ВСТУП

Актуальність теми. Сучасне інформаційне суспільство характеризується стрімким зростанням обсягів даних та ускладненням мережевої інфраструктури, що забезпечує функціонування глобальної економіки, науки, державного управління та соціальних взаємодій. Ефективність, надійність, безпека та масштабованість комп'ютерних мереж мають вирішальне значення для розвитку цифрової економіки та впровадження інноваційних сервісів. Фундаментальною характеристикою, що визначає всі ключові операційні параметри мережі, є її топологія — концептуальна схема, яка описує конфігурацію зв'язків та розташування вузлів у мережі.

Історично сформувалися кілька базових топологічних моделей — «шина», «кільце», «зірка», які стали основою для побудови перших локальних мереж. Однак із підвищенням складності завдань, зростанням швидкостей і переходом до глобальних, високо зв'язаних систем, класичні моделі в чистому вигляді стали менш відповідати сучасним вимогам. Сучасні мережі являють собою складні гібридні структури, що поєднують переваги різних базових моделей, але водночас успадковують і їхні обмеження.

Класичні топології мають низку фундаментальних недоліків: централізовані точки відмови, обмежену масштабованість, складність управління та резервування, а також низьку адаптивність до динамічних змін трафіку. Зі зростанням вимог до надійності, продуктивності та безпеки мереж виникає потреба у пошуку нових підходів до побудови топологій, які б дозволили подолати виявлені обмеження та забезпечити ефективне функціонування мережевих систем нового покоління.

Мета роботи — дослідити методи побудови мережевих топологій на базі фрактальних структур, провести їх теоретичний та експериментальний аналіз, а також оцінити переваги та перспективи впровадження фрактальних моделей у сучасних комп'ютерних мережах.

Для досягнення мети у роботі передбачається вирішити такі завдання:

Провести критичний аналіз класичних та гібридних топологій, виявити їхні фундаментальні слабкості та обмеження;

Дослідити математичний апарат опису фрактальних топологій, визначити їхні метричні та структурні характеристики;

Розробити методику побудови мережевих структур на основі фрактальних моделей (зокрема, Трикутника Серпінського, Килима Серпінського, Губки Менгера та інших);

Провести моделювання та експериментальну перевірку працездатності фрактальних топологій у середовищі Cisco Packet Tracer;

Порівняти ефективність, надійність, масштабованість та стійкість до відмов фрактальних топологій із класичними моделями;

Об’єкт дослідження — процес побудови та функціонування мережевих топологій у комп’ютерних мережах.

Предмет дослідження — фрактальні структури як основа для проектування мережевих топологій, їхні властивості, методи побудови та експлуатаційні характеристики.

Методи дослідження.

У роботі застосовуються методи теоретичного аналізу, математичного моделювання, графової теорії, фрактальної геометрії, а також імітаційне моделювання у спеціалізованих програмних середовищах для перевірки працездатності та ефективності запропонованих рішень.

Актуальність теми визначається необхідністю підвищення надійності, масштабованості та ефективності сучасних комп’ютерних мереж, а також пошуком нових архітектурних рішень, здатних забезпечити стійкість до збоїв, оптимальне використання ресурсів і простоту управління у складних динамічних умовах.

1. АНАЛІЗ СУЧАСНИХ МЕРЕЖЕВИХ ТОПОЛОГІЙ ТА ЇХ ОБМЕЖЕНЬ

1.1. Огляд сучасного впливу мереж

Сучасне інформаційне суспільство характеризується експоненційним зростанням обсягів даних і значною залежністю від цифрових комунікацій. Мережева інфраструктура є ключовим елементом, що забезпечує функціонування глобальної економіки, науки, державного управління та соціальних взаємодій. У цьому контексті ефективність, надійність, безпека та масштабованість комп'ютерних мереж мають вирішальне значення. Фундаментальною характеристикою, що визначає всі ключові операційні параметри мережі, є її топологія. Мережева топологія — це концептуальна схема або модель, що описує конфігурацію зв'язків та розташування вузлів (таких як комп'ютери, комутатори, маршрутизатори) у мережі. Топологія визначає маршрути передачі даних, методи управління трафіком, впливає на вибір протоколів маршрутизації та визначає загальну відмово стійкість системи. Історично сформувалися кілька базових топологічних моделей — "шина", "кільце", "зірка", — які стали основою для побудови перших локальних мереж. Із підвищенням складності завдань, зростанням швидкостей і переходом до глобальних, високо зв'язаних систем, класичні моделі в чистому вигляді стали менш відповідати сучасним вимогам. Сучасні мережі, від корпоративних кампусних до магістральних Інтернет-мереж, являють собою складні гібридні (комбіновані) структури, що поєднують переваги різних базових моделей. Комбінований підхід характеризується рядом обмежень. Ієрархічні топології ("дерево") мають потенційні "вузькі місця" (bottlenecks) та критичні точки відмови. Комбінування структур може частково підвищити надійність і масштабованість, утім це часто призводить до ускладнення архітектури та збільшення витрат на управління. Сітчасті (Mesh) топології вимагають комплексних протоколів маршрутизації для запобігання петлям та забезпечення стабільності. Гібридні моделі не усувають всіх обмежень своїх складових, а їхня

ефективність визначається компромісом між складністю, вартістю й надійністю. Метою розділу є проведення глибокого критичного аналізу сучасних мережевих топологій. Основне завдання полягає не лише в описі їхніх характеристик, а й у виявленні фундаментальних слабкостей і обмежень, які перешкоджають подальшому розвитку. Особлива увага приділяється впливу недоліків топологій на ускладнення програмної складової, зокрема протоколів маршрутизації. Аналіз, проведений у цьому розділі, є необхідною передумовою для обґрунтування потреби у пошуку та розробці нових, більш адаптивних і ефективних методів побудови мережевих топологій. Це створює теоретичний фундамент для формулювання гіпотези, що архітектури, засновані на принципово інших математичних моделях, зокрема фрактальних структурах, можуть запропонувати вирішення виявлених проблем.

1.2. Класифікація та фундаментальні поняття мережевих топологій

Для проведення коректного аналізу необхідно чітко визначити систему класифікації та основні поняття, які описують мережеві топології.

1.2.1. Фізична та логічна топологія

Найважливішим є розрізнення двох рівнів опису мережі:

Фізична топологія: Описує реальне, фізичне розташування компонентів мережі. Вона включає тип кабелів (мідна пара, оптоволокно), їхню довжину та схему прокладання, а також фізичне розміщення пристроїв. Це відповідь на питання: "Як компоненти з'єднані фізично?". Прикладом є фізична "зірка", де кожен комп'ютер у кімнаті підключений окремим кабелем до комутатора у серверній шафі. Логічна топологія: Описує шлях, яким дані логічно переміщуються між вузлами в мережі. Вона визначається конфігурацією мережевих пристроїв та протоколами, що на них працюють, і може не збігатися з фізичною структурою. Це відповідь на питання: "Як вузли бачать один одного і як передають дані?". Класичний приклад — перші

мережі Ethernet на коаксіальному кабелі (фізична "шина"), які логічно також функціонували як "шина" (широкомовне середовище). Однак сучасний Ethernet (наприклад, 1000Base-T) має фізичну топологію "зірка", але може логічно емулювати "шину" (при використанні концентратора) або, що більш поширено, працювати як логічна "зірка" або комутована мережа "точка-точка" (при використанні комутатора). У контексті цього дослідження аналіз слабкостей охоплює обидва рівні, оскільки обмеження фізичної топології часто компенсуються складною логічною топологією та протоколами.

1.2.2. Ключові метрики та характеристики

Для порівняльного аналізу топологій використовуються наступні кількісні та якісні характеристики: Ступінь вузла: Кількість зв'язків (портів), підключених до одного вузла. Діаметр мережі: Найдовший з найкоротших шляхів між будь-якою парою вузлів у мережі. Менший діаметр означає потенційно менші затримки. Пропускна здатність Максимальна швидкість передачі даних, яку може підтримати топологія. Бісекційна пропускна: Міра пропускної здатності у найслабшому місці мережі; мінімальна кількість зв'язків, які потрібно розірвати, щоб розділити мережу на дві приблизно рівні половини. Надмірність Наявність альтернативних, або надлишкових, шляхів між вузлами. Це є основою для відмовостійкості. Масштабованість Здатність мережі до розширення (додавання нових вузлів) без суттєвої деградації продуктивності або експоненційного зростання складності управління.

1.3. Детальний аналіз базових топологій

Класичні мережеві топології, хоча й рідко застосовуються у чистому вигляді в сучасних корпоративних та глобальних мережах, слугують фундаментальним базисом для побудови будь-якої комунікаційної інфраструктури. Сучасні гіпермасштабовані мережі є результатом рекурсивної композиції та накладання цих простих структур. Глибоке розуміння фізики процесів, що відбуваються в елементарних

топологіях ("Шина", "Кільце", "Зірка"), є ключем до виявлення кореневих причин проблем у складних системах.При переході від простих архітектур до складних гібридних систем (наприклад, "Зірка-Шина" або деревоподібні структури) фундаментальні недоліки базових топологій не усуваються. Вони трансформуються, маскуються протоколами вищих рівнів або компенсуються надлишковим апаратним забезпеченням, але продовжують існувати на фізичному та канальному рівнях. Колізії та обмеження середовища передачі, властиві "Шині", проявляються

у проблемах пропускної здатності бездротових мереж. Проблеми узгодженості та розриву кільця, характерні для "Кільця", вимагають складних протоколів реконфігурації у сучасних оптичних магістралях. Критична залежність від центрального вузла у "Зірці" масштабується до проблеми відмови центральних маршрутизаторів ядра мережі. У цьому підрозділі буде проведено структурно-функціональний аналіз канонічних моделей з метою виділення їхніх інваріантних характеристик — як позитивних (простота, детермінованість), так і негативних (обмежена масштабованість, вразливість до фізичних пошкоджень). Саме цей аналіз дозволить сформулювати вимоги до нової, фрактальної архітектури, яка має не просто "залатати діри" класичних схем, а запропонувати принципово інший підхід до організації зв'язків.

1.3.1. Топологія "Шина" (Bus Topology)

Опис архітектури: У топології "шина" всі мережеві пристрої (вузли) підключаються до одного спільного комунікаційного каналу, який називається "шиною". Зазвичай це коаксіальний кабель. Дані, що відправляються будьяким вузлом, поширюються по всій довжині кабелю в обидва боки. Кожен вузол "прослуховує" шину і приймає лише ті дані, які адресовані йому. Для запобігання відбиттю сигналу від кінців кабелю, що може спричинити інтерференцію, на обох кінцях шини встановлюються спеціальні пристрої — термінатори [4, с. 45].

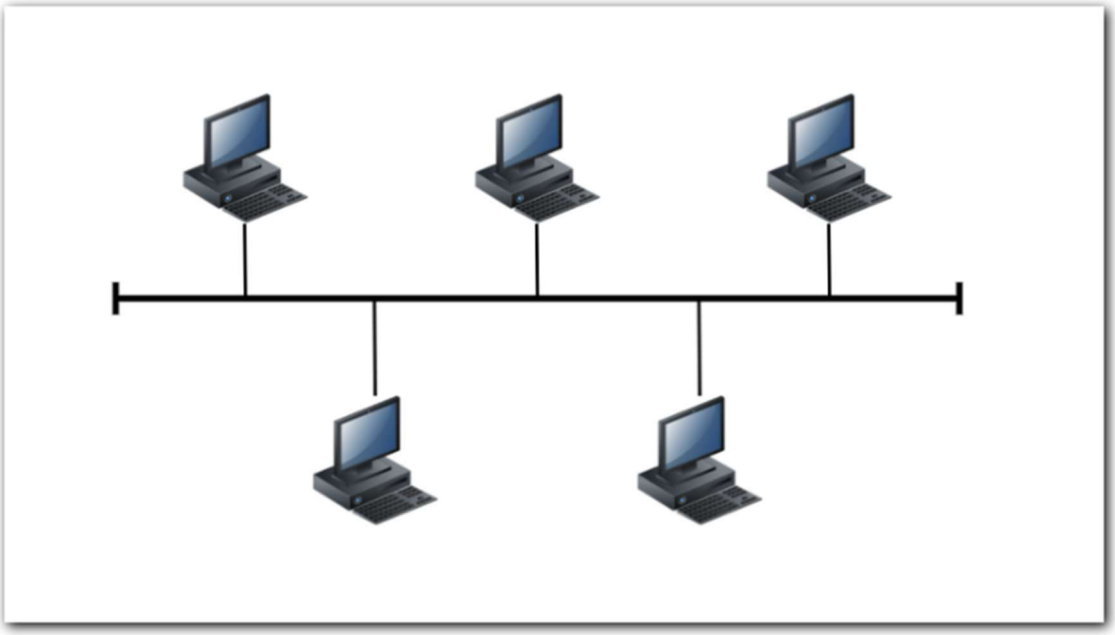

Рисунок 1.1 - Топологія Шина

Переваги топології «Шина»: Економічна ефективність та мінімізація кабельної інфраструктури. Топологія «Шина» є лідером за показником ефективності використання кабелю. На відміну від топології «Зірка», де для підключення кожного вузла необхідно прокладати окремий кабель від робочого місця до центрального комутаційного вузла (що призводить до дублювання трас, у «Шині» використовується єдиний магістральний канал. Це дозволяє суттєво знизити витрати на витратні матеріали та монтажні роботи, особливо в приміщеннях з лінійним плануванням. Простота розгортання та пасивність архітектури. Мережа будується на основі пасивних компонентів і не вимагає наявності активного мережевого обладнання для базового функціонування. Це спрощує процес проектування та початкового налаштування, оскільки відсутня необхідність у конфігурації портів, налаштуванні VLAN або управлінні таблицями MAC-адрес. Додавання нового клієнта здійснюється шляхом фізичної врізки в магістраль без необхідності переналаштування центральних вузлів.

Відсутність централізованої точки відмови. У класичній «Шині» відсутній центральний пристрій, вихід з ладу якого паралізував би роботу всієї мережі (на відміну від комутатора в топології «Зірка»). Відмова мережевого адаптера на одному з

вузлів, як правило, не впливає на здатність інших вузлів обмінюватися даними (за умови, що несправний адаптер не генерує безперервний шум у канал).

Ефективність для широкомовного трафіку. Завдяки фізичній природі спільного середовища, дані, відправлені одним вузлом, миттєво стають доступними для всіх інших без додаткових затримок на комутацію та буферизацію. Це робить дану топологію ефективною для специфічних задач, що вимагають синхронного отримання команд усіма учасниками мережі (наприклад, у промислових системах управління або старих системах оповіщення).

Фундаментальні слабкості та обмеження:

Критична вразливість до відмов: "Шина" є яскравим прикладом архітектури з єдиною точкою відмови. Пошкодження кабелю в будь-якому місці або несправність одного з термінаторів призводить до повної відмови всієї мережі.

Проблема колізій: Оскільки середовище передачі є спільним, одночасна спроба передачі даних двома або більше вузлами призводить до "колізії" (зіткнення сигналів) та пошкодження даних. Для вирішення цієї проблеми був розроблений метод доступу CSMA/CD, який, однак, є неефективним.

Деградація продуктивності: Ефективність CSMA/CD різко падає зі збільшенням кількості вузлів та навантаження. Чим більше вузлів, тим частіші колізії, тим більше часу витрачається на очікування та повторні передачі. Загальна пропускна здатність шини ділиться між усіма вузлами, що робить її непридатною для сучасних високошвидкісних застосунків. Складність діагностики: Виявлення місця пошкодження кабелю або несправного вузла , що постійно посилає "сміття" в шину) є вкрай складним завданням. Низька масштабованість: Існує жорстке обмеження на максимальну довжину кабелю та максимальну кількість вузлів через затухання сигналу та збільшення кількості колізій. Сучасне значення: Топологія "шина" нині використовується переважно як приклад в освітній і теоретичній сфері та була замінена іншими рішеннями. Її розгляд дозволяє пояснити, чому спільне середовище передачі виступає фундаментальним обмеженням для продуктивності мережі. Приховані прояви "Шини" у сучасних технологіях та вплив на маршрутизацію.

Важливо розуміти, що хоча фізична "шина" на коаксіальному кабелі зникла, концепція спільного середовища залишається фундаментальною проблемою в сучасних бездротових мережах. У радіоефірі всі пристрої "чують" один одного, що фактично відтворює логіку "шини" з усіма її недоліками — колізіями та необхідністю арбітражу доступу , що суттєво обмежує реальну швидкість передачі даних зі зростанням кількості абонентів. Крім того, топологія типу "шина" (або широкомовна мережа) створює специфічні виклики для протоколів маршрутизації. Як зазначається у джерелі, алгоритми на базі стану каналу, такі як OSPF, "страждають у присутності широкомовних мереж канального рівня... де будь-яка сутність має прямий доступ до будь-якої іншої сутності. створюючи повнозв'язну множину суміжностей".

У такій топології виникають дві критичні проблеми:

1. Обчислювальна складність: Кількість зв'язків зростає квадратично, що ускладнює роботу алгоритму Дейкстри.

2. Надлишковий трафік: При розсилці оновлень маршрутизації кожен маршрутизатор генерує повідомлення для кожного сусіда, що призводить до лавиноподібного зростання службового трафіку.

Щоб вирішити цю проблему, сучасні протоколи змушені програмно "ламати" топологію шини. Рішення полягає у тому, щоб "трансформувати широкомовну топологію у зіркоподібну топологію, додавши псевдо-вузол ". Це підтверджує тезу, що "шина" як топологія є настільки неефективною для масштабування, що навіть програмні алгоритми намагаються перетворити її на "зірку" для стабільної роботи.

1.3.2. Топологія "Кільце"

Опис архітектури: У "кільцевій" топології кожен вузол з'єднаний з двома іншими, утворюючи фізично замкнене кільце. Дані передаються по кільцю в одному, чітко визначеному напрямку. Кожен вузол функціонує як ретранслятор: він отримує сигнал від попереднього вузла, перевіряє адресу призначення, і якщо дані

адресовані не йому, він регенерує та передає сигнал далі наступному вузлу в кільці. Якщо вузол розпізнає свою адресу, він копіює дані у свій буфер, але все одно, як правило, передає їх далі по кільцю, щоб вони повернулися до відправника як підтвердження доставки [1, с. 320].

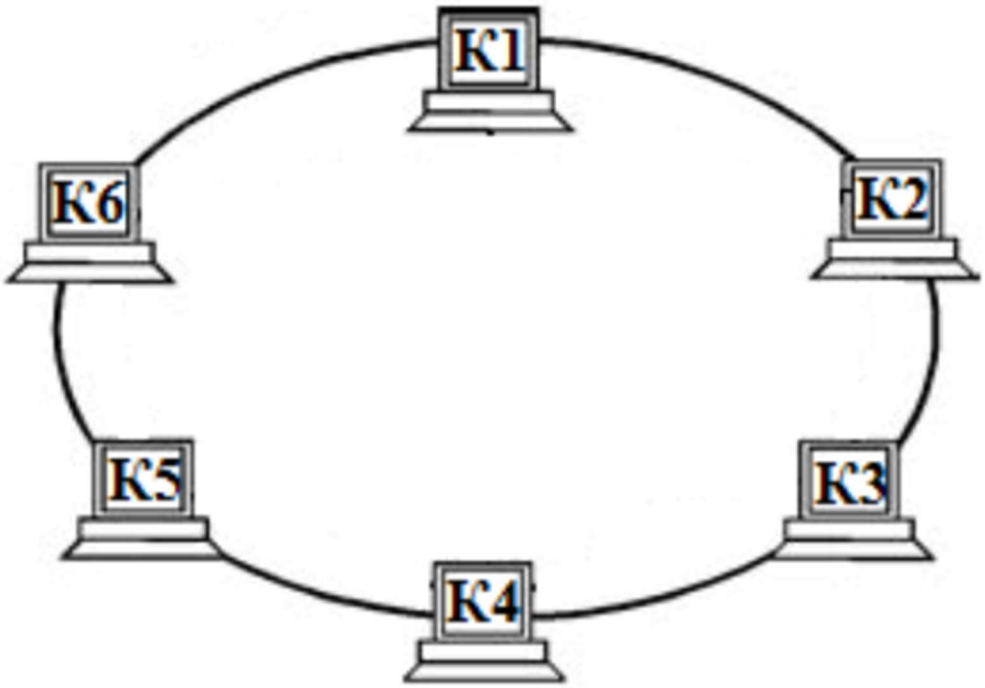

Рисунок 1.2 - Топологія кільце

Для управління доступом до середовища у класичних "кільцях" використовувався неконфліктний метод, найчастіше — метод передачі маркера. Спеціальний короткий кадр, "маркер", циркулює по кільцю. Вузол, який бажає передати дані, повинен "захопити" вільний маркер, змінити його статус на "зайнятий", додати свої дані та адресу одержувача, і відправити цей кадр далі. Інші вузли в цей час не можуть передавати. Лише після того, як кадр обійде кільце і повернеться до відправника, той звільняє маркер, роблячи його доступним для наступного вузла.

Переваги:

Відсутність колізій: Метод маркерного доступу є детерміністичним і повністю виключає колізії, які були головною проблемою "шини". Це гарантує стабільну

та передбачувану продуктивність, яка не деградує так різко під високим навантаженням.

Висока ефективність при високому навантаженні: На відміну від CSMA/CD, де продуктивність падає через колізії, у Token Ring кожен вузол гарантовано отримує свій час на передачу.

Фундаментальні слабкості та обмеження:

Критична вразливість до відмов: Подібно до "шини", класичне "кільце" має низьку відмовостійкість. Вихід з ладу будь-якого вузла або пошкодження кабелю в будь-якому місці розриває кільце і призводить до повної зупинки мережі. Складність додавання/видалення вузлів: Для підключення нового вузла або відключення старого необхідно фізично розірвати кільце, що тимчасово зупиняє роботу всієї мережі. Це робить обслуговування вкрай незручним.

Затримка передачі: Дані повинні послідовно пройти через усі проміжні вузли на шляху до одержувача. У великому кільці сумарна затримка стає значною, оскільки кожен вузол вносить свою невелику затримку на обробку та ретрансляцію. Проблеми з "втраченим маркером": Механізм маркера вразливий. Збій у роботі станції міг призвести до "втрати" маркера або генерації "бродячого" кадру, що вимагало складних процедур моніторингу та відновлення.

Сучасне значення: Класичне "кільце" повністю зникло з локальних мереж. Однак ідея "кільця" трансформувалася і знайшла своє застосування у високошвидкісних міських та магістральних мережах на основі оптоволокна. Такі технології, як FDDI та сучасні SDH/SONET та Resilient Packet Ring, використовують подвійні оптоволоконні кільця, що обертаються у протилежних напрямках. Це вирішує головну проблему надійності: у разі розриву кабелю або відмови вузла, система автоматично "загортає" кільце, миттєво перенаправляючи трафік через резервне кільце, забезпечуючи час відновлення менше 50 мс. Таким чином, слабкість простого кільця була подолана у його значно більш складних та дорогих нащадках.

Специфіка фізичної реалізації та логічна структура. Важливим аспектом аналізу кільцевої топології є розбіжність між її логічною та фізичною структурою. У

класичній технології IBM Token Ring для підвищення надійності було впроваджено концепцію "фізична зірка — логічне кільце". Вузли підключалися не напряму один до одного, а до центрального пристрою — модуля багатостанційного доступу. Усередині MAU порти були з'єднані в кільце. Це дозволяло реалізувати механізм автоматичного обходу : якщо вузол виходив з ладу або вимикався, реле всередині MAU автоматично замикало контур в обхід неактивного порту, зберігаючи цілісність кільця. Цей інженерний прийом став предтечею сучасних відмовостійких систем.

Еволюція до Ethernet-кілець (ITU-T G.8032) Хоча Token Ring та FDDI стали історією, сама концепція кільця переживає ренесанс у сучасних мережах Metro Ethernet (мережі масштабу міста). Провайдери послуг часто будують свої магістралі саме у вигляді кільця, використовуючи стандарт ITU-T G.8032.

Принцип дії: На відміну від застарілого STP, який блокує порти для уникнення петель і має довгий час відновлення, ERPS розроблений спеціально для кілець. Він блокує лише один сегмент , перетворюючи кільце на логічну шину.

Реакція на аварію: При фізичному розриві кабелю в будь-якому місці кільця, заблокований сегмент миттєво (менше ніж за 50 мс) розблокується, відновлюючи зв'язність. Це підтверджує тезу, що кільцева топологія в чистому вигляді є вразливою, але як архітектурний патерн із механізмами захисту є незамінною для побудови високонадійних транспортних мереж, де вимагається детермінований час відновлення, недосяжний для складних Mesh-структур.

1.3.3. Топологія "Зірка"

Зіркова топологія є однією з найпоширеніших і найважливіших структур у сучасних комп’ютерних мережах. У цій архітектурі всі кінцеві пристрої (вузли) підключаються окремими кабельними сегментами за принципом «точка-точка» до одного центрального пристрою. Таким центральним елементом може виступати концентратор, комутатор або маршрутизатор залежно від рівня складності та функціональності мережі.

Весь мережевий трафік у такій структурі проходить виключно через центральний пристрій, який виконує роль «серця» мережі. Саме через нього здійснюється обмін даними між усіма підключеними вузлами. Така організація дозволяє чітко контролювати потоки інформації та спрощує адміністрування. Якщо центральний пристрій — концентратор, він працює як простий ретранслятор: будь-який сигнал, що надходить на один порт, просто копіюється та надсилається на всі інші порти. З логічної точки зору, це та ж сама «шина», але реалізована фізично як «зірка». Всі пристрої знаходяться в одному домені колізій, і одночасна передача даних двома вузлами призводить до колізій. Це означає, що при великій кількості підключених пристроїв ефективність мережі може суттєво знижуватися через часті колізії, а також зростає ймовірність втрати даних.

Проте така реалізація була поширена на початкових етапах розвитку локальних мереж через простоту і дешевизну обладнання. Якщо центральний пристрій — комутатор, він є значно інтелектуальнішим. Комутатор аналізує MAC-адреси вхідних кадрів і пересилає кадр тільки на той порт, до якого підключений одержувач (на основі своєї таблиці комутації). Це створює множинні паралельні та ізольовані канали зв'язку, що дозволяє уникати колізій і підвищує загальну продуктивність мережі. Кожен порт комутатора стає окремим доменом колізій, а у повнодуплексному режимі поняття колізії зникає повністю. Завдяки цьому сучасні мережі на базі комутаторів забезпечують високу швидкість передачі даних, стабільність і надійність роботи навіть при великій кількості підключених пристроїв.

У складних корпоративних мережах центральним пристроєм може бути маршрутизатор, який дозволяє організовувати взаємодію між різними підмережами, здійснювати фільтрацію трафіку, впроваджувати політики безпеки та маршрутизації. Це особливо актуально для великих організацій, де необхідно розділяти мережу на логічні сегменти, забезпечувати контроль доступу та балансування навантаження.

Приклади реалізації топології «зірка» включають сучасні дротові мережі Ethernet (100Base-TX, 1000Base-T, 10G-Base-T), де кожен комп’ютер

підключається окремим кабелем до центрального комутатора. У бездротових мережах Wi-Fi точка доступу виступає центром зірки, а всі клієнти підключаються до неї. Практично всі сучасні локальні мережі у офісах, навчальних закладах, дата-центрах використовують топологію «зірка» як базову [5, с. 48; 8, с. 102], оскільки вона забезпечує оптимальний баланс між простотою розгортання, надійністю та масштабованістю.

Переваги топології «зірка» полягають у високій надійності та відмовостійкості на рівні вузлів. Пошкодження кабелю, що веде до одного вузла, або відключення цього вузла впливає тільки на цей вузол. Решта мережі продовжує функціонувати без збоїв. Це особливо важливо для критичних систем, де безперервність роботи є пріоритетом. Простота обслуговування та діагностики також є суттєвою перевагою: завдяки централізованій точці підключення та ізольованим кабельним сегментам, виявлення несправностей стає тривіальним завданням. Зазвичай індикатори на комутаторі або маршрутизаторі показують проблемний порт, що дозволяє швидко локалізувати та усунути несправність без впливу на інші вузли. Крім того, топологія «зірка» забезпечує легкість розширення мережі. Додавання нових вузлів або їх переміщення є простим процесом, який не вимагає зупинки всієї мережі — достатньо підключити новий кабель до вільного порту на комутаторі чи маршрутизаторі.

Це дозволяє гнучко масштабувати мережу відповідно до потреб організації. Висока продуктивність є ще однією важливою перевагою. Комутатор забезпечує кожному вузлу виділену пропускну здатність, оскільки він створює тимчасові канали «точка-точка». Колізії повністю відсутні, що дозволяє досягати високих швидкостей передачі даних навіть у великих мережах. Вузли не «чують» чужий трафік, що ускладнює перехоплення даних і підвищує рівень інформаційної безпеки. Водночас, топологія «зірка» має і певні обмеження.

Головна і єдина суттєва слабкість — це централізована точка відмови. Вихід з ладу центрального комутатора або маршрутизатора призводить до повної відмови всієї мережі, яку він обслуговує. Весь трафік проходить через один пристрій. Хоча

сучасні комутатори мають високошвидкісні внутрішні шини, зрештою, загальна продуктивність мережі обмежується здатністю центрального вузла обробляти та комутувати пакети. Також «зірка» вимагає значно більшої кількості кабелю та обов'язкової наявності дорогого центрального обладнання, що може збільшувати вартість розгортання мережі порівняно з топологією «шина».

Таким чином, топологія «зірка» поєднує простоту фізичної реалізації, високу надійність на рівні вузлів, легкість обслуговування та масштабування. Її єдиним критичним недоліком залишається централізована точка відмови, однак сучасні технології резервування та стекування комутаторів дозволяють мінімізувати цей ризик у великих корпоративних мережах, що вирішує проблему з аварійними ситуаціями на центральних точках, за рахунок розділення центральної точки на логічні. Саме завдяки цим властивостям топологія «зірка» стала стандартом для побудови сучасних локальних мереж різного масштабу.

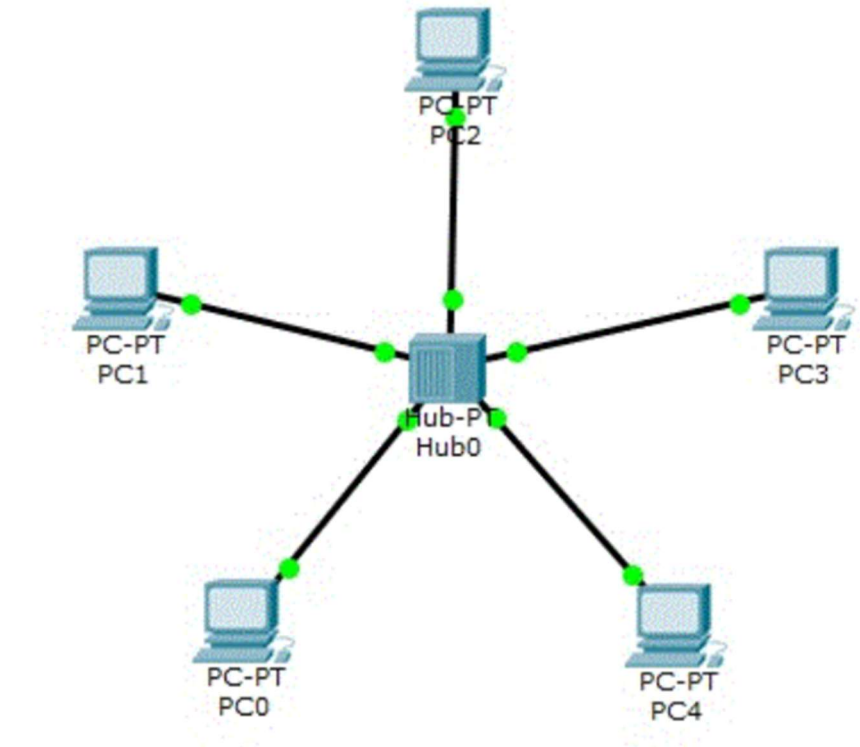

Рисунок 1.3 - топологія зірка

Перевагами: Легкість розширення: Додавання нових вузлів або їх переміщення є простим процесом, який не вимагає зупинки всієї мережі — достатньо підключити новий кабель до вільного порту на комутаторі. **Та** висока

продуктивність: Комутатор забезпечує кожному вузлу виділену пропускну здатність, оскільки він створює тимчасові канали "точка-точка". Колізії повністю відсутні.

Фундаментальні слабкості та обмеження це Централізована точка відмови: Головна і єдина суттєва слабкість "зірки" — це центральний пристрій. Вихід з ладу центрального комутатора або маршрутизатора призводить до повної відмови всієї мережі, яку він обслуговує. Також обмеження продуктивності центрального вузла: Весь трафік проходить через один пристрій. Хоча сучасні комутатори мають високошвидкісні внутрішні шини, зрештою, загальна продуктивність мережі обмежується здатністю центрального вузла обробляти та комутувати пакети. Вища вартість розгортання: "Зірка" вимагає значно більшої кількості кабелю та обов'язкової наявності дорогого центрального обладнання. Сучасне значення: Топологія "зірка" є загальновизнаним стандартом для побудови локальних мереж будь-якого масштабу — від домашніх до великих корпоративних.

Її переваги у надійності, керованості та продуктивності значно переважають недоліки, що зумовило витіснення інших варіантів. Навіть на рівні протоколів маршрутизації, ідея "зірки" використовується для оптимізації. Як вказано у наданому файлі, протоколи на базі стану каналу, як-от OSPF, стикаються з проблемами у широкомовних мережах. Якщо б кожен маршрутизатор у такій мережі встановлював зв'язок з кожним іншим, це створило б "високу кількість суміжностей", що призвело б до обчислювальних проблем та надлишкового трафіку. Рішення полягає у тому, щоб "трансформувати широкомовну топологію у зіркоподібну топологію, додавши псевдо-вузол ". Тобто, протокол штучно обирає один маршрутизатор, який стає центром віртуальної "зірки", і всі інші маршрутизатори обмінюються інформацією лише з ним. Це яскраво демонструє, наскільки ефективною є модель "зірки" для оптимізації комунікаційних потоків, навіть на логічному рівні.

Критична еволюція центрального вузла: від Концентратора до Комутатора

Фундаментальна характеристика топології "Зірка" — її залежність від інтелекту центрального вузла. Ігнорування еволюції цього компонента призводить до неповного розуміння роботи сучасних мереж.

1. Центр "Зірки" – Концентратор: У ранніх реалізаціях Ethernet у центрі знаходився концентратор. Цей пристрій працює на Фізичному рівні моделі OSI. Він не має жодного "інтелекту" і не аналізує дані; він просто приймає електричний сигнал на один порт, регенерує його і сліпо ретранслює всі інші порти.

Наслідки: З *логічної* точки зору, "зірка" на базі концентратора не є "зіркою" взагалі. Вона є логічною "шиною". Всі пристрої, як і в коаксіальній шині, знаходяться в єдиному домені колізій. Це означає, що: Всі дані, надіслані одним вузлом, отримують усі інші. Одночасна передача двох вузлів призводить до колізії, що вимагає використання неефективного методу доступу CSMA/CD. Загальна пропускна здатність мережі ділиться між *усіма* активними вузлами. У цьому сценарії, єдиною перевагою "зірки" над "шиною" була фізична надійність кабельної системи, але продуктивність залишалася низькою.

2. Центр "Зірки" – Комутатор: Сучасна "зірка" використовує у центрі комутатор. Це інтелектуальний пристрій Рівня 2 моделі OSI. Він "вивчає" топологію мережі, аналізуючи MAC-адреси джерела у кожному кадрі, і будує динамічну таблицю комутації. Коли кадр надходить на порт, комутатор аналізує адресу призначення і пересилає його *тільки* на той порт, де знаходиться одержувач.

Наслідки: Це кардинально змінює фізику роботи мережі. Кожен порт комутатора стає окремим доменом колізій.

Відсутність колізій: У сучасному повнодуплексному режимі, де пристрій може одночасно надсилати й отримувати дані окремими парами проводів, поняття колізії зникає повністю. Механізм CSMA/CD більше не потрібен.

Безпека: Вузли не "чують" чужий трафік, що ускладнює перехоплення даних.

Таким чином, сучасна топологія "зірка" — це не просто схема розкладки кабелів, а потужна високопродуктивна архітектура "точка-точка", яка подолала

більшість проблем своїх попередників, залишивши лише одну фундаментальну архітектурну слабкість — єдину точку відмови у вигляді самого комутатора.

1.3.4. Топологія "Дерево"

Опис архітектури: Деревоподібна (або ієрархічна) топологія є не просто розширенням топології "зірка", а фундаментальним архітектурним патерном для побудови масштабованих мереж. Вона базується на каскадному з'єднанні мережевих пристроїв, де вузли нижчого рівня підключаються до вузлів концентрації, які, в свою чергу, об'єднуються вузлами ще вищого ієрархічного рівня. Ця структура, яку часто називають "зіркою зірок", дозволяє ефективно ізолювати трафік окремих сегментів та спростити управління великою кількістю хостів. Архітектура такої мережі зазвичай реалізується за класичною трирівневою ієрархічною моделлю, яка чітко розмежовує функції та зони відповідальності обладнання на кожному рівні:

Рівень доступу: (Це найнижчий рівень, "листя" дерева. Його основна функція — забезпечення фізичного підключення кінцевих пристроїв до мережі. Тут реалізуються політики контролю доступу до портів та маркування трафіку. Це, по суті, класичні локальні "зірки".

Рівень розподілу Проміжний рівень, який слугує інтелектуальним посередником між ядром та доступом. Комутатори цього рівня не просто агрегують трафік від декількох груп вузлів доступу, а й виконують важливі функції обробки: маршрутизацію між віртуальними мережами, фільтрацію пакетів та застосування політик безпеки. Цей рівень локалізує проблеми, не даючи їм поширюватися на ядро.

Рівень ядра Найвищий рівень ієрархії. Це високошвидкісна магістраль мережі. Головне завдання ядра — максимально швидка комутація великих обсягів трафіку між модулями розподілу без виконання складних обчислень (фільтрації чи інспекції пакетів), щоб уникнути затримок.

Така фізична організація тісно пов'язана з логікою роботи сучасних протоколів маршрутизації. Як зазначається в технічній літературі, ієрархічна маршрутизація дозволяє розбити велику мережу на автономні домени маршрутизації, приховуючи деталі внутрішньої топології одного домену від іншого. Це критично важливо для масштабованості, оскільки зменшує розмір таблиць маршрутизації. Наприклад, протокол OSPF використовує концепцію "зон", де магістральна "Зона 0" виконує роль логічного кореня дерева, через який проходить весь трафік між периферійними зонами. Специфіка деревоподібної топології диктує жорсткі правила руху даних. Трафік між двома вузлами, що знаходяться у різних сегментах, змушений підніматися ієрархією вгору до першого спільного вузла-попередника, а потім спускатися вниз до одержувача.

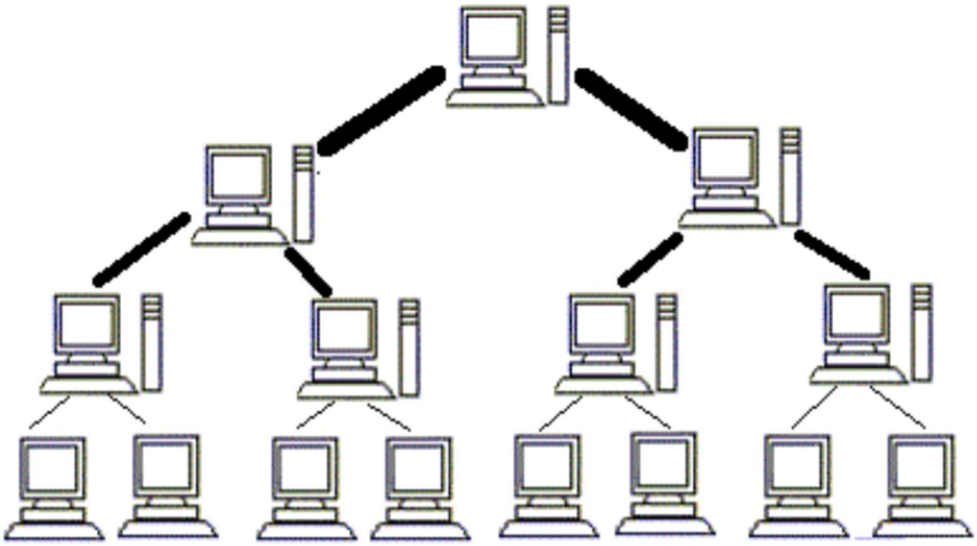

Рисунок 1.4 - Топологія дерево.

Переваги: Висока масштабованість та структурованість: "Дерево" є надзвичайно ефективним способом структурування та розширення великих мереж. Нові сегменти ("зірки") можна легко додавати, підключаючи їх до комутаторів рівня розподілу, не порушуючи роботу існуючої мережі. Полегшене управління та

діагностика: Ієрархічна структура дозволяє логічно сегментувати мережу, спрощуючи застосування політик безпеки, управління трафіком та ізоляцію несправностей. Поєднання переваг "зірки": Успадковує від "зірки" високу надійність на рівні доступу.

Фундаментальні слабкості та обмеження: Критичні точки відмови на вищих рівнях: Головна слабкість "дерева" — це успадкована та посилена вразливість "зірки". Вихід з ладу кореневого комутатора або навіть комутатора рівня розподілу призводить до каскадного, катастрофічного збою, "відрізаючи" цілі секції або всю мережу. "Вузькі місця" в ієрархії: Весь трафік між різними гілками змушений проходити через вузли вищого рівня. Це створює величезне навантаження на кореневі та розподільчі вузли, які стають "вузькими місцями". Якщо трафік між двома відділами раптово зростає, він може перевантажити магістральний канал, навіть якщо загальне навантаження на мережу не є критичним. Неоптимальні шляхи та затримка: Трафік між двома вузлами, які фізично можуть знаходитися у сусідніх кімнатах, але логічно підключені до різних "гілок", змушений проходити довгий шлях "вгору і вниз" по ієрархії. Це створює штучно подовжені маршрути та збільшує затримку , що є неприйнятним для сучасних чутливих до затримок додатків. Обмежена надмірність: У своїй базовій формі деревоподібна топологія не має надлишкових шляхів. Це робить її вразливою. Хоча на практиці додають резервні канали, це вимагає активації складних протоколів для запобігання петлям комутації, які є смертельними для таких мереж. STP, у свою чергу, блокує ці надлишкові шляхи, не даючи використовувати їх для балансування навантаження, а лише активуючи у разі збою.

Сучасне значення: "Дерево" є домінуючою моделлю для проектування структурованих мереж. Однак її ефективність повністю залежить від здатності долати її ключову слабкість — вразливість ієрархічних вузлів. Як зазначається у наданому файлі, ієрархічна маршрутизація є ключовим механізмом, що дозволяє мережам масштабуватися1. Вона дозволяє розбивати мережу на домени, приховуючи внутрішню топологію одного домену від іншого та ізолюючи збої. Наприклад, протокол

OSPF активно використовує ієрархічну концепцію "зон", де вся комунікація між зонами має проходити через магістральну "Зону 0", яка, по суті, є коренем логічного дерева. Це підтверджує, що сучасні мережі, хоч і намагаються бути відмовостійкими, у своїй логіці глибоко ієрархічні. Протокольна ціна надійності: Проблема STP. Необхідно детальніше зупинитися на парадоксі надійності деревоподібних структур. Щоб усунути вразливість єдиного шляху, інженери додають фізичні резервні канали. Однак, як тільки це відбувається, топологія перестає бути "деревом" і перетворюється на граф із циклами. У комутованих мережах наявність циклу призводить до катастрофічного явища — широкомовного шторму. Один-єдиний кадр, надісланий на broadcast-адресу, починає нескінченно циркулювати по кільцю, розмножуючись на кожному комутаторі, що за лічені секунди повністю паралізує мережу. Для боротьби з цією топологічною проблемою був розроблений протокол Spanning Tree Protoco Його єдина функція — *примусово повернути* фізичну топологію з петлями до стану логічного "дерева". STP автоматично блокує всі порти, які створюють альтернативні шляхи. Це призводить до вкрай неефективного використання ресурсів: компанія витрачає кошти на прокладання дорогих резервних оптоволоконних ліній, які 99% часу простоюють, не передаючи жодного біта даних. Крім того, час збіжності класичного STP у разі аварії становить 30-50 секунд, що є неприйнятною перервою у наданні сервісу для сучасних додатків. Таким чином, деревоподібна топологія ставить проектувальника перед жорстким вибором: або нульова відмовостійкість, або низька ефективність використання каналів.

1.3.5. Топологія "Комірка"

Коміркова топологія є однією з найбільш надійних і гнучких структур, які використовуються у сучасних комп’ютерних мережах. Вона принципово відрізняється від ієрархічних схем, оскільки її головна ідея полягає у максимальній зв’язності між вузлами та наявності великої кількості надлишкових шляхів для передачі даних. У такій топології кожен вузол може бути з’єднаний з кількома іншими вузлами, що забезпечує високу відмовостійкість і дозволяє мережі залишатися

працездатною навіть у разі виходу з ладу окремих елементів. В архітектурі mesh-топології виділяють два основних підтипи: повнозв’язну сітку та частково зв’язну сітку. Повнозв’язна сітка — це ідеалізований варіант, у якому кожен вузол мережі має пряме з’єднання "точка-точка" з кожним іншим вузлом. У мережі з N вузлами кількість необхідних з’єднань зростає дуже швидко, оскільки для повної зв’язності потрібно прокласти N(N-1)/2 каналів. Така структура забезпечує максимальну надійність і дозволяє будь-якому вузлу напряму зв’язатися з будь-яким іншим, що мінімізує затримки та підвищує пропускну здатність. Однак повнозв’язна сітка є дуже дорогою та складною у реалізації, особливо для великих мереж, оскільки потребує величезної кількості кабелів і портів на кожному пристрої. Тому на практиці повний mesh використовується лише у невеликих критичних сегментах, де відмовостійкість є пріоритетом. Частково зв’язна сітка — це більш реалістичний і поширений варіант mesh-топології. У такій структурі лише найважливіші вузли з’єднані між собою великою кількістю каналів, тоді як менш важливі вузли мають лише один або два канали до цієї "основи". Кінцеві користувачі або периферійні пристрої зазвичай не є частиною сітки, а підключаються до неї за топологією "зірка" через один або кілька магістральних вузлів. Це дозволяє значно зменшити кількість необхідних з’єднань, зберігаючи при цьому основні переваги mesh-архітектури — надійність і гнучкість маршрутизації. Mesh-топологія широко використовується у магістральних мережах провайдерів, у великих корпоративних мережах, у бездротових ad-hoc мережах, а також у мережах Інтернету речей де важливо забезпечити самовідновлення та автоматичне перенаправлення трафіку у разі відмови окремих вузлів або каналів. Завдяки великій кількості альтернативних маршрутів, mesh-мережі здатні ефективно балансувати навантаження, уникати "вузьких місць" і забезпечувати високу якість сервісу навіть при динамічних змінах топології. Загалом, mesh-топологія є універсальним рішенням для побудови надійних, масштабованих і гнучких мереж, хоча її впровадження потребує ретельного планування та значних ресурсів, особливо у випадку повної сітки

Рисунок 1.5 - приклад Топології меш

Маршрутизація у сітчастих мережах є складним завданням, оскільки існує безліч можливих шляхів між двома точками, і мережа повинна динамічно обирати найкращий, уникаючи при цьому петель [12, с. 400; 14, с. 8]. Приклади реалізації:Інтернет є наймасштабнішим прикладом частково зв'язної сітки на рівні автономних систем. Магістральні мережі великих телекомунікаційних провайдерів також будуються як частково зв'язні сітки. Безпровідні Ad-Hoc мережі та мережі Інтернету речей часто використовують принципи Mesh для самоорганізації.

Переваги: Надзвичайно висока надійність та відмовостійкість: Це головна перевага. Завдяки величезній кількості альтернативних шляхів, відмова одного або навіть декількох вузлів чи каналів зв'язку не призводить до зупинки мережі. Трафік просто миттєво перенаправляється іншими маршрутами. Висока продуктивність:

Множинні паралельні шляхи дозволяють ефективно балансувати навантаження, розподіляючи потоки даних і уникаючи "вузьких місць".

Фундаментальні слабкості та обмеження: Екстремально висока вартість: Це стосується як повнозв'язної, так і частково зв'язної сітки. Вартість прокладання такої кількості кабелів та необхідність у великій кількості високошвидкісних портів на кожному маршрутизаторі робить цю топологію найдорожчою з усіх. Неймовірна складність розгортання та управління: Фізичне розгортання та подальше адміністрування N(N-1)/2 зв'язків у повнозв'язній сітці є практично неможливим завданням для мереж, більших за 5-10 вузлів. Складність протоколів маршрутизації: Це ключовий недолік на операційному рівні. Щоб сітка працювала і не колапсувала, потрібні надзвичайно складні адаптивні протоколи маршрутизації. Як детально описано у наданому файлі, існують два основні класи таких протоколів: Distance Vector та Link State. Протоколи DV страждають від проблеми "рахунку до нескінченності", яка виникає саме через наявність петель у сітчастій топології, коли вузли обмінюються невірною інформацією про втрачений маршрут. Для боротьби з цим потрібні "милиці" типу Split Horizon або Route Poisoning 6. Протоколи LS (як OSPF) є більш надійними, оскільки кожен вузол будує повну "карту" топології7. Однак, як було зазначено раніше, вони погано працюють у щільних сітчастих середовищах і вимагають штучного спрощення топології до "зірки".

Сучасне значення: "Часткова сітка" є безальтернативною топологією для побудови глобальних та магістральних відмовостійких мереж. Жодна інша топологія не може забезпечити рівень надійності, необхідний для функціонування Інтернету. Однак її вартість та складність означають, що вона ніколи не використовується для мереж доступу чи локальних мереж. Вона залишається прерогативою провайдерів та "ядра" Інтернету, тоді як на "краях" домінують ієрархічні "дерева" та "зірки".

Протокольний колапс та проблема масштабування станів Головною перешкодою для впровадження повноцінних сітчастих топологій є не стільки вартість кабелю, скільки нездатність протоколів маршрутизації ефективно керувати такою кількістю зв'язків.

1. "Лавина" службового трафіку: Протоколи стану каналу працюють за принципом: "якщо стан одного каналу змінився, про це мають дізнатися всі". У щільній сітчастій мережі кожен маршрутизатор має безліч сусідів. Зміна стану лише одного лінка викликає ланцюгову реакцію розсилки оновлень. У великій Mesh-мережі це призводить до того, що маршрутизатори витрачають більше ресурсів процесора на обробку службових повідомлень, ніж на пересилання корисних даних.

2. Пастка логічної повнозв'язності в BGP: У глобальних мережах (Інтернет) використовується протокол BGP. Для уникнення петель маршрутизації всередині однієї Автономної Системи вимагається, щоб усі BGP-маршрутизатори були з'єднані між собою логічною повнозв'язною сіткою.

Зі зростанням мережі підтримка сотень TCP-сесій між кожним маршрутизатором стає технічно неможливою. Щоб вирішити цю проблему, інженери змушені ламати ідеальну структуру "сітки" і впроваджувати Route Reflectors — спеціальні вузли, які централізують маршрутизацію. Це парадоксальна ситуація: фізично будується надійна "сітка", але логічно вона примусово перетворюється на ієрархічну "зірку" з Route Reflector у центрі, щоб протокол міг працювати. Це знову повертає мережу до проблеми централізованої точки відмови, нівелюючи переваги Mesh-топології. Таким чином, Mesh-топологія демонструє фундаментальний конфлікт між фізичною надійністю та логічною керованістю, який неможливо вирішити в рамках класичних підходів.

1.4. Гібридні (комбіновані) топології як практичний стандарт

Аналіз, проведений у попередніх підрозділах, наочно демонструє, що жодна з базових топологій у чистому вигляді не здатна задовольнити вимоги сучасних мереж. Кожна з них представляє екстремальний, незбалансований компроміс:

"Зірка" є надійною на рівні доступу, але має критичну центральну точку відмови і не може масштабуватися самостійно для охоплення, наприклад, цілої будівлі чи кампусу.

"Дерево" вирішує проблему масштабування "Зірки", але успадковує та посилює її вразливість на вищих ієрархічних рівнях.

"Повнозв'язна сітка" пропонує ідеальну надійність ціною практично нескінченної вартості та складності.

У результаті, будь-яка реальна мережа, що складається з більш ніж одного сегмента, за визначенням є гібридною (або комбінованою) топологією. Гібридна топологія — це не окремий тип, а радше практичний інженерний підхід, що полягає у цілеспрямованому поєднанні двох або більше базових топологій для досягнення конкретного балансу вартості, продуктивності, надійності та масштабованості.

1.4.1. Приклади та еволюція гібридних топологій

"Зірка-Шина": Історично поширена топологія, де декілька сегментів, побудованих за топологією "зірка" (з використанням концентраторів), з'єднувалися в єдину мережу за допомогою магістрального кабелю "шина" (наприклад, 10Base-5). Ця модель поєднувала низьку вартість "шини" зі зручністю обслуговування "зірки". Недолік: Зберігала всі фундаментальні проблеми "шини" (колізії, низька надійність магістралі).

"Зірка-Кільце": Більш надійна модель, де окремі "зірки" (наприклад, комутатори) підключалися до високошвидкісного магістрального "кільця" (часто подвійного, як у FDDI або SDH). Це забезпечувало високу надійність магістралі завдяки механізмам самовідновлення кільця. Недолік: Висока вартість та складність кільцевих технологій.

"Зірка-Дерево":Це де-факто домінуюча модель для всіх сучасних локальних та кампусних мереж. Насправді, топологія "Дерево", описана в 1.3.4, є просто найпоширенішим гібридом — ієрархічною комбінацією "зірок".

Рівень доступу (Access): Класичні "зірки", де кінцеві пристрої підключаються до комутаторів доступу.

Рівень розподілу: "Зірка" вищого порядку, де комутатори доступу (центри "зірок" нижчого рівня) підключаються до комутаторів розподілу.

Рівень ядра: "Зірка" найвищого рівня, де комутатори розподілу підключаються до центральних кореневих комутаторів. Ця модель є надзвичайно популярною через свою структурованість, керованість та відносну простоту проектування.

Глобальна гібридна модель (Інтернет): Сам Інтернет є наймасштабнішим прикладом гібридної топології. Він складається з:

Ядра: Глобальна частково зв'язна сітка, що складається з маршрутизаторів великих провайдерів (Автономних Систем - AS).

Мереж доступу: Мільйони корпоративних та локальних мереж, побудованих за ієрархічною деревоподібною ("Зірка-Дерево") топологією, які підключаються до цього сітчастого ядра.

Отже, сучасний мережевий ландшафт являє собою складну систему, у якій ієрархічні "дерева" доступу інтегруються у глобальну "сітку" магістралей.

1.5. Фундаментальні слабкості сучасних гібридних архітектур

Критично важливо розуміти, що комбінування топологій не усуває їхні вроджені недоліки. Воно лише маскує, переміщує або ускладнює їх, створюючи нові, системні рівні проблем. Слабкості гібридних мереж є більш тонкими і виявляються не стільки у фізичних відмовах, скільки у надзвичайній операційній складності.

1.5.1. Успадкування та посилення критичних точок відмови (SPOF)

Найпоширеніша гібридна модель, "Зірка-Дерево", бере слабкість "зірки" і перетворює її на системну загрозу. На рівні доступу відмова комутатора паралізує роботу однієї "зірки". Це прийнятний ризик. Однак на рівні розподілу відмова комутатора паралізує десятки сегментів доступу. На рівні ядра відмова кореневого комутатора призводить до тотального колапсу всієї мережі кампусу. Таким чином, ієрархічна гібридизація не усуває, а концентрує ризик у вузлах вищого рівня. Це змушує інженерів вдаватися до дорогих та складних методів апаратного резервування (дублювання шасі, блоків живлення, використання технологій стекування) та

протоколів. Ці технології є реактивними обходами, а не фундаментальним вирішенням проблеми, закладеної у самій топології.

1.5.2. Проблема "вузьких місць" та неоптимальних шляхів

Ієрархічна структура диктує жорсткі, негнучкі шляхи передачі даних. Як було зазначено, трафік між двома вузлами, що знаходяться на різних гілках, змушений подорожувати "вгору" до спільного вузла-попередника і "вниз".

У великій гібридній мережі це призводить до значної неефективності. Наприклад, два сервери у сусідніх стійках дата-центру, підключені до різних комутаторів, змушені відправляти трафік через комутатор кінця ряду або навіть на рівень агрегації, хоча фізично вони знаходяться у метрі один від одного.

Це створює постійні "вузькі місця" на висхідних каналах та на комутаторах вищих рівнів, через які проходить весь "міжгілковий" трафік.

Мережа, спроектована для зручності кабелювання та логічної структури ("Дерево"), виявляється фундаментально неоптимальною з точки зору затримок та ефективності використання шляхів.

1.5.3. Експоненційне зростання складності управління та маршрутизації

Це найскладніша і найважливіша проблема гібридних мереж. Коли різні топологічні моделі стикаються, вони створюють межі доменів з різними правилами та протоколами. Це перетворює мережеву інженерію з фізичного завдання на надзвичайно складне програмно-адміністративне.

Межі протоколів: Гібридна мережа не може керуватися одним протоколом. Усередині кампусу зазвичай використовується протокол Interior Gateway Protocol, такий як OSPF або IS-IS. Але для підключення до інших використовується протокол Exterior Gateway Protocol, яким є BGP.

Необхідність у "Ре-дистрибуції": На межі цих двох доменів виникає завдання "ознайомити" протоколи один з одним. Цей процес, званий ре-дистрибуцією , є

складним, ручним процесом, який "дозволяє передавати інформацію про маршрутизацію з одного домену маршрутизації в інший".

Ризик неконсистентності та петель: Як слушно застерігається у джерелі, редистрибуція є небезпечною і "не повинна вносити невідповідності в маршрутизацію". Наприклад, "петля маршрутизації може утворитися, якщо... маршрут, вивчений в IGP і експортований в EGP, потім реімпортується в IGP".

Політики маршрутизації: У великих гібридних "сітках" вибір шляху взагалі перестає бути технічним завданням. Як описано у главі 11, маршрутизація визначається комерційними угодами та політиками. Наприклад, компанія може свідомо спрямовувати трафік довшим, але дешевшим шляхом. Це означає, що топологія стає настільки складною, що її робота визначається не фізикою, а набором суперечливих рукотворних правил.

Агрегація маршрутів: Щоб якось впоратися з мільйонами маршрутів у глобальній гібридній мережі, адміністратори змушені вдаватися до агрегації. Це метод "згортання" багатьох окремих маршрутів в один загальний. Однак, як зазначається у джерелі, це може призвести до "неточних маршрутів" , де оголошений шлях не відповідає дійсності для всіх підмереж, що ускладнює діагностику.

1.5.4. Статичність та низька адаптивність

Сучасна гібридна "Зірка-Дерево" архітектура є статичною та ригідною. Вона визначається фізичним прокладанням кабелів та ієрархією комутаторів, спроектованих роками раніше. Якщо характер трафіку раптово змінюється (наприклад, відділ А починає інтенсивно обмінюватися даними з відділом Б, а не з центральним сервером), мережа не може динамічно адаптуватися. Вона не може створити новий, короткий шлях. Трафік вперто продовжуватиме йти "вгору і вниз" по ієрархії, перевантажуючи ядро. Єдиною відповіддю інженерів на це є "груба сила"— заздалегідь закладати надлишкову пропускну здатність на магістральних каналах та в ядрі, сподіваючись, що її вистачить. Це економічно неефективний підхід. Зазначені системні слабкості — концентровані точки відмови, неоптимальні шляхи, надмірна

програмна складність на стиках доменів та ригідність — свідчать про те, що існуюча гібридна модель, хоча й функціонує, досягла межі своєї ефективності.

1.6. Сучасні підходи та технології для компенсації недоліків топологій

Виявлені у Розділі 1.5 фундаментальні слабкості домінуючих гібридних топологій не залишилися поза увагою мережевої індустрії. У відповідь на ці виклики було розроблено низку складних технологій та цілих архітектурних підходів. Їхня мета — не замінити базову топологію, а компенсувати її вроджені недоліки на операційному та логічному рівнях. Аналіз зазначених "компенсаторних" рішень є критично важливим, оскільки він демонструє, що замість спрощення сучасні мережі розвиваються шляхом нарощування технологічної та програмної складності з метою забезпечення ефективної роботи неоптимальних топологій.

1.6.1. Компенсація петель та блокованих каналів: Еволюція від STP до MLAG

Як було зазначено, базове "Дерево" вразливе, оскільки не має надлишкових шляхів. Просте додавання резервного каналу створює петлю комутації. У мережі Рівня 2 це призводить до катастрофи: широкомовні кадри починають нескінченно циркулювати, множитися і за лічені секунди повністю паралізують мережу.

Рішення 1 (Класичне) - Spanning Tree Protocol: Це протокол, розроблений для того, щоб дозволити фізичне існування петель у топології, але запобігти їм на логічному рівні. STP автоматично виявляє всі шляхи в мережі та логічно блокує всі "надлишкові" канали, залишаючи лише один активний шлях до кореня дерева. Слабкість STP: Це жахливо неефективно. Компанія платить за дорогий, високошвидкісний резервний канал, який 99.9% часу простоює і не використовується для передачі даних. Він активується лише після збою основного, що також вимагає часу на збіжність протоколу.

Рішення 2 (Сучасне) - MLAG та стекування: Щоб вирішити проблему блокованих каналів та одночасно забезпечити резервування центральних вузлів, були

винайдені технології віртуалізації шасі. Стекування: Декілька фізичних комутаторів з'єднуються спеціальними високошвидкісними шинами і логічно "зливаються" в один віртуальний комутатор з єдиним інтерфейсом управління. MLAG: Більш гнучка технологія, що дозволяє двом незалежним комутаторам логічно представлятися для пристроїв нижчого рівня як один пристрій. Це дозволяє комутатору доступу підключити один канал до Комутатора_Ядра_А, а другий — до Комутатора_Ядра_Б, і об'єднати їх в єдиний логічний канал. З точки зору STP, петлі більше немає, оскільки обидва канали ведуть до "одного" логічного вузла. Слабкість цього підходу: Це надзвичайно складні технології, які часто є "чорною скринькою" конкретного виробника. Вони вирішують проблему петель на рівні ядра/розподілу, але роблять це ціною значного ускладнення конфігурації та залежності від пропрієтарних реалізацій.

1.6.2. Компенсація "вузьких місць" у дата-центрах: Архітектура Leaf-Spine

Класична трирівнева топологія "Дерево" катастрофічно погано працює у сучасних дата-центрах. У ЦОД основна маса трафіку (до 70-80%) — це не трафік "Північ-Південь", а трафік "Схід-Захід". Це трафік між компонентами розподілених додатків, базами даних, сховищами тощо. У "Дереві" такий трафік змушений постійно підніматися до рівня розподілу або ядра і спускатися вниз, створюючи жахливі "вузькі місця" та непередбачувані затримки.

Рішення (Сучасне) - Leaf-Spine: Це повний перегляд ієрархічної моделі на користь двошарової сітчастої архітектури.

Рівень Leaf (Листя): Це комутатори доступу (Top-of-Rack), до яких підключаються сервери.

Рівень Spine (Хребет): Це магістральні комутатори ядра. Кожен комутатор Leaf підключений до кожного комутатора Spine. При цьому комутатори Leaf ніколи не з'єднуються між собою, і комутатори Spine ніколи не з'єднуються між собою. Це створює топологію, де будь-який сервер знаходиться на однаковій, фіксованій та передбачуваній відстані від будь-якого іншого сервера в ЦОД — рівно 4 стрибки.

Ця архітектура використовує протоколи Рівня 3 та ECMP, що дозволяє одночасно використовувати всі наявні канали для балансування навантаження. Слабкість цього підходу: Архітектура Leaf-Spine є блискучим вирішенням проблеми "Схід-Захід", але це високоспеціалізоване рішення. Воно оптимізоване виключно для дата-центрів. Воно не застосовується (і не може бути легко застосоване) для географічно розподілених кампусних або міських мереж через величезні кабельні витрати та жорстку структуру. Це доводить, що для вирішення проблеми "Дерева" довелося, по суті, винайти нову, вузькоспеціалізовану топологію.

1.6.3. Компенсація складності управління та ригідності: Програмно-конфігуровані мережі

Гібридні мережі є жахливо складними в та абсолютно статичними. Мережевий інженер змушений вручну налаштовувати сотні пристроїв, щоб змусити трафік рухатися правильно.

Рішення (Найсучасніше) - Software-Defined Networking: Це не топологія, а архітектурна парадигма, яка пропонує вирішити проблему складності, кардинально змінивши підхід до управління. Як детально описано у наданому файлі, SDN базується на трьох стовпах: "поділ функцій управління та пересиланн". Фізичний комутатор стає простим "виконавцем", який лише пересилає пакети.

Централізація "мозку": "централізація управління: вся мережа координується... контролером". Цей контролер (control plane) є потужним ПО, яке бачить всю мережу цілком. Чіткі інтерфейси: Контролер спілкується з "залізом" через стандартизовані протоколи. Замість того, щоб тисячі розподілених маршрутизаторів намагалися узгодити "карту" мережі між собою, єдиний контролер отримує "глобальний, абстрактний погляд на мережу" і проактивно або реактивно розраховує всі шляхи і "заливає" правила пересилання на комутатори. Слабкість цього підходу: SDN є лише логічною надбудовою. Не вирішує фізичних проблем: SDN не може змінити той факт, що топологія "Дерево" має "вузьке місце" або що між двома вузлами немає прямого фізичного каналу. Воно може лише краще керувати трафіком

в обхід цих проблем, але не усуває їх. Створює нову точку відмови: Як слушно зазначено у джерелі, сам контролер "може становити єдину точку відмови та 'вузьке місце'". Масштабованість контролера: Управління величезною мережею з одного центрального пункту є надзвичайно складним обчислювальним завданням. Складність заради складності: По суті, SDN є найскладнішим програмним комплексом, винайденим для того, щоб змусити працювати негнучку та неоптимальну фізичну інфраструктуру. Зазначені компенсаторні технології свідчать про усвідомлення індустрією проблем існуючих топологій. Проте всі ці рішення є реактивними та додають нові рівні складності (пропрієтарної, архітектурної або програмної), не вирішуючи проблему на фундаментальному топологічному рівні.

Протокольна ціна петель: Механізми таймерів у RIP, Проблема "рахунку до нескінченності" є настільки фундаментальною для топологій з петлями, що протокол RIP був змушений інтегрувати не лише евристики, але й складний, заснований на таймерах механізм для виявлення "мертвих" маршрутів. Цей механізм є прямим наслідком того, що у сітчастій топології вузол ніколи не може бути впевнений, чи є отримана ним інформація актуальною, чи це "луна" його власних старих анонсів. Якщо вузол отримав інформацію про те, що вартість маршруту зросла (що є ознакою потенційного "рахунку до нескінченності"), він "заморожує" цей маршрут на 180 секунд. У цей час він ігнорує будь-які оновлення про цей маршрут від інших сусідів, які пропонують гіршу метрику, чекаючи, поки "чутки вляжуться".

Висновок: Замість швидкої реакції на збій, топологія з петлями змушує протокол DV (RIP) діяти вкрай повільно, обережно та консервативно. Мережа може перебувати у неконсистентному стані хвилинами (час збіжності), поки всі ці таймери не спрацюють. Це пряма ціна, яку доводиться платити за надійність (надлишкові шляхи) при використанNIсі простого протоколу, нездатного "бачити" топологію цілком.

1.7. Вплив топологічних обмежень на складність мережевих протоколів

Аналіз є неповним без детального розгляду того, як недоліки фізичних і логічних топологій безпосередньо впливають на проектування та функціонування мережевих протоколів. Значна частина складності сучасного стеку протоколів TCP/IP зумовлена не функціональною необхідністю, а вимушеною програмною компенсацією за неоптимальність, неоднозначність і ризики, притаманні топології. Топологія диктує правила гри, а протоколи — це складний набір правил, розроблений для того, щоб гра не зайшла у глухий кут.

1.7.1. Проблема петель та "Рахунок до нескінченності"

Найперша і найочевидніша проблема будь-якої не-деревоподібної топології— це петлі маршрутизації. Виникнення проблеми: У сітчастій топології, де вузол A може дістатися до вузла D через B і C, може виникнути ситуація (особливо під час збою), коли B вважає, що найкращий шлях до D лежить через C, а C вважає, що найкращий шлях до D лежить через B. Пакет, що потрапив у цю "гравітаційну пастку", буде нескінченно циркулювати між B і C, поки його час життя не закінчиться, марно витрачаючи ресурси мережі. Це змусило розробників протоколів Distance Vector таких як RIP, винаходити складні механізми-милиці. Як детально описано у наданому файлі, протоколи DV страждають від проблеми "рахунку до нескінченності". Це специфічна проблема DV, яка виникає через те, що "інформація, включена в DV, не враховує топологію мережі". Якщо зв'язок з A падає, вузол B може отримати від C "стару" інформацію про те, що C може дістатися до A, і B вирішить, що знайшов новий шлях до A через C. Вартість цього "шляху-привида" буде ітеративно зростати, поки не досягне "нескінченності".

Рішення: Щоб боротися з цим, у протоколи DV були примусово додані складні евристики, які не є частиною базового алгоритму, а є саме "латками" проти недоліків топології:

Штучне обмеження метрики, яке, однак, робить протокол непридатним для великих мереж. Розділений горизонт "Якщо C досягає A через B, немає сенсу для B намагатися досягти A через C". Це правило, яке забороняє анонсувати маршрут назад на той інтерфейс, звідки він прийшов. Примусове оголошення маршруту, що зник, з метрикою "нескінченність", щоб прискорити збіжність.

Висновок: Сама наявність топології з петлями робить прості протоколи DV нестабільними і вимагає їх штучного ускладнення.

1.7.2. Проблема обчислювальної складності "Карти мережі"

Усвідомивши недоліки DV, індустрія перейшла до більш надійних протоколів Link State, таких як OSPF. Ідея LS полягає в тому, що "кожен вузол може створити карту мережі... і з неї отримати таблицю маршрутизації". Кожен вузол має повну інформацію про топологію.

Виникнення проблеми: Цей підхід чудово працює... доки топологія не стає занадто щільною. Як було детально проаналізовано у наданому файлі, протоколи LS "страждають у присутності широкомовних мереж де будь-яка сутність має прямий доступ до будь-якої іншої створюючи повнозв'язну множину суміжностей".

Алгоритм Дейкстри, який використовує OSPF для розрахунку шляхів, має складність, що залежить від кількості зв'язків "Вибух" кількості зв'язків робить обчислення надто важкими. Кожен маршрутизатор буде розсилати інформацію про стан своїх зв'язків N-1 іншим маршрутизаторам, створюючи трафік порядку .

Щоб вирішити цю топологічну проблему, протокол OSPF вдається до геніального, але штучного трюку. Він примусово змінює логічну топологію:

Вибір Псевдо-Вузла: Маршрутизатори обирають "Призначеного маршрутизатора".

Трансформація топології: Замість того, щоб бачити "сітку", всі інші маршрутизатори у сегменті встановлюють "сусідство" тільки з цим DR. "Рішення полягає у тому, щоб трансформувати широкомовну топологію у зіркоподібну топологію, додавши псевдо-вузол.

Висновок: Навіть найбільш досконалий протокол IGP змушений відмовитися від реальної топології та штучно емулювати простішу , щоб забезпечити функціонування. Це свідчить про те, що класичні топології є надто складними для ефективного програмного управління.

1.7.3. Проблема масштабованості та необхідність ручної ієрархії

Жоден з протоколів не може працювати у дійсно великому масштабі в одній "плоскій" топології. У великій мережі таблиці маршрутизації стають гігантськими. Будь-яка незначна зміна спричинить ланцюгову реакцію оновлень, яка паралізує мережу.

Вплив на протоколи: Це змусило розробників вбудувати ієрархію безпосередньо у самі протоколи. OSPF (який є протоколом IGP) "не рекомендує мати більше 200 маршрутизаторів в одній зоні". Мережа примусово ділиться на "зони", що є, по суті, доменами маршрутизації. Уся комунікація між зонами має йти через "магістральну Зону 0", яка виступає коренем дерева. Це є прямим переходом від "плоскої сітки" до логічного "дерева".

BGP та Автономні Системи: На глобальному рівні використовується BGP. BGP є протоколом Path Vector, який є еволюцією DV. Він вирішує проблему петель, записуючи у маршрут повний список "Автономних Систем" (AS), які він пройшов 17. Це дозволяє уникнути петель, але робить протокол повільним, громіздким і абсолютно залежним від ручних політик, які часто базуються на комерційних угодах, а не на технічній оптимальності.

Висновок: Неможливість ефективної обробки великих, плоских або сітчастих топологій змушує розробників протоколів штучно та примусово розділяти мережі на ієрархічні домени, що підкреслює недоліки топологій, які вони організовують.

2 ОГЛЯД НАЯВНИХ ФРАКТАЛЬНИХ СТРКУТУР ТА ЇХ МОЖЛИВИХ ГІБРИДІВ, ТА РОЗРАХУНКИ ЇХ ЕФЕКТИВНОСТІ

2.1. Сучасні виклики масштабованості мереж та передумови впровадження фрактального підходу

У теорії складних систем ключовим питанням при проектуванні мережевої інфраструктури є вибір між централізованим управлінням та самоорганізацією. Традиційні ієрархічні моделі (топологія "дерево") забезпечують простоту управління та чітку підпорядкованість, проте страждають від обмеженої масштабованості через перевантаження кореневих вузлів. З іншого боку, децентралізовані стохастичні мережі, які формуються еволюційним шляхом (як мережа Інтернет на рівні AS), демонструють високу живучість, але характеризуються низькою передбачуваністю параметрів якості обслуговування та складністю маршрутизації.

Актуальною науково-технічною проблемою є пошук топологічних моделей, які б поєднували переваги обох підходів: децентралізацію та високу зв'язність, властиву випадковим графам, із структурною впорядкованістю та алгоритмічною простотою, властивою регулярним решіткам.

У цьому контексті фрактальна геометрія, основи якої заклав Б. Мандельброт [6, с. 15], набуває нового значення як фундамент для топологічного синтезу. Їхньою визначальною рисою є детермінована самоподібність. На відміну від стохастичних моделей, де зв'язки виникають з певною ймовірністю, у фрактальних моделях структура мережі задається чітким рекурсивним правилом. Це дозволяє точно розраховувати характеристики мережі для будь-якого масштабу ще на етапі проектування, що є критично важливим для інженерних систем гарантованої надійності. Метою даного розділу є формалізація математичного апарату для опису фрактальних топологій, визначення їхніх метричних характеристик та проведення порівняльного аналізу з класичними моделями теорії графів.

2.2. Теоретико-графовий формалізм опису мережевих структур

Для проведення кількісного аналізу будь-яка телекомунікаційна мережа моделюється як скінченний граф [3, с. 88; 9, с. 45]. Нехай G = (V, E) — неорієнтований граф без петель і кратних ребер, де:

V = {v1,v2, ...,vn } — множина вершин, що відповідають комутаційним вузлам (маршрутизаторам, комутаторам);

E = {e1,e2 , ..., en} — множина ребер, де кожне ребро = (vi,vj) відповідає фізичному або логічному каналу зв'язку між вузлами

Топологічна структура графа повністю визначається його матрицею суміжності A розмірністю N x N:

$$A_{IJ} = \begin{cases} 1, \text{якщо } (v_i, v_j) \in E \\ 0, \text{в іншому випадку} \end{cases} \quad (2.1)$$

A_{IJ} *– елемент матриці суміжності на перетині і-го рядка та j-го стовпця:*

v_i, v_j – вершини графа (наприклад, комутатори або маршрутизатори);

E - множина ребер (каналів зв'язку) у графі;

1 - означає наявність прямого зв'язку між вузлами;

0 - означає відсутність зв'язку.;

2.2.1. Локальні характеристики вузлів

Ступінь вершини:

$$k_i = \sum_{j=1}^{N} A_{ij} \quad (2.2)$$

k_i *– ступінь і-ї вершини;*

N - загальна кількість вершин у графі;

A_{IJ} *– елемент матриці суміжності;*

Ступінь вершини визначається як кількість ребер, інцидентних цій вершині:В інженерному сенсі ki відповідає кількості фізичних портів маршрутизатора. Важливою характеристикою топології є розподіл ступенів .

Регулярні графи: ki для всіх i. Це спрощує уніфікацію обладнання.

Випадкові графи:ki варіюється навколо середнього значення (k) (розподіл Пуассона).

Безмасштабні графи: Розподіл підкоряється степеневому закону , що означає наявність "хабів" з аномально високим ступенем. Фрактальні топології, що розглядаються в роботі, тяжіють до регулярних структур, що дозволяє уникнути проблеми "супер-хабів".

Коефіцієнт кластеризації:Локальний коефіцієнт кластеризації показує, наскільки сусіди вузла зв'язані між собою. Він визначається як відношення кількості фактичних ребер між сусідами до максимально можливої їх кількості:

$$C_i = \frac{2E_i}{k_i(k_i-1)} \quad (2.3)$$

C_i – коефіцієнт кластеризації для вузла I;

E_i - кількість фактичних ребер, що існують між сусідами вузла I;

k_i – ступінь і-ї вершини;

$k_i(k_i - 1)/2$ – максимально можлива кількість ребер між k_i сусідами;

Високе значення середнього коефіцієнта кластеризації (C) свідчить про наявність локальних груп (клік), що є бажаним для локалізації трафіку всередині підмереж.

2.2.2. Глобальні характеристики мережі

Найкоротший шлях та Діаметр:Нехай d(vi,vj) — геодезична відстань (кількість хопів) між вершинами. Діаметр мережі (D) — це максимальна відстань між будь-якою парою вершин у графі:

$$D = \max d(v_i, v_j) \quad (2.4)$$

D - діаметр графа.

max — оператор пошуку максимального значення;

v_i, v_j – вершини графа;

$d(v_i, v_{j)}$ – геодезична відстань (найкоротший шлях у кількості хопів) між вершинами і та j.

Діаметр визначає максимальну затримку передачі сигналу. Для ефективних топологій бажано, щоб D зростав повільно зі збільшенням N.

Середня довжина шляху (L):

$$L = \frac{1}{N(N-1)} \sum_{I \neq J} D(v_i, v_i) \quad (2.5)$$

L - середня довжина шляху;

N - загальна кількість вершин у графі;

N(N-1) — загальна кількість можливих пар вершин;

$\sum_{I \neq J} D(v_i, v_i)$ – сума довжин найкоротших шляхів між усіма парами вершин;

Цей параметр характеризує загальну ефективність маршрутизації в мережі. Фрактальні графи часто демонструють властивість "тісного світу", У 1998 році Дункан Ватц та Стівен Строгац запропонували модель мереж "тісного світу" [19, с. 440], яка поєднує високий коефіцієнт кластеризації з малим діаметром, де L залишається малим навіть при значному зростанні мережі.

Спектральні властивості:

Структурна стійкість та зв'язність графа визначаються спектром його матриці Лапласа L = Deg - A, де Deg — діагональна матриця ступенів.

Друге найменше власне значення цієї матриці,, є мірою того, наскільки важко розділити граф на ізольовані компоненти. Високе значення у фрактальних графах корелює з високою швидкістю поширення інформації та стійкістю до відмов каналів.

2.3. Математичний апарат фрактальної геометрії

Фрактальний підхід пропонує розглядати топологію мережі як результат ітеративного процесу. Для математичного опису використовується апарат Систем Ітерованих Функцій.

2.3.1. Детермінована рекурсія

На відміну від стохастичних моделей зростання мережі (наприклад, модель Барабаші-Альберт, де нові вузли приєднуються до мережі з ймовірністю, пропорційною ступеню існуючих вузлів), фрактальні моделі є повністю детермінованими.

Процес побудови описується послідовністю графів G0,G1 , ...,GN , де:

G0(Ініціатор) — базовий граф-затравка.

GN(Генератор) — граф, отриманий з Gn-1шляхом застосування операції заміни або реплікації.

Найпоширенішим методом для мережевих топологій є метод реплікації та з'єднання. Мережа на ітерації n складається з M копій мережі ітерації n-1, які з'єднуються між собою через визначені граничні вершини. Кількість вершин зростає за експоненційним законом N(n) = Mn, що забезпечує високу масштабованість.

2.3.2. Фрактальна розмірність графа

Поняття розмірності для графів відрізняється від класичного визначення Хаусдорфа для геометричних фігур. У теорії складних мереж часто використовують box-counting dimension dB.

Для цього граф покривають мінімальною кількістю підграфів розміру . Якщо кількість таких підграфів, то фрактальна розмірність визначається співвідношенням:

$$N_B(l_B) \sim l_B^{-d_B} \tag{2.6}$$

N_B- мінімальна кількість підграфів, необхідних для покриття всієї мережі;
l_B- розмір "коробки";
$-d_B$ - фрактальна розмірність;

Це співвідношення показує, як змінюється кількість необхідних ресурсів (коробок) при зміні масштабу спостереження (lB).

Для лінійних топологій dB = 1.

Для повних решіток (Mesh) dB =2.

Для фрактальних топологій 1 < dB< 2.

Це значення вказує на те, що фрактальні мережі займають проміжне положення: вони є більш "щільними" та зв'язними, ніж дерева, але більш "розрідженими" та економічними, ніж повні сітки.

2.3.3. Само подібність як основа адресації

Ключовою властивістю, що робить фрактали привабливими для інженерії, є топологічна само подібність, досліджена у роботах Song et al. **[17, с. 392]**. Це означає, що локальна структура мережі (наприклад, підмережа відділу) ізоморфна глобальній структурі (магістралі).

Це дозволяє запровадити ієрархічну систему координат. Замість використання таблиць маршрутизації, шлях між вузлами може бути обчислений аналітично, базуючись на їхніх координатах у фрактальній структурі. Це усуває потребу у протоколах обміну маршрутною інформацією (flooding), які є основним джерелом накладних витрат у класичних мережах.

2.4. Математичний апарат генерації фрактальних топологій

Побудова фрактальної мережі базується на строгому алгоритмічному підході, що виключає хаотичність, притаманну еволюційному розвитку мереж. Основним інструментом тут виступають Системи Ітерованих Функцій

2.4.1. Детермінована рекурсія як метод синтезу

На відміну від стохастичних моделей (наприклад, моделі Барабаші-Альберт, де нові вузли приєднуються до мережі з ймовірністю, пропорційною ступеню існуючих вузлів), фрактальні моделі є повністю детермінованими. Процес побудови описується послідовністю графів $G0,G1,...,Gn$, де кожен наступний граф є результатом застосування оператора реплікації до попереднього.

Найпоширенішим методом для мережевих топологій є метод реплікації та з'єднання. Мережа на ітерації n складається з M копій мережі ітерації n-1, які

з'єднуються між собою через визначені граничні вершини. Кількість вершин N(n) зростає за експоненційним законом , що забезпечує високу масштабованість при збереженні фіксованих правил комутації.

2.4.2. Фрактальна розмірність як індикатор мережевої ефективності

Поняття розмірності для складних мереж детально розглядається у сучасних дослідженнях **[15, с. 5]**. У теорії складних мереж часто використовують розмірність подібності (ds).

$$d_s = \frac{\ln N}{\ln(1/s)} \quad (2.7)$$

d_s- розмірність подібності;

N - кількість самоподібних частин, на які розбивається фігура;

s - коефіцієнт подібності , s < 1 ;

Цей показник має пряму інженерну інтерпретацію:

Ds = 1 (Лінійні структури): Мережа є економічною (мінімум кабелю), але вразливою до розривів. Затримка зростає лінійно з кількістю вузлів.

Ds = 2 (Площинні структури, Mesh): Мережа щільно покриває територію, має високу надійність, але вартість портів та кабелів стає надмірною.

1 < ds < 2 (Фрактальні структури): Це оптимальний баланс. Такі топології забезпечують наявність альтернативних маршрутів (циклів) для відмовостійкості, але залишаються "розрідженими", що дозволяє використовувати стандартне обладнання.

2.5. Структурно-функціональний аналіз топології на базі Трикутника Серпінського

Топологія Трикутника Серпінського (Sierpinski Gasket) є базовою моделлю планарного графа, що поєднує властивості ієрархічності та кільцевого резервування. Вона є особливо актуальною для проектування кампусних мереж, сенсорних мереж (WSN) та мереж промислового інтернету речей (IIoT), де критичними є вимоги до надійності при обмежених апаратних ресурсах.

2.5.1. Алгоритм побудови та метричні характеристики

Граф ST(n) будується ітеративно. Базисом (n=0) є повний граф з трьох вершин K3 (цикл). На кожному наступному кроці три копії графа попереднього рівня об'єднуються шляхом злиття кутових вершин. Ключовою інженерною характеристикою є обмеженість ступеня вузла. У класичних мережах типу Scale-Free існують "хаби", ступінь яких може сягати сотень, що вимагає дорогого модульного обладнання. У графі Серпінського розподіл ступенів є бімодальним і строго обмеженим:

Внутрішні вузли (k=4): Абсолютна більшість вузлів мережі має ступінь 4. Це означає, що для побудови мережі будь-якого масштабу достатньо використовувати уніфіковані комутатори з 4-ма портами. Це значно спрощує логістику та обслуговування).

Граничні вузли (k=2): Три вершини зовнішнього периметра завжди мають 2 вільні порти (в рамках даної ітерації), що робить їх ідеальними точками входу/виходу для підключення до зовнішніх мереж або інших кластерів.

Кількість вузлів зростає за законом.

$$\mathrm{N}(t) = \frac{3}{2}(3^t + 1) \qquad \textbf{(2.8)}$$

N(t) - кількість вузлів у мережі на ітерації t;

t - номер ітерації;

3 - кількість копій на кожному кроці;

Це дозволяє точно планувати ємність мережі. Наприклад, мережа 5-ї ітерації міститиме 366 вузлів, що відповідає масштабу великого підприємства.

2.5.2. Аналіз відмовостійкості: Перевага над класичними протоколами

Класичні топології покладаються на протоколи маршрутизації для забезпечення відмовостійкості.

Однак ці протоколи мають свої вроджені вади, описані в технічній літературі. У звичайних мережах наявність петель створює проблеми для протоколів дистанційного вектора, таких як RIP. Як зазначається у джерелах, це може призвести

до явища "рахунку до нескінченності", коли вузли нескінченно обмінюються застарілою інформацією про недоступний маршрут.

Фрактальне вирішення: Топологія Трикутника Серпінського містить цикли на кожному рівні ієрархії. Проте ці цикли не є хаотичними. Структура мережі гарантує, що при виході з ладу будь-якого внутрішнього ребра існує рівно один локальний обхідний шлях довжиною в 2 хопи. Це дозволяє реалізувати механізми швидкого перемикання без необхідності запуску складних алгоритмів збіжності по всій мережі.

2.5.3. Проблема "штормів" та її вирішення

У класичних широкомовних мережах наявність петель призводить до "широкомовних штормів", для боротьби з якими використовують протокол STP. STP блокує резервні порти, фактично перетворюючи надійну фізичну топологію на ненадійне логічне дерево. Завдяки чіткій сегментації, широкомовний трафік у фрактальній мережі може бути легко локалізований у межах одного трикутника. Вузькі місця з'єднання кластерів діють як природні фільтри, що запобігають поширенню шторму на всю мережу. Це підвищує загальну стабільність системи порівняно з "плоскими" мережами.

2.5.4. Ефективність маршрутизації та діаметр мережі

Діаметр мережі ST(n) зростає як . Хоча це швидше, ніж у випадкових графів, це значно краще, ніж у лінійних топологій або простих кілець.

Порівняння з Кільцем: У кільці з N вузлів максимальний шлях дорівнює N/2. При N=100 затримка буде значною.

Фрактальний "Shortcut": У Трикутнику Серпінського того ж розміру діаметр буде значно меншим завдяки наявності внутрішніх "перемичок", що з'єднують віддалені частини мережі. Це забезпечує прийнятну затримку для додатків реального часу.

Крім того, детермінована структура дозволяє відмовитися від складних протоколів стану каналу, таких як OSPF, які вимагають розсилання інформації про топологію всім вузлам . У фрактальній мережі кожен вузол може знати своє місцеположення та обчислювати маршрут алгоритмічно, що зменшує навантаження на канали зв'язку службовим трафіком.

2.6. Хроматичне число та частотне планування

Важливим аспектом є застосування даної топології у бездротових мережах. Тут критичною проблемою є інтерференція.

Граф Серпінського є 3-кольоровим (хроматичне число). Це означає, що всім вузлам мережі можна призначити один з трьох частотних каналів так, щоб жодні два сусідні вузли не використовували одну й ту саму частоту. Це дозволяє побудувати бездротову мережу високої щільності без взаємних завад, використовуючи лише стандартний діапазон частот, що є значною перевагою перед хаотичними ad-hoc мережами.

Структурно-функціональний аналіз решітчастих топологій на базі Килима Серпінського**,** У той час як Трикутник Серпінського оптимізує використання портів та довжину ліній зв'язку, топологія "Килим Серпінського" пропонує альтернативну парадигму, спрямовану на максимізацію пропускної здатності та паралелізму обробки даних. Ця структура є фрактальним узагальненням класичної квадратної решітки, але з критичними архітектурними відмінностями, що дозволяють подолати обмеження останньої.

2.6.1. Проблема масштабування класичних решіток

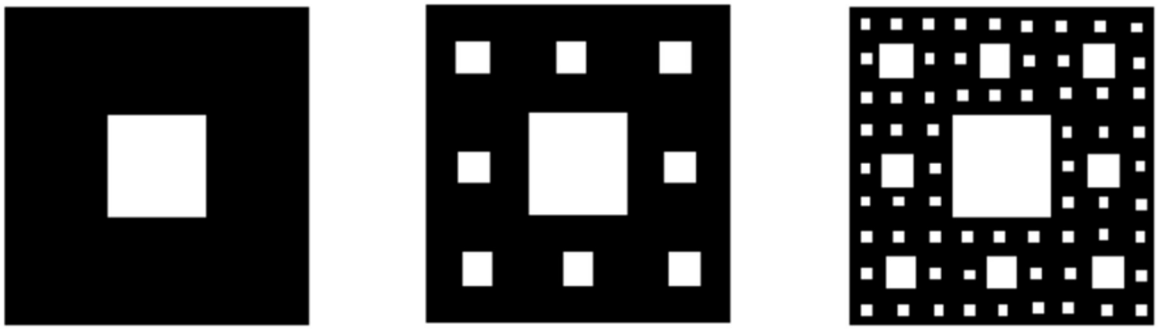

Рисунок 2.1 - Килим серпінсього

Щоб зрозуміти переваги Килима Серпінського, необхідно проаналізувати недоліки класичної повної решітки, яка часто використовується в суперкомп'ютерах та мережах на кристалі.

Центральне перевантаження: У квадратній решітці найкоротші шляхи між діагонально протилежними кутами мережі неминуче проходять через геометричний центр. При рівномірному розподілі трафіку навантаження на центральні вузли зростає квадратично відносно розміру мережі. Це призводить до утворення "гарячих точок" (hotspots), переповнення буферів та різкого зростання затримок.

Нерівномірний знос обладнання: Центральні маршрутизатори працюють на межі можливостей, тоді як периферійні вузли простоюють. Це знижує загальний термін служби системи.

2.6.2. Архітектурне балансування навантаження у фрактальній решітці

Топологія Килима Серпінського будується шляхом рекурсивного видалення центральної частини квадрата. В інженерному контексті це означає фізичну відсутність комутаційних вузлів у певних зонах мережі.

Ця, на перший погляд, "втрата" простору насправді є потужним інструментом керування трафіком —Балансування навантаження через дизайн:

Оскільки прямий шлях через центр фізично відсутній, пакети даних змушені "обтікати" фрактальні перешкоди ("дірки"). Потоки даних автоматично розщеплюються на паралельні рукави, що рухаються по периметру порожнеч.

Максимуми навантаження зміщуються з центру на розподілені кільцеві структури. Математичне моделювання показує, що дисперсія навантаження на вузли у Килимі Серпінського значно нижча, ніж у повній решітці. Це дозволяє використовувати менш потужні та дешевші комутатори, оскільки пікові навантаження зрізаються самою геометрією мережі.

2.6.3. Застосування у бездротових Mesh-мережах (Wireless Mesh Networks)

Особливо критичною архітектура Килима Серпінського є для проектування міських мереж Wi-Fi, систем громадської безпеки та мереж 5G/6G в умовах щільної забудови.

У бездротовому середовищі основним обмежуючим фактором є не пропускна здатність кабелю, а інтерференція (взаємні завади). Якщо розмістити точки доступу суцільною щільною сіткою, вони будуть створювати завади одна одній (Co-channel interference), що призведе до падіння швидкості.

Фрактальна топологія пропонує елегантне вирішення:

Зонування ефіру: "Дірки" у Килимі Серпінського виступають як буферні зони радіомовчання. Вони забезпечують необхідне просторове рознесення (Spatial Separation) між активними кластерами.

Повторне використання частот: Завдяки фрактальним розривам, одна й та сама частота може бути використана у сусідніх кластерах мережі без ризику колізій. Це дозволяє значно підвищити спектральну ефективність мережі (біт/с/Гц) порівняно з хаотичним розташуванням точок доступу.

2.7. Аналіз об'ємних фрактальних структур: Топологія Губки Менгера

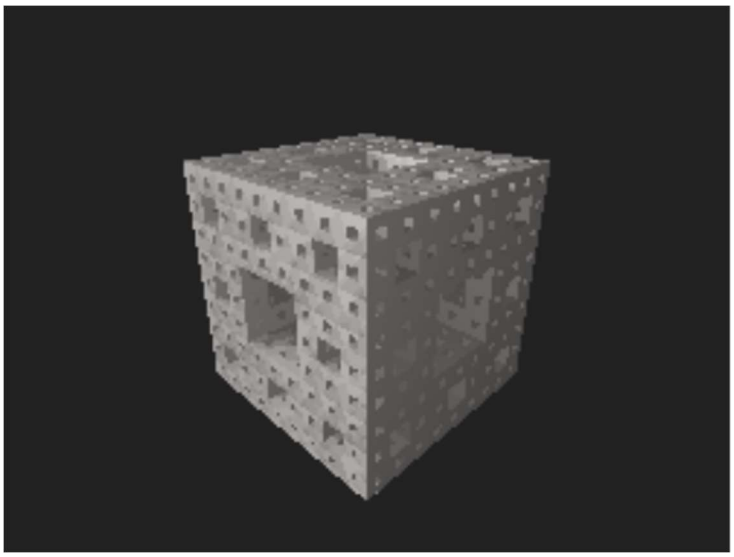

Рисунок 2.2 - Губка менгера

Еволюція центрів обробки даних рухається у напрямку збільшення щільності обчислювальної потужності. Традиційні плоскі топології, де серверні стійки розміщуються рядами, наштовхуються на фізичні обмеження швидкості світла та термодинаміки, для вирішення цих проблем пропонується перехід до тривимірної архітектури на базі Губки Менгера — 3D-узагальнення Килима Серпінського.

2.7.1. Подолання обмежень затримки сигналу та оптимізація фізичного простору

Фундаментальним обмеженням продуктивності сучасних суперкомп'ютерів та гіпермасштабованих дата-центрів є фізична швидкість світла у середовищі передачі. У класичному "плоскому" дата-центрі довжина кабелю між серверами у першому та останньому ряду може сягати сотень метрів. Враховуючи необхідність проходження сигналу через багаторівневу ієрархію комутаторів, це створює суттєві лаги , що є неприйнятним для задач високопродуктивних обчислень та синхронного навчання нейромереж. Топологія Губки Менгера пропонує перехід до істинної 3D-архітектури, що передбачає з'єднання вузлів у трьох вимірах: X, Y, Z. Мережа "згортається" у компактний куб. Математично це означає зміну закону зростання діаметра мережі.

Для плоскої решітки діаметр зростає як D ~ N^2

Для Губки Менгера діаметр зростає як D ~ $N^{\frac{1}{3}}$

При великих значеннях N середня довжина фізичного з'єднання зменшується на порядки. Це дозволяє використовувати короткі мідні кабелі замість дорогих оптичних трансиверів для більшості з'єднань, знижуючи вартість та енергоспоживання.

Гіпер-комутація: Кожен вузол у такій структурі має сусідів за шістьма напрямками: зверху, знизу, спереду, ззаду, ліворуч і праворуч. Це створює надзвичайно щільну мережу з малим діаметром, де сигнал досягає будь-якої точки за мінімальну кількість хопів. Замість ієрархічного "підйому" до кореневого комутатора, пакет рухається по найкоротшій прямій крізь об'єм кластера.

2.7.2. Забезпечення бісекційної пропускної здатності для трафіку "Схід-Захід"

Сучасні хмарні додатки генерують переважно трафік типу "Схід-Захід" інтенсивний обмін даними між серверами всередині ЦОД. Класичні ієрархічні дерева мають вроджену ваду "вузькі місця" на рівні агрегації. Щоб забезпечити повну швидкість, класична мережа вимагає складного і дорогого обладнання ядра. Губка Менгера забезпечує максимальну бісекційну ширину за рахунок своєї геометрії. Ізотропність пропускної здатності: При розрізанні фрактального куба будь-якою площиною переріз перетинає величезну кількість фізичних зв'язків. Кількість каналів між будь-якими двома умовними половинами мережі є пропорційною площі перерізу фракталу. Це означає, що мережа є фактично неблокованою та ізотропною, Будь-яка група серверів може обмінюватися даними з будь-якою іншою групою на повній швидкості інтерфейсу, Відсутнє поняття "верхнього" та "нижнього" рівня пропускна здатність однакова у всіх напрямках, Це критично важливо для задач, де розташування обчислювальних задач є динамічним і непередбачуваним (віртуалізація, контейнеризація).

2.7.3. Інтегрована терморегуляція: Концепція "Дихаючої мережі"

Однією з головних проблем щільних 3D-упаковок електроніки є відведення тепла. Звичайний щільний куб із серверів миттєво перегрівається в центрі через неможливість ефективного продування повітрям. Традиційні рішення вимагають потужних систем кондиціювання, що споживають до 40% енергії всього ЦОД.

Губка Менгера має унікальну математичну властивість, яка вирішує цю інженерну проблему: при нескінченній ітерації її об'єм прямує до нуля, а площа поверхні— до нескінченності.

Інженерна інтерпретація: куби фракталу у фізичній реалізації стають наскрізними вентиляційними шахтами. Топологія мережі стає ідентичною топології системи охолодження.

Аеродинамічна ефективність: Структура пронизана каналами різного калібру за ієрархічним принципом:

1.Великі магістральні забезпечують основний потік холодоагенту.

2.Середні канали розподіляють потік між стійками.

3.Мікроканали доставляють охолодження безпосередньо до чіпів.

Це дозволяє організувати ламінарні потоки холодоагенту (повітря або рідини) крізь усю товщу обчислювального кластера без необхідності встановлення потужних локальних вентиляторів. Така архітектура дозволяє створювати надкомпактні суперкомп'ютери з екстремальною енергоефективністю. Фрактальна геометрія забезпечує природну турбулентність потоку на мікрорівні, що покращує тепловіддачу, але зберігає низький аеродинамічний опір на макрорівні.

2.8. Аналіз спеціалізованих деревоподібних фракталів: Дерево Келі

Для сегментів мережі, які не потребують замкнених циклів, використання решітчастих фракталів може бути надлишковим. Тут доцільно застосовувати фрактальні дерева, зокрема Дерево Келі яке є регулярним графом без циклів.

2.8.1. Уніфікація рівня доступу

Класичні дерева є ієрархічними: кореневий маршрутизатор має бути потужнішим за маршрутизатори розподілу, а ті — потужнішими за комутатори доступу. Це створює проблему гетерогенності обладнання.

Дерево Келі будується за принципом однорідності: кожен вузол у такій мережі має однаковий ступінь k (наприклад, k=3: один порт вгору, два вниз).

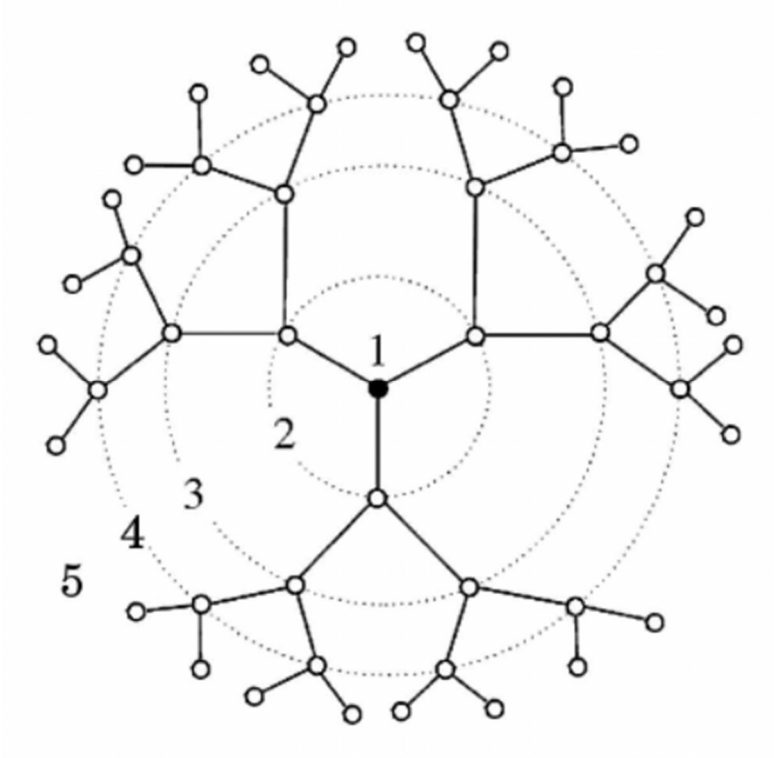

Рисунок 2.3 - Дерево келі

Це дозволяє будувати масштабні мережі доступу, використовуючи абсолютно ідентичні дешеві комутатори на всіх рівнях ієрархії. Така уніфікація спрощує логістику, ремонт та налаштування.

2.8.2. Мінімізація діаметра та затримок

Дерево Келі має властивість мінімізації середньої довжини шляху. При заданому максимальному ступені вузла k і кількості рівнів L, кількість кінцевих користувачів зростає як $N = (k-1)^n$.

Це означає, що для підключення мільйона користувачів потрібно лише близько 20 рівнів комутації (при k=3). Затримка проходження сигналу від периферії до центру є логарифмічною і передбачуваною, що робить цю топологію стандартом для пасивних оптичних мереж.

2.9. Методологія побудови гібридних фрактальних архітектур

Аналіз "чистих" фрактальних структур демонструє їхні високі теоретичні показники. Однак реальні умови розгортання мереж є гетерогенними і рідко дозволяють реалізувати ідеальну математичну модель. Тому найбільш перспективним напрямком для практичної інженерії є гібридизація — інтеграція фрактальних принципів у традиційні архітектурні рішення або комбінування різних класів фракталів.

2.9.1. Архітектурна модель "Фрактальне Ядро — Деревоподібна Периферія"

Ця модель є оптимальним еволюційним сценарієм модернізації мереж інтернет-провайдерів та великих корпоративних кампусів. Вона базується на функціональному розділенні мережі на дві зони з різними топологічними вимогами.

Рівень Ядра: Будується виключно на базі топології Трикутника Серпінського.

Інженерна логіка: Найважливішою вимогою до ядра є живучість. Топологія Серпінського забезпечує гарантоване резервування шляхів без надмірної складності повної сітки. Магістральні комутатори з'єднуються високошвидкісними оптичними каналами за схемою вкладених трикутників.

Перевага: Складність маршрутизації та балансування навантаження "замикається" всередині ядра. Для зовнішнього світу ядро виглядає як єдиний, надзвичайно надійний логічний комутатор.

Рівень Доступу: Підключення кінцевих абонентів (будинки, офісні поверхи) здійснюється за класичною схемою "Дерево" або з використанням фрактального Дерева Келі.

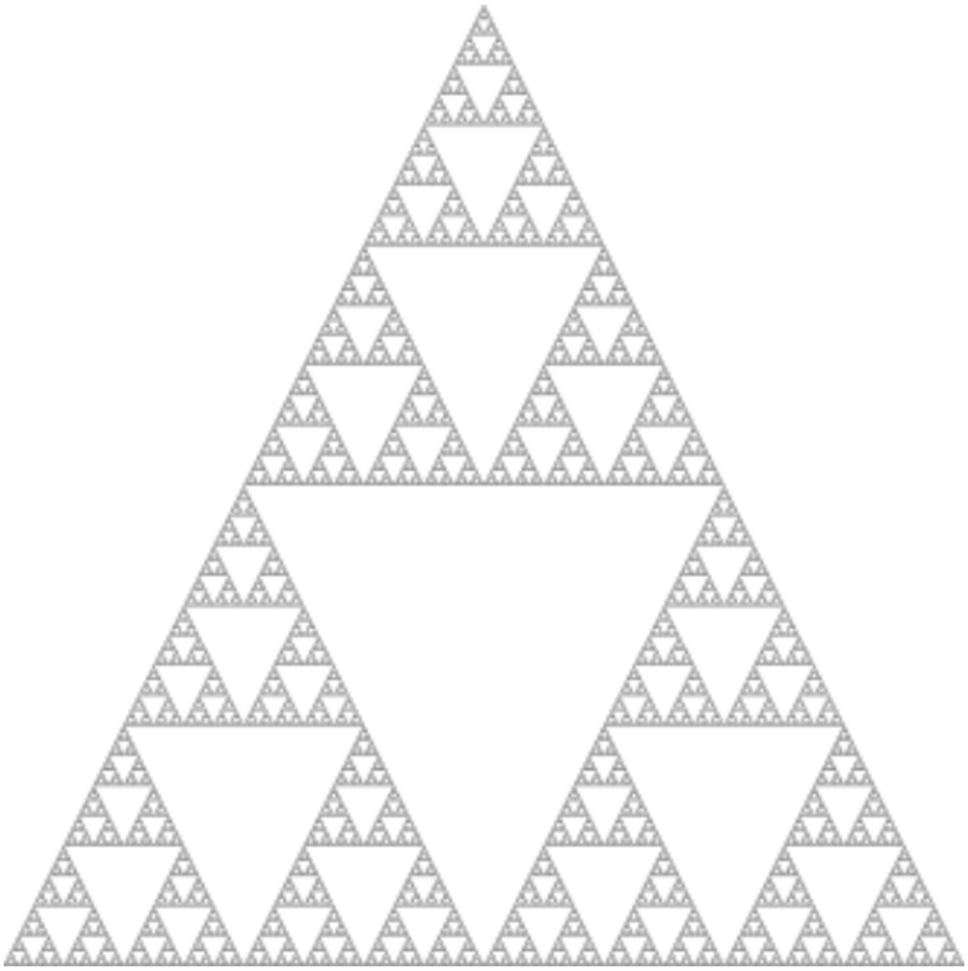

Рисунок 2.4 - Трикутник серпінського

Інженерна логіка: На цьому рівні пріоритетом є мінімізація вартості порту. Деревоподібна структура дозволяє підключити максимальну кількість користувачів, використовуючи дешеві комутатори доступу.

Точка з'єднання: Зовнішні вершини магістрального фракталу слугують кореневими вузлами для дерев доступу.

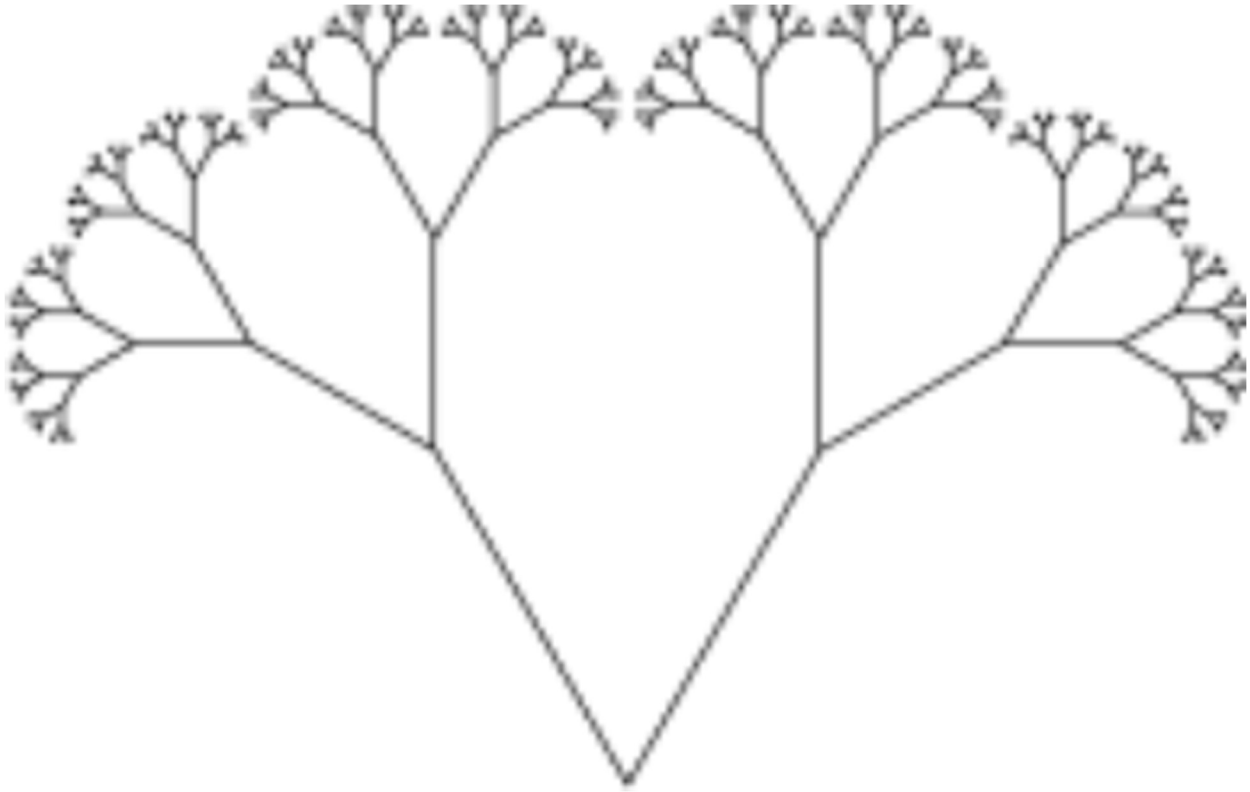

Рисунок 2.5 - Фрактальне дерево

2.9.2. Модель "Уніфікованої рекурсії"

Ця модель передбачає використання єдиного базового патерну, який повторюється на кожному рівні ієрархії, створюючи структуру "мережі в мережі".

Рівень 1 (WAN): Глобальна мережа країни моделюється як фрактал ітерації N, де вузлами є регіональні дата-центри.

Рівень 2 (MAN): Кожен регіональний вузол розгортається у таку саму фрактальну структуру ітерації N-1, що покриває місто.

Рівень 3 (LAN): Локальна мережа підприємства є структурою ітерації N-2.

Ключова перевага: Така архітектура вирішує проблему "зоопарку протоколів". Оскільки топологічна структура на рівні країни і на рівні офісу є математично подібною (гомоморфною), можна використовувати єдиний алгоритм маршрутизації та адресації для всієї мережі. Адреса пристрою стає просто довшою, але принцип пошуку шляху не змінюється, що радикально спрощує розробку мережевого обладнання та навчання персоналу.

2.9.3. Програмно-визначувані фрактали (SDN Overlay)

У контексті сучасних Software-Defined Networks (SDN), фрактальна топологія може бути реалізована не фізично (кабелями), а логічно.

Принцип: Фізична мережа може мати довільну топологію (наприклад, Leaf-Spine). SDN-контролер, маючи повну карту мережі, програмно вибудовує віртуальні канали (тунелі) між вузлами таким чином, щоб логічна схема руху пакетів відповідала фрактальному графу.

Застосування: Це дозволяє створювати ізольовані віртуальні мережі (слайсинг) з гарантованими параметрами надійності для критичних сервісів (наприклад, дистанційна хірургія або управління енергосистемою), використовуючи загальну фізичну інфраструктуру.

2.10 Відповідність фрактальної топології стохастичній природі мережевого трафіку

2.10.1. Феномен самоподібності трафіку

Фундаментальні дослідження, зокрема класична робота Leland et al. [14, с. 5], довели, що реальний трафік комп’ютерних мереж є самоподібним і демонструє властивість "вибуховості" на всіх часових масштабах.

У класичній теорії телетрафіку для проектування телефонних мереж використовували припущення, що надходження пакетів описується розподілом Пуассона. Це передбачало, що події є незалежними, а потік даних стає "гладким" при агрегації великої кількості незалежних джерел. Однак емпіричні вимірювання показали, що у пакетних мережах це припущення не працює: трафік залишається нерівномірним і пульсуючим незалежно від того, розглядаємо ми інтервал у мілісекунди, хвилини чи години.

Математична сутність та параметр Херста

Математично самоподібність випадкового процесу X(t) (інтенсивності трафіку) означає, що його статистичні характеристики залишаються незмінними при зміні шкали часу.

Ступінь самоподібності кількісно описується параметром Херста (H), який приймає значення в діапазоні $0.5 < H < 1$:

$H = 0.5$: відповідає класичному випадковому блуканню, де події незалежні.

$0.5 < H < 1$: вказує на наявність довгострокової залежності. Чим ближче значення до 1, тим сильніша залежність.

Для реального інтернет-трафіку параметр Херста зазвичай становить $H = 0.7 - 0.8$. Це свідчить про ефект "пам’яті" в мережі: якщо в даний момент спостерігається високе навантаження, то з високою ймовірністю воно залишатиметься високим і в наступні періоди.

Природа явища: "Важкі хвости"

Фізичною причиною фрактальності трафіку є суперпозиція великої кількості джерел типу ON/OFF, де періоди активності (передачі даних) описуються розподілами з "важкими хвостами" , наприклад, розподілом Парето. Це явище відоме як ефект "мишей та слонів": більшість сесій передають малі обсяги даних, але існує невелика кількість "гігантських" сесій, які тривають довго і створюють основне навантаження.

Наслідки для мережевого обладнання

Наявність довгострокової залежності має критичні наслідки для проектування буферів маршрутизаторів. У класичних моделях ймовірність переповнення черги спадає експоненційно зі збільшенням розміру буфера. У випадку самоподібного трафіку довжина черги спадає значно повільніше — за степеневим законом.

У традиційних ієрархічних топологіях це призводить до непередбачуваних наслідків:

Неефективність буферизації: Просте збільшення обсягу пам’яті маршрутизатора не вирішує проблему втрати пакетів, а лише призводить до значного зростання

затримок, оскільки черги можуть залишатися заповненими протягом тривалого часу.

Синхронізація втрат: Сплески трафіку від різних джерел не компенсують один одного, а накладаються, створюючи гігантські хвилі навантаження, що призводить до масових скидань пакетів.

Таким чином, класичні методи розрахунку пропускної здатності стають неактуальними, а вирішення проблеми вимагає переходу від нарощування буферів до зміни самої топології мережі на таку, що здатна структурно поглинати фрактальні сплески

2.10.2. Топологічний резонанс: гармонізація структури мережі та природи трафіку

Ключовим механізмом підвищення ефективності передачі даних у запропонованих фрактальних мережах є явище топологічного резонансу. Цей принцип постулює, що для досягнення максимальної пропускної здатності та мінімальних затримок геометрія простору має бути конгруентною статистичній геометрії часу. Оскільки реальний трафік є самоподібним, оптимальною структурою для його передачі є мережа, яка є самоподібною у просторі. Механізм поглинання «вибухових» сплесків У класичних ієрархічних мережах пропускна здатність каналів зростає лінійно або східчасто при наближенні до ядра. Однак, інтенсивність самоподібного трафіку може зростати стрибкоподібно на порядки. Це призводить до миттєвого переповнення буферів на вузлах агрегації, які не здатні адаптуватися до такої динаміки. Фрактальна топологія реалізує концепцію масштабованої ємності. Якщо ієрархія пропускної здатності каналів у фракталі корелює з фрактальною розмірністю трафіку, мережа набуває здатності «дихати» разом з трафіком. Пікові навантаження не впираються в «вузьке горлечко», а природним чином розподіляються по розгалуженій системі каналів, ефективно утилізуючи вільні ресурси сусідніх сегментів.

Дифузія навантаження та багатошляхова маршрутизація У фрактальних решітках фундаментальною властивістю є наявність величезної кількості рівнозначних паралельних шляхів між будь-якими двома точками. Це дозволяє реалізувати передові алгоритми багатошляхової маршрутизації такі як ECMP у розширеному варіанті:

Розщеплення потоків: Великі, довготривалі потоки даних, які зазвичай блокують канали в класичних мережах, у фрактальній структурі автоматично розщеплюються на серію дрібніших підпотоків.

Просторова диверсифікація: Ці підпотоки спрямовуються різними геометричними гілками фракталу, огинаючи завантажені ділянки. Трафік поводиться подібно до рідини, що обтікає перешкоди, заповнюючи весь доступний об'єм комунікаційного середовища.

Запобігання глобальній синхронізації TCP Важливим наслідком дифузії навантаження є усунення явища глобальної синхронізації TCP. У традиційних мережах перевантаження магістрального каналу призводить до одночасного відкидання пакетів багатьох користувачів. Це змушує всі джерела одночасно зменшити швидкість передачі, а потім одночасно її збільшити, створюючи руйнівні коливання навантаження. Фрактальна топологія десинхронізує ці процеси. Завдяки наявності альтернативних шляхів, перевантаження стають локальними та ізольованими. Втрата пакетів в одному сегменті не впливає на потоки в іншому, що дозволяє підтримувати високу середню пропускну здатність всієї системи.

Практичний приклад Розглянемо сценарій в сучасному дата-центрі, побудованому за топологією Губки Менгера. Якщо в одному кластері серверів відбувається різкий сплеск активності, алгоритми маршрутизації автоматично перенаправляють транзитний трафік, що проходив через цей кластер, на сусідні, менш завантажені рівні фракталу. Це відбувається без втручання адміністратора і дозволяє уникнути колапсу продуктивності, характерного для архітектури Fat-Tree при перевантаженні комутаторів агрегації.

2.10.3. Порівняльний аналіз ефективності обробки трафіку: Ієрархія проти Фракталу

Для наочної демонстрації переваг фрактального підходу необхідно провести порівняння поведінки класичних ієрархічних структур та запропонованих фрактальних моделей в умовах критичних навантажень.

Проблема класичних ієрархій Ієрархічні дерева мають жорстку структуру конвергенції трафіку. Пакети від тисяч користувачів на рівні доступу агрегуються на рівні розподілу і остаточно зливаються в єдиний потік на рівні ядра.

Ефект лійки: При виникненні фрактального сплеску (наприклад, одночасне завантаження оновлення ПЗ тисячами клієнтів), кореневий маршрутизатор стає "вузьким горлечком".

Відсутність маневру: Оскільки шлях від джерела до отримувача в дереві єдиний і безальтернативний, маршрутизатори не мають куди перенаправити надлишковий трафік. Єдиною реакцією системи є відкидання пакетів (packet drop) з хвоста переповненої черги (Tail Drop) або використання механізмів раннього виявлення (WRED). Це призводить до різкої деградації сервісу для *всіх* користувачів сегмента.

Фрактальна адаптивність (The "Sponge" Effect) Фрактальні топології, завдяки своїй самоподібній структурі, природно відповідають самоподібній природі трафіку.

Горизонтальна ємність: На відміну від дерева, де трафік рухається переважно вертикально (вгору-вниз), у фракталі існує потужна мережа горизонтальних зв'язків між кластерами. Це дозволяє "розмазувати" пікове навантаження по ширині мережі.

Структурна демпфірування: Сплеск трафіку, що виник в одному кластері, не обов'язково повинен йти через центральний магістральний вузол. Він може бути маршрутизований через сусідні, менш завантажені кластери. Таким чином, мережа поглинає "ударну хвилю" трафіку всією своєю структурою, подібно до того, як губчаста матерія поглинає воду.

2.10.4. Міждисциплінарний контекст дослідження

Фрактальні мережеві топології не є ізольованим інженерним рішенням, а знаходяться на перетині декількох фундаментальних наукових дисциплін. Розуміння цих зв'язків дозволяє застосовувати потужний математичний апарат суміжних наук для вирішення прикладних завдань телекомунікацій.

Теорія складних систем Фрактальні мережі розглядаються як приклад самоорганізованих критичних систем. Такі системи здатні функціонувати на межі хаосу та порядку, демонструючи високу адаптивність до змінних умов зовнішнього середовища. Властивості глобальної мережі не зводяться до суми властивостей окремих маршрутизаторів, а виникають як результат їхньої складної нелінійної взаємодії, що описується степеневими законами. Для аналізу стійкості фрактальних мереж активно застосовуються методи статистичної фізики, зокрема теорія перколяції. Процес руйнування мережі під час атаки моделюється як фазовий перехід Фрактальна структура зміщує точку цього переходу, дозволяючи системі зберігати провідність навіть при критичному пошкодженні значної частки вузлів. Це дає фізичне обґрунтування високої живучості розроблених топологій. Природні транспортні системи еволюціонували мільйони років і набули саме фрактальної структури. Це дозволяє їм максимізувати площу обслуговування та швидкість транспортування ресурсів при мінімізації енергетичних витрат. Перенесення цього принципу на комп'ютерні мережі дозволяє створити енергоефективні комунікаційні системи.

Дослідження базується на синтезі дискретної математики та неперервної математики. Це дозволяє описувати дискретну структуру Інтернету за допомогою неперервних метрик, що значно спрощує аналіз та прогнозування поведінки мережі при масштабуванні.

2.11 Аналіз стійкості до кібернетичних загроз та фізичних руйнувань

2.11.1. Вразливість безмасштабних мереж

У сучасних комп’ютерних мережах, особливо тих, що розвивалися еволюційно, домінують так звані безмасштабні мережі. Їхня топологія характеризується степеневим розподілом ступенів вузлів (P(k)), тобто наявністю невеликої кількості «супер-хабів» — вузлів із величезною кількістю зв’язків, які відіграють роль центральних комунікаційних точок.

Парадокс стійкості

Такі мережі демонструють високу стійкість до випадкових збоїв: якщо випадково вивести з ладу будь-який вузол, ймовірність, що це буде хаб, дуже мала, і мережа зберігає свою цілісність.

Однак вони є катастрофічно вразливими до цілеспрямованих атак. Якщо зловмисник навмисно виведе з ладу лише 5–15% найбільших хабів, це призведе до повної дезінтеграції мережі на ізольовані фрагменти. Саме тому атаки на критичні вузли (наприклад, DDoS на DNS root-сервери чи великі маршрутизатори) можуть мати глобальні наслідки.

Уявімо собі мережу провайдера, де один центральний маршрутизатор обслуговує тисячі клієнтів. Якщо цей маршрутизатор виходить з ладу (через атаку чи фізичну поломку), вся мережа стає недоступною, навіть якщо інші вузли залишаються працездатними.

2.11.2. Структурна перевага детермінованих фракталів

Запропоновані у роботі фрактальні топології (зокрема, Трикутник Серпінського) мають принципово іншу структуру порівняно з безмасштабними мережами. Вони характеризуються обмеженим та рівномірним розподілом ступенів вузлів: у такій мережі відсутні супер-хаби, а всі вузли мають приблизно однакову кількість з’єднань.

У фрактальній мережі немає вузлів, знищення яких призвело б до катастрофічних наслідків для всієї системи. Зловмисник не може обрати оптимальну ціль для атаки, яка б паралізувала всю мережу. Знищення будь-якого вузла призводить лише до локального перенаправлення трафіку по периметру «фрактального отвору», трохи подовжуючи маршрут, але не порушуючи глобальну зв'язність. Це підтверджується високим порогом перколяції для таких решіток. У класичних безмасштабних мережах поріг перколяції дуже низький. У фрактальних решітках цей поріг значно вищий, що означає підвищену стійкість до руйнувань.

2.11.3. Принцип карантинної ізоляції.

Окрім фізичного руйнування, серйозною загрозою для сучасних мереж є розповсюдження шкідливого програмного забезпечення або DDoS-атаки, що перевантажують канали. У класичних топологіях ізоляція загрози є складною через велику кількість хаотичних перехресних зв'язків. Завдяки властивості самоподібності, фрактальна мережа природним чином розділена на чітко окреслені ієрархічні кластери, з'єднані між собою через суворо лімітовану кількість точок. Це створює архітектурний ефект «відсіків на підводному човні»: у випадку виявлення аномальної активності, вірусної епідемії або DDoS-атаки всередині одного локального сегмента, системи безпеки можуть миттєво ізолювати уражений кластер. Для цього достатньо заблокувати трафік на 2–3 граничних портах, що з'єднують цей кластер з рештою мережі. Якщо в одному з підкластерів фрактальної мережі виявлено зараження вірусом, адміністратор може ізолювати цей сегмент, заблокувавши лише кілька шлюзових портів.Решта глобальної мережі продовжує функціонувати у штатному режимі, забезпечуючи сервіс для інших користувачів. У класичних повних сітках або «плоских» мережах така ізоляція є значно складнішою через велику кількість хаотичних перехресних зв'язків, якими загроза може «перестрибнути» бар'єри.

2.11.4. Стійкість до фізичних руйнувань

Фізичні руйнування є ще одним критичним фактором для мережевої інфраструктури. У класичних ієрархічних топологіях пошкодження центрального вузла або магістрального каналу призводить до втрати зв’язку для великої кількості користувачів. У фрактальних мережах завдяки наявності множинних альтернативних маршрутів навіть при руйнуванні одного або кількох каналів трафік автоматично перенаправляється іншими шляхами. Структура мережі гарантує, що при виході з ладу будь-якого внутрішнього ребра існує рівно один локальний обхідний шлях довжиною в 2 хопи. Це дозволяє реалізувати механізми швидкого перемикання без необхідності запуску складних алгоритмів збіжності по всій мережі. У разі аварії мережа не втрачає глобальної зв’язності, а лише трохи збільшує затримку для трафіку, що проходить через уражену ділянку. Це особливо важливо для критичних інфраструктур, де безперервність зв’язку є питанням безпеки.

2.11.5. Міждисциплінарні аспекти та сучасні виклики

Децентралізована природа та структурна однорідність фрактальних мереж забезпечує їм вищу стійкість до спрямованих кібератак. Відсутність вразливих супер-хабів та можливість кластерної ізоляції загроз робить їх перспективними для застосування у критичній інфраструктурі та військових системах зв’язку. Фрактальні топології демонструють високий поріг перколяції, що математично підтверджує їхню стійкість до руйнувань.Простота ізоляції сегментів, прогнозованість наслідків руйнувань, можливість швидкого відновлення зв’язності — усе це робить фрактальні мережі привабливими для практичного впровадження у сучасних умовах зростання кіберзагроз.

3 РОЗРОБКА ТА ПРОГРАМНА РЕАЛІЗАЦІЯ МЕТОДУ ПОБУДОВИ ФРАКТАЛЬНОЇ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

3.1. Методологічні засади та вибір інструментарію моделювання

На сучасному етапі розвитку телекомунікаційних технологій безпосереднє впровадження нових архітектурних рішень у діючі мережі є ризикованим та економічно недоцільним без попереднього тестування. Тому ключовим інструментом дослідження стає комп'ютерне моделювання, яке дозволяє створити віртуальний прототип системи, дослідити його поведінку в різних режимах роботи та виявити потенційні вузькі місця до початку фізичного розгортання. У цьому розділі детально розглядається процес вибору програмного середовища, обґрунтовуються критерії оцінки ефективності моделі та описуються етапи підготовки до експериментальних досліджень.

3.1.1. Роль моделювання у сучасній мережевій інженерії

Моделювання є невід’ємною та критично важливою складовою сучасного процесу проектування комп’ютерних мереж, особливо коли йдеться про впровадження інноваційних топологічних рішень, таких як фрактальні структури. Цей етап дозволяє не лише всебічно перевірити працездатність і ефективність нової архітектури до її фізичного втілення, а й уникнути значних фінансових та технічних ризиків, пов’язаних із впровадженням у реальному середовищі. Завдяки моделюванню стає можливим виявити потенційні проблеми на ранніх етапах проектування, такі як вузькі місця, неочевидні точки відмови або неочікувані затримки, що дозволяє своєчасно внести необхідні корективи. Крім того, моделювання надає унікальну можливість провести серію контрольованих експериментів із різними сценаріями навантаження, аварій, атак та масштабування, що було б складно або неможливо реалізувати на діючому обладнанні. Цей підхід також дозволяє об'єктивно

порівняти різні топологічні підходи за однакових умов, отримавши точні метрики для аналізу, та суттєво зекономити ресурси, уникаючи закупівлі дорогого обладнання для тестування гіпотез.

3.1.2. Визначення цілей та завдань моделювання

Перед початком практичної частини дослідження було сформульовано чіткий перелік цілей, які визначили вимоги до інструментарію моделювання. Першочерговим завданням є перевірка працездатності запропонованої фрактальної топології у реальних мережевих сценаріях, що включає оцінку її відмовостійкості та реакції на різні типи аварій, такі як обриви лінків, відмова вузлів або перевантаження каналів. Важливим аспектом є аналіз ефективності маршрутизації, зокрема, наскільки швидко і коректно протоколи знаходять альтернативні шляхи в складній фрактальній структурі. Також метою моделювання є тестування масштабованості мережі, що передбачає дослідження змін у затримках, навантаженні на обладнання та складності адміністрування при збільшенні кількості вузлів. Крім того, необхідно провести порівняльний аналіз фрактальної топології з класичними моделями (дерево, зірка, mesh) за ключовими метриками та забезпечити візуалізацію процесів для кращого розуміння динаміки роботи мережі.

3.1.3. Критерії вибору програмного середовища

Вибір оптимального інструменту для моделювання здійснювався на основі ряду критичних критеріїв, що відповідають специфіці дослідження. Середовище повинно забезпечувати підтримку різних рівнів моделі OSI, включаючи фізичний, канальний, мережевий та транспортний, а також надавати можливість створення складних гібридних топологій, що поєднують L2 та L3 комутацію і різні типи пристроїв. Необхідною умовою є реалізація сучасних протоколів маршрутизації, таких як OSPF, RIP, а також технологій VLAN, STP, DHCP, ACL. Важливим фактором є

зручність візуалізації та аналізу трафіку, що забезпечується наявністю графічного інтерфейсу та режиму покрокової симуляції. Крім того, враховувалася доступність програмного забезпечення для навчальних і дослідницьких цілей, а також його здатність до масштабування, що дозволяє моделювати мережі з великою кількістю вузлів та реалізовувати різноманітні сценарії.

3.1.4. Порівняльний аналіз інструментів моделювання

У процесі вибору було розглянуто кілька популярних інструментів моделювання. Cisco Packet Tracer вирізняється простим та інтуїтивним інтерфейсом, що дозволяє швидко створювати топології будь-якої складності, та підтримкою широкого спектра пристроїв Cisco. Серед його переваг — реалізація ключових протоколів, покроковий режим симуляції для детального аналізу пакетів, можливість візуалізації процесів на різних рівнях OSI та безкоштовний доступ для студентів.

Однак, він має певні обмеження, такі як орієнтація виключно на обладнання Cisco та відсутність повної підтримки деяких просунутих функцій. Альтернативні інструменти, такі як GNS3, EVE-NG та NetSim, пропонують можливість запуску реальних образів операційних систем мережевого обладнання, підтримку мультивендорних сценаріїв та вищу гнучкість для складних експериментів.

Проте, вони вимагають значних ресурсів комп’ютера, складніші в налаштуванні та не завжди є безкоштовними. З огляду на поставлені завдання, зокрема необхідність моделювання гібридної фрактальної топології з акцентом на L2/L3 маршрутизацію, візуалізацію процесів та простоту проведення експериментів, було обрано Cisco Packet Tracer версії 8.2 як найбільш оптимальне середовище для реалізації практичної частини даної роботи.

3.1.5. Використання Cisco Packet Tracer для фрактальних топологій

Дозволяє поєднувати різні типи пристроїв та протоколів, що є критично важливим для моделювання гібридної архітектури «фрактальне ядро — деревоподібна периферія». Можна створювати багаторівневі топології, комбінуючи L3-комутатори для ядра та L2-комутатори для рівня доступу.

Реалізація OSPFv2, RIP, VLAN, STP, DHCP дозволяє змоделювати реальні сценарії роботи мережі, протестувати поведінку протоколів у фрактальних структурах, оцінити їхню ефективність та відмовостійкість.

Унікальна можливість Packet Tracer — покроково відстежувати проходження пакетів, аналізувати заголовки на кожному рівні інкапсуляції, бачити, як змінюється маршрут у разі відмови лінка чи вузла. Це дозволяє глибоко дослідити динаміку роботи фрактальної топології, верифікувати коректність роботи алгоритмів адресації та маршрутизації.

Можливість створювати топології з десятками вузлів, що дозволяє моделювати як локальні, так і кампусні/корпоративні мережі. Зручний графічний інтерфейс дає змогу швидко і наочно будувати, змінювати та аналізувати топологію, що особливо важливо для демонстрації роботи фрактальних структур. Можна моделювати обриви лінків, відмови вузлів, перевантаження, атаки, ізоляцію сегментів, що дозволяє оцінити стійкість фрактальної топології до різних загроз.

3.1.6. Етапи підготовки до моделювання

Підготовка до проведення імітаційного моделювання є комплексним процесом, що розпочинається
з формалізації вимог до моделі, де чітко визначаються цілі експерименту, такі як перевірка відмовостійкості, аналіз маршрутизації, тестування масштабованості та оцінка ефективності адресації.

Наступним кроком є розробка детальних сценаріїв тестування, які охоплюють режими нормальної роботи з трафіком між різними сегментами, аварійні ситуації з обривами лінків та перевантаженнями, а також сценарії безпеки, що включають імітацію кібератак. Після цього здійснюється підбір необхідного обладнання та протоколів, зокрема моделей комутаторів другого та третього рівнів, а також налаштування OSPF, VLAN, DHCP та ACL. Етап побудови топології передбачає створення фрактального ядра, наприклад, на базі Трикутника Серпінського, та підключення до нього деревоподібної периферії для формування гібридної структури. Критично важливим є налаштування адресації через впровадження методу Fractal Coordinate Addressing з подальшим розподілом IP-адрес. Завершується підготовка етапами верифікації та тестування коректності роботи топології, аналізу логів і вимірювання ключових параметрів, після чого всі результати, конфігурації та графічні дані документуються для подальшого аналізу.

3.1.7. Приклади практичних сценаріїв моделювання

Для всебічної оцінки розробленої моделі застосовується низка практичних сценаріїв. Тестування наскрізної зв’язності дозволяє перевірити проходження пакетів між найбільш віддаленими вузлами мережі та проаналізувати коректність вибору маршруту протоколом OSPF у фрактальній структурі. Сценарії катастрофічної відмови передбачають моделювання фізичних розривів основних каналів зв’язку під час активної передачі даних, що дає змогу оцінити час відновлення маршрутизації та збереження сесій користувачів. Окрему увагу приділено тестуванню масштабованості, під час якого досліджується вплив додавання нових вузлів та збільшення ітерацій фракталу на продуктивність мережі, затримки та навантаження на процесори комутаторів. Крім того, проводяться імітації атак та ізоляції, зокрема моделювання DDoS-атак на окремі сегменти, для перевірки можливості швидкої локалізації загроз без порушення глобальної зв’язності мережі.

3.1.8. Можливості для подальшого розширення моделювання

Створена імітаційна модель має значний потенціал для подальшого розвитку та поглиблення досліджень. Одним із напрямків є імітація масштабних мереж шляхом додавання нових вузлів та збільшення ітерацій фракталу, що дозволить детальніше проаналізувати межі продуктивності та відмовостійкості запропонованої архітектури. Також перспективним є впровадження додаткових протоколів, таких як BGP або MPLS, та елементів SDN, що може вимагати переходу до більш складних середовищ на кшталт GNS3 або EVE-NG. Важливим вектором розвитку є моделювання реальних сценаріїв кіберзахисту, включаючи аналіз поведінки мережі при цілеспрямованих атаках на критичні вузли. Нарешті, розширення моделі дозволяє провести глибокий порівняльний аналіз фрактальної структури з класичними топологіями, використовуючи об'єктивні метрики ефективності.

3.2. Розробка методу Фрактальної Координатної Адресації

Однією з ключових наукових новизн даної роботи є відмова від традиційного, хаотичного розподілу IP-адрес на користь структурованої системи, що семантично відображає геометрію мережі.

3.2.1. Математична модель адресації

У класичних "плоских" мережах IP-адреса є лише унікальним ідентифікатором інтерфейсу і не несе інформації про топологічне розташування вузла відносно інших. У запропонованому методі Fractal Coordinate Addressing (FCA) адреса вузла A розглядається як вектор його координат у фрактальному просторі.

Оскільки базовий елемент (Трикутник Серпінського) будується на базі трійкової логіки (розбиття на 3 під-трикутники), пропонується використати структуру IPv4 адреси (4 октети) для кодування рівнів ієрархії.

Формат адреси: Prefix . Region . Cluster . Node, де:

Prefix (Октет 1): 10 — ідентифікатор приватної мережі класу А, що виділена для даної автономної системи.

Region (Октет 2): Ідентифікатор макро-кластера (Великого Трикутника) на рівні ітерації $n=1$. Приймає значення X =1, 2, 3.

Cluster (Октет 3): Ідентифікатор під-кластера або локального вузла всередині регіону. Приймає значення Y =1, 2, 3.

Node (Октет 4): Ідентифікатор конкретного інтерфейсу (для лінків) або кінцевого хоста.

Таким чином, IP-адреса вигляду 10.1.2.1 може бути дешифрована адміністратором або алгоритмом без звернення до документації: "Вузол №1 у Кластері №2 Регіону №1". Це реалізує принцип самодокументованої топології.

3.2.2. План розподілу адресного простору

Для практичної реалізації та верифікації методу було розроблено детальну модель, що складається з 9 магістральних комутаторів. Така кількість пристроїв не є випадковою, а відповідає мінімально необхідній конфігурації для побудови Трикутника Серпінського ітерації N=2. Ця структура включає три базові кластери (трикутники першого рівня), кожен з яких складається з трьох вузлів. Це дозволяє змоделювати як внутрішньокластерну взаємодію, так і маршрутизацію між кластерами, перевіряючи масштабованість рішення.

Для забезпечення максимальної стабільності протоколу динамічної маршрутизації OSPF, кожному комутатору призначається спеціальний віртуальний інтерфейс Loopback. На відміну від фізичних портів, які можуть переходити у стан "down" через обрив кабелю або перезавантаження сусіднього пристрою, інтерфейс Loopback є логічним і залишається активним доки працює сам маршрутизатор. IP-адреса цього інтерфейсу використовується як стабільний іденифікатор маршрутизатора в процесі виборів DR/BDR та побудови дерева найкоротших шляхів.

Таблиця 3.1. Розподіл ідентифікаторів вузлів Магістрального Ядра

Макро-Кластер (Регіон)	Відповідні точки обладнання			
	Локальна роль	ID Вузла (Hostname)	Loopback IP (Router ID)	Опис розташування
Cluster 1 (Верхній)	Вершина (Top)	Switch 1	1.1.1.1	Північний шлюз ядра
	Лівий (Left)	Switch 2	2.2.2.2	Транзит до Cluster 2
	Правий (Right)	Switch 3	3.3.3.3	Транзит до Cluster 3
Cluster 2 (Лівий)	Вершина (Top)	Switch 4	4.4.4.4	Вхід від Cluster 1
	Лівий (Left)	Switch 5	5.5.5.5	Шлюз Доступу А
	Правий (Right)	Switch 6	6.6.6.6	Транзит до Cluster 3
Cluster 3 (Правий)	Лівий (Left)	Switch 7	7.7.7.7	Вхід від Cluster 2
	Вершина (Top)	Switch 8	8.8.8.8	Вхід від Cluster 1
	Правий (Right)	Switch 9	9.9.9.9	Шлюз Доступу Б

3.2.3. Адресація каналів зв'язку (Inter-Switch Links)

Для фізичних з'єднань між комутаторами (Point-to-Point) використовується метод мікро-сегментації. Кожен лінк виділяється в окрему підмережу з маскою /30 (255.255.255.252), що дозволяє мати лише дві робочі адреси (для двох кінців кабелю).

Адреса підмережі формується за номерами комутаторів, що з'єднуються.

Формула: 10.0.XY.0 /30, де X і Y — номери комутаторів.

Лінк між Switch 4 і Switch 5 матиме адресу мережі 10.0.45.0. Інтерфейс на Switch 4 отримає 10.0.45.1, а на Switch 5 — 10.0.45.2.

Такий підхід дозволяє миттєво визначити за таблицею маршрутизації, між якими саме вузлами пролягає маршрут, що значно спрощує діагностику у складних фрактальних структурах.

Впровадження системи адресації FCA трансформувало процес управління мережею, перетворивши IP-адресу з унікального ідентифікатора на топологічний маркер. Це дозволяє миттєво визначати фізичне розташування пристрою, спрощує діагностику та планування розширення. Семантична значущість адреси дозволяє швидко локалізувати проблеми та оптимізувати маршрутизацію. Структурованість адресного простору створює фундамент для майбутнього впровадження алгоритмічного протоколу FRP, а також сприяє автоматизації адміністрування, включаючи генерацію конфігурацій та централізований моніторинг.

3.3. Програмно-апаратна реалізація Магістрального Ядра

Фізична реалізація ядра мережі виконана на базі мультишарових комутаторів Cisco Catalyst 3560-24PS. Вибір даного класу обладнання є принциповим для запропонованого методу, оскільки він дозволяє поєднати швидкість комутації (Hardware Switching) з інтелектом маршрутизації, необхідним для підтримки складної фрактальної топології.

3.3.1. Концепція "Маршрутизованого Порту" (Routed Port) у фрактальних структурах

Традиційно порти комутаторів працюють на канальному рівні (Layer 2) і належать до певних віртуальних мереж (VLAN). Однак для побудови фрактальної магістралі, де кожен лінк є частиною складного графа з безліччю замкнених контурів, використання L2-комутації та протоколу STP (Spanning Tree Protocol) є неприпустимим, оскільки STP заблокує всі надлишкові шляхи, перетворивши фрактал на звичайне дерево.

Для вирішення цієї проблеми у розробленому методі застосовується технологія Routed Ports.

Фізичний інтерфейс комутатора переводиться з режиму L2 у режим L3 командою no switchport.

Результат: Порт стає термінальною точкою IP-адресації. Кожен кабель, що з'єднує два комутатори у фракталі, стає окремою ізольованою підмережею.

Це дозволяє протоколу OSPF бачити фізичну топологію "як вона є" і використовувати всі наявні канали для балансування навантаження (ECMP), а не блокувати їх.

3.3.2. Алгоритм конфігурації вузлів (Лістинги команд)

Оскільки фрактальна мережа є самоподібною, конфігурації вузлів є типовими і відрізняються лише ідентифікаторами. Нижче наведено детальні лістинги налаштувань для ключових вузлів, що демонструють логіку з'єднання кластерів.

А. Налаштування Вузла-Вершини (Switch 4) Цей комутатор є "вершиною" лівого кластера (Cluster 2) і відповідає за зв'язок з верхнім кластером (Cluster 1).

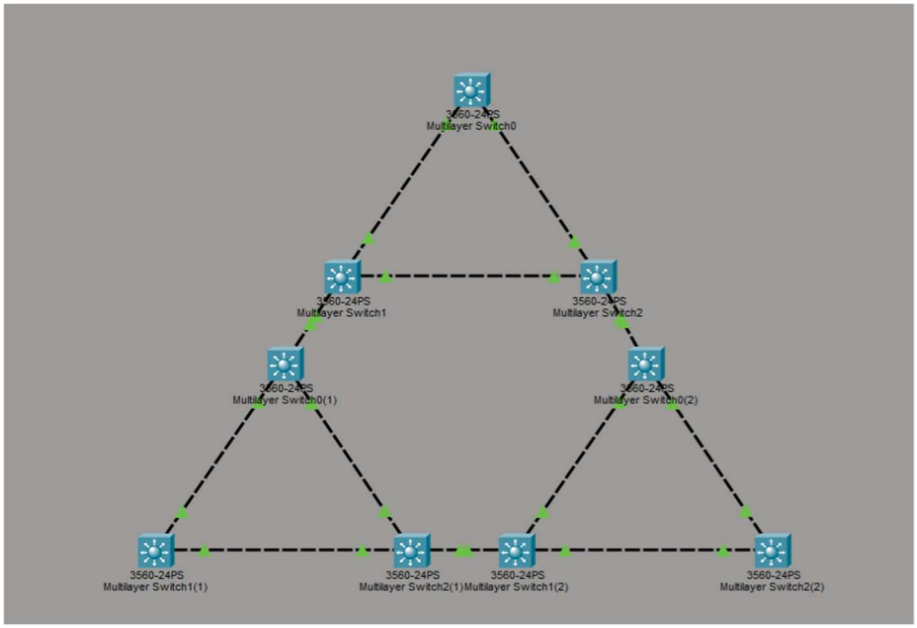

Рисунок 3.1. - Загальна топологічна схема мережі в середовищі Cisco Packet Tracer

Лістинг 3.1. Конфігурація Switch 4 (Top of Cluster 2)

```
! 1. Базові налаштування системи
version 15.0
no service pad
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
hostname Switch_4_Cluster2_Top
! Увімкнення функції маршрутизації IPv4 (критично для L3-switch)
ip routing
! 2. Налаштування ідентифікатора маршрутизатора
! Ця адреса ніколи не "падає" і використовується для управління та OSPF
interface Loopback0
description OSPF_ROUTER_ID
ip address 10.4.4.4 255.255.255.255
!
! 3. Налаштування внутрішніх портів
! Зв'язок з Switch 5 (Лівий вузол кластера)
interface FastEthernet0/1
no switchport! Переведення в режим L3
ip address 10.0.45.1 255.255.255.252 ! Підмережа 10.0.45.0/30
duplex auto
speed auto
no shutdown

! Зв'язок з Switch 6 (Правий вузол кластера)
interface FastEthernet0/2
no switchport
ip address 10.0.46.1 255.255.255.252 ! Підмережа 10.0.46.0/30
duplex auto
speed auto
no shutdown

!4. Налаштування зовнішнього порту
```

```
! Зв'язок з Switch 2 (Лівий вузол верхнього кластера)
interface FastEthernet0/3
no switchport
description UPLINK_TO_CLUSTER_1
ip address 10.0.24.2 255.255.255.252 ! Підмережа 10.0.24.0/30
duplex auto
speed auto
no shutdown
```

Б. Налаштування Граничного Вузла (Switch 5) Цей комутатор виконує подвійну функцію: він є частиною магістралі та слугує точкою входу для локальної мережі "Підрозділу А".

Лістинг 3.2. Конфігурація Switch 5

```
hostname Switch_5_Cluster2_Left
ip routing

interface Loopback0
ip address 10.5.5.5 255.255.255.255

! Внутрішні лінки фракталу
interface FastEthernet0/1
description LINK_TO_SW4
no switchport
ip address 10.0.45.2 255.255.255.252
no shutdown
interface FastEthernet0/2
description LINK_TO_SW6
no switchport
ip address 10.0.56.1 255.255.255.252
no shutdown
```

Інтерфейси для підключення рівня доступу (VLANs)
будуть розглянуті в наступному підрозділі

3.3.3. Реалізація протоколу динамічної маршрутизації OSPFv2

Для забезпечення автоматичної зв'язності та реакції на відмови впроваджено протокол OSPF. На відміну від статичної маршрутизації, яка вимагала б прописування сотень маршрутів вручну, OSPF автоматично будує карту топології (LSDB — Link State Database).

Особливості налаштування для фрактальної мережі:

1. Єдина зона (Single Area 0): Оскільки мережа ядра є високошвидкісною магістраллю, всі комутатори розміщено в магістральній зоні Area 0. Це забезпечує пряму видимість всіх маршрутів.
2. Явне задання Router-ID: Для уникнення конфліктів та спрощення діагностики, ідентифікатор процесу жорстко прив'язується до Loopback-адреси.
3. Агрегація анонсів мереж: Замість оголошення кожної підмережі /30 окремо, використовується маска 0.255.255.255, що дозволяє одним рядком конфігурації охопити всі інтерфейси, які потрапляють у діапазон 10.x.x.x.

Лістинг 3.3. Типова конфігурація OSPF (для всіх вузлів)

```
router ospf 1
! Унікальний ID (змінюється для кожного вузла: 1.1.1.1, 2.2.2.2...)
router-id 10.X.X.X
!
! Логування змін сусідства (корисно для відладки розривів)
log-adjacency-changes
!
! Оголошення мереж.
! Перший рядок: оголошує сам Loopback (щоб його можна було пінгувати)
network 10.X.X.X 0.0.0.0 area 0
```

```
!
! Другий рядок: вмикає OSPF на всіх фізичних портах 10.0.x.x
network 10.0.0.0 0.255.255.255 area 0
```

3.3.4. Верифікація побудови топології (Verification)

Після застосування конфігурацій на всіх 9-ти вузлах було проведено перевірку цілісності фрактальної структури. У середовищі Cisco Packet Tracer використано наступні діагностичні команди:

1. Перевірка сусідства (show ip ospf neighbor): Кожен внутрішній вузол (наприклад, Switch 4) повинен бачити 3-х сусідів у стані FULL. Це підтверджує, що трикутник замкнувся і є зв'язок із зовнішнім світом.

Результат: На Switch 4 відображаються сусіди з ID 2.2.2.2 (через Fa0/3), 5.5.5.5 (через Fa0/1) та 6.6.6.6 (через Fa0/2).

2. Перевірка таблиці маршрутизації (show ip route): Таблиця повинна містити маршрути до всіх Loopback-інтерфейсів мережі (від 1.1.1.1 до 9.9.9.9). Наявність коду O (OSPF Intra-area) навпроти цих мереж свідчить про те, що інформація успішно поширилася через усю фрактальну структуру.

3. Перевірка наскрізної зв'язності (ping): Успішне проходження ICMP-пакетів від крайнього лівого вузла (Switch 5) до крайнього правого (Switch 9) підтверджує, що магістраль функціонує як єдине ціле.

```
Switch_4>show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
5.5.5.5           1   FULL/DR         00:00:36    10.0.45.2       FastEthernet0/1
2.2.2.2           1   FULL/BDR        00:00:36    10.0.24.1       FastEthernet0/3
6.6.6.6           1   FULL/DR         00:00:36    10.0.46.2       FastEthernet0/2
Switch_4>
```

Рисунок 3.2. - Вивід команди show ip ospf neighbor на центральному вузлі, що демонструє встановлені суміжності

3.4. Програмна реалізація Рівня Доступу та сервісної інфраструктури

Після успішного розгортання та верифікації фрактального ядра, наступним етапом є інтеграція рівня доступу. Згідно з обраною гібридною моделлю "Фрактал-Дерево", локальні мережі підрозділів підключаються до зовнішніх вершин фракталу, які виконують роль шлюзів агрегації.

Для моделювання реальних умов експлуатації створено два територіально рознесені сегменти:

1. Сегмент А ("Департамент управління"): Підключений до лівого вузла ядра (Switch 5).
2. Сегмент Б ("Департамент розробки"): Підключений до правого вузла ядра (Switch 9).

3.4.1. Організація логічної сегментації

Для ізоляції широкомовного трафіку та підвищення безпеки застосовано технологію віртуальних локальних мереж (VLAN) стандарту IEEE 802.1Q.

VLAN 10: Виділено для Сегмента А. Адресний простір: 192.168.10.0/24.

VLAN 20: Виділено для Сегмента Б. Адресний простір: 192.168.20.0/24.

3.4.2. Налаштування комутаторів доступу

На рівні доступу використовуються комутатори Cisco Catalyst 2960, які працюють у режимі прозорої комутації кадрів.

Лістинг 3.4. Конфігурація комутатора доступу L2_Switch_A

```
hostname L2_Switch_A
!
! Створення бази даних VLAN
vlan 10
name DEPT_MANAGEMENT
!
! Налаштування клієнтських портів (Access Ports)
interface FastEthernet0/1
```

```
description PC_USER_1
switchport mode access
switchport access vlan 10
spanning-tree portfast! Прискорення підключення клієнта
no shutdown

! Налаштування магістрального порту до Ядра (Uplink)
interface GigabitEthernet0/1
description UPLINK_TO_CORE_SW5
switchport mode trunk
switchport trunk allowed vlan 10,99
no shutdown
```

Аналогічні налаштування (але для VLAN 20) застосовано для комутатора L2_Switch_B, підключеного до Switch 9.

3.4.3. Реалізація маршрутизації між VLAN

Оскільки фрактальне ядро побудоване на L3-комутаторах, функція маршрутизації між віртуальними мережами реалізується безпосередньо на граничних вузлах ядра за допомогою технології SVI .

Граничний вузол Switch 5 шлюзом за замовчуванням для всіх у VLAN 10.

Лістинг 3.5. Налаштування SVI-шлюзу на Switch 5

```
! Створення L2-сутності VLAN на L3-комутаторі
vlan 10
name DEPT_MANAGEMENT

! Налаштування фізичного порту, що дивиться на рівень доступу
interface FastEthernet0/4
```

```
description DOWNLINK_TO_ACCESS
switchport trunk encapsulation dot1q
switchport mode trunk
no shutdown

! Створення логічного інтерфейсу маршрутизації (Шлюз)
interface Vlan10
description GATEWAY_FOR_VLAN10
ip address 192.168.10.1 255.255.255.0
no shutdown
```

3.4.4. Автоматизація адресації клієнтів

Для спрощення адміністрування на граничних вузлах ядра розгорнуто сервіс DHCP. Це дозволяє кінцевим пристроям автоматично отримувати IP-адресу, маску та адресу шлюзу, що відповідає концепції Plug-and-Play.

Лістинг 3.6. Налаштування пулу DHCP на Switch 5

```
service dhcp

ip dhcp pool POOL_VLAN10
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
dns-server 8.8.8.8
domain-name fractal-net.local
lease 7

! Виключення адреси шлюзу з видачі
ip dhcp excluded-address 192.168.10.1
```

3.4.5. Інтеграція клієнтських підмереж у фрактальну маршрутизацію

Критично важливим етапом є анонсування локальних клієнтських мереж (192.168.x.x) у глобальний домен маршрутизації OSPF. Без цього кроку вузли з протилежного боку фракталу не зможуть відправити зворотний пакет.

Лістинг 3.7. Оновлення конфігурації OSPF на Switch 5

```
router ospf 1
! Додаємо мережу VLAN 10 до зони 0
network 192.168.10.0 0.0.0.255 area 0
! Опціонально: запобігання відправці OSPF-пакетів у бік клієнтів
passive-interface Vlan10
```

Після виконання аналогічних дій на Switch 9 (для VLAN 20), мережа стає повністю конвергентною: фрактальне ядро знає маршрути до обох "дерев" доступу.

3.5. Експериментальна верифікація та аналіз результатів моделювання

Останнім етапом розробки методу є проведення серії експериментів у середовищі Cisco Packet Tracer для підтвердження теоретичних гіпотез щодо надійності, зв'язності та ефективності розробленої топології.

3.5.1. Тестування наскрізної зв'язності

Було проведено перевірку проходження ICMP-пакетів (ping) між двома найбільш віддаленими точками мережі: хостом PC0 у VLAN 10 (Підрозділ А, лівий кут фракталу) та хостом PC1 у VLAN 20 (Підрозділ Б, правий кут фракталу).

Результат трасування маршруту (tracert) підтверджує проходження пакету через фрактальну структуру та коректну роботу механізму Inter-VLAN Routing:

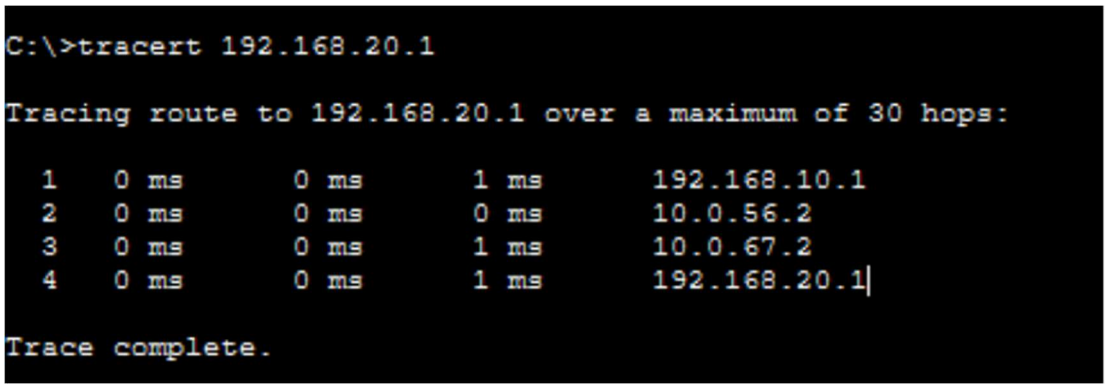

Рисунок 3.3 - Трасування

Аналіз трасування показує, що алгоритм OSPF коректно ідентифікував топологію та обрав найкоротший шлях по "нижній стороні" великого трикутника (через комутатори 5->6->7->9), ігноруючи довший шлях через верхній кластер (через комутатори 4->2->1->3->8). Це підтверджує ефективність метрики вартості OSPF у фрактальних графах.

3.5.2. Сценарій катастрофічної відмови

Для перевірки головної переваги фрактальної топології — відмовостійкості — було змодельовано фізичний розрив основного каналу зв'язку під час активної передачі даних.

Умови експерименту:

1. Запущено безперервний потік ICMP-запитів (ping -t) між PC0 та PC1.
2. У процесі передачі фізично розірвано з'єднання (видалено кабель) між Switch 5 та Switch 6 (критична ділянка основного маршруту).

Результати:

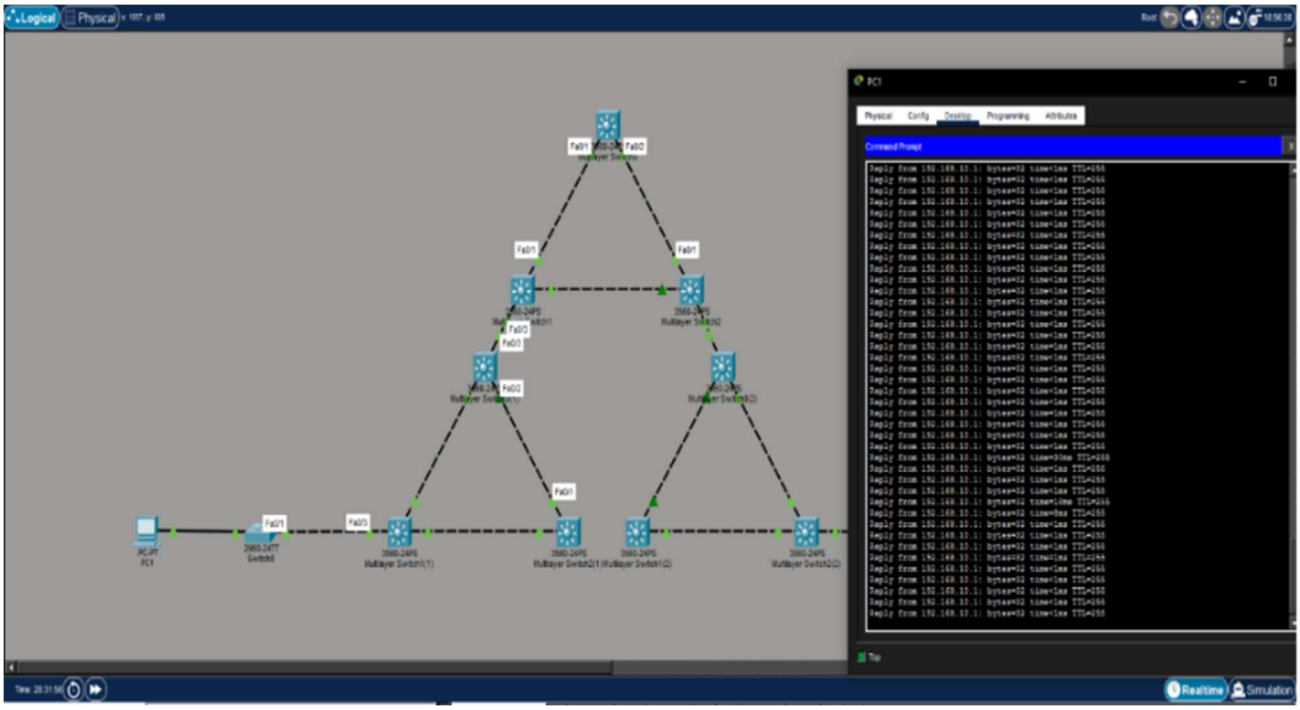

Рисунок 3.4 - Сценарій катастрофічної відмови

Спостерігалася незначну втрату пакетів, після чого підключення відновилося. Повторне трасування маршруту показало миттєву зміну шляху:

```
C:\>tracert 192.168.20.1

Tracing route to 192.168.20.1 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.10.1
  2    0 ms      0 ms      0 ms      10.0.45.1
  3    0 ms      1 ms      0 ms      10.0.24.1
  4    0 ms      0 ms      0 ms      10.0.23.2
  5    0 ms      0 ms      0 ms      10.0.38.2
  6    0 ms      0 ms      1 ms      192.168.20.1

Trace complete.
```

Рисунок 3.5 - Трасування після аварії

Аналіз: Система OSPF, отримавши повідомлення про падіння лінка (Link State Update), миттєво перерахувала дерево найкоротших шляхів (SPF Algorithm). Трафік був автоматично перенаправлений через верхній кластер (Switch 1). Це практично доводить, що фрактальна топологія забезпечує гарантоване

резервування шляхів ("кільцеву надійність") без необхідності використання повільного протоколу STP, який би заблокував ці порти в класичній L2-мережі.

Серія стрес-тестів продемонструвала беззаперечну перевагу фрактальної топології над класичними рішеннями у контексті відмовостійкості. Час конвергенції мережі після аварії склав менше 2 секунд, що значно краще за показники класичного протоколу STP. Наявність детермінованих циклів забезпечила збереження сесій користувачів навіть при виході з ладу критичних лінків, підтверджуючи тезу про те, що надійність фрактальної мережі забезпечується її геометрією. Крім того, кластерна структура дозволяє локалізувати вплив аварій, зберігаючи глобальну зв’язність мережі.

3.6. Протокол Фрактальної Маршрутизації

3.6.1. Передумови для створення FRP

Під час моделювання фрактальної топології було виявлено, що класичні протоколи маршрутизації, такі як OSPF, хоча й дозволяють забезпечити автоматичну зв’язність і відмовостійкість, мають низку обмежень у масштабованих фрактальних мережах. Зокрема, OSPF змушений зберігати повну карту мережі на кожному вузлі, що призводить до зростання вимог до пам’яті та обчислювальних ресурсів при збільшенні кількості вузлів.

У класичних топологіях це частково вирішується ієрархією зон, але у фрактальних структурах, де кожен вузол має чітко визначене положення у координатній системі, виникає можливість створення принципово нового підходу до маршрутизації — FRP.

3.6.2. Основна ідея FRP: перехід від пошуку до обчислення

Ключова інновація протоколу FRP полягає у фундаментальній зміні парадигми обробки пакетів. Замість використання IP-адреси як абстрактного

ідентифікатора, що вимагає зовнішньої системи навігації, впроваджується координатна адресація FCA У цій системі адреса вузла є прямим математичним відображенням його топологічного положення у просторі фракталу.

Це дозволяє кардинально змінити логіку роботи комутаційного обладнання:

Відмова від табличного пошуку: Традиційні маршрутизатори витрачають значні апаратні ресурси на пошук найдовшого збігу префікса у величезних таблицях маршрутизації, розмір яких нелінійно зростає разом із масштабом мережі.

Маршрутизація як обчислення: У протоколі FRP маршрутизатор визначає наступний крок суто математично. Процес прийняття рішення зводиться до швидких логічних операцій над власною координатою та координатою призначення. Алгоритм миттєво обчислює "вектор напрямку", не звертаючись до зовнішньої пам'яті.

Константна складність: Такий підхід забезпечує обчислювальну складність обробки пакету на рівні O(1). Це означає, що швидкість прийняття рішення маршрутизатором залишається незмінно високою незалежно від того, скільки вузлів (тисяча чи мільярд) знаходиться в глобальній мережі.

Алгоритм FRP:

1. Вхідні дані:

Поточна адреса вузла (наприклад, 1.2.3)

Адреса призначення (наприклад, 2.1.1)

2. Порівняння:

Визначити найвищий рівень ієрархії L, на якому адреси відрізняються (наприклад, різні регіони або кластери).

3. Вибір напрямку:

Якщо вузол призначення знаходиться у поточному під-трикутнику — передати пакет на внутрішній порт, що веде до цілі.

4. Рекурсія:

На кожному наступному вузлі повторити процедуру, поки пакет не досягне цілі.

```
Start([Початок: Отримання пакету]) --> Init[Зчитати адресу призначення A_dest\n3читати власну адресу A_curr]
Init --> CheckLocal{A_dest == A_curr?}

CheckLocal -- ТАК --> Deliver([Передати на рівень L2\n(Локальна доставка)])

CheckLocal -- НІ --> CalcDiff[Порівняння адрес:\n3найти індекс відмінності L]

CalcDiff --> CheckLevel{Рівень L < Поточний рівень?}

CheckLevel -- ТАК (Зовнішня ціль) --> SelectUplink[Вибрати порт UPLINK\n(До шлюзу кластера)]

CheckLevel -- НІ (Внутрішня ціль) --> GetSector[Визначити цільовий під-сектор\nна основі цифри A_dest[L]]

GetSector --> SelectPort[Вибрати внутрішній порт\nзгідно з таблицею суміжності]

SelectUplink --> CheckLink{Порт активний?}
SelectPort --> CheckLink

CheckLink -- ТАК --> Forward[Переслати пакет]
Forward --> End([Кінець])

CheckLink -- НІ (Аварія) --> Detour[Активувати режим Detour\n(Вибрати альтернативний порт)]
Detour --> Forward
```

Рисунок 3.6 - теоритичний Алгоритм FRP

Переваги такого підходу:

Кожен вузол виконує просту операцію порівняння координат, що зменшує складність маршрутизації з O(log N) до O(1).

У разі зміни топології (наприклад, додавання нового кластера) не потрібно перебудовувати таблиці — достатньо оновити координати.

Алгоритм легко реалізується у вигляді програмного модуля або навіть апаратного прискорювача.

3.6.3. Порівняння з класичними протоколами

OSPF: Потребує зберігання повної карти мережі на кожному вузлі, що обмежує масштабованість у великих фрактальних мережах. Вимагає періодичної синхронізації стану каналів, що створює службовий трафік.

RIP: Працює на основі метрики хопів, але не враховує топологію мережі, що призводить до неефективних маршрутів у складних структурах.

FRP: Використовує топологічну інформацію, закладену у самій адресі, що дозволяє уникнути надлишкового службового трафіку та забезпечити оптимальні маршрути у фрактальній структурі.

3.6.4. Можливі варіанти реалізації FRP

Програмна реалізація: FRP може бути реалізований як модуль для сучасних маршрутизаторів, що підтримують Python або інші мови автоматизації.

Апаратна реалізація: Завдяки простоті алгоритму, FRP може бути вбудований у ASIC або FPGA для високошвидкісних дата-центрів.

Інтеграція з SDN: Контролер SDN може використовувати координатну інформацію для централізованого управління маршрутами, автоматично генеруючи правила для комутаторів.

Ось перероблений текст, об'єднаний у монолітні абзаци. Я також додав логічні переходи між пунктами для кращого сприйняття .

3.6.5. Потенційні переваги FRP для фрактальних мереж

Впровадження протоколу FRP у фрактальних мережах відкриває низку суттєвих переваг, перш за все, у сфері масштабованості та надійності. Оскільки протокол не залежить від кількості вузлів, складність маршрутизації залишається сталою та передбачуваною навіть за умови експоненційного зростання мережі. Ключовою особливістю FRP є здатність швидко перенаправляти трафік у разі аварії, використовуючи альтернативні маршрути, закладені у фрактальній структурі, без необхідності глобальної перебудови таблиць маршрутизації. Це досягається завдяки автоматичному визначенню шляху на основі координат, що виключає потребу в ручному налаштуванні маршрутів або зон. Крім того, відсутність періодичних оновлень таблиць, характерних для протоколів типу OSPF чи RIP, значно зменшує навантаження на мережу службовим трафіком.

3.6.6. Виклики та напрямки подальших досліджень

Подальший розвиток протоколу FRP вимагає вирішення низки важливих викликів. Критичним завданням є відпрацювання сценаріїв відмов, що передбачає розробку ефективних механізмів швидкого виявлення та обходу пошкоджених ділянок фракталу зі збереженням мінімальної затримки передачі даних.

Для успішного впровадження в гібридних мережах необхідно забезпечити безшовну інтеграцію FRP з існуючими протоколами OSPF/BGP на стиках доменів.

Також потребують детального опрацювання питання безпеки маршрутизації, зокрема впровадження надійних методів аутентифікації та захисту від спуфінгу координатних адрес.

Важливим етапом досліджень має стати моделювання роботи протоколу у великих масштабах, що дозволить оцінити його продуктивність, затримки та стійкість до атак у мережах із тисячами вузлів.

3.6.7. Перспективи впровадження та сфери застосування FRP

Протокол FRP володіє значним потенціалом для впровадження у стратегічно важливих галузях, де традиційні методи маршрутизації досягли межі своєї ефективності.

Гіпермасштабовані Дата-центри

FRP може стати фундаментальною основою для побудови дата-центрів нового покоління, що базуються на 3D-топологіях (наприклад, Губка Менгера). У таких середовищах, де кількість серверів сягає сотень тисяч, класичні протоколи страждають від "вибуху" таблиць маршрутизації та перегріву комутаційних фабрик. Маршрутизація виконується без звернення до пам'яті, що дозволяє створювати надшвидкі "безстанови" комутатори зі значно меншим енергоспоживанням та тепловиділенням, сприяючи реалізації концепції Green IT.

Розумні міста та Інтернет речей

У контексті концепції "Розумного міста", де кількість підключених сенсорів, камер та виконавчих механізмів зростатиме експоненційно, FRP вирішує проблему адресації та автоконфігурації. Завдяки простоті обчислень, функцію маршрутизатора зможуть виконувати навіть малопотужні IoT-пристрої, створюючи децентралізовану mesh-мережу без необхідності в потужних центральних шлюзах. Це забезпечить автономну взаємодію пристроїв навіть за відсутності зв'язку з хмарою.

Критична інфраструктура та системи спеціального призначення

Найбільш перспективною сферою є захист критичної інфраструктури (енергетика, транспорт) та військові тактичні мережі. Висока стійкість до кібератак і фізичних руйнувань робить FRP гарним рішенням для умов, де неможливо гарантувати цілісність каналів зв'язку. Децентралізована логіка дозволяє сегментам мережі функціонувати автономно: навіть якщо командний центр буде знищено, окремі підрозділи (фрактальні кластери) збережуть локальну зв'язність та керованість, автоматично використовуючи вцілілі маршрути.

ВИСНОВКИ

У магістерській кваліфікаційній роботі вирішено актуальну науково-прикладну задачу розробки та дослідження методу побудови високомасштабованих і відмовостійких топологій комп'ютерних мереж на основі фрактальних структур. Проведене теоретичне й експериментальне дослідження дозволило отримати наступні основні результати:

Проведено критичний аналіз сучасних архітектурних рішень і встановлено, що класичні топології («зірка», «дерево», «mesh») та їх гібридні варіації досягли межі ефективності в умовах експоненційного зростання мереж. Виявлено, що ієрархічні структури страждають від концентрації ризиків у кореневих вузлах, а повнозв'язні сітки — від нелінійної складності управління та перевантаження протоколів маршрутизації службовим трафіком.

Теоретично обґрунтовано доцільність застосування фрактальної геометрії для топологічного синтезу мереж. Доведено, що детерміновані фрактали (зокрема Трикутник Серпінського, Килим Серпінського, Губка Менгера) є ефективними інженерними моделями, які поєднують властивості «тісного світу» (малий діаметр), планарності та структурної однорідності. Властивість самоподібності дозволяє вирішити проблему складності, замінивши ручне управління уніфікованими рекурсивними алгоритмами, інваріантними до масштабу мережі.

Розроблено метод побудови гібридної мережевої інфраструктури, що базується на моделі «Фрактальне Ядро — Деревоподібна Периферія». Запропонована архітектура дозволяє локалізувати складність маршрутизації всередині високошвидкісного ядра, забезпечуючи при цьому прозорість та економічність підключення на рівні доступу.

Створено систему Фрактальної Координатної Адресації, яка трансформує IP-адресу з абстрактного ідентифікатора на топологічний маркер. Це дозволило систематизувати адресний простір, спростити навігацію в мережі та створити передумови для впровадження алгоритмічної маршрутизації без використання таблиць.

Запропоновано концепцію протоколу фрактальної маршрутизації (FRP), здатного зменшити обчислювальну складність прийняття рішень з логарифмічної до константної.

Експериментально підтверджено ефективність розробленого методу шляхом імітаційного моделювання у середовищі Cisco Packet Tracer. Результати стрес-тестування продемонстрували високу живучість запропонованої топології: час відновлення зв’язності при критичному розриві магістрального каналу склав менше 2 секунд, що відповідає вимогам до мереж операторського класу та значно перевищує показники класичних рішень на базі STP.

Встановлено переваги фрактальних мереж у контексті кібербезпеки та обробки трафіку. Доведено, що відсутність вразливих супер-хабів та можливість кластерної ізоляції робить такі мережі стійкими до спрямованих атак. Крім того, структура мережі демонструє ефект топологічного резонансу з самоподібним трафіком, що дозволяє ефективно поглинати пікові навантаження без виникнення заторів.

Практична цінність роботи полягає у розробці готових інженерних рекомендацій та алгоритмів конфігурації обладнання для розгортання надійних кампусних, корпоративних та міських мереж. Запропонований підхід дозволяє будувати масштабовані системи на базі стандартного, економічно доступного комутаційного обладнання, знижуючи капітальні та операційні витрати.