МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
УМАНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ САДІВНИЦТВА
Факультет економіки і підприємництва
Кафедра інформаційних технологій

Допущено до захисту
"_____" _____ 2023 р.
Зав. кафедри, к.т.н., доцент
_____ **Ліщук Р.І.**

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ

Виконав – студент 2 курсу, групи 21м-кн
освітньої програми "Комп’ютерні науки"
спеціальності 122 Комп’ютерні науки
Недбайло Владислав Віталійович

Науковий керівник – к.т.н., доцент
Ліщук Роман Ігорович

Умань – 2023

Зміст

ВСТУП 3

РОЗДІЛ 1 АНАЛІЗ ПРОБЛЕМИ ТА ПОСТАНОВКА ЗАДАЧІ 5

1.1. Аналіз проблеми..... **Помилка! Закладку не визначено.**

1.2. Підходи до локалізації об’єктів інтересу на зображенні ... **Помилка! Закладку не визначено.**

1.3. Постановка задачі 6

РОЗДІЛ 2 ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ КЛАСИФІКАЦІЙНОГО АНАЛІЗУ ДЕРМОСКОПІЧНИХ ЗОБРАЖЕНЬ 17

2.1. Архітектура екстрактора ознак..... 17

2.2. Архітектура детектора..... 19

2.3. Метрики оцінки ефективності класифікатора ..... **Помилка! Закладку не визначено.**

РОЗДІЛ 3 ПРОГРАМНА РЕАЛІЗАЦІЯ ТА АНАЛІЗ РЕЗУЛЬТАТІВ..... 25

3.1. Формування вхідного математичного опису**Помилка! Закладку не визначено.**

3.2. Короткий опис програмної реалізації системи**Помилка! Закладку не визначено.**

3.3. Аналіз результатів моделювання**Помилка! Закладку не визначено.**

ВИСНОВКИ..... 37

СПИСОК ЛІТЕРАТУРИ..... 48

ДОДАТКИ..... 50

ВСТУП

Робота великих телекоммунікаційних мереж, переміщення повідомлень між різними підмережами та досягнення ними кінцевих пунктів призначення майже неможливі без забезпечення функціонування технології динамічної маршрутизації. Застосування протоколів динамічної маршрутизації значно полегшують роботу мережевим інженерам та адміністраторам, так як дозволяє уникнути необхідності ручного налаштування всіх маршрутів, що значно знижує ризики виникнення можливих помилок в мережі в майбутньому. Головною метою протоколів динамічної маршрутизації є забезпечення передачі пакетів даних від точки до точки через мережу [1].

Існує багато протоколів динамічної маршрутизації, таких як DSR (Dynamic Source Routing), RIP (Routing Information Protocol), BGP (Border Gateway Protocol) та ін., а також протокол OSPF, який розглядається в даній роботі в порівнянні з EIGRP протоколом.

Open Shortest Path First (OSPF) – це адаптивний інструмент для передачі інформації про маршрути в межах однієї автономної системи. Протокол OSPF є динамічним протоколом, який надає мережі більше стабільності та забезмечує сумісність.

Другий протокол, який використовується в даній роботі, це протокол Enhanced Interior Gateway Routing Protocol (EIGRP), це безкласовий протокол маршрутизації. Завдяки ряду переваг EIGRP протокол широко використовується в корпоративних мережах. Цей протокол використовує ефективний алгоритм DUAL (Diffusing Update Algorithm) для заходження оптимального шляху до цільової мережі без петель [2]. Таким чином, об'єктом дослідження даної роботи було обрано технології забезпечення динамічної маршрутизації. Ще на початковому етапі проектування мережі адміністратор повинен мати чітке розуміння, який з застосованих протоколів виявиться найбільш ефективним в тих чи інших створених умовах роботи мережі.

Таким чином, встановлення недоліків та переваг таких поширених протоколів динамічної маршрутизації, як EIGRP та OSPF, та способів підвищення показників їхньої ефективності визначено предметом дослідження даної роботи.

В ході даної роботи змодельовано корпоративну мережу з конфігурацією OSPF протоколу, було складено рекомендації відносно зменшення обсягу трафіку протоколу задля збереження пропускної здатності каналу зв’язку, а також з метою відстеження пошкоджень та несправностей в топології мережі створено програмний додаток. Отримані результати дослідження можуть стати у нагоді мережевим інженерам, як під час практичного проектування та налаштування комп'ютерних мереж, так і у вивченні протоколу OSPF, як технології динамічної маршрутизації.

РОЗДІЛ 1 ДИНАМІЧНА МАРШРУТИЗАЦІЯ ТА ХАРАКТЕРИСТИКА ЇЇ ПРОТОКОЛІВ

1.1. Динамічна маршрутизація: принципи роботи та основні задачі

Динамічна (адаптивна) маршрутизація визначається здатністю маршрутизатора самостійно визначати нові шляхи, або змінювати дані про вже наявні [3]. Даний тип маршрутизації найбільш широко застосовується у великих мережах, що мають різні за своїми характеристиками канали та надлишкові лінії. Здатність динамічної маршрутизації швидко адаптуватися до відстежуваних змін топології та стану з'єднань [4], та знаходити альтернативний шлях відповідно до змін поточного стану мережі, забезпечують їй перевагу над статичною маршрутизацією, яка, в порівнянні, у разі модифікації структури мережі, потребує ручного переналаштування маршрутів лише після того, як така зміна вже сталася.

Динамічна маршрутизація є найскладнішою функцією мережі, а тому й найбільшою життєво важливою. До основних функцій адаптивної маршрутизації належать наступні:

1. Динамічне виявлення доступних маршрутів, що виключає необхідність попереднього налаштування кінцевих систем і маршрутизаторів між ними під час топологічних змін [5].

2. У разі виникненні перевантажень або несправностей на лінії допускається зміна маршрутів, що дозволяє досягнути ефективного балансування навантаження та зберегти досяжність кінцевої мережі у випадку втрати нод або зв'язку між ними. В залежності від характеристик всі протоколи маршрутизації поділяються на дві основні категорії [6]: протоколи внутрішнього (IGP) та зовнішнього (EGP) шлюзу (рис. 1.1).

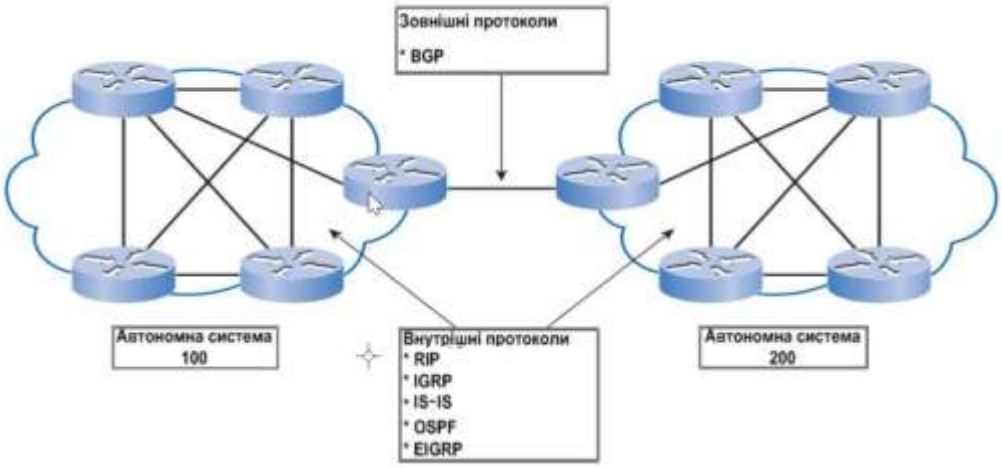


Рис. 1.1 - Групи протоколів маршрутизації

Для більш чіткого розуміння різниці між поданими групами протоколів слід дати визначення поняттю «автономна система». Автономна система (АС) – це група мереж, які перебувають під спільним адміністративним керуванням і в якій застосовуються однакові правила маршрутизації. Слід зазначити, що АС сприймається зовнішніми мережами як єдиний об’єкт. Таким чином, протоколи внутрішньої маршрутизації застосовуються в межах окремої АТ, а зовнішні, відповідно, використовуються для з’єднання автономних систем між собою.

Протоколи маршрутизації внутрішнього шлюзу поділяються на Distance-Vector (DVA) та Link State (LSA). До головних відмінностей між даними видами належать різниця в типах даних якими обмінюються маршрутизатори (таблиця маршрутизації для DVA, та таблиця топології для LSA), процесі визначення оптимального шляху та відомостях роутера про мережу (DVA – мають уявлення лише по сусідів, LSA - володіють інформацією про мережу вцілому) [7].

Незважаючи на те, що кількість актуальних протоколів досить незначна, можлива ситуація, коли на маршрутизаторі запускається відразу декілька протоколів з різною логікою вибору оптимального маршруту. Для того щоб відповісти на питання, який маршрут обере роутер в даному випадку, потрібно дати визначення терміну «адміністративна дистанція». Адміністративна дистанція (АД), яка також називається адміністративною відстанню, – це

ступінь надійності джерела маршрутної інформації, виражена у вигляді цілого значення від 0 до 255. Тобто, чим нижче значення має адміністративна відстань, тим більший пріоритет довіри у джерела маршруту. Приклади значень АД за замовчуванням для протоколів, які підтримуються Cisco наведено в Таблиці 1.1.

Таблиця 1.1. Пріоритет джерел маршрутів відповідно величини АД

Протокол	Адміністративна дистанція
Connected (підключений інтерфейс)	0
Static (статичний інтерфейс)	1
Протокол NDP	2
Об’єднаний маршрут по протоколу EIGRP	5
Протокол BGP	20
Внутрішній протокол EIGRP	90
Протокол IGRP	100
Протокол OSPF	110
Протокол IS-IS	115
Протокол RIP	120
Протокол EGP	140
Протокол ODR	160
Зовнішній протокол EIGRP	170
Внутрішній протокол BGP	200
Unknown (Невідомий)	255

1.2. Протокол динамічної маршрутизації Enhanced Interior Gateway Routing Protocol (EIGRP)

IGRP (англ. Interior Gateway Routing Protocol) - протокол маршрутизації DVA, який був спроектований фірмою Cisco та застосовується в TCP/IP та OSI мережах. Перша IP-версія протоколу була розроблена та успішно впроваджена

у 1986 році. IGRP розглядається як IGP-протокол, але він також широко застосовується як EGP для міждоменної маршрутизації [10].

Інформація про відстань в IGRP представляє собою набір відомостей, які дозволяють точно налаштовувати характеристики каналу для вибору оптимальних маршрутів, а саме:

- доступної смуги пропускання;

- часу затримки;

- завантаження та надійності каналу зв'язку.

EIGRP (Enhanced Interior Gateway Routing Protocol) – це покращена версія IGRP, де використовується та ж технологія DVA, та основна дистанційна інформація залишається незмінною. За разунок EIGRP протоколу забезпечується сумісність та повна взаємодія з IGRP роутерами. За замовчуванням маршрути IGRP мають вищий пріоритет, ніж маршрути його розширеної версії. Властивості збіжності та ефективність роботи цього протоколу були значно покращені [10].

В EIGRP для отримання безпетлевих маршрутів у кожен момент часу їх розрахунку застосовується розподілений оновлюваний алгоритм DUAL, що дозволяє синхронізувати всі маршрутизатори, що у зміні топології. Маршрутизатори, на які не впливають зміни топології, не беруть участь у цьому процесі.

EIGRP протокол включає наступні головні складові[9]: Neighbor Discovery and Recovery – виявляє та відновлює сусідні маршрутизатори, Reliable Transport Protocol (RTP) - надійний транспортний протокол, DUAL Finite State Machine - кінцеві станів алгоритму DUAL, Protocol Dependent Modules (PDM) - залежні від протоколів модулі.

Протокол EIGRP використовує п'ять типів пакетів [8, 10]:

- HELLO/ACK – multicast-пакети, що надсилаються для виявлення/відновлення сусіда, які не потребують підтвердження отримання. Пакет HELLO, який не містить даних, так само використовується в якості

підтвердження. Пакет підтвердження ACK завжди надсилається в режимі поодинокого відправлення та включає в себе ненульовий номер підтвердження;

- UPDATE - пакети з оновленнями, які застосовуються для надсилання характеристик вузлів призначення. Щойно сусіда встановлено, йому надсилаються UPDATE пакети для створення його власної таблиці топології. Оновлення завжди передаються із підтвердженням;

- QUERY та REPLY. Пакети QUERY запитів та REPLY відгуків відправляються з переходом маршрутів призначень до активного стану. У випадку якщо QUERY пакети вони не надсилаються у unicast режимі у відповідь на запит, вони запит завжди відправляють у режимі multicast. З метою сповіщення того, хто надіслав запит, про те, що переходити в активний стан не потрібно через наявність можливих наступних елементів у того, що відповідає, у відповідь на QUERY запит завжди відсилаються REPLY пакети., Пакети REPLY надсилаються в режимі поодинокої відправки запитувачу. Запити та відповіді передаються з підтвердженням;

- REQUEST-пакети використовуються для отримання специфічних (конкретних потрібних в даний момент) даних від одного або кількох сусідів, можуть передаватися в multicast- або unicast-режимах. Запити передаються із негарантованою доставкою.

Метрика EIGRP заснована на 5 компонентах [11]:

1) bandwidth (BW) –пропускна спроможність (виражено в Кбіт/с). Для розрахунку вартості маршруту обирається найменьше значення до цільової мережі. Зміна даного показника впливає лише на визначення вартості;

2) delay ($DELAY$) – визначає сумарний час (в мікросекундах) затримки пакету по всьому шляху;

3) reliability (REL) – динамічний показник (від 0-250) визначає ймовірність втрати з’єднання. Розраховується на підставі отримання keepalive-повідомлень.;

4) load ($LOAD$) –показник завантаженності каналу (від 1-255, 255 – навища ступінь завантаження) на всьому маршруті. Розраховуються залежно від рівня передачі пакетів та конфыгурації пропускної спроможності на інтерфейсах;

5) MTU –найменший показник MTU всього маршруту, який хоча і входить до складу EIGRP оновлень, та практично не застосовується у підрахунку EIGRP метрики.

