МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему:

«Протоколи динамічної маршрутизації в корпоративних мережах»

Завідувач
випускаючої кафедри **Довбиш А.С.**

Керівник роботи **Великодний Д.В.**

Студента групи ІК.мз – 91.с **Сергієнка Ю.С.**

СУМИ 2020

Сумський державний університет

(назва вузу)

Факультет *ЕлІТ* Кафедра *Комп'ютерних наук*

Спеціальність *«Інформаційно-комунікаційні технології»*

Затверджую:

зав.кафедрою _____

_____

"_____" _____ 20___р.

ЗАВДАННЯ
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТОВІ

Сергієнку Юрію Сергійовичу

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) *Протоколи динамічної маршрутизації в корпоративних мережах*

затверджую наказом по інституту від "____" _____ 20 ___ р. № _____

2. Термін здачі студентом закінченого проекту (роботи) _____

3. Вхідні данні до проекту (роботи) _____
_____
_____
_____

4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити) *1) Аналіз проблеми. Постановка задачі дослідження. 2) Визначення методів забезпечення динамічної маршрутизації 3) Дослідження ефективності роботи протоколів динамічної маршрутизації 4) Розробка інформаційного та програмного забезпечення дослідження роботи мережі*

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) _____
_____
_____
_____
_____

6. Консультанти до проекту (роботи), із значенням розділів проекту, що стосується їх

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання _____

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів дипломного проекту (роботи)	Термін виконання проекту (роботи)	Примітка
1.	*Аналіз проблеми. Постановка задачі дослідження*		
2.	*Визначення методів забезпечення динамічної маршрутизації*		
3.	*Дослідження ефективності роботи протоколів динамічної маршрутизації*		
4.	*Розробка інформаційного та програмного забезпечення дослідження роботи мережі*		
5.	*Оформлення пояснювальної записки до дипломної роботи*		

Студент – дипломник _____
(підпис)

Керівник проекту _____
(підпис)

РЕФЕРАТ

Записка: 56 стор., 19 рис., 9 табл., 2 додатка, 17 джерел.

Об'єкт дослідження — динамічна маршрутизація та технології її забезпечення.

Мета роботи — підвищення ефективності роботи корпоративної мережі.

Методи дослідження — моделювання мережі в лабораторних умовах та аналіз її ефективності.

Результати — змодельовано модель OSPF мережі, за результатами дослідження – зроблено висновники задля підвищення ефективності роботи корпоративної мережі. Також створено програмне забезпечення для моніторингу цілісності топології, на мові програмування Python.

ДИНАМІЧНА МАРШРУТИЗАЦІЯ, ЗБІЖНІСТЬ ПРОТОКОЛІВ, ENHANCED INTERIOR GATEWAY PROTOCOL,

OPEN SHORTEST PATH FIRST, SIMPLE NETWORK MANAGEMENT PROTOCOL, МОНІТОРИНГ МЕРЕЖІ.

Зміст

ВСТУП

Забезпечення технології динамічної маршрутизації є одним з ключових завдань роботи корпоративної мережі. Відмовостійкість, ефективне використання ресурсів та їх підвищення, масштабованість мережі забезпечуються за допомогою використання відповідних протоколів динамічної маршрутизації. Ці властивості слугують обґрунтовунням того, що корпоративні мережі повинні функціонувати не лише на основі статичного оголошення маршрутів, а й їх використанням технологій динамічної маршрутизації.

Поміж найпопулярніших протоколів внутрішньої маршрутизації можна виділити наступні: OSPF, EIGRP, RIP, IS-IS та інші. Всі вони є потужними інструментами, дія яких базується на дотриманні основного закладеного алгоритму пошуку найкоротшого шляху до кінцевої точки призначення.

У рамках даної роботи було обрано об’єктом дослідження технології з забезпечення динамічної маршрутизації. Адміністратор мережі повинен чітко розуміти як саме спрацює маршрутизація при використанні того чи іншого протоколу ще на етапі проектування, та який саме протокол буде найефективніший відповідно до заданих умов. Отже виявлення переваг, недоліків найпоширеніших протоколів та засобів підвищення їх ефективності стало предметом дослідження.

