процесів, що керують потоками даних.

4. Автоматичне розгортання ресурсів та операційних систем

Система дозволяє швидко та стандартизовано встановлювати ОС на фізичні та віртуальні сервери, інтегруючи процеси розгортання з мережею та іншими сервісами. Вплив на автоматизацію мереж:

- при розгортанні ВМ або фізичних серверів автоматично конфігуруються мережеві параметри, включаючи IP-адресацію та підключення до VLAN;
- забезпечується єдина політика мережевих налаштувань для всіх серверів, що скорочує ризик помилок;
- інтеграція з функціями управління патчами та програмним забезпеченням дозволяє оновлювати мережеві елементи без ручного втручання.

5. Виконання скриптів та автоматизація завдань

Модуль Run Scripts дозволяє запускати сценарії на багатьох серверах одночасно, що критично для масштабної автоматизації мережевих процесів:

- налаштування мережевих політик та правил маршрутизації на численних серверах і віртуальних машинах;

- синхронне оновлення конфігурацій мережевих інтерфейсів та firewall-політик;
- контроль доступу та журналювання дій для безпечного застосування змін у мережевому середовищі.

6. Інформація про пристрої та аудит (Device Explorer)

Інструмент дозволяє відстежувати стан серверів і мережевих компонентів, їх конфігурації та історію змін. Це сприяє:

- автоматичному збору інформації для налаштування мережевих правил;
- перевірці відповідності мережевих налаштувань корпоративним стандартам;
- підготовці звітів для планування змін у мережевій архітектурі.

7. Управління віртуалізацією та інтеграція з мережами

HPE SA інтегрується з VMware vCenter, Microsoft SCVMM та OpenStack, що дозволяє:

- автоматично створювати віртуальні машини з необхідними мережевими параметрами;
- керувати підключенням ВМ до віртуальних мереж та VLAN;
- забезпечувати відповідність корпоративним та нормативним мережевим політикам;
- швидко виявляти проблеми у віртуалізованих мережевих середовищах.

8. Виявлення серверів без агента та їх інтеграція у мережу

Ця функція дозволяє:

- автоматично знаходити сервери без HPE SA агента;
- встановлювати агенти та інтегрувати їх у централізоване управління;
- автоматично підключати нові сервери до мережевих політик і конфігурацій.

В результаті мережеві процеси, включно з маршрутизацією, безпекою та обміном даними, стають автоматизованими, а адміністратори отримують контроль над усім середовищем.

Вплив HPE Server Automation на автоматизацію мереж

Завдяки комплексним функціям, HPE SA дозволяє:

1. **Централізоване управління мережевими параметрами** для фізичних і віртуальних серверів.
2. **Стандартизацію конфігурацій мережевих інтерфейсів** та VLAN у великих дата-центрах.
3. **Автоматичне оновлення та поширення політик безпеки** по всій інфраструктурі.
4. **Інтеграцію управління серверами та мережевою архітектурою**, що зменшує людський фактор і прискорює процеси.
5. **Візуалізацію та аудит мережевих потоків**, що допомагає планувати розширення та оптимізацію мереж.

В результаті HPE Server Automation не лише оптимізує серверне управління, але й значно підвищує рівень автоматизації мереж, зменшує витрати часу на ручні налаштування та підвищує стабільність роботи всіх IT-сервісів.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було проведено комплексне дослідження методів та інструментів оптимізації процесів автоматизації у сучасних телекомунікаційних мережах. Аналіз охоплював як традиційні, так і віртуалізовані мережеві інфраструктури, а також підходи до управління сервісами, конфігураціями та дата-центрами.

Було встановлено, що впровадження систем моніторингу та самовідновлення сервісів дозволяє значно підвищити надійність та стійкість мереж, скоротити час простою і мінімізувати ризики людських помилок. Використання системи управління IP-адресами (IPAM) та системи опису мережевих сервісів забезпечує централізоване управління ресурсами та автоматичне відображення актуального стану мережевої інфраструктури.

Розробка механізмів ініціалізації пристроїв та доставки конфігурації на основі вендор-агностичних моделей дозволяє уніфікувати налаштування обладнання різних виробників, що значно прискорює розгортання мережевих сервісів і знижує операційні витрати. Основні переваги автоматизованої доставки конфігурацій включають підвищену ефективність управління, зменшення ручної роботи та підвищення стабільності мережевих сервісів.

Дослідження технологій віртуалізації, таких як GRE, IP-in-IP, MPLS, MPLS L2/L3VPN, VXLAN, GENEVE, MPLSoverUDP та MPLSoverGRE, показало, що їх інтеграція в автоматизовані мережі дозволяє створювати ефективні оверлейні мережі з можливістю гнучкого масштабування та ізоляції трафіку. Використання концепції Underlay та Overlay у поєднанні з VNF (Virtual Network Function) забезпечує гнучке розгортання сервісів, оптимізацію внутрішньої топології дата-центрів та підвищення продуктивності мережевих функцій.

Було також проаналізовано організацію DCI через архітектуру Edge-Leaf та використання протоколів маршрутизації BGP ASN, що дозволяє ефективно з’єднувати дата-центри та забезпечувати надійну маршрутизацію між ними. Крім того, автоматизація роботи з серверами за допомогою HPE Server Automation

дозволяє централізовано керувати апаратними та програмними ресурсами, підвищуючи ефективність обслуговування серверної інфраструктури.

Таким чином, реалізація комплексної системи автоматизації у телекомунікаційних мережах дозволяє досягти високої ефективності, надійності та гнучкості управління інфраструктурою. Впровадження описаних методів та технологій є ключовим фактором для оптимізації процесів адміністрування, скорочення операційних витрат та забезпечення безперебійного функціонування сучасних телекомунікаційних систем.

