**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**
**КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ**

# КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Відмовостійкі корпоративні мережі з використанням протоколів динамічної маршрутизації»

на здобуття освітнього ступеня бакалавра
зі спеціальності 123 Комп'ютерної інженерії
*(код, найменування спеціальності)*
освітньо-професійної програми Комп'ютерна інженерія
*(назва)*

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

_____ *Юрій Бова*
*(підпис)* *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. КІД-42
Бова Юрій
Ім'я, ПРІЗВИЩЕ

Керівник: Соколов Кирило PhD
*науковий ступінь, вчене звання* Ім'я, ПРІЗВИЩЕ

Рецензент: _____
*науковий ступінь, вчене звання* Ім'я, ПРІЗВИЩЕ

**Київ 2026**

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**Навчально-науковий інститут Інформаційних технологій**

Кафедра 123 Комп'ютерної інженерії

Ступінь вищої освіти бакалавр

Спеціальність 123 Комп'ютерної інженерії

Освітньо-професійна програма Комп'ютерна інженерія

**ЗАТВЕРДЖУЮ**
Завідувач кафедри
Комп'ютерної інженерії
_____ Наталія ЛАЩЕВСЬКА
_____
«_____» _____ 2026р.

# ЗАВДАННЯ
# НА КВАЛІФІКАЦІЙНУ РОБОТУ

Бова Юрій Володимирович
*(прізвище, ім'я, по батькові здобувача)*

1. Тема кваліфікаційної роботи: Відмовостійкі корпоративні мережі з використанням протоколів динамічної маршрутизації
керівник кваліфікаційної роботи Соколов Кирило PhD,
*(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)*
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «24» лютого 2026р. № 56
2. Строк подання кваліфікаційної роботи «5» червня 2026р.
3. Вихідні дані до кваліфікаційної роботи: типи маршрутизації : статична маршрутизація, динамічна маршрутизація; класифікація протоколів за сферою застосування: IGP, EGP; алгоритмічні парадигми : дистанційно-векторна, стан каналу, шлях-вектор; ключові протоколи: RIP, OSPF, EIGRP, IS-IS, BGP; концепції високої доступності та швидкої збіжності: Збіжність, BFD, IP Fast Reroute, BGP PI; Сучасні тенденції та еволюція: Segment Routing, SDN
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
   1. Архітектура та еволюція протоколів динамічної маршрутизації в сучасних гетерогенних мережах.
   2. Порівняльний аналіз протоколів динамічної маршрутизації в архітектурах високої доступності корпоративних мереж.
   3. Архітектура та механізми швидкої збіжності в сучасних IP-мережах.
   4. Перелік ілюстративного матеріалу: *презентація*
   5. Дата видачі завдання«24» лютого 2026р.

# КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Збір даних | 25.02-24.03.2026 | Виконано |
| 2 | Обробка матеріалу | 23.03-10.04.2026 | Виконано |
| 3 | Розробка теоретичної частини | 10.04-18.04.2026 | Виконано |
| 4 | Розробка моделі мережі | 18.04-22.04.2026 | Виконано |
| 5 | Оформлення звіту | 22.04-24.04 2026 | Виконано |

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

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

# РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 47 стор., 10 рис., 10 табл., 30 джерел.

*Мета роботи* – Дослідити різницю між статичною та динамічною маршрутизацією в межах корпоративних мереж, та перевірка корпоративної мережі на її відмово стійкість

*Об'єкт дослідження* – Корпоративна комп'ютерна мережа з динамічною та статичною маршрутизацією

*Предмет дослідження* – Комп'ютерна мережа

*Короткий зміст роботи:* Робота присвячена аналізу динамічноїмаршрутизації як фундаментального механізму для забезпечення масштабованості та відмовостійкості сучасних комп'ютерних мереж. Автор розглядає класифікацію протоколів на внутрішні (IGP), такі як RIP, OSPF, EIGRP та IS-IS, що діють у межах однієї автономної системи, та зовнішні (EGP), представлені протоколом BGP, який забезпечує глобальну зв'язність інтернету. У дослідженні детально порівнюються алгоритмічні підходи: дистанційно-векторний метод (RIP), стан каналу (OSPF, IS-IS) та шлях-вектор (BGP), а також гібридний алгоритм DUAL, що використовується в EIGRP для миттєвого перемикання на резервні шляхи. Особлива увага приділяється механізмам швидкої збіжності, зокрема використанню протоколу BFD для мілісекундного виявлення збоїв та технологій локального ремонту трафіку, таких як LFA та TI-LFA в архітектурах Segment Routing. Розглянуто еволюцію протоколів у контексті переходу на IPv6, де OSPFv3 та впровадження TLV-структур в IS-IS забезпечують стабільність великих інфраструктур. Практична частина роботи, виконана в середовищі Cisco Packet Tracer, наочно демонструє переваги динамічної маршрутизації над статичною: при імітації обриву зв'язку протокол OSPF автоматично перераховує шлях та відновлює передачу даних, тоді як статична архітектура призводить до повної втрати

зв'язності. На завершення аналізуються ринкові тенденції на 2025-2026 роки, що вказують на зростаючу роль програмно-визначених мереж (SDN) та централізованого обчислення шляхів для підтримки вимогливих сервісів 5G та хмарних технологій.

**Зміст**

**Вступ……....10**

**1. Архітектура та еволюція протоколів динамічної маршрутизації в сучасних гетерогенних мережах……11**

1.1 Статична проти динамічної маршрутизації: Технічний компроміс…….11

1.2 Протокол RIP: Спадщина та обмеження……13

1.3 Протокол OSPF: Промисловий стандарт ієрархічних мереж……14

1.4 Аналіз ринкових тенденцій на 2025-2026 роки……..18

**2. Порівняльний аналіз протоколів динамічної маршрутизації в архітектурах високої доступності корпоративних мереж……19**

2.1 Порівняння OSPF та EIGRP у контексті швидкості конвергенції та відмовостійкості……19

2.2 Механізми Link-State у OSPF та вплив LSA Flooding на стабільність…20

2.3 Стратегії BGP Multihoming для забезпечення високої доступності на межі мережі……23

2.4 Гібридні дизайни: IGP та BGP в ієрархії……26

**3. Архітектура та механізми швидкої збіжності в сучасних IP-мережах……..28**

3.1 Еволюція та архітектурні стадії мережевої збіжності……...28

3.2 Протокол Bidirectional Forwarding Detection (BFD)……...30

3.3 Механізми Throttling для LSA та SPF……..31

3.4 Topology-Independent LFA (TI-LFA) та Segment Routing……...34

**4. Порівняння статичної маршрутизації та динамічної в середовищі Cisco Packet Tracer……..37**

4.1 Структура мережі……..……37

4.2 Статична маршрутизація……...38

4.3 Динамічна маршрутизація (OSPF)……...41

4.4 Порівння статичної та динамічної маршрутизації в разі недоступності одного з прямих маршрутів……..43

Висновки…….46
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ……..47
Додаток А……...49

# ВСТУП

Актуальність теми. У сучасному цифровому світі безперервність бізнес-процесів критично залежить від стабільності та доступності мережевої інфраструктури. Корпоративні мережі перетворилися на складні гетерогенні системи, де будь-яка затримка або втрата зв’язку може призвести до значних фінансових збитків. Традиційні методи статичної маршрутизації, хоча і забезпечують високу передбачуваність, виявляються неефективними у великих динамічних інфраструктурах через складність масштабування та відсутність автоматичної адаптації до збоїв.

Забезпечення відмовостійкості (High Availability) стає визначальним фактором при проектуванні сучасних мереж. Це вимагає впровадження протоколів динамічної маршрутизації, які здатні самостійно виявляти зміни в топології та перераховувати оптимальні шляхи за мілісекунди. З огляду на ринкові тенденції 2025–2026 років, особливого значення набувають механізми швидкої збіжності, такі як BFD та IP Fast Reroute, а також еволюція мереж у бік програмно-визначених архітектур (SDN) та Segment Routing

# 1.Архітектура та еволюція протоколів динамічної маршрутизації в сучасних гетерогенних мережах

Динамічна маршрутизація представляє собою критично важливий механізм функціонування комп'ютерних мереж, який забезпечує автоматичну адаптацію маршрутизаторів до змін топології та умов передачі даних. На відміну від статичної маршрутизації, де кожен шлях програмується вручну адміністратором, динамічні протоколи дозволяють пристроям самостійно виявляти мережі, обмінюватися інформацією про доступність вузлів та обчислювати оптимальні маршрути за допомогою спеціалізованих алгоритмів. Ця здатність до самоорганізації стає фундаментальною умовою масштабованості та відмовостійкості сучасних корпоративних мереж, інфраструктур постачальників послуг та глобального інтернету. Фундаментальні концепції та класифікація систем маршрутизації. Протоколи динамічної маршрутизації класифікуються на основі їхнього призначення, алгоритмічної бази та способу обробки адресної інформації. Розуміння цих відмінностей є необхідним для проектування ефективних мережевих архітектур, оскільки кожен клас протоколів вирішує специфічні завдання та має унікальні вимоги до апаратних ресурсів. IGP та EGP: Внутрішня та зовнішня маршрутизація**.** Глобальна мережева інфраструктура організована за принципом автономних систем (AS), що являють собою групи IP-мереж під єдиним адміністративним управлінням. В залежності від того, де відбувається обмін маршрутною інформацією — всередині такої системи чи між ними — протоколи поділяються на дві великі категорії.

Внутрішні протоколи шлюзу (Interior Gateway Protocols, IGP) використовуються для маршрутизації всередині організації або автономної системи. Їхня головна мета — забезпечити швидку конвергенцію та ефективне використання внутрішніх каналів зв'язку. До основних представників IGP належать RIP, OSPF, EIGRP та IS-IS.

Зовнішні протоколи шлюзу (Exterior Gateway Protocols, EGP) призначені для зв'язку між різними автономними системами та постачальниками послуг. У сучасному ландшафті єдиним функціонуючим протоколом цього класу є Border Gateway Protocol (BGP), який забезпечує зв'язність всього інтернету.

## 1.1 Статична проти динамічної маршрутизації: Технічний компроміс

Хоча динамічна маршрутизація пропонує автоматизацію, статичні маршрути залишаються актуальними для специфічних сценаріїв, таких як тупикові мережі

або канали з обмеженою пропускною здатністю. Статична маршрутизація вимагає менше обчислювальних ресурсів та забезпечує вищий рівень передбачуваності, проте стає некерованою у великих інфраструктурах.

Таблиця 1.1 – порівння характеристики статичної та динамічної маршрутизації

| **Характеристика** | **Статична маршрутизація** | **Динамічна маршрутизація** |
|---|---|---|
| Масштабованість | Низька; складність зростає з кожним вузлом | Висока; автоматичне виявлення сусіда |
| Використання ресурсів CPU | Мінімальне | Потребує значної пам'яті та ресурсів CPU |
| Адаптація до збоїв | Відсутня (ручне втручання) | Автоматичне перерахування шляхів |
| Передбачуваність | Повна; маршрут не змінюється | Залежить від метрик та стану лінків |
| Сфера застосування | Малі стабільні мережі | Великі, динамічні інфраструктури |

Алгоритмічні парадигми динамічного обміну даними. Ефективність протоколу визначається алгоритмом, за допомогою якого він обчислює найкращий шлях. В інженерній практиці виділяють три основні підходи: дистанційно-векторний, стан каналу та шлях-вектор. Дистанційно-векторна маршрутизація та алгоритм Беллмана-Форда

Дистанційно-векторні протоколи (Distance Vector) базуються на принципі, що кожен маршрутизатор повідомляє сусідам свою відстань (метрику) та напрямок (вектор) до кожної відомої йому мережі. Це часто називають "маршрутизацією за чутками" (routing by rumour), оскільки пристрій не має карти всієї мережі, а лише довіряє інформації від суміжних пристроїв.

Основним механізмом тут є алгоритм Беллмана-Форда. У математичному представленні, якщо $D_x(y)$ — це оцінка найкоротшої відстані від вузла $x$ до вузла $y$, а $c(x,v)$ — вартість лінка до безпосереднього сусіда $v$, то оновлення відбувається за формулою:

$$D_x(y) = \min_v\{c(x,v) + D_v(y)\}$$

де мінімум береться по всіх сусідах $v$. Хоча цей підхід споживає мало пам'яті, він схильний до повільної збіжності та утворення маршрутних петель. Маршрутизація стану каналу та алгоритм Дейкстри

Протоколи стану каналу (Link-State), такі як OSPF та IS-IS, працюють інакше: кожен маршрутизатор збирає інформацію про стан усіх з'єднань у всій зоні або мережі. Замість передачі таблиць маршрутизації, пристрої розсилають оголошення про стан каналів (LSA — Link State Advertisements), які наповнюють ідентичну базу даних стану каналів (LSDB) на кожному пристрої.

Маючи повну картину топології, маршрутизатор використовує алгоритм SPF (Shortest Path First), також відомий як алгоритм Дейкстри, для побудови дерева найкоротших шляхів з собою в ролі кореня. Це забезпечує надзвичайно швидку конвергенцію та повну відсутність петель всередині домену, проте вимагає суттєвих апаратних витрат. Протоколи шляху-вектора . Ця категорія представлена протоколом BGP і використовується для міждоменної маршрутизації. Замість використання математичних метрик (як-от затримка або кількість хопів), цей метод анонсує повний список атрибутів, включаючи список автономних систем (AS_PATH). Це дозволяє не лише запобігати петлям (якщо маршрутизатор бачить свою AS у списку, він відкидає шлях), а й приймати рішення на основі бізнес-політик та контрактних зобов'язань.

## 1.2 Протокол RIP: Спадщина та обмеження

Routing Information Protocol (RIP) — один із найстаріших IGP, вперше стандартизований у RFC 1058. Як дистанційно-векторний протокол, він використовує кількість переходів (hop count) як метрику, де максимальна відстань обмежена 15 хопами. 16-й хоп вважається нескінченністю, що робить мережу недосяжною. Еволюція версій RIP:

Протягом десятиліть RIP адаптувався до вимог мереж, що розвивалися:

1. RIPv1: Класовий протокол, який не передає інформацію про маску підмережі

та використовує широкомовні повідомлення кожні 30 секунд, що створює зайвий шум у мережі.

2. RIPv2: Впровадив підтримку безкласової маршрутизації (VLSM/CIDR), автентифікацію та мультикаст-розсилку на адресу 224.0.0.9, що значно покращило безпеку та ефективність.
3. RIPng: Версія для IPv6, яка працює на порту UDP 521 і зберігає обмеження у 15 хопів.

Незважаючи на простоту налаштування, RIP сьогодні витіснений з великих мереж через повільну збіжність та неефективну метрику, яка не враховує швидкість каналів.

### 1.3 Протокол OSPF: Промисловий стандарт ієрархічних мереж

Open Shortest Path First (OSPF) є найбільш розповсюдженим внутрішнім протоколом у корпоративному секторі. Він був створений IETF як відкрита альтернатива пропрієтарним рішенням для подолання обмежень RIP. Ієрархічна структура та типи областей. OSPF забезпечує масштабованість через розділення мережі на області (Areas). Це дозволяє обмежити розповсюдження LSA лише певною частиною мережі, зменшуючи навантаження на пам'ять та процесор маршрутизаторів. Центральною є магістральна область (Area 0), до якої повинні бути підключені всі інші області для забезпечення міжобласного зв'язку.

Маршрутизатори в OSPF виконують різні ролі:

- Internal Router: Всі інтерфейси знаходяться в одній області.
- ABR (Area Border Router): З’єднує одну або декілька областей з Area 0.
- ASBR (Autonomous System Boundary Router): Точка перерозподілу (redistribution) маршрутів між OSPF та іншими доменами (EIGRP, BGP, статичні маршрути). OSPFv3: Нова архітектура для епохи IPv6 Впровадження IPv6 вимагало фундаментального перегляду OSPF, що призвело до створення OSPFv3. Хоча основна логіка SPF залишилася незмінною, механізми обробки інформації зазнали радикальних змін.

Найважливішою зміною є відокремлення топології від адресації. У OSPFv2 LSA типів 1 та 2 містили як топологічну інформацію, так і IP-адреси. У OSPFv3 ці LSA описують лише зв'язки між вузлами, а префікси анонсуються через нові типи — Link LSA (Type 8) та Intra-Area Prefix LSA (Type 9). Це означає, що зміна IP-адреси на інтерфейсі більше не викликає повного перерахунку дерева найкоротших шляхів, що значно підвищує стабільність великих мереж.

Таблиця 1.2- Відмінності версій OSFP v2 та v3

| Ознака | OSPFv2 | OSPFv3 |
|---|---|---|
| Протокольна база | IPv4 | IPv6 |
| Формування сусідства | На основі IPv4 підмереж | На основі Link-local адрес |
| Автентифікація | Вбудована (MD5/Plain) | Покладається на IPsec |
| Кількість інстансів | Один на інтерфейс | Можливість кількох на одному лінку |
| Опис префіксів | Мережа + маска | Префікс + довжина |

Протокол IS-IS: Вибір сервіс-провайдерів Intermediate System to Intermediate System (IS-IS) часто порівнюють з OSPF через спільну алгоритмічну основу (алгоритм Дейкстри). Проте, завдяки своїй здатності працювати безпосередньо над рівнем L2 (Data Link), IS-IS пропонує унікальні переваги в плані масштабованості та безпеки. Модульність та розширюваність через TLV Однією з найсильніших сторін IS-IS є використання структур TLV (Type-Length-Value). Це дозволяє додавати підтримку нових протоколів та технологій (як-от IPv6, Segment Routing, Traffic Engineering) без необхідності переписувати основний код протоколу. Саме тому підтримка IPv6 в IS-IS була реалізована значно простіше, ніж в OSPF: просто додаванням нових TLV (232 для адрес та 236 для доступності) до існуючих повідомлень.

Ієрархія рівнів (Levels)

На відміну від областей OSPF, IS-IS використовує концепцію рівнів:

- Level 1: Внутрішньообласна маршрутизація (аналог OSPF intra-area).
- Level 2: Магістральна маршрутизація між областями (аналог OSPF Area 0).
- L1/L2: Маршрутизатори, що виконують обидві ролі, забезпечуючи зв'язність між рівнями.

Оператори віддають перевагу IS-IS для побудови великих "пласких" мереж,

оскільки він створює менше службового трафіку та краще справляється з великою кількістю префіксів у межах одного домену. Протокол EIGRP: Гібридний підхід Cisco. Enhanced Interior Gateway Routing Protocol (EIGRP) займає особливе місце, поєднуючи швидкість конвергенції протоколів стану каналу з простотою дистанційно-векторних. До 2013 року він був повністю закритим (proprietary), що змушувало організації будувати мережі виключно на обладнанні Cisco. Алгоритм DUAL та резервні маршрути "Секретна формула" EIGRP — це алгоритм DUAL (Diffusing Update Algorithm). Він підтримує три ключові таблиці: сусідів, топології та маршрутизації. На відміну від OSPF, який зберігає повну топологію всієї мережі, EIGRP зберігає лише кращі шляхи (Successors) та гарантовано безпетлеві резервні шляхи (Feasible Successors) від сусідів.

Якщо основний маршрут зникає, EIGRP не запускає важкий процес перерахунку, а миттєво перемикається на Feasible Successor, що забезпечує конвергенцію за мілісекунди. Крім того, EIGRP є єдиним протоколом, що дозволяє Unequal Cost Load Balancing, дозволяючи використовувати канали з різною пропускною здатністю одночасно.

Метрика EIGRP Композитна метрика EIGRP враховує пропускну здатність та сумарну затримку за замовчуванням, але може бути налаштована на врахування надійності та завантаженості каналу.

$$\text{Metric} = 256 \times \left( \frac{10^7}{\min(\text{bandwidth})} + \sum \text{delay} \right)$$

Ця формула забезпечує набагато точніший вибір шляху порівняно з RIP. BGP: Зовнішня маршрутизація та політики Border Gateway Protocol (BGP) — це "клей", що тримає інтернет разом. Як протокол шляху-вектора, він працює не на основі швидкості лінків, а на основі атрибутів шляху, що дозволяє реалізовувати складні економічні та політичні стратегії маршрутизації. Атрибути та процес вибору шляху BGP використовує багатокритеріальний процес вибору кращого маршруту. Основні атрибути включають:

1. Weight: Локальний параметр (тільки для одного маршрутизатора).
2. Local Preference: Пріоритет виходу з автономної системи (чим вище, тим краще).
3. AS_PATH: Список автономних систем, через які пройшов анонс (коротший

список пріоритетніший).

4. MED (Multi-Exit Discriminator): Підказка суміжній AS про бажану точку входу в вашу мережу.

Останнім часом спостерігається зсув у використанні BGP: з периферії мережі він переміщується в її серце — центри обробки даних. Гіганти на кшталт Microsoft та Facebook використовують eBGP як основний протокол у своїх Leaf-Spine топологіях. Це дозволяє уникнути складнощів з областями OSPF, забезпечує кращу масштабованість до сотень тисяч серверів та дозволяє легко керувати трафіком через стандартні механізми BGP Communities.

Таблиця 1.3 – Порівння протоколів OSFP ТА BGP в межах ЦОД

| **Фактор** | **OSPF у ЦОД** | **BGP у ЦОД (RFC 7938)** |
|---|---|---|
| Масштабованість префіксів | Обмежена розміром LSDB | Дуже висока (мільйони маршрутів) |
| Керування трафіком | Тільки через зміну вартості лінків | Гнучкі політики та Communities |
| Складність | Зростає з кількістю областей | Однорідна структура (EBGP) |
| Конвергенція | Дуже швидка | Може бути повільною (потребує тюнінгу) |

Еволюція до Segment Routing та SDNT. Традиційна маршрутизація базується на розподіленому прийнятті рішень: кожен вузол незалежно вирішує, куди відправити пакет. Сучасні вимоги до гнучкості та програмованості призвели до появи нових підходів. Segment Routing (SR): Маршрутизація від джерела

Segment Routing радикально спрощує мережевий стек, видаляючи складні протоколи сигналізації, такі як LDP або RSVP-TE. Вся інформація про шлях тепер вбудовується безпосередньо в заголовок пакету у вигляді списку сегментів (міток в MPLS або адрес в IPv6).

Реалізація SRv6 (Segment Routing over IPv6) перетворює мережу на програмовану платформу. Кожен сегмент (SID) — це 128-бітна IPv6 адреса, яка складається з

локатора (адреса вузла) та функції (що цей вузол має зробити). Це дозволяє реалізовувати Service Function Chaining (SFC): пакет може бути направлений через послідовність функцій (наприклад, DPI -> Firewall -> NAT) просто шляхом перерахування їхніх ідентифікаторів у заголовку. Роль SDN-контролерів та PCEP. У програмно-визначених мережах (SDN) функція обчислення шляхів виноситься на централізований вузол — Path Computation Element (PCE). Контролер отримує повну топологію мережі від маршрутизаторів через протокол BGP-LS (Link-State). Коли з’являється вимога щодо створення специфічного шляху (наприклад, з гарантованою затримкою менше 10мс), PCE обчислює його і "прошиває" в мережу за допомогою протоколу PCEP (Path Computation Element Protocol).

Ця архітектура дозволяє реалізувати Application-Aware Networking, де мережа динамічно підлаштовується під потреби конкретних додатків у реальному часі.

### 1.4 Аналіз ринкових тенденцій на 2025-2026 роки

Ринок протоколів маршрутизації перебуває у фазі активної трансформації, зумовленої розгортанням мереж 5G та масовим переходом до хмарних інфраструктур. Згідно з аналітичними даними, світовий ринок рішень для Segment Routing, який оцінювався у $3.8 млрд у 2025 році, зростатиме з темпом 12.8% і досягне $11.2 млрд до 2034 року.

Драйвери зростання

1. Розгортання 5G Standalone (SA): Вимоги до ультранизької затримки (URLLC) та мережевого слайсингу (Network Slicing) роблять SRv6 безальтернативним вибором для транспортних мереж операторів.
2. Міграція на IPv6: Необхідність підтримки величезної кількості підключених пристроїв (IoT) стимулює впровадження OSPFv3 та MP-BGP.
3. Технологія uSID (Micro-SID): Розробки компанії Cisco та інших вендорів дозволили значно зменшити накладні витрати SRv6 заголовків, що прискорило перехід великих операторів з традиційного MPLS на нативну IPv6 маршрутизацію.

Стабільність глобальної системи BGP. Незважаючи на зростання кількості префіксів в інтернеті (до 1.2 млн у IPv4 на початок 2026 року), глобальна система залишається відносно стабільною. Цікаво, що лише 5% нестабільних префіксів генерують понад 50% всіх оновлень BGP, що вказує на локалізований характер більшості проблем зв'язності. Водночас мережа IPv6 характеризується більшим рівнем "шуму" та нестабільності порівняно з IPv4, що потребує посиленої уваги до потужностей процесорів на граничних маршрутизаторах.

# 2. Порівняльний аналіз протоколів динамічної маршрутизації в архітектурах високої доступності корпоративних мереж

Сучасна парадигма побудови корпоративних мереж висуває безпрецедентні вимоги до надійності та швидкодії інфраструктури передачі даних. У системі, де критичні бізнес-процеси залежать від постійного доступу до хмарних сервісів, розподілених баз даних та систем реального часу, поняття відмовостійкості (High Availability) стає визначальним фактором проектування. Динамічна маршрутизація відіграє роль "центральної нервової системи" мережі, забезпечуючи інтелектуальний перерозподіл трафіку при виникненні апаратних або лінійних збоїв. Проте вибір конкретного протоколу — OSPF, EIGRP, BGP або IS-IS — не може бути випадковим, оскільки кожен із них базується на різних математичних алгоритмах та механізмах обробки подій, що безпосередньо впливає на час відновлення працездатності мережі та її загальну стаійкість.

## 2.1 Порівняння OSPF та EIGRP у контексті швидкості конвергенції та відмовостійкості

Центральною проблемою при виборі внутрішнього протоколу шлюзу (IGP) є швидкість конвергенції — інтервал часу, протягом якого всі маршрутизатори в межах домену маршрутизації узгоджують нову топологію після зміни стану будь-якого сегмента. У цьому контексті протистояння OSPF (Open Shortest Path First) та EIGRP (Enhanced Interior Gateway Routing Protocol) представляє два принципово різні підходи до обробки інформації про стан мережі.

Внутрішні механізми EIGRP та переваги алгоритму DUAL. Протокол EIGRP, будучи вдосконаленим дистанційно-векторним протоколом, використовує дифузний алгоритм оновлення (Diffusing Update Algorithm — DUAL). Фундаментальна перевага EIGRP у контексті високої доступності полягає в здатності заздалегідь обчислювати резервні шляхи, що дозволяє уникнути тривалих обчислень безпосередньо в момент аварії. У системі EIGRP кожен маршрутизатор підтримує три ключові таблиці: таблицю сусідів, таблицю топології та таблицю маршрутизації. Найважливішою для забезпечення відмовостійкості є таблиця топології, де зберігаються всі анонсовані сусідами маршрути.

Логіка роботи DUAL базується на концепції наступника (Successor) та допустимого наступника (Feasible Successor). Successor — це сусідній маршрутизатор, який забезпечує шлях із найменшою метрикою до цільової мережі; ця метрика називається допустимою відстанню (Feasible Distance — FD). Feasible Successor

(FS) — це маршрутизатор, який надає альтернативний шлях без петель. Для того, щоб вузол став FS, він повинен задовольняти умові допустимості (Feasibility Condition): анонсована цим вузлом відстань (Reported Distance — RD) до цілі має бути строго меншою, ніж поточна FD основного маршрутизатора. Це математичне обмеження гарантує, що шлях через FS не проходить через сам локальний маршрутизатор, що виключає виникнення петель маршрутизації.

При розриві основного лінка, якщо в таблиці топології існує ідентифікований FS, EIGRP миттєво переносить цей запит до таблиці маршрутизації. Конвергенція в такому разі є майже миттєвою (субсекундною), оскільки вона не потребує розсилання запитів сусідам або складних обчислень дерева SPF. Однак, за відсутності FS, маршрутизатор переходить у активний стан і починає процес розсилання запитів (Queries) до сусідів. У великих, недостатньо структурованих мережах це може призвести до стану Stuck-In-Active (SIA), коли маршрутизатор не може завершити конвергенцію через затримку відповіді від одного з вузлів, що негативно впливає на загальну доступність мережі.

Для розрахунку метрики EIGRP використовує складену формулу, яка враховує смугу пропускання та затримку за замовчуванням, а також може включати надійність та завантаженість: Metric = \left \cdot \left

Тут $BW$ — це мінімальна смуга пропускання на шляху, а $Delay$ — сумарна затримка. Використання такої детальної метрики дозволяє EIGRP більш точно оцінювати якість каналів порівняно з OSPF, який за замовчуванням враховує лише пропускну здатність.

## 2.2 Механізми Link-State у OSPF та вплив LSA Flooding на стабільність

Протокол OSPF використовує алгоритм найкоротшого шляху (Shortest Path First — SPF) Дейкстри. На відміну від EIGRP, кожен маршрутизатор OSPF володіє повною картиною топології в межах своєї зони (Area), яка зберігається у базі даних стану зв’язків (LSDB). Відмовостійкість OSPF забезпечується механізмом лавинної розсилки оголошень про стан зв’язків (LSA Flooding). Коли стається обрив лінка, маршрутизатор, що виявив зміну, негайно генерує нове LSA і розсилає його всім сусідам. Отримавши LSA, кожен маршрутизатор оновлює свою LSDB і запускає алгоритм SPF для перерахунку дерева найкоротших шляхів.

Хоча OSPF є відкритим стандартом і забезпечує високу точність вибору шляхів, процес конвергенції зазвичай повільніший, ніж у EIGRP, через кілька факторів:

- Таймери очікування: OSPF зазвичай очікує завершення процесу flooding перед

запуском SPF, щоб мінімізувати кількість перерахунків при множинних змінах топології.

- Обчислювальне навантаження: Алгоритм SPF є ресурсномістким; у мережах з великою кількістю вузлів у межах однієї зони перерахунок може створювати значне навантаження на CPU.
- Ієрархічна структура: Для масштабування OSPF вимагає поділу на зони, де всі зони мають підключатися до магістральної зони (Area 0). Будь-яка нестабільність у магістралі впливає на всю автономну систему.

Проте в сучасних реалізаціях OSPF можна значно прискорити за допомогою Loop-Free Alternate (LFA). LFA дозволяє OSPF заздалегідь розрахувати резервний шлях, аналогічно до Feasible Successor в EIGRP, що дозволяє виконувати перемикання на рівні апаратного забезпечення (FIB) за мілісекунди після виявлення відмови інтерфейсу.

Таблиця 2.1 – Порівнння EIGRP та OSPF

| Параметр порівняння | EIGRP | OSPF |
|---|---|---|
| Алгоритм | DUAL (дифузні оновлення) | SPF (алгоритм Дейкстри) |
| Тип протоколу | Гібридний (Advance Distance Vector) | Link-State (стан зв’язків) |
| Швидкість конвергенції | Мілісекунди (при наявності FS) | Секунди (за замовчуванням) |

Подовження таблиці 2.1

| Параметр порівняння | EIGRP | OSPF |
|---|---|---|
| Резервування | Feasible Successors (вбудовано) | LFA (потребує налаштування) |
| Використання ресурсів | Низьке (тільки зміни) | Високе (повний SPF при кожній зміні) |
| Метрика | Складена (BW, Delay, Load, Reliability) | Вартість (залежить від BW) |
| Масштабування | Плоска або ієрархічна структура | Обов'язкова ієрархія (Areas) |

Аналіз показує, що EIGRP демонструє кращі результати за часом відновлення завдяки наявності попередньо перевірених шляхів без петель, тоді як OSPF потребує реактивного підходу — розповсюдження інформації та подальшого обчислення, що робить його більш вразливим до затримок у великих доменах маршрутизації.

## 2.3 Стратегії BGP Multihoming для забезпечення високої доступності на межі мережі

У корпоративних середовищах вихід у мережу Інтернет часто є критичною точкою відмови. Використання одного інтернет-провайдера (ISP) створює ризики, пов'язані не лише з обривом фізичного кабелю, а й з внутрішніми проблемами в мережі самого ISP. Рішенням є BGP Multihoming — підключення до двох або більше автономних систем.Архітектура iBGP та eBGP у Multihoming-сценаріях

Для побудови надійного підключення корпоративна мережа зазвичай використовує eBGP (External BGP) для взаємодії з кожним провайдером та iBGP (Internal BGP) для синхронізації маршрутної інформації між власними межовими маршрутизаторами. Важливою вимогою є використання Loopback-інтерфейсів для встановлення сесій iBGP. Це гарантує, що BGP-сесія між внутрішніми маршрутизаторами не впаде при відмові одного з фізичних інтерфейсів, якщо існує альтернативний шлях усередині мережі.

У дизайні високої доступності часто використовуються два межові маршрутизатори (Edge Routers), кожен з яких підключений до окремого ISP. Це усуває єдину точку

відмови на рівні обладнання. Сесія iBGP між ними дозволяє одному маршрутизатору знати про маршрути, отримані іншим, що забезпечує автоматичне перенаправлення трафіку при виході з ладу одного з каналів.

Механізми виявлення відмов та відновлення зв'язку. BGP за своєю природою є повільним протоколом, орієнтованим на стабільність. Стандартні тайметри (60 секунд для Keepalive та 180 секунд для Hold Timer) є неприйнятними для сучасних бізнес-додатків, оскільки падіння ISP може призвести до трихвилинного простою. Для вирішення цієї проблеми застосовуються два підходи:

1. Агресивні таймери: Зменшення Hold Timer до 3 або 9 секунд. Однак це підвищує навантаження на CPU і може призвести до нестабільності при незначних затримках у передачі пакетів.
2. BFD (Bidirectional Forwarding Detection): Це універсальний механізм швидкого виявлення розриву каналу, який працює на рівні мілісекунд (зазвичай 300 мс). BFD інтегрується з BGP, і при виявленні втрати зв'язку негайно сигналізує BGP про необхідність закриття сесії та перемикання на резервного провайдера.Керування вхідним та вихідним трафіком Для забезпечення виживання мережі при падінні ISP необхідно не лише перенаправити вихідний трафік, а й забезпечити, щоб зовнішній світ знав, як доставити пакети до вашої мережі через іншого провайдера.

- Вихідний трафік: Контролюється атрибутом Local Preference. При отриманні маршрутів від обох ISP, адміністратор може встановити вищий Local Preference для основного каналу. При його падінні BGP автоматично обере шлях через резервного провайдера з нижчим Local Preference.
- Вхідний трафік: Контролюється складніше, оскільки рішення приймають зовнішні автономні системи. Основним методом є AS-Path Prepending — штучне подовження власного номера AS у анонсах до резервного ISP. Це робить шлях через резервного провайдера менш привабливим для решти Інтернету. Також використовуються BGP Communities, які дозволяють просити провайдера змінити пріоритетність анонсів усередині його мережі.

Таблиця 2.2 - Атрибути BGP

| Атрибут BGP | Сфера впливу | Призначення в НА |
|---|---|---|
| Local Preference | Вихідний трафік | Вибір пріоритетного ISP для виходу в мережу |
| AS-Path Prepend | Вхідний трафік | Створення "довшого" шляху через резервний канал |
| MED | Вхідний трафік | Вплив на вхідні точки при підключенні до одного ISP у кількох точках |
| Weight (Cisco) | Вихідний трафік | Локальний пріоритет на конкретному маршрутизаторі |

Застосування Multihoming з підтримкою BFD дозволяє досягти показників доступності 99.99% і вище, скорочуючи річний час простою з годин до лічених хвилин.

IS-IS як фундамент масштабованих та безпечних мереж. Протокол IS-IS (Intermediate System to Intermediate System) хоча і менш поширений у чисто корпоративних LAN-середовищах порівняно з OSPF, займає домінуючі позиції в мережах сервіс-провайдерів та великих дата-центрів завдяки своїй унікальній архітектурі.

Масштабованість та ієрархія: IS-IS проти OSPF**.** IS-IS також є Link-State протоколом, що використовує алгоритм SPF, але він має більш гнучку структуру рівнів (Level 1 та Level 2). На відміну від OSPF, де межі зон проходять через

маршрутизатори, у IS-IS маршрутизатор повністю належить до певного рівня або є прикордонним (L1/L2). Це дозволяє будувати значно більші та стабільніші мережі без жорстких обмежень "зіркоподібної" топології Area 0.

Технічна перевага IS-IS у масштабуванні полягає в ефективності кодування даних. IS-IS використовує TLV (Type-Length-Value) структури, що робить його надзвичайно гнучким для розширення без зміни формату пакетів. У порівнянні пам'яті:

- OSPF: Кожен зовнішній маршрут потребує 36 октетів плюс додаткові 12 октетів для кожного типу сервісу.
- IS-IS: Вимагає лише 12 октетів на зовнішній префікс, що дозволяє зберігати в три рази більше маршрутів при тих же обсягах пам'яті.

Стійкість до атак та безпека Layer 2. Однією з найбільш недооцінених переваг IS-IS у контексті мережевої безпеки є те, що він не працює поверх IP. IS-IS інкапсулюється безпосередньо в кадри канального рівня (Layer 2) за допомогою протоколу CLNS. Це дає протоколу кілька рівнів захисту від атак, властивих OSPF або BGP:

1. Незалежність від IP-адресації: Маршрутизатор IS-IS ідентифікується за допомогою NET (Network Entity Title), а не IP-адреси. Це унеможливлює атаки типу IP-spoofing або спроби відправити підроблені маршрутні оновлення з іншої підмережі.
2. Захист від DoS-атак: Оскільки IS-IS пакети не мають IP-заголовка, вони не можуть бути маршрутизовані за межі безпосереднього сегмента мережі. Будь-яка спроба "бомбардування" мережі OSPF-пакетами з віддаленої точки Інтернету є потенційно можливою, тоді як IS-IS-пакети просто будуть відкинуті першим же маршрутизатором, що не підтримує CLNS на інтерфейсі.
3. Ефективність автентифікації: IS-IS підтримує автентифікацію через змінні поля TLV. На відміну від OSPF, де поле автентифікації фіксоване (64 біти), IS-IS може використовувати довші ключі та сучасніші алгоритми хешування (наприклад, HMAC-SHA) без порушення сумісності.

Інтеграція технологій для максимальної стійкості інфраструктуриАналітичний огляд протоколів показує, що для побудови справді відмовостійкої мережі недостатньо обрати "найкращий" протокол. Сучасний дизайн високої доступності передбачає синергію кількох технологій.

Роль BFD у всіх протоколах маршрутизації Як було зазначено для BGP, BFD є ключовим компонентом HA і для OSPF, EIGRP та IS-IS. Оскільки ці протоколи покладаються на власні Hello-таймери для виявлення падіння сусіда (зазвичай 10-

40 секунд), використання BFD дозволяє скоротити час реакції до мілісекунд. У критичних мережах це запобігає розриву TCP-сесій користувачів при аваріях на фізичному рівні.

## 2.4 Гібридні дизайни: IGP та BGP в ієрархії

Для великих корпорацій оптимальним вважається використання IS-IS або OSPF усередині мережі (як транспорт для Loopback-адрес та інфраструктури) та iBGP для передачі клієнтських або сервісних префіксів. Це дозволяє IGP залишатися компактним і швидким, фокусуючись лише на топології, тоді як BGP бере на себе навантаження з управління величезною кількістю маршрутів та політиками безпеки. У хмарних та віртуалізованих середовищах (наприклад, VMware NSX-T) BGP часто є основним протоколом навіть усередині мережі через його здатність підтримувати ECMP (Equal-Cost Multi-Path) на багатьох рівнях та гнучкість у роботі з кількома зонами доступності (Multi-AZ).

Таблиця 2.3 – Особливості протоколів та сфера застосування

| Технологія | Вплив на відмовостійкість | Рекомендована сфера застосування |
|---|---|---|
| BFD | Субсекундне виявлення збоїв | Всі критичні інтерфейси між маршрутизаторами |
| LFA (FRR) | Негайне перемикання на резерв | Мережі реального часу (VoIP, відео) |
| Graceful Restart | Збереження трафіку при рестарті процесу | Планове обслуговування ядра мережі |

Подовження таблиці 2.3

| Технологія | Вплив на відмовостійкість | Рекомендована сфера застосування |
|---|---|---|
| Summarization | Обмеження поширення нестабільності | Межі зон (ABR) або рівнів (L1/L2) |

# 3.Архітектура та механізми швидкої збіжності в сучасних IP-мережах

Поняття збіжності в сучасних телекомунікаційних системах визначає здатність мережі адаптуватися до змін топології, забезпечуючи безперервність передачі даних навіть за умов критичних відмов окремих компонентів. Збіжність є розподіленим процесом, у ході якого всі маршрутизатори приходять до єдиного узгодженого бачення оптимальних шляхів після виникнення події, що змінює доступність ресурсів. У контексті сучасних вимог до якості обслуговування (QoS) та угод про рівень послуг (SLA), стандартні механізми протоколів маршрутизації, розроблені в епоху мереж «найкращих зусиль» (best-effort), виявляються недостатніми. Необхідність підтримки критичних додатків, таких як Voice over IP (VoIP), фінансові транзакції в реальному часі та мультимедійне мовлення, трансформувала цільові показники збіжності з десятисекундних інтервалів до мілісекунд.

## 3.1 Еволюція та архітектурні стадії мережевої збіжності

Мережева збіжність не є одномоментним актом; це послідовність взаємопов'язаних етапів, кожен з яких вносить свій внесок у загальну затримку відновлення працездатності. Час між виникненням несправності та відновленням сервісу складається з чотирьох основних компонентів: виявлення відмови, розповсюдження інформації про подію, обчислення нових маршрутів та встановлення цих маршрутів у апаратне забезпечення для пересилання пакетів.

Перший етап — виявлення відмови — визначає швидкість, з якою пристрій ідентифікує несправність локального каналу або втрату зв'язку з сусіднім вузлом. Це найбільш критична ланка, оскільки без ідентифікації проблеми жоден з подальших механізмів відновлення не буде ініційований. Другий етап полягає у розповсюдженні інформації по всій мережі. У протоколах стану каналу (Link-State), таких як OSPF або IS-IS, це включає генерацію нових оголошень про стан каналів (LSA або LSP) та їх розсилку (flooding) до всіх інших маршрутизаторів у домені маршрутизації. Третій етап — це обчислення альтернативного шляху. Маршрутизатори, отримавши оновлення, запускають алгоритм найкоротшого шляху (SPF), щоб визначити нову топологію. Останній етап включає оновлення бази маршрутної інформації (RIB) та, що критично важливо, оновлення апаратної таблиці пересилання (Forwarding Information Base, FIB).

Таблиця 3.1 – Етапи збіжності

| **Етап збіжності** | **Опис механізму** | **Вплив на загальний час** |
|---|---|---|
| Виявлення відмови | Ідентифікація фізичного розриву або втрати логічного зв'язку | Найбільший потенціал для оптимізації (від мікросекунд до секунд) |
| Розповсюдження інформації | Flooding оновлених LSA/LSP по всій мережі | Залежить від топології та налаштувань таймерів розсилки |
| Обчислення шляху | Запуск алгоритму Dijkstra (SPF) для перерахунку топології | Залежить від потужності CPU та розміру бази даних станів каналів |
| Оновлення FIB | Встановлення нових маршрутів у апаратну частину (Line Cards) | Може бути «вузьким місцем» при великій кількості префіксів |

Збіжність може бути як запланованою, наприклад, при виведенні ліній з експлуатації для модернізації, так і раптовою, спричиненою аварійними ситуаціями. У випадку запланованих змін оператор може завчасно перенаправити трафік (процес, відомий як «draining»), тоді як раптові відмови потребують миттєвої реакції автоматизованих систем для запобігання утворенню «чорних дір» та тимчасових петель маршрутизації. Тимчасові петлі є особливо небезпечними, оскільки вони не тільки спричиняють втрату пакетів, але й марно споживають ресурси каналів зв'язку та процесорів, погіршуючи стан мережі під час кризи.

Стратегії швидкого виявлення несправностей. Швидкість виявлення відмови безпосередньо залежить від рівня моделі OSI, на якому вона відбувається. Найбільш ефективним є виявлення на фізичному рівні, оскільки воно базується на апаратних сигналах (Loss of Signal, LOS) і зазвичай відбувається миттєво.

Апаратне виявлення та таймери фізичного рівня На Ethernet-інтерфейсах маршрутизатор може миттєво виявити відсутність несучого сигналу. Проте існують ситуації, коли фізичний рівень залишається активним, але передача даних неможлива (наприклад, через несправність комутатора в середині каналу). Для оптимізації реакції на фізичні події використовуються такі параметри:

- Carrier-delay: Цей параметр визначає затримку перед тим, як маршрутизатор повідомить програмному забезпеченню про те, що канал ліг. Налаштування carrier-delay msec 0 дозволяє миттєво реагувати на події.
- Debounce Timer: Використовується для запобігання надмірній реакції на короткочасні коливання сигналу (link flapping).

- Таймери SONET/SDH**:** У магістральних мережах використовуються вбудовані механізми виявлення APS (Automatic Protection Switching), які забезпечують відновлення на рівні оптики.

Якщо пряме апаратне виявлення неможливе, традиційно використовувалися протокольні механізми Keepalive (Hello-пакети). Проте стандартні таймери OSPF (10 секунд для Hello та 40 секунд для Dead) занадто повільні для сучасних потреб. Хоча ці таймери можна агресивно налаштувати до субсекундних значень (Fast Hellos), це призводить до значного навантаження на центральний процесор (CPU) маршрутизатора, оскільки кожна Hello-пачка повинна оброблятися керуючою площиною (Control Plane).

## 3.2 Протокол Bidirectional Forwarding Detection (BFD)

BFD (RFC 5880) став революційним рішенням для уніфікації та прискорення виявлення відмов незалежно від середовища передачі та протоколу маршрутизації. Основна ідея BFD полягає у створенні легковагової сесії між двома пристроями для моніторингу працездатності шляху передачі даних.

Ключові характеристики BFD, що забезпечують швидку збіжність:

1. Протокольна незалежність: BFD працює як окремий сервіс, що надає інформацію про відмови іншим протоколам, таким як BGP, OSPF, IS-IS, EIGRP та навіть механізмам резервування шлюзів типу HSRP.
2. Обробка в апаратній частині: На відміну від Hello-пакетів протоколів маршрутизації, контрольні пакети BFD можуть оброблятися безпосередньо лінійними картами або мережевими процесорами, що дозволяє використовувати інтервали в десятки мілісекунд без ризику перевантаження основного CPU.
3. Конфігуровані інтервали: Типове налаштування передбачає передачу пакетів кожні 50 мілісекунд з множником 3, що забезпечує виявлення відмови за 150 мілісекунд.

Таблиця 3.2- Параметри BFD та їх опис

| Параметр BFD | Значення для швидкої збіжності | Опис |
|---|---|---|
| Desired Min Tx Interval | 50 мс | Частота відправки власних пакетів |

Подовження таблиці 3.2

| Параметр BFD | Значення для швидкої збіжності | Опис |
|---|---|---|
| Required Min Rx Interval | 50 мс | Очікувана частота отримання пакетів від сусіда |
| Detect Multiplier | 3 мс | Кількість пропущених пакетів перед оголошенням відмови |

BFD підтримує два режими роботи: асинхронний, де пакети надсилаються безперервно, та режим запиту (demand mode), де перевірка ініціюється лише за потреби. Також існує режим "Echo", де маршрутизатор надсилає пакет самому собі через сусідній пристрій, що дозволяє перевірити шлях пересилання даних (Forwarding Plane) сусіда без залучення його Control Plane.

Оптимізація внутрішньодоменних протоколів (IGP). Після того, як відмова виявлена (через BFD або фізичний рівень), протоколи стану каналу повинні негайно проінформувати решту мережі та перерахувати шляхи. Стандартні алгоритми OSPF та IS-IS були спроектовані з великими затримками для забезпечення стабільності мережі, але для швидкої збіжності ці затримки мають бути мінімізовані за допомогою адаптивних механізмів.

### 3.3 Механізми Throttling для LSA та SPF

Проблема швидкої реакції полягає в тому, що мережа може стати нестабільною (наприклад, канал постійно вмикається та вимикається). Якщо маршрутизатор буде миттєво генерувати оновлення та запускати перерахунок SPF при кожному такому "флапі", це призведе до вичерпання ресурсів CPU та хаосу в таблицях маршрутизації. Вирішенням є використання експоненціальної витримки (exponential backoff).

Адаптивні таймери працюють за принципом: перша подія обробляється миттєво, а кожна наступна подія протягом певного вікна стабільності карається збільшенням часу очікування.

Таймери SPF Throttling:

- SPF-start: Початкова затримка перед запуском розрахунку найкоротшого шляху. У режимі швидкої збіжності це значення встановлюється в межах 1-50 мс.
- SPF-hold: Мінімальний інтервал між двома послідовними розрахунками. Якщо подія стається під час дії цього таймера, він подвоюється.
- SPF-max-wait**:** Максимальне значення, якого може досягти час очікування.

Аналогічні механізми застосовуються до генерації оновлень — LSA/LSP Throttling. Це дозволяє маршрутизатору, який першим виявив проблему, миттєво відправити повідомлення сусідам, забезпечуючи швидке розповсюдження інформації, але при цьому захищає мережу від перевантаження у разі тривалої нестабільності.

Удосконалення обчислювальної логіки: iSPF та PRC. Для великих топологій повний перерахунок алгоритму Dijkstra може бути ресурсомістким завданням. Сучасні імплементації використовують оптимізації, що дозволяють обчислювати лише ті частини графа мережі, які були затронуті зміною.

- Incremental SPF (iSPF): Замість того, щоб будувати дерево найкоротших шляхів (SPT) з нуля, маршрутизатор модифікує існуюче дерево, додаючи або видаляючи лише змінені вузли та зв'язки.
- Partial Route Calculation (PRC): У протоколі IS-IS зміна префікса (IP-адреси), яка не впливає на фізичну топологію вузлів, не потребує перерахунку всього дерева SPT. PRC дозволяє просто оновити інформацію про доступність префікса, що відбувається значно швидше.

Ще одним методом прискорення є LSA Group Pacing. Замість того, щоб обробляти кожне оголошення індивідуально, маршрутизатор групує їх для сумісної обробки та перевірки контрольних сум, що зменшує загальну кількість циклів CPU та кількість пакетів оновлення в мережі.

Технології локального ремонту: IP Fast Reroute (IPFRR). Навіть при ідеальній оптимізації IGP-таймерів, мережі все одно потрібен час для розповсюдження інформації про відмову (Flooding) та перерахунку маршрутів на всіх вузлах. Цей час зазвичай перевищує поріг у 50 мілісекунд, необхідний для голосового трафіку. Щоб подолати цей бар'єр, було впроваджено концепцію локального ремонту (local repair), де маршрутизатор, безпосередньо підключений до місця аварії (Point of Local Repair, PLR), самостійно перенаправляє трафік на заздалегідь обчислений резервний шлях.

Loop-Free Alternates (LFA).LFA (RFC 5286) є базовим механізмом IPFRR. Його суть полягає в тому, що маршрутизатор ще в стабільному стані мережі шукає серед своїх сусідів такого, який може доставити пакет до місця призначення без ризику виникнення петлі назад через пошкоджений канал.

Для того, щоб сусід N вважався "loop-free" альтернативою для маршрутизатора S на шляху до цілі $D$ при відмові каналу $S-E$, він повинен відповідати математичній нерівності:

Distance_opt(N, D) < Distance_opt(N, S) + Distance_opt(S, D)

Ця умова гарантує, що найкоротший шлях від сусіда N до призначення D не проходить через початковий маршрутизатор S.

Таблиця 3.3 - Типи захисту LFA

| **Тип захисту LFA** | **Опис** | **Умова вибору** |
|---|---|---|
| Link Protection | Захист від виходу з ладу конкретного інтерфейсу | Шлях сусіда не проходить через пошкоджений канал |
| Node Protection | Захист від виходу з ладу всього сусіднього маршрутизатора | Шлях сусіда не проходить через вузол, що відмовив |
| SRLG Protection | Захист від відмови групи каналів з спільним ризиком (наприклад, один оптоволоконний кабель) | Резервний шлях не поділяє спільних ризиків з основним |

Головним недоліком класичного LFA є обмеженість топологією. У багатьох реальних мережах (наприклад, у кільцях) такого сусіда просто не існує, оскільки всі альтернативні шляхи проходять через вузол, що обчислює маршрут.

Remote LFA та PQ-вузли. Щоб розширити покриття захисту, була запропонована технологія Remote LFA (RFC 7490). Вона дозволяє використовувати тунелювання (зазвичай MPLS LDP) для доставки пакета до вузла, який знаходиться далі, ніж безпосередній сусід, але який здатний доставити пакет далі без петель.

Розрахунок базується на двох множинах вузлів:

1. P-Space: Множина вузлів, які досяжні з PLR без використання пошкодженого каналу.

2. Q-Space**:** Множина вузлів, з яких можна досягти призначення, не проходячи через пошкоджений канал.

Вузол, який знаходиться на перетині цих просторів (PQ-вузол), стає кінцевою точкою ремонтного тунелю. Це значно підвищує відсоток захищених маршрутів, але вимагає підтримки MPLS у всій мережі та створення цільових LDP-сесій, що ускладнює керування.

### 3.4 Topology-Independent LFA (TI-LFA) та Segment Routing

Найбільш досконалим методом локального відновлення є TI-LFA, що працює в архітектурі Segment Routing (SR). TI-LFA забезпечує 100% покриття в будь-якій зв'язній мережі та гарантує, що трафік буде спрямований по шляху, який стане оптимальним після завершення глобальної збіжності (post-convergence path).

Механізм TI-LFA використовує список сегментів (Segment List) для примусового спрямування пакетів через вузли, що знаходяться за межами зони аварії. Завдяки SR, для цього не потрібно створювати додаткові протокольні сесії або підтримувати складний стан у ядрі мережі; вся інформація про шлях інкапсулюється безпосередньо в заголовок пакета на вузлі PLR. Це дозволяє досягти часу перемикання менше 50 мс навіть у найскладніших випадках відмов вузлів або груп каналів.

BGP Prefix Independent Convergence (BGP PIC). У великих мережах інтернет-провайдерів основною проблемою є не тільки швидкість IGP, але й масштабованість BGP. Стандартна таблиця маршрутизації Internet містить близько мільйона префіксів. Коли трапляється аварія на межі мережі (Edge) або в її ядрі (Core), маршрутизатору доводиться оновлювати кожен запис у FIB окремо, що при швидкості обробки в десятки тисяч префіксів за секунду призводить до простою тривалістю в десятки секунд.

BGP PIC вирішує цю проблему за допомогою ієрархічної структури даних у площині пересилання.

Ієрархічна структура FIB та індирекція. Традиційна архітектура FIB передбачає прямий зв'язок між префіксом та вихідним інтерфейсом з L2-заголовком. При зміні шляху потрібно переписати кожен запис префікса. Ієрархічна FIB впроваджує рівень непрямої адресації (indirection), де тисячі префіксів посилаються на один об'єкт "Next-Hop".

PIC Core: Захищає від відмов усередині автономної системи. Коли IGP-шлях до BGP Next-Hop змінюється (наприклад, через відмову лінка в ядрі), маршрутизатору достатньо оновити лише один запис в ієрархії — шлях до Next-Hop. Оскільки всі BGP-префікси посилаються на цей запис через вказівник, вони миттєво "дізнаються" про новий шлях без необхідності індивідуального оновлення.

PIC Edge: Захищає від відмов на межі мережі, наприклад, при виході з ладу PE-маршрутизатора або каналу до клієнта.

- Для реалізації PIC Edge маршрутизатор повинен заздалегідь розрахувати та встановити в FIB резервний BGP-шлях.
- Це вимагає використання технологій, таких як BGP Add-Path, щоб Route Reflector міг передавати більше одного варіанту шляху до межових пристроїв.
- При виявленні відмови основного PE, вхідний маршрутизатор просто перемикає вказівник на резервний PE. Оскільки перемикання відбувається на рівні ієрархії "Next-Hop List", воно є незалежним від кількості префіксів (Prefix Independent).

Таблиця 3.4 – Режими BGP PIC

| **Режим BGP PIC** | **Тип відмови** | **Механізм перемикання** | **Залежність від кількості префіксів** |
|---|---|---|---|
| PIC Core | Канал або вузол у ядрі мережі | Оновлення IGP-шляху до BGP Next-Hop | Відсутня (Prefix Independent) |
| PIC Edge | Канал PE-CE або весь PE-вузол | Перемикання на резервний BGP Next-Hop | Відсутня (Prefix Independent) |

Для коректної роботи PIC Edge без утворення мікро-петель критично важливо забезпечити тунелювання трафіку між PE-маршрутизаторами (через MPLS або GRE), щоб транзитні вузли в ядрі не приймали самостійних рішень щодо маршрутизації пакетів, які знаходяться в процесі відновлення.

Практичні аспекти та апаратні обмеження. Реалізація механізмів швидкої збіжності накладає певні вимоги на апаратне забезпечення. У сучасних маршрутизаторах критично важливою є повна ізоляція Control Plane від Data Plane. Це дозволяє протоколам маршрутизації (які працюють на центральному CPU) обчислювати зміни, тоді як спеціалізовані ASIC продовжують пересилати пакети за старими або заздалегідь підготовленими резервними шляхами.

Однією з проблем є швидкість завантаження FIB з пам'яті керуючого процесора (RP) в пам'ять лінійних карт (LC). У розподілених системах процес оновлення FIB може стати вузьким місцем. Для вирішення цього використовується пріоритезація префіксів: спочатку оновлюються маршрути до Loopback-інтерфейсів інших PE (що важливо для BGP та VPN), а потім — усі інші інтернет-маршрути.

Також слід враховувати обмеження конкретних платформ. Наприклад, деякі старі шасі (такі як Cisco Catalyst 7600) потребують рециркуляції пакетів для підтримки ієрархічної FIB, що може вдвічі знизити пропускну здатність пристрою під час роботи механізмів PIC. Сучасні платформи на базі чіпсетів типу Cisco NCS або Juniper Trio підтримують глибоку ієрархію вказівників (chained composite next hops) на апаратному рівні без втрати продуктивності.

# 4. Порівняння статичної маршрутизації та динамічної в середовищі Cisco Packet Tracer

## 4.1 Структура мережі

Ця топологія, створена у Cisco Packet Tracer, є моделью для демонстрації принципів побудови мереж середнього масштабу. Вона має кільцеву структуру (mesh), що є ідеальним майданчиком для порівняння статична маршрутизація та динамічний протокол (OSPF).

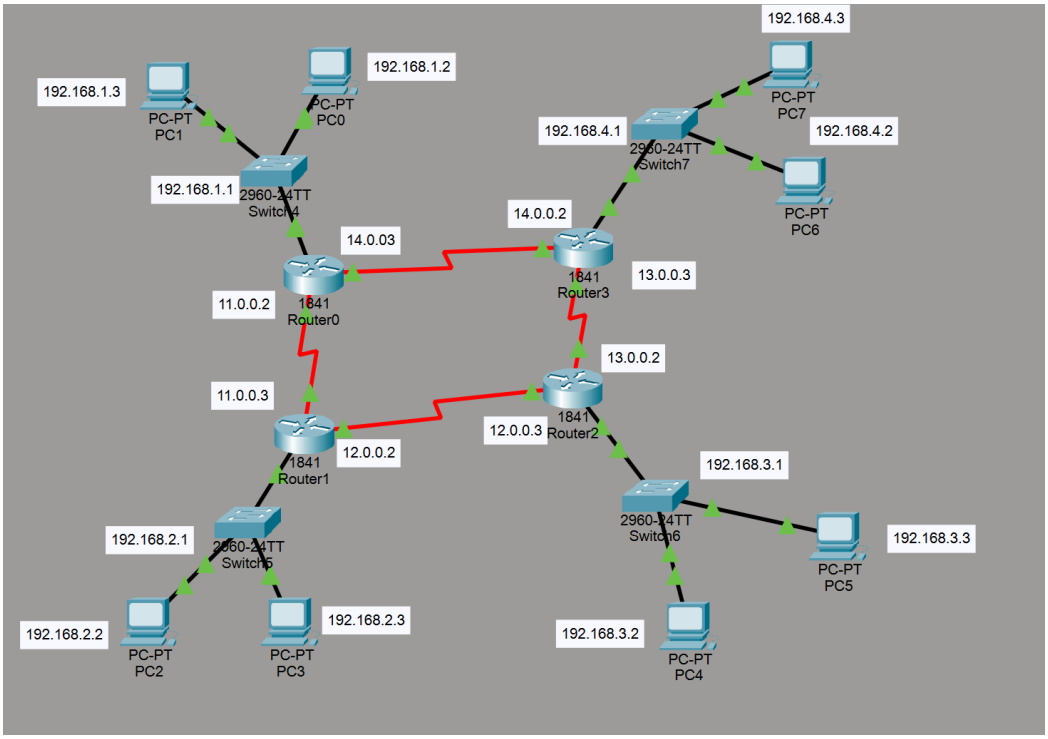



Рисунок 4.1 – Демонстраційна модель корпоративної мережі

Мережа складається з чотирьох сегментів, кожен з яких має свій маршрутизатор (Router 1841), комутатор та кінцеві пристрої (ПК):

Локальні мережі (LAN): Кожен маршрутизатор обслуговує свою підмережу класу C (192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0)

Магістральні канали (WAN): Маршрутизатори з'єднані між собою послідовними Serial, що утворюють замкнений контур. Використовуються підмережі 11.0.0.0, 12.0.0.0, 13.0.0.0 та 14.0.0.0.

## 4.2 Статична маршрутизація

Для статичної маршрутизації потрібно власноруч прописувати основні маршрути та їх резервні версії за для збільшення відмово стійкості мережі вразі виникнення неполадок або надмірних навантажень на один з маршрутизаторів.

Налаштування маршрутизаторів:

Router0 (Верхній ліворуч) Цей роутер обслуговує локальну мережу 192.168.1.0/24.

- Шлях до мережі Router1 (192.168.2.0): Пакет йде через сусідній інтерфейс 11.0.0.3.
- Шлях до мережі Router2 (192.168.3.0): Також через 11.0.0.3 (транзитом через Router1).
- Шлях до мережі Router3 (192.168.4.0): Прямий зв'язок через 14.0.0.2 (транзитом через Router1).
- Службові маршрути: Прописані шляхи до транзитних мереж 12.0.0.0 та 13.0.0.0.

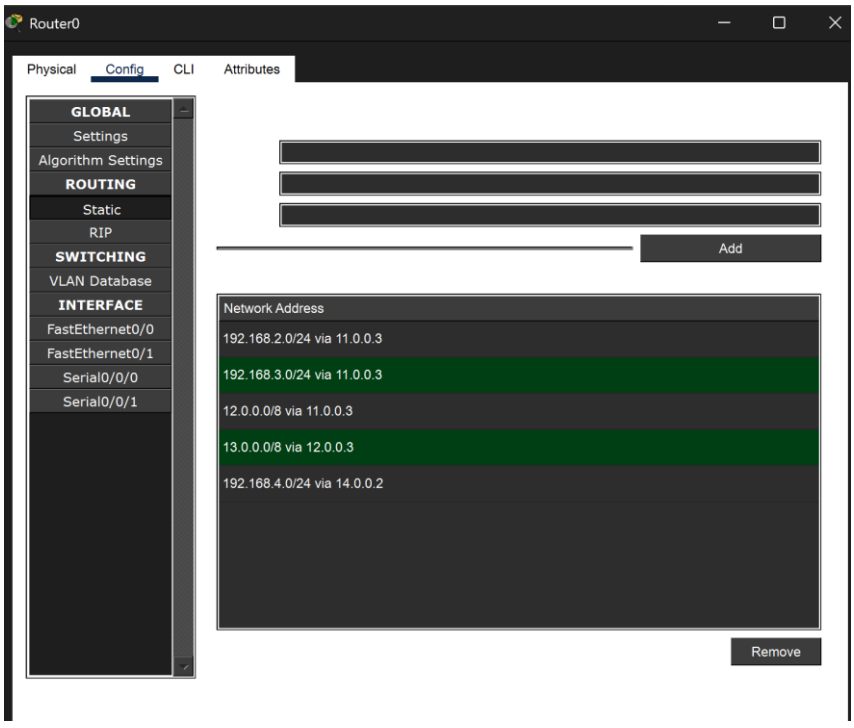



Рисунок 4.2 – Налаштування статичної маршрутизації на ротері№0

Router1 (Нижній ліворуч) Обслуговує локальну мережу 192.168.2.0/24.

- Шлях до Router0 (192.168.1.0): Прямий вихід через 11.0.0.2.
- Шлях до Router2 (192.168.3.0): Прямий вихід через 12.0.0.3.
- Шлях до Router3 (192.168.4.0): Пакет йде транзитом через Router2 (12.0.0.3).
- Транзит: Має маршрут до мережі 13.0.0.0 через 12.0.0.3, щоб "бачити" лінію між Router2 та Router3.

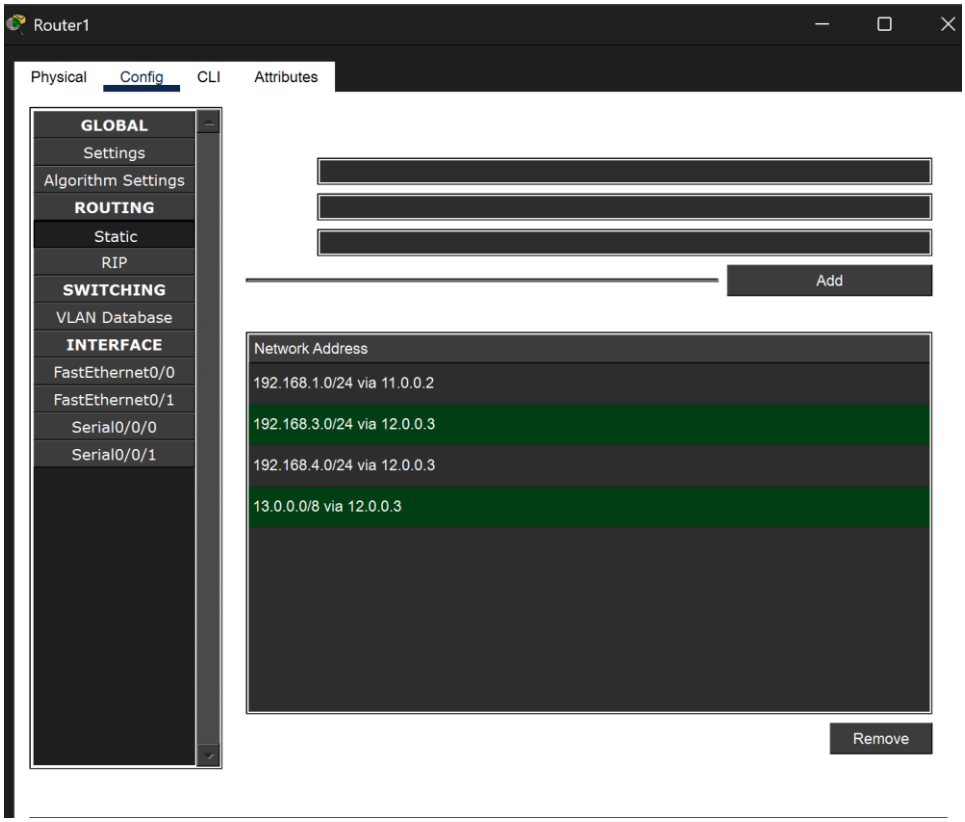



Рисунок 4.3 – Налаштування статичної маршрутизації на ротері№1

Router2 (Нижній праворуч) Обслуговує локальну мережу 192.168.3.0/24.

- Шлях до Router1 (192.168.2.0): Прямий зв'язок через 12.0.0.2.
- Шлях до Router0 (192.168.1.0): Транзитом через Router1 (12.0.0.2).
- Шлях до Router3 (192.168.4.0): Прямий вихід через 13.0.0.3.
- Транзит: Знає про мережу 11.0.0.0 через сусідній Router1 (12.0.0.2).

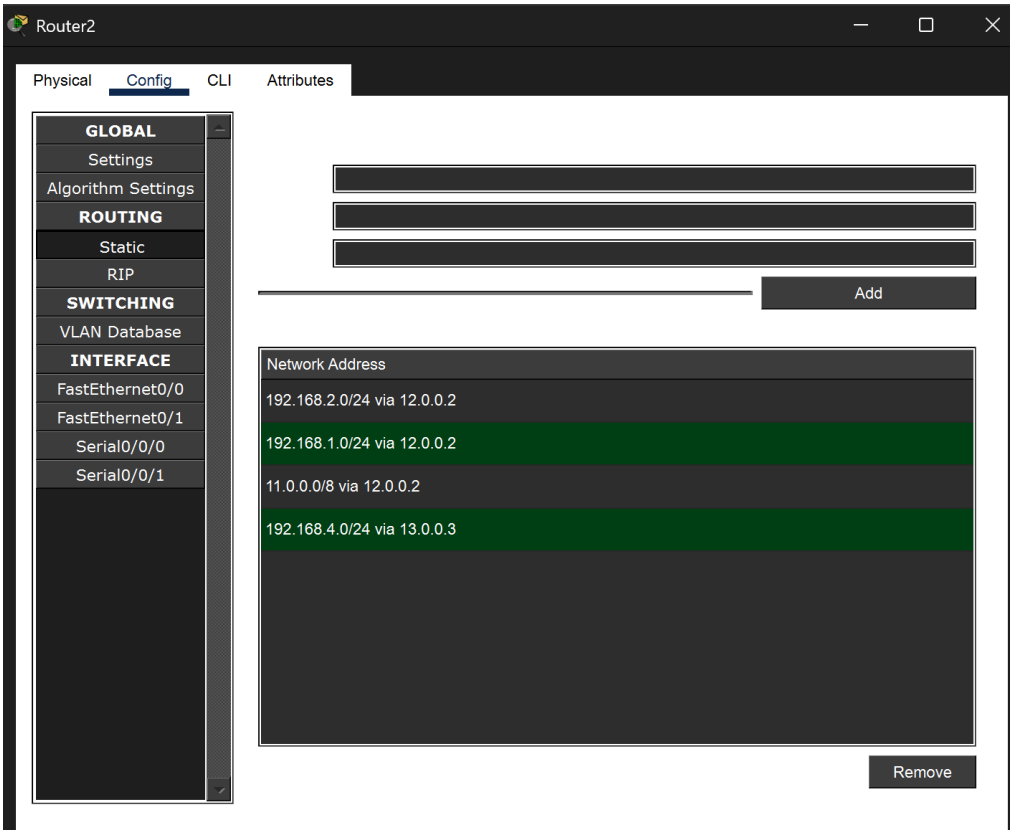



Рисунок 4.4 – Налаштування статичної маршрутизації на ротері№2

Router3 (Верхній праворуч) Обслуговує локальну мережу 192.168.4.0/24.

- Шлях до Router2 (192.168.3.0): Прямий зв'язок через 13.0.0.2.
- Шлях до Router1 (192.168.2.0): Транзитом через Router2 (13.0.0.2).
- Шлях до Router0 (192.168.1.0): Прямий зв'язок через 14.0.0.3
- Службові маршрути: Вказані шляхи до дальніх ліній 12.0.0.0 та 11.0.0.0.

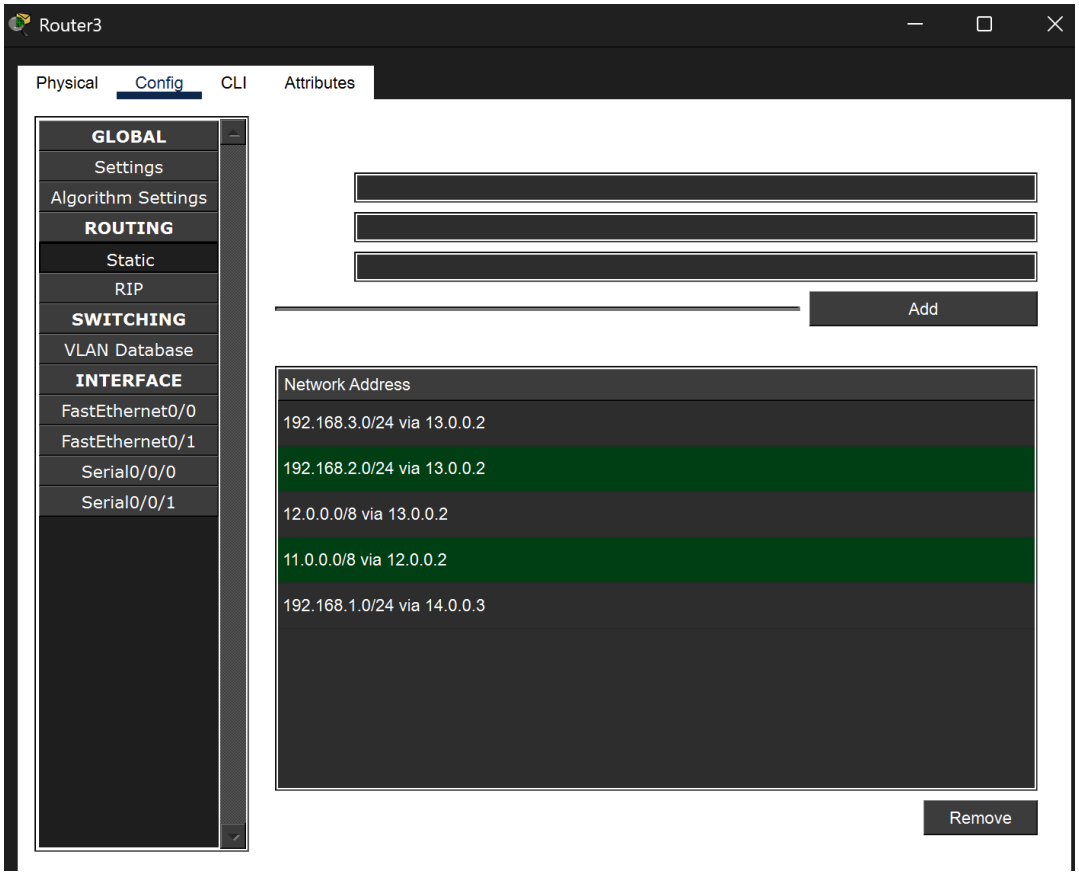



Рисунок 4.5 – Налаштування статичної маршрутизації на ротері№3

## 4.3 Динамічна маршрутизація (OSPF)

OSPF (Open Shortest Path First) працює зовсім інакше. Роутери постійно "спілкуються" між собою, обмінюючись інформацією про стан каналів (Link State).Кожен маршрутизатор знає всю карту мережі. Він обчислює найкоротший шлях за допомогою алгоритму Дейкстри. У нормальному стані трафік від Router0 до Router3 йде напряму через мережу 14.0.0.0.

Налаштування маршрутизаторів відбувалося за допомогою команд:

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#network 11.0.0.0 0.0.0.255 area 0
Router(config-router)#network 14.0.0.0 0.0.0.255 area 0
```

Рисунок 4.6 –Термінал з демонстрацією налаштування роутерів.

Ось що означає кожен крок:

1. enable

Це перехід з User EXEC mode (користувацький режим) до Privileged EXEC mode (привілейований режим).Тільки в цьому режимі можна переглядати повну конфігурацію (show run) та переходити до налаштувань. Це своєрідний «запуск від імені адміністратора».

2. configure terminal

Перехід до Global Configuration mode (режим глобальної конфігурації).Тут вводяться команди, які впливають на весь пристрій (назва роутера, паролі, запуск протоколів маршрутизації).

3. router ospf 1

Ця команда запускає сам процес маршрутизації OSPF на роутері.

- Запрошення: Змінюється на Router(config-router)#.
- Цифра «1»: Це Process ID (ідентифікатор процесу). Він має значення лише локально на цьому роутері (на сусідніх роутерах він може бути іншим, наприклад router ospf 10, і все працюватиме). Це дозволяє запускати кілька незалежних процесів OSPF на одному пристрої, якщо це потрібно.

4. Команда network (Найважливіша)

Команда network 192.168.1.0 0.0.0.255 area 0 каже роутеру дві речі:

1. Які інтерфейси задіяти: Роутер дивиться на свої IP-адреси. Якщо адреса інтерфейсу потрапляє в діапазон 192.168.1.0, він починає надсилати через нього «Hello-пакети» для пошуку сусідів.
2. Яку мережу рекламувати: Він розповідає іншим роутерам, що мережа 192.168.1.0 знаходиться за ним.

Розбір параметрів:

- 192.168.1.0: Адреса мережі, яку ми хочемо включити в OSPF.
- 0.0.0.255: Це Wildcard mask (зворотна маска).

- Вона обчислюється як 255.255.255.255 мінус ваша маска підмережі.
- Наприклад, для маски 255.255.255.0 зворотна буде 0.0.0.255. Вона вказує OSPF, на які біти адреси звертати увагу (0 — перевіряти суворо, 255 — ігнорувати).

- area 0: Номер зони. OSPF використовує зони для масштабування. Area 0 — це магістральна (backbone) зона. Усі інші зони обов'язково повинні підключатися до неї. У невеликих мережах всі роутери зазвичай знаходяться в одній зоні 0.

## 4.4 Порівння статичної та динамічної маршрутизації в разі недоступності одного з прямих маршрутів

На рисунко №4.7 зображенно відсутність звязку між маршрутизатором 0 та 3, що демонструється червоними трикутниками. В даній ситуації демонструється умовна не справність одного портів маршрутизатора.

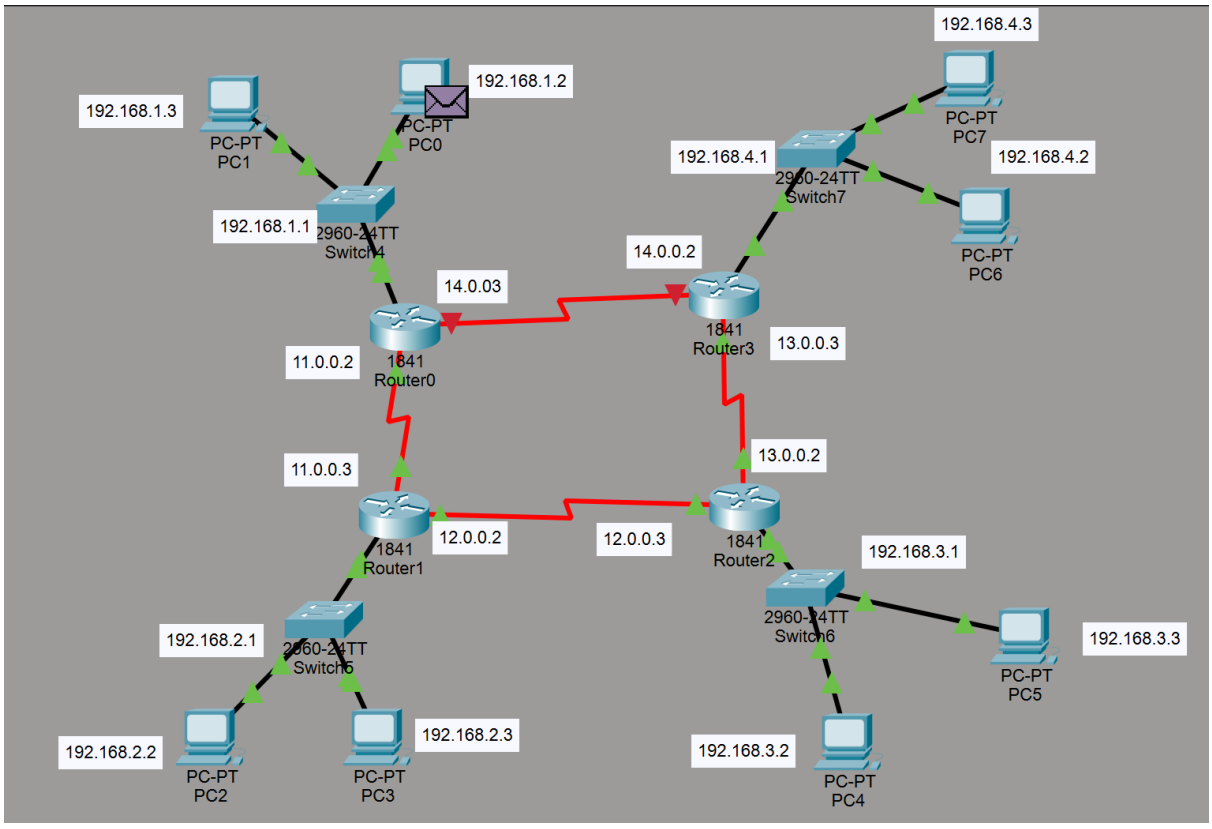



Рисунок 4.7 – Демонстраційна модель корпоративної мережі з симуляцією поломки

На рисунку №4.7 зображено мережу зі статичною маршрутизацією і спробу виконати команду ping до комп'ютера 6 з IP- адресую 192.168.4.2. Оскільки відсутній маршрут до маршрутизатора №3 то жоден пакет не дійшов.




Рисунок 4.8 – Демонстрація команди "ping"

На відмінно від мережі зі статичним адресуванням на рисунку №4.8 ми можемо побачити що всі пакети дійшли якщо порівнювати зі стандартним маршрутом. При порівняні зі штатною ситуацією можемо помітити невелику різницю в затримках пакетів оскільки пакети були автоматично перенаправленні іншим, більш довгим маршрутом, що в решті решт і привило до збільшення затримок.

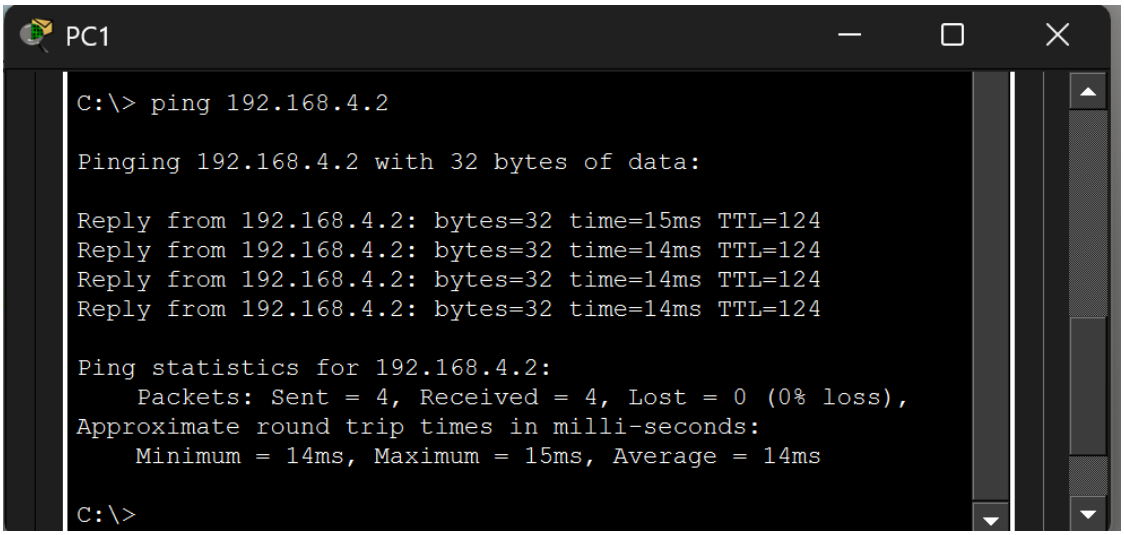



Рисунок 4.9 – Демонстрація команди "ping"

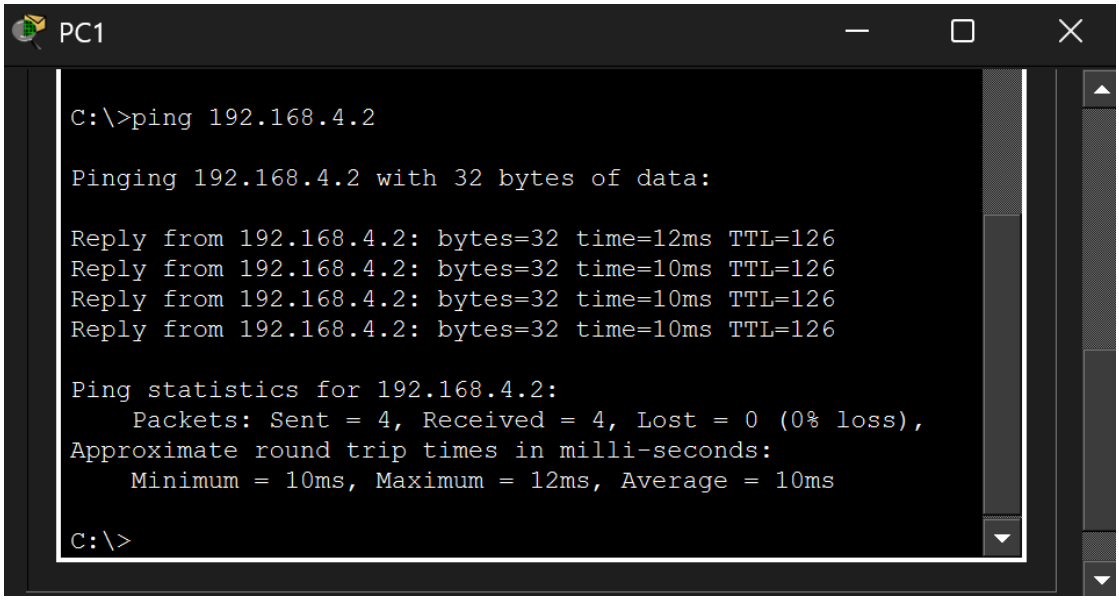



Рисунок 4.10 – Демонстрація команди “ping”

Для корпоративної мережі таких масштабів зростання затримок не є критичним на відмінну від втрати пакетних даних. Втрата до прямого доступу до одного з маршрутизаторів потребує уваги системного адміністратора та можливі затримки в робочому процесі або повна зупинка роботи. Звісно при будь-якій поломці навіть якщо вона не призвела до критичних наслідків потрібна увага системного адміністратора але при динамічній маршрутизації вирішення проблеми можна відкласти на неробочий для системи час або до планових технічних робіт найближчим часом.

## Висновки

Після детального вивчення динамічної маршрутизації, її протоколів та особливостей можна сказати, що в більшості випадків вона спроможна замінити статичну маршрутизацію. Хоча динамічна маршрутизація є більш відмовостійким рішенням для маршрутизації, що можна побачити в останньому розділі, її доцільність у корпоративних мережах малого масштабу та зі слабкою інфраструктурою є дуже сумнівною. Для корпоративних мереж великого масштабу з інфраструктурою, що має великі запаси потужності, динамічна маршрутизація стає доцільною та досить виправданою, оскільки прорахування нових маршрутів для такої мережі займе долі секунди, а проблеми, які можуть виникнути в певному вузлі, не залишать всю мережу недієздатною. Це, своєю чергою, дозволить працівникам та компаніям залишатися продуктивними в той час, як системний адміністратор знайде причину поломки та усуне її.

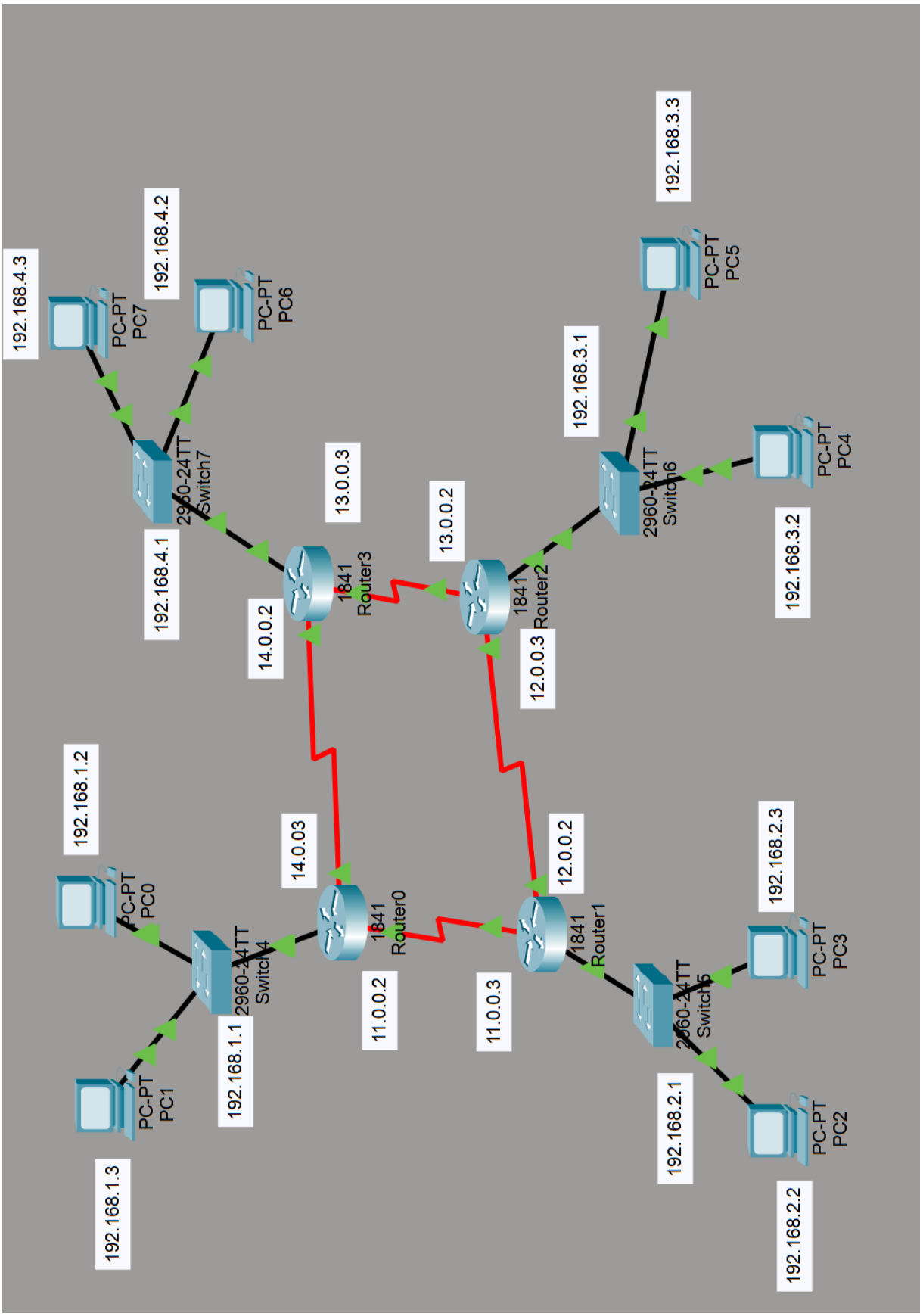
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. https://www.cisco.com Дата звернення 27.02.2026
2. https://www.cs.princeton.edu Дата звернення 28.02.2026
3. https://www.rfc-editor.org Дата звернення 28.02.2026
4. https://network-insight.net Дата звернення 02.03.2026
5. https://medium.com Дата звернення 02.03.2026
6. https://www.packetcoders.io Дата звернення 06.03.2026
7. https://www.catchpoint.com Дата звернення 07.03.2026
8. https://community.cisco.com Дата звернення 07.03.2026
9. https://networklessons.com Дата звернення 07.03.2026
10. http://courses.washington.edu Дата звернення 07.03.2026
11. https://aws.amazon.com Дата звернення 07.03.2026
12. https://networkdevicesinc.com Дата звернення 07.03.2026
13. https://www.geeksforgeeks.org Дата звернення 07.03.2026
14. https://www.fs.com Дата звернення 07.03.2026
15. https://media.techtarget.com Дата звернення 08.03.2026
16. https://networkengineering.stackexchange.com Дата звернення 08.03.2026
17. https://www.networkershome.com Дата звернення 08.03.2026
18. https://www.mdpi.com Дата звернення 12.03.2026
19. https://wehaveservers.com Дата звернення 12.03.2026
20. https://www.scribd.com Дата звернення 12.03.2026
21. https://arubanetworking.hpe.com Дата звернення 12.03.2026
22. https://techdocs.broadcom.com Дата звернення 12.03.2026
23. https://www.serverion.com Дата звернення 20.03.2026
24. https://www.researchgate.net Дата звернення 20.03.2026
25. https://labs.apnic.net Дата звернення 22.03.2026
26. https://www.ipspace.net Дата звернення 22.03.2026
27. https://www.ietf.org Дата звернення 22.03.2026
28. https://iris.gssi.it Дата звернення 22.03.2026

29.https://www.usenix.org Дата звернення 22.03.2026
30.https://oneuptime.com Дата звернення 24.03.2026

Додаток А

Приклад фізичної топології мережі



**ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ**

(Презентація)

ДУІКТ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**



**Навчально-науковий інститут Інформаційних технологій**
**Кафедра Комп'ютерної інженерії**

**КВАЛІФІКАЦІЙНА РОБОТА**
**НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА**

**на тему: «**Відмовостійкі корпоративні мережі з використанням протоколів динамічної маршрутизації**»**

Виконав студент групи КІД-42
Бова Юрій Володимирович
Керівник кваліфікаційної роботи: Соколов Кирило Анатолієвич PhD

**Київ – 2026**

***Мета роботи*** –Дослідити різницю між статичною та динамічною маршрутизацією в межах корпоративних мереж, та перевірка корпоративної мережі на її відмово стійкість

- ***Об'єкт дослідження*** – Корпоративна комп'ютерна мережа з динамічною та статичною маршрутизацією
- ***Предмет дослідження*** – Комп'ютерна мережа

## Актуальність теми.

У сучасному цифровому світі безперервність бізнес-процесів критично залежить від стабільності та доступності мережевої інфраструктури. Корпоративні мережі перетворилися на складні гетерогенні системи, де будь-яка затримка або втрата зв'язку може призвести до значних фінансових збитків. Традиційні методи статичної маршрутизації, хоча і забезпечують високу передбачуваність, виявляються неефективними у великих динамічних інфраструктурах через складність масштабування та відсутність автоматичної адаптації до збоїв.



## Архітектура та еволюція протоколів динамічної маршрутизації в сучасних гетерогенних мережах

Динамічна маршрутизація представляє собою критично важливий механізм функціонування комп'ютерних мереж, який забезпечує автоматичну адаптацію маршрутизаторів до змін топології та умов передачі даних. На відміну від статичної маршрутизації, де кожен шлях програмується вручну адміністратором, динамічні протоколи дозволяють пристроям самостійно виявляти мережі, обмінюватися інформацією про доступність вузлів та обчислювати оптимальні маршрути за допомогою спеціалізованих алгоритмів. Ця здатність до самоорганізації стає фундаментальною умовою масштабованості та відмовостійкості сучасних корпоративних мереж, інфраструктур постачальників послуг та глобального інтернету. Фундаментальні концепції та класифікація систем маршрутизації. Протоколи динамічної маршрутизації класифікуються на основі їхнього призначення, алгоритмічної бази та способу обробки адресної інформації.

# Статична проти динамічної маршрутизації: Технічний компроміс

Хоча динамічна маршрутизація пропонує автоматизацію, статичні маршрути залишаються актуальними для специфічних сценаріїв, таких як тупикові мережі або канали з обмеженою пропускною здатністю. Статична маршрутизація вимагає менше обчислювальних ресурсів та забезпечує вищий рівень передбачуваності, проте стає некерованою у великих інфраструктурах.

Таблиця 1 – порівння характеристики статичної та динамічної маршрутизації