У результаті роботи було побудовано комп’ютерну модель корпоративної мережі з налаштуванням OSPF, на основі якої було зібрано перелік рекомендацій, щодо підвищення ефективності роботи мережі. Також було створено програмне забезпечення, для моніторингу цілісності топології. Результати можуть бути використані мережевими адміністраторами при конфігурації та проектуванні мережі, а також при вивченні технології роботи протоколу.

1. ПРОТОКОЛИ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ

1.1 Основні принцип роботи динамічної маршрутизації та її задачі

Для детального аналізу розглянимо основні задачі та принципи работи динамічної маршрутизації. Адаптивна маршрутизація або динамічна, описує здатність системи, в якій шляхи визначаються точками призначення, знаходити альтернативний маршрут в змінних умовах. Адаптація націлена на знаходження найбільшої кількості доступних шляхів, що зберігають досяжність кінцевих точок, у разі втрати нод або зв'язку між частиною нод. Ця особливість забезпечує перевагу над статичною маршрутизацією з використанням якої, проблеми відмови шляху можуть буди вирішені тільки пост-фактум. Авжеж, можна передбачити наперед і задати декілька статичних резервних маршрутів, але якщо мережа постійно розширюється та розвивається, в решті-решт це призведе до збільшення трудозатрат на її підтримку та неодмінно призведе до виникнення петель маршрутизації.

Усі протоколи маршрутизаціїї можна поділити на дві великі групи [1]: зовнішні (EGP – Exterior Gateway Protocol) та внутрішні (IGP – Interior Gateway Protocol). Для того щоб пояснити різниці між ними введемо поняття «автономної системи» (AS) - в загальному сенсі називається група маршрутизаторів, що знаходяться під спільним управлінням. Протоколи внутрішньої маршрутизації використовуються в середені самої автономній системі, зовнішні, в свою чергу, для з'єднання автономних систем між собою. Внутрішні протоколи поділяються на Link State (OSPF, IS-IS) та Distance-Vector (RIP, EIGRP). Принципова різниця між цими двома видами полягає в наступному [2]:

1. Процесі вибору найкращого маршруту;

2. Кількості інформації про мережу, що зберігається кожним маршрутизатором: у разі використання Link State – мають уявлення про всю мережу, DV протоколів – відомі тільки свої сусіди;
3. Типом інформації, яким обмінюються маршрутизатори: таблиці топології у Link State та таблиці маршрутизації у DV.

Для випадків коли маршрутизатор налаштований враховувати різні протоколи маршрутизації або задані деякі статичні маршрути вводиться термін: адміністративна дистанція (AD). AD – це ціле число від 0 до 255, що виражає «міру довіри» маршрутизатора до певного маршруту. Чим менша AD, тим більша довіра. У таблиці 1.1 наводиться приклад розподілу значень AD з точки зору Cisco.

Таблиця 1.1 Пріоритети маршрутів згідно значення AD

Протокол	Адміністративна дистанція
Connected interface	0
Static route	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
IGRP	100
OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140

Продовження таблиці 1.1

Протокол	Адміністративна дистанція
On Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200
Unknown	255

1.2 EIGRP протокол - динамічна

EIGRP – вдосконалений дистанційно-векторний протокол динамічної маршрутизації, розроблений компанією Cisco [3].

Основними характеристиками протоколу є:

- швидка збіжність (у порівнянні з іншими дистанційно-векторними протоколами);
- часткові оновлення;
- підтримка VLSM;
- складна метрика;
- підтримка різних протоколів мережевого рівня (IP, IPX, AppleTalk);
- використання multicast (224.0.0.10) та unicast адрес, замість широкомовної розсилки;
- однакові налаштування протоколу при використанні різноманітних протоколів канального рівня (наприклад, у OSPF налаштування відрізняються для Ethernet та Frame Relay).

Всі повідомлення EIGRP інкапсулюються до IP-пакети, номер EIGRP у полі protocol IP-пакету – 88.

Протоколом EIGRP використовується 5 типових повідомлень:

Hello – маршрутизатори застосовують hello-пакети для того щоб знайти сусідів. Пакети відправляються в режимі multicast і не вимагають підтвердження про отримання.