ПЕРЕЛІК ПОСИЛАНЬ

1. Альошин Г. В., Панченко С. В., Приходько С. І. Оптимізація цифрових систем передачі: Підручник. – Харків: УкрДУЗТ, 2019. – 142 с.
2. Голь В. Д. Телекомунікаційні та інформаційні мережі: Навчальний посібник. – Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2021. – 250 с. телекомунікаційних мереж, з акцентом на автоматизацію процесів.
3. Хорольський В. П., Коренець Ю. М. Автоматизація виробничих процесів: Підручник. – Кривий Ріг: ДонНУЕТ, 2022. – 400 с.
4. Микитишин А. Г., Міщенко М. М. Телекомунікаційні системи та мережі: Навчальний посібник. – Львів: Львівська політехніка, 2020. – 300 с.
5. Микитишин А. Г., Міщенко М. М. Телекомунікаційні системи та мережі: Навчальний посібник. – Львів: Львівська політехніка, 2020. – 300 с.
6. Візір Ю. С. Інформаційні технології в телекомунікаціях: Навчальний посібник. – Харків: ХНУРЕ, 2023. – 350 с.
7. Васильківський М. Оптимізація інтелектуальних телекомунікаційних мереж. – Вісник Хмельницького національного університету, 2023.
8. Радзівілов Г. Д., Дєгтяр О. А., Безносенко С. Ю., Ткаченко А. Л. Сучасні можливості управління мобільними телекомунікаційними мережами з використанням безпілотних літальних апаратів. – Комп'ютерно-інтегровані технології, 2024.
9. Хлапонін Ю. І. Аналіз та моніторинг телекомунікаційної мережі на основі статистичних методів. – CEUR Workshop Proceedings, 2016.
10. Нікітіна Л. О. ІТ та технології штучного інтелекту у підготовці фахівців з телекомунікацій. – Сучасні наукові дослідження, 2023.
11. Візір Ю. С. Збірник наукових статей кафедри комп'ютерно-інтегрованих технологій. – Харків: ХНУРЕ, 2024.
12. Недацьківський О. Л. Перспективні компоненти та засоби інфокомунікаційних мереж. – ДУІКТ, 2020.

13. Забродський А. І. Вдосконалення лінії ВОЛЗ у телекомунікаційних мережах. – Телекомунікаційні системи та мережі, 2023.
14. Вельчко В., Войнова С., Граняк В., Іванова Л., Котлик С., Кудряшова А., Кунуп Т., Малахов К., Піх І., Пунченко Н., Сенківський В., Сергєєва О., Соколова О., Федосов С., Хошаба О., Цира О., Чаплінський Ю., Гурський О., Завертайло К., Котлик Д. Нові інформаційні технології, моделювання та автоматизація. – 2023.
15. Мата Х., де Мігель І., Дюран Р. Х., Мерайо Н., Сінгх С. К., Юкан А., Чамання М. Методи штучного інтелекту в оптичних мережах: Комплексний огляд. – 2018.
16. Лежнюк П. Д. Технологія структурного проектування технологічних комплексів. – 2012.
17. Мата Х., де Мігель І., Дюран Р. Х., Мерайо Н., Сінгх С. К., Юкан А., Чамання М. Методи штучного інтелекту в оптичних мережах: Комплексний огляд. – 2018.
18. Мата Х., де Мігель І., Дюран Р. Х., Мерайо Н., Сінгх С. К., Юкан А., Чамання М. Методи штучного інтелекту в оптичних мережах: Комплексний огляд. – 2018.
19. Resende, M. G. C., & Pardalos, P. M. (Eds.). (2006). Handbook of Optimization in Telecommunications. Springer.
20. Sun, X. M. (2022). Control and Optimization Based on Network Communication. Springer.
21. Kibria, M. G., Nguyen, K., Villardi, G. P., Zhao, O., Ishizu, K., & Kojima, F. (2017). Big Data Analytics, Machine Learning and Artificial Intelligence in Next-Generation Wireless Networks.
22. Adamuz-Hinojosa, O., Ordonez-Lucena, J., Ameigeiras, P., Ramos-Munoz, J. J., Lopez, D., & Folgueira, J. (2018). Automated Network Service Scaling in NFV: Concepts, Mechanisms and Scaling Workflow.
23. El Rajab, M., Yang, L., & Shami, A. (2023). Zero-Touch Networks: Towards Next-Generation Network Automation.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ

КВАЛІФІКАЦІЙНА РОБОТА

ОПТИМІЗАЦІЯ ПРОЦЕСІВ АВТОМАТИЗАЦІЇ У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

ВИКОНАВ:
СТУДЕНТ ГРУПИ ТСДМ-61
ІЛЛЯ БУЛАВІН

МЕТА РОБОТИ ТА АКТУАЛЬНІСТЬ

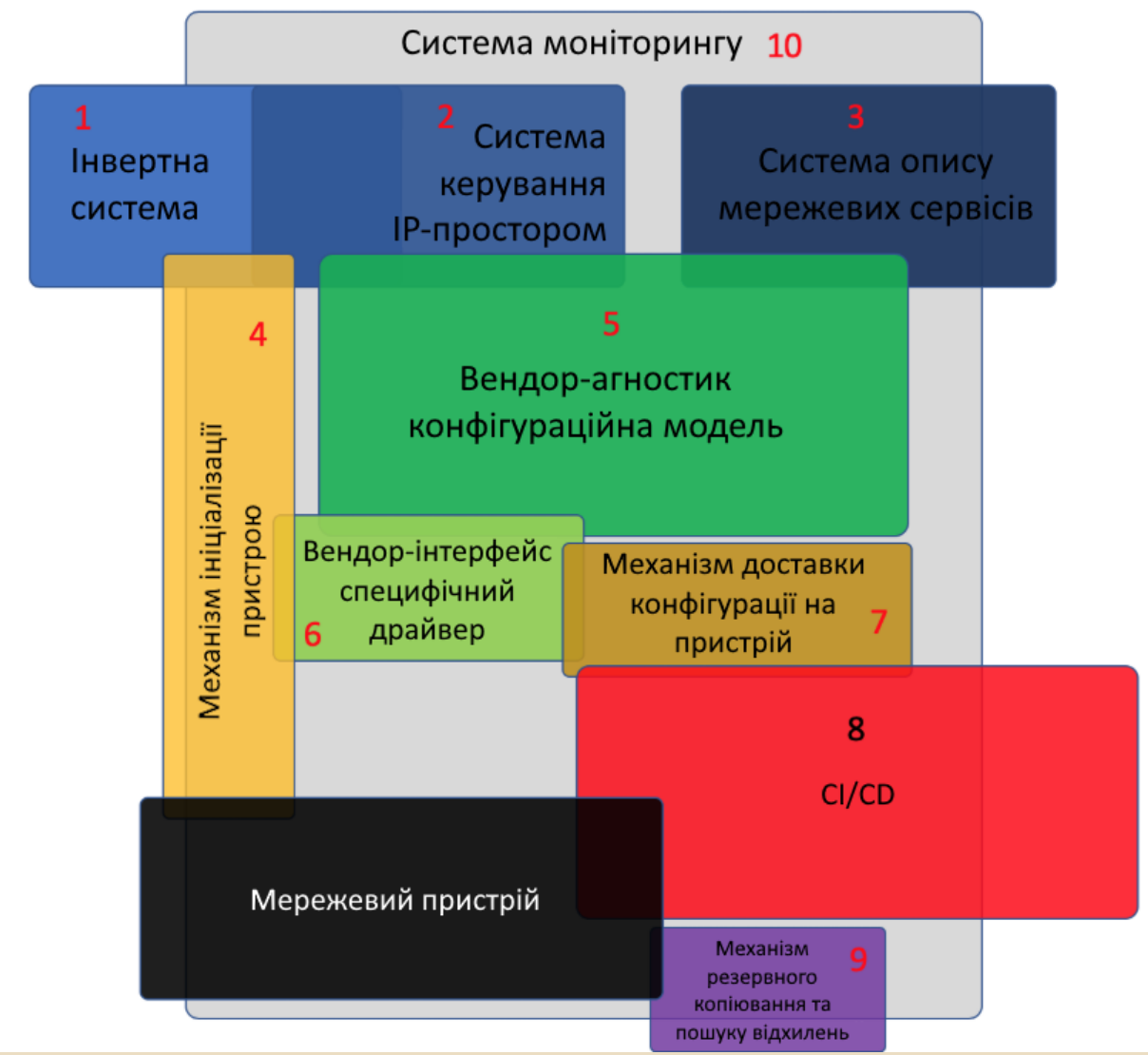
- Мета роботи – підвищення ефективності управління телекомунікаційними мережами шляхом впровадження методів автоматизації процесів конфігурації, моніторингу та самовідновлення сервісів на основі сучасних технологій віртуалізації, стандартизованих протоколів управління та концепцій CI/CD.
- Об’єкт дослідження – елекомунікаційна мережа як складна розподілена система, що включає фізичну (underlay) та віртуальну (overlay) інфраструктури, а також системи керування, моніторингу та забезпечення надійності її функціонування.
- Предмет дослідження – методи та засоби автоматизації управління телекомунікаційними мережами.