| Характеристика | Статична маршрутизація | Динамічна маршрутизація |
|---|---|---|
| Масштабованість | Низька; складність зростає з кожним вузлом | Висока; автоматичне виявлення сусіда |
| Використання ресурсів CPU | Мінімальне | Потребує значної пам'яті та ресурсів CPU |
| Адаптація до збоїв | Відсутня (ручне втручання) | Автоматичне перерахування шляхів |
| Передбачуваність | Повна; маршрут не змінюється | Залежить від метрик та стану лінків |
| Сфера застосування | Малі стабільні мережі | Великі, динамічні інфраструктури |



# Протокол OSPF: Промисловий стандарт ієрархічних мереж

Open Shortest Path First (OSPF) є найбільш розповсюдженим внутрішнім протоколом у корпоративному секторі. Він був створений IETF як відкрита альтернатива пропрієтарним рішенням для подолання обмежень RIP. Ієрархічна структура та типи областей. OSPF забезпечує масштабованість через розділення мережі на області (Areas). Це дозволяє обмежити розповсюдження LSA лише певною частиною мережі, зменшуючи навантаження на пам'ять та процесор маршрутизаторів. Центральною є магістральна область (Area 0), до якої повинні бути підключені всі інші області для забезпечення міжобласного зв'язку.

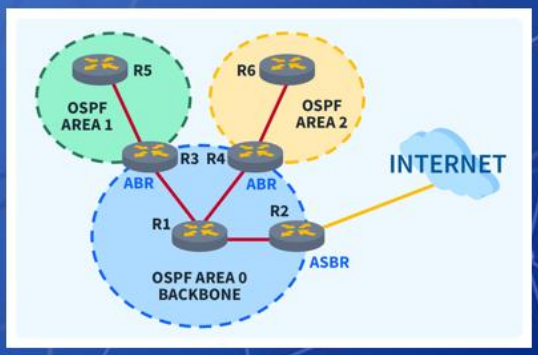



Рисунок 2 –Зображення Мережевих областей(Areas)

# Порівняльний аналіз протоколів динамічної маршрутизації в архітектурах високої доступності корпоративних мереж

Сучасна парадигма побудови корпоративних мереж висуває безпрецедентні вимоги до надійності та швидкодії інфраструктури передачі даних. У системі, де критичні бізнес-процеси залежать від постійного доступу до хмарних сервісів, розподілених баз даних та систем реального часу, поняття відмовостійкості (High Availability) стає визначальним фактором проектування. Динамічна маршрутизація відіграє роль "центральної нервової системи" мережі, забезпечуючи інтелектуальний перерозподіл трафіку при виникненні апаратних або лінійних збоїв. Проте вибір конкретного протоколу — OSPF, EIGRP, BGP або IS-IS — не може бути випадковим, оскільки кожен із них базується на різних математичних алгоритмах та механізмах обробки подій, що безпосередньо впливає на час відновлення працездатності мережі та її загальну стаійкість.



# Порівняння OSPF та EIGRP у контексті швидкості конвергенції та відмово стійкості

Центральною проблемою при виборі внутрішнього протоколу шлюзу (IGP) є швидкість конвергенції — інтервал часу, протягом якого всі маршрутизатори в межах домену маршрутизації узгоджують нову топологію після зміни стану будь-якого сегмента. У цьому контексті протистояння OSPF (Open Shortest Path First) та EIGRP (Enhanced Interior Gateway Routing Protocol) представляє два принципово різні підходи до обробки інформації про стан мережі.

Таблиця 2 – Порівнння EIGRP та OSPF

| Параметр порівняння | EIGRP | OSPF |
|---|---|---|
| Алгоритм | DUAL (дифузні оновлення) | SPF (алгоритм Дейкстри) |
| Тип протоколу | Гібридний (Advance Distance Vector) | Link-State (стан зв'язків) |
| Швидкість конвергенції | Мілісекунди (при наявності FS) | Секунди (за замовчуванням) |
| Резервування | Feasible Successors (вбудовано) | LFA (потребує налаштування) |
| Використання ресурсів | Низьке (тільки зміни) | Високе (повний SPF при кожній зміні) |
| Метрика | Складена (BW, Delay, Load, Reliability) | Вартість (залежить від BW) |
| Масштабування | Плоска або ієрархічна структура | Обов'язкова ієрархія (Areas) |

# Стратегії BGP Multihoming для забезпечення високої доступності на межі мережі

У корпоративних середовищах вихід у мережу Інтернет часто є критичною точкою відмови. Використання одного інтернет-провайдера (ISP) створює ризики, пов'язані не лише з обривом фізичного кабелю, а й з внутрішніми проблемами в мережі самого ISP. Рішенням є BGP Multihoming — підключення до двох або більше автономних систем.Архітектура iBGP та eBGP у Multihoming-сценаріях

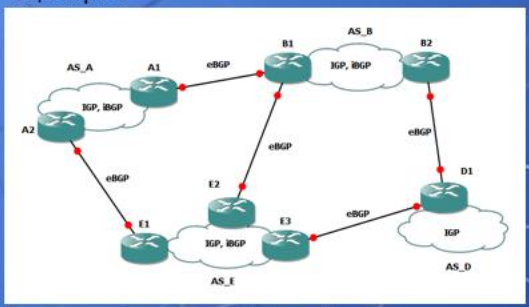



Рисунок 2 – BGP Multihoming

Для побудови надійного підключення корпоративна мережа зазвичай використовує eBGP (External BGP) для взаємодії з кожним провайдером та iBGP (Internal BGP) для синхронізації маршрутної інформації між власними межовими маршрутизаторами. Важливою вимогою є використання Loopback-інтерфейсів для встановлення сесій iBGP. Це гарантує, що BGP-сесія між внутрішніми маршрутизаторами не впаде при відмові одного з фізичних інтерфейсів, якщо існує альтернативний шлях усередині мережі.



# Гібридні дизайни: IGP та BGP в ієрархії

Для великих корпорацій оптимальним вважається використання IS-IS або OSPF усередині мережі (як транспорт для Loopback-адрес та інфраструктури) та iBGP для передачі клієнтських або сервісних префіксів. Це дозволяє IGP залишатися компактним і швидким, фокусуючись лише на топології, тоді як BGP бере на себе навантаження з управління величезною кількістю маршрутів та політиками безпеки. У хмарних та віртуалізованих середовищах (наприклад, VMware NSX-T) BGP часто є основним протоколом навіть усередині мережі через його здатність підтримувати ECMP (Equal-Cost Multi-Path) на багатьох рівнях та гнучкість у роботі з кількома зонами доступності (Multi-AZ).

Таблиця 3 – Особливості протоколів та сфера застосування

| Технологія | Вплив на відмовостійкість | Рекомендована сфера застосування |
|---|---|---|
| BFD | Субсекундне виявлення збоїв | Всі критичні інтерфейси між маршрутизаторами |
| LFA (FRR) | Негайне перемикання на резерв | Мережі реального часу (VoIP, відео) |
| Graceful Restart | Збереження трафіку при рестарті процесу | Планове обслуговування ядра мережі |
| Summarization | Обмеження поширення нестабільності | Межі зон (ABR) або рівнів (L1/L2) |

# Архітектура та механізми швидкої збіжності в сучасних IP-мережах

Поняття збіжності в сучасних телекомунікаційних системах визначає здатність мережі адаптуватися до змін топології, забезпечуючи безперервність передачі даних навіть за умов критичних відмов окремих компонентів. Збіжність є розподіленим процесом, у ході якого всі маршрутизатори приходять до єдиного узгодженого бачення оптимальних шляхів після виникнення події, що змінює доступність ресурсів. У контексті сучасних вимог до якості обслуговування (QoS) та угод про рівень послуг (SLA), стандартні механізми протоколів маршрутизації, розроблені в епоху мереж «найкращих зусиль» (best-effort), виявляються недостатніми. Необхідність підтримки критичних додатків, таких як Voice over IP (VoIP), фінансові транзакції в реальному часі та мультимедійне мовлення, трансформувала цільові показники збіжності з десятисекундних інтервалів до мілісекунд.



# Порівняння статичної маршрутизації та динамічної в середовищі Cisco Packet Tracer

Ця топологія, створена у Cisco Packet Tracer, є моделью для демонстрації принципів побудови мереж середнього масштабу. Вона має кільцеву структуру (mesh), що є ідеальним майданчиком для порівняння статична маршрутизація та динамічний протокол (OSPF).
Мережа складається з чотирьох сегментів, кожен з яких має свій маршрутизатор (Router 1841), комутатор та кінцеві пристрої (ПК):
Локальні мережі (LAN): Кожен маршрутизатор обслуговує свою підмережу класу C (192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0)
Магістральні канали (WAN): Маршрутизатори з'єднані між собою послідовними Serial, що утворюють замкнений контур.
Використовуються підмережі 11.0.0.0, 12.0.0.0, 13.0.0.0 та 14.0.0.0

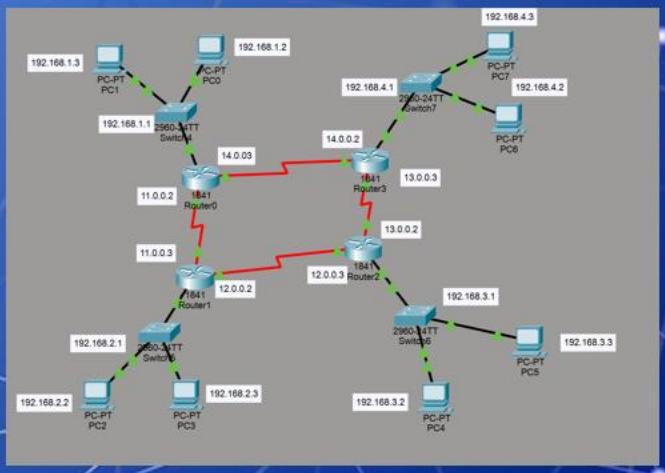



Рисунок 3 – Демонстраційна модель корпоративної мережі

# Порівння статичної та динамічної маршрутизації в разі недоступності одного з прямих маршрутів

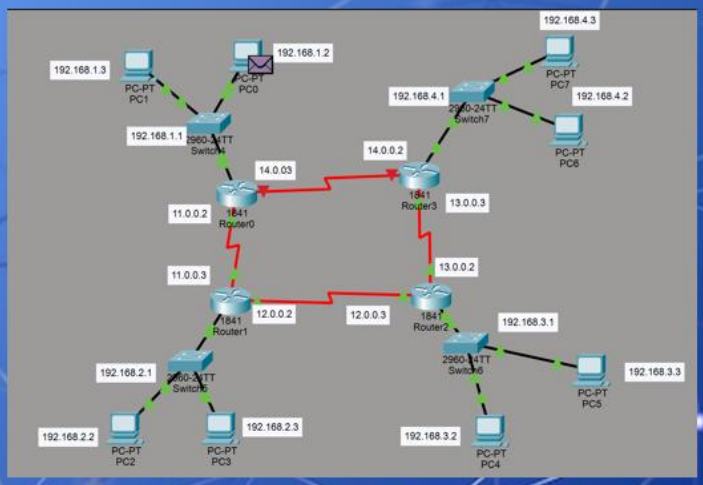



Рисунок 4 – Демонстраційна модель корпоративної мережі з симуляцією поломки



# Демонстрація команди “ping” за відсутності несправностей

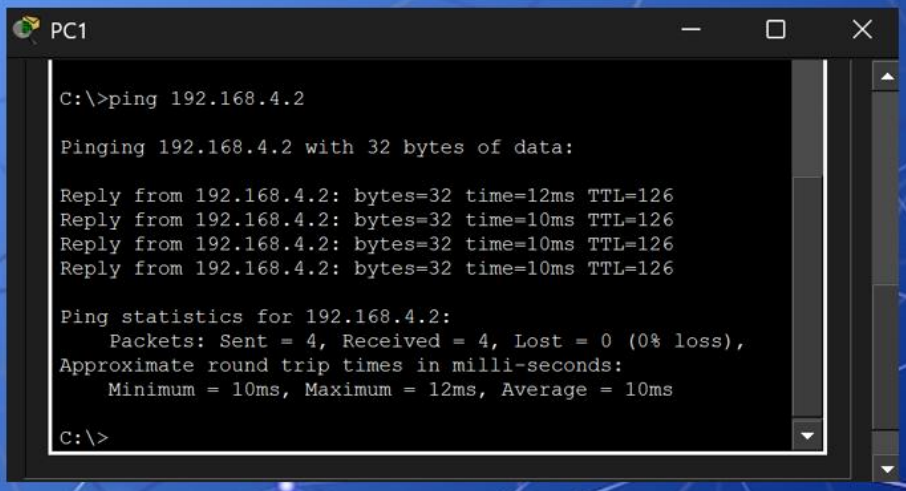



Рисунок 5 – Демонстрація команди “ping”

# Статична маршрутизація та перевірка доступності

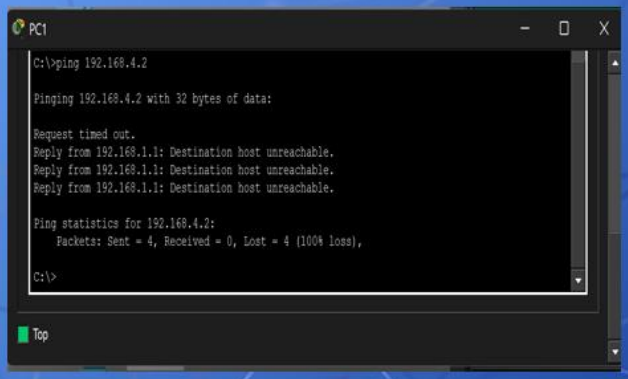



Рисунок 6 – Демонстрація команди "ping"

Зображено мережу зі статичною маршрутизацією і спробу виконати команду ping до комп'ютера 6 з IP-адресою 192.168.4.2. Оскільки відсутній маршрут до маршрутизатора №3 то жоден пакет не дійшов.



# Динамічна маршрутизація та перевірка доступності

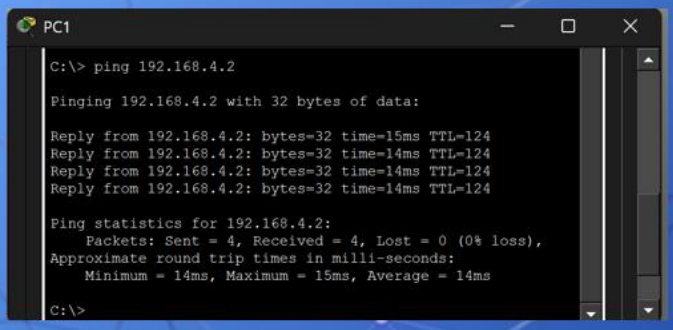



Рисунок 7 – Демонстрація команди "ping"

На відмінно від мережі зі статичним адресуванням на зображенні ми можемо побачити що всі пакети дійшли якщо порівнювати зі стандартним маршрутом. При порівняні зі штатною ситуацією можемо помітити невелику різницю в затримках пакетів оскільки пакети були автоматично перенаправленні іншим, більш довгим маршрутом, що в решті решт і привило до збільшення затримок.

# Висновки

Після детального вивчення динамічної маршрутизації, її протоколів та особливостей можна сказати, що в більшості випадків вона спроможна замінити статичну маршрутизацію. Хоча динамічна маршрутизація є більш відмовостійким рішенням для маршрутизації, що можна побачити в останньому розділі, її доцільність у корпоративних мережах малого масштабу та зі слабкою інфраструктурою є дуже сумнівною. Для корпоративних мереж великого масштабу з інфраструктурою, що має великі запаси потужності, динамічна маршрутизація стає доцільною та досить виправданою, оскільки прорахування нових маршрутів для такої мережі займе долі секунди, а проблеми, які можуть виникнути в певному вузлі, не залишать всю мережу недієздатною. Це, своєю чергою, дозволить працівникам та компаніям залишатися продуктивними в той час, як системний адміністратор знайде причину поломки та усуне її.