Update – містить інформацію про зміни маршрутів. Вони надсилаються тільки на маршрутизатори, яких стосується оновлення. Update пакети можуть бути надіслані конкретному маршрутизатору (unicast) або групі маршрутизаторів (multicast). Отримання update-пакету підтверджується пакетом ACK пакету.

Query – при виконанні маршрутизатором підрахунку маршруту і якщо feasible successor відсутній, маршрутизатор надсилає query-пакет своїм сусідам щоб визначити чи нема feasible successor для пункту призначення. Query-пакети, зазвичай, надсилаються в режимі multicast. Отримання query-пакету підтверджується надсиланням ACK пакету отримувачем.

Reply – надсилается у відповідь на query-пакет. Reply-пакети надсилаються unicast, до відправника query-пакету. Отримання query-пакету підтверджується надсиланням ACK пакету.

ACK – підтверджує отримання пакетів update, query, reply. ACK-пакети выдправляються в режимі unicast і містять у собі acknowledgment number. Фактично це hello-пакети, що не передають даних. Для ACK пакетів використовується негарантована доставка.

Процесом відправки та отримання пакетів EIGRP управляє протокол RTP (Reliable Transport Protocol). З його допомогою відбувається гарантована доставка пакетів. Для цього використовується пропрієтарний алгоритм Cisco, reliable multicast. Пакети надсилаються на multicast-адресу 224.0.0.10. При отриманні такого пакету надсилається підтвердження відправнику. RTP

також забезпечує збереження порядку пакетів. У кожному пакеті використовується два номера послідовності. Кожен пакет включає в себе номер присвоєний йому відправником. Цей номер інкрементується при кожному надсиланні нового пакету маршрутизатором. Відправник також розміщує в пакеті номер останнього отриманого пакету від відправника.

У деяких випадках RTP використовує негарантовану доставку. У таких пакетах не проставляються номера послідовностей і вони не потребують підтвердження отримання.

Дослідження маршрутів відбувається за етапами.

Новий маршрутизатор, при завантаженні, надсилає hello-пакет через усі інтерфейси, які сконфігуровано для EIGRP.

Усі маршрутизатори, які отримали такий пакет на свій інтерфейс, надсилають назад свій hello-пакет, а далі update-пакет, який містить інформацію про всі маршрути з таблиці маршрутизації, за винятком маршрутів, у яких напрямок руху трафіку йде через цей же інтерфейс (Split Horizon).

Для того щоб маршрутизатори стали сусідами повинні виконуватись такі умови:

- Маршрутизатори повинні бути в одній AS;
- Маршрутизатори повинні пройти аутентифікацію;
- Повинні співпадати значення K-коефіцієнтів;
- Відношення сусідства мають установлюватися на primary-адресах.

Після встановлення сусідських відношень, новий маршрутизатор надсилає сусідам підтвердження про отримання update-пакетів.

Маршрутизатор вносить в свою таблицю топології всі дані з отриманих update-пакетів.

Запис маршруту у таблиці топології може знаходитись у двох станах: активному або пасивному. Нормальний стан – пасивний. Запис перейде в активний стан, у випадку якщо successor для даного маршруту - недоступний і в таблиці топології немає feasible successor для цього маршруту. Тоді відбувається перерахунок таблиці для вибору нового successor-а.

Далі новий маршрутизатор надсилає сусідам Update пакет зі своїми маршрутами, за винятком тих, що направлені через цей же інтерфейс.

Сусіди надсилають назад підтвердження про отримання.

Після чого маршрутизатори готові до оновлення таблиці маршрутизації.

EIGRP підраховує метрику з використанням коефіцієнтів. За замовчування, значення коефіцієнтів наступні: К1=К3=1, К2=К4=К5=0.

Загальна метрика підраховується за допомогою показників bandwith (пропускна здатність) та delay (затримка). Для обчислення значення bandwith використовується формула (1.1):

$$Bandwith = (10^7/bandwidth(i))*256; \quad (1.1)$$

- де bandwidth(i) – найменша пропускна здатність з усіх вихідних інтерфейсів на шляху у мережу призначення, виражається в кілобітах за секунду.

Формула для обчислення значення delay (1.2):

$$Delay = delay(i) * 256; \quad (1.2)$$

- де delay(i) – сумма всіх затримок сконфігурованих на вихідних інтерфейсах на шляху в мережу призначення, виражається в десятках мікросекунд. Затримка, що показується командою ‘ip eigrp topology’ або ‘show interface’ вказана в мікросекундах.

Для обчислення метрики, у випадку коли K5=0, використовується наступна формула (1.3):

M = (K1*bandwidth)+[(K2*bandwidth)/(256-load)]+(K3*delay); (1.3)

- де load – завантаження (оцінка від 1 до 255).

Якщо K5 не дорівнює 0 (1.4), то додатково виконується наступна операція:

Metric = M*[K5/(Reliability+K4)]; (1.4)

- де Reliability – надійність (оцінка від 1 до 255).

Експерти Cisco не рекомендують змінювати значення коефіцієнтів метрики за замовчуванням для уникнення петель маршрутизації [3].

Diffusing Update Algorithm (DUAL) – алгоритм який використовує протокол EIGRP для підрахунку маршрутів.

Визначення у термінології алгоритму:

Successor – маршрутизатор через який проходить оптимальний маршрут в мережу призначення.

Feasible Successor (FS) – резервний маршрутизатор, через який можна дістатись в мережу призначення, у випадку якщо successor стане недоступним.

Feasible distance (FD) – метрика для маршруту в мережу призначення.

Advertised distance (AD) або Reported distance (RD) – метрика маршруту в мережу, для того маршрутизатора який оголошує про цей маршрут.

Feasible Condition (FC) – для того, щоб маршрутизатор міг бути обраний в якості FS для певного маршруту, AD для цього маршрутизатору

повинно бути менше ніж FD для основного маршруту. Іншими словами, резервний маршрутизатор має бути ближче до мережі призначення ніж маршрутизатор для якого він буде резервним.

1.3 Open Shortest Path First (OSPF) протокол

OSPF (Open Shortest Path Fist) – стандартизований протокол динамічної маршрутизації, створений IETF. OSPFv2 це поточна версія для IPv4. Базується на технології link-state (SPF) [4].

OSPF інкапсулюється в IP, номер протокола – 89.

Для передачі пакетів використовуються мультикаст адреси:

1. 224.0.0.5 всі маршрутизатори OSPF;
2. 224.0.0.6 всі DR.

Перелік типів мереж, що підтримуються протоколом OSPF:

1. Точка-точка (point-to-point): тунелі, T1, E1, PPP, Frame-Relay, P-to-P;
2. Широкомовні мережі з множинним доступом (broadcast): Ethernet;
3. Нешироковомовні мережі з множинним доступом (Non Broadcast Multiple Access, NBMA): Frame-Relay, ATM, X.25.

Метрика (metric) – умовний показчик відстані до мережі призначення.

Вартість (cost) – умовний показчик «вартості» пересилання даних каналом. Вартыть в OSPF залежить безпосередньо від пропускної здатності інтерфейса (bandwidth).

Ідентифікатор маршрутизатору (router ID, RID) – унікальне 32-бітне число, яке ідентифікує маршрутизатор в межах однієї автономної системи

Зона (area) – сукупність мереж і маршрутизаторів, що мають однаковый ідентифікатор зони.

База даних стану каналів (Link state database, LSDB) – список всіх записів про стан каналів (LSA). Зустрічається також термін топологічна база даних (topological database), використовується як синонім бази даних станів каналів.

Оголошення про стан каналу (link-state advertisement, LSA) – одиниця даних, яка описує локальний стан маршрутизатору або мережі.

Сусіди (neighbours) – два маршрутизатори, інтерфейси яких знаходяться в одному широкомовному сегменті (і на яких увімкнений OSPF на цих інтерфейсах)

Відношення сусідства (adjacency) – взаємозв’язок між сусыдами, сусідніми маршрутизаторами, встановлений з метою синхронізації інформації.

Hello-протокол (hello protocol) – протокол, що використовується для встановлення і підтримки сусідських відношень.

База даних сусідів (neighbours database) – список всіх сусідів.

Hello – пакети, що використовуються для визначення сусідів, встