

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»**

Навчально-науковий інститут телекомунікаційних систем

Кафедра електронних комунікацій та інтернету речей

«На правах рукопису»
УДК 621.391

До захисту допущено:
ВО завідувача кафедри
_____ Галина СОЗОННИК
«__» _____ 20__ р.

Магістерська дисертація

на здобуття ступеня магістра

**за освітньо-професійною програмою «Системи електронних комунікацій
та Інтернету речей»**

зі спеціальності 172 «Телекомунікації та радіотехніка»

**на тему: «Порівняльний аналіз протоколів маршрутизації OSPF і EIGRP
для використання в корпоративних IP-мережах»**

Виконав (-ла):

студент (-ка) II курсу, групи ТС-21мп
Коваль Олег Сергійович _____

Науковий керівник:

ст. викладач кафедри ЕКІР, к. т. н.
Новіков Валерій Іванович _____

Рецензент:

Професор кафедри ТК, д.т.н., професор
Лисенко Олександр Іванович _____

Засвідчую, що у цій магістерській
дисертації немає запозичень з праць
інших авторів без відповідних посилань.
Студент (-ка) _____

Київ – 2024 року

**Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий інститут телекомунікаційних систем
Кафедра електронних комунікацій та інтернету речей**

Рівень вищої освіти – другий (магістерський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Системи електронних комунікацій та Інтернету речей»

ЗАТВЕРДЖУЮ

ВО завідувача кафедри

_____ Галина СОЗОННИК

«___» _____ 20__ р.

**ЗАВДАННЯ
на магістерську дисертацію студенту**

Ковалю Олегу Сергійовичу

1. Тема дисертації «Порівняльний аналіз протоколів маршрутизації OSPF і EIGRP для використання в корпоративних IP-мережах», науковий керівник дисертації Новіков Валерій Іванович, ст.викладач, ктн , затверджені наказом по університету від «___» _____ 20__ р. № _____

2. Термін подання студентом дисертації _____

3. Об'єкт дослідження: Протоколи внутрішньої маршрутизації OSPF та EIGRP

4. Вихідні дані: Покроковий план написання магістерської дисертації

5. Перелік завдань, які потрібно розробити: дослідити основні поняття та принципи внутрішньої маршрутизації; здійснити загальний огляд протоколів внутрішньої маршрутизації; дослідити загальний принцип роботи протоколу OSPF; провести аналіз протоколу OSPF для кількох областей; розглянути процес налаштування протоколу OSPF в IP-мережах; проаналізувати характеристики та функції протоколу EIGRP; розглянути процес налаштування протоколу EIGRP; проаналізувати переваги й недоліки використання EIGR в корпоративних IP мережах; визначити методологію проведення дослідження мережі; провести експерименти і проаналізувати отримані дані.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу: презентація Power Point (10 слайдів)

7. Дата видачі завдання 10.10.2022

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Аналіз літературних джерел по тематиці роботи	10.10.2022р - 31.10.2022р	
2	Формулювання теми, мети, об'єкту та предмету дослідження у магістерській роботі	07.11.2022р – 21.11.2022р	
3	Формулювання проблематики та визначення актуальності магістерської роботи. Зв'язок тематики магістерської роботи із сучасними інноваційними трендами в інформаційному середовищі	23.11.2022р – 26.12.2022р	
4	Формування структури магістерської роботи	23.01.2023р-06.03.2023р	
5	Формування вступної частини та наповнення теоричної частини	20.03.2023р-20.04.2023р	
6	Проведення досліджень для вирішення наукових завдань	19.06.2023р– 26.07.2023р	
7	Формування кінцевої структури магістерської роботи	25.09.2023р-03.11.2023р	
8	Формування кінцевих висновків та списку використаних літературних джерел	06.11.2023р-20.11.2023р	
9	Підготовка до захисту дипломної роботи	01.12.2023р-14.01.2024р	

Студент

Олег КОВАЛЬ

Науковий керівник

Валерій НОВІКОВ

РЕФЕРАТ

Темою магістерської дисертації є порівняльний аналіз протоколів маршрутизації OSPF і EIGRP для використання в корпоративних IP-мережах.

Робота містить 107 сторінок, 34 ілюстрації, 16 таблиць, 18 джерел інформації.

Актуальність теми обумовлена необхідністю вибору протоколу маршрутизації, зокрема між OSPF і EIGRP, що визначається необхідністю забезпечення ефективності та безпеки корпоративних IP-мереж в умовах зростання обсягу даних, великої кількості підключених пристроїв і постійної потреби у високій доступності. Це вимагає ретельного порівняльного аналізу, оскільки вибір протоколу може суттєво впливати на продуктивність мережі.

Метою даної магістерської роботи є проведення порівняльного аналізу протоколів маршрутизації OSPF і EIGRP, а також проведення дослідження для визначення їхньої ефективності та оптимального використання в корпоративних IP-мережах.

Відповідно до мети поставлено наступні завдання:

- дослідити основні поняття та принципи внутрішньої маршрутизації;
- здійснити загальний огляд протоколів внутрішньої маршрутизації;
- дослідити загальний принцип роботи протоколу OSPF;
- провести аналіз протоколу OSPF для кількох областей;
- розглянути процес налаштування протоколу OSPF в IP-мережах;
- проаналізувати характеристики та функції протоколу EIGRP;
- розглянути процес налаштування протоколу EIGRP;
- проаналізувати переваги й недоліки використання EIGR в корпоративних IP мережах;
- визначити методологію проведення дослідження мережі;
- Провести експерименти і проаналізувати отримані дані.

Об'єкт дослідження: протоколи внутрішньої маршрутизації OSPF та EIGRP.

Предмет дослідження: ефективність використання протоколів OSPF та EIGRP в корпоративних IP-мережах із різними топологіями.

Методи дослідження. Для вирішення поставлених у роботі завдань використано загальноприйняті методи наукового пізнання та дослідження, зокрема: емпіричний (використання програмного забезпечення Cisco Packet Tracer для моделювання та імітації роботи корпоративної IP-мережі з протоколами OSPF і EIGRP), експериментальний (проведення тестових випробувань та вимірювань продуктивності для аналізу реальної ефективності протоколів маршрутизації в різних топологіях), моделювання (використання технік моделювання для створення абстрактної репрезентації досліджуваної мережі для подальшого аналізу та експериментів), статистичний (обробка та аналіз отриманих статистичних даних щодо продуктивності, затримок, часу конвергенції тощо), кількісний (розрахунок та порівняння метрик, вартостей, та інших кількісних параметрів для оцінки ефективності протоколів), системний аналіз (комплексний підхід до вивчення взаємодії елементів системи мережі з метою визначення її ефективності та найкращих практик використання протоколів маршрутизації).

Наукова новизна даної роботи полягає в системному підході до вирішення проблем, тобто дослідження аспектів ефективності протоколів в контексті різних мережевих топологій, що дозволяє зробити обґрунтовані висновки та рекомендації для вибору оптимального протоколу маршрутизації в конкретній корпоративній мережі. Цей підхід надає можливість не лише вивчати окремі аспекти протоколів, а й розглядати їх в контексті конкретних сценаріїв корпоративних мереж.

Практичне значення одержаних результатів. Проведене дослідження важливе для мережних адміністраторів, проєктувальників інфраструктури та всіх, хто відповідає за ефективність та стійкість корпоративних IP-мереж. Висновки дослідження можуть слугувати важливим підґрунтям для прийняття рішень щодо вибору протоколу маршрутизації в конкретних корпоративних середовищах.

Ключові слова: ПРОТОКОЛИ МАРШРУТИЗАЦІЇ, OSPF, EIGRP,
КОРПОРАТИВНІ ІР-МЕРЕЖІ

ABSTRACT

The topic of the master's thesis is a comparative analysis of OSPF and EIGRP routing protocols for use in corporate IP networks.

The work comprises 107 pages, 34 illustrations, 16 tables, and 31 sources of information.

The relevance of the topic arises from the need to choose a routing protocol, specifically between OSPF and EIGRP. This choice is driven by the imperative to ensure the efficiency and security of corporate IP networks in the face of growing data volumes, a large number of connected devices, and the constant need for high availability. This necessitates careful benchmarking, as the choice of protocol can significantly impact network performance.

The purpose of this master's thesis is to conduct a comparative analysis of the OSPF and EIGRP routing protocols and to perform research to determine their effectiveness and optimal use in corporate IP networks. In accordance with this purpose, the following tasks were set:

- Explore the basic concepts and principles of internal routing.
- Perform a general review of internal routing protocols.
- Investigate the general principle of operation of the OSPF protocol.
- Analyze the OSPF protocol for several areas.
- Consider the OSPF protocol configuration process in IP networks.
- Analyze the characteristics and functions of the EIGRP protocol.
- Consider the EIGRP protocol configuration process.
- Analyze the advantages and disadvantages of using EIGRP in corporate IP networks.
- Determine the methodology of network research.
- Conduct experiments and analyze the obtained data.

Study object: Internal routing protocols OSPF and EIGRP.

Study subject: The effectiveness of using OSPF and EIGRP protocols in corporate IP networks with different topologies.

Research methods: To solve the tasks outlined in the work, generally accepted methods of scientific knowledge and research were used, including empirical (using Cisco Packet Tracer software to model and simulate the operation of a corporate IP network with OSPF and EIGRP protocols), experimental (conducting test trials and performance measurements to analyze the real efficiency of routing protocols in different topologies), modeling (using modeling techniques to create an abstract representation of the investigated network for further analysis and experiments), statistical (processing and analyzing obtained statistical data on performance, delays, convergence time, etc.), quantitative (calculating and comparing metrics, values, and other quantitative parameters for evaluating the effectiveness of protocols), and system analysis (a comprehensive approach to studying the interaction of network system elements to determine its effectiveness and best practices for using routing protocols).

The scientific novelty of this work consists of a systematic approach to solving problems, i.e. researching the aspects of the effectiveness of protocols in the context of different network topologies, which allows you to draw reasonable conclusions and recommendations for choosing the optimal routing protocol in a specific corporate network. This approach provides an opportunity not only to study individual aspects of protocols, but also to consider them in the context of specific scenarios of corporate networks.

Practical significance of the obtained results. The research is important for network administrators, infrastructure designers, and anyone responsible for the efficiency and resilience of enterprise IP networks. The research findings can serve as an important basis for making decisions about the choice of routing protocol in specific corporate environments.

Keywords: ROUTING PROTOCOLS, OSPF, EIGRP, CORPORATE IP NETWORKS.

Зміст

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ	10
ВСТУП.....	12
1 ОГЛЯД ПРОТОКОЛІВ ВНУТРІШНЬОЇ МАРШРУТИЗАЦІЇ В IP-МЕРЕЖАХ	14
1.1 Основні поняття та принципи внутрішньої маршрутизації	14
1.2 Загальний огляд протоколів внутрішньої маршрутизації	21
1.3 Висновки з розділу 1	34
2 АНАЛІЗ ПРОТОКОЛУ ВНУТРІШНЬОЇ МАРШРУТИЗАЦІЇ OSPF В IP-МЕРЕЖАХ.....	36
2.1 Принцип роботи протоколу OSPF	36
2.2 Аналіз протоколу OSPF для кількох областей	52
2.3 Базові налаштування OSPF на маршрутизаторах Cisco	58
2.4 Висновки з розділу 2	61
3 АНАЛІЗ ПРОТОКОЛУ ВНУТРІШНЬОЇ МАРШРУТИЗАЦІЇ EIGRP В IP-МЕРЕЖАХ.....	64
3.1 Характеристики та функції протоколу EIGRP	64
3.2 Налаштування протоколу EIGRP на маршрутизаторах Cisco	75
3.3 Переваги й недоліки використання EIGR в корпоративних IP мережах	81
3.4 Висновки з розділу 3	82
4 ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ OSPF І EIGRP ДЛЯ ВИКОРИСТАННЯ В КОРПОРАТИВНИХ IP-МЕРЕЖАХ.....	85
4.1 Методологія проведення дослідження.....	85
4.2 Проведення експериментів і аналіз отриманих даних	90
4.3 Висновки з розділу 4.....	103
ВИСНОВКИ.....	104
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	106

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

ABR	Area Border Router – Граничний маршрутизатор області
AD	Administrative Distance – Адміністративна відстань
ASBR	Autonomous System Boundary Router - Граничний маршрутизатор автономної системи
BDR	Backup Designated Router – Резервний призначений маршрутизатор
BGP	Border Gateway Protocol – Протокол граничного шлюзу
CIDR	Classless Inter-Domain Routing – Безкласова міждоменна маршрутизація
DBD	Database Descriptor – Дескриптор бази даних
DR	Designated router – Призначений маршрутизатор
DUAL	Diffusing Update Algorithm – Алгоритм дифузного оновлення
EGP	Exterior Gateway Protocol – Протокол зовнішнього шлюзу
EIGRP	Enhanced Interior Gateway Routing Protocol – Удосконалений протокол маршрутизації внутрішнього шлюзу
FD	Feasible Distance – Допустима відстань
ICMP	Internet Router Discovery Protocol – Протокол виявлення маршрутизатора в Інтернеті
IGP	Interior Gateway Routing Protocol – Протокол внутрішнього шлюзу
IGRP	Interior Gateway Routing Protocol – Протокол маршрутизації внутрішнього шлюзу
IS-IS	Intermediate System to Intermediate System – Проміжна система до проміжної системи
LSA	Link-State Advertisement – Об’ява про стан каналу
LSDB	Link State Database – База даних стану каналу
LSR	Label Switch Router – Маршрутизатор з перемикачем міток
LSU	Link State Update – Оновлення стану каналу
OSI	Open Systems Interconnection – Взаємозв’язок відкритих систем
OSPF	Open Shortest Path First – Першочергове виявлення найкоротших маршрутів

RD	Reported Distance – Заявлена відстань
RIP	Routing Information Protocol – Протокол маршрутної інформації
RTP	Real-time Transport Protocol – Транспортний протокол реального часу
SPF	Shortest Path First – Першочергове знаходження найкоротшого шляху
VLSM	Variable Length Subnet Mask – Маска підмережі зі змінною довжиною

ВСТУП

У сучасному світі, де інформаційні технології стали необхідною складовою успішного функціонування корпорацій та підприємств, комп'ютерні мережі стають визначальним елементом для обміну даними та забезпечення надійного зв'язку. Вибір оптимального протоколу маршрутизації для корпоративних IP-мереж впливає не лише на ефективність роботи інформаційно-комунікаційної інфраструктури, але й на конкурентоспроможність бізнесу. В цьому контексті дослідження ефективності протоколів OSPF та EIGRP має велике значення.

OSPF (Open Shortest Path First) та EIGRP (Enhanced Interior Gateway Routing Protocol) являють собою два основні протоколи маршрутизації, що широко використовуються в корпоративних мережах. Обидва протоколи дозволяють маршрутизаторам визначати найоптимальніший шлях для пересилання даних у мережі, проте вони мають свої особливості та властивості, які варто ретельно розглянути.

В даній магістерській дисертації буде проведено порівняльний аналіз протоколів OSPF та EIGRP для визначення їхньої ефективності в корпоративних IP-мережах. З урахуванням специфіки роботи корпорацій та підприємств, де важлива надійність, швидкість та оптимізація трафіку, важливо визначити, який саме протокол краще відповідатиме потребам конкретної компанії.

У ході дослідження буде здійснено моделювання корпоративної IP-мережі з використанням програмного забезпечення Cisco Packet Tracer. Будуть розглянуті різні мережеві топології, зокрема кільцева та сітчаста, для оцінки роботи протоколів у різних умовах. Важливим етапом дослідження є визначення часу конвергенції, який впливає на швидкість відновлення мережі після змін у топології.

Однією з ключових відмінностей між OSPF та EIGRP є їхня архітектура. OSPF базується на принципах стану каналу, де маршрутизатори обмінюються інформацією про стан кожного з'єднання. З іншого боку, EIGRP використовує

концепцію векторів відстані та адаптивної маршрутизації, що дозволяє швидше реагувати на зміни у мережі.

Розглядаючи ефективність протоколів, буде вивчено величину затримки у різних топологіях мережі, розраховано середній час конвергенції та визначено загальну завантаженість мережі. Це дозволить отримати повний обсяг інформації про роботу кожного протоколу в реальних умовах експлуатації.

Також будуть обґрунтовані рекомендації щодо вибору протоколу маршрутизації в залежності від конкретних вимог та потреб корпоративної IP-мережі. Це дозволить впроваджувати оптимальні технології та підвищувати загальну ефективність інформаційно-комунікаційних систем підприємств. Такий підхід має велике значення для сучасних бізнес-структур, які прагнуть до найкращих показників у сфері мережевого адміністрування та оптимізації трафіку.

1 ОГЛЯД ПРОТОКОЛІВ ВНУТРІШНЬОЇ МАРШРУТИЗАЦІЇ В IP-МЕРЕЖАХ

1.1 Основні поняття та принципи внутрішньої маршрутизації

Роль маршрутизації в функціонуванні корпоративних комп'ютерних мереж є надзвичайно важливою. Маршрутизатори виконують функцію визначення оптимальних шляхів передачі даних між різними сегментами мережі, забезпечують ефективність та стійкість зв'язку. Ці пристрої функціонують на третьому (мережевому) рівні моделі OSI. Маршрутизація дозволяє ефективно керувати трафіком, забезпечує швидку і надійну передачу інформації в середовищі корпоративного використання. Розглянемо більш детально її основні принципи.

Маршрутизація – це процес, за якого маршрутизатор отримує IP-пакет через один інтерфейс та визначає, яким інтерфейсом використовувати для пересилання пакета до його призначення. Цей інтерфейс може бути кінцевою точкою маршруту або мережею, з'єднаною з іншим маршрутизатором, що використовується для досягнення мережі призначення.

Маршрутизатор виконує дві основні функції:

- Визначає найкращий шлях для пересилання пакетів на основі інформації, яка міститься в таблиці маршрутизації;
- Пересилає пакети до місця призначення.

Для знаходження оптимального шляху пересилання пакетів – маршрутизатор використовує свою таблицю маршрутизації. При отриманні пакета маршрутизатор перевіряє адресу призначення та скористовується таблицею маршрутизації для знаходження найбільш ефективного маршруту до відповідної мережі. Також, у таблиці маршрутизації враховується, який інтерфейс слід використовувати для пересилання пакетів у кожному відому мережу. Після визначення оптимального маршруту маршрутизатор інкапсулює пакет у кадр вихідного або вхідного інтерфейсу та відправляє його до пункту призначення.

Маршрутизатор може отримувати пакет, що вкладений у кадр каналу передачі даних одного типу, та пересилати цей пакет через інтерфейс, який

використовує інший тип кадру даних. Наприклад, маршрутизатор може прийняти пакет через інтерфейс Ethernet, але передати його через інтерфейс, налаштований з використанням протоколу «точка-точка» (PPP). Інкапсуляція каналу передачі даних залежить від типу інтерфейсу маршрутизатора і типу середовища, до якого він підключений. Різні технології каналів передачі даних, до яких може підключитися маршрутизатор, включають PPP, Ethernet, DSL, Frame Relay, бездротові (наприклад, Bluetooth, 802.11) і кабельні мережі.

Розглянемо способи, якими маршрутизатор може отримати дані до таблиці маршрутизації. Для наочності використаємо маршрутизатор R1 (рис. 1.1). Всі мережі IPv4 і IPv6, які виділені жовтим кольором, є безпосередньо під'єднаними до нього мережами. Мережі IPv4 і IPv6, що виділені синім кольором, є віддаленими мережами.

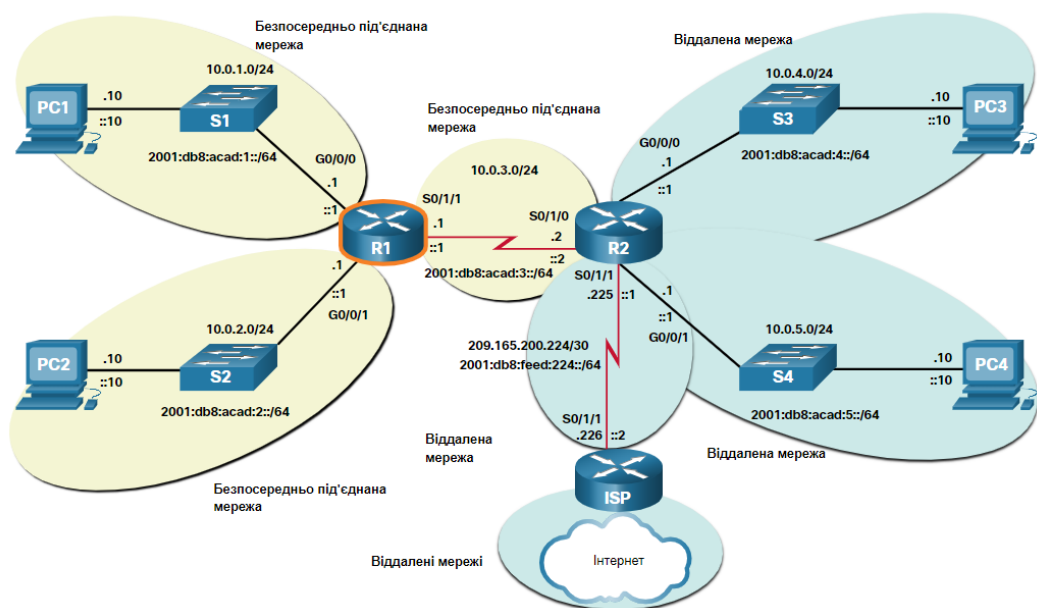


Рисунок 1.1 – Мережі з позиції маршрутизатора R1 [1]

Способи отримання даних маршрутизатором

1) Безпосередньо під'єднані мережі – це мережі, які налаштовані на активних інтерфейсах маршрутизатора. Безпосередньо під'єднана мережа додається в таблицю маршрутизації, коли на інтерфейсі налаштована IP-адреса і маска підмережі (довжина префікса) і він активований (стан up).

2) Віддалені мережі – це мережі, що безпосередньо не під'єднані до маршрутизатора. Маршрутизатор може дізнатися про віддалені мережі в один з двох способів:

- статичні маршрути – додаються до таблиці маршрутизації при ручному налаштуванні маршруту;
- протоколи динамічної маршрутизації – додаються до таблиці маршрутизації, коли протоколи маршрутизації динамічно дізнаються про віддалену мережу. При отриманні інформації про зміну мережевої топології протокол маршрутизації автоматично оновлює маршрути.

3) Маршрут за замовчуванням. Він визначає маршрутизатор наступного переходу, який буде використовуватися, якщо таблиця маршрутизації не містить визначеного маршруту, відповідного IP-адресі призначення. Маршрут за замовчуванням може бути введений вручну як статичний маршрут або отримуватися автоматично через протокол динамічної маршрутизації.

Маршрут за замовчуванням через IPv4 записується як 0.0.0.0/0, а для IPv6 має вигляд ::/0. Довжина префікса /0 вказує на те, що нуль бітів або жоден біт не повинен відповідати IP-адресі призначення для використання цього запису про маршрут. Якщо немає маршрутів з довшим збігом, більше 0 біт, то для пересилання пакета використовується маршрут за замовчуванням. Маршрут за замовчуванням іноді називають шлюзом останньої надії.

На рис. 1.2 (маршрутизатор R1) та рис. 1.3 (маршрутизатор R2) наведено приклад таблиці маршрутизації після налаштування безпосередньо під'єднаних мереж, статичної та динамічної маршрутизації (див. рис. 1.1).

```

R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 10.0.3.2 to network 0.0.0.0
O*E2 0.0.0.0/0 [110/1] via 10.0.3.2, 00:51:34, Serial0/1/1
    10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C 10.0.1.0/24 is directly connected, GigabitEthernet0/0/0
L 10.0.1.1/32 is directly connected, GigabitEthernet0/0/0
C 10.0.2.0/24 is directly connected, GigabitEthernet0/0/1
L 10.0.2.1/32 is directly connected, GigabitEthernet0/0/1
C 10.0.3.0/24 is directly connected, Serial0/1/1
L 10.0.3.1/32 is directly connected, Serial0/1/1
O 10.0.4.0/24 [110/50] via 10.0.3.2, 00:24:22, Serial0/1/1
O 10.0.5.0/24 [110/50] via 10.0.3.2, 00:24:15, Serial0/1/1
R1#

```

Рисунок 1.2 – Таблиця маршрутизації маршрутизатора R1 [2]

```

R2# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 209.165.200.226
    10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O 10.0.1.0/24 [110/65] via 10.0.3.1, 00:31:38, Serial0/1/0
O 10.0.2.0/24 [110/65] via 10.0.3.1, 00:31:38, Serial0/1/0
C 10.0.3.0/24 is directly connected, Serial0/1/0
L 10.0.3.2/32 is directly connected, Serial0/1/0
C 10.0.4.0/24 is directly connected, GigabitEthernet0/0/0
L 10.0.4.1/32 is directly connected, GigabitEthernet0/0/0
C 10.0.5.0/24 is directly connected, GigabitEthernet0/0/1
L 10.0.5.1/32 is directly connected, GigabitEthernet0/0/1
    209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.165.200.224/30 is directly connected, Serial0/1/1
L 209.165.200.225/32 is directly connected, Serial0/1/1
R2#

```

Рисунок 1.3 – Таблиця маршрутизації маршрутизатора R2 [2]

Як видно з вищенаведених таблиць, джерела для кожного маршруту визначаються кодом. Код визначає спосіб отримання маршруту. Деякі приклади поширених кодів включають:

- L – вказує на адресу, призначену конкретному інтерфейсу маршрутизатора. Цей код допомагає маршрутизатору швидко визначити, що отриманий пакет призначений саме для цього інтерфейсу і не потребує подальшого пересилання
- C – визначає безпосередньо під'єднану мережу.
- S – визначає статичний маршрут, створений для досягнення певної мережі.
- O – визначає мережу, яка отримана динамічно від іншого маршрутизатора за допомогою протоколу OSPF.
- * – цей маршрут є кандидатом на маршрут за замовчуванням.

Механізми пересилання пакетів

Основне завдання функції пересилання пакетів полягає в інкапсуляції пакетів у тип кадру канального рівня, що відповідає вихідному інтерфейсу. Чим ефективніше маршрутизатор може виконати це завдання, тим швидше він надсилатиме пакети. Маршрутизатори підтримують такі три механізми пересилання пакетів [3]:

- Програмна комутація (Process switching)
- Швидка комутація (Fast switching)
- Cisco Express Forwarding (CEF)

Програмна комутація

Застарілий механізм пересилання пакетів, але все ще доступний на деяких маршрутизаторах. Коли пакет надходить на інтерфейс, він пересилається на рівень керування, де ЦП зіставляє адресу призначення із записом у таблиці маршрутизації, а потім визначає вихідний інтерфейс і пересилає пакет (рис 1.4) Маршрутизатор проводить цю операцію з кожним пакетом, навіть якщо цілий потік пакетів прямує за однією адресою призначення. Механізм програмної комутації працює дуже повільно і рідко застосовується в сучасних мережах.

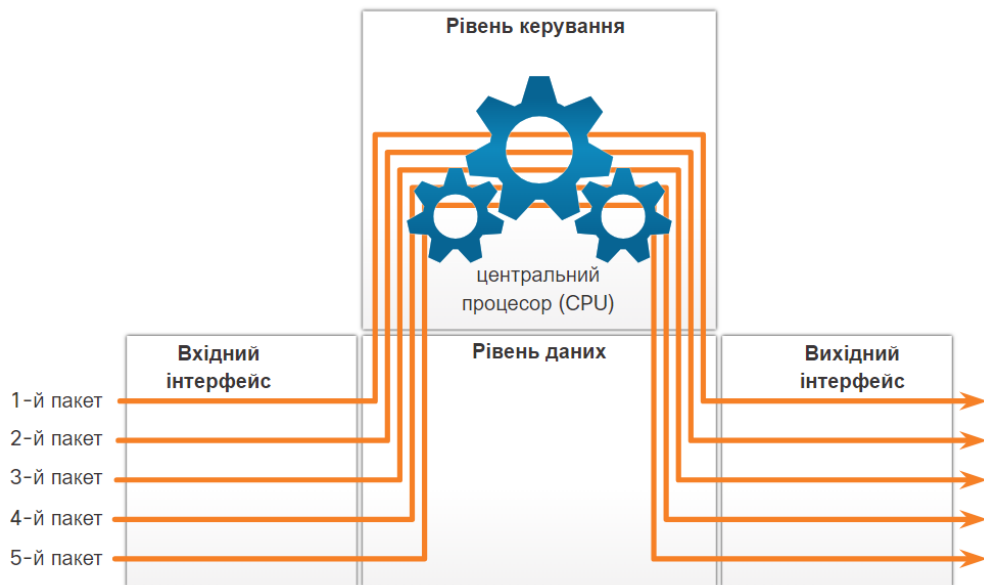


Рисунок 1.4 – Програмна комутація [4]

Швидка комутація (Fast switching)

Швидка комутація – це ще один застарілий механізм переадресації пакетів, який був наступником програмної комутації. Швидка комутація використовує кеш швидкої комутації для зберігання інформації про наступне пересилання. Коли пакет надходить на інтерфейс, він пересилається на рівень керування, де ЦП шукає відповідність у кеші швидкої комутації. Якщо збігів не знайдено, пакет проходить програмну комутацію і пересилається на вихідний інтерфейс. Інформація про трафік для пакетів також зберігається у кеші швидкої комутації. Якщо на інтерфейс надходить інший пакет із тим самим призначенням, то інформація з кеш-пам'яті про наступний перехід повторно використовується без втручання ЦП.

При швидкій комутації тільки перший пакет потоку проходить програмну комутацію, після чого він додається до кешу швидкої комутації. Наступні чотири пакети швидко обробляються, виходячи з інформації у кеш-пам'яті.

Схема схожа на процесорну комутацію, за винятком того, що пакети відправляються через Fast Forward Cache, а не через рівень керування, якщо попередній пакет має те ж місце призначення, що і пакет, який пересилається в місце призначення без втручання рівня керування (рис. 1.5).

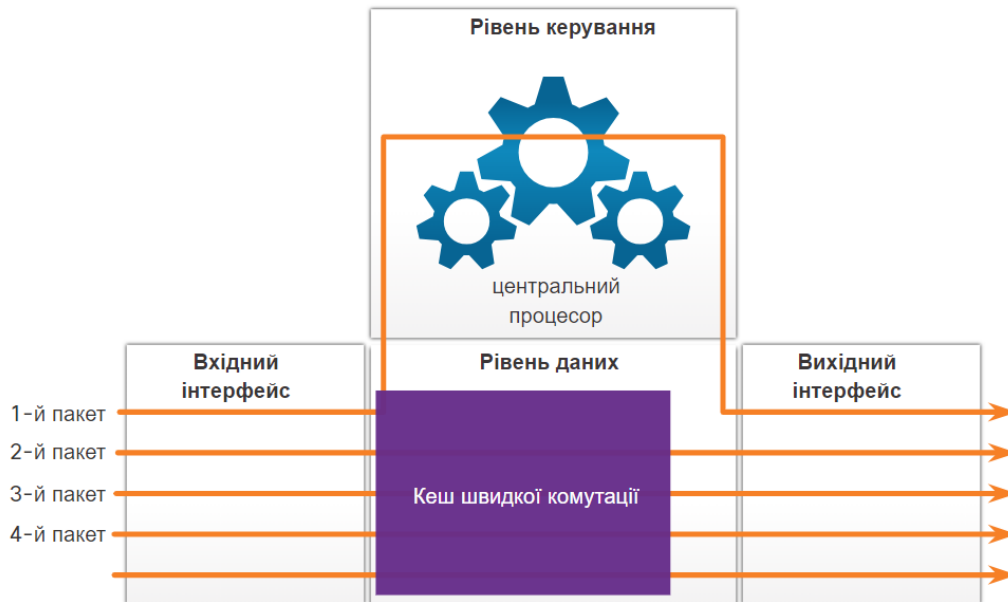


Рисунок 1.5 – Швидка комутація [4]

Cisco Express Forwarding (CEF)

CEF є найновішим механізмом пересилання пакетів Cisco IOS і використовується за замовчуванням. Як і швидка комутація, CEF створює 24-портову базу даних переадресації (FIB) і таблицю суміжності (adjacency table). Однак записи таблиці ініційовані не пакетами, як при швидкій комутації, а змінами – наприклад змінами в мережній топології. Таким чином, після настання збіжності мережі в базі даних FIB і таблиці суміжності міститься вся інформація, необхідна маршрутизатору при пересиланні пакета. Комутація Cisco Express Forwarding – це найшвидший механізм пересилання, що застосовується за замовчуванням на маршрутизаторах Cisco і багаторівневих комутаторах.

Після збіжності мережі CEF формує базу даних FIB і таблицю суміжності. Всі п'ять пакетів швидко опрацьовуються на рівні даних (рис. 1.6)

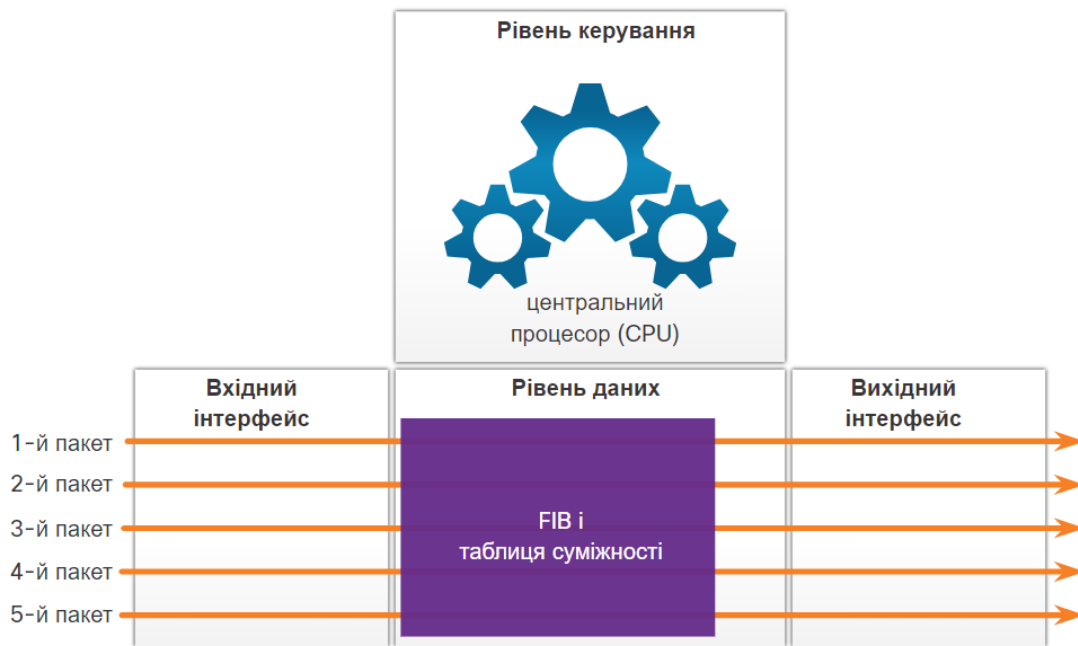


Рисунок 1.6 – Cisco Express Forwarding (CEF) [4]

Отже, три механізми пересилання пакетів можна описати, провівши наступну аналогію:

- Програмна комутація робить всі розрахунки кожного разу, навіть у випадку рішення ідентичних проблем.
- Швидка комутація робить розрахунки один раз, запам'ятовуючи відповідь для наступних ідентичних випадків.
- Механізм CEF вирішує кожну з можливих проблем заздалегідь, вносячи її в електронну таблицю.

1.2 Загальний огляд протоколів внутрішньої маршрутизації

Протоколи динамічної маршрутизації спрощують обмін інформацією маршрутами між маршрутизаторами. Протокол маршрутизації являє собою набір процесів, алгоритмів та повідомлень, що використовуються для обміну даними маршрутизації та наповнення таблиці маршрутизації оптимальними шляхами.

Протоколи динамічної маршрутизації виконують різноманітні функції, такі як визначення віддалених мереж, оновлення маршрутних даних, вибір

найоптимальнішого маршруту та пошук нового оптимального шляху у випадку недоступності поточного шляху. Протоколи маршрутизації можна класифікувати за різними групами відповідно до їх характеристик. Зокрема, протоколи маршрутизації можна класифікувати за такими ознаками:

- За призначення – внутрішній протокол маршрутизації (IGP) або зовнішній протокол маршрутизації (EGP);
- Дія – протокол вектора відстані, протокол стану каналу або протокол векторного шляху;
- Поведінка – класовий (застарілий) або безкласовий протокол.

Наприклад, протоколи маршрутизації IPv4 можна класифікувати наступним чином:

- IGRP (застарілий) – представляє собою дистанційно-векторний класовий протокол внутрішньої маршрутизації, що був розроблений компанією Cisco (не використовується після виходу IOS 12.2 та пізніших версій).
- RIPv1 (застарілий) – це дистанційно-векторний класовий протокол внутрішньої маршрутизації.
- RIPv2 – є безкласовим протоколом вектора відстані для внутрішньої маршрутизації.
- OSPF – представляє собою безкласовий протокол внутрішньої маршрутизації, орієнтований на стан каналу.
- EIGRP – це дистанційно-векторний безкласовий протокол внутрішньої маршрутизації, розроблений компанією Cisco.
- IS-IS – є безкласовим протоколом внутрішньої маршрутизації, також орієнтованим на стан каналу.
- BGP – представляє собою безкласовий протокол зовнішньої маршрутизації за вектором маршруту.

Протоколи класової маршрутизації RIPv1 та IGRP є застарілими протоколами та використовуються лише у старих мережевих топологіях. Пізніше ці протоколи були вдосконалені у протоколи безкласової маршрутизації – RIPv2 та EIGRP. За своєю суттю протоколи маршрутизації стану каналу належать до протоколів безкласової маршрутизації. [1]

Ієрархічний вид класифікації протоколів динамічної маршрутизації можна зобразити графічно наступним чином (рис. 1.7):

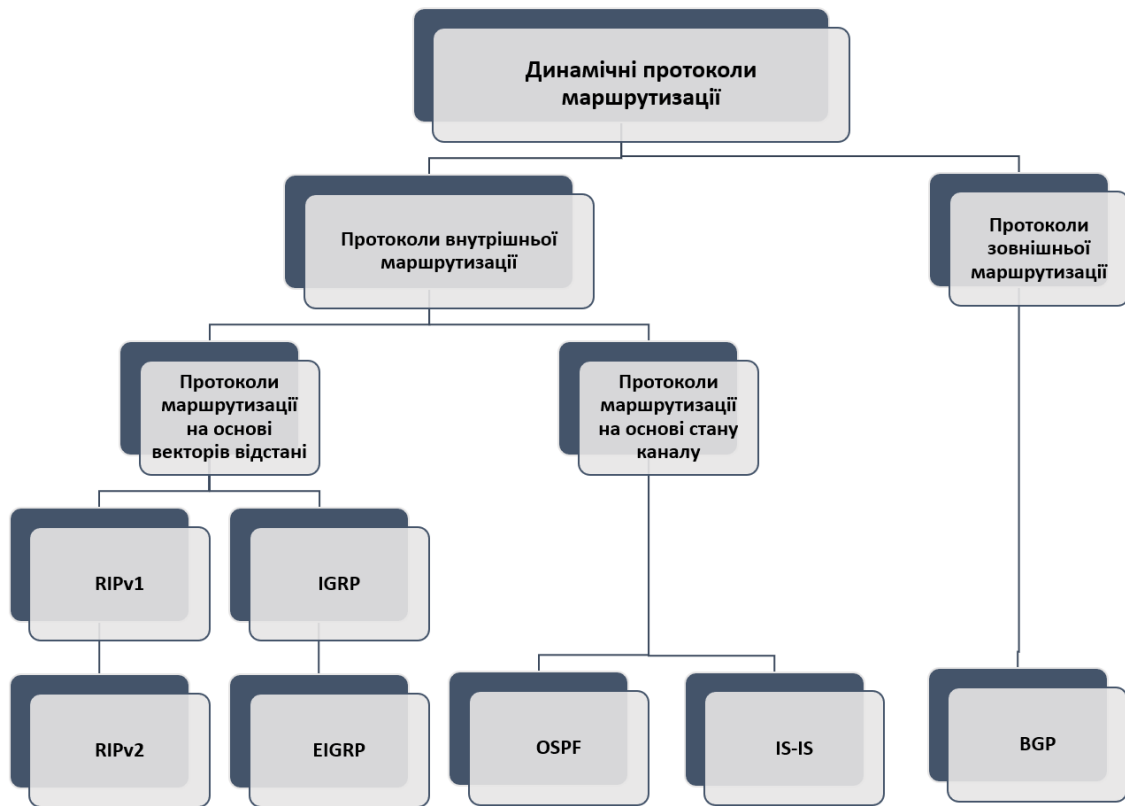


Рисунок 1.7 – Ієрархічна класифікація протоколів динамічної маршрутизації [5]

Протоколи маршрутизації IGP та EGP

Автономна система (AS) представляє собою групу маршрутизаторів, які керуються одним оператором, таким як компанія або організація. Також використовується термін «домен маршрутизації» для опису автономної системи. Зазвичай автономні системи включають внутрішню мережу компанії або мережу інтернет-провайдера.

Інтернет будується на основі концепції автономних систем, тому вона вимагає використання двох типів протоколів маршрутизації:

1) Протоколи внутрішньої маршрутизації використовуються для керування маршрутизацією всередині автономної системи. Цей вид маршрутизації також відомий як внутрішня маршрутизація автономної системи.

Організації, фірми і навіть оператори зв'язку користуються протоколами внутрішньої маршрутизації для управління внутрішніми мережами. Протоколи, що використовуються для внутрішньої маршрутизації, включають в себе OSPF, RIP, EIGRP, і IS-IS.

2) Протоколи зовнішнього шлюзу (EGP) використовуються для управління маршрутизацією між різними автономними системами. Цей тип маршрутизації також відомий як зовнішня маршрутизація автономної системи. Цей процес взаємодії між мережами операторів зв'язку та великих компаній може здійснюватися через протокол зовнішньої маршрутизації. Протокол граничного шлюзу (BGP) є єдиним офіційним протоколом маршрутизації EGP, що використовується в Інтернеті.

Так як BGP єдиний доступний протокол для зовнішньої маршрутизації, термін «протокол зовнішньої маршрутизації» рідко використовується. Натомість терміну мережеві фахівці використовують термін протокол BGP.[1]

Принцип роботи протоколів динамічної маршрутизації

Всі протоколи маршрутизації розроблені для отримання даних про віддалені мережі та швидку адаптацію до будь-яких змін у топології. Спосіб виконання цих завдань протоколом маршрутизації залежить від обраного алгоритму та експлуатаційних характеристик даного протоколу.

Загалом, роботу протоколу динамічної маршрутизації можна описати в такий спосіб.

1) Маршрутизатор відправляє та отримує повідомлення щодо маршрутизації на своїх інтерфейсах.

2) Маршрутизатор представляє спільний доступ до повідомлень маршрутизації та даних про маршрути для інших маршрутизаторів, які використовують той самий протокол маршрутизації.

3) Маршрутизатори взаємодіють, обмінюючись даними маршрутизації, щоб отримати інформацію про віддалені мережі.

4) Коли маршрутизатор виявляє зміну топології, протокол маршрутизації може оголосити цю зміну іншим маршрутизаторам.

Характеристики протоколів маршрутизації

Протоколи маршрутизації можна порівняти на основі таких характеристик:

- Швидкість збіжності – визначає швидкість обміну даними маршрутизації та досягнення узгодженості даних між маршрутизаторами в рамках мережевої топології. Чим вища швидкість збіжності, тим краще підходить даний протокол. Можуть виникати петлі маршрутизації, якщо невідповідні таблиці маршрутизації не синхронізуються чи не оновлюються через повільну збіжність у мережі, що змінюється.

- Масштабованість – визначення максимально можливого розміру мережі з урахуванням протоколу маршрутизації. Чим більший розмір мережі, тим більше можливостей масштабування має бути передбачено протоколом маршрутизації.

- Протоколи маршрутизації можуть бути класовими або безкласовими (з використанням VLSM): класові протоколи маршрутизації не містять інформацію про маску підмережі та не підтримують використання VLSM. Протоколи маршрутизації безкласового типу включають інформацію про маску підмережі у свої оновлення. Ці протоколи підтримують використання VLSM та забезпечують більш гнучке поєднання маршрутів.

- Споживання ресурсів включає в себе вимоги до протоколу маршрутизації, такі як обсяг використаної пам'яті (ОЗП), використання ресурсів центрального процесора (ЦП) та смуги пропускання каналу. Чим більше ресурсів потрібно, тим потужніше має бути апаратне забезпечення для ефективної підтримки роботи протоколу маршрутизації, за винятком процесів, пов'язаних із пересиланням пакетів.

- Реалізація і обслуговування – характеристика, яка описує рівень знань, необхідний адміністратору мережі для реалізації та обслуговування мережі на базі розгорнутого протоколу.

У таблиці представлений короткий огляд показників кожного протоколу маршрутизації (табл. 1.1)

Таблиця 1.1 – Порівняння протоколів маршрутизації

	Вектор відстані				Стан каналу	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
Швидкість взаємодії	Повільна	Повільна	Повільна	Висока	Висока	Висока
Масштабованість, розмір мережі	Малі	Малі	Малі	Великі	Великі	Великі
Використання VLSM	Ні	Так	Ні	Так	Так	Так
Використання ресурсів	Низьке	Низьке	Низьке	Середнє	Високе	Високе
Реалізація і обслуговування	Проста	Проста	Проста	Складна	Складна	Складна

Джерело: побудовано автором на основі [6]

Можна зробити висновок, що протоколи RIPv1, RIPv2 та IGRP мають низьке використання ресурсів, прості в реалізації та обслуговуванні, але при цьому підходять лише для невеликих мереж та мають низьку швидкість взаємодії. В той же час протоколи EIGRP, OSPF, IS-IS мають високу швидкість та підходять для великих мереж, але складні в реалізації та обслуговуванні та використовують більше ресурсів.

Протоколи маршрутизації на базі векторів відстані

«Дистанційно-векторний» означає, що маршрути оголошуються шляхом зазначення двох характеристик:

- Відстань – це визначення віддаленості мережі призначення; базується на різних метриках, таких як кількість переходів, вартість, пропускна здатність, значення затримки та інші.
- Вектор вказує напрямок маршрутизатора для наступного переходу або вихідного інтерфейсу маршруту для досягнення адреси призначення.

Маршрутизатор, який оперує за допомогою дистанційно-векторного протоколу, не має інформації про повний маршрут до мережі призначення.

Протоколи маршрутизації на основі векторів відстані використовують маршрутизатори як вказівники шляху до кінцевої точки призначення. Єдині відомості, які доступні маршрутизатору щодо віддаленої мережі, - це відстань або метрика до цієї мережі, а також інтерфейс чи шлях, який використовується для доступу до неї. Протоколи маршрутизації на основі векторів відстані не мають схеми топології мережі, як інші типи протоколів маршрутизації.

- Існують чотири дистанційно-векторні протоколи внутрішньої маршрутизації для IPv4:

- RIPv1 – перша версія застарілого протоколу;
- RIPv2 – простий дистанційно-векторний протокол;
- IGRP – оригінальний запатентований протокол Cisco (наразі застарілий і замінений EIGRP);
- EIGRP – це розширена версія дистанційно-векторного протоколу. [7]

Протоколи маршрутизації на основі стану каналу

На відміну від маршрутизаторів, налаштованих для роботи дистанційно-векторного протоколу, маршрутизатори, які використовують протокол маршрутизації за станом каналу, можуть створювати повне уявлення чи збір інформації від інших маршрутизаторів для визначення топології мережі.

Можна порівняти використання протоколу маршрутизації за станом каналу з використанням детальної карти мережевої топології. Вказівники шляху від джерела до призначення не є необхідними, оскільки всі маршрутизатори, які оперують за станом каналу, використовують однакову карту мережі. Маршрутизатор на основі протоколу стану каналу використовує дані про стан каналу для створення карти топології та вибору оптимального шляху до всіх мереж призначення в топології.

Протоколи маршрутизації стану каналу не використовують регулярні оновлення. І навпаки, маршрутизатори за допомогою протоколу RIP відправляють періодичні оновлення маршрутної інформації своїм сусіднім пристроям. Після того як маршрутизатори дізналися про всі необхідні мережі (досягнута конвергенція), оновлення стану каналу відправляється тільки при зміні топології.

Застосування протоколів маршрутизації за станом каналу є доцільним у таких випадках:

- Мережа має ієрархічну структуру, що, як правило, характерне для великих мереж.
- Швидка адаптація до змін мережі має вирішальне значення.
- Адміністратори добре обізнані з реалізацією та обслуговуванням протоколу маршрутизації на основі стану каналу.

Є два протоколи внутрішньої маршрутизації для IPv4, які враховують стан каналу:

- Протокол OSPF – поширений, заснований на стандартах протокол маршрутизації.
- IS-IS – протокол, поширений у мережах операторів зв'язку.

Протоколи маршрутизації за станом каналу також відомі як протоколи маршрутизації найкоротшого шляху. Протоколи такого типу використовують алгоритм маршрутизації найкоротшого шляху (SPF), розроблений Едсгером Дейкстрою. Вони вважаються більш складними порівняно з дистанційно-векторними протоколами, але базові функції та налаштування протоколів маршрутизації за станом каналу лишаються простими.

Протоколи маршрутизації за станом каналу мають низку переваг перед дистанційно-векторними протоколами [8]:

- Створюють топологічну схему. Протоколи маршрутизації з урахуванням стану каналу створюють топологічну схему чи дерево SPF топології мережі. Оскільки протоколи маршрутизації, що використовують стан каналу, взаємодіють через обмін пакетами стану каналу, алгоритм пошуку найкоротшого шляху може сформувати дерево найкоротших шляхів SPF для всієї мережі. За допомогою дерева найкоротших шляхів SPF, кожен маршрутизатор може автоматично встановити найкоротший шлях до кожної мережі.
- Швидка збіжність. Коли отримується пакет, протоколи маршрутизації за станом каналу безперервно відправляють цей пакет з усіх інтерфейсів, за винятком того, з якого він був отриманий. Напроти, протокол

RIP повинен обробити кожне оновлення маршрутизації та оновлення таблиці маршрутизації перед тим, як виконати лавинну розсилку з інших інтерфейсів.

- Оновлення за подією. Після відправки початкової хвилі пакетів стану каналу, протоколи маршрутизації розсилають пакети стану каналу лише у випадку внесення змін у топологію. Пакет стану каналу містить лише інформацію щодо відповідного каналу. На відміну від деяких дистанційно-векторних протоколів, протоколи маршрутизації за станом каналу не відправляють регулярні оновлення

- Ієрархічна структура. Протоколи маршрутизації за станом каналу оперують концепцією областей. Декілька областей утворюють ієрархічну структуру мережі, що забезпечує ефективне об'єднання маршрутів та ізоляцію проблем маршрутизації в межах конкретної області.

Класові протоколи маршрутизації

Основна відмінність між класовими та безкласовими протоколами маршрутизації полягає у тому, що класові протоколи маршрутизації не включають інформацію щодо маски підмережі у свої оновлення маршрутизації. З іншого боку, безкласові протоколи маршрутизації передають дані про маску підмережі разом із своїми оновленнями маршрутизації.

На початковому етапі було створено два протоколи маршрутизації для IPv4 – RIPv1 та IGRP. Ці протоколи були розроблені тоді, коли мережеві адреси виділялися відповідно до класів (наприклад, класу А, В або С). Тодішні протоколи маршрутизації не вимагали включення маски підмережі в пакети оновлень, оскільки за першим октетом мережевої адреси можна було визначити відповідну маску мережі.

До класових протоколів маршрутизації належать лише протоколи RIPv1 та IGRP. Усі інші протоколи маршрутизації для IPv4 і IPv6 є безкласовими. Класова адресація ніколи не використовувалася в IPv6.

Те, що протоколи RIPv1 та IGRP не включають інформацію про маску підмережі в оновлення, означає, що вони не підтримують маски підмережі змінної довжини (VLSM) і, відповідно, не можуть бути використані в контексті безкласового протоколу міждоменної маршрутизації (CIDR). Інакше кажучи,

класові протоколи маршрутизації не можуть бути використані, якщо мережа поділена на підмережі з використанням більш ніж однією маскою підмережі (рис. 1.8)

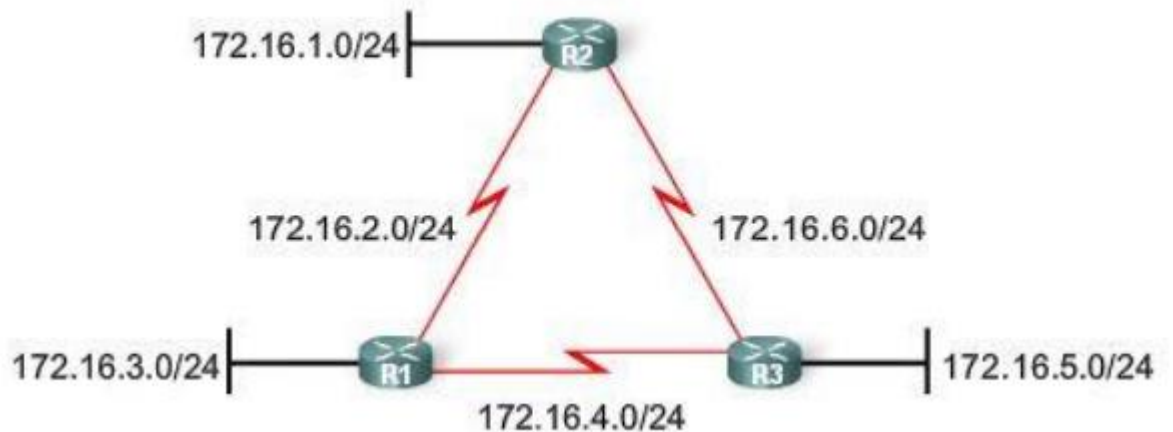


Рисунок 1.8 – Для всієї топології використовується одна маска підмережі (класова маршрутизація) [3]

Протоколи маршрутизації, які використовують класову адресацію, також можуть викликати проблеми у мережах з «розірваною» структурою. Мережа вважається «розірваною» у випадку, якщо підмережі в рамках однієї основної класової мережі розділені іншою класовою мережевою адресою.

Безкласові протоколи маршрутизації

Сучасні мережі більше не використовують класову IP-адресацію, тому маска підмережі не може бути визначена за значенням першого октету. Протоколи маршрутизації IPv4 без використання класів (RIPv2, EIGRP, OSPF та IS-IS) включають інформацію щодо маски підмережі в оновлення маршрутизації, разом з мережевою адресою. Ці протоколи безкласової маршрутизації підтримують використання VLSM і CIDR.

Протоколи маршрутизації IPv6 є безкласовими. Відмінності між класовими чи безкласовими протоколами стосуються лише протоколів маршрутизації IPv4. Всі протоколи маршрутизації для IPv6 розглядаються як безкласові, оскільки вони включають довжину префікса разом із IPv6-адресою.

На рисунку 1.9 наведено безкласову версію мережі, де для однієї і тієї ж топології використовуються маски /30 і /27. Крім того, слід відзначити, що ця топологія включає несуміжні мережі.

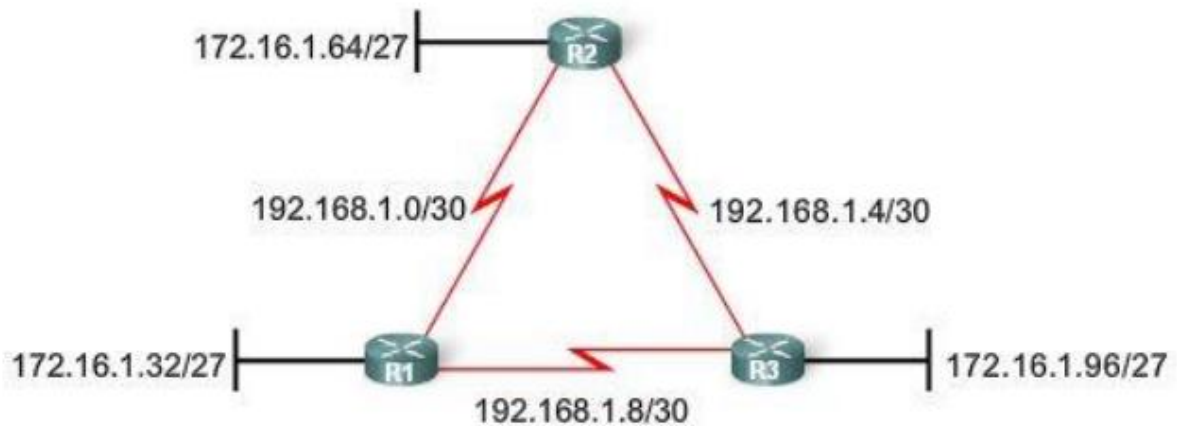


Рисунок 1.9 – В топології використано різні маски підмереж (безкласова маршрутизація) [3]

Метрики протоколів маршрутизації

У деяких ситуаціях протокол маршрутизації може мати кілька маршрутів до одного пункту призначення. При виборі кращого шляху протокол маршрутизації повинен мати можливість оцінювати та вибирати між доступними шляхами. Це завдання виконується за допомогою метрик маршрутизації.

Метрика – це значення, яке присвоюється протоколом маршрутизації різним маршрутам, враховуючи корисність кожного з них. Коли існує декілька маршрутів до однієї віддаленої мережі, метрики маршрутизації використовуються для визначення «вартості» шляху від джерела до пункту призначення. Протоколи маршрутизації вибирають оптимальний шлях, враховуючи маршрут з найменшою вартістю.

Різні протоколи маршрутизації використовують різні метрики. Метрика, що використовується одним протоколом маршрутизації, несумісна з метрикою, яка використовується іншим. В результаті два різних протоколи маршрутизації можуть обирати відмінні шляхи до одного і того ж місця призначення.

Метрики, які використовуються протоколами IP-маршрутизації, наведені в таблиці 1.2.

Таблиця 1.2 – Метрики протоколів IP-маршрутизації

Метрика	Пояснення
Hop count (простий показник)	Вказує кількість маршрутизаторів, які повинен пройти пакет.
Bandwidth (пропускна здатність)	Перевага надається маршрутові з найвищою пропускною здатністю.
Load (завантаження)	Розглядається трафік для конкретного каналу зв'язку.
Delay (затримка)	Враховує час, необхідний пакету для подолання шляху.
Reliability (надійність)	Оцінює ймовірність відмови каналу зв'язку, розраховується на основі кількості помилок на інтерфейсі або попередніх відмов каналу.
Cost (вартість)	Значення, що встановлюється IOS або мережевим адміністратором для вказівки переваги маршруту. Вартість може бути метрикою, комбінацією метрик або політикою.

Джерело: побудовано автором на основі: [9]

Список динамічних протоколів та метрики, що ними використовуються:

- Протокол RIP – кількість переходів.
- Протокол OSPF («алгоритм найкоротшого шляху») – метрика компанії Cisco, яка оснований на загальній пропускній здатності шляху від вихідного пункту до пункту призначення.
- Протокол EIGRP (удосконалений протокол внутрішньої маршрутизації між шлюзами, EIGRP) – мінімальна пропускна здатність, затримка, навантаження та надійність.

Адміністративна відстань

За винятком особливих обставин, на маршрутизаторі повинен застосовуватися лише один протокол динамічної маршрутизації. Однак на маршрутизаторі можна налаштувати як OSPF, так і EIGRP, і обидва протоколи маршрутизації можуть дізнатися про одну і ту ж мережу призначення. Кожен протокол маршрутизації може вибирати свій шлях для досягнення пункту призначення на основі метрики цього протоколу маршрутизації.

В маршрутизаторах компанії Cisco для визначення маршруту і занесення його до таблиці IP-маршрутизації застосовується адміністративна відстань (administrative distance, AD). Ця величина позначає надійність маршруту. Чим нижче значення AD, тим вища надійність.

У таблиці 1.3 наведені різні протоколи маршрутизації і відповідні їм значення AD.

Таблиця 1.3 – Протоколи маршрутизації і відповідні їм значення AD

Джерело Маршруту	Адміністративна відстань
Безпосереднє під'єднання	0
Статичний маршрут	1
Узагальнений маршрут EIGRP	5
Зовнішній BGP	20
Внутрішній EIGRP	90
OSPF	110
IS-IS	115
RIP	120
Зовнішній EIGRP	170
Внутрішній BGP	200

Джерело: побудовано автором на основі [9]

Найбільш поширеним прикладом є маршрутизатор, який дізнається про одну і ту ж мережеву адресу завдяки статичному маршруту і протоколу динамічної маршрутизації, наприклад OSPF. Статичний маршрут має AD 1, тоді як маршрут, виявлений за допомогою OSPF, має AD 110. За наявності двох різних маршрутів до тієї ж самої точки призначення, маршрутизатор обирає маршрут із найнижчим значенням AD. При виборі між статичним маршрутом і розрахованим маршрутом за OSPF, вибирається статичний маршрут.

Безпосередньо під'єднані мережі мають найменшу AD, яка дорівнює 0. Тільки безпосередньо під'єднана мережа може мати AD, рівну 0.

Балансування навантаження (Load Balancing)

Якщо в таблиці маршрутизації містяться два або більше шляхів з однаковими індикаторами алгоритмів для досягнення тієї ж самої мережі призначення, то він відправляє пакети по обох шляхах. Це називається рівноправним розподілом навантаження. Таблиця маршрутизації містить одну мережу призначення, але для кожного шляху існує окремий вихідний інтерфейс у таблиці маршрутизації, і маршрутизатор використовує ці інтерфейси для пересилання пакетів через різні шляхи з однаковою вартістю.

При належній конфігурації, розподіл навантаження може покращити ефективність та продуктивність мережі.

Балансування навантаження з однаковою вартістю реалізується автоматично за допомогою протоколів динамічної маршрутизації. Воно включається для статичних маршрутів, коли існує кілька статичних маршрутів в одну і ту ж мережу призначення з використанням різних маршрутизаторів наступного переходу.

Протокол EIGRP також підтримує розподіл навантаження з нерівною вартістю.

1.3 Висновки з розділу 1

В даному розділі було розглянуто основні поняття та принципи внутрішньої маршрутизації, а також проведено детальний аналіз протоколів внутрішньої маршрутизації, зроблені наступні висновки:

1) Основні принципи маршрутизації включають визначення оптимального шляху для передачі даних та пересилання пакетів до місця призначення. Маршрутизатор використовує таблицю маршрутизації для визначення оптимального маршруту на основі адреси призначення пакета.

2) Таблиця маршрутизації може включати безпосередньо під'єднані мережі, віддалені мережі (які можуть бути вивчені статично або динамічно) та маршрут за замовчуванням. Механізми пересилання пакетів, такі як програмна комутація, швидка комутація та Cisco Express Forwarding, визначають

ефективність і швидкодію маршрутизатора у виконанні завдань інкапсуляції та пересилання пакетів.

3) Основні завдання протоколів динамічної маршрутизації, такі як ідентифікація віддалених мереж, оновлення маршрутних даних, визначення оптимального маршруту до призначених мереж та пошук нового оптимального маршруту у випадку недоступності поточного шляху.

4) Визначено способи класифікації протоколів динамічної маршрутизації, а саме: за призначенням, за дією, за поведінкою. Виявлено, що в сучасних мережах рекомендується використовувати безкласові протоколи внутрішньої маршрутизації, такі як RIPv2, EIGRP, OSPF, для досягнення оптимальної маршрутизації.

5) На основі порівняння протоколів маршрутизації було визначено, що для невеликих мереж із обмеженими ресурсами, простий протокол, такий як RIPv2, може бути відмінним вибором, тоді як великим мережам доцільніше використовувати протоколи EIGRP, OSPF або IS-IS з вищою швидкістю та масштабованістю.

6) Розглянуто дистанційно-векторні протоколи та протоколи за станом каналу, проаналізовано їх переваги й недоліки, з чого можна зробити висновок, що вибір між дистанційно-векторними та протоколами маршрутизації за станом каналу залежить від розміру та характеристик конкретної мережі, а також від вимог до швидкодії та ефективності маршрутизації.

7) Проаналізовано класові та безкласові протоколи маршрутизації, визначено переваги безкласових над класовими протоколів. З'ясовано, що перехід на безкласові протоколи забезпечив більшу гнучкість та ефективність мережевого проєктування.

8) Проаналізовано метрики маршрутизації для різних протоколів, розглянуто поняття адміністративна відстань і балансування навантаження. Правильний вибір метрик і розуміння їх використання в протоколах маршрутизації є ключовим для ефективного та надійного функціонування мережі.

2 АНАЛІЗ ПРОТОКОЛУ ВНУТРІШНЬОЇ МАРШРУТИЗАЦІЇ OSPF В IP-МЕРЕЖАХ

2.1 Принцип роботи протоколу OSPF

OSPF – протокол маршрутизації за станом каналів, розроблений як альтернатива протоколу маршрутизації з урахуванням векторів відстані RIP. Протокол RIP був прийнятим у якості протоколу маршрутизації на початкових стадіях розвитку мережових технологій та Інтернету. Проте використання протоколом RIP числа переходів як єдиної метрики визначення оптимального маршруту незабаром призвело до ряду труднощів. Використання цього методу обмежує можливості масштабування великих мереж, які містять кілька шляхів з різними швидкостями. У протокола OSPF володіє кількома значними перевагами у порівнянні з протоколом RIP, забезпечуючи швидшу збіжність та можливість масштабування з метою побудови більш великих мереж.

Протокол OSPF використовує концепцію областей для масштабування та є протоколом маршрутизації без врахування класів.

Розвиток протоколу OSPF

Розробку OSPF у 1987 році розпочала робоча група OSPF у складі Інженерної групи з розвитку Інтернету (IETF). На той час Інтернет використовувався в основному як академічна та дослідна мережа, розгорнута урядом США. [10]

У 1989 році була опублікована специфікація протоколу OSPFv1 через запит для коментарів (RFC) 1131. Здійснено дві реалізації, одна з яких була призначена для використання з маршрутизаторами, а інша – з робочими станціями під управлінням UNIX. Друга реалізація стала популярним сервісом UNIX, відомим як GATED. OSPFv1 був позначений як експериментальний протокол маршрутизації, і його впровадження не відбулося.

В 1991 році Джон Мії представив протокол OSPFv2 у рамках запиту для коментарів (RFC) 1247. Протокол OSPFv2 пропонував суттєві технічні переваги порівняно з протоколом OSPFv1. Цей протокол є безкласовим, отже, підтримує використання VLSM та маршрутизації CIDR.

В той період, коли протокол OSPF був введений, робоча група ISO розробляла власний протокол маршрутизації за станом каналу, відомий як протокол проміжних систем (IS-IS). Інженерна група з розвитку Інтернету (IETF) обрала протокол OSPF як рекомендований протокол внутрішньої маршрутизації.

У 1998 році специфікація протоколу OSPFv2 була оновлена у запиті для коментарів (RFC) 2328, що є актуальним і на сьогоднішній день RFC для протоколу OSPF.

В 1999 році було опубліковано протокол OSPFv3 для IPv6 у RFC 2740. Протокол OSPF для IPv6, розроблений Джоном Мойєм, Робом Колтаном і Деннісом Фергюсоном, є не лише новою реалізацією протоколу для IPv6, а й новим словом у роботі протоколів загалом.

В 2008 році протокол OSPFv3 був вдосконалений за допомогою RFC 5340, яке визначило його як протокол OSPF для IPv6.

У 2010 р. в RFC 5838 було введено підтримку сімейств адрес (AF) в OSPFv3. Використання сімейств адрес дозволяє протоколу маршрутизації підтримувати обидва протоколи, IPv4 і IPv6, в межах одного уніфікованого процесу налаштування конфігурації.

Етапи розвитку протоколу OSPF продемонстровано за допомогою лінії часу (рис. 2.1)

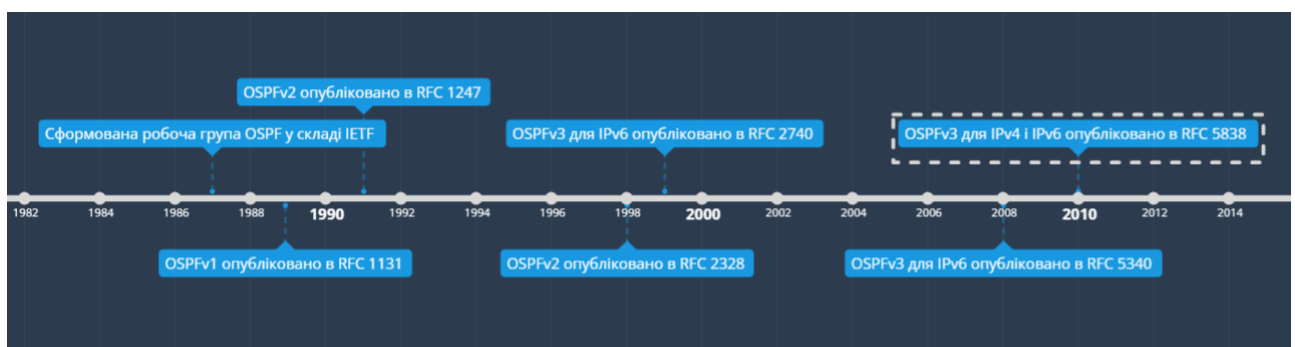


Рисунок 2.1 – Лінія часу: етапи розвитку протоколу OSPF

Джерело: побудовано автором за допомогою ресурсу time.graphics

Протокол OSPF має наступні властивості.

- Без класів: OSPFv2 з самого початку створений як безкласовий протокол, тому він підтримує VLSM та CIDR в IPv4.
- Швидка збіжність – ефективна адаптація до змін у мережі. Швидка збіжність – швидка трансляція змін мережі.
- Ефективність – активує оновлення маршрутизації при внесенні змін (без регулярних оновлень). Протокол застосовує алгоритм пошуку найкоротшого шляху SPF для вибору найкращого маршруту.
- Масштабованість – придатний для використання як у невеликих, так і великих мережах. З метою забезпечення ієрархічної структури, маршрутизатори групуються в області.
- Безпека: OSPFv2 підтримує аутентифікацію на основі MD5 (Message Digest 5) та SHA (алгоритму безпечного хешування). У OSPFv3 для додаткової аутентифікації пакетів використовується протокол IPsec. Якщо аутентифікація дозволена, маршрутизатори OSPF можуть приймати від однорангових вузлів лише повідомлення про оновлення маршрутизації, які зашифровані з попередньо узгодженим паролем.

Адміністративна відстань (AD) є значенням надійності (або переваги) джерела маршруту. Протокол OSPF має адміністративну відстань за замовчуванням зі значенням 110.

Компоненти протоколу OSPF

Всі протоколи маршрутизації використовують аналогічні компоненти.

Вони використовують повідомлення маршрутизації для обміну даними про маршрутизацію. Ці повідомлення служать основою для формування структур даних, які подальше обробляються в рамках алгоритму маршрутизації.

Протокол OSPF створює та обслуговує три бази даних (табл. 2.1):

- База даних суміжності – створює таблицю сусідніх пристроїв.
- База даних на основі стану каналу (LSDB) – створює таблицю топології.
- База даних пересилання – створення таблиці маршрутизації.

У цих таблицях вказано перелік сусідніх маршрутизаторів, які беруть участь у взаємному обміні даними маршрутизації. Інформація в таблицях зберігається та обробляється у відомій як оперативна пам'ять (ОЗП).

Таблиця 2.1 – Структура даних OSPF [11]

База даних	Таблиця	Опис
База даних суміжності	Таблиця сусідів	- Список всіх сусідніх маршрутизаторів, з якими встановлено двосторонній обмін даними. - Для кожного маршрутизатора існує унікальна таблиця
База даних станів каналів (LSDB)	Таблиця топології	- Містить дані про всі маршрутизатори в мережі. - Ця база даних представляє топологію мережі. - Всі маршрути в області використовують ідентичні бази даних станів каналів (LSDB)
База даних пересилання	Таблиця маршрутизації	- Містить дані про маршрути, які створені під час запуску алгоритму в базі даних станів каналу. - Кожен маршрутизатор використовує унікальну таблицю маршрутизації, яка містить дані про спосіб і місце відправки пакетів на інші маршрутизатори

Принцип роботи маршрутизації OSPF

Для обміну інформацією маршрутизації за допомогою протоколу OSPF, маршрутизатори виконують загальні кроки маршрутизації за станом каналу з метою досягнення стану збіжності:

1) Встановлення відносин суміжності із сусідніми пристроями. Маршрутизатори з підтримкою OSPF повинні виявити одне одного у мережі, щоб обмінюватися даними. Маршрутизатор, який використовує OSPF, висилає пакети вітання з усіх активних інтерфейсів з увімкненим OSPF, ідентифікуючи всі пристрої, що розташовані на цих каналах. Якщо на каналі присутній

сусідній пристрій, маршрутизатор, який використовує OSPF, намагатиметься встановити з ним відносини сусідності.

2) Обмін оголошеннями про стан каналу. Після встановлення взаємозв'язку суміжності, маршрутизатори розпочинають взаємний обмін оголошеннями про стан каналу (LSA). LSA містять інформацію про стан та вартість кожного каналу з прямим підключенням. Маршрутизатори передають свої оголошення про стан каналу (LSA) своїм сусідам. При отриманні LSA, суміжні пристрої негайно ретранслюють свої LSA сусідам з прямим з'єднанням, і цей процес триває, доки всі маршрутизатори області не отримають повну інформацію про LSA.

3) Створення таблиці топології відбувається після отримання оголошень про стан каналу (LSA). Маршрутизатори, які використовують OSPF, формують базу даних топології, ураховуючи інформацію, отриману з цих пакетів. Ця база даних поступово накопичує всю необхідну інформацію про топологію мережі.

4) Після отримання оголошень про стан каналу (LSA), маршрутизатори, що використовують OSPF, запускають алгоритм пошуку найкоротшого шляху (SPF). Цей алгоритм формує дерево найкоротших шляхів SPF.

На підставі даних дерева SPF пропонуються найкращі шляхи для таблиці IP-маршрутизації. Маршрут додається до таблиці маршрутизації, якщо немає джерела маршруту до тієї ж мережі з меншою адміністративною відстанню, наприклад статичного маршруту. Рішення щодо маршрутизації приймаються на основі записів у таблиці маршрутизації.

У таблиці на рисунку 2.2 показано найкоротший шлях і накопичену вартість досягнення визначених мереж призначення з точки зору маршрутизатора R1.

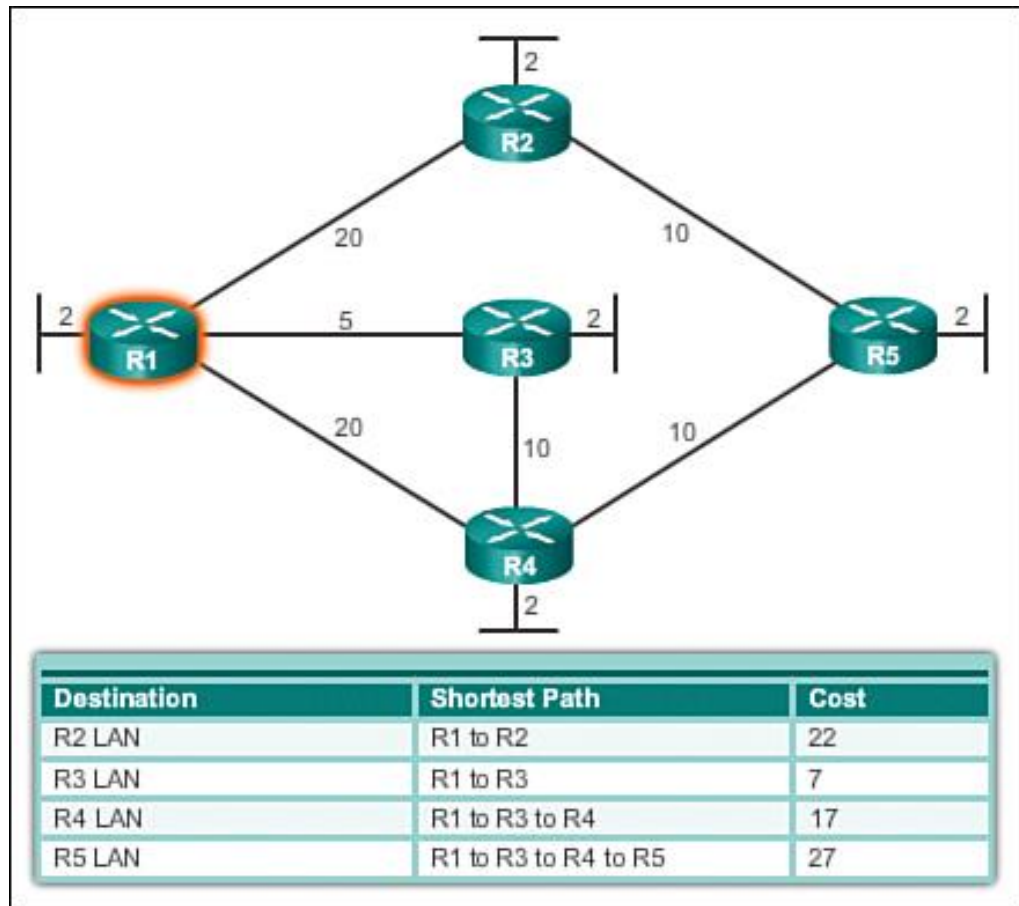


Рисунок 2.2 – Приклад дерева SPF [10]

Найкоротший шлях – це не обов’язково шлях із найменшою кількістю переходів. Розглянемо шлях до локальної мережі R5. Можна припустити, що R1 надсилатиме дані безпосередньо до R4, а не через R3. Однак вартість прямого досягнення R4 (22) вища, ніж вартість досягнення R4 через R3 (17).

Типи пакетів OSPF

OSPF використовує пакети стану каналу для установки та збереження відносин суміжності, а також для обміну оновленнями маршрутизації. Кожен тип пакета виконує певне завдання у процесі маршрутизації OSPF:

- Тип 1: пакет привітання (hello) – використовується для встановлення та підтримання відносин суміжності з маршрутизаторами OSPF.
- Тип 2: пакет опису бази даних або дескриптор бази даних (DBD) – містить скорочений список баз даних станів каналів відправляючого маршрутизатора. Використовується приймаючими маршрутизаторами для звірки з локальною базою даних стану каналу. Для створення точного дерева найкоротших шляхів SPF маршрутизатори, які використовують протоколи

маршрутизації за станом каналу в межах області, повинні використовувати однакову базу даних стану каналу.

- Тип 3: пакет запиту стану каналу (LSR) – маршрутизатори, які отримують дані, можуть запитати додаткову інформацію про будь-який запис у пакеті опису бази даних (DBD), використовуючи пакет запиту стану каналу (LSR).

- Тип 4: пакет оновлення стану каналу (LSU) – Застосовується для відправлення відповідей на запити стану каналу (LSR) та для оголошення нових даних. В пакетах оновлення стану каналу (LSU) включено сім різновидів записів LSA.

- Тип 5: пакет підтвердження стану каналу (LSAck) – при отриманні пакету оновлення стану каналу (LSU), маршрутизатор висилає підтвердження отримання у вигляді пакету підтвердження стану каналу (LSAck), і поле даних у LSAck залишається порожнім.

Пакет привітання

Пакет протоколу OSPF 1-го типу – це пакет привітання або hello-пакет. Він використовується в таких цілях:

- Виявлення сусідніх пристроїв OSPF та встановлення відносин суміжності з ними.
- Оголошення параметрів, у яких два маршрутизатори зобов'язані погодитися встановити відносини суміжності.
- У мережах з множинним доступом (Ethernet та Frame Relay) необхідно вибрати виділений маршрутизатор (DR) та резервний виділений маршрутизатор (BDR). В каналах виду «точка-точка» наявність DR або BDR не обов'язкова.

В таблиці 2.2 показано поля, що містяться в пакеті вітання OSPFv2 1-го типу.

Таблиця 2.2 – Вміст пакету привітання OSPF[5]

Версія	Тип = 1	Довжина пакета	
Ідентифікатор маршрутизатора			
Ідентифікатор області			
Контрольна сума		Тип аутентифікації	
Аутентифікація			
Аутентифікація			
Маска підмережі			
Інтервал привітання		Параметр	Пріоритет маршрутизатора
Інтервал простою			
Призначений маршрутизатор (DR)			
Резервний призначений маршрутизатор (DBR)			
Список сусідніх пристроїв			

До найважливіших полів, вказаних в таблиці, відносяться такі:

- Тип – визначення типу пакета. Число 1 означає пакет привітання. Число 2 позначає пакет DBD, 3 – пакет LSR, 4 – пакет LSU, а 5 – пакет LSAck.
- Ідентифікатор маршрутизатора – 32-бітове значення, представлене в десятковому записі з точками (подібно до IPv4), яке використовується для однозначної ідентифікації вихідного маршрутизатора.
 - Ідентифікатор області – номер області, з якої виходить пакет.
 - Маска підмережі – маска підмережі, що пов'язана з інтерфейсом.
 - Інтервал привітання (HelloInterval) – інтервал (у секундах), після якого маршрутизатор надсилає наступний пакет привітання. У мережах з множинним доступом інтервал стандартного привітання заданий зі значенням 10 секунд. У сусідніх маршрутизаторах повинен використовуватися той самий таймер, інакше відносини суміжності не встановлюються.
- Пріоритет маршрутизатора – використовується для вибору DR/BDR. За замовчанням для всіх маршрутизаторів OSPF встановлено пріоритет 1, однак можна його змінити, обравши значення у діапазоні від 0 до 255. Чим більше його значення, тим більша ймовірність, що маршрутизатор буде використовуватися як виділений маршрутизатор (DR) на цьому каналі.
- Інтервал простою (RouterDeadInterval) – інтервал (у секундах) маршрутизатор очікує сигнал від сусіднього пристрою, після якого сусідній

маршрутизатор визначається як «мертвий», що свідчить про його недієздатність. Зазвичай, чим вище значення інтервалу простою (встановленого вручну у діапазоні від 0 до 255), тим більше часу маршрутизатор чекає на сигнал від сусіда перед визнанням його недієздатним. У сусідніх маршрутизаторах повинен використовуватися той самий таймер, інакше не вийде встановити відносини суміжності.

- Виділений маршрутизатор (DR) – ідентифікатор маршрутизатора DR.
- Виділений резервний маршрутизатор (BDR) – ідентифікатор маршрутизатора BDR.
- Список сусідніх пристроїв – список, який визначає ідентифікатори всіх суміжних маршрутизаторів.

Інтервали надсилання пакетів привітання

Пакети привітання OSPF з наступними інтервалами:

- 10 секунд (за замовчуванням у мережах з множинним доступом та мережах типу «точка-точка»);
- 30 секунд (значення за замовчанням для мереж без ширококомовних розсилок з множинним доступом, наприклад Frame Relay).

Інтервал простою є інтервалом часу в секундах, протягом якого маршрутизатор очікує на отримання пакета привітання перед тим, як оголосити сусідній пристрій непрацюючим. Якщо інтервал простою закінчується до отримання маршрутизаторами пакета привітання, OSPF видаляє цей сусідній пристрій зі своєї бази даних станів каналів. Маршрутизатор виконує лавинну розсилку бази даних станів каналів, що містить дані про сусідній пристрій, що не працює, з усіх інтерфейсів, що використовують OSPF.

Наприклад, у пристроях Cisco інтервал простою дорівнює 4 інтервалам і використовує надсилання hello-пакетів:

- 40 секунд (за замовчуванням у мережах із множинним доступом та мережах типу «точка-точка»);
- 120 секунд (за замовчуванням у неширокомовних мережах множинного доступу, наприклад Frame Relay).

Оновлення стану каналу

Маршрутизатори спочатку обмінюються пакетами DBD (пакетами 2-го типу), тобто скороченими списками бази даних станів каналів відправляючого маршрутизатора, що використовуються маршрутизаторами для звірки з локальною базою даних станів каналів. [1]

Пакет LSR (пакет 3-го типу) використовується приймаючими маршрутизаторами для запиту додаткових даних про запис у пакеті DBD.

Пакет LSU (пакет 4-го типу) використовується для надсилання відгуку на отриманий пакет LSR.

Пакет 5-го типу використовується для підтвердження отримання LSU 4-го типу.

Пакети LSU також використовуються для пересилання оновлень маршрутизації OSPF, наприклад, даних про зміну каналу. Зокрема, пакет LSU може містити 11 різних типів об'яв стану каналу (LSA) протоколу OSPFv2, (табл. 2.3). Протокол OSPFv3 перейменував деякі з цих пакетів LSA і також містить два додаткові пакети LSA.

Таблиця 2.3 – Пакети LSA[5]

Тип LSA	Опис
1	Пакети LSA маршрутизатора
2	Пакети LSA мережі
3 або 4	Сумарні LSA
5	Пакети LSA зовнішньої автономної мережі
6	Пакети LSA багатонаддресної розсилки в середовищі OSPF
7	Визначаються для не повністю тупикових зон (not-so-stubby-area)
8	LSA зовнішніх атрибутів для протокола BGP
9, 10, 11	Непрозорі пакети LSA

Робочі стани OSPF

Під час першого підключення маршрутизатора OSPF до мережі він намагається:

- встановити відносини суміжності із сусідніми вузлами;
- здійснити обмін даними маршрутизації;
- розрахувати оптимальні маршрути;

- досягти стану збіжності.

Протокол OSPF проходить кілька станів у процесі досягнення збіжності: стан Down; стан Init, стан Two-Way, стан ExStart, стан Exchange, стан Loading, стан Full.

В таблиці 2.4 наведено перехід між станами OSPF

Таблиця 2.4 – Перехід між станами OSPF[1]

Встановлення відносин суміжності із сусідніми пристроями	Стан Down	• не отримано жодного пакета привітання; • маршрутизатор надсилає пакет привітання; • перехід в стан Init
	Стан Init	• пакети привітання надходять від сусідніх пристроїв; • вони містять ідентифікатор відправляючого маршрутизатора; • перехід в стан Two-Way
	Стан Two-Way	• в каналах Ethernet необхідно обрати виділений маршрутизатор (DR) і резервний призначений маршрутизатор (DBR); • перехід в стан ExStart
Синхронізація баз даних OSPF	Стан ExStart	• узгодження відносин основного та другорядного пристрою і порядкового номеру пакета DBD; • основний пристрій ініціює обмін пакетами DBD
	Стан Exchange	• маршрутизатори обмінюються пакетами DBD; • якщо потрібні дані про маршрутизатор, виконується перехід в стан Loading, в іншому випадку – в стан Full
	Стан Loading	• LSR і LSU використовуються для отримання додаткової інформації про маршрут; • маршрути обробляються за допомогою алгоритму пошуку найкоротшого шляху; • перехід в стан Full
	Стан Full	• маршрутизатори досягли стану збіжності

Встановлення відносин суміжності із сусідніми пристроями

Якщо протокол OSPF активовано на інтерфейсі, маршрутизатор має визначити наявність іншого сусіднього пристрою OSPF у каналі. Для цього

маршрутизатор висилає пакет привітання, який включає ідентифікатор маршрутизатора з усіх інтерфейсів, що підтримують OSPF. Ідентифікатор OSPF маршрутизатора використовується процесом OSPF для унікального визначення кожного маршрутизатора в межах області OSPF. Ідентифікатор маршрутизатора – 32-бітове число, відформатоване як IP-адреса та призначене для унікальної ідентифікації маршрутизатора серед однорангових пристроїв OSPF.

Якщо сусідній маршрутизатор, на якому активовано протокол OSPF, отримує пакет привітання з ідентифікатором маршрутизатора, який не знаходиться у списку сусідніх пристроїв, намагається встановити відносини суміжності з ініціюючим маршрутизатором.

Розглянемо на прикладі процес встановлення відносин суміжності (рис. 2.3).



Рисунок 2.3 – Перехід зі стану Down в стан Init [3]

На рис. 2.4 маршрутизатор R2 приймає пакет вітання від маршрутизатора R1 і додає ідентифікатор маршрутизатора R1 до свого списку сусідніх пристроїв. Після цього маршрутизатор R2 надсилає пакет вітання на маршрутизатор R1. Пакет містить ідентифікатор маршрутизатора R2 та маршрутизатора R1 у своєму списку сусідніх пристроїв на тому ж інтерфейсі.

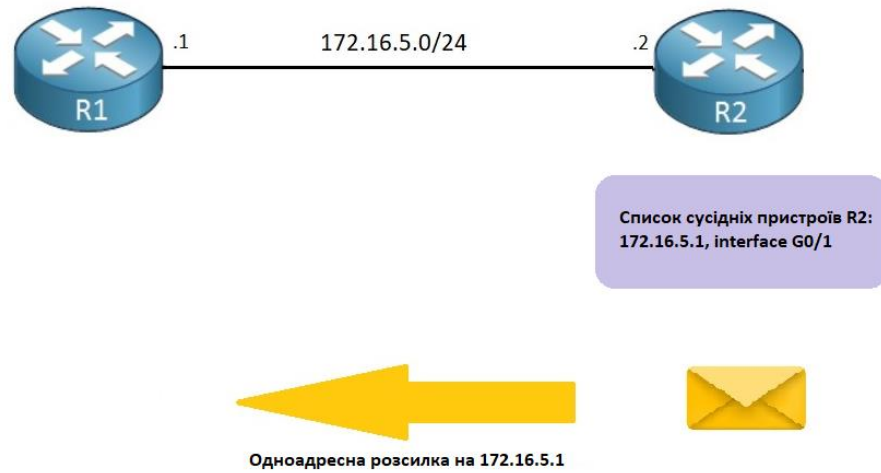


Рисунок 2.4 – Стан Init[3]

Потім маршрутизатор R1 приймає пакет вітання та додає ідентифікатор маршрутизатора R2 до свого списку сусідніх пристроїв OSPF. Він також бачить власний ідентифікатор маршрутизатора в пакеті вітання від сусідніх пристроїв. Коли маршрутизатор приймає пакет вітання, що містить його ідентифікатор у списку сусідніх пристроїв, він переходить зі стану Init до стану Two-Way. (рис. 2.5)

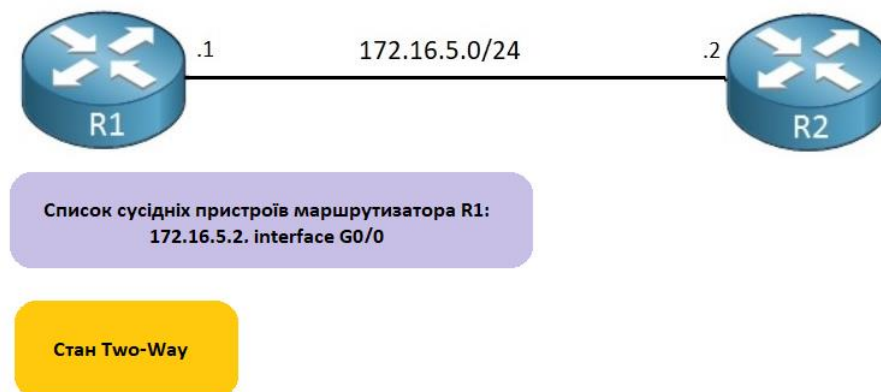


Рисунок 2.5 – Стан Two-Way[3]

Дія, яка виконується в стані Two-Way, визначається типом взаємодії між суміжними маршрутизаторами:

- Якщо два суміжні сусідні пристрої взаємодіють через канал типу «точка-точка», вони негайно переходять зі стану Two-Way у фазу синхронізації бази даних.

- Якщо маршрутизатори взаємодіють за допомогою спільної мережі Ethernet, необхідно обрати виділений маршрутизатор (DR) та резервний виділений маршрутизатор (BDR).

Оскільки маршрутизатори R1 і R2 взаємодіють через мережу Ethernet, обираються виділений маршрутизатор (DR) та резервний виділений маршрутизатор (BDR). Цей процес виконується лише у мережах множинного доступу (наприклад, мережах LAN стандарту Ethernet).

З метою оновлення даних маршрутизації здійснюється безперервний обмін пакетами вітання.

Виділений маршрутизатор (DR) та резервний виділений маршрутизатор (BDR)

- У мережах з багатьма точками доступу протокол OSPF може стикатися з двома проблемами, пов'язаними з масовим відправленням пакетів LSA.

- Встановлення великої кількості відносин суміжності. Мережі Ethernet можуть забезпечити потенційну взаємодію між численними маршрутизаторами OSPF через спільний канал. Здійснювати встановлення відносин суміжності із кожним маршрутизатором не є обов'язковим і навіть небажаним. Це може призвести до великої кількості пакетів LSA, які обмінюються маршрутизаторами в межах однієї мережі.

- Надмірна лавинна розсилка пакетів LSA. Маршрутизатори, що використовують протокол OSPF за станом каналу, відправляють свої пакети LSA в лавинному режимі при кожному запуску протоколу OSPF або у випадку зміни топології. Подібна масова розсилка може бути надто інтенсивною.

Щоб зрозуміти проблему, пов'язану з надмірним числом відносин суміжності, розглянемо таку формулу:

Для будь-якого числа маршрутизаторів (позначених як n) у мережі з множинним доступом буде $n(n - 1) / 2$ відносин суміжності.

Проблема управління великою кількістю відносин суміжності та лавинної розсилки пакетів LSA у мережах з множинним доступом це питання вирішується через призначення виділеного маршрутизатора (DR). Протокол

OSPF визначає маршрутизатор як DR, який виступає точкою збору та розповсюдження пакетів LSA, надісланих та отриманих. Також, для випадків відмови DR, обирається резервний маршрутизатор (BDR). Усі інші маршрутизатори отримують статус DROthers. Маршрутизатор DROTHER – це той, що не є або DR, або BDR.

Синхронізація баз даних OSPF

Після виходу зі стану Two-Way маршрутизатори переходять у стан синхронізації бази даних. Пакет привітання використовується для встановлення відносин суміжності із сусідніми пристроями, тоді як решта чотирьох типів пакетів OSPF використовуються в процесі обміну та синхронізації баз даних станів каналів.

У стані ExStart два маршрутизатори приймають рішення, який із них передаватиме пакети DBD першим. Маршрутизатор із вищим ідентифікатором маршрутизатора стає першим, що передає пакети DBD у стані Exchange.

У стані Exchange два маршрутизатори обмінюються одним або декількома пакетами DBD. Пакет DBD включає інформацію про заголовок запису LSA, який відображається в базі даних станів каналів маршрутизатора. Записи можуть містити дані про канал або мережу. Кожен заголовок запису LSA містить дані про тип стану каналу, адресу маршрутизатора, який оголошує, вартість каналу та порядковий номер. Маршрутизатор використовує порядковий номер для визначення актуальності даних про стан каналу.

На рис. 2.6 маршрутизатор R2 передає пакет DBD маршрутизатору R1. Коли маршрутизатор R1 отримує пакет DBD, він виконує такі дії:

- 1) Маршрутизатор підтверджує отримання пакета DBD за допомогою пакета LSAck.
- 2) Потім маршрутизатор R1 надсилає пакети DBD маршрутизатору R2.
- 3) Маршрутизатор R2 надсилає підтвердження маршрутизатору R1.

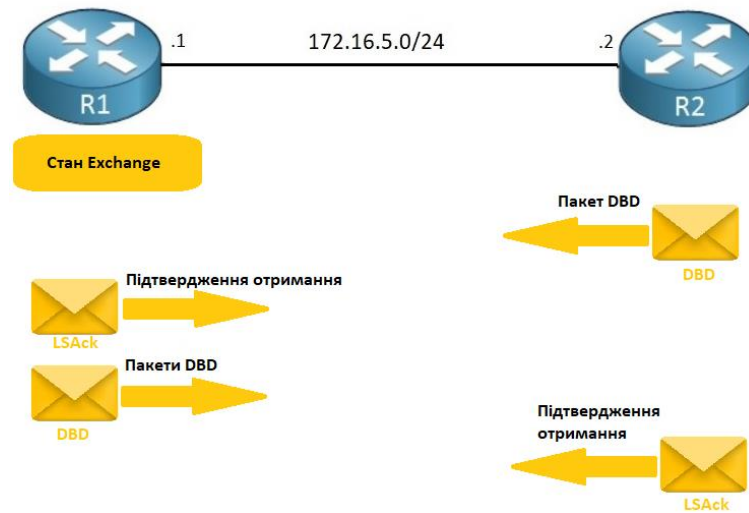


Рисунок 2.6 – Обмін пакетами DBD[3]

Маршрутизатор R1 порівнює отримані дані з даними, які містяться в його базі даних станів каналів. Якщо пакет DBD містить актуальніший запис про стан каналу, маршрутизатор переходить у стан Loading.

Наприклад, на рис. 2.7 маршрутизатор R1 відправляє пакет LSR з даними мережі 172.16.6.0 на маршрутизатор R2. Маршрутизатор R2 відправляє відповідь, що містить повні дані мережі 172.16.6.0, в пакеті LSU. Знову ж таки, коли маршрутизатор R1 приймає пакет LSU, він у відповідь відправляє пакет LSAck. Маршрутизатор R1 потім додає нові записи про стан каналу в свою базу даних станів каналів.

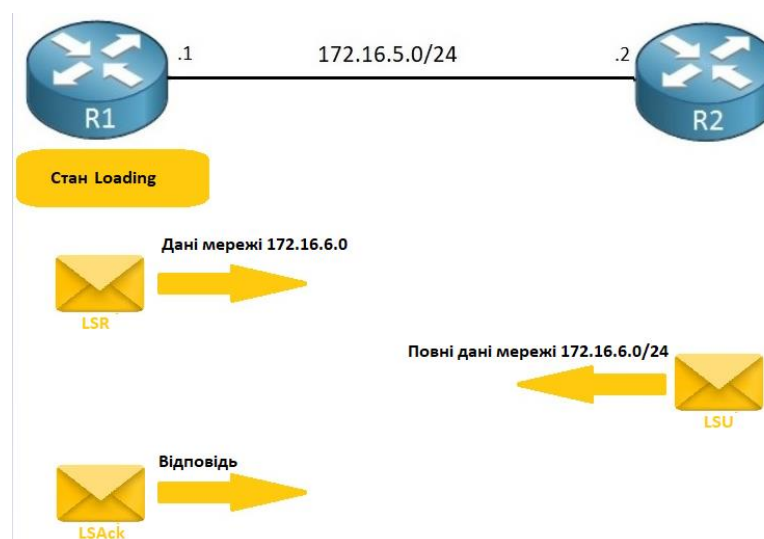


Рисунок 2.7 – Отримання додаткових даних про маршрут [3]

Після того, як на всі пакети LSR для даного маршрутизатора надіслано відповідь, суміжні маршрутизатори вважаються синхронізованими та переведеними у стан Full.

До тих пір, поки сусідні маршрутизатори будуть отримувати пакети привітання, дані про мережу, що містяться в переданих пакетах LSA, вони залишаються в базі даних топології. Після синхронізації топологічних баз даних оновлення (LSU) передаються лише сусіднім пристроям:

- коли виявляються зміни (інкрементні оновлення);
- через 30 хвилин.

2.2 Аналіз протоколу OSPF для кількох областей

Для підвищення ефективності і масштабованості, протокол OSPF підтримує ієрархічну маршрутизацію за допомогою областей [5]. Область OSPF являє собою групу маршрутизаторів, що використовують однакові дані про стан каналу у своїх базах даних наявних каналів.

Протокол OSPF можна використовувати одним із наступних способів:

- OSPF для однієї області (рис. 2.8) – усі маршрутизатори знаходяться в одній області, яка називається магістральною або нульовою областю (область 0).

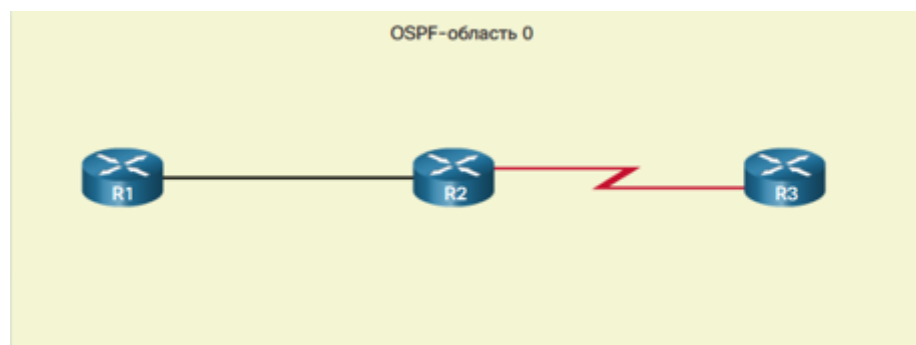


Рисунок 2.8 – OSPF для однієї області [1]

- OSPF для кількох областей (рис. 2.9) – протокол OSPF використовується для кількох областей в ієрархічному порядку. Усі області

мають бути підключені до магістральної області (область 0). Маршрутизатори, що з'єднують області, називаються граничними маршрутизаторами області (ABR). На рисунку – це маршрутизатори R1 та R2.

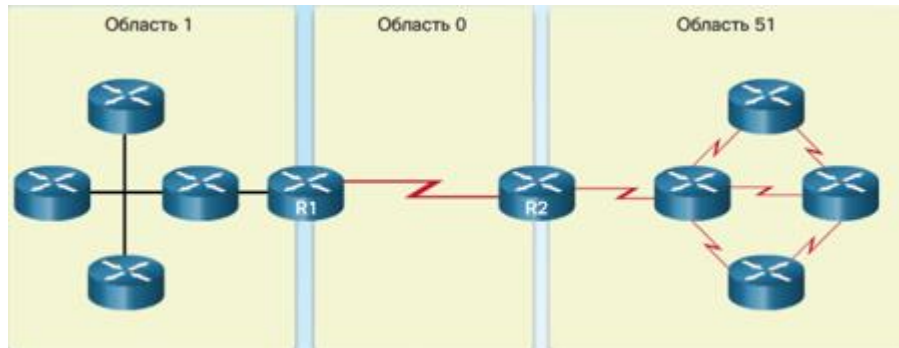


Рисунок 2.9 – OSPF для кількох областей [1]

OSPF для однієї області

Використання OSPF для однієї області є виправданим у невеликих мережах з простою системою каналів маршрутизаторів і маршрутів, які легко визначаються до конкретних вузлів призначення. Але якщо область стає занадто великою, виникають наступні проблеми.

- Велика таблиця маршрутизації – OSPF не агрегує автоматично маршрути за замовчуванням. Якщо агрегація маршрутів не відбувається, таблиця маршрутизації може значно збільшитися в залежності від розміру мережі.
- Велика база даних на основі стану каналу (LSDB) – в OSPF для однієї області база LSDB містить відомості для топології всього домену маршрутизації. Кожен маршрутизатор повинен зберігати докладну інформацію про кожен мережу домену маршрутизації.
- Часті розрахунки алгоритму SPF – великі мережі часто піддаються змінам, що призводить до значного витрачання ресурсів процесора маршрутизаторами на перерахунок алгоритму SPF та оновлення таблиці маршрутизації.

Щоб підвищити ефективність та масштабованість, протокол OSPF підтримує ієрархічну маршрутизацію з використанням областей. Область OSPF

– це група маршрутизаторів, які спільно використовують такі ж дані про стан каналів у своїх базах даних.

OSPF для кількох областей

Поділ великої області OSPF на області меншого розміру називається OSPF для кількох областей. Використання OSPF для кількох областей є доцільним у більш великих мережах, що дозволить зменшити споживання ресурсів ЦП та пам'яті.

Наприклад, при кожній зміні топологічних даних, таких як додавання, видалення або зміна каналу, маршрутизатор повинен знову виконати алгоритм SPF, створити нове дерево SPF і оновити таблицю маршрутизації. Оскільки алгоритм SPF вимагає значних ресурсів центрального процесора, час, необхідний для виконання цих розрахунків, залежить від розміру області. Занадто велика кількість маршрутизаторів в одній області збільшує розмір бази даних LSDB та навантаження на ЦП. Отже, розподіл маршрутизаторів по областях дозволяє розділити одну велику базу даних на кілька баз даних меншого розміру, якими легко управляти.

У випадку OSPF для кількох областей потрібна ієрархічна структура мережі. Головна область називається магістральною областю (область 0, рис. 2.9), проте інші області повинні підключатися до неї. При використанні ієрархічної маршрутизації, маршрутизація, як і раніше, виконується між областями (називається міжобласною маршрутизацією). Проте перерахунок алгоритму SPF, для якого потрібно багато ресурсів ЦП, виконується лише для маршрутів всередині області. У разі зміни конфігурації в одній області алгоритм SPF не перераховується в інших областях.

Ієрархічна топологія OSPF для кількох областей забезпечує наступні переваги:

- Таблиці маршрутизації меншого розміру. Число записів у таблиці маршрутизації зменшується, оскільки мережеві адреси в областях можуть бути об'єднані. Крім того, маршрутизатори в одній області для адрес за межами свого призначення повинні використовувати тільки маршрут за замовчуванням. Наприклад, маршрутизатор R1 поєднує маршрути з області 1 в область 0, а

маршрутизатор R2 – маршрути з області 51 в область 0. Маршрутизатори R1 і R2 також розповсюджують статичний маршрут за замовчуванням в область 1 та 51 (рис. 2.9).

- Скорочення витрат ресурсів для передачі оновлень стану каналів. Вимоги до процесора та пам'яті зводяться до мінімуму за рахунок меншого числа маршрутизаторів, які обмінюються повідомленнями LSA з детальною інформацією про топологію.

- Зниження частоти розрахунків SPF. Вплив змін топології локалізується у межах області. Наприклад, мінімізується вплив оновлень маршрутизації, оскільки лавинне розсилання повідомлень LSA зупиняється на межі області.

Припустимо, відмовив канал між двома внутрішніми маршрутизаторами області 51 (рис. 2.9). Тільки маршрутизатори області 51 обмінюються повідомленнями LSA, для чого потрібно повторне виконання алгоритму SPF. Маршрутизатор R1 отримує інший тип LSA з 51 області і не перераховує алгоритм SPF.

OSPF реалізує сувору дворівневу ієрархію областей. Фізична структура мережі, що використовується, повинна відповідати дворівневій структурі областей, причому всі немагістральні області повинні мати пряме підключення до області 0. Увесь трафік, що направляється з однієї області в іншу, має проходити через магістральну область. Такий трафік називається міжобласним.

Оптимальна кількість маршрутизаторів у кожній області залежить від низки чинників, таких як стійкість мережі, проте компанія Cisco рекомендує дотримуватися таких умов [12]:

- Область не повинна містити понад 50 маршрутизаторів.
- Маршрутизатор не повинен перебувати більш ніж у 3 областях.
- Кількість сусідніх маршрутизаторів для будь-якого окремого маршрутизатора не повинна перевищувати 60.

Типи маршрутизаторів OSPF

Маршрутизатори OSPF різних типів дозволяють керувати трафіком, який передається в область та з області. Маршрутизатори OSPF класифікуються на основі функції, яку вони виконують у домені маршрутизації.

Існує чотири різні типи маршрутизаторів OSPF (рис. 2.10)

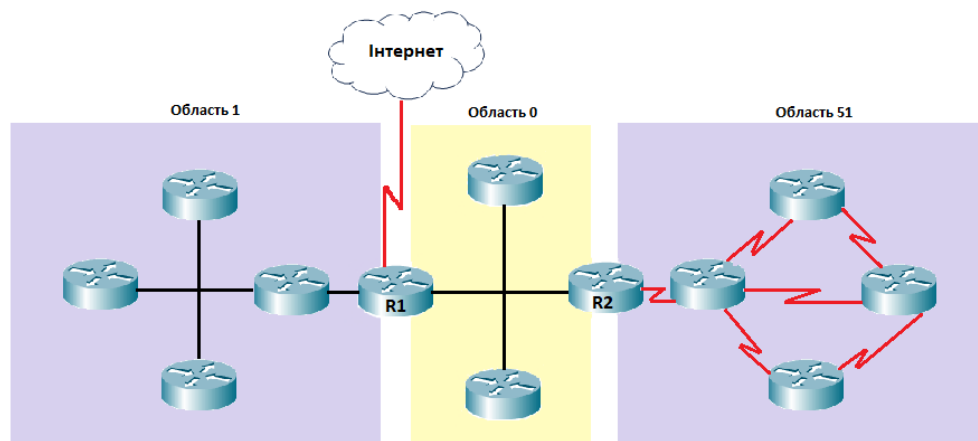


Рисунок 2.10 – Типи маршрутизаторів по областях[3]

- Внутрішній маршрутизатор – це маршрутизатор, усі інтерфейси якого знаходяться в одній області. Усі внутрішні маршрутизатори області мають однакові бази даних станів каналів, LSDB. На рис. 2.10 – це всі маршрутизатори, розташовані всередині областей 1, 0 та 51.
- Магістральний маршрутизатор – це маршрутизатор, який знаходиться в магістральній області. Магістральна область – це область 0. На рис. 2.10 це маршрутизатори R1 і R2 та 2 інших маршрутизатора всередині області 0.
- Граничний маршрутизатор області (ABR) – це маршрутизатор, інтерфейси якого підключено до кількох областей. Він повинен вести бази LSDB окремо для кожної області, до якої він підключений, і може виконувати маршрутизацію між областями. Граничні маршрутизатори виконують функції точок входу/виходу цієї області. Це означає, що інформація про маршрути, адресована іншій області, може надсилатися лише через граничний маршрутизатор локальної області. Граничні маршрутизатори можуть бути налаштовані для об'єднання даних про маршрути з бази LSDB відповідних

підключених областей. Граничні маршрутизатори розповсюджують дані про маршрути до магістральної області. Потім магістральні маршрутизатори передають інформацію іншим маршрутизаторам ABR. У мережі з кількома областями область може знаходитись один або кілька граничних маршрутизаторів. На рис. 2.10 – це маршрутизатори R1 і R2.

- Граничний маршрутизатор автономної системи (ASBR) – це маршрутизатор, який має принаймні один інтерфейс підключений до зовнішньої об'єднаної мережі. Зовнішня мережа – це мережа, яка не входить до домену маршрутизації OSPF. Приклад – мережеве з'єднання з інтернет-провайдером. Граничний маршрутизатор автономної системи може імпортувати інформацію про зовнішню мережу в мережу OSPF і навпаки, використовуючи процес, який називається перерозподілом маршрутів. На рис. 2.10 – це маршрутизатор R1.

Реалізація OSPF для кількох областей

OSPF можна реалізувати як протокол для однієї області або кількох областей. Вибраний тип реалізації OSPF залежить від конкретних вимог до проектування мереж та існуючої топології.

Реалізація OSPF для кількох областей складається з 4 кроків [13].

Етапи 1 та 2 є частиною процесу планування.

Етап 1. Збір вимог до мережі та мережевих параметрів. Сюди входить визначення числа вузлів та мережевих пристроїв, схеми IP-адресації (якщо вона вже створена), розміру домену маршрутизації, розміру таблиць маршрутизації, ризику змін топології, підтримки OSPF існуючими маршрутизаторами та іншими характеристиками мережі.

Етап 2. Визначення параметрів OSPF. На основі отриманої інформації на першому етапі., необхідно визначити кращий варіант OSPF – для однієї області або кількох областей. Якщо обрано варіант OSPF для кількох областей, необхідно, визначаючи параметри OSPF, врахувати ряд особливостей, а саме:

- План IP-адресації. Цей план визначає можливості розгортання OSPF та масштабування його розгортання. Необхідно розробити вичерпний план IP-адресації, який включатиме дані про IP-підмережі. Ефективний план IP-

адресації повинен ураховувати застосування архітектури та використання OSPF для організації кількох областей. Цей план полегшує масштабування мережі, а також оптимізує роботу OSPF та розповсюдження LSA.

- Області OSPF. Розділення мережі OSPF в області зменшує розмір бази LSDB і обмежує передачу оновлень станів каналів у випадку зміни топології. Необхідно визначити, які маршрутизатори виконуватимуть ролі ABR та ASBR та які з маршрутизаторів ABR та ASBR мають здійснювати об'єднання чи перерозподіл.

- Топологія мережі. Ця структура включає канали, які з'єднують різні елементи мережевого обладнання та приналежать різним областям OSPF в архітектурі OSPF для кількох областей. Топологія мережі є ключовою для визначення основних та резервних каналів. Основні та резервні канали визначаються зміною вартості OSPF для інтерфейсів. Якщо використовується OSPF для кількох областей, докладну топологію мережі також слід використовувати для ідентифікації різних областей OSPF, маршрутизаторів ABR та ASBR, а також точок об'єднання та перерозподілу.

Етап 3. Налаштування реалізації OSPF для кількох областей виходячи із заданих параметрів.

Етап 4. Перевірка реалізації OSPF для кількох областей виходячи із заданих параметрів.

2.3 Базові налаштування OSPF на маршрутизаторах Cisco

Налаштування OSPF на маршрутизаторах Cisco включає кілька кроків [1]. Спочатку необхідно *визначити OSPF процес на маршрутизаторі*. Для цього вводиться з режиму глобальної конфігурації команда:

```
Router(config)# router ospf [process-id]
```

Значенням process-id є число від 1 до 65535, яке обирається мережевим адміністратором. Значення process-id використовується локально, тобто воно не обов'язково повинно збігатися з відповідним значенням на інших маршрутизаторах OSPF, щоб між ними встановилися відносини суміжності.

Також для включення домену маршрутизації OSPF всім маршрутизаторам потрібен *ідентифікатор*.

Він задається адміністратором або автоматично призначається маршрутизатором. Маршрутизатор з підтримкою протоколу OSPF використовує ідентифікатор у таких цілях:

- Унікальна ідентифікація маршрутизатора – ідентифікатор маршрутизатора використовується іншими маршрутизаторами для унікальної ідентифікації в межах домену OSPF кожного з маршрутизаторів, а також усіх пакетів, що надходять від них.
- Участь у виборі маршрутизатора DR – у мережі LAN множинного доступу вибір маршрутизатора DR здійснюється під час початкової організації мережі OSPF. У разі активації каналів OSPF пристрій маршрутизації, для якого налаштовано найвищий пріоритет, призначається маршрутизатором DR. Якщо пріоритет не налаштований або він співпадає, маршрутизатор із найвищим значенням ідентифікатора вибирається маршрутизатором DR. Пристрій маршрутизації з наступним ідентифікатором вибирається як маршрутизатор BDR.

Для налаштування ідентифікатора потрібно ввести команду:

```
Router(config)# router-id rid
```

Значення *rid* – це будь-яке 32-розрядне число у форматі IPv4 адреси.

Ввімкнення OSPF на інтерфейсах

Необхідно визначити, які інтерфейси беруть участь у процесі маршрутизації області OSPF. Вказівка маршрутизатору про свою мережу означає додавання мережевої інформації до таблиці OSPF. Це робиться за допомогою команди *network* в режимі конфігурації OSPF:

```
Router(config-router)# network [network-id] [wildcard-mask] area [area-id]
```

network-id – це адреса IP мережі, *wildcard-mask* – маска підмережі в зворотному форматі, *area-id* – ідентифікатор області OSPF.

При налаштуванні конфігурації OSPF для однієї області команда *network* повинна використовуватися з одним і тим же значенням *area-id* на всіх маршрутизаторах.

Якщо маршрутизатор налаштовується у якості **DR/BDR** – вводиться наступна команда:

```
Router(config-router)# ip ospf priority [priority]
```

priority – це пріоритет (значення від 0 до 255). Більше значення означає вищий пріоритет. За замовчуванням, всі маршрутизатори мають пріоритет 1.

Для правильного налаштування інтерфейсів для OSPF на слід вказати, які інтерфейси беруть участь у процесі OSPF та в якій області вони знаходяться. Для цього використовуються такі команди:

```
Router(config)# interface [interface_type] [interface_number]
```

```
Router(config-if)# ip ospf [process_id] area [area_id]
```

- *interface_type*: тип інтерфейсу, такий як Ethernet, GigabitEthernet, Serial тощо.
- *interface_number*: номер конкретного інтерфейсу.
- *process_id*: ідентифікатор процесу OSPF, який використовується на даному маршрутизаторі.
- *area_id*: ідентифікатор області OSPF, в яку включається цей інтерфейс.

Розрахунок вартості OSPF

OSPF використовує метрику визначення оптимального шляху пакета в мережі. В даному контексті, метрика вказує на те, яке навантаження очікується при транспортуванні пакетів через конкретний інтерфейс. Протокол OSPF використовує термін «вартість» для визначення метрики. Шлях із меншою вартістю розглядається як оптимальний у порівнянні з тим, який має більшу вартість.

Вартість інтерфейсу обернено пропорційна його пропускній здатності. Отже, більш висока пропускна здатність свідчить про нижчу вартість. Більш високе навантаження і значення затримки часу вказують на більш високу вартість. Отже, лінія Ethernet 10 Мбіт/с має більшу вартість, чим лінія Ethernet 100 Мбіт/с.

Формула розрахунку вартості OSPF:

- $\text{Вартість} = \frac{\text{еталонна пропускна спроможність}}{\text{пропускна спроможність інтерфейсу}}$

Задана пропускна здатність дорівнює за замовчанням 10^8 (100000000).

Отже, потрібно використати наступну формулу розрахунку:

- $\text{Вартість} = \frac{100\,000\,000 \text{ біт/с}}{\text{пропускна спроможність інтерфейсу в біт/с.}}$

Перевірка стану OSPF

Команду `show ip ospf neighbor` використовують для перевірки встановлення маршрутизатором відносин суміжності із сусідніми маршрутизаторами. Якщо ідентифікатор сусіднього маршрутизатора не відображається, або стан цього маршрутизатора не є FULL, це означає, що ці маршрутизатори не встановили відносини суміжності OSPF.

Команда `show ip protocols` забезпечує швидку перевірку критично важливих конфігураційних даних OSPF. До них належать ідентифікатор процесу OSPF, ідентифікатор маршрутизатора, мережі, що оголошуються маршрутизатором, сусідні пристрої, від яких маршрутизатор отримує оновлення, та адміністративна відстань за замовчанням, яка дорівнює 110 для протокола OSPF.

Команду `show ip ospf` можна також використовувати для перевірки ідентифікатора процесу та ідентифікатора маршрутизатора в протоколі OSPF. Ця команда відображає дані області OSPF та показує час останнього розрахунку алгоритму SPF.

2.4 Висновки з розділу 2

В даному розділі було детально проаналізовано протокол OSPF, його принцип роботи та базові налаштування, зроблено наступні висновки:

- 1) Протокол OSPF представляє собою ефективну альтернативу протоколу маршрутизації за векторами відстані RIP, який використовувався на ранніх етапах розвитку мережевих технологій. Завдяки безкласовості та

використанню концепції областей, OSPF забезпечує швидшу збіжність та масштабованість, що робить його ефективним рішенням для великих мереж.

2) Компоненти протоколу OSPF включають базу даних суміжності, базу даних на основі стану каналу (LSDB) та базу даних пересилання. Ці компоненти дозволяють маршрутизаторам обмінюватися даними маршрутизації та будувати оптимальні маршрути.

3) Принцип роботи OSPF включає етапи встановлення відносин суміжності, обміну оголошеннями про стан каналу, створення таблиці топології та виконання алгоритму пошуку найкоротшого шляху SPF. Цей процес сприяє досягненню стану збіжності та побудові оптимальних маршрутів для подальшого використання в таблиці маршрутизації. Загальною вагомою особливістю OSPF є його здатність до масштабування та ефективного використання ресурсів мережі, забезпечуючи швидкість збіжності та надійність маршрутизації. Це робить протокол OSPF популярним і ефективним інструментом для розбудови та управління сучасними комплексними корпоративними мережами.

4) Протокол OSPF використовує різні типи пакетів для забезпечення ефективного обміну інформацією та встановлення відносин суміжності між маршрутизаторами. Кожен тип пакета має конкретне призначення у процесі маршрутизації OSPF.

5) Встановлення відносин суміжності між маршрутизаторами в OSPF є критичним етапом для ефективного обміну даними маршрутизації та побудови актуальних таблиць топології. Детально розглянуто приклад встановлення відносин суміжності та етапи зміни станів від Down до Init, Init до Two-Way, і подальший вибір виділених маршрутизаторів (DR, BDR) у мережах Ethernet.

6) Синхронізація баз даних OSPF включає важливі етапи, які забезпечують узгодженість інформації між сусідніми маршрутизаторами. Процес синхронізації проходить кілька станів, таких як ExStart, Exchange і Loading. Після успішної синхронізації маршрутизатори переходять у стан Full, в якому вони вважаються повністю синхронізованими.

7) OSPF для однієї області є ефективним у невеликих мережах з простою топологією. Проте, при збільшенні розміру мережі виникають проблеми, такі як велика таблиця маршрутизації і база даних стану каналу та часті розрахунки алгоритму SPF. Основним рішенням для подолання цих проблем є використання OSPF для кількох областей. Ієрархічна структура мережі з декількома областями забезпечує зменшення розміру таблиці маршрутизації, витрат ресурсів для передачі оновлень стану каналу та зниження частоти розрахунків алгоритму SPF. Поділ великої мережі на області дозволяє покращити ефективність та масштабованість OSPF. Хоча це вимагає ієрархічної структури та дотримання певних правил, таких як обов'язкове підключення всіх областей до магістральної області, але це дозволяє управляти розміром таблиць маршрутизації та збільшує ефективність роботи протоколу OSPF в розширених мережах.

8) Розглянуто процес налаштування OSPF на маршрутизаторах Cisco і визначено, що він складається з кількох важливих кроків, які дозволяють забезпечити оптимальну роботу протоколу в мережі. Ці кроки включають в себе визначення OSPF процесу на маршрутизаторі, включення маршрутизатора до домену маршрутизації OSPF, включення OSPF на інтерфейсах, що беруть участь у процесі маршрутизації області OSPF, налаштування пріоритету інтерфейсів для визначення DR та BDR, визначення вартості OSPF для розрахунку оптимального маршруту.

3 АНАЛІЗ ПРОТОКОЛУ ВНУТРІШНЬОЇ МАРШРУТИЗАЦІЇ EIGRP В IP-МЕРЕЖАХ

3.1 Характеристики та функції протоколу EIGRP

Протокол EIGRP (Enhanced Interior Gateway Routing Protocol) представляє собою вдосконалену систему внутрішньої маршрутизації на основі векторів відстані, розроблену компанією Cisco Systems. EIGRP є еволюцією іншого протоколу маршрутизації від Cisco – протоколу внутрішньої маршрутизації (IGRP). IGRP представляє собою застарілий протокол маршрутизації, що ґрунтується на класах та векторах відстані.

EIGRP також включає функції протоколів маршрутизації з урахуванням стану каналу. EIGRP підходить для багатьох різних топологій і середовищ. В якісно спроектованій мережі EIGRP може масштабуватись для інтегрування різних топологій, та може забезпечити дуже швидку збіжність з мінімальним обсягом мережевого трафіку.

Протокол EIGRP з'явився в 1992 році як пропрієтарний протокол, тобто доступний лише на пристроях Cisco. Але в 2013 році Cisco представила ключові функції протоколу EIGRP у формі відкритого стандарту, опублікувавши їх в інформаційному документі RFC для організації IETF. Це означає, що інші виробники мережевого обладнання можуть використовувати EIGRP на своїх пристроях для взаємодії з маршрутизаторами Cisco та іншими виробниками, які підтримують протокол EIGRP. Але додаткові функції EIGRP, наприклад тупикова мережа EIGRP, необхідні для розгортання динамічної віртуальної багатоточкової приватної мережі (DMVPN), не представлені в IETF. Компанія Cisco продовжує підтримку EIGRP у вигляді інформаційного документа RFC.

Протокол EIGRP об'єднує в собі характеристики як протоколів маршрутизації зі станом каналів, так і протоколів з використанням векторів відстані. Але EIGRP все ж ґрунтується на ключовому принципі протоколу маршрутизації на основі векторів відстані, що передбачає, що інформація про інші частини мережі отримується від сусідніх маршрутизаторів, що безпосередньо з'єднані з поточним маршрутизатором.

EIGRP – це вдосконалений протокол маршрутизації на основі векторів відстані, який включає у себе функції, недоступні в інших протоколах маршрутизації на основі векторів відстаней, таких як RIP та IGRP.

Протокол EIGRP підтримує наступні функції:

- *Алгоритм дифузного оновлення.* Алгоритм дифузного оновлення (DUAL) – механізм розрахунків, на яких заснована робота EIGRP, тому він займає центральне місце у цьому протоколі маршрутизації. Алгоритм DUAL гарантує відсутність петель у маршрутах та наявність альтернативних маршрутів для всього домену маршрутизації. Завдяки DUAL, протокол EIGRP зберігає всі наявні резервні маршрути до мереж призначення, що дозволяє швидко переключатися на запасні маршрути у випадку потреби.
- *Встановлення відносин суміжності із сусідніми пристроями.* EIGRP встановлює зв'язки з безпосередньо підключеними маршрутизаторами, які також підтримують EIGRP. Відносини суміжності із сусідніми пристроями використовуються для відстеження статусу сусідніх пристроїв.
- *Надійний транспортний протокол (RTP).* Протокол RTP використовується лише в EIGRP і забезпечує доставку пакетів EIGRP сусіднім пристроям. RTP та відстеження відносин суміжності із сусідніми пристроями утворюють основу для функціонування алгоритму DUAL..
- *Часткові та обмежені оновлення.* Оновлення в EIGRP бувають частковими та обмеженими. На відміну від RIP, протокол EIGRP не регулярно відправляє оновлення, і записи маршрутів не застарівають. Термін «часткові» означає, що оновлення містить лише дані про зміни маршрутів, наприклад, про новий канал або про канал, що став недоступним. Термін «обмежені» стосується поширення часткових оновлень, які надсилаються тільки тим маршрутизаторам, на функціонування котрих впливають ці зміни, що зменшує вимоги до пропускної здатності, необхідної для передачі оновлень EIGRP.
- *Розподіл навантаження з рівною та нерівною вартістю.* EIGRP підтримує розподіл навантаження з рівною та нерівною вартістю, що допомагає адміністраторам оптимізувати потік трафіку у своїх мережах.

Важливо відзначити, що у деяких старих документах стосовно EIGRP може зустрічатися термін «гібридний протокол маршрутизації». Однак це може вводити в оману, оскільки EIGRP не є гібридом між протоколами на основі векторів відстані та протоколами маршрутизації з урахуванням стану каналів. Слід зауважити, що Cisco більше не використовує цей термін для характеристики протоколу. [1].

Розглянемо функції протоколу EIGRP детальніше.

Протоколожалежні модулі

EIGRP може виконувати маршрутизацію для різних протоколів, включаючи IPv4 та IPv6. Для цього EIGRP використовує модулі окремих протоколів (PDM). Модулі PDM також застосовувалися для підтримки застарілих протоколів мережевого рівня – IPX компанії Novell і AppleTalk компанії Apple Computer.

Модулі PDM відповідають за виконання завдань, що пов'язані з конкретним протоколом мережевого рівня. Наприклад, модуль EIGRP призначений для передачі та отримання пакетів EIGRP, які інкапсулюються в IPv4. Цей модуль також виконує аналіз пакетів EIGRP та передає отримані нові дані в алгоритм DUAL. Протокол EIGRP використовує алгоритм DUAL для ухвалення рішень щодо маршрутизації, проте його вихідні дані зберігаються в таблиці маршрутизації IPv4.

Модулі PDM виконують конкретні завдання маршрутизації для кожного протоколу мережного рівня:

- ведення для маршрутизаторів EIGRP таблиць сусідніх пристроїв та топології, що належать до цієї групи протоколів;
- створення пакетів для конкретного протоколу та їх подальше перетворення за допомогою алгоритму DUAL;
- забезпечення взаємодії між алгоритмом DUAL та таблицею маршрутизації конкретного протоколу;
- обчислення метрики та передача цих відомостей до алгоритму DUAL;
- реалізація списків фільтрації та доступу;

- виконання функцій перерозподілу між EIGRP та іншими протоколами маршрутизації;
- перерозподіл маршрутів, одержаних іншими протоколами маршрутизації.

Після виявлення нового сусіднього пристрою, маршрутизатор вносить запис, який включає адресу та інтерфейс сусіднього пристрою, в таблицю сусідів. Кожен модуль, що залежить від протоколу, наприклад IPv4, управляє своєю власною таблицею сусідів. Для протоколу EIGRP також ведеться окрема таблиця топології, яка містить всі мережі призначення, що були оголошені сусідніми маршрутизаторами. Таблиці топології також підтримуються окремо для кожного PDM.

Надійний транспортний протокол (RTP)

Навіть за наявності слова «надійний» у назві RTP, цей протокол забезпечує як надійну, так і ненадійну доставку пакетів EIGRP, аналогічно до TCP і UDP відповідно. Якщо пакет RTP є надійним, відправник очікує підтвердження від одержувача. Для ненадійного пакета RTP підтвердження не потрібне. Наприклад, пакет оновлення EIGRP надсилається по RTP надійним способом і вимагає підтвердження. Пакет привітання EIGRP також надсилається по RTP, але ненадійним чином. Це означає, що пакети привітання EIGRP не потребують підтвердження.

RTP може надсилати пакети EIGRP, використовуючи одноадресну передачу або групову розсилку.

- У пакетах групової розсилки EIGRP для IPv4 використовується зарезервована IPv4-адреса групової розсилки 224.0.0.10.
- Пакети групової розсилки EIGRP для IPv6 надсилаються на зарезервовану IPv6-адресу FF02::A.

Аутентифікація

Так само, як і для інших протоколів маршрутизації, EIGRP може використовувати налаштування аутентифікації. Для кожного з протоколів, таких як RIPv2, EIGRP, OSPF, IS-IS і BGP, може бути встановлена аутентифікація відповідно до інформації про маршрути.

Рекомендується використовувати аутентифікацію для передачі інформації про маршрути. Це забезпечить, що маршрутизатори будуть приймати інформацію про маршрути тільки в разі, якщо на цих маршрутизаторах встановлено однаковий пароль або параметри аутентифікації. [14].

Але аутентифікація не забезпечує шифрування оновлень маршрутизації EIGRP.

Типи пакетів EIGRP

Протокол EIGRP застосовує п'ять типів пакетів, і деякі з них використовуються парами. Пакети EIGRP передаються за допомогою або надійної або ненадійної доставки. Пакети RTP для передачі можуть відправлятися як одноадресні, групові або в обидва способи. Ці види пакетів EIGRP часто називають форматами або повідомленнями EIGRP.

В таблиці 3.1 наведено типи пакетів, їх призначення та спосіб відправки

Таблиця 3.1 – Типи пакетів[3]

Тип пакету	Призначення	Спосіб доставки
Пакети привітання	Для виявлення сусідніх маршрутизаторів та підтримки відносин суміжності з сусідніми маршрутизаторами.	• Надсилаються за допомогою ненадійної доставки. • Групова розсилка (для більшості типів мереж).
Пакети оновлень	Передають дані про маршрути сусіднім пристроям EIGRP.	• Надсилаються за допомогою надійної доставки. • Одноадресна передача або групова розсилка.
Пакети підтверджень	Для підтвердження отримання EIGRP повідомлення, відправленого за допомогою надійної доставки.	• Надсилаються за допомогою ненадійної доставки. • Індивідуальна розсилка.
Пакети запитів	Використовуються для запиту маршрутів із сусідніх пристроїв.	• Надсилаються за допомогою надійної доставки. • Одноадресна передача або групова розсилка.
Пакети відповідей	Надсилаються у відповідь на запит EIGRP.	• Надсилаються за допомогою надійної доставки. • Індивідуальна розсилка.

На рис. 3.1 і рис. 3.2 показано, що EIGRP повідомлення зазвичай інкапсулюються в пакети IPv4 або IPv6. Повідомлення EIGRP для IPv4 використовують IPv4 як протокол мережевого рівня. Щоб вказати, що частина даних пакета є повідомленням EIGRP для IPv4, в полі IPv4 використовується значення 88. Повідомлення EIGRP для IPv6 інкапсулюються в пакети IPv6, використовуючи наступне поле заголовка зі значенням 88. Аналогічно з полем протоколу для IPv4, наступне поле заголовка IPv6 містить тип даних, які передаються в пакеті IPv6.

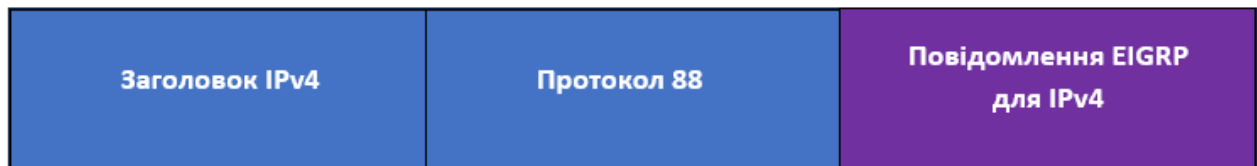


Рисунок 3.1 – Інкапсуляція EIGRP повідомлення для IPv4 [1]

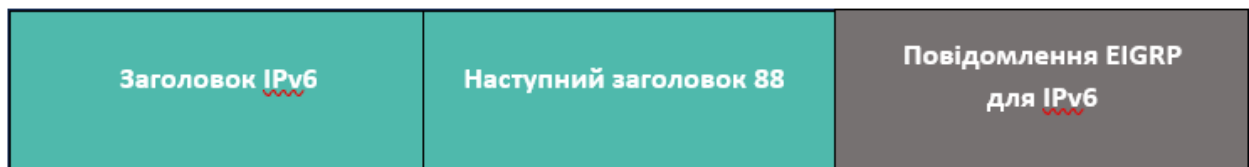


Рисунок 3.2 – Інкапсуляція EIGRP повідомлення для IPv6 [1]

Пакети привітання EIGRP

EIGRP використовує невеликі пакети привітання в каналах, що безпосередньо підключені, для виявлення інших маршрутизаторів з увімкненою підтримкою EIGRP. Пакети привітання використовуються маршрутизаторами для створення відносин суміжності із сусідніми пристроями EIGRP.

Пакети привітання EIGRP надсилаються як групові розсилки IPv4 або IPv6 і використовують ненадійну доставку RTP. Це означає, що одержувач не надсилає у відповідь пакет підтвердження.

Як вже зазначалося, зарезервованою адресою групової розсилки EIGRP для IPv4 є 224.0.0.10, а для IPv6 – FF02::A.

За допомогою пакетів привітання маршрутизатори EIGRP виявляють сусідні пристрої та встановлюють відносини суміжності із сусідніми маршрутизаторами. У більшості сучасних мереж пакети привітання EIGRP відправляються на групову адресу кожні 5 секунд. Але в мережах «точка-багатоточка» із множинним доступом без можливості широкошовного розсилання (NBMA), з каналами доступу T1 (1,544 Мбіт/с) або повільнішими, пакети привітання відправляються за однією адресою кожні 60 секунд. До мереж NBMA з повільнішими інтерфейсами відносяться застарілі мережі X.25, Frame Relay та ATM (режим асинхронної передачі). [15]

В EIGRP пакети привітання також використовуються для підтримки встановлених відносин суміжності. З точки зору маршрутизатора EIGRP, поки надходять пакети привітання від сусіднього маршрутизатора, сусідній маршрутизатор та маршрути, які він використовує, продовжують функціонувати.

Протокол EIGRP використовує таймер утримання для визначення максимального періоду очікування, під час якого маршрутизатор очікує отримання наступного пакету привітання., перш ніж відповідний сусідній маршрутизатор буде оголошено недоступним. За замовчуванням, час утримання рівний трьом інтервалам передачі пакетів привітання, що становить 15 секунд для більшості мереж та 180 секунд в низькошвидкісних мережах NBMA. Після закінчення часу утримання EIGRP визнає маршрут неактивним, і алгоритм DUAL розпочинає пошук нового шляху, ініціюючи відповідні запити.

В таблиці 3.2 наведено значення за замовчуванням для інтервалів привітання і часу утримання для EIGRP.

Таблиця 3.2 – Значення за замовчуванням для інтервалів EIGRP[16]

Пропускна спроможність	Приклад каналу	Інтервал привітання за замовчуванням	Час утримання за замовчуванням
1,544 Мбіт/с	Багатоточковий Frame Relay	60 секунд	180 секунд
Більш ніж 1,544 Мбіт/с	T1, Ethernet	5 секунд	15 секунд

Пакети оновлень EIGRP

EIGRP передає пакети оновлень, для розповсюдження інформації про маршрути. Пакети оновлень надсилаються лише у разі потреби. Оновлення EIGRP містять лише необхідну інформацію про маршрути і надсилаються лише маршрутизаторам, яким потрібні ці оновлення.

На відміну від старого протоколу маршрутизації на базі векторів відстані RIP, протокол EIGRP не здійснює надсилання періодичних оновлень, та записи маршрутів не застарівають. Замість цього EIGRP передає інкрементні оновлення лише за зміни стану мережі призначення. Це може трапитися у випадках, коли нова мережа стає доступною, існуюча мережа стає недоступною або відбуваються зміни в метриці маршрутизації існуючої мережі.

Пакети підтверджень EIGRP

У разі використання надійної доставки EIGRP передає пакети підтверджень (ACK). Підтвердження EIGRP є пакетом привітання EIGRP без даних. RTP використовує надійну доставку для передачі пакетів оновлень, запитів та відповідей. Для надсилання пакетів підтверджень EIGRP завжди використовується ненадійне одноадресна розсилка. Сенса ненадійної доставки полягає у тому, щоб уникнути нескінченного циклу підтверджень.

Пакети запитів EIGRP

Для пошуку мереж та виконання інших завдань DUAL використовує пакети запитів та відповідей. Для запитів та відповідей використовується доставка із забезпеченням надійності. Запити можуть бути передані шляхом групової розсилки або передачі на конкретну адресу, а відповіді завжди передаються як одноадресні пакети.

Пакети відповідей EIGRP

Відповідь повинні надіслати всі сусідні пристрої, незалежно від наявності у них маршруту до вимкненої мережі. Оскільки для передачі відповідей також використовується надійна доставка, маршрутизатори повинні надсилати підтвердження.

Інкапсуляція повідомлень EIGRP

Частина даних EIGRP інкапсулюється в пакет. Таке поле даних має назву «тип, довжина, значення» (type, length, value, TLV). Типи TLV – параметри EIGRP, внутрішні маршрути IP та зовнішні маршрути IP.

До кожного пакету EIGRP, незалежно від типу, додається заголовок EIGRP. Потім заголовок пакету EIGRP та TLV інкапсулюються в пакет IPv4. У заголовку IPv4 пакету, значення поля протоколу встановлюється на 88, що визначає EIGRP, а адреса призначення IPv4 встановлюється рівною адресі групової розсилки 224.0.0.10. Якщо пакет EIGRP інкапсулюється в кадр Ethernet, адреса групової розсилки також виступає в ролі MAC-адреси призначення, 01-00-5E-00-00-0A.

В таблиці 3.3 показаний кадр каналу передачі Ethernet.

Таблиця 3.3 – Інкапсуляція повідомлень EIGRP

Заголовок кадра каналу передачі даних	Заголовок пакета IP	Заголовок пакета EIGRP	Типи TLV
Кадр каналу передачі даних MAC-адреса джерела Адреса відправляючого інтерфейсу MAC-адреса призначення Групова розсилка: 01-00-5E-00-00-0A	IP-пакет IPv4-адреса джерела Адреса відправляючого інтерфейсу IPv4-адреса призначення Групова розсилка: 224.0.0.10 Поле протоколу = 88 для EIGRP	Заголовок пакета EIGRP Код операції для типу пакета EIGRP Номер автономної системи	Типи містять: 0x0001 параметри EIGRP 0x0102 внутрішні IP-маршрути 0x0103 зовнішні IP-маршрути

Джерело: [8]

EIGRP для IPv4 інкапсулюється в пакет IPv4. Для EIGRP IPv6 використовується аналогічний тип інкапсуляції. EIGRP для IPv6 інкапсулюється в заголовок IPv6. Адресою призначення IPv6 буде адреса призначення FF02::A, а наступне поле заголовка буде встановлено 88.

Алгоритм DUAL

Алгоритм DUAL або алгоритм дифузного оновлення – це ключовий механізм протоколу маршрутизації EIGRP. Він відповідає за вибір оптимального маршруту та управління роботою EIGRP в умовах зміни стану мережі. Алгоритм DUAL забезпечує наступні можливості:

- Шляхи без петель;
- Резервні шляхи без петель з можливістю негайного використання;
- Швидка конвергенція;
- Мінімальне використання пропускної спроможності завдяки обмеженим оновленням.

Алгоритм DUAL використовується для усунення петель для кожного випадку під час обчислення маршруту. Він дозволяє в один час синхронізувати всі маршрутизатори, що беруть участь в зміні топології. Маршрутизатори, яких не торкнулися зміни топології, не беруть участь у повторному розрахунку. Цей метод дозволяє EIGRP скоротити час збіжності у порівнянні з іншими протоколами маршрутизації на основі векторів відстані.

При здійсненні всіх обчислень маршрутів приймається рішення за допомогою алгоритму DUAL з використанням кінцевого автомата (FSM). FSM – це модель робочого процесу, аналогічна блок-схемі. Вона складається з наступних компонентів:

- Кінцева кількість етапів (станів)
- Перехід між цими етапами
- Операції

Кінцевий автомат DUAL (рис. 3.3) відстежує всі маршрути та використовує показники EIGRP для вибору ефективних шляхів без петель та для визначення маршрутів найменшої вартості, що будуть додані до таблиці маршрутизації.

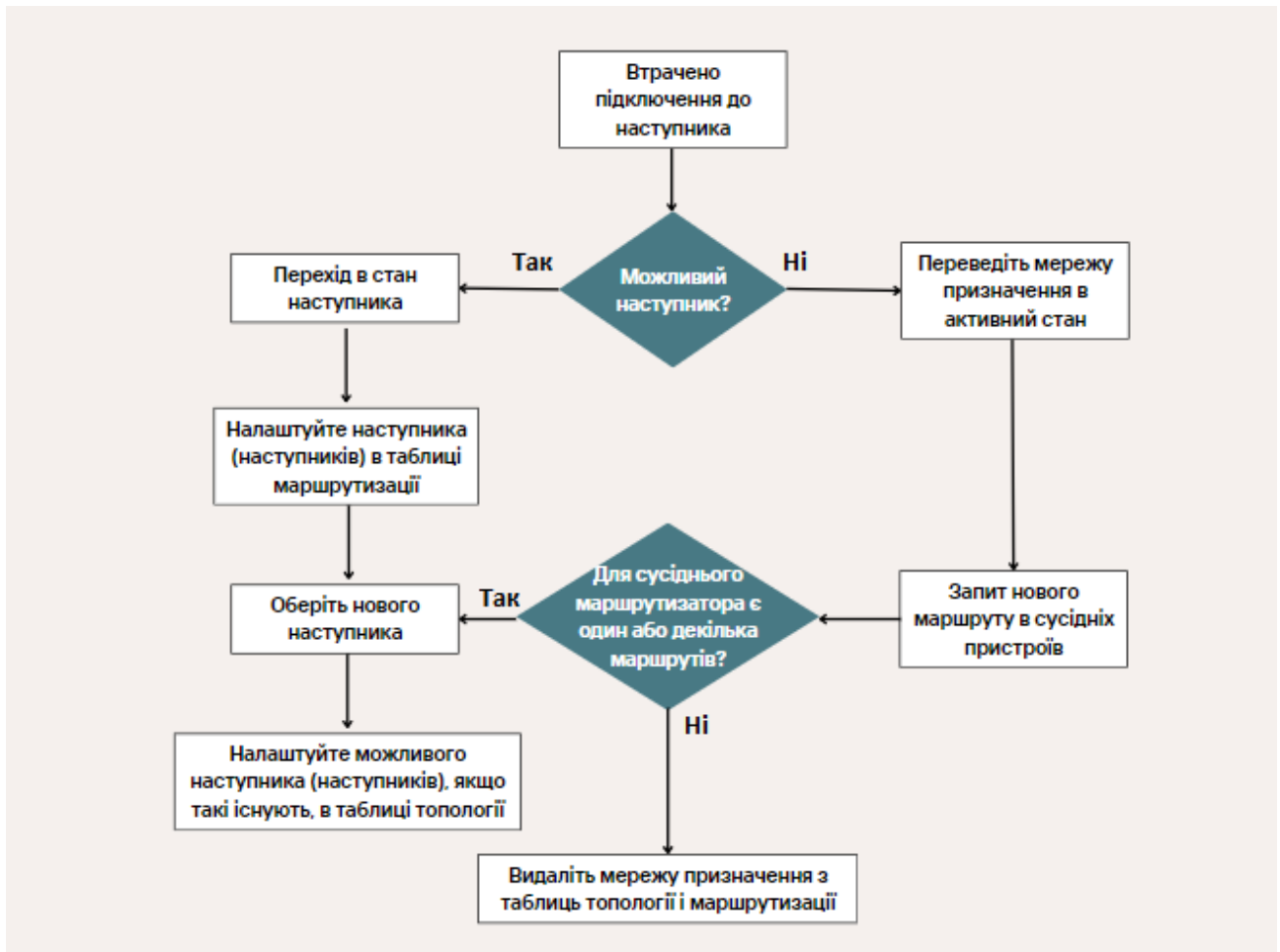


Рисунок 3.3 – Кінцевий автомат алгоритму DUAL [8]

Алгоритм DUAL використовує низку наступних термінів:

- Successor (наступник) – це маршрут з найменшою метрикою до конкретної мережі призначення. Successor використовується для надсилання даних.
- Feasible Successor (можливий наступник) – це резервний маршрут до мережі призначення, який має меншу метрику, ніж поточний Successor. Feasible Successor використовується як альтернативний маршрут, який може бути активований, якщо поточний Successor стане недоступним.
- FD (Feasible Distance – можлива відстань) – це метрика найменшого Successor’а до конкретного призначення. FD порівнюється з іншими метриками для визначення Feasible Successor.
- RD (Reported Distance – повідомлена відстань). RD – це метрика найменшого Successor’а, яка надходить від іншого маршрутизатора. RD допомагає визначити, чи існує Feasible Successor.

Загалом, процес роботи алгоритму DUAL можна розділити на кілька етапів:

- 1) Ініціалізація. Кожен маршрутизатор має свою таблицю DUAL, де зберігаються Successor та Feasible Successor для кожного призначення. На початку усі Successor є невідомими, а FD встановлено як нескінченність.
- 2) Запит (Query) та відповідь (Reply). Якщо маршрутизатор втрачає Successor для певної мережі призначення, він надсилає запит своїм сусідам.
- 3) Сусідні маршрутизатори, які мають Feasible Successor для цього місця призначення, надсилають відповідь, і тоді їх FD може стати новим Successor.
- 4) Перевірка умов DUAL. DUAL перевіряє низку умов для визначення, чи може маршрут бути Successor або Feasible Successor. Ці умови включають порівняння FD та RD, і якщо RD менше за FD, то маршрут може бути Feasible Successor.
- 5) Оновлення таблиці маршрутизації. Після виявлення нових Successor або Feasible Successor, таблиця маршрутизації оновлюється, і новий Successor використовується для відсилання даних.

3.2 Налаштування протоколу EIGRP на маршрутизаторах Cisco

Номер автономної системи

В конфігурації EIGRP використовується номер автономної системи. Він важливий тільки для домена маршрутизації EIGRP і відіграє роль ідентифікатора процесу, допомагаючи маршрутизаторам відстежувати кілька працюючих екземплярів EIGRP. Це є необхідним, оскільки в одній мережі може діяти декілька екземплярів EIGRP. Кожен екземпляр EIGRP може бути налаштований для підтримки оновлень маршрутизації для різних мереж та обміну цими оновленнями.

Налаштування відбувається в режимі глобальної конфігурації:

```
Router(config)# router eigrp <autonomous-system>
```

Значенням *autonomous-system* може бути будь-яке 16-бітове значення від 1 до 65535. Усі роутери у домені маршрутизації EIGRP повинні мати однаковий номер автономної системи.

Важливо зазначити, що номер автономної системи, який використовується в конфігурації EIGRP, не пов'язаний із глобально призначеними номерами автономних систем IANA, які використовуються зовнішніми протоколами маршрутизації [17].

Команда *router eigrp <autonomous-system>* не запускає сам процес EIGRP, маршрутизатор не почне відправляти оновлення. Навпаки, ця команда лише надає доступ до налаштування параметрів EIGRP.

Якщо необхідно повністю видалити процес маршрутизації EIGRP з пристрою, використовується команда режиму глобальної конфігурації:

```
Router(config)# no router eigrp <autonomous-system>
```

Ця команда зупиняє процес EIGRP та видаляє всі наявні конфігурації маршрутизатора EIGRP.

Щоб налаштувати номер автономної системи для IPv6, використовується команда:

```
Router(config)# ipv6 router eigrp <autonomous-system>
```

Так само, як у випадку EIGRP для IPv4, значення *autonomous-system* повинно бути однаковим на всіх роутерах у домені маршрутизації. Процес маршрутизації EIGRP для IPv6 не буде налаштований, до тих пір, поки маршрутизація IPv6 не буде активована командою *ipv6 unicast-routing* у режимі глобальної конфігурації.

Ідентифікатор маршрутизатора EIGRP

Ідентифікатор маршрутизатора EIGRP використовується, щоб унікальним чином ідентифікувати кожен маршрутизатор у домені маршрутизації EIGRP.

Щоб визначити свій ідентифікатор, маршрутизатор із Cisco IOS використовуватиме наступні три правила у вказаному порядку:

1) Використовує адресу, задану за допомогою команди *eigrp router-id ipv4-address* режиму глобальної конфігурації маршрутизатора.

2) Якщо ідентифікатор маршрутизатора не налаштований, обирає найвище значення IPv4 адреси будь-якого з налаштованих інтерфейсів зворотної петлі.

3) За відсутності налаштованих інтерфейсів зворотної петлі обирає найвище значення активної IPv4-адреси будь-якого з фізичних інтерфейсів.

Отже, щоб задати ідентифікатор маршрутизатора для IPv4, використовується наступна команда:

```
Router(config)# eigrp router-id <ipv4-address>
```

Аргументу *ipv4-address* можна призначити будь-яку адресу IPv4, окрім 0.0.0.0 та 255.255.255.255. Ідентифікатор маршрутизатора має бути 32-бітовим числом, унікальним у домені маршрутизації EIGRP. В іншому випадку можливі конфлікти маршрутизації.

Якщо ідентифікатор маршрутизатора не визначено за допомогою команди *eigrp router-id ipv4-address*, EIGRP генерує свій власний ідентифікатор маршрутизатора, використовуючи IPv4-адресу, інтерфейс *loopback* або фізичний інтерфейс. *Loopback*-адреса є віртуальним інтерфейсом, який автоматично активується після налаштування. Інтерфейс не обов'язково повинен підтримувати протокол EIGRP, тобто його не обов'язково включати в одну з команд EIGRP *network*. Але інтерфейс має бути в активному стані (*up/up*).

Для активації та конфігурування інтерфейсу *loopback* використовуються наступні команди:

```
Router(config)# interface loopback <number>
```

```
Router(config-if)# ip address <ipv4-address> <subnet-mask>
```

Для IPv6 для налаштування ідентифікатора маршрутизатора також використовується команда *eigrp router-id*. Для ідентифікатора маршрутизатора використовується 32-бітове значення. Щоб отримати це значення, протокол EIGRP для IPv6 застосовує такий метод, що і EIGRP для IPv4.

Але за замовчуванням процес EIGRP для IPv6 перебуває у вимкненому стані. Щоб увімкнути процес EIGRP для IPv6, потрібна команда *no shutdown*. У випадку EIGRP для IPv4 ця команда не потрібна.

Ввімкнення маршрутизації EIGRP на інтерфейсі

Для того, щоб увімкнути маршрутизацію EIGRP для IPv4 на інтерфейсі, використовується команда:

```
Router(config-router)# network <IPv4 network address>
```

Аргумент *IPv4 network address* – це класова мережева адреса для кожної безпосередньо підключеної мережі.

Команда *network* використовується так само, як і для інших внутрішньосистемних протоколів маршрутизації (IGP). У протоколі EIGRP ця команда працює наступним чином:

- Вмикає для будь-якого інтерфейсу цього маршрутизатора, який відповідає мережевій адресі команди режиму конфігурації маршрутизатора *network*, надсилання та отримання оновлень EIGRP.
- Мережа інтерфейсів включається до оновлення маршрутизації EIGRP.

За замовчуванням, використання команди *network* та мережевої адреси IPv4 вмикає EIGRP для всіх інтерфейсів маршрутизатора, що належать цій класовій адресі мережі. Але можливі ситуації, коли необхідно ввімкнути EIGRP не для всіх інтерфейсів. В такому випадку для оголошення лише конкретних підмереж, використовується параметр *subnet mask* (шаблонна маска) з командою *network*:

```
Router(config-router)# network <IPv4 network> <subnet mask>
```

EIGRP для IPv6 активується за допомогою іншого методу для увімкнення інтерфейсу, порівняно з EIGRP для IPv4. Замість використання команди *network* у режимі конфігурації маршрутизатора для вказівки відповідних адрес інтерфейсів, в EIGRP для IPv6 налаштування проводиться безпосередньо на рівні самого інтерфейсу.

Щоб увімкнути EIGRP для IPv6 на інтерфейсі, використовується наступна команда режиму конфігурації інтерфейсу:

```
Router(config-if)# ipv6 eigrp <autonomous-system>
```

Значення *autonomous-system* має збігатися з номером автономної системи, який використовувався для включення процесу маршрутизації EIGRP.

Аналогічно команді *network*, яка використовується в EIGRP для IPv4, інтерфейсна команда *ipv6 eigrp*:

- дозволяє інтерфейсу встановити відносини суміжності та надсилати або отримувати оновлення EIGRP для IPv6;
- включає префікс (мережу) цього інтерфейсу до оновлення маршрутизації EIGRP для IPv6.

Композитна метрика EIGRP

За замовчуванням протокол EIGRP використовує для розрахунку бажаного маршруту до мережі у своїй складеній метриці наступні значення.

- Bandwidth (пропускна здатність). Мінімальна пропускна здатність серед всіх вихідних інтерфейсів на маршруті від джерела до призначення.
- Delay (затримка). Загальна кількість затримок на всіх інтерфейсах вздовж маршруту, виміряна в десятках мікросекунд

Також можна використовувати інші значення, але їх застосування не є рекомендованим, оскільки це зазвичай спричинює часті перерахунки таблиці топології.

- Reliability (надійність). Забезпечує максимальну надійність маршруту від відправника до отримувача, базуючись на використанні повідомлень перевірки активності (keepalive).
- Load (завантаженість) означає найвищу завантаженість для каналу між джерелом і місцем призначення, що вирахована на основі швидкості передачі пакета та налаштованої пропускної здатності інтерфейсу.

Формула для розрахунку композитної метрики виглядає наступним чином [14]:

$$Metric = K1 \times \frac{Bandwidth}{K3 + Bandwidth} + K2 \times \frac{K5 \times Delay}{K4 + K5 \times Delay} \quad (3.1)$$

K1 і K3 вказують на пропускну здатність та затримку відповідно. K2 представляє навантаження, а K4 і K5 – надійність. За замовчуванням значення K1 і K3 становлять 1, тоді як значення K2, K4 і K5 прирівнюються до 0.

Bandwidth – ширина каналу в бітах в секунду. Delay – затримка в мікросекундах.

Ця формула обчислюється для кожного маршруту, і в результаті отримується композитна метрика. Маршрут із меншою композитною метрикою вважається оптимальним.

Значення K можна змінювати за допомогою команди режиму глобальної конфігурації маршрутизатора *metric weights*:

Router (config-router) # metric weights tos k1 k2 k3 k4 k5

де *tos* – бажане нове значення.

Перевірка налаштувань

В таблиці 3.4 наведено команди, які допоможуть перевірити конфігурацію і налаштування протоколу EIGRP та для його діагностики. Вони вводяться з привілейованого режиму маршрутизатора.

Таблиця 3.4 – Команди для перевірки налаштувань протоколу EIGRP[1]

Команда	Призначення
show ip protocols	Відображення загальної інформації про EIGRP
show ip eigrp topology	Відображення інформації про топологію EIGRP
show ip eigrp interfaces	Відображення інформації про інтерфейси, які використовують EIGRP
show ip route eigrp	Відображення таблиці маршрутів EIGRP
show ip eigrp neighbors	Відображення інформації про сусідні маршрутизатори EIGRP
show ip eigrp interface <interface>	Відображення інформації про параметри EIGRP для конкретного інтерфейсу
show ip eigrp topology all-links	Відображення інформації про метрику маршрутів EIGRP
show running-config section eigrp	Відображення інформації про параметри EIGRP, налаштовані на маршрутизаторі
show ip eigrp events	Перегляд історії змін стану EIGRP

За допомогою цих команд можливо переглядати різні аспекти роботи протоколу EIGRP на маршрутизаторах з операційною системою IOS.

3.3 Переваги й недоліки використання EIGR в корпоративних IP мережах

На основі проведеного аналізу визначимо основні переваги й недоліки використання протоколу EIGRP в корпоративних IP мережах.

Швидка збіжність та ефективне використання пропускної спроможності роблять його привабливим для великих корпоративних мереж з високим рівнем динаміки та змін у топології. Механізми, такі як можливі наступники (Feasible Successors) та оптимізація використання шляхів, покращують відновлення мережі в разі втрати основного маршруту.

З іншого боку, важливо враховувати його пропрієтарний характер та обмежену взаємодію з обладнанням інших виробників. Це може обмежувати гнучкість та масштабованість мережі у випадках, коли використовується обладнання різних виробників. Крім того, споживання ресурсів та складність конфігурації можуть стати проблемою великих мереж або для тих, хто має обмежені технічні ресурси.

Отже до переваг використання протоколу EIGRP можна віднести:

- *Швидка збіжність.* EIGRP може швидко адаптуватися до змін у мережі, що робить його ефективним для великих та розподілених мереж.
- *Мінімальне використання ширини каналу.* Протокол ефективно використовує пропускну спроможність, мінімізує обсяги обміну інформацією маршрутизаторами.
- *Динамічна адаптація до змін у мережі.* EIGRP вміє адаптуватися до змін у топології мережі, забезпечуючи оптимальний маршрут для передачі даних.
- *Підтримка VLSM.* Протокол підтримує Variable Length Subnet Masking (VLSM), що дозволяє ефективно використовувати IP-адреси в мережі.
- *Наявність можливих наступників (Feasible Successors).* EIGRP підтримує можливих наступників, що забезпечує швидке відновлення маршрутів при втраті основного маршруту.
- *Ієрархічна структура.* Протокол використовує ієрархічну структуру, що полегшує масштабування великих мереж.

Недоліки використання EIGRP в корпоративних IP мережах:

- *Пропрієтарність.* EIGRP – пропрієтарний протокол, розроблений компанією Cisco, що обмежує його використання на обладнанні інших виробників.
- *Обмежена підтримка для інших виробників.* Хоча й існують спроби розширення взаємодії EIGRP з іншими виробниками, налагоджений сценарій частіше за все базується на обладнанні Cisco.
- *Споживання ресурсів.* Великі мережі зі значною кількістю маршрутів можуть споживати великі обсяги пам'яті та обчислювальних ресурсів.
- *Складність конфігурації.* Конфігурація EIGRP може бути складним завданням, особливо в розподілених середовищах.
- *Оптимізація для обладнання Cisco.* EIGRP оптимізований для використання на обладнанні Cisco, і його ефективність може бути нижчою на пристроях інших виробників.
- *Потребує правильних налаштувань для оптимальної роботи.* Для досягнення оптимальної продуктивності, EIGRP може вимагати ретельного налаштування та управління.

3.4 Висновки з розділу 3

В даному розділі було детально проаналізовано протокол EIGRP, його принцип роботи, базові налаштування, виявлено переваги й недоліки використання в корпоративних IP мережах. Зроблено наступні висновки.

1) Протокол EIGRP (Enhanced Interior Gateway Routing Protocol) є сучасним та ефективним методом внутрішньої маршрутизації, розроблений компанією Cisco Systems. EIGRP поєднує у собі якості протоколів маршрутизації з урахуванням стану каналу, так і протоколів на основі векторів відстані. Його ключовий алгоритм DUAL гарантує належну роботу та наявність маршрутів без петель в усьому домені маршрутизації.

2) Модулі протоколозалежної маршрутизації (PDM) у протоколі EIGRP відіграють ключову роль у забезпеченні ефективного та надійного функціонування протоколу. Ці параметри відповідають за конкретні функції маршрутизації для кожного протоколу на мережевому рівні та включають в себе управління таблицями сусідніх пристроїв, створення та обробку пакетів конкретного протоколу, взаємодію з алгоритмом DUAL, обчислення метрик, реалізацію списків фільтрації та доступу, а також перерозподіл маршрутів між EIGRP та іншими протоколами маршрутизації.

3) Надійний транспортний протокол (RTP) використовується для передачі пакетів EIGRP, забезпечуючи як надійну, так і ненадійну доставку. RTP може використовувати як одноадресну передачу, так і групову розсилку для обміну інформацією між маршрутизаторами.

4) Протокол EIGRP використовує різні типи пакетів для виконання різноманітних функцій у процесі обміну інформацією між маршрутизаторами. Ці типи пакетів включають: пакети привітання, оновлень, підтверджень, запитів та відповідей. Ці типи пакетів визначають способи обміну інформацією та взаємодії між маршрутизаторами у мережі EIGRP. Кожен тип пакету має своє призначення та спосіб доставки, що дозволяє протоколу ефективно адаптуватися до різних умов мережі.

5) Алгоритм DUAL є важливим компонентом протоколу маршрутизації EIGRP, забезпечує ефективний вибір оптимальних маршрутів та управління змінами стану мережі. Його ключові характеристики, такі як відсутність петель, наявність резервних шляхів та швидка конвергенція, роблять протокол EIGRP ефективним і надійним для використання в різноманітних мережевих умовах.

6) Розглянуто базові налаштування протоколу EIGRP на маршрутизаторах Cisco, такі як: номер автономної системи, ідентифікатор маршрутизатора EIGRP, ввімкнення EIGRP на інтерфейсах. Проаналізовано таке поняття як композитна метрика, розглянуто формулу для її обчислення. Проаналізовано команди для перевірки конфігурації і налаштування протоколу EIGRP та для його діагностики.

7) Загальний аналіз переваг та недоліків використання протоколу EIGRP в корпоративних IP мережах вказує на його значний внесок у поліпшення ефективності та швидкодії великих та динамічних мереж. Швидка збіжність, ефективне використання пропускної спроможності, можливі наступники та ієрархічна структура роблять EIGRP привабливим вибором для складних корпоративних середовищ. Також EIGRP має і низку недоліків, тож перед вибором EIGRP, слід враховувати його особливості та підготувати відповідні ресурси для оптимальної конфігурації та управління.

4 ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ OSPF І EIGRP ДЛЯ ВИКОРИСТАННЯ В КОРПОРАТИВНИХ IP-МЕРЕЖАХ

4.1 Методологія проведення дослідження

Мета цього дослідження полягає у визначенні, який з протоколів маршрутизації OSPF чи EIGRP має кращі показники для корпоративних IP-мереж, а також в знаходженні найкращої топології для кожного протоколу маршрутизації. Оскільки кожен з протоколів маршрутизації має різні характеристики, дослідження буде виконано з використанням OSPF і EIGRP та протестоване шляхом моделювання.

Для проведення моделювання, в цьому дослідженні використовується програмне забезпечення Cisco Packet Tracer. За допомогою нього було спроектовано корпоративну IP-мережу та налаштовано моделювання передачі даних в мережі на основі кільцевої та сітчастої топології з використанням протоколів маршрутизації EIGRP та OSPF. Чотири маршрутизатори налаштовані з використанням кільцевої та сітчастої топології з послідовним кабелем для підключення маршрутизаторів і перехресним кабелем для підключення маршрутизатора до комутатора та комутатора до персонального комп'ютера. В ході виконання дослідження буде перевірено з'єднання між вузлами мережі для визначення часу, що знадобиться для передачі даних. Буде відстежено маршрут, щоб дізнатися, якими шляхами піде пакет даних. Також у цій симуляції один із зв'язків, який зазвичай використовується, буде роз'єднано, щоб дізнатися, який шлях використовуватиметься після роз'єднання зв'язку. Крім того, параметри метрики та вартості в моделюванні також порівнюватимуться з розрахунками за формулою, щоб визначити правильність результатів моделювання (рис. 4.1).

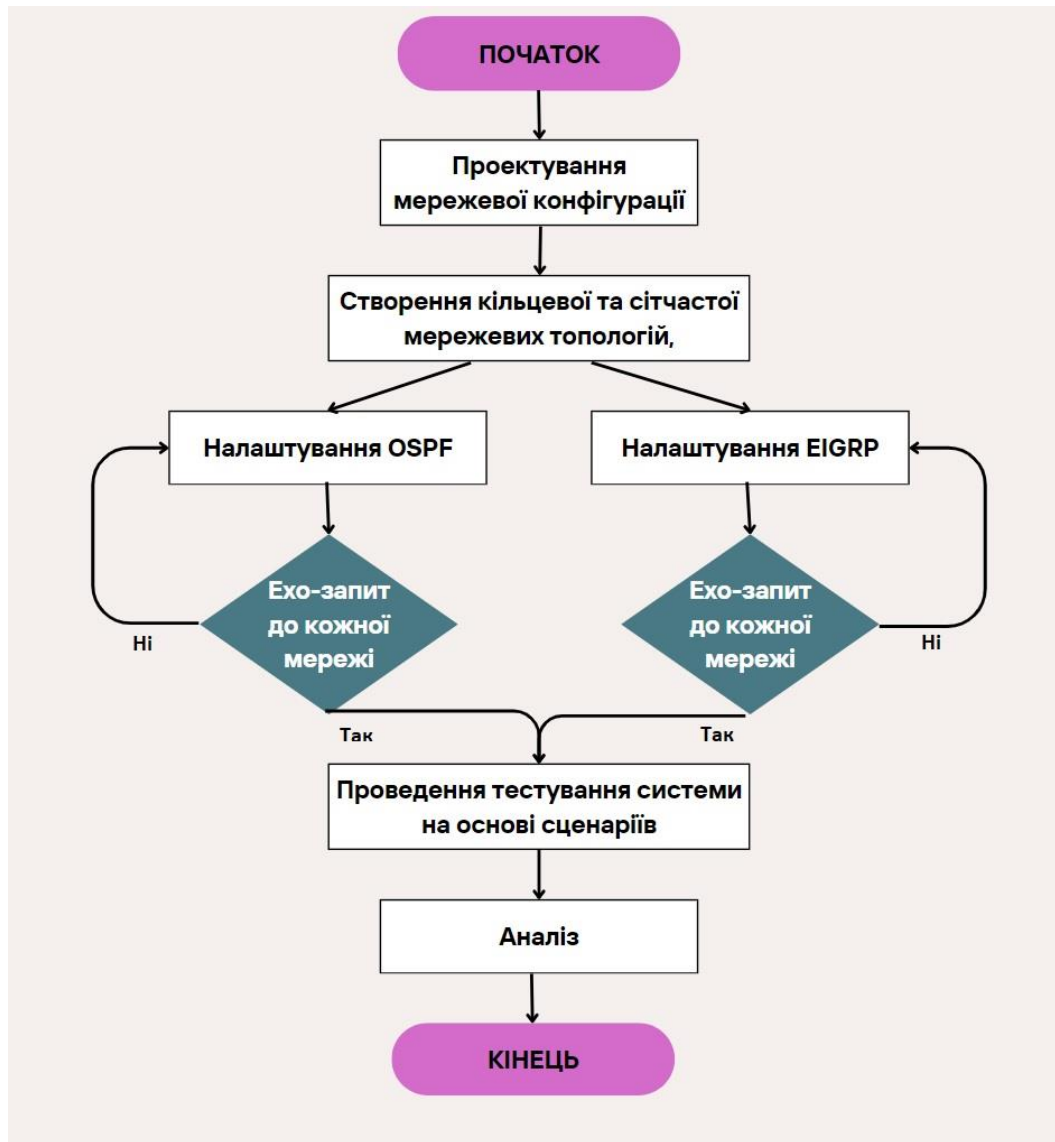


Рисунок 4.1 – Блок-схема тесту продуктивності
Виконано автором на основі [18]

На рис 4.1 зображено етапи проєктування та моделювання продуктивності в корпоративних мережах з використанням протоколів EIGRP та OSPF у кільцевій і сітчастій топологіях. Моделювання виконується за допомогою програмного середовища Cisco Packet Tracer в такому порядку: налаштування мережі, створення мережевих топологій, а саме кільцевої та сітчастої, налаштування IP-адрес на пристроях та на кожному інтерфейсі. Обидві топології налаштовується за допомогою протоколів маршрутизації EIGRP і OSPF. Після налаштування протоколів маршрутизації виконується ring-тест на кожному ПК мережі. Після успішного тестування системи на основі сценарію проводиться аналіз.

Топологія мережі

В моделюванні використовуються дві топології – кільцева та сітчаста із використанням 4 маршрутизаторів, 4 комутаторів і 8 ПК. На рис. 4.2 зображено кільцеву топологію для протоколів маршрутизації EIGRP і OSPF: 4 маршрутизатори (із 4 послідовними кабелями для з'єднання маршрутизаторів), 4 комутатори та 8 ПК.

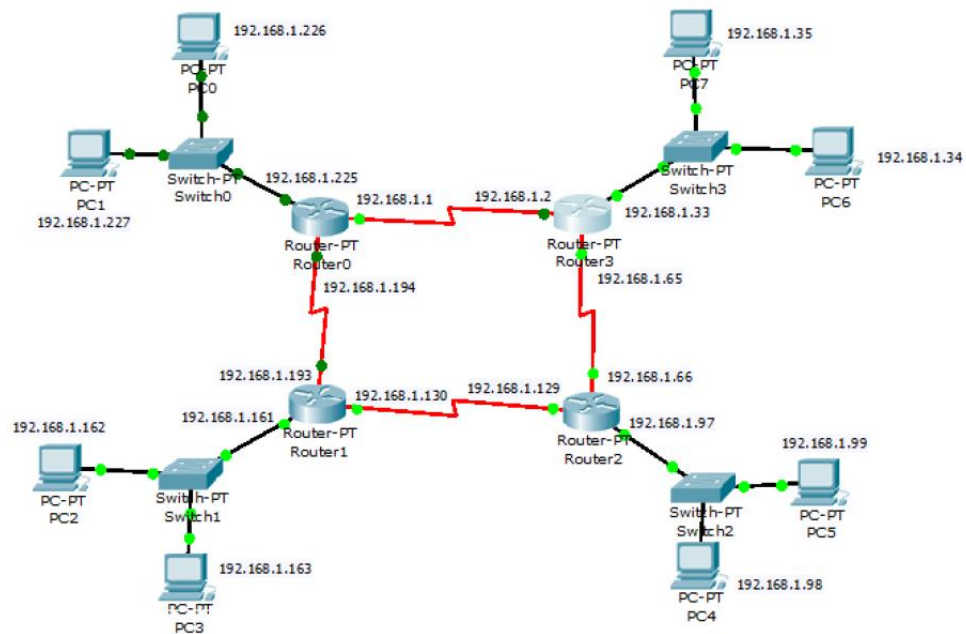


Рисунок 4.2 – Кільцева топологія

На рис. 4.3 зображено сітчасту топологію для протоколів маршрутизації EIGRP і OSPF: 4 маршрутизатори (із 6 послідовними кабелями для з'єднання маршрутизаторів), 4 комутатори та 8 ПК.

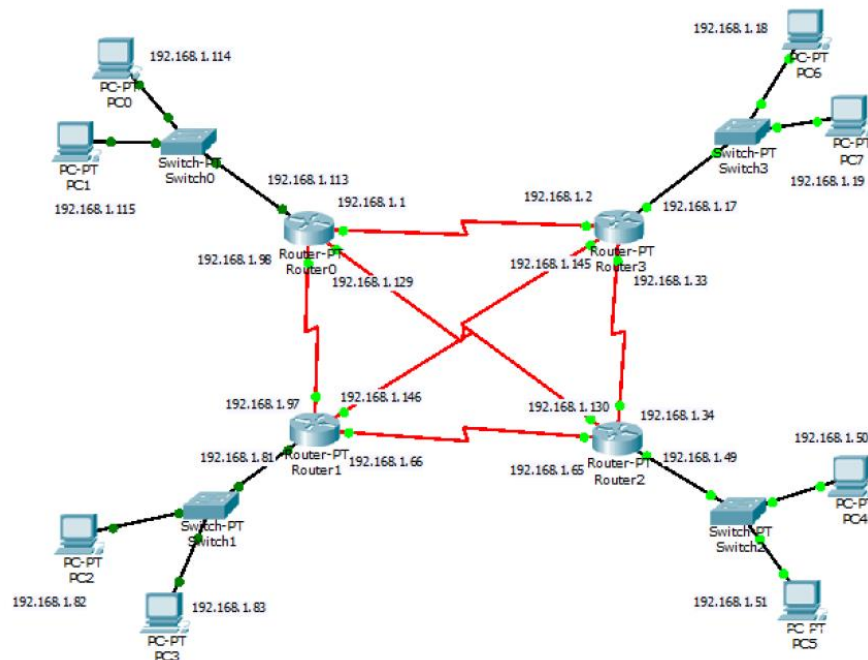


Рисунок 4.3 – Сітчаста топологія

Розрахунок IP-адреси

Розбиття на підмережі здійснюється на основі необхідної кількості мереж, щоб не витратити надто багато мережових адрес. Використаємо мережову адресу 192.168.1.0. Розрахунок IP-адреси проведено на основі техніки підмереж IPv4.

Для кільцевої топології:

Кількість двійкових одиниць у масці підмережі (n), яку треба додати, задля досягнення чи перевищення кількості необхідних мереж, може бути виражена умовою $2^n \geq x$, тоді як x – кількість необхідних підмереж, тому формула виглядає так:

$$2^n \geq x \quad (4.1)$$

$$2^n \geq 8$$

Якщо $n=3$, то

$$8 \geq 8$$

Якщо додати 3 біти до маски підмережі 255.255.255.0/24, отримаємо:

11111111.11111111.11111111.11100000 /27 або
255.255.255.248 /27

Із розрахунку вище, загальна кількість вузлів дорівнює 256 мінус 224. Щоб діапазон IP-адрес, які можна використовувати для кожної підмережі, обчислимо:

$$256 - 224 = 32$$

Розбиття на 8 підмереж і 29 нових вузлів у кожній підмережі наведено в табл. 4.1:

Таблиця 4.1 – Розподілення адрес в мережі з кільцевою топологією

№ підмережі	Діапазон IP-адрес	Мережева адреса	Широкомовна адреса
1	192.168.1.0 – 192.168.1.31	192.168.1.0	192.168.1.31
2	192.168.1.32 – 192.168.1.63	192.168.1.32	192.168.1.63
3	192.168.1.64 – 192.168.1.95	192.168.1.64	192.168.1.95
4	192.168.1.96 – 192.168.1.127	192.168.1.96	192.168.1.127
5	192.168.1.128 – 192.168.1.159	192.168.1.128	192.168.1.159
6	192.168.1.160 – 192.168.1.191	192.168.1.160	192.168.1.191
7	192.168.1.192 – 192.168.1.223	192.168.1.192	192.168.1.223
8	192.168.1.224 – 192.168.1.255	192.168.1.224	192.168.1.255

Для сітчастої топології:

$$2^n \geq x \quad (4.2)$$

$$2^n \geq 10$$

Якщо $n=4$, то

$$16 \geq 10$$

Якщо додати 3 біти до маски підмережі 255.255.255.0/24, отримаємо:

11111111.11111111.11111111.11100000 /28 або

255.255.255.240 /28

Із розрахунку вище, загальна кількість вузлів дорівнює 256 мінус 224. Щоб діапазон IP-адрес, які можна використовувати для кожної підмережі, обчислимо:

$$256 - 240 = 16$$

Розбиття на 16 підмереж і 14 нових вузлів у кожній підмережі наведено в табл. 4.2:

Таблиця 4.2 – Розподілення адрес в мережі з сітчастою топологією

№ підмережі	Діапазон IP-адрес	Мережева адреса	Широкомовна адреса
1	192.168.1.0 – 192.168.1.15	192.168.1.0	192.168.1.15
2	192.168.1.16 – 192.168.1.31	192.168.1.16	192.168.1.31
3	192.168.1.32 – 192.168.1.47	192.168.1.32	192.168.1.47
4	192.168.1.48 – 192.168.1.63	192.168.1.48	192.168.1.63
5	192.168.1.64 – 192.168.1.79	192.168.1.64	192.168.1.79
6	192.168.1.80 – 192.168.1.95	192.168.1.80	192.168.1.95
7	192.168.1.96 – 192.168.1.111	192.168.1.96	192.168.1.111
8	192.168.1.112 – 192.168.1.127	192.168.1.112	192.168.1.127
9	192.168.1.128 – 192.168.1.143	192.168.1.128	192.168.1.143
10	192.168.1.144 – 192.168.1.159	192.168.1.144	192.168.1.159
11	192.168.1.160 – 192.168.1.175	192.168.1.160	192.168.1.175
12	192.168.1.176 – 192.168.1.191	192.168.1.176	192.168.1.191
13	192.168.1.192 – 192.168.1.207	192.168.1.192	192.168.1.207
14	192.168.1.208 – 192.168.1.223	192.168.1.208	192.168.1.223
15	192.168.1.224 – 192.168.1.239	192.168.1.224	192.168.1.239
16	192.168.1.240 – 192.168.1.255	192.168.1.240	192.168.1.255

4.2 Проведення експериментів і аналіз отриманих даних

Результати моделювання, отримані в ході цього дослідження, ґрунтуються на використанні робочого простору та моделювання в реальному часі в програмі Cisco Packet Tracer для кожного протоколу маршрутизації.

Тестовий сценарій виконується таким чином:

1. Виявлення часу затримки надсилання пакетів даних з одного ПК на інший, коли трафік завантажений.
2. Спостереження за маршрутом трасування або шляхом, який зазвичай проходить пакет даних під час надсилання, а потім розрив зв'язку, через який зазвичай проходить пакет даних для з'ясування різниці в обраному маршруті.

Перший сценарій

Перший сценарій тестування було проведено шляхом надсилання пакетів протоколу керуючих повідомлень Інтернету (ICMP) у п'яти випадках з завантаженим трафіком. Кожен випадок повторювався п'ять разів. Для збільшення потоку трафіка в мережі було додано 4 пакети ICMP з однаковими умовами для кожного випадку. П'ять випадків змодельовано як в кільцевій, так і в сітчастій топології.

В таблиці 4.3 наведено сценарій для надсилання даних з ПК на ПК.

Таблиця 4.3 – Сценарій надсилання пакетів даних

Випадок 1		Випадок 2		Випадок 3		Випадок 4		Випадок 5	
Відпр.	Одерж.	Відпр.	Одерж.	Відпр.	Одерж.	Відпр.	Одерж.	Відпр.	Одерж.
ПК 0	ПК 5	ПК 1	ПК 2	ПК 2	ПК 4	ПК 4	ПК 7	ПК 6	ПК 5
ПК 1	ПК 2	ПК 2	ПК 4	ПК 4	ПК 7	ПК 6	ПК 5	ПК 0	ПК 5
ПК 2	ПК 4	ПК 4	ПК 7	ПК 6	ПК 5	ПК 0	ПК 5	ПК 1	ПК 2
ПК 4	ПК 7	ПК 6	ПК 5	ПК 0	ПК 5	ПК 1	ПК 2	ПК 2	ПК 4
ПК 6	ПК 5	ПК 0	ПК 5	ПК 1	ПК 2	ПК 2	ПК 4	ПК 4	ПК 7

Досліджуваний пакет – перший запис в таблиці (виділено сірим кольором). Решта – це пакети, надіслані для збільшення трафіку в мережі.

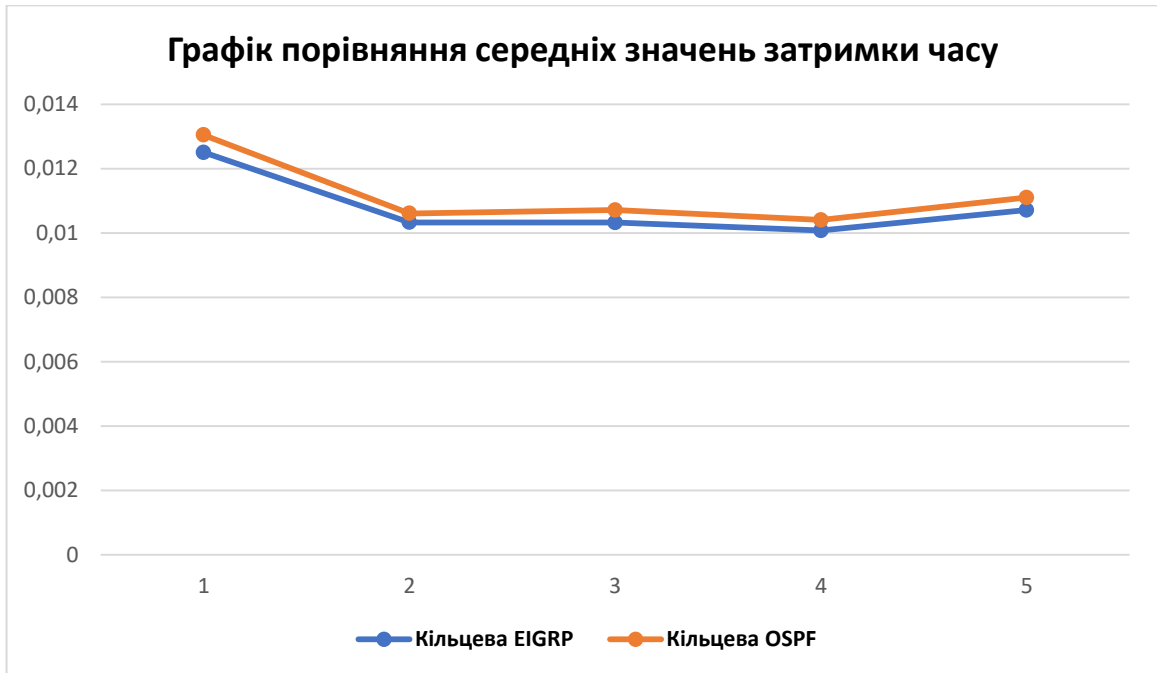
Порівняння значень для кільцевої топології з EIGRP та OSPF.

Отримані результати для кільцевої топології з використанням обох протоколів маршрутизації наведено в таблиці 4.3

Таблиця 4.3 – Середній час затримки пакетів з використанням протоколів OSPF та EIGRP

Порівняння середніх значень затримки (в секундах)					
Топологія та протоколи маршрутизації	Випадок				
	1	2	3	4	5
Кільцева EIGRP	0,012505	0,01033	0,010325	0,01008	0,010715
Кільцева OSPF	0,01305	0,01061	0,010715	0,010405	0,011105

Для наочності побудуємо графік на основі отриманих даних:



Діаграма 4.1 – Порівняння середніх значень затримки часу для кільцевої топології EIGRP і OSPF

Як видно з діаграми, час затримки для протоколу OSPF незначно більший.

Якщо усереднити значення затримки для кожного протоколу маршрутизації для кожного випадку, отримаємо:

Кільцева топологія EIGRP:

$$\frac{0,012505 + 0,01033 + 0,010325 + 0,01008 + 0,010715}{5} = 0,010791 \text{ секунд}$$

Кільцева топологія OSPF:

$$\frac{0,01305 + 0,01061 + 0,010715 + 0,010715 + 0,011105}{5} = 0,011177 \text{ секунд}$$

Значення для кільцевої топології з EIGRP на 0,000386 секунди краще, ніж для кільцевої OSPF.

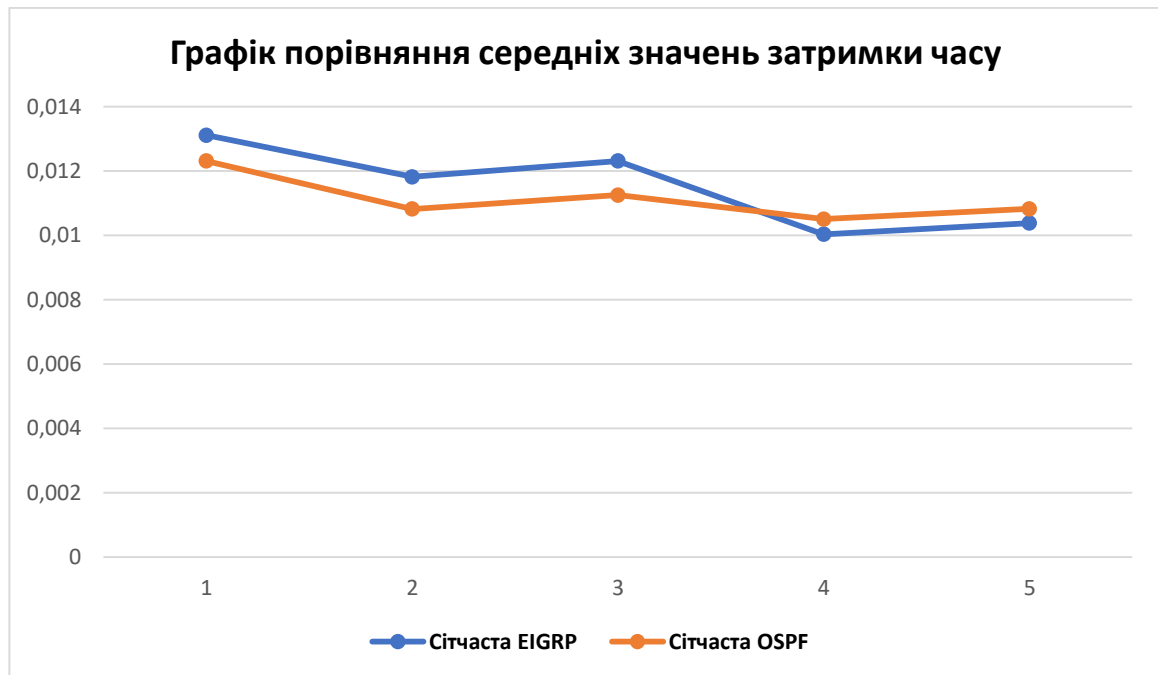
Порівняння значень для сітчастої топології з EIGRP та OSPF.

Отримані результати для сітчастої топології з використанням обох протоколів маршрутизації наведено в таблиці 4.4

Таблиця 4.4. – Середній час затримки пакетів з використанням протоколів OSPF та EIGRP

Порівняння середніх значень затримки (в секундах)					
Топологія та протоколи маршрутизації	Випадок				
	1	2	3	4	5
Сітчаста EIGRP	0,013115	0,01182	0,01231	0,010035	0,01038
Сітчаста OSPF	0,01231	0,01082	0,01125	0,010505	0,010825

Для наочності побудуємо графік на основі отриманих даних:



Діаграма 4.2 – Порівняння середніх значень затримки часу для сітчастої топології EIGRP і OSPF

Як видно з діаграми, в 3 з 5 випадках значення EIGRP краще.

Якщо усереднення значення затримки для кожного протоколу маршрутизації для кожного випадку, отримаємо:

Сітчаста топологія EIGRP:

$$\frac{0,013115 + 0,01182 + 0,01231 + 0,010035 + 0,01038}{5} = 0,011595 \text{ секунд}$$

Сітчаста топологія OSPF:

$$\frac{0,01231 + 0,01082 + 0,01125 + 0,010505 + 0,010825}{5} = 0,011142 \text{ секунд}$$

Отже, загалом значення для сітчастої топології EIGRP на 0,000453 секунди краще, ніж для сітчастої OSPF.

Другий сценарій

Тестування другого сценарію виконується шляхом відслідковування маршрутизатора, через який проходить пакет даних, а потім від'єднання кількох шляхів, через які проходить пакет, для виявлення зміни в маршруті проходження пакета.

Результати перевірки другого сценарію до розірвання зв'язку

Кільцева топологія EIGRP

Шлях, який проходять пакети ICMP для доставки від ПК 0 до ПК 5, такий: ПК 0 – комутатор 0 – маршрутизатор 0 – маршрутизатор 3 – маршрутизатор 2 – комутатор 2 – ПК 5 (рис. 4.2). Це тому, що вибір шляху в EIGRP здійснюється за значенням метрики. Значення метрики обчислюється із загальної кількості маршрутів, що передаються від вихідного до кінцевого маршрутизатора за допомогою наступної формули [18]:

$$\text{метрика} = 256 * \left(\frac{10^7}{\text{мінімальна пропускна здатність}} + \frac{\text{загальна затримка}}{10} \right) \quad (4.3)$$

Отже, шлях доставки пакетів з мережевої адреси маршрутизатора 0 до мережевої адреси маршрутизатора 2 через маршрутизатор 3 із мінімальною пропускною здатністю 100 Кбіт/с, затримкою Serial interface 20 000 мкс і Fast Ethernet 100 – мкс. Розрахунок метрики виглядає наступним чином:

$$\text{метрика} = 256 * \left(\frac{10^7}{100 \text{Кбіт/с}} + \frac{20000 \text{мкс} + 20000 \text{мкс} + 100 \text{мкс}}{10} \right) = 26626560$$

Якщо пакет надсилається із мережевої адреси маршрутизатора 0 на мережеву адресу маршрутизатора 2 через маршрутизатор 1 із мінімальною пропускною здатністю 50 Кбіт/с, затримка Serial interface становить 20 000 мкс, а затримка Fast Ethernet – 100 мкс. Розрахунок метрики виглядає наступним чином:

$$\text{метрика} = 256 * \left(\frac{10^7}{50 \text{ Кбіт/с}} + \frac{20000 \text{ мкс} + 20000 \text{ мкс} + 100 \text{ мкс}}{10} \right) = 52226560$$

З цих обчислень метрики можна довести, що пакет даних, щоб досягти місця призначення, проходитиме через шлях з найменшим значенням метрики – 26626560, у порівнянні з проходженням через маршрут із значенням метрики 52226560.

Сітчаста топологія EIGRP

Шлях, який проходять пакети ICMP для доставки від ПК 0 до ПК 5, такий: ПК 0 – комутатор 0 – маршрутизатор 0 – маршрутизатор 3 – маршрутизатор 2 – комутатор 2 – ПК 5 (рис. 4.3).

Отже, маршрут доставки пакетів від мережевої адреси маршрутизатора 0 до мережевої адреси маршрутизатора 2 через маршрутизатор 3 із мінімальною пропускною здатністю 100 Кбіт/с, затримкою Serial interface 20000 мкс і затримкою Fast Ethernet 100 мкс. Розрахунок метрики виглядає наступним чином:

$$\text{метрика} = 256 * \left(\frac{10^7}{100 \text{ Кбіт/с}} + \frac{20000 \text{ мкс} + 20000 \text{ мкс} + 100 \text{ мкс}}{10} \right) = 26626560$$

Якщо пакет надсилається із мережевої адреси маршрутизатора 0 на мережеву адресу маршрутизатора 2 через маршрутизатор 1 із мінімальною пропускною здатністю 25 Кбіт/с, затримка Serial interface становить 20 000 мкс, а затримка Fast Ethernet – 100 мкс. Розрахунок метрики виглядає наступним чином:

$$\text{метрика} = 256 * \left(\frac{10^7}{25 \text{ Кбіт/с}} + \frac{20000 \text{ мкс} + 20000 \text{ мкс} + 100 \text{ мкс}}{10} \right) = 103426560$$

Якщо пакет надсилається з мережевої адреси маршрутизатора 0 безпосередньо на мережеву адресу маршрутизатора 2 з мінімальною пропускною здатністю 50 Кбіт/с, затримка Serial interface становить 20 000 мкс,

а затримка Fast Ethernet становить 100 мкс. Розрахунок метричного значення відбувається наступним чином:

$$\text{метрика} = 256 * \left(\frac{10^7}{50 \text{ Кбіт/с}} + \frac{(20000 \text{ мкс} + 100 \text{ мкс})}{10} \right) = 51714560$$

З обчислень метрики можна довести, що пакет даних проходитиме через шлях з найменшим значенням метрики – 26626560 для досягнення пункту призначення, порівняно з проходженням через шляхи з більшими значеннями метрики – 51714560 і 103426560.

Кільцева топологія OSPF

Шлях, який проходять пакети ICMP для доставки від ПК0 до ПК 5: ПК 0 – комутатор 0 – маршрутизатор 0 – маршрутизатор 3 – маршрутизатор 2 – комутатор 2 – ПК 5. Це тому, що вибір шляху в OSPF визначається за допомогою параметра Cost (вартість). Вона відрізняється для кожного шляху, значення вартості обчислюється для кожного інтерфейсу від вихідного до кінцевого маршрутизатора, за допомогою наступної формули:

$$\text{Вартість} = \frac{100 \text{ Мбіт/с}}{\text{Пропускна здатність}} \quad (4.4)$$

Розрахунок маршруту доставки пакетів від мережевої адреси маршрутизатора 0 до мережевої адреси маршрутизатора 2 через маршрутизатор 3 із пропускнуою здатністю 100 Кбіт/с кожен, виглядає наступним чином:

$$\text{Вартість (загальна)} = \frac{100 \text{ Мбіт/с}}{100 \text{ Кбіт/с}} + \frac{100 \text{ Мбіт/с}}{100 \text{ Кбіт/с}} + \frac{100 \text{ Мбіт/с}}{100 \text{ Кбіт/с}} = 2001$$

Отже, вартість шляху до маршрутизатора 2 становить 2001. Це можна підтвердити ввівши на маршрутизаторі команду «show ip route» (рис. 4.4):

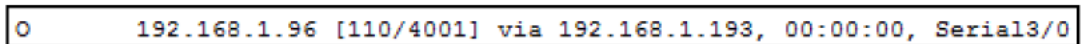
```
O          192.168.1.96 [110/2001] via 192.168.1.2, 00:00:20, Serial2/0
```

Рисунок 4.4 – Значення вартості маршруту від інтерфейсу 192.168.1.1 до інтерфейсу 192.168.1.97 через маршрутизатор 3

Якщо надсилати пакет із мережевої адреси маршрутизатора 0 на мережеву адресу маршрутизатора 2 через маршрутизатор 1 із пропускною здатністю 50 Кбіт/с для кожного інтерфейсу, розрахунок вартості буде таким:

$$\text{Вартість (загальна)} = \frac{100 \text{ Мбіт/с}}{50 \text{ Кбіт/с}} + \frac{100 \text{ Мбіт/с}}{50 \text{ Кбіт/с}} + \frac{100 \text{ Мбіт/с}}{100 \text{ Кбіт/с}} = 4001$$

Отже, вартість шляху до маршрутизатора 2 становить 4001. Це можна підтвердити ввівши на маршрутизаторі команду «show ip route» (рис. 4.5):



```

O          192.168.1.96 [110/4001] via 192.168.1.193, 00:00:00, Serial3/0
  
```

Рисунок 4.5 – Значення вартості маршруту від інтерфейсу 192.168.1.194 до інтерфейсу 192.168.1.97 через маршрутизатор 1

З розрахунку вартості можна довести, що пакет даних, для досягнення пункту призначення, проходитиме через шлях з найменшим значенням вартості, а саме 2001, а не через шлях з більшою вартістю, яка становить 4001.

Сімчаста топологія OSPF

Шлях, який проходять пакети ICMP для доставки від ПК 0 до ПК 5: ПК 0 – комутатор 0 – маршрутизатор 0 – (маршрутизатор 3 – маршрутизатор 2) / (маршрутизатор 2) – комутатор 2 – ПК 5.

Розрахунок маршруту доставки пакетів з мережевої адреси маршрутизатора 0 на мережеву адресу маршрутизатора 2 через маршрутизатор 3 із пропускною здатністю 100 Кбіт/с кожен, виглядає наступним чином:

$$\text{Вартість (загальна)} = \frac{100 \text{ Мбіт/с}}{100 \text{ Кбіт/с}} + \frac{100 \text{ Мбіт/с}}{100 \text{ Кбіт/с}} + \frac{100 \text{ Мбіт/с}}{100 \text{ Кбіт/с}} = 2001$$

Отже, вартість шляху до маршрутизатора 2 становить 2001. Це можна підтвердити ввівши на маршрутизаторі команду «show ip route» (рис. 4.6):

```
O 192.168.1.48 [110/2001] via 192.168.1.130, 00:03:33, Serial6/0
```

Рисунок 4.6 – Значення вартості маршруту від інтерфейсу 192.168.1.1 до інтерфейсу 192.168.1.49 через маршрутизатор 3

Якщо надсилати пакет із мережевої адреси маршрутизатора 0 на мережеву адресу маршрутизатора 2 через маршрутизатор 1 із пропускною здатністю 25 Кбіт/с для кожного інтерфейсу, розрахунок вартості буде таким:

$$\text{Вартість (загальна)} = \frac{100 \text{ Мбіт/с}}{25 \text{ Кбіт/с}} + \frac{100 \text{ Мбіт/с}}{25 \text{ Кбіт/с}} + \frac{100 \text{ Мбіт/с}}{100 \text{ Кбіт/с}} = 8001$$

Вартість шляху до маршрутизатора 2 становить 2001. Це можна підтвердити ввівши на маршрутизаторі команду «show ip route» (рис. 4.7):

```
O 192.168.1.48 [110/8001] via 192.168.1.97, 00:00:28, Serial3/0
```

Рисунок 4.7 – Значення вартості маршруту від інтерфейсу 192.168.1.98 до інтерфейсу 192.168.1.49 через маршрутизатор 1

Якщо пакета надсилається з мережевої адреси маршрутизатора 0 безпосередньо на мережеву адресу маршрутизатора 2 із пропускною спроможністю 50 Кбіт/с, розрахунок вартості виглядатиме наступним чином:

$$\text{Вартість (загальна)} = \frac{100 \text{ Мбіт/с}}{50 \text{ Кбіт/с}} + \frac{100 \text{ Мбіт/с}}{100 \text{ Кбіт/с}} = 2001$$

Отже, вартість шляху до маршрутизатора 2 становить 2001. Це можна підтвердити ввівши на маршрутизаторі команду «show ip route» (рис. 4.8):

```
O 192.168.1.48 [110/2001] via 192.168.1.130, 00:00:39, Serial6/0
```

Рисунок 4.8 – Значення вартості маршруту від інтерфейсу 192.168.1.129 до інтерфейсу 192.168.1.49

З розрахунків вартості можна довести, що пакет даних пройде через маршрут з найменшою вартістю, а саме 2001, а не через шлях з вартістю 4001. В цьому експерименті є 2 маршрути з однаковою вартістю – 2001, тож OSPF може обрати будь-який з двох шляхів.

Результати тестування другого сценарію після роз'єднання зв'язку

Після того, як буде відомий маршрут, через який проходить пакет даних ICMP за допомогою команди ping, шлях, яким зазвичай проходить пакет роз'єднується, для виявлення резервного шляху, який має кожен протокол маршрутизації в кожній топології. Шлях, що роз'єднано, – це шлях, який з'єднує маршрутизатор 0 із маршрутизатором 3. Результати тестування виявилися такими:

1) Кільцева топологія EIGRP

Після роз'єднання зв'язку маршрут від ПК 0 до ПК 5 виглядає так: ПК 0 – комутатор 0 – маршрутизатор 0 – маршрутизатор 1 – маршрутизатор 2 – комутатор 2 – ПК 5. Пакет даних проходитиме через маршрут зі значенням метрики 52226560. Це відповідає результатам попередніх розрахунків метрики.

2) Сітчаста топологія EIGRP

Після роз'єднання зв'язку маршрут від ПК 0 до ПК 5 буде таким: ПК 0 – комутатор 0 – маршрутизатор 0 – маршрутизатор 2 – комутатор 2 – ПК 5. Пакет даних проходитиме через шлях з другим найменшим значенням метрики, а також він є найкоротшим шляхом серед всіх існуючих, а саме маршрут з метрикою 51714560. Це відповідає результатам попередніх обчислень метрики, де пакети даних не проходять через маршрут з більшою метрикою – 103426560.

3) Кільцева топологія OSPF

Після роз'єднання зв'язку маршрут від ПК 0 до ПК 5 буде таким: ПК 0 – комутатор 0 – маршрутизатор 0 – маршрутизатор 1 – маршрутизатор 2 – комутатор 2 – ПК 5. Пакет даних пройде через маршрут з вартістю 4001. Це відповідає результатам попереднього розрахунку вартості.

4) Сітчаста топологія OSPF

Після роз'єднання зв'язку маршрут від ПК 0 до ПК 5: ПК 0 – комутатор 0 – маршрутизатор 0 – маршрутизатор 2 – комутатор 2 – ПК 5. Пакет даних проходитиме через другий шлях з найменшим значенням вартості, а також найкоротший з усіх існуючих, а саме 2001. Це відповідає результатам попередніх розрахунків вартості, де пакети даних не проходитимуть через маршрути з більшою вартістю, а саме 4001.

Час конвергенції

У третьому сценарії досліджено час конвергенції, а саме час, протягом якого кожен маршрутизатор отримує інформацію від інших маршрутизаторів і готовий надсилати пакети.

Час конвергенції кільцевої топології EIGRP

Дізнаємось час конвергенції за допомогою команди «show ip EIGRP neighbors» за допомогою CLI на маршрутизаторі (рис. 4.9):

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num
0	192.168.1.2	Se3/0	11 00:07:20	40	1000	0	15
1	192.168.1.193	Se2/0	13 00:07:18	40	1000	0	15

Рисунок 4.9 – Час конвергенції змодельованої кільцевої топології EIGRP

На рисунку можна побачити в стовпці Hold (сек) час очікування пакетів Hello від інших маршрутизаторів. Цей час лежить в основі конвергенції на кожному маршрутизаторі, де інтервал Hello за замовчуванням становить 5 секунд, а інтервал утримання/вимкнення за замовчуванням становить 15 секунд. Отже, середній час конвергенції для кожного маршрутизатора становить:

$$\text{Середній час конвергенції} = \frac{13+13+11+14}{4} = 12,5 \text{ секунд}$$

Час конвергенції сітчастої топології EIGRP

Дізнаємось час конвергенції за допомогою команди «show ip EIGRP neighbors» за допомогою CLI на маршрутизаторі.

$$\text{Середній час конвергенції} = \frac{14+14+13+11}{4} = 13 \text{ секунд}$$

Час конвергенції кільцевої топології OSPF

Дізнаємось час конвергенції за допомогою команди «show ip OSPF neighbors» за допомогою CLI на маршрутизаторі (рис. 4.10).

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	0	FULL/ -	00:00:31	192.168.1.2	Serial2/0
1.1.1.1	0	FULL/ -	00:00:32	192.168.1.193	Serial3/0

Рисунок 4.10 – Час конвергенції змодельованої кільцевої топології OSPF

На рисунку можна побачити в стовпці Dead Time час очікування пакетів Hello від інших маршрутизаторів. Цей час лежить в основі конвергенції на кожному маршрутизаторі, де інтервал Hello за замовчуванням становить 10 секунд, а інтервал утримання/вимкнення за замовчуванням становить 40 секунд. Отже, середній час конвергенції для кожного маршрутизатора становить:

$$\text{Середній час конвергенції} = \frac{32+32+36+38}{4} = 34,5 \text{ секунд}$$

Час конвергенції сітчастої топології OSPF

Щоб дізнатися час конвергенції кільця OSPF, необхідно використати команду «show ip OSPF neighbors» за допомогою CLI на маршрутизаторі. Результати наступні:

$$\text{Середній час конвергенції} = \frac{32+36+39+34}{4} = 35,25 \text{ секунд}$$

Висновки з дослідження

За результатами тестування кільцевої та сітчастої мережевих топологій на протоколах маршрутизації EIGRP і OSPF зроблено такі висновки:

- 1) Під час тестування кільцевої топології загальне значення затримки для EIGRP на 386 мкс менше, для OSPF.
- 2) Під час тестування сітчастої топології загальне значення затримки OSPF було на 453 мкс меншим, ніж значення затримки EIGRP.
- 3) Для сітчастої топології протокол OSPF працює краще, ніж для EIGRP, оскільки він може обрати найкоротший шлях порівняно з EIGRP за тієї

самої пропускної здатності. Так відбувається тому, що обчислення значень вартості простіше, ніж обчислення значень метрики EIGRP.

4) OSPF є протоколом на основі стану каналу, тому пакети з однаковою вартістю надсилатимуться не завжди за найкоротшим, а іноді й за найдовшим маршрутом.

5) Середній час конвергенції для кільцевої топології EIGRP становить 12,75 секунди, а OSPF – 34,5 секунди.

6) Середній час конвергенції для сітчастої топології EIGRP становить 13 секунд, а для сітчастої топології OSPF – 35,25 секунди.

7) Інтервал утримання EIGRP становить 15 секунд, тоді як OSPF – 40 секунд, тому час збіжності мережі EIGRP менший, ніж OSPF.

Вибір між протоколами маршрутизації для корпоративних IP-мереж повинен враховувати конкретні потреби та характеристики самої мережі. На підставі проведених досліджень можна зазначити, що обидва протоколи, OSPF і EIGRP, мають свої переваги та обмеження.

Якщо пріоритетними є низька затримка та швидка конвергенція мережі в кільцевій топології, то протокол EIGRP стане чудовим вибором. Це може бути важливим для додатків, які вимагають високої продуктивності та мінімізації часу відновлення.

З іншого боку, якщо важливо мати більшу гнучкість у виборі найкоротших маршрутів, особливо в сітчастій топології, та простіше обчислення вартостей, то OSPF може бути більш оптимальним варіантом. Особливо це актуально для мереж, де важливо ефективно використовувати ресурси та мінімізувати загальну затримку.

Таким чином, обираючи між OSPF і EIGRP для корпоративної мережі, слід враховувати конкретні вимоги до продуктивності, ступінь складності конфігурації та адаптивність до змін у топології. Вирішальним фактором також може бути вартість утримання та ресурси, що доступні для адміністрування мережі.

4.3 Висновки з розділу 4

1) Мета проведення дослідження полягає в об'єктивному визначенні, який з протоколів маршрутизації, OSPF чи EIGRP, виявиться більш ефективним для корпоративних IP-мереж, а також у визначенні оптимальної топології для кожного з цих протоколів. Оскільки кожен з протоколів маршрутизації має свої унікальні характеристики, дослідження було проведено з використанням протоколів маршрутизації OSPF і EIGRP та протестоване через моделювання.

2) Для моделювання було використане програмне забезпечення Cisco Packet Tracer. З його допомогою була розроблена корпоративна IP-мережа, та налаштовано моделювання передачі даних в мережі, використовуючи кільцеву та сітчасту топології із застосуванням протоколів маршрутизації EIGRP та OSPF. Чотири маршрутизатори було налаштовано з використанням кільцевої та сітчастої топології.

3) В ході проведення дослідження було здійснено перевірку з'єднань між вузлами мережі для визначення часу, необхідного для передачі даних. Було відстежено маршрут для визначення шляхів, якими пройде пакет даних. Також у симуляції один із зв'язків було роз'єднано для визначення шляху, який використовуватиметься після роз'єднання. Параметри метрики та вартості в моделі також порівняно з розрахунками за формулою для визначення точності результатів моделювання.

4) Проаналізувавши результати дослідження було з'ясовано, що вибір між OSPF і EIGRP для корпоративних IP-мереж повинен враховувати конкретні потреби та характеристики самої мережі. Обидва протоколи мають свої переваги та обмеження. Якщо пріоритетними є низька затримка та швидка конвергенція в кільцевій топології, EIGRP може бути кращим варіантом. З іншого боку, для більшої гнучкості у виборі найкоротших маршрутів та простоти вартостей, OSPF може виявитися більш оптимальним протоколом маршрутизації. Кінцевий вибір також залежить від вимог до продуктивності, складності конфігурації та адаптивності до змін у топології, а також вартості утримання та наявних ресурсів для адміністрування мережі.

ВИСНОВКИ

На підставі проведеного дослідження можна зробити наступні висновки.

Розглянуто основні поняття та принципи внутрішньої маршрутизації, проведено детальний аналіз протоколів внутрішньої маршрутизації. Визначено способи класифікації протоколів динамічної маршрутизації, а саме: за призначенням, за дією, за поведінкою. Виявлено, що в сучасних мережах рекомендується використовувати безкласові протоколи внутрішньої маршрутизації, такі як RIPv2, EIGRP, OSPF, для досягнення оптимальної маршрутизації.

На основі порівняння протоколів маршрутизації було визначено, що для невеликих мереж із обмеженими ресурсами, простий протокол, такий як RIPv2, може бути відмінним вибором, тоді як великим мережам доцільніше використовувати протоколи EIGRP, OSPF або IS-IS з вищою швидкістю та масштабованістю.

Розглянуто дистанційно-векторні протоколи та протоколи за станом каналу, проаналізовано їх переваги й недоліки, з чого можна зробити висновок, що вибір між дистанційно-векторними та протоколами маршрутизації за станом каналу залежить від розміру та характеристик конкретної мережі, а також від вимог до швидкодії та ефективності маршрутизації.

Виявлено, що протокол OSPF представляє собою ефективну альтернативу протоколу маршрутизації за векторами відстані RIP, який використовувався на ранніх етапах розвитку мережевих технологій. Завдяки безкласовості та використанню концепції областей, OSPF забезпечує швидшу збіжність та масштабованість, що робить його ефективним рішенням для великих мереж.

Виявлено, що до переваг застосування протоколу EIGRP відноситься швидка збіжність, ефективне використання пропускної здатності, використання можливих наступників та ієрархічна структура роблять EIGRP привабливим вибором для складних корпоративних середовищ. Але перед вибором протоколу EIGRP, слід враховувати його особливості та підготувати відповідні ресурси для оптимальної конфігурації та управління.

Проведено дослідження, мета якого полягає в об'єктивному визначенні, який з протоколів маршрутизації, виявиться більш ефективним для корпоративних IP-мереж, а також у визначенні оптимальної топології для кожного з цих протоколів. Оскільки кожен з протоколів маршрутизації має свої унікальні характеристики, дослідження було проведено з використанням протоколів маршрутизації OSPF і EIGRP та протестоване за допомогою моделювання.

Проаналізувавши результати дослідження було з'ясовано, що вибір між OSPF і EIGRP для корпоративних IP-мереж повинен враховувати конкретні потреби та характеристики самої мережі. Обидва протоколи мають свої переваги та обмеження. Якщо пріоритетними є низька затримка та швидка конвергенція в кільцевій топології, EIGRP може бути кращим варіантом. З іншого боку, для більшої гнучкості у виборі найкоротших маршрутів та простоти вартостей, OSPF може виявитися більш оптимальним протоколом маршрутизації. Кінцевий вибір також залежить від вимог до продуктивності, складності конфігурації та адаптивності до змін у топології, а також вартості утримання та наявних ресурсів для адміністрування мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Програма мережевої академії Cisco CCNA 7.0 «Switching, Routing, and Wireless Essentials» – електронний курс.
2. Routing and Switching Essentials v6 Companion Guide. Cisco Press, 2016
3. IPv4 Routing Protocol Concepts. Cisco Press [Electronic resource]. — Mode of access:
<https://www.ciscopress.com/articles/article.asp?p=2262897&seqNum=5>
4. Types of Routing Protocols – The Ultimate Guide. Comparitech [Electronic resource]. — Mode of access: <https://www.comparitech.com/net-admin/routing-protocol-types-guide/>
5. Динамічна маршрутизація в IP-мережах. Протокол OSPF: Навч. посібник / С. В. Панченко, С. І. Приходько, О. С. Жученко та ін. – Харків: УкрДУЗТ, 2018. – 209 с.
6. Cisco Networking Academy's Introduction to Routing Dynamically. Cisco Press [Electronic resource]. — Mode of access:
<https://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=11>
7. What is IP Routing? Types, Routing Table, Protocols, Commands [Electronic resource]. — Mode of access: <https://www.guru99.com/ip-routing.html>
8. Мережна маршрутизація та комутація: навчально-методичний посібник / Полякова Н. П.; Запорізька державна інженерна академія. – Запоріжжя: ЗДІА, 2018. – 160с.
9. TCP/IP network administration. Configuring routing [Electronic resource]. — Mode of access:
https://www.cs.ait.ac.th/~on/O/oreilly/tcpip/tcpip/ch07_04.htm
10. OSPF Cost and SPF Algorithm. IPCisco.com [Electronic resource]. — Mode of access: <https://ipcisco.com/lesson/ospf-cost-and-spf-algorithm/>
11. Tanenbaum A.S., Computer Networks, 5th Ed./ Andrew S. Tanenbaum, David J. Wetherall. – Prentice Hall, Cloth, 2011. – 960 p.

12. Cisco Networking Academy's Introduction to Routing Dynamically. Cisco Press [Electronic resource]. — Mode of access:
<https://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=11>
13. Жураковський, Б. Ю. Комп'ютерні мережі. Частина 1. Навчальний посібник — Київ : КПІ ім. Ігоря Сікорського, 2020. — 328 с.
14. EIGRP Network Design Solutions. Cisco Press [Electronic resource]. — Mode of access:
https://api.pageplace.de/preview/DT0400.9781587058950_A23907356/preview-9781587058950_A23907356.pdf
15. Карпенко М. Ю. Конспект лекцій з курсу «Комп'ютерні мережі» (для студентів усіх форм навчання спеціальностей 122 – Комп'ютерні науки, 151 –Автоматизація та комп'ютерно-інтегровані технології, 126 – Інформаційні системи та технології) / М. Ю. Карпенко, Н. В. Макогон; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. — Харків : ХНУМГ ім. О. М. Бекетова, 2019. — 99 с.
16. Комп'ютерні мережі : курс лекцій / Ю. В. Волосюк. — Миколаїв: МНАУ, 2019. — 203 с.
17. Комп'ютерні мережі : навчальний посібник / [Азаров О. Д., Захарченко С. М., Кадук О. В. та ін.] — Вінниця : ВНТУ, 2013. — 371 с.
18. Performance Analysis of RIPv2, OSPF and EIGRP Protocols using Cisco Packet Tracer Simulator 7.2. Murali Krishna M, Prasantha R. Mudimela, Pitcheri Praveen Kumar // International Journal of Engineering and Advanced Technology (IJEAT), Volume-9 Issue-3, February, 2020