За стандартом технології в EIGRP метриці головне використовуються два показники, BW та DELAY, оскільки застосування інших критеріїів може стати причиною частих перерахунків маршрутів.

Технологія EIGRP для підрахунку метрики використвоує K характеристики, які надсилаються HELLO пакетами. Дефолтні значення коефіцієнтів виражено:

Якщо $K5 = 0$, то приватна при REL визначається як 1.

Загальна метрика обчислюється за допомогою значень BW та $DELAY$. Використовується така формула для обчислення значення BW:

$$BW = \frac{1000000}{BW_i} \cdot 256, \quad (1)$$

де BWi є найменшою пропускною спроможністю з усіх вихідних інтерфейсів на шляху до мережі призначення, представлена в кілобітах.

Формула для обчислення значення $DELAY$:

$$DELAY = DELAYi \cdot 256, \quad (2)$$

де $DELAYi$ є сумою всіх затримок, налаштованих на вихідних інтерфейсах на шляху до мережі призначення, в десятках мікросекунд.

EIGRP використовує отримані значення під час підрахунку загальної метрики.

При обчисленні метрики, коли $K5 = 0$ (значення за замовчуванням), використовується формула

$$metric_1 = K_1 BW + \frac{K_2 BW}{256 - LOAD} + K_3 DELAY \quad (3)$$

Якщо значення коефіцієнтів $K1$, $K2$, $K3$ дорівнюють значенням за умовчанням, то формула набуває такого вигляду:

$$metric1 = BW + DELAY \quad (4)$$

Якщо $K5$ не дорівнює 0, то додатково виконується така операція:

$$metric_2 = metric_1 \cdot \frac{K_5}{REL + K_4} \quad (5)$$

Таким чином, складова метрика EIGRP дозволяє оптимально налаштовувати роботу мереж передачі даних.

1.3. Протокол динамічної маршрутизації Open Shortest Path First (OSPF)

Протокол OSPF (Open Shortest Path First) –це сучасний протокол, який служить для маршрутизації трафіку TCP/IP. Протокол OSPF належить до внутрішніх протоколів маршрутизації - це означає, що маршрутна інформація поширюється серед роутерів однієї АС. Протокол OSPF працює на основі технології SPF (або link-state – стан каналу) та, на відміну від дистанційно-векторних протоколів, таких як RIP, у протоколі OSPF та інших протоколів з урахуванням стану каналу, маршрутизатори спочатку вивчають всю архітектуру мережі і тільки після цього виконується розрахунок найкоротших шляхів [9].

Протокол OSPF підготовлений однойменною робочою групою IETF і призначений для використання у середовищах TCP/IP. Протокол підтримує безкласову адресацію та встановлення міток (англ. tagging) під час використання зовнішньої маршрутної інформації. Також OSPF використовує аутентифікацію та групову адресацію (англ. IP multicast) під час обміну маршрутними повідомленнями.

OSPF забезпечує маршрутизацію IP пакетів виключно на основі IP-адрес одержувачів, які визначаються заголовком IP пакетів. Пакети IP

маршрутизуються без змін, тобто інкапсуляція в інші пакети не використовується. OSPF є динамічним протоколом маршрутизації, що забезпечує швидке виявлення топологічних змін в АС (наприклад, збої маршрутизаторів або каналів) та розрахунок нових безпетлевих (англ. loop-free) альтернативних маршрутів. Період збіжності (англ. convergence) – розрахунок нового маршруту - досить короткий і рівень службового трафіку невеликий [9].

У протоколах з урахуванням стану каналів кожен маршрутизатор підтримує базу даних із описом топології автономної системи. Ці бази називають базами даних про стан каналів (англ. link-state database). Бази даних всіх маршрутизаторів однієї області ідентичні. Кожен елемент бази даних представляє собою локальний стан окремого маршрутизатора (наприклад, інтерфейси, що підтримуються, або доступні сусіди). Маршрутизатори розповсюджують інформацію про свій локальний стан шляхом лавинної маршрутизації (англ. flooding).

Усі маршрутизатори працюють паралельно, використовуючи однаковий алгоритм. На основі базами даних про стан каналів кожен маршрутизатор будує свого роду дерево найкоротших шляхів, корінням якого є маршрутизатор. Це дерево містить маршрути до всіх адресатів усередині АС. Маршрутна інформація зовнішнього походження представляється як листя дерева.

За наявності кількох шляхів рівної вартості одного адресату трафік порівну розподіляється між усіма маршрутами (по кожному з маршрутів пакети відправляються поперемінно). Вартість маршруту описується безрозмірною метрикою, яка подається у вигляді одного числа. За замовчуванням у цій метриці враховується пропускна спроможність каналів зв'язку. Наприклад, для Ethernet значення дорівнює 10, Fast Ethernet – 1, для каналу Т-11 – 65, для каналу з пропускною спроможністю 56 Кбіт/с – 1785. За наявності високошвидкісних каналів, таких як Gigabit Ethernet, адміністратору потрібно задати іншу шкалу швидкостей, призначивши одиничну відстань найбільш швидкісному каналу [6]. Допускається застосування інших метрик, одна з них враховує затримки, а інша – надійність передачі пакетів каналами зв'язку. OSPF

протокол конфігурує таблицю маршрутизації відповідно до кожної окремої метрики. Вибір потрібної таблиці відбувається залежно від значень бітів TOS (англ. Type of Service) у заголовку IP-пакета, що прийшов.

OSPF дозволяє групувати мережі в області. Топологія кожної окремої області невидима решті АС. Такого роду маскування надлишкових даних дає змогу відчутно зменшити показники службового трафіку.

З метою убезпечення використання зонами мережі некоректних даних, процес встановлення оптимального маршруту в межах певної зони обмежується топологією винятково цієї зони, де поняття зони (області) є узагальненням IP підмереж.

OSPF забезпечує можливість гнучкого налаштування підмереж IP. Кожен маршрут в OSPF поширюється із зазначенням адресата та маски підмережі. Дві різних підмережі однієї мережі IP можуть мати різні розміри (тобто різні маски). Маршрути до хостів розглядаються як шляхи підмережі з маскою з одних одиниць (0xffffffff або 255.255.255.255).

Протокол OSPF інкапсулюється в IP, використовуючи ідентифікатор 89 та не вимагає ніякої додаткової фрагментації або збирання пакетів – у разі такої необхідності використовується звичайна фрагментація та складання IP. Пакети протоколу OSPF мають такий формат, що великі блоки протокольної інформації можна легко розділити на дрібніші пакети.

Усі пакети протоколу OSPF використовують однотипні заголовки. Протокол OSPF використовує пакети Hello для організації та підтримки сусідських відносин. Пакети Database Description (опис бази даних) та Link State Request (запит стану каналу) слугують для підтримки відносин суміжності. Гарантований обмін оновленнями OSPF базується на обміні пакетами Link State Update (оновлення стану каналу) та Link State Acknowledgment (підтвердження прийому оновлення). Типи пакетів OSPF наведено в Таблиці 2.1.

Таблиця 2.1 – Типи пакетів OSPF протоколу

Тип	Назва	Призначення
1	Hello	Виявлення та підтримка сусідства
2	Database Description	Резюмування змісту бази даних
3	Link State Request	Завантаження бази даних
4	Link State Update	Оновлення бази даних
5	Link State Acknowledgment	Підтвердження лавинної розсилки

Кожен пакет Link State Update містить набір нових анонсів стану каналів (англ. link-state advertisement, LSA – оголошення про стан каналу) наодин інтерв ал (англ. hop), віддалених від пункту генерації анонсу. Один пакет Link State Update може містити анонси LSA від кількох маршрутизаторів. Кожний запис LSA позначається ідентифікатором маршрутизатора, що створив анонс, і супроводжується контрольною сумою вмісту. У кожному записі LSA є також поле типу. Можливі варіанти цього поля описані у Таблиці 2.2

Таблиця 2.2 – Типи анонсів LSA в OSPF протоколі

Тип	Ім’я LSA	Опис LSA
1	Router-LSA	Генеруються всіма маршрутизаторами. Цей тип LSA визначає стан інтерфейсів маршрутизатора в області. Анонс розсилається в лавинному режимі всередині області.
2	Network-LSA	Генерується виділеним маршрутизатором DR для широкомовних та NBMA-мереж. Цей тип LSA включає список маршрутизаторів, підключених до мережі. Розсилається у лавинному режимі всередині області.

3, 4	Summary-LSA	Генерується граничними маршрутизаторами областей та розсилається в лавинному режимі в межах пов'язаної з LSA області. Кожен анонс summary-LSA описує маршрут до адресата поза межами даної області, але всередині даної АС (міждоменний маршрут). Тип 3 summary-LSA описує маршрути в мережі, а тип 4 - описує маршрути до граничних маршрутизаторів АС.
5	External-LSA	Генерується граничними маршрутизаторами AS і розсилається по всієї автономної системи. Кожен анонс AS-external-LSA описує маршрут до адресатів до іншої AS. Прийняті за замовчуванням маршрутизатори AS можуть описуватися в AS-external-LSA.

Пакети протоколу OSPF (за винятком пакетів Hello) передаються лише між суміжними маршрутизаторами. Це означає, що всі пакети протоколу OSPF проходять лише один інтервал між маршрутизаторами, за винятком тих ситуацій, коли суміжність підтримується через віртуальні з'єднання (англ. virtual adjacency). IP-адреса відправника пакету OSPF є адресою одного із суміжних маршрутизаторів, а IP-адреса одержувача є адресою другого із суміжних маршрутизаторів або груповою IP-адресою [7].

Таким чином, до основних переваг OSPF можна віднести наступне: висока швидкість збіжності в порівнянні з протоколами, що використовують дистанційно-векторну маршрутизацію; підтримка мереж зі змінним розміром (робота з мережевими масками змінної довжини); оптимальне використання пропускної спроможності (низький рівень службового трафіку) за рахунок побудови дерева найкоротших шляхів, що дозволяє використовувати даний протокол навіть у дуже великих мережах (висока масштабованість).

Однак, слід зазначити, що OSPF протоколу також властиві певні недоліки, а саме, складність, яка вимагає грамотного планування, більш комплексного налаштування та адміністрування. Ще одним недоліком є те, що через використання алгоритму Дейкстри під час побудови дерева найкоротших шляхів протокол не захищає мережу від навантажень, тобто відстеження завантаження каналу у поступовій динаміці відсутнє, що, в свою чергу, створює необхідність впровадження допоміжних методів для зменшення ризиків перевантаження лінії.

1.4. Постановка задачі

Виходячи з наведених результатів огляду літературних джерел постановку задачі можна сформулювати наступним чином:

1. Провести аналіз якісних показників найбільш використовуваних протоколів маршрутизації мереж (OSPF, EIGRP), з метою визначення їхніх переваг та явних недоліків.

2. Спираючись на раніше отримані дані побудувати модель корпоративної мережі у середовищі графічного симулятора на OPNET Modeler та встановити способи підвищення продуктивності протоколів адаптивної маршрутизації.

3. Написати програмне забезпечення, що дозволить виявляти проблемні області в корпоративній мережі ще на стадії моніторингу мережі.

РОЗДІЛ 2 ДОСЛІДЖЕННЯ ПРОДУКТИВНОСТІ EIGRP ТА OSPF ПРОТОКОЛІВ З ВИКОРИСТАННЯМ ПРОГРАМНОГО СЕРЕДОВИЩА OPNET

2.1. Огляд функцій програмного додатку OPNET Modeler

В наш час для моделювання та дослідження інформаційних систем та мереж широко застосовуються інформаційні технології, які виражаються у створенні різноманітних спеціалізованих програмних продуктів. Таке програмне забезпечення надає можливість більш вивчати об’єкт дослідження всесторонньо та більш ґрунтовно завдяки вбудованим аналітичним та імітаційним методам моделювання. До програмних засобів, які використовуються в моделюванні та дослідженні мереж належать такі, як OPNET Modeler, OMNeT, NS-2, NS-3, Cisco Packet Tracer та ін.

Інструментом моделювання в межах даної роботи було обрано Optimized Network Engineering Tools (OPNET) Modeler. OPNET Modeler є найпопулярнішим продуктом компанії OPNET, який було розроблено для моделювання комп'ютерних мереж. Він широко використовуються в сфері освіти для викладання тем з передачі даних та комп'ютерних мереж, а також в промисловості для моделювання, вивчення, аналізу та прогнозування ефективності різних мережевих систем. Точність результатів, багатий функціонал і простота використання є основними перевагами цього програмного пакету. OPNET Modeler дозволяє користувачам розробляти власні моделі, які імітують нові протоколи або модифікації існуючих протоколів.

OPNET Modeler — це програма зі зручним графічним інтерфейсом, яка пропонує комплексну бібліотеку мережевих протоколів та моделей, за допомогою яких можливе створення практично будь-якої існуючої мережі на основі моделювання та аналізу мереж з метою порівняння впливу різних сценаріїв та технологій на поведінку мережі в цілому.

OPNET Modeler завдяки своїй зручності та функціональності може використовуватися під час виконання широкого спектру задач, таких як

налаштування та тестування якісних показників протоколів зв'язку, проектування та підвищення ефективності мережі, перевірки коректності моделі мережі з точки зору аналітики, та ін. [13]. До особливостей OPNET Modeler в порівнянні з іншими симуляторами відносяться:

- потужний високорівневий інструмент симуляції подій мережевого рівня;

- використовуватися як інструмент дослідження, або як інструмент проектування чи аналізу мережі;

- працює з різними типами програм для створення комунікаційних мереж, компіляції протоколів та програмування додатків;

- має широкий спектр інструментів для проектування, аналізу, а також створення моделей різних типів мереж, та дослідження їх продуктивності;

- прискорює процес досліджень та розробок потрібних для аналізу та проектування комунікаційних мереж, протоколів, пристроїв та програм.

Функції пакету програми Opnet Modeler можна розділити на три групи, а саме:

1) Перша група функцій підтримує імітаційне моделювання мереж, сегментів та пристроїв за допомогою попередньо встановленої бібліотеки об'єктів. Детальна модель реальної мережі створюється шляхом перетягування необхідних об'єктів в проектний редактор та їх з’єднанням сполучними лініями. До палітри об'єктів включено досить широкий спектр елементів палітри, більше того, з метою максимального наближення моделі до реальної мережі розроблена доступна функція налаштування кожного пристрою окремо. Опція детальної статистики забезпечує проведення аналізу якісних показників роботи мережі наприкінці симуляції.

2) Друга група функцій забезпечує створення користувачів об'єктів (кінцевих, мережевих, протоколів, та ін.)

3) Третя група включає комплект утиліт для всебічного дослідження налаштувань мережі за рахунок їх перенесення в Opnet середовище. Опцію імпорту підтримують конфігураційні файли окремих пристроїв, дані про інтерфейси та сполучні лінії, та ін.

2.2. Конвергенція протоколів динамічної маршрутизації

Завдяки своїм характеристикам, таким як висока пропускна здатність, гнучкість, масштабованість, простота в конфігурації, протоколи динамічної маршрутизації є напрямком, який найбільш швидко розвивається в галузі мережевих технологій. Та все ж, час конвергенції є критичною проблемою для будь-якого з динамічних протоколів, так як вона характеризує, як швидко відбувається сходження маршрутизації у разі зміни топології. Саме показники конвергенції і було прийнято за основну підставу для оцінки під час порівняння та аналізу продуктивності роботи протоколів адаптивної маршрутизації в даній роботі.

Конвергенція, або збіжність, - це процес узгодження між роутерами мережі даних про доступні маршрути. Важливим моментом є те, щоб у разі змін, що відбулися в мережі, обмін оновленнями відновив узгоджену мережеву інформацію. Час збіжності - це час, який було витрачено маршрутизатором для обміну інформацією, перерахунку найоптимальнішого маршруту та оновлення таблиць маршрутизіції. Більшість мереж потребує короткого часу конвергенції, адже мережа не може функціонувати повноцінно, доки мережа не зходиться. Наприклад, у разі відмови одного з роутерів, іншим роутерам мережі необхідно перерахували маршрути та вибрали оптимальний, тому дуже важливо, щоб повідомлення про оновлення мережі дійшло до інших роутерів якнайшвидше. Алгоритми з повільною конвергенцією можуть стати причиною виходу з ладу всієї мережі.

До часових витрат OSPF, які здійснюють прямий влив на швидкість збіжності, відносяться: час, що використовується на встановлення проблем на фізичному рівні (для перевірки доступності каналу роутер обмінюється з сусідніми маршрутизаторами маленькими HELLO-пакетами кожні 10 сек., сусід буде вважатися недосяжним у разі відсутності відповіді на 4 HELLO-пакети відісланих поспіль); час, що витрачається на розсилання пакетів LSA по мережі; час, який потрібний для оновлення даних таблиць маршрутизації.

В середовищі OPNET була здійснена статистична оцінка за такими ознаками, як: тривалість конвергенції (Network Convergence Duration) EIGRP та OSPF протоколів; запис хвиль змін (Network Convergence Activity) на осі ординат між значенням 1 (активний процес конвергенції) та 0 (активність конвергенції відсутня в мережі); обсяг мережевого трафіку.

2.3. Аналіз отриманих даних збіжності OSPF та EIGRP протоколів в середовищі OPNET

В графічному симуляторі OPNET Modeler було змодельовано мережу з розподілом на 5 логічних підрозділів (subnet_1 - subnet_5), кожен з яких включає в себе по 10 моделей роутерів Cisco. Таким чином, в результаті отримали корпоративну мережу, яку формують 50 роутерів та 87 локальних мереж. Кожна підмережа сполучена дуплексним каналом PPP DS3 (44.736 Мб/с).

Загальний вид топології на рівні підмереж зображений на рис. 2.1

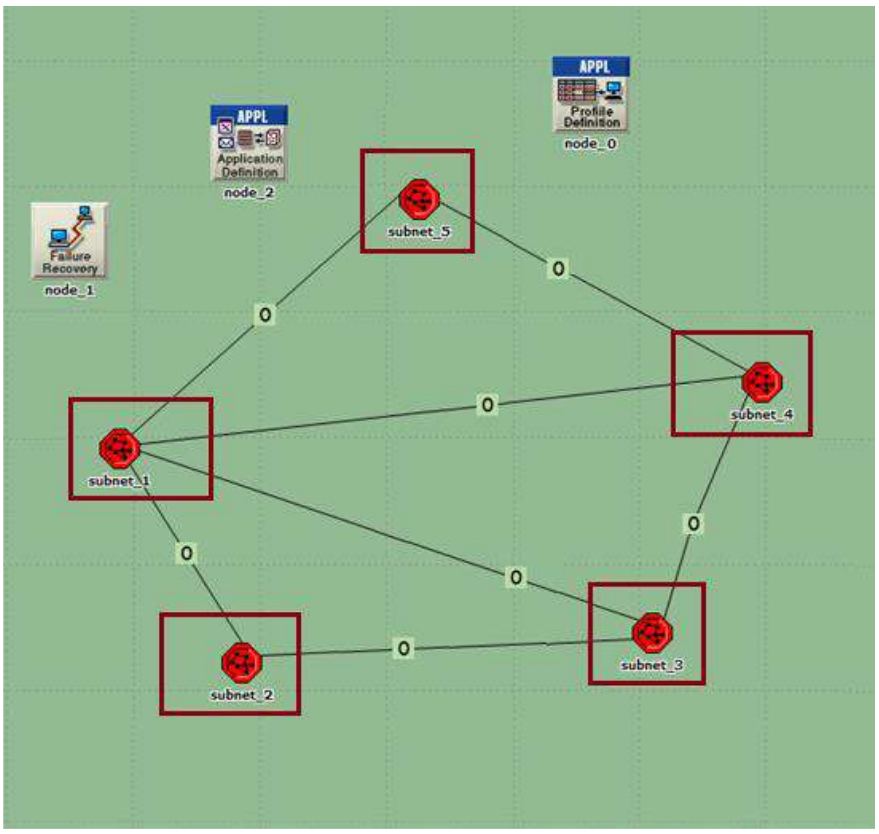


Рис. 2.1 – OPNET проект зі створеними підмережами (subnet_1 - subnet_5)

Топологію кожної з п’яти підмереж було змодельовано по аналогії підмережі subnet_1, зображеної на Рисунку 2.2.

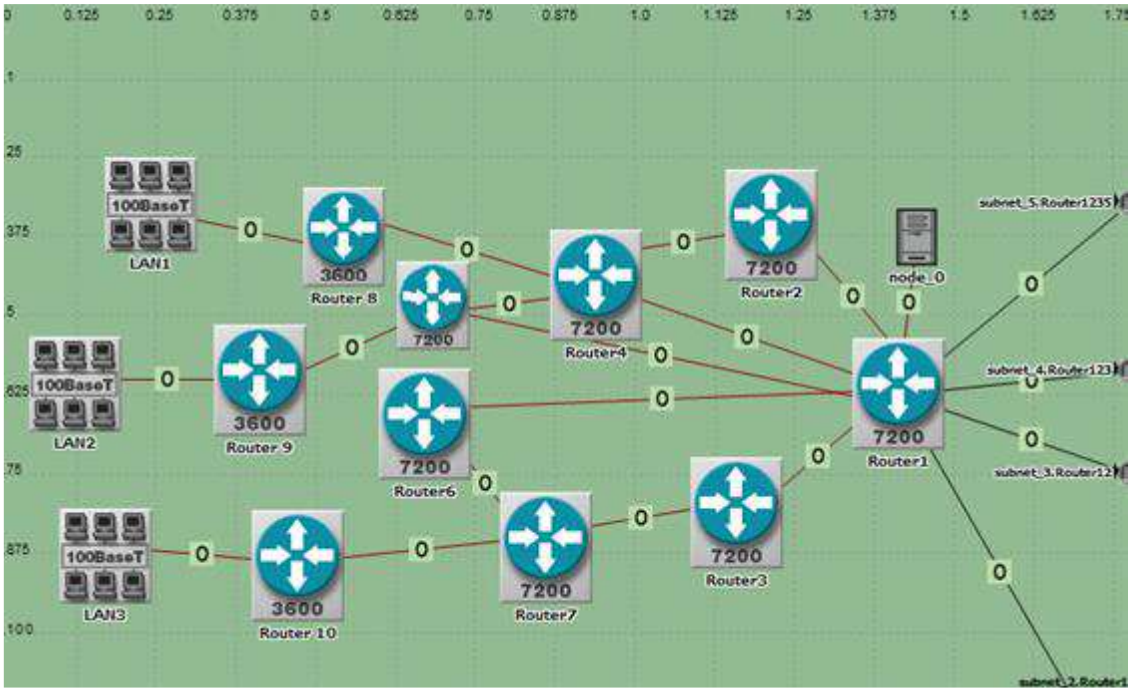


Рис. 2.2 – Топологія subnet_1 з OSPF конфігурацією

На Рисунку 2.3 можемо бачити показники збіжності, які були отримані в ході проведеного спостереження.

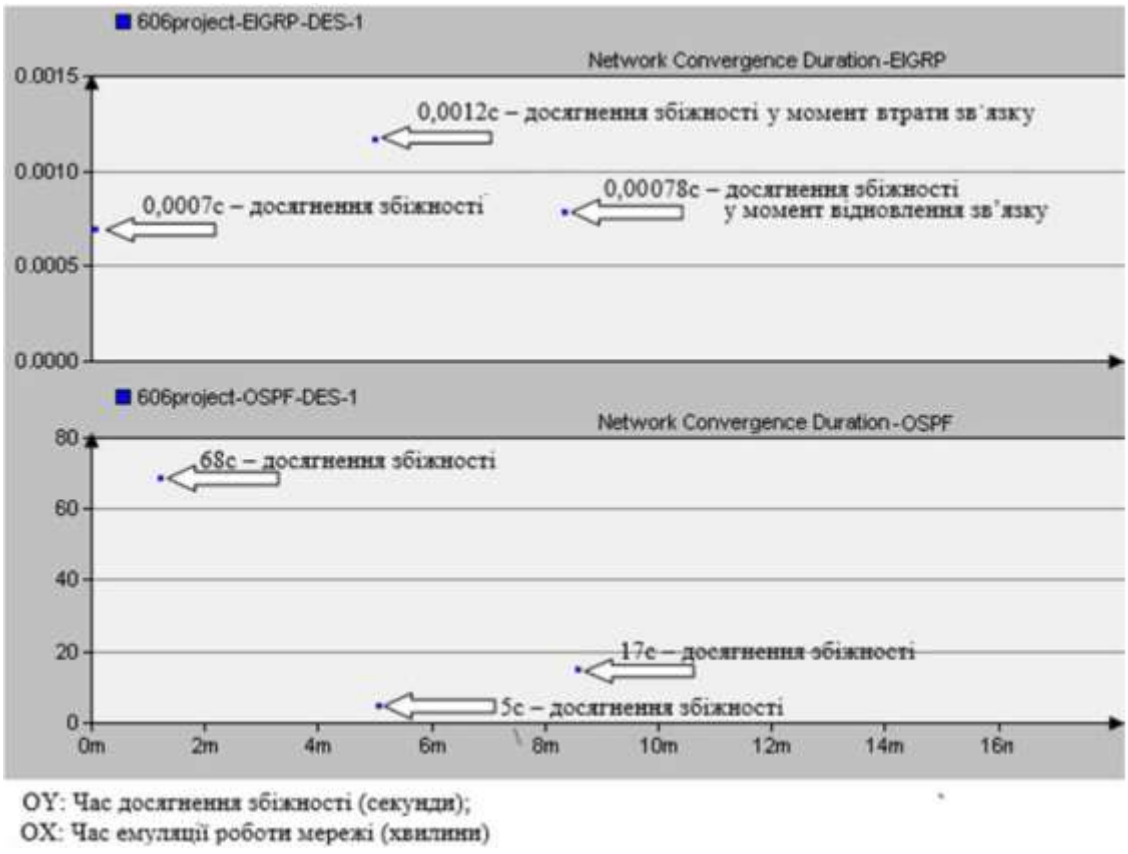


Рис. 2.3 – Довжина конвергенції для EIGRP/OSPF протоколів

Спираючись на отриманні в ході дослідження показники збіжності спостерігаємо, що EIGRP досягає збіжності в момент отримання кожним маршрутизатором найбільш свіжих даних про маршрути: ініціалізація мережі - за 0,0007сек. у випадку виходу з ладу одного з маршрутів – за 0,0012сек., при поновленні зв'язку – за 0,00078сек. В той час коли OSPF протокол досягає збіжності за більш тривалий час, а саме: під час ініціалізації – 68сек., у випадку відмови звязку – 5 сек., при поновленні зв'язку – 17сек. Таким чином бачимо, що у разі виходу з ладу однієї з нод OSPF протокол витрачає більше часу на актуалізацію маршрутних даних саме під час першого запуску, тоді як EIGRP – при відновленні шляхів. Отже, можемо зробити висновок, EIGRP протокол має значно більшу швидкість досягнення конвергенції в порівнянні з OSPF протоколом.

Показники швидкості збіжності EIGRP та OSPF протоколів також продемонстровано на Рисунках 2.4 та 2.5.

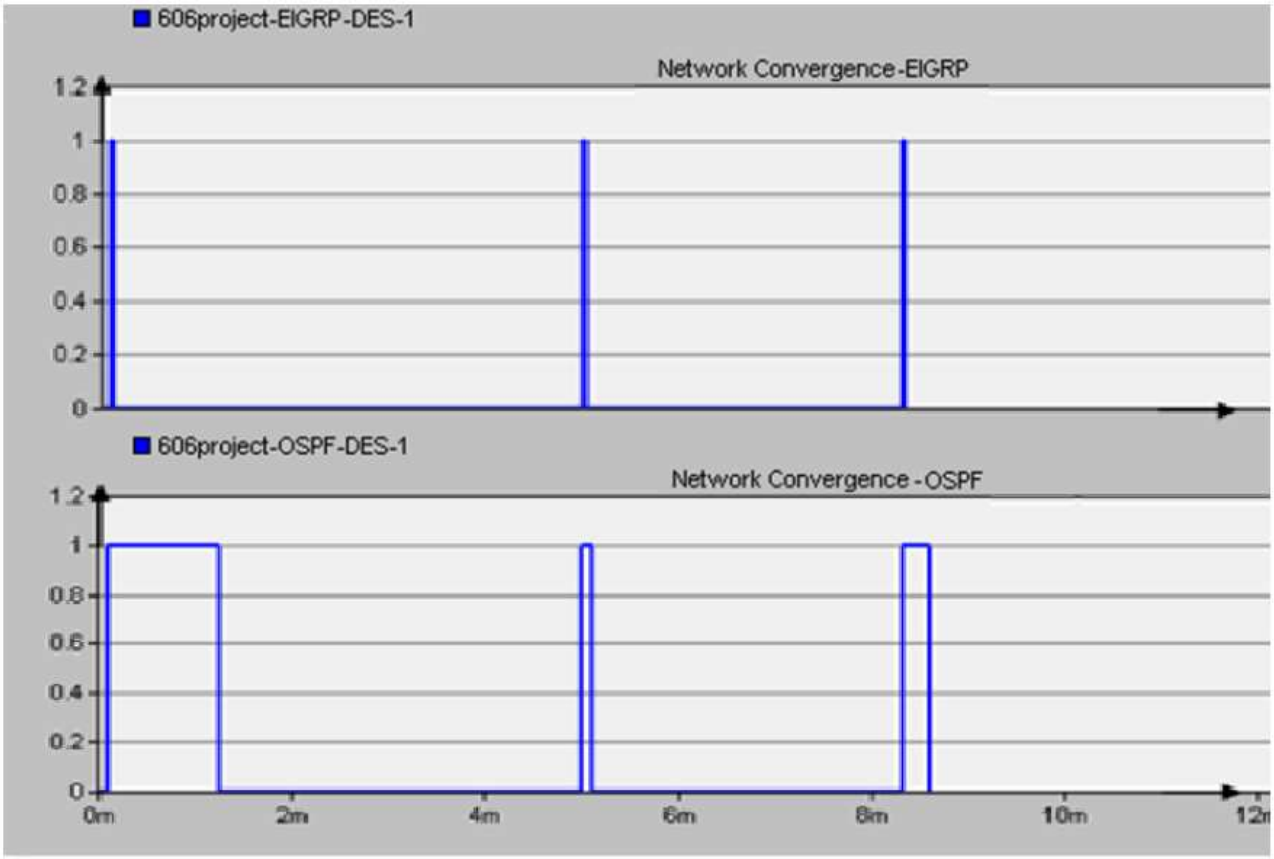


Рис. 2.4 – Активність OSPF/EIGRP в досягненні збіжності

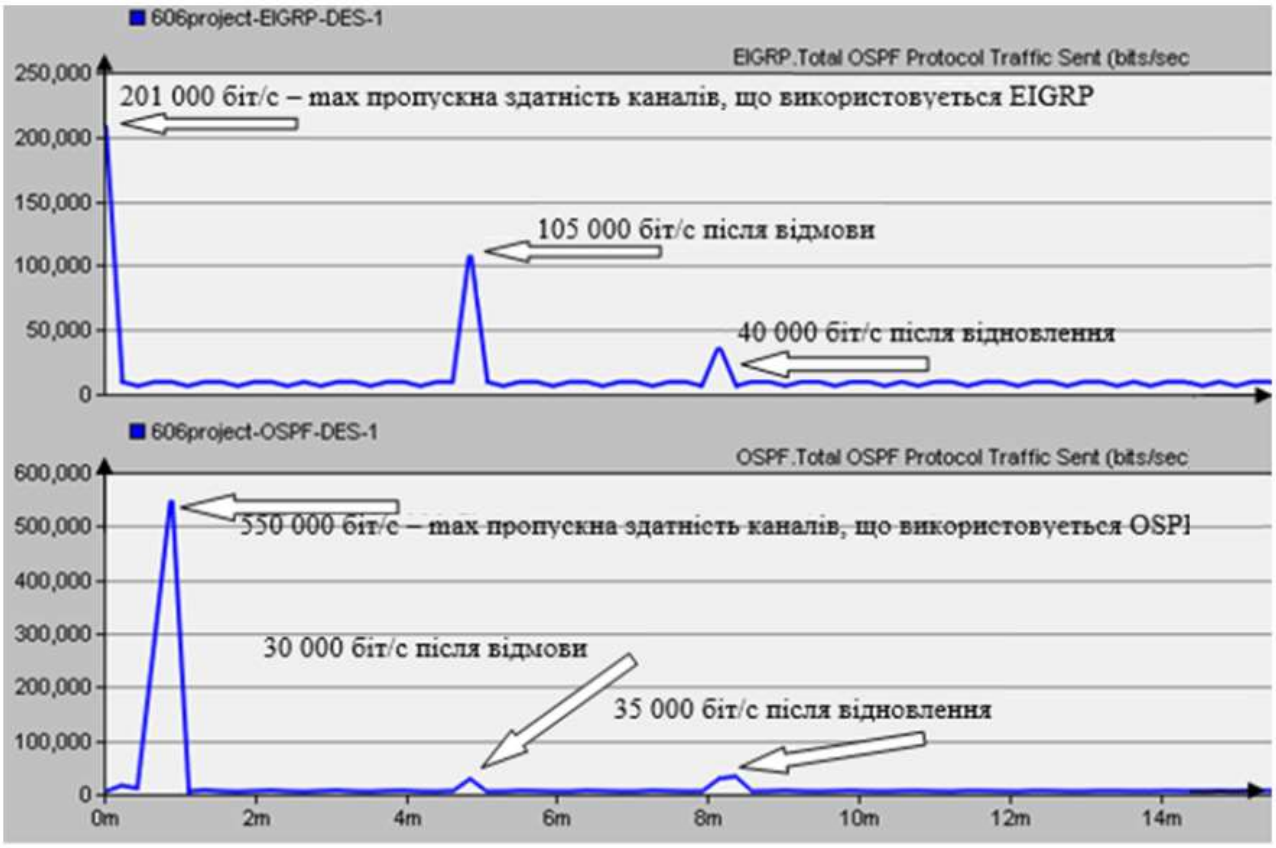


Рис. 2.5 – Надісланий OSPF/EIGRP трафік (біт/сек)

З показників швидкості досягнення конвергенції наведених на Рисунках 2.4 та 2.5 спостерігаємо, що обсяг інформації надісланої OSPF під час ініціалізації мережі більш ніж вдвічі перевищує пікові показники EIGRP, а саме 550000 біт/сек для OSPF, та 201000 біт/сек для EIGRP. В той час, коли при зміні конфігурації мережі OSPF займає значно менше трафіку в порівнянні з EIGRP, 30000 біт/сек та 105 біт/сек відповідно.

Як бачимо робота в графічному середовищі Opnet Modeler виключає необхідність проведення складних попередніх підрахунків з метою виявлення слабких місць в мережі. Для отримання необхідних показників дослідження мережі достатньо лише спроектувати модель та створити відповідні умови для відтворення певного мережевого сценарію. В даному випадку, за допомогою

OPNET додатку було проаналізовано змодельовані мережі з налаштованими EIGRP та OSPF протоколів з точки зору показників конвергенції та обсягу мережевого трафіку.

РОЗДІЛ 3 МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОБОТИ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ ТА ЇХ РЕАЛІЗАЦІЯ

3.1. Моделювання топології мережі

Спираючись на отримані в межах попереднього розділу дані, можна стверджувати, EIGRP має перевагу за якісними показниками в порівнянні з OSPF протоколом. В той же час, слід пам'ятати про певні недоліки протоколу EIGRP, які значною мірою звужують коло можливостей його застосування в мультивендорних комп’ютерних мережах, а саме його пропрієтарність та можливість здійснення налаштувань виключно на Cisco устаткуванні. Тому, на підставі вищевикладеного, в даному розділі розглянемо саме протокол OSPF, який представляє собою відкритий стандарт та підтримується переважною більшість виробників маршртизаторів.

OSPF протокол підтримує наступні методи контролю мережевих ресурсів з точки зору доцільності використання[15]:

1. Введення мультизонової мережі;

2. Виділення призначеного маршрутизатору (DR, designated router) та резервного призначеного маршрутизатору (BDR, backup designated router);

3. Підсумовування підмереж на рівні прикордонного маршрутизатору (ABR, Area border router).

Більш детально вищезазначені функції розглядаються за рахунок побудови моделі мережі у графічному симуляторі мережі GNS3.

Топологія побудованої моделі комп’ютерної мережі зображено на рисунку 3.1

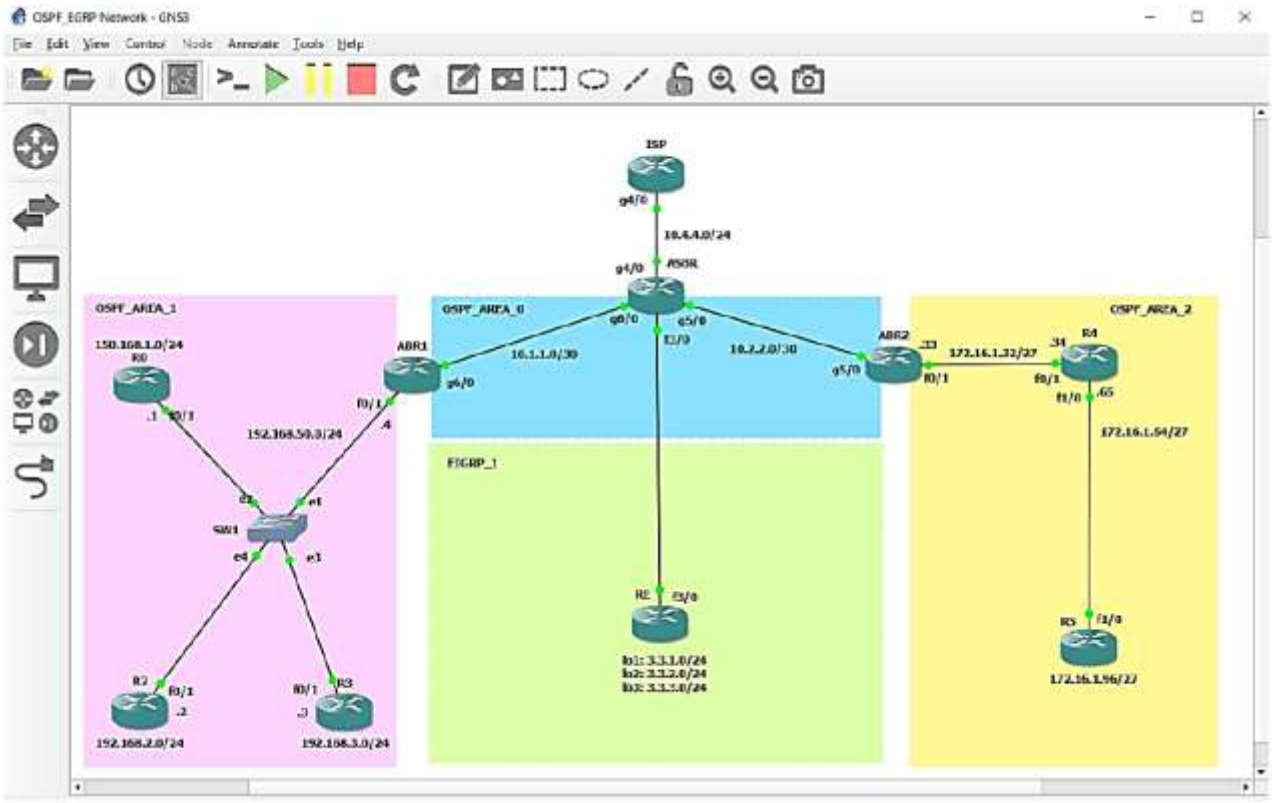


Рис. 3.1 – Топологія корпоративної мережі побудованої на OSPF та EIGRP технологіях

В якості маршрутизаторів було використано роутери Cisco 7200 моделі, та Fast Ethernet та Gigabit Ethernet інтерфейси.

ISP роутер відіграє роль обладнання провайдера інтернет сервісу, який перебуває поза грани АС.

На прикордонному маршрутизаторі автономної системи (ASBR, AS boundary router), який знаходиться на межі між АС та зовнішньою мережею, будо задіяно 3 інтерфейси, а саме Gigabit Ethernet - g6/0, g5/0, які відносяться до OSPF_Area_0 області, та Fast Ethernet - f3/0, який має EIGRP конфігурацію.

ABR1 та ABR2 роутери відіграють функції прикордонних маршрутизаторів областей. Інтерфейси g6/0 (ABR1) та g5/0 (ABR2) належать до основної області – OSPF_Area_0.

EIGRP домен включає ASBR<->RE сполучення та налаштовані loopback інтерфейси на RE роутері.

OSPF_Area_0 – область першого рівеня , яка сполучає OSPF_Area_1 та OSPF_Area_2, області другого рівня, і таким чином забезпечує дворівневість ієрархічній мережі.

До складу зони OSPF_Area_1 входять: роутери R0, R2, R3, ABR1, та Ethernet комутатор SW1.

Зона OSPF_Area_1 включає в себе: роутери ABR2, R2, R5.

З метою подальшого забезпечення підсумування мережевих маршрутів на інтерфейсах кожного з прикордоних маршрутизаторі областей мережі потрібно зпланувати IP-адресацію. IP-план корпоративної мережі має відповідати певним критеріям, а саме бути чіткості та легко розширюваності (Таблиця 3.1). IP-адреси мереж мають обиратися з сусідніх діапазонів.

Таблиця 3.1 IP-план корпоративної комп’ютерної мережі.

Призначення	Адреса та маска мережі	Назва хосту	Інтерфейси (номер останнього октету)
Зовнішня мережа	10.4.4.0/24	ISP	g4/0 (.1)
		ASBR	g4/0 (.2)
OSPF_Area_0	10.2.2.0/30	ASBR	g5/0 (.2)
		ABR2	g5/0 (.1)
	10.1.1.0/30	ASBR	g6/0 (.2)
		ABR1	g6/0 (.1)
EIGRP_1	10.3.3.0/30	ASBR	f3/0 (.2)
		RE	f3/0 (.1)
	3.3.1.0/24	RE	lo1 (.1)
	3.3.2.0/24	RE	lo2 (.1)
	3.3.3.0/24	RE	lo3 (.1)
OSPF_Area_1	192.168.50.0/24	ABR1	f0/1 (.4)
		R0	f0/1 (.1)

Продовження таблиці 3.1

Призначення	Адреса та маска мережі	Назва хосту	Інтерфейси (номер останнього октету)
		R2	f0/1 (.2)
		R3	f0/1 (.3)
	192.168.3.0/24	R3	lo1 (.1)
	192.168.2.0/24	R2	lo1 (.1)
	192.168.1.0/24	R0	lo1 (.1)
OSPF_Area_2	172.16.1.32/27	ABR2	f0/1 (.33)
		R4	f0/1 (.34)
	172.16.1.64/27	R4	f1/0 (.65)
		R5	f0/1 (.66)
	172.16.1.96/27	R5	lo1 (.97)

3.2. Налаштування агрегування маршрутів

Процес побудови моделі мережі розпочинається присвоєння інтерфейсам роутерів IP-адрес та конфігурації протоколів динамічної маршрутизації.

Першою стадією моделювання є налаштування адресації обладнання згідно спроектованого плану адресації. Конфігурація OSPF протоколу здійснено за допомогою слідуючих команд:

- #router ospf 1 – запуск OSPF процесу на роутері (останнє число – це індентифікатор процесу);

- #network <ip address> <inverted subnet mask> area <n> – дана команда повідомляє роутер про те з яких інтерфейсів будуть анонсуватися підмережі по OSPF. <ip address> - номер мережі, <inverted subnet mask> - зворотна маска та <n> - номер зони мережі.

- #default-information originate – задання даної команди потрібне для анонсування маршруту за замовчуванням. Дана команда була задана на прикордонних маршрутизаторах першої та другої зон.

Для конфігурації EIGRP протоколу на маршрутизаторах було застосовано такі команди:

- #router eigrp 1 – запуск EIGRP процесу на роутері (останнє число – це індентифікатор процесу);

- #network <ip_address> <subnet_mask> – дана команда застосовується для анонсування мережі

- #no auto-summary – команда використовується з метою відключення автоматичного підсумовування мереж.

Шляхом запуску команди ‘area <N> range <summarized_network_ip_address> <wildcard_subnet_mask>’ (де N – номер зони, summarized_network_ip_address – узагальнена адреса підмереж, wildcard_subnet_mask – зворотна маска підмережі) відбувається конфігурація підсумовування маршрутів на прикордонних роутерах зони ABR1 та зони ABR2, що представяє собою другу стадію моделювання мережі.

Зупинимося детальніше на особливостях розрахунку сумарної адреси та маски підмережі на прикладах адрес, представлених в бінарній формі, наведених нижче:

· 192.168.50.0/24 - 11000000.10101000.00110010.00000000

· 192.168.1.0/24 - 11000000.10101000.00000001.00000000

· 192.168.2.0/24 - 11000000.10101000.00000010.00000000

· 192.168.3.0/24 - 11000000.10101000.00000011.00000000

Як бачимо, з наведеного вище прикладу, початок відмінностей між адресами мереж починається з 3го біту 3го октету. Далі з метою розрахунку сумарного маршруту всі однакові біти 3го октету замінимо одиницями, а ті біти, які відрізняються – нулями, в результаті маємо бінарне значення-11000000.10101000.11000000.00000000, або десяткове - 255.255.192.0.

Щоб виділити адресу сумарного маршруту після 2го біту 3го октету замінимо всі біти на нульові значення, отримаємо - 11000000.10101000.00000000.00000000, що в десятковій формі має вигляд -

192.168.0.0. Звідси отримали значення 192.168.0.0 255.255.192.0 (192.168.0.0/18) – сумарний маршрут.

З рис. 3.2 бачимо, за результатом запуску команди # show ip route в на ASBR роутері в таблиці маршрутизації виведено лише один рядок сумарного маршруту, замість чотирьох тих, які не входять до зони 1.

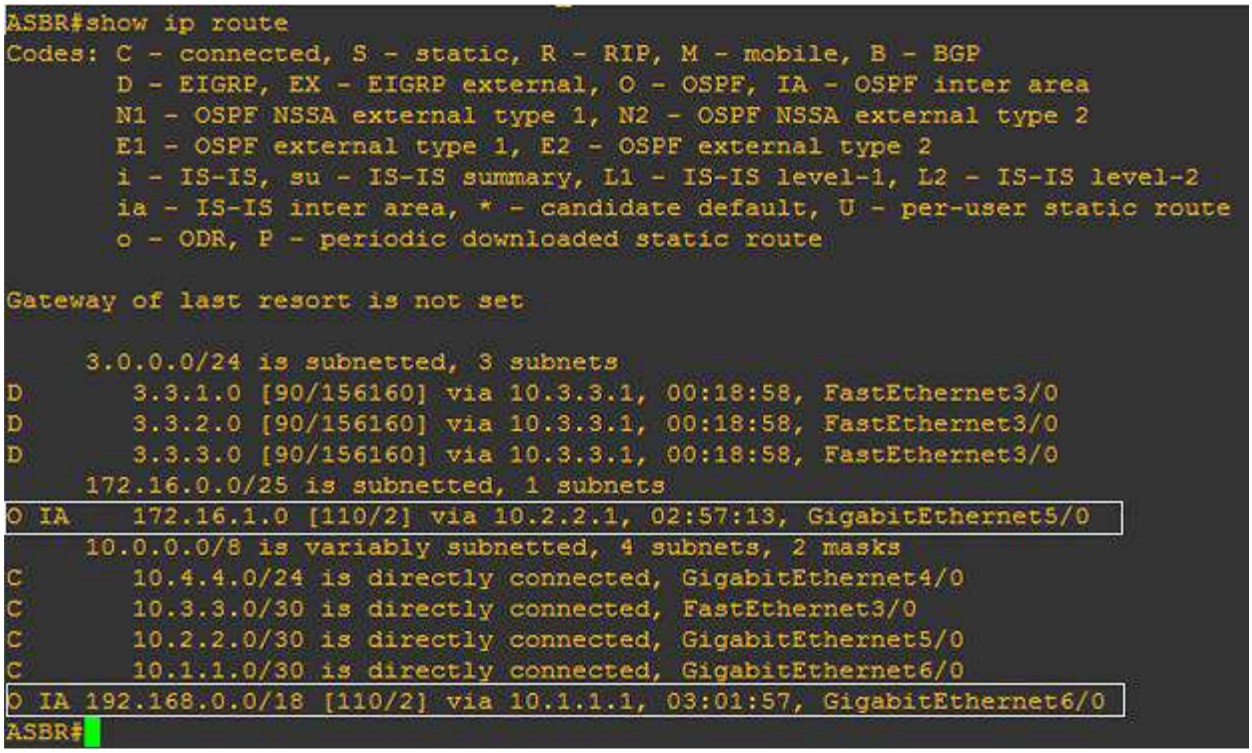


Рис. 3.2 – Сумарні маршрути в таблиці маршрутизації ASBR роутеру

Оптимізація таблиці маршрутизації за рахунок скорочення її записів сприяє зменшенню кількості даних, які надсилаються LSA поза зоною. Даний підхід слід застосовувати у мережах, які складаються з чималої кількості обладнання та зон, оскільки такі мережі підтримують зменшення ступеню деталізації топологічних відомостей зон 2го рівня на маршрутизаторах з метою зменшення розміру LSA пакетів.

3.3. Функції DR та BDR роутерів у мережі з множинним методом доступу

В межах третьої стадії побудови моделі мережі відбувається конфігурація DR та BDR маршрутизаторів. У випадку мереж з множинним доступом важливо відстежувати та тримати під контролем, який саме маршрутизатор буде обробляти LSA, коли область зазнає оновлень.

Прикладом схожої мережі на побудованій моделі виступає OSPF Area 1 зона. З рисунок 3.1 бачимо, що в межах першої зони чотири маршрутизатори сполучені мережею - 192.168.50.0/24.

У випадку надмірної завантаженості лінії LSU/LSA пакетами, яка може виникати унаслідок змін топології мережі, головною задачею для DR є збереження ресурсів інших маршрутизаторів певної зони шляхом забезпечення точки розрахунку найоптимальніших шляхів у разі оновлень топології.

OSPF обирає призначений маршрутизатор (DR) та резервний призначений маршрутизатор (BDR) у кожному сегменті. Вибори DR та BDR проводяться Hello протоколом, в залежності від певних чинників, а саме від пріоритету, який було задано на інтерфейсі, ідентифікатору роутеру (Router ID), та найбільшої IP-адреси призначеної на інтерфейсах. Слід зазаначити, що порівняно до вищевказаних значень, при виборі DR перевага надається саме параметру пріоритету з найбільшим значенням у сегменті. За замовчуванням пріоритет на інтерфейсах дорівнює – 1. У випадку, якщо роутери мають однакові значення пріоритету, DR та BDR обираються за Router ID параметром. Маршрутизатор, який має найвище Router ID значення, призначається DR, а маршрутизатор з другим найвищим значенням – BDR.

Присвоєння пріоритету на інтерфейсі здійснюється командою: #ip ospf priority <priority-value>, де priority-value – значення від 1 до 255, яке визначає пріоритетність маршрутизатору. Чим вище значення пріоритету, тим більше шансів у роутера бути обраним DR роутером.

Суміжні DR/BDR роутери для R3 маршрутизатору OSPF Area 1 області виведені на рис. 3.3 шляхом виконання команди #show ip ospf neighor.

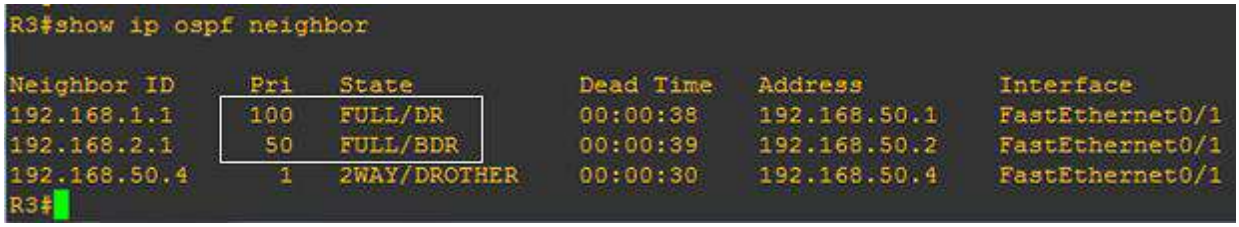


Рис. 3.3 – OSPF сусідство R3 роутеру

3.3. Динамічний перерозподіл маршрутної інформаціїї між OSPF та EIGRP

Під час розширення мережі за рахунок приєднання до неї об’єднаних підмереж, можливе виникнення потреби у встановленні зв’язку між сегментами, які налаштовані на різних технологіях динамічної маршрутизації.

Звертаючись до змодельованої мережі бачимо, крім налаштувань OSPF протоколу на g5/0 та g6/0 інтерфейсах, ASBR маршрутизатор також сполучений 10.3.3.0/30 мережею, яка підтримує EIGRP технологію. В даному випадку обмін інформацією між таблицями маршрутизації можна забезпечити за рахунок двонаправленого перерозподілу маршрутів, де - ASBR маршрутизатор буде відігравати роль ключового.

Передача маршрутної інформації з протоколу маршрутизації OSPF в протокол EIGRP здійснюється за рахунок команд: router ospf 1 та redistribute eigrp 1 subnets. Слід зауважити, зазначення subnets опції у випадку безкласової IP адресації є неухильною умовою.

Кінцевий підсумок налаштувань перерозподілу маршрутної інформації наведено на рисунку 3.4. Як бачимо, в OSPF домен було динамічно передано дані про маршрути, які, напередодні, були відомі виключно для EIGRP мережі.

```
Gateway of last resort is not set

     3.0.0.0/24 is subnetted, 3 subnets
O E2    3.3.1.0 [110/20] via 10.1.1.2, 00:00:08, GigabitEthernet6/0
O E2    3.3.2.0 [110/20] via 10.1.1.2, 00:00:08, GigabitEthernet6/0
O E2    3.3.3.0 [110/20] via 10.1.1.2, 00:00:08, GigabitEthernet6/0
     172.16.0.0/25 is subnetted, 1 subnets
O IA    172.16.1.0 [110/3] via 10.1.1.2, 00:00:08, GigabitEthernet6/0
     10.0.0.0/30 is subnetted, 3 subnets
O E2    10.3.3.0 [110/20] via 10.1.1.2, 00:00:08, GigabitEthernet6/0
O       10.2.2.0 [110/2] via 10.1.1.2, 00:00:08, GigabitEthernet6/0
C       10.1.1.0 is directly connected, GigabitEthernet6/0
C    192.168.50.0/24 is directly connected, FastEthernet0/1
     192.168.1.0/32 is subnetted, 1 subnets
O       192.168.1.1 [110/2] via 192.168.50.1, 00:14:22, FastEthernet0/1
     192.168.2.0/32 is subnetted, 1 subnets
O       192.168.2.1 [110/2] via 192.168.50.2, 00:15:02, FastEthernet0/1
     192.168.3.0/32 is subnetted, 1 subnets
O       192.168.3.1 [110/2] via 192.168.50.3, 00:15:02, FastEthernet0/1
O    192.168.0.0/18 is a summary, 00:15:03, Null0
```

Рис. 3.4 – Таблиця маршрутизації роутера ABR1

Тим не менш, за результатом перевірки стану з'єднання між інтерфейсами 192.168.50.4 (ABR1) та 3.3.1.1 (RE) шляхом виконання команди ping спостерігаємо, що з'єднання відсутнє (рис. 3.4.2). Це пояснюється тим фактом, що у роутера RE відсутні дані щодо мережі з якої було виконано дану команду перевірки мережевого зв'язку. Отже, робимо висновок, що на даному етапі односторонній перерозподіл маршрутної інформації не можна вважати достатнім.

```
ABR1#ping 3.3.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Рис. 3.5 – Команда ping RE lol

Таким чином, за аналогією, маємо виконати конфігурацію перерозподілу маршрутної інформації з протоколу EIGRP в протокол маршрутизації OSPF. Для цього виконуємо команди: router eigrp 1 та redistribute ospf 1 metric 1111. З наведеної на рисунку 3.6 таблиці маршрутизації роутеру RE виведено дані про

маршрути, які було проаналізовано OSPF мережею та передано до RE роутеру.

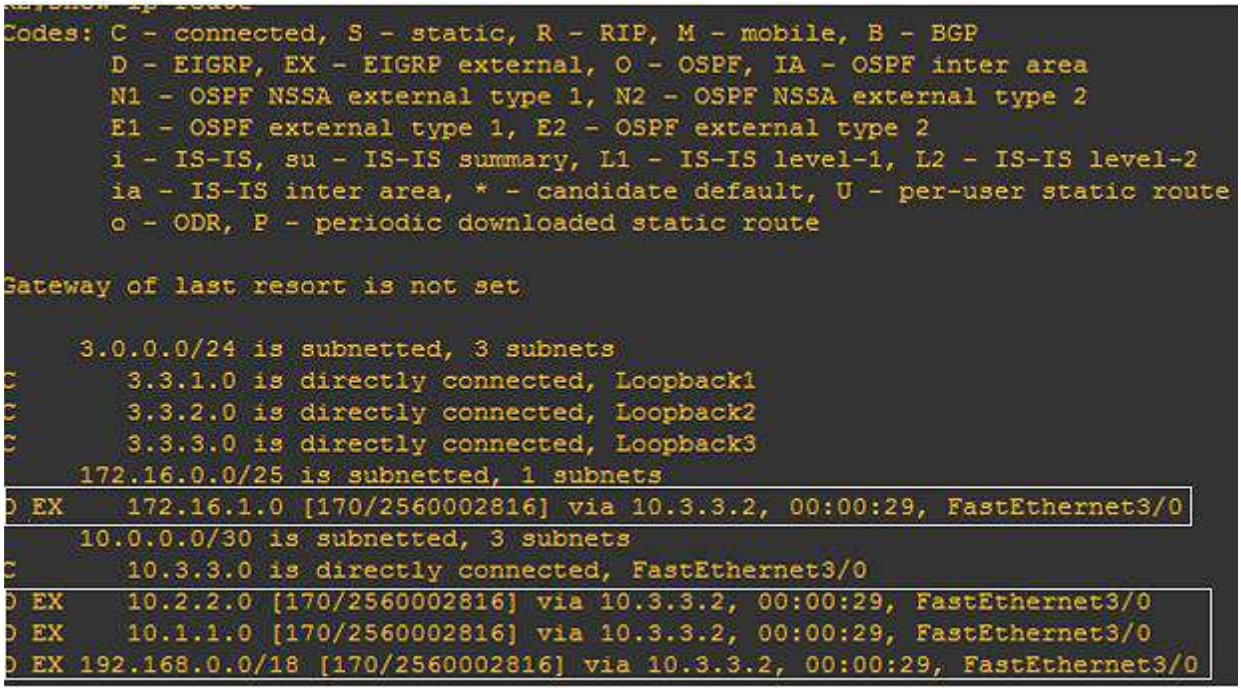


Рис. 3.6 – Маршрути, передані на RE роутер

Під час перерозподілу маршрутної інформації, у випадку виникнення необхідності під’єднання нової мережі до маршрутизатору ASBR, вирішальне значенння відіграє ризик втрати інформації щодо прямо під’єднаних до нього маршрутів. В якості прикладу, в якості нової точки з'єднання OSPF домену застосуємо новий інтерфейс ASBR роутеру та земулюємо схожий випадок зі втратою даних.

Далі застосовуємо route-map для здійснення перерозподілу нової маршрутної інформації та виведемо таблицю маршрутизації роутеру ABR1 з отриманими результатами (Рис. 3.7).

int loopback 22

ip address 10.5.5.1 255.255.255.252

Route-map CONN>OSPF

match interface loopback 22

router ospf 1

redistribute connected route-map CONN>OSPF subnets

З наведеної таблиці маршрутизації роутеру ABR1 демонструємо втрату напередодні отриманої інформації про 10.3.3.0/30 мережу.

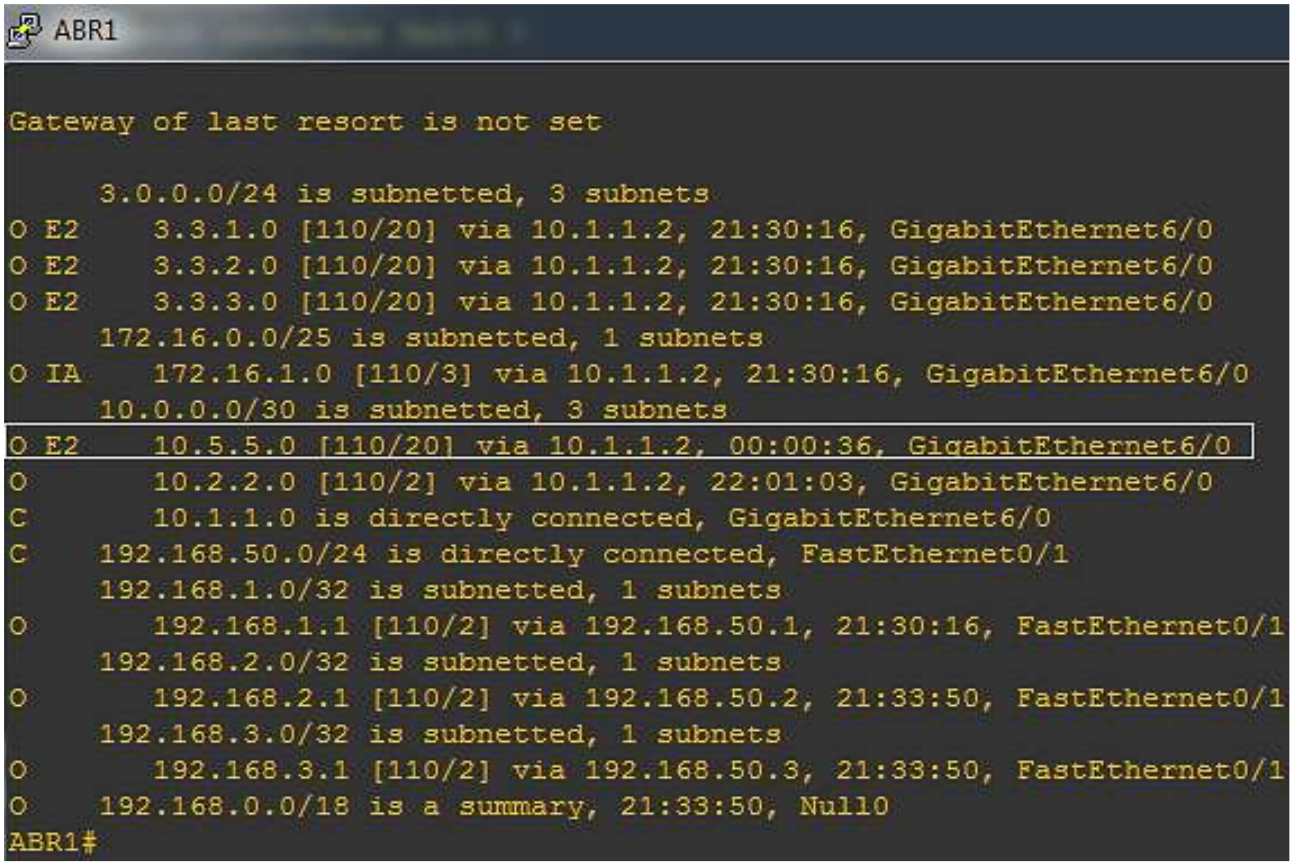


Рис. 3.7 – Перерозподіл маршрутної інформації нової мережі на ABR1 роутері

З метою вирішення такого роду проблеми опрацювання даних про прямо підключені мережі, що входять до інших доменів, застосовуємо route-map на fa0/3 інтерфейсі роутеру ASBR:

route-map CONN>OSPF

match interface fa3/0

Після повторного виведення таблиці маршрутизації (рис. 3.8) пересвідчуємося в коректності перерозподілу маршрутних даних 10.3.3.0/30 мережі.

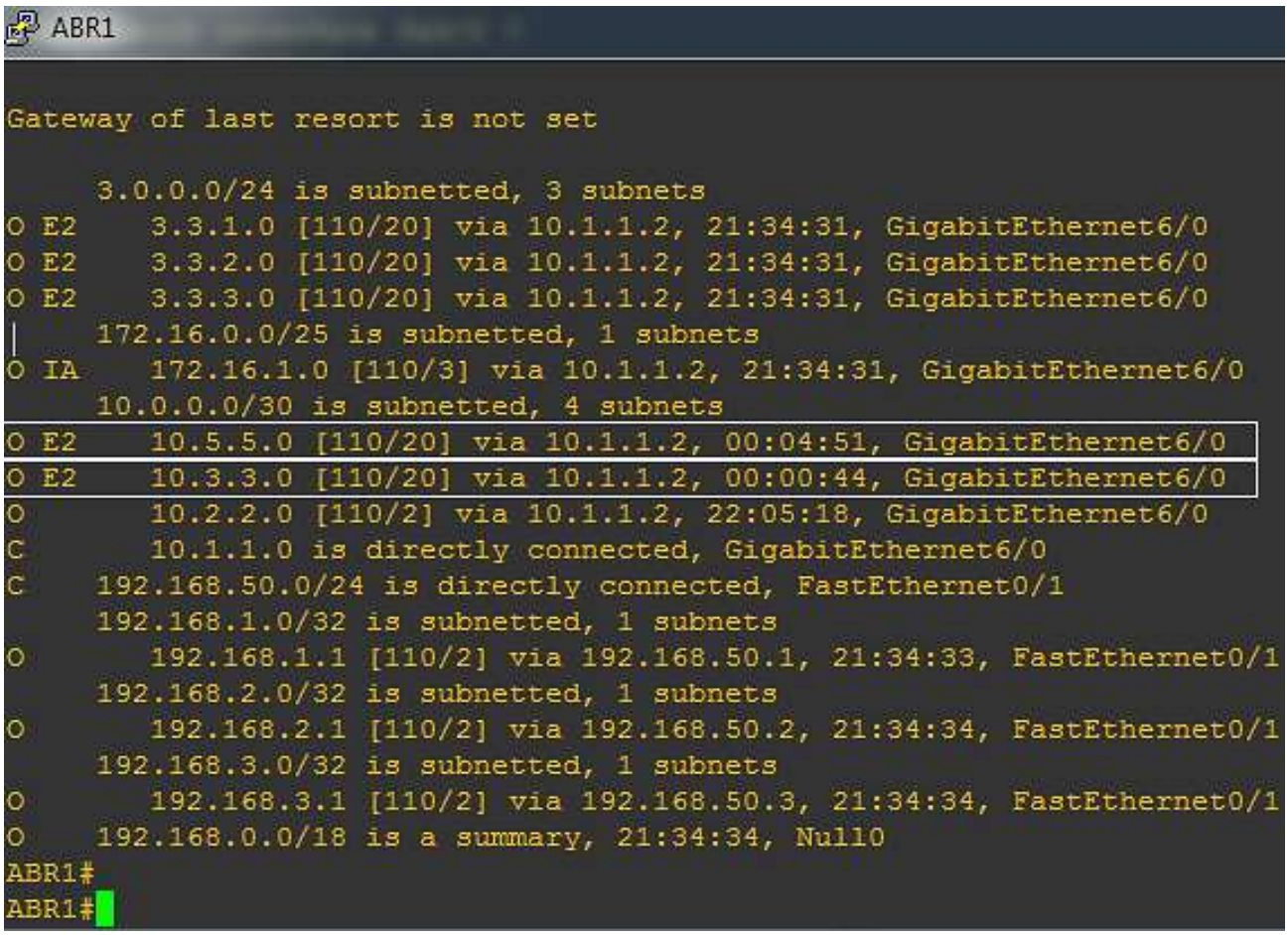


Рис. 3.4.5 – Повторний вивід таблиці маршрутизації ABR1 з результатами перерозподілу

Деталі конфігурації роутерів ASBR, ABR1, R0 та RE викладено в Додатку А.

РОЗДІЛ 4 АНАЛІЗ OSPF ПРОТОКОЛУ НА ОСНОВІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

4.1. Огляд алгоритму роботи програмного забезпечення

Виявлення пошкоджень та несправностей після проектування та побудови топології мережі є однією з основних завдань мережевого адміністратора. Розробка процесу, який спроможний працювати автоматично, значно скорочує робочий час, необхідний інженеру для діагностування мережі, та гарантує оперативне усунення виявлених пошкоджень та недоліків.

Саме тому в межах даного дослідження було розроблено додаток, головним призначенням якого є встановлення випадків, коли лінія зв'язку або мережеве устаткування є недоступними, та який надає можливість вивчення мережевої топології OSPF шляхом виконання запитів SNMP (Simple Network Management Protocol) до обладнання мережі.

Додаток виконує такі функції:

- Віддалене спостереження за станом роботи мережі та обробка мережевих даних в умовах реального часу віддалено (без повного перерахунку IP-адрес одиниць обладнання);

- Попередження та обмеження наслідків, як результату некоректного налаштування OSPF протоколу, виведення з ладу мережевого пристрою або певного його інтерфейсу.

Розроблене програмне забезпечення може бути використаним під час вивчення та дослідження протоколів динамічної маршрутизаціях, а також мережевими інженерами в справжніх системах.

Для створення додатку було використано мову програмування Python (2.7.0 Release), застосовуючи як стандартні програмні модулі, так і спеціалізовані.

SNMP (Simple Network Management - простий протокол керування мережею), технологія інтернет-стандарту для збору даних про керовані пристрої в IP- мережах на основі TCP/UDP структури мережі, формує

кореневий функціонал додатку. Даний тип протоколу надає можливість мережевому адміністратору моніторити, контролювати продуктивність мережі та змінювати налаштування підключених до мережі пристроїв.

SNMP технологія – простий та ефективний спосіб для збору інформації між мультивендорним обладнанням, яке працює на різному програмному забезпеченні. SNMP архітектуру складають наступні рівні:

- Система мережевого управління (Network Management System, NMS) - віддалено слідкує, отримує дані про стан мережі, налаштування, її продуктивність та ін;

- Мастер-агенти – представляють собою програмне забезпечення яке повязує менеджера мережі з агентами. Мастер-агент проводить аналіз запитів від NMS менеджеру та надсилає їх агентам. Сформувавши зібрані відповіді від агентів відсилає їх мережеву, та, нотифікує того у разі відсутності необхідних даних з запиту, або якщо запит є некоректним.

- Агенти – програмне забезпечення, яке забезпечує направлення зібраних даних мастер-агенту.

- Керовані компоненти – це програмне забезпечення з вбудованим агентом (антивірусне ПЗ, системи резервного копіювання, ДБЖ), або підключене до мережі обладнання (маршрутизатори, комутатори, сервери, IP відеокамери, IP телефонія та МФУ).

Обмін даними між менеджером та агентом здійснюється за рахунок User Datagram Protocol (UDP) протоколу, на заміну якому також можуть використовуватися TCP, IPX або ж протокол MAC рівня. Безпосередньо сам процес обміну інформацією базується на Protocol Data Unit (PDU)

Загалом в технології SNMP нараховується сім PDU:

- GET — запит NMS на отримання інформації від вузлу мережі.

- GETNEXT – запит працює по аналогії з GET, відмінність лише тому, що NMS менеджер робить запит на дані елементу наступного після вузлу за ієрархією.

- SET — за рахунок даної команди менеджер або надає пристрою нові дані.

- RESPONSE - відповідь від агента на запит даних.

- TRAP — агент оперативно надсилає дане повідомлення про подію або помилку, не чекаючи на отримання запиту від менеджера.

- GETBULK – покращена версія запиту GETNEXT, даний запит надсилається агенту на вилучення масиву даних з пристрою.

- INFORM – запит аналогічний до TRAP, але в даному випадку агент продовжуватиме відправляти запити до тих пір, доки не отримає підтвердження від менеджера про його отримання.

Познайомимося з основними імпортованими пакетами для роботи даного програмного забезпечення [14]:

- Модуль pysnmp та CommandGenerator([snmpEngine]) клас забезпечують застосування функціоналу SNMP технології.

- Для перевірки доступності введеної IP адреси інтерфейсу використовуємо модуль subprocess та функцію call().

- З метою полегшення сприйняття інформації користувачем модуль binascii перетворює значення, які були отримані SNMP командою за ідентифікатором об’єкта (OID), у десяткову величину.

- Надання доступу до певних змінних та функцій, які взаємодіють Python інтерпретатором, здійснюється за рахунок використання sys модулю.

- Matplotlib – бібліотека для мови програмування, яка дозволяє створювати рисунки високої якості та різноманітних форматів. Matplotlib представляє собою модуль-пакет для python. У даній роботі використовувався високорівневий інтерфейс matplotlib.pyplot.

- Імпортований модуль networkx – пакет для створення, маніпуляції та вивчення структури, динаміки та функцій складної комп’ютерної мережі. Одне з призначень пакету – генерація графу мережі. Для розуміння логіки роботи розробленого програмного забезпечення розглянемо послідовність етапів роботи програми продемонстрованої на рисунку 4.1.



Рис. 4.1 – Послідовність етапів роботи додатку вивчення OSPF топології

Опис функцій та змінних, що забезпечують основний функціонал наведені у таблиці 4.2 та 4.3 відповідно.

Таблиця 4.2 Головні функції додатку дослідження топології OSPF мережі

Функція	Характеристика функції
split('delimiter')	Вбудована функція Python, завданням якої є розділення ряду символів вказаним роздільником.
ip_is_valid()	Дана користувацька функція була створена для валідації заданої IP-адреси

snmp_get(ip)	Дана функція є користувацькою, яка використовує змінні для отримання інформації напряму від пристрою за рахунок SNMP запиту.
call(args,, stdin=None, stdout=None, stderr=None, shell=False, timeout=None)*	Дана функція входить до складу вбудованого subprocess модулю. Вона виконує команду зазначену в аргументі, після закінчення виконання якої видає код повернення. В межах даного додатку вона застосовується для надсилання ping команди на введену IP-адресу.
cmdgen.CommandGenerator()	Ініціює виклик конструктуру класу генерації команд. Функцію влючено до pysnmp модулю.
add_edges_from()	Дана ф-я Graph класу (networkx пакет) здійснює ініціалізацію ліній (ребер) графу.
cmdGen.nextCmd()	Функція надсилає SNMP GETNEXT запити для визначених OSPF OID, далі повертає впорядковану сукупність значень: - errorIndication - errorStatus - errorIndex - varBindTable
	В якості змінних застосовувалися значення snmp community, UDP інтерфейсу та OID інформації з таблиці сусідніх пристроїв (pysnmp модуль)
find_unqueried_neighbors()	Дана користувацька ф-я використовуэться з метою встановлення маршрутизаторів з існуючого переліку сусідів, від яких ще не було надіслано інформації за шляхом snmp getnext запиту.
nx.Graph()	Функція здійснює іціалізацію об’єкту класу Graph (відбувається у networkx)

hexlify(string)	Дану функція використовує дані отримані через snmp запит. Вона передбачена для перетворення бінарного рядку до шістнадцяткового запису для того, щоб надалі перекласти у десятковий (binascii модуль).
spring_layout ()	Функція позиціонує вузли мережі (networkx)
nx.draw()	Використовується з метою відтворення рисунку мережевого графу (networkx)

До основних змінних програмного забезпечення належать наступні:

- ✓ comm – змінна SNMP community, яку сконфігурова на маршрутизаторах, які входять до АС.
- ✓ ip – значення IP-адреси, яка вводиться на початку роботи додатку у формі символьного рядку.
- ✓ nbriplist - перелік IP-address сусідніх пристроїв;
- ✓ nbridlist – перелік router id сусідніх пристроїв;
- ✓ ping_reply – змінна (цілочисельна), яка розпізнає відповіді на команду ping;
- ✓ ospf – перелік словників з інформацією про сусідні пристрої;
- ✓ ospf_devices – словник, який містить Host, HostID, NbrRtrId, NbrRtrIp параметри;
- ✓ ospf_host_id - router ID хосту;
- ✓ ospf_host – імя хосту;
- ✓ all_nbr_ids - перелік всіх значень ідентифікаторів сусідніх пристроїв;
- ✓ all_host_ids – перелік всіх значень ідентифікаторів хостів;

✓ all_outsiders - перелік сусідів, які не визначені в якості хосту в списку хостів.

4.2. Тестування розробленого програмного забезпечення на моделі мережі

В межах тесту додатку було змодельовано мережу у графічний симуляторі мереж GNS3, топологію якої продемонстрована на рис.4.2

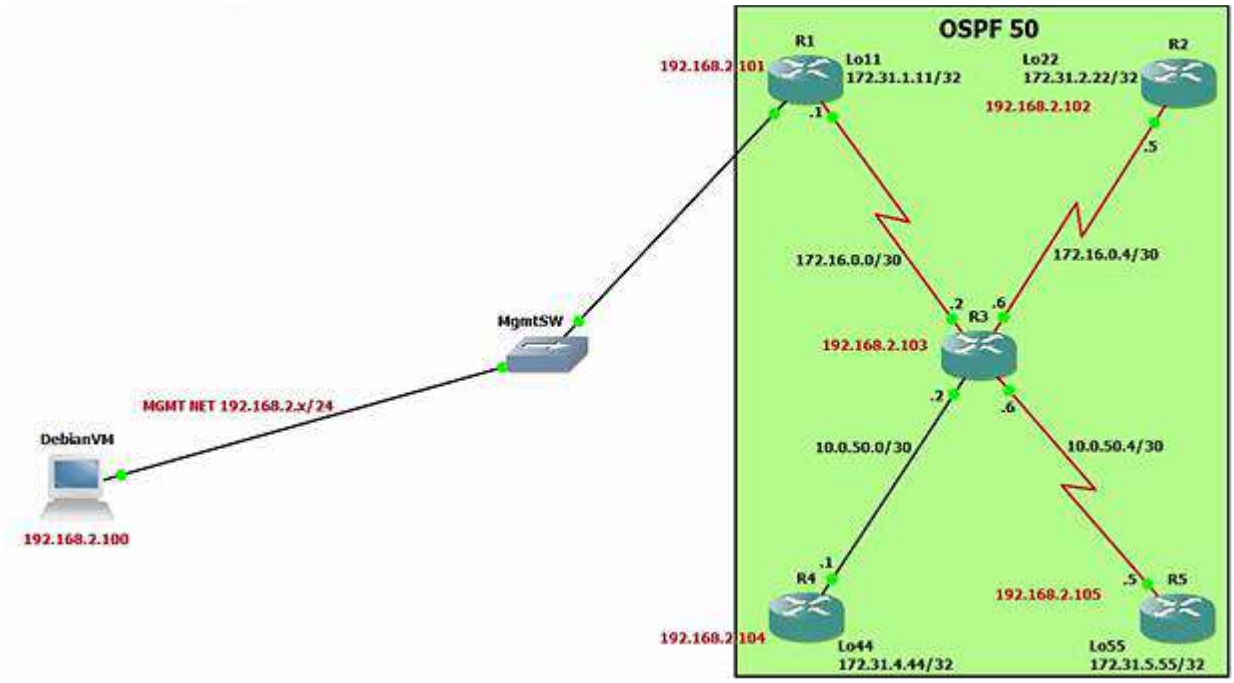


Рисунок 4.1 – Модель тестової мережі

Кожен вузол мережі має сконфігуровану динамічну маршрутизацію на базі OSPF технології. Маршрутизатори входять до спільної зони - area id 50.

Запуск розроблене програмне забезпечення буде здійснено на базі ВМ з інстальованим Linux (Debian 7.0). Слід підкреслити, необхідною умовою перед запуском додатку є попереднє здійснення конфігурації AC snmp community string на кожному з маршрутизаторів. Такі налаштування забезпечать надсилання SNMP запитів до обладнання з автентифікацією клієнтів, таких як snmp-server community public RO (public – вільне значення ідентифікатору/паролю).

Для збереження ресурсів ВМ для програми було обрано інтерфейс командного рядка (рис. 4.2)

```
SNMP community string should be the same on all devices running OSPF!

* Please enter root device IP: 192.168.2.101

* Please enter community string: public

* Valid IP address. Checking IP reachability...

* Device is reachable. Performing SNMP extraction...

* This may take a few moments...

* Please choose an action:

1 - Display OSPF devices on the screen
2 - Export OSPF devices to CSV file
3 - Generate OSPF network topology
e - Exit

* Enter your choice: 3
```

Рисунок 4.2 – Запит на виведення OSPF інформації

Як бачимо з зображеного інтерфейсу, опція "3" ініціює створення графу мережі представляючи назви вузлів, як – Router ID, та порти на ребрах графу, як – IP address. В якості прикладу демонстрації тестового графу для створеної мережевої топології розглянемо рисунок 4.3

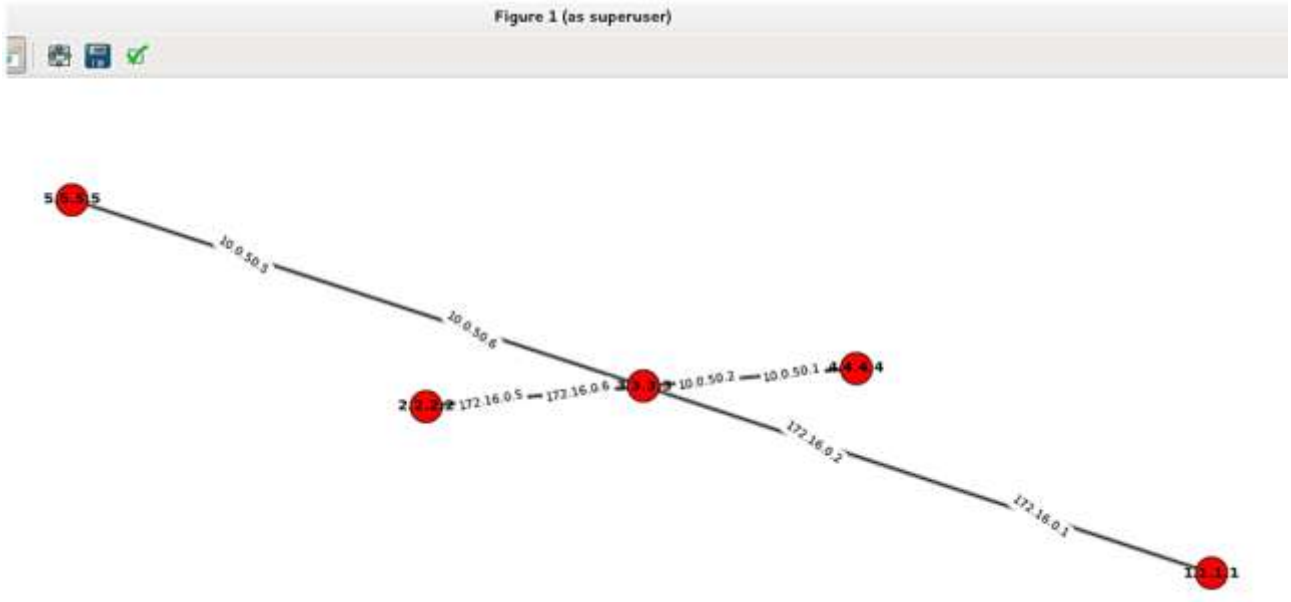


Рисунок 4. 3 – Відображення графу змодельованої мережі

Опція збереження файлу у різних форматах підтримується за рахунок інтерфейсу matplotlib модулю (рис. 4.4).

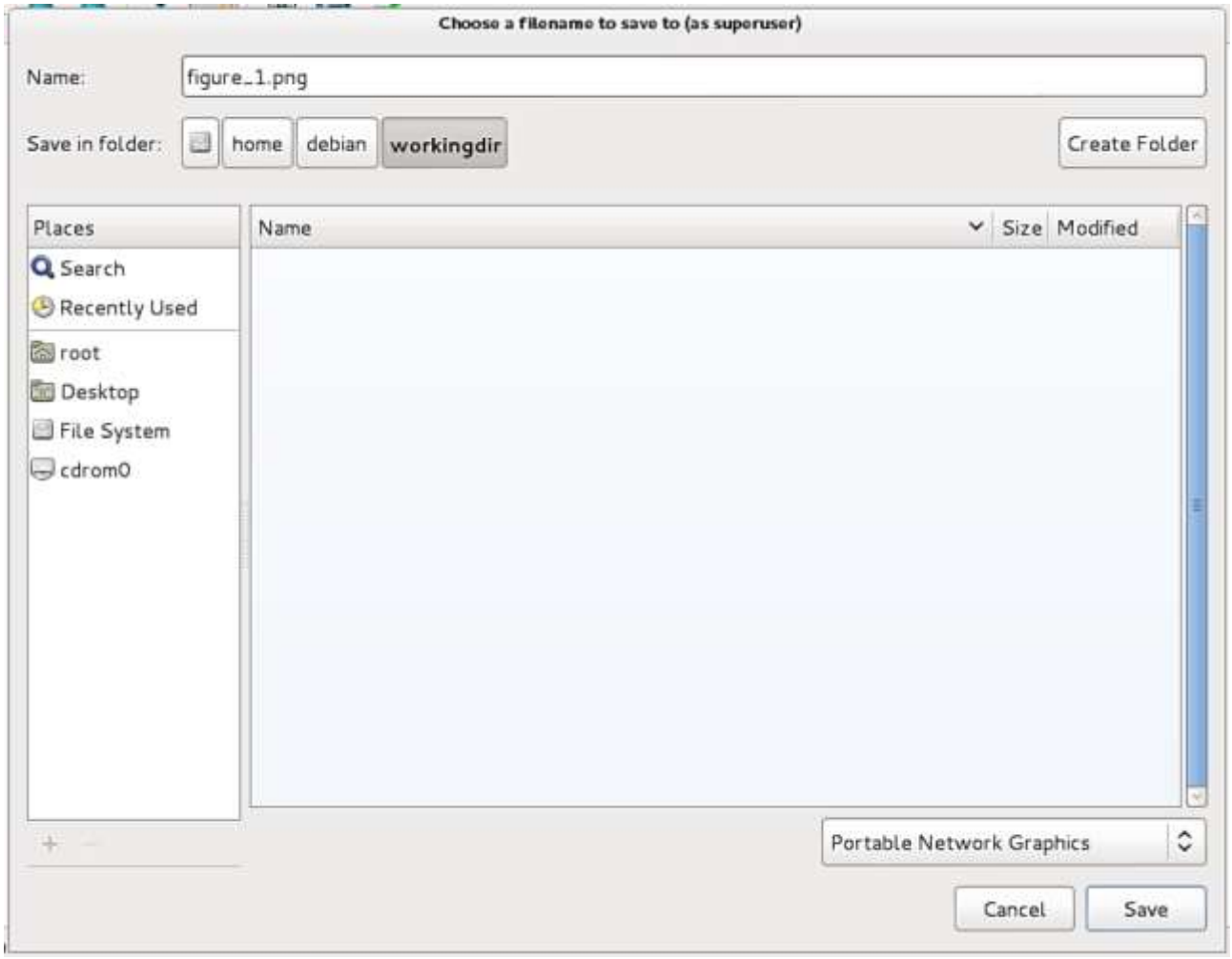


Рисунок 4.4 – Інтерфейс для збереження файлу і різних форматах

Програма також підтримує збереження таких даних, як Host Router ID, Hostname, Neighbors Router IP, Neighbors Router ID у CSV форматі. Така опція надасть можливість у подальшому працювати з отриманими даними у електронних таблицях MS Excel (Рис. 4.5).

```
* Enter your choice: 2


* Generating OSPF_DEVICES file...

* Check the script folder. Import the file into Excel fo
evices.

* Please choose an action:

1 - Display OSPF devices on the screen
2 - Export OSPF devices to CSV file
3 - Generate OSPF network topology
e - Exit

* Enter your choice: e


* Exiting... Bye!
```

Рисунок 4. 5 – Діалогове вікно збереження файлу CSV

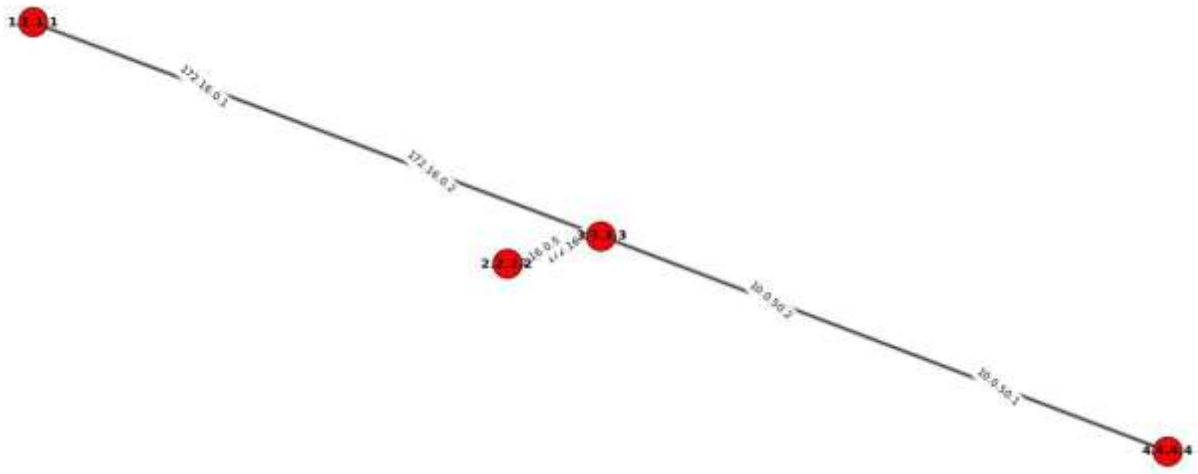


Рисунок 4.6- Оновлений граф без інформації про R5 роутер

В якості демонстрації програмного забезпечення, з метою відтворення ситуації відсутності зв'язку між вузлами мережі, емулюємо вихід з ладу se0/0 порту, що належить R5 маршрутизатору. Далі ініціюємо ще один запуск додатку задля повторного перерахунку інформації. На рисунку 4.6 бачимо оновлену топологію.

ВИСНОВКИ

У ході роботи було досліджено OSPF та EIGRP протоколи динамічної маршрутизації. Шляхом проектування комп’ютерної моделі корпоративної телекомунікаційної мережі та емуляції її роботи в графічному середовищі OPNET Modeler було зібрано дані на основі яких була встановлена якісна різниця в роботі зазначених протоколів.

З отриманих під час моделювання результатів дійшли висновку, що збіжність в протоколі EIGRP швидша, та з точки зору ефективності використання каналу зв'язку даний протокол має більшу продуктивність в порівнянні з OSPF протоколом. Однак, слід зазначити, що у випадку з великими мережами, що використовують обладнання різних виробників та мають тенденцією до масштабування, перевага все ж надається OSPF протоколу. Задля підвищення продуктивності роботи OSPF протоколу, за результатами моделювання мережі, було складено рекомендації відносно зменшення обсягу трафіку протоколу з метою збереження максимальної швидкості передачі даних по каналу зв’язку.

Для підтримки корпоративної мережі на етапі збору первинних даних про роботу мереж було створено програмний додаток, метою якого є перевірка топології мережі з точки зори її цілісності на випадок виходу з ладу мережевого обладнання.

Представлені в роботі результати моделювання, можуть бути корисними мережевим адміністраторам при проектуванні корпоративних телекомунікаційних мереж, оскільки вибір правильного протоколу динамічної маршрутизації дозволить підвищити продуктивність мережі та забезпечити стабільність мережі в цілому під час передачі чутливого до затримок трафіку через нестабільні лінії зв'язку.

СПИСОК ЛІТЕРАТУРИ

1. Celik, F., A. Zengin and B. Cobanglu, 2013. Discrete event simulation-based performance evaluation of internet routing protocols. Turk. J. Electr. Eng. Co., 21: 1720-1736.

2. Pethe, R.M. and S.R. Burnase, 2011. Technical era language of the networking-EIGRP. Int. J. Eng. Sci. Technol., 3: 1-5.

3. James F. Kurose. "Computer Networking:: A Top-Down Approach", Prentice Hall, 5th Edition, pp.420-450, 2010.

4. Nefkens P-J. Phase Three: Design, Deploy, and Extend. In: Transforming Campus Networks to Intent-Based Networking. Cisco Press; 2019.

5. Бачинский В.А., Гіоргізова-Гай В.Ш., Вибір протоколу динамічної маршрутизації в корпоративній IP-мережі // Системні дослідження та інформаційні технології, №1, 2015 – 100с.

6. Vishal sharma; Rajneesh Narula; Sameer khullar.“Performance Analysis of IEEE 802.3 using IGRP and EIGRP Routing Protocols”, International Journal of Computer Applications (0975 – 8887), (April 2012) , Volume 44, No13.

7. Don Xu and Ljiljana Trajković, Performance Analysis of RIP, EIGRP, and OSPF using OPNET // Simon Fraser University, Canada, 2011

8. Natalia Olifer and Victor Olifer, "Computer Networks: Principles, Technologies and Protocols for Network Design", Wiley; pp. 220-240, 3th. Edition, 2006

9. Moy J. RFC2328. OSPF Version 2. Westford, 1998 [Електронний ресурс]: http://tools.ietf.org/rfc/rfc2328.txt

10. Introduction to EIGRP [Електронний ресурс] // Cisco Systems, Inc. – Режим доступу: https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gatewayrouting-protocol-eigrp/13669-1.html

11. Mustafa Abdulkadhim, Routing Protocols Convergence Activity and Protocols Related Traffic Simulation With It’s Impact on the Network, International

Journal of Computer Science Engineering and Technology, Vol.5, Issue 3, March 2015 – 40-43 p.

12. R. Prasad and F. J. Velez, WiMAX Networks: Techno-Economic Vision and Challenges, Netherlands: Springer, 2010, doi:10.1007/978-90-481-8752-2.

13. Mohsin Masood, Mohamed Abuhelala, prof. Ivan Glesk, A comprehensive study of Routing Protocols Performance with Topological Changes in the Network // University of Strathclyde, Scotland UK, 2015

14. Enhanced Interior Gateway Routing Protocol // Cisco [електронний ресурс] - http://docwiki.cisco.com/wiki/Enhanced_Interior_Gateway_Routing_Protocol

15. Documentation Python Tutorials – Modules // Python [електронний ресурс] - https://docs.python.org/2/tutorial/modules.html

ДОДАТКИ

ДОДАТОК А

```
interface FastEthernet0/1
ip address 192.168.50.4 255.255.255.0
interface GigabitEthernet6/0
 ip address 10.1.1.1 255.255.255.252
router ospf 1
 log-adjacency-changes
 area 1 range 192.168.0.0 255.255.192.0
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.50.0 0.0.0.255 area 1
```

Конфігурація R0:

```
hostname R0
interface Loopback1
 ip address 192.168.1.1 255.255.255.0
interface FastEthernet0/1
 ip address 192.168.50.1 255.255.255.0
 ip ospf priority 100
router ospf 1
 log-adjacency-changes
 network 192.168.1.0 0.0.0.255 area 1
 network 192.168.50.0 0.0.0.255 area 1
```

Конфігурація RE:

```
hostname RE
interface Loopback1
 ip address 3.3.1.1 255.255.255.0
interface Loopback2
 ip address 3.3.2.1 255.255.255.0
interface Loopback3
 ip address 3.3.3.1 255.255.255.0
interface FastEthernet3/0
 ip address 10.3.3.1 255.255.255.252
router eigrp 1
 network 3.3.0.0 0.0.3.255
 network 10.3.3.0 0.0.0.3
 no auto-summary
```