Актуальність.

- У сучасних телекомунікаційних системах постійно зростають обсяги трафіку, кількість мережевих пристроїв та складність архітектури. Це вимагає переходу від ручного керування до повної автоматизації процесів конфігурації, моніторингу та самовідновлення мереж. Запропонована в роботі тематика є актуальною, оскільки відповідає світовим тенденціям розвитку SDN (Software Defined Networking), NFV (Network Function Virtualization), CI/CD-процесів та вендор-незалежних моделей управління мережею. Розробка комплексних методів автоматизації дозволяє зменшити людський фактор, підвищити надійність сервісів і забезпечити масштабованість телекомунікаційних інфраструктур, що є критично важливим для операторів зв’язку та корпоративних дата-центрів.

ПЛАНУВАННЯ МЕРЕЖІ

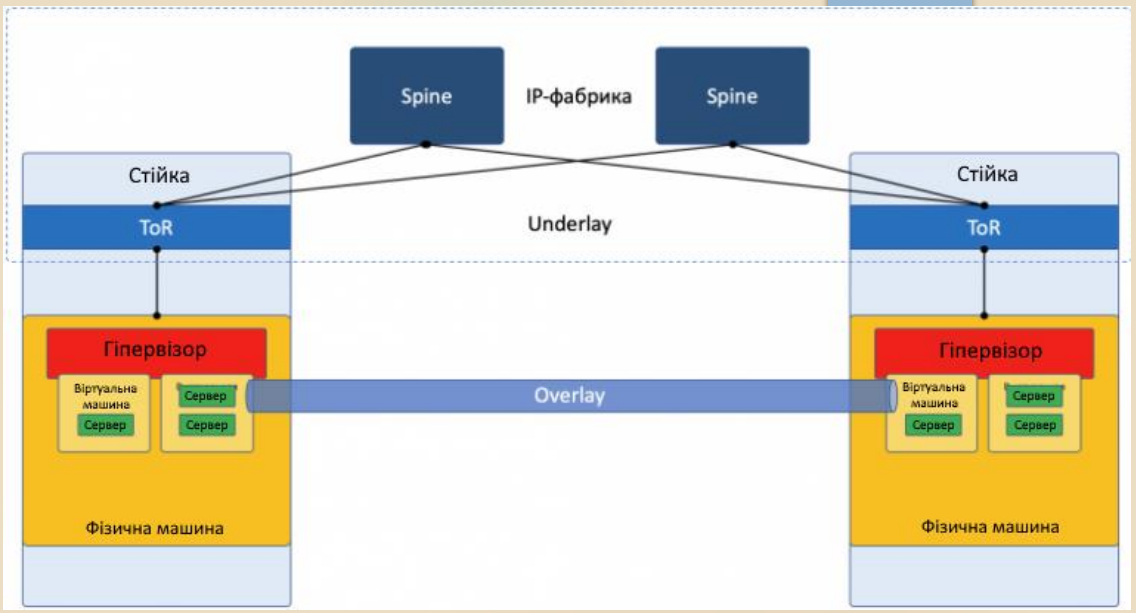
- Сучасні телекомунікаційні мережі управляються як єдина інтегрована система, а не окремі пристрої, що підвищує ефективність і зменшує людські помилки. Автоматизація, CI/CD, тестування конфігурацій і версіонування забезпечують безпечне впровадження змін. Системи інвентаризації (DCIM) та управління IP-адресами (IPAM) централізують дані про пристрої, топологію та ресурси, дозволяючи швидко застосовувати стандартизовані конфігурації. Система опису мережевих сервісів уніфікує налаштування інфраструктурних і клієнтських сервісів. Механізми ініціалізації та вендор-агностична конфігураційна модель забезпечують швидке, масштабоване та безпечне підключення пристроїв. Моніторинг і Self-Healing гарантують стабільність мережі та сервісів.



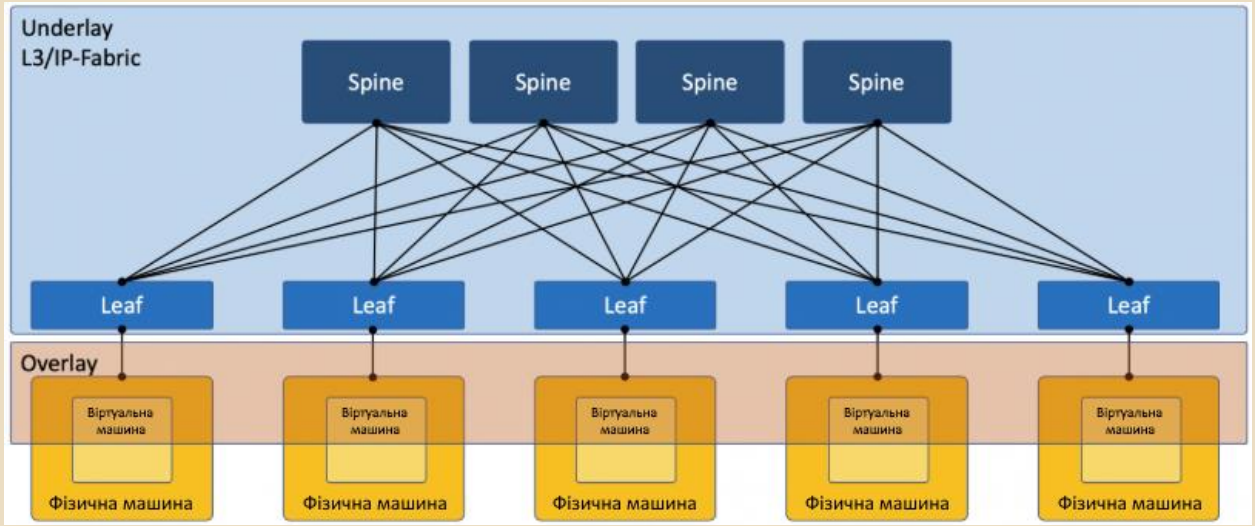
Зображено усі компоненти та власне пристрій. Пересічні компоненти взаємодіють один з одним. Чим більше блок, тим більше уваги потрібно приділити цьому компоненту

ТЕХНОЛОГІЇ ВІРТУАЛІЗАЦІЇ В АВТОМАТИЗОВАНИХ МЕРЕЖАХ

- Мережа — основа інфраструктури: будь-які зміни можуть паралізувати сервіси. Щоб зменшити ручне налаштування та ризики, застосовують оверлейні мережі (GRE, VXLAN, MPLS VPN), які накладаються на фізичну Underlay. Overlay дозволяє налаштовувати лише кінцеві вузли, приховуючи топологію від транзитних пристроїв, спрощує таблиці маршрутизації та підвищує масштабованість. Автоматизація забезпечує централізоване управління, швидке розгортання сервісів, контроль продуктивності і самовідновлення. Underlay — стабільна фізична мережа; Overlay — логічна мережа для ізоляції тенантів і гнучкого масштабування. Разом вони дозволяють ефективно управляти сучасними дата-центрами.



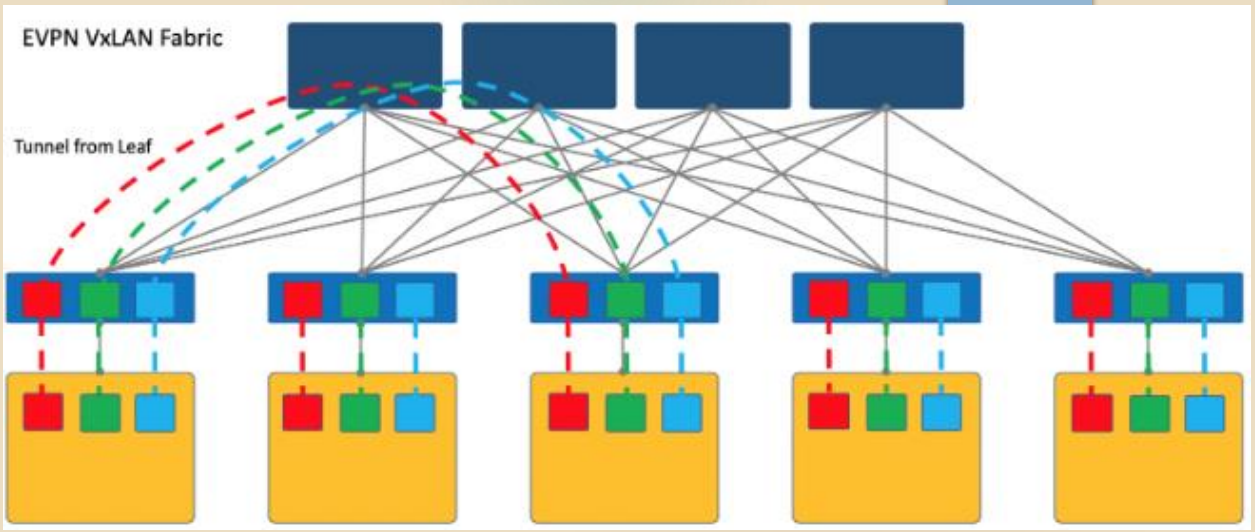
Приклад віртуалізації мережі



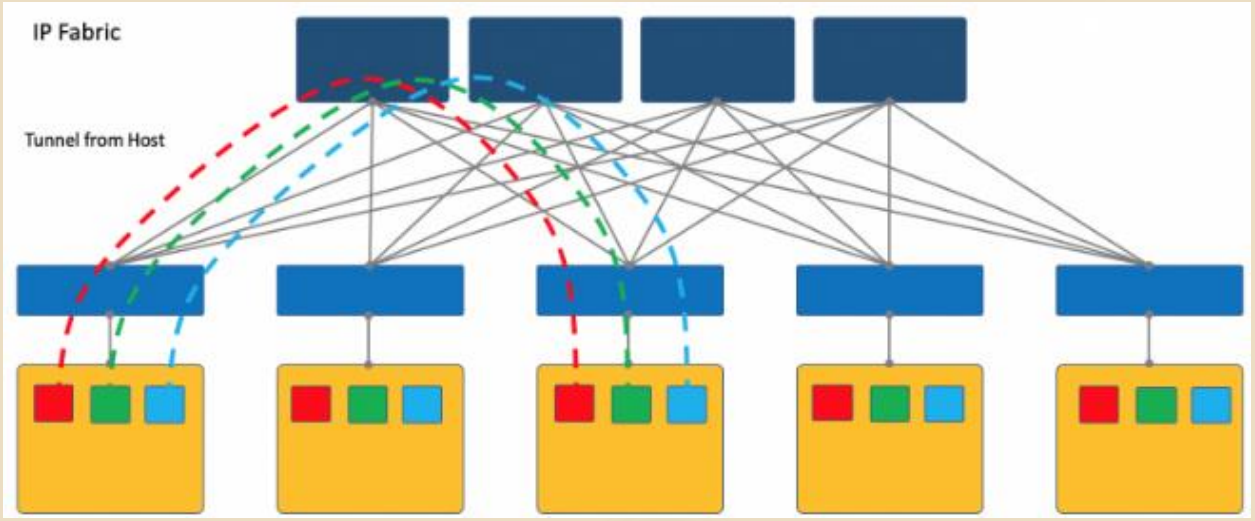
Дві частини – Underlay та Overlay

Варіанти розгортання Overlay

- Існують два підходи до організації Overlay у дата-центрах. **Overlay на ToR** починається на комутаторі доступу: ToR ізолює трафік різних сервісів і тенантів, керується централізовано через SDN, забезпечує масштабованість, багатотенантність і контроль політик безпеки. Недоліки — складність налаштування та потреба взаємодії з адміністраторами ВМ. **Overlay на хості** створюється і завершується безпосередньо на серверах: логіка інкапсуляції, маршрутизації і політик безпеки переноситься на хости. Переваги — простіші ToR, мультивендорна сумісність, швидке масштабування та автоматизація Overlay без втручання у фізичну мережу.



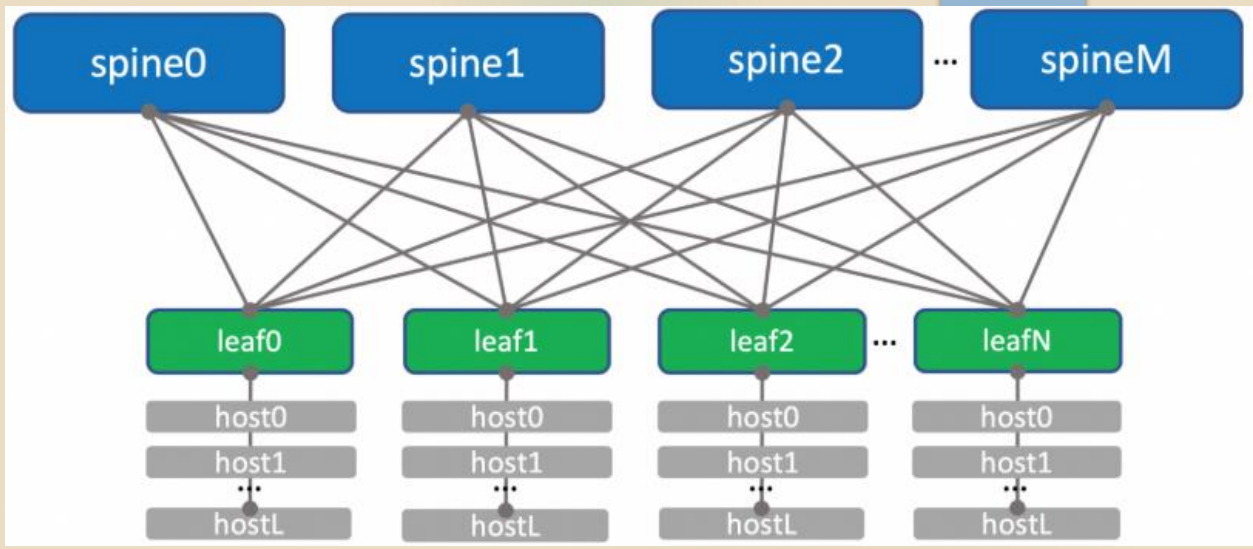
Overlay на ToR-комутаторі



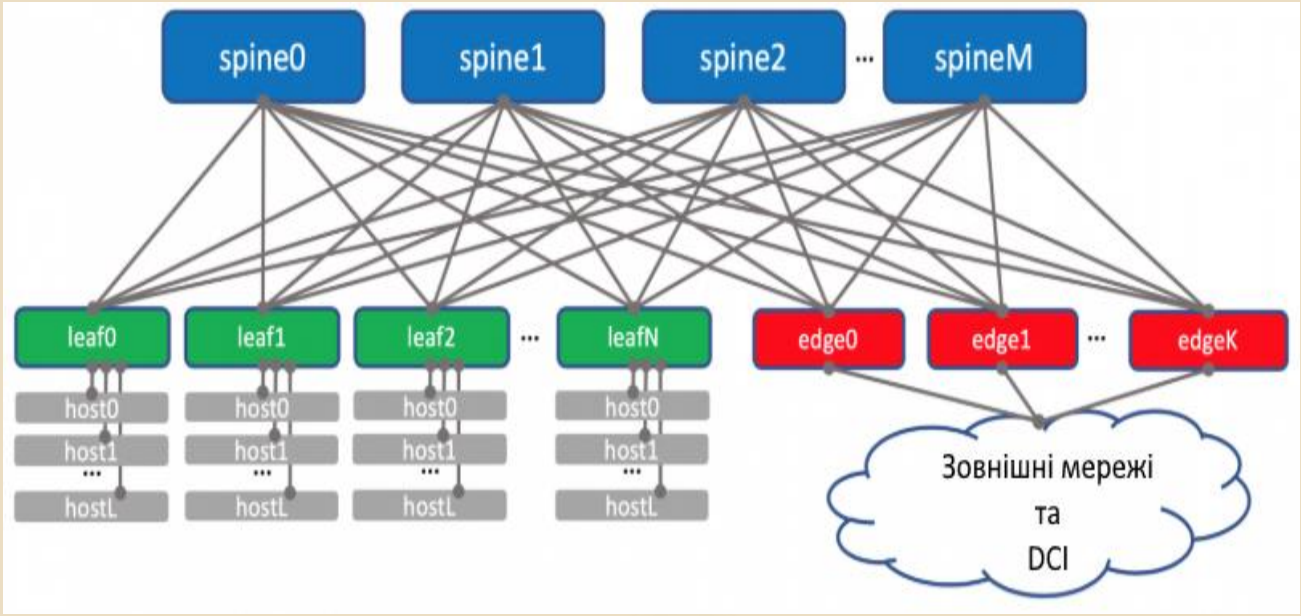
Overlay з хоста

Внутрішня топологія дата-центрів

- Сучасні дата-центри будуються за топологією Клоза для високої доступності та рівномірного навантаження. Кожна стійка містить ~30 серверів та ToR-комутатор (Leaf), що агрегує трафік хостів і підключається до чотирьох Spine-комутаторів, які забезпечують зв'язність між Leaf. Edge-Leaf комутатори керують трафіком між дата-центрами та зовнішніми мережами, маршрутизація виконується BGP і анонсується як VPNv4 через VRF UNDERLAY. Іменування пристроїв: XXX-leafY, XXX-spineY, XXX-edgeY. Централізоване управління через SDN і CI/CD дозволяє автоматично додавати нові стійки, оновлювати маршрути та ізолювати клієнтський трафік, забезпечуючи безпеку, масштабованість і відмовостійкість мережі.

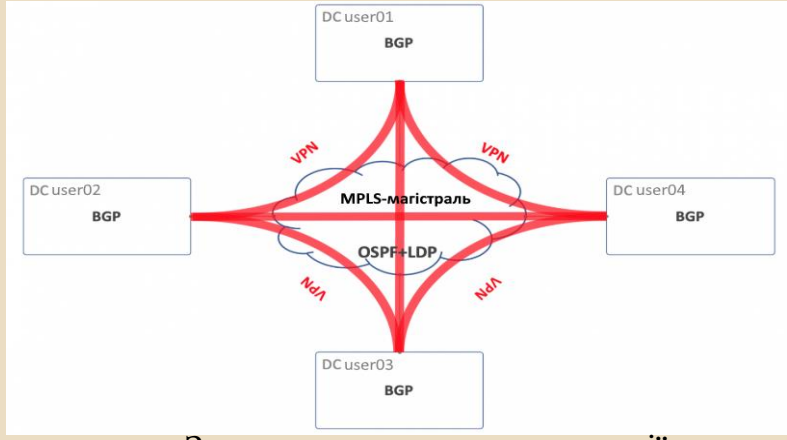


Структура мережі

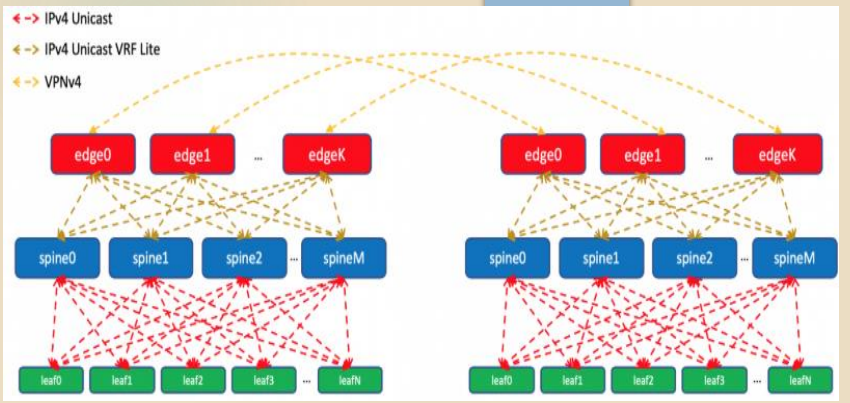


Базова фізична мережа дата-центру

DCI та маршрутизація

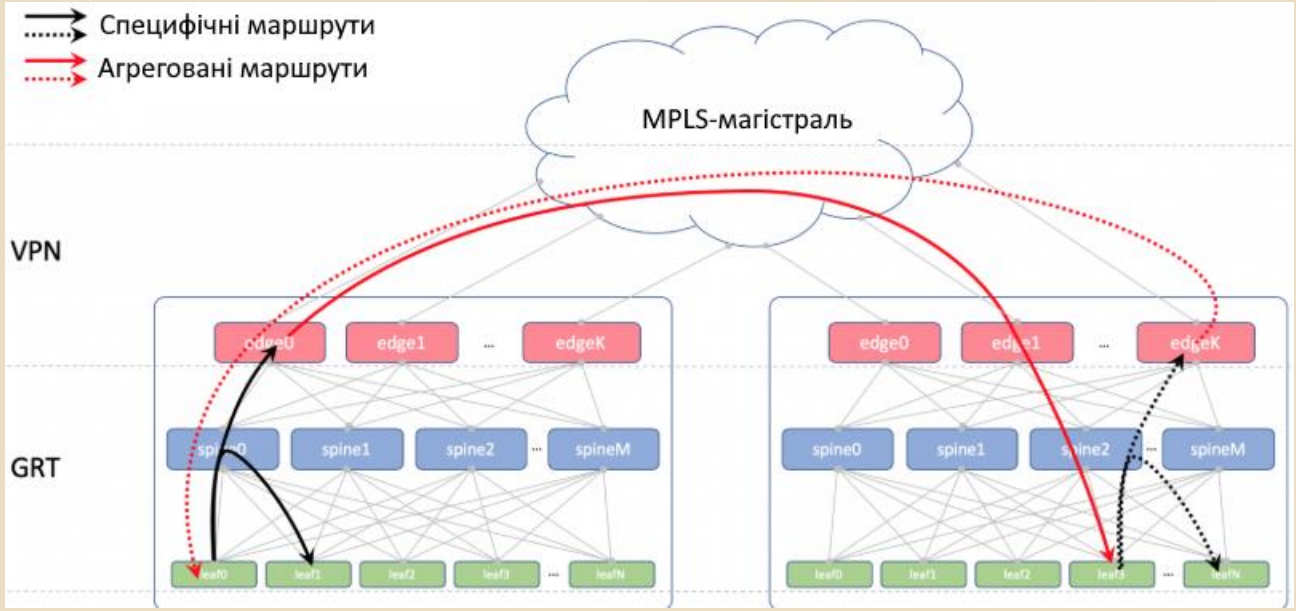


Загальна схема маршрутизації



Імпортовані префікси

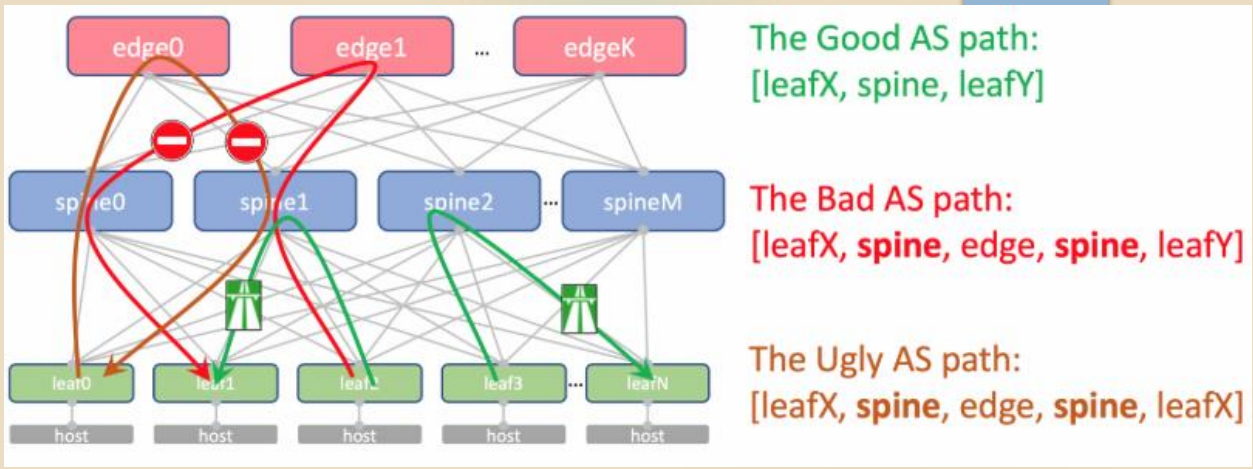
- Для організації DCI використовується Edge-Leaf: Leaf-комутатори збирають маршрути від ToR і піднімають їх до Spine через iBGP. Edge-Leaf виступають точками виходу в MPLS-магістраль, де трафік між дата-центрами передається як VPNv4 у VRF UNDERLAY, ізолюючи внутрішні маршрути від зовнішніх. Усередині ДЦ BGP керує префіксами між Leaf і Spine, забезпечуючи динамічну видимість топології, балансування навантаження та автоматичне перенаправлення при збоях. Централізована автоматизація через SDN і CI/CD дозволяє швидко змінювати конфігурації, оновлювати маршрути та підтримувати мульти-тенантні середовища без ручного втручання.



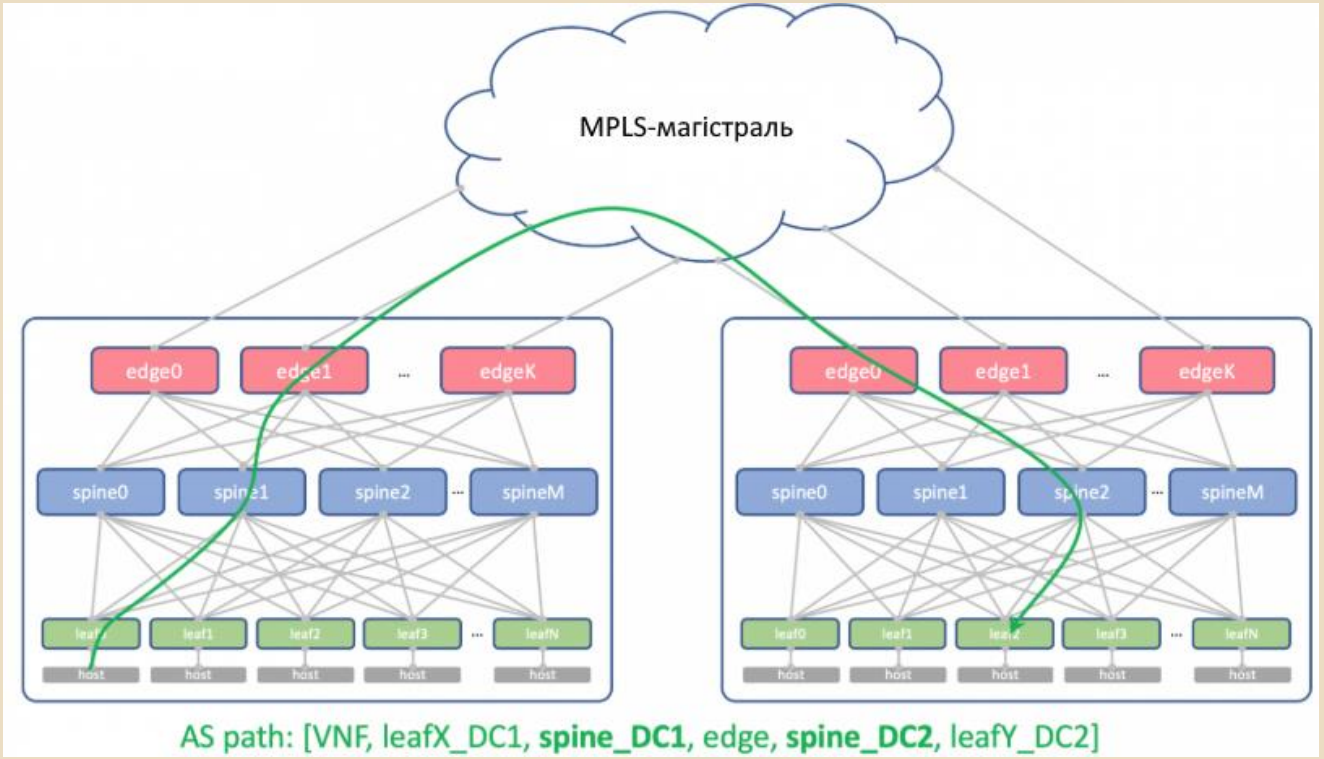
Передача маршрутів як VPNv4 для організації DCI

Використання BGP ASN

- У всіх Edge-Leaf комутаторах одного дата-центру використовується один ASN для організації iBGP-сесій і обміну маршрутами всередині ДЦ. Spine комутатори кожного ДЦ мають унікальний ASN, що дозволяє ізолювати маршрути між ДЦ, уникати конфліктів AS-Path і спрощувати інтеграцію з зовнішніми мережами. Один ASN на Spine запобігає петлям маршрутизації, а різні ASN між ДЦ забезпечують коректну передачу маршрутів через DCI. Чітке визначення ASN спрощує автоматизацію BGP, підтримує прозорість маршрутів, стабільність мережі та безпечну комунікацію між хостами та сервісами у масштабних інфраструктурах.



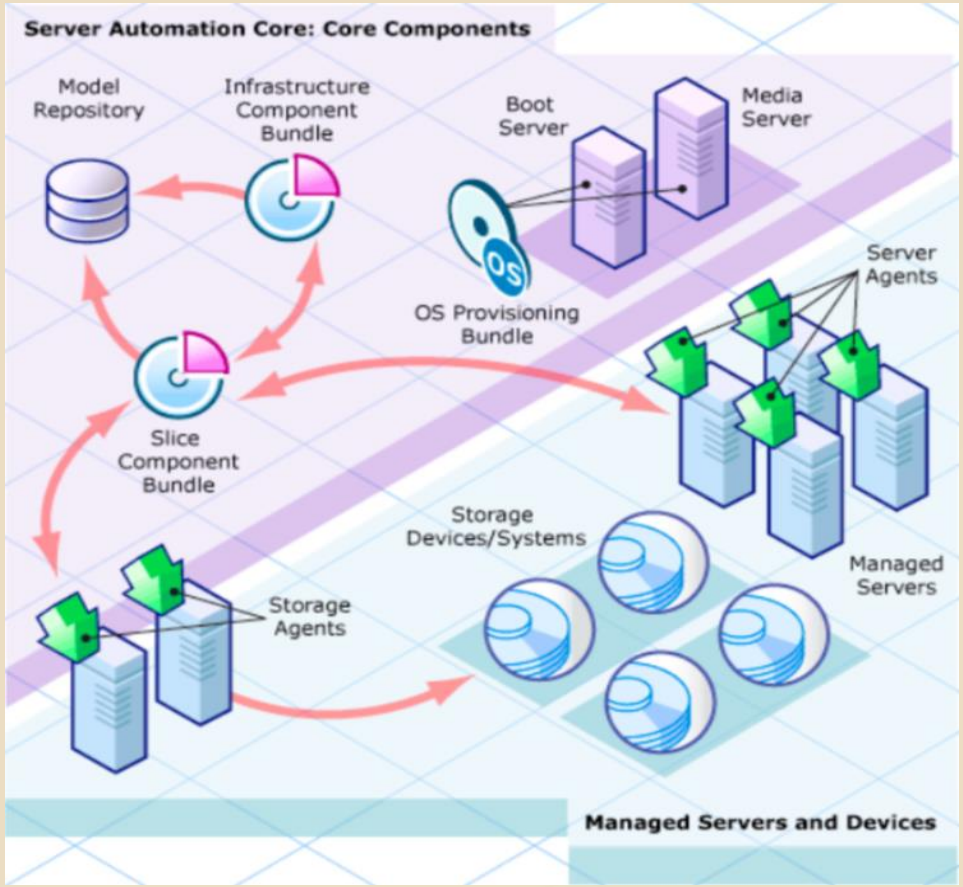
Комунікація між хостами всередині ДЦ відбувається в межах спайнів



Virtual Network Gateway

Конфігурація HPE Server Automation

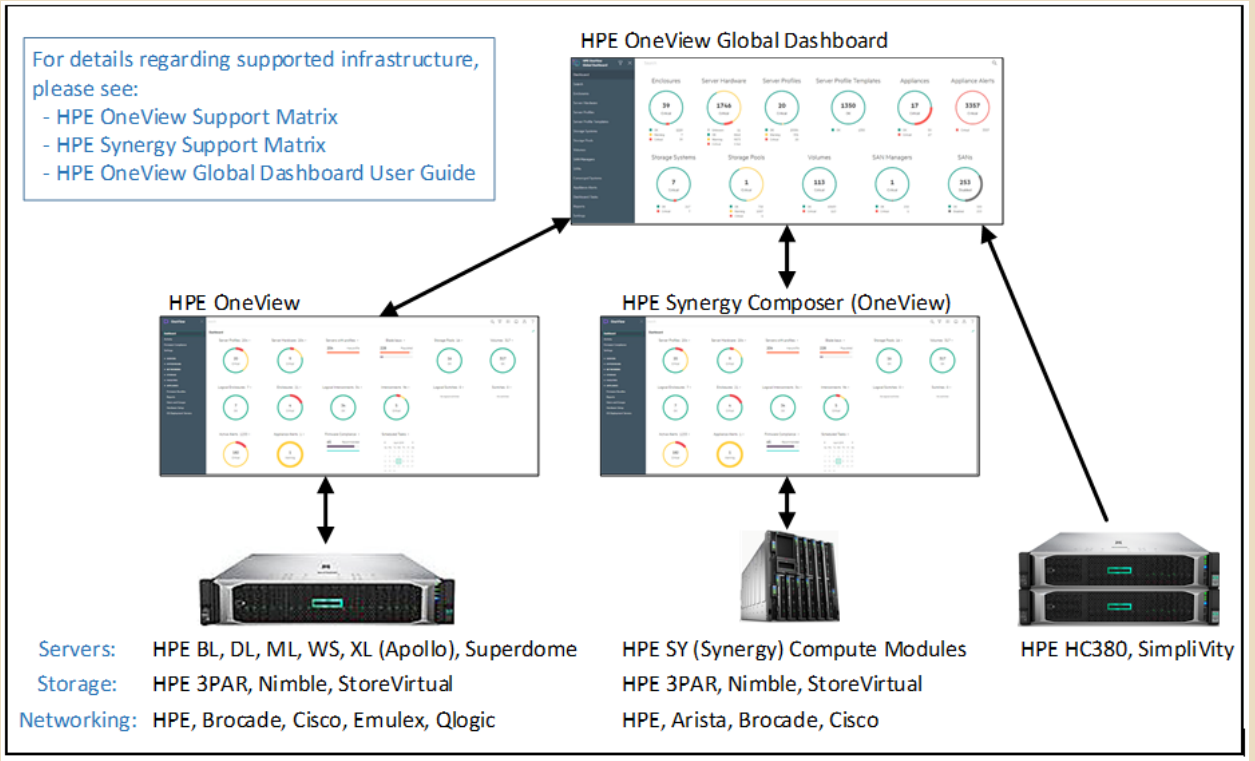
- HPE Server Automation (HPE SA) — комплексна платформа для централізованого управління фізичними й віртуальними серверами. Система автоматично виявляє пристрої в мережі, встановлює агентів, розгортає операційні системи (Windows, Linux, Solaris) і програмне забезпечення за заданими політиками. Модуль Audit and Remediation контролює відповідність конфігурацій стандартам безпеки та автоматично виправляє відхилення. Application Deployment забезпечує розгортання і відкат версій додатків. HPE SA використовує базу Oracle, підтримує багаторівневу архітектуру з віддаленими датацентрами, забезпечує аудит, оновлення, моніторинг і стандартизацію серверних середовищ у масштабних інфраструктурах.



Іллюстрація концептуальної структури можливостей конфігурованих параметрів

Можливості Hewlett Packard Enterprise Server Automation

- HPE Server Automation забезпечує повну автоматизацію управління серверною та мережевою інфраструктурою. Система включає візуалізацію архітектури (SAV), автоматизацію сховищ, формування звітів, розгортання ОС, виконання скриптів і аудит пристроїв. Вона дозволяє централізовано керувати мережевими параметрами, автоматично конфігурувати VLAN, IP-адресацію, політики безпеки та маршрутизацію. Інтеграція з VMware, SCVMM і OpenStack забезпечує ефективне управління віртуальними мережами. HPE SA підвищує продуктивність, зменшує ручну працю, стандартизує налаштування, покращує моніторинг і контроль усіх компонентів, що сприяє стабільності та гнучкості IT-інфраструктури.



Централізоване управління серверами та інтеграція з IT-інфраструктурою для ефективної автоматизації процесів

ВИСНОВКИ

- У кваліфікаційній роботі проведено комплексне дослідження методів і засобів автоматизації управління сучасними телекомунікаційними мережами.
- Розглянуто підходи до оптимізації процесів конфігурації, моніторингу, самовідновлення сервісів та централізованого управління мережевими ресурсами.
- Встановлено, що впровадження систем IPAM, опису мережевих сервісів і вендор-агностичних моделей забезпечує узгодженість конфігурацій і скорочує операційні витрати.
- Досліджено технології віртуалізації (GRE, MPLS, VXLAN, GENEVE тощо) та концепції Underlay/Overlay, які підвищують гнучкість і масштабованість мереж.
- Проаналізовано архітектуру Edge-Leaf, протоколи маршрутизації BGP ASN та засоби централізованого управління серверами HPE Server Automation.

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: Ілля БУЛАВІН

Назва: ОПТИМІЗАЦІЯ ПРОЦЕСІВ АВТОМАТИЗАЦІЇ У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Координатор: В'ячеслав ТРЕЙТЯК

Підрозділ: ННІТ

Коефіцієнт подібності 1:1.3

Коефіцієнт подібності 2:0.3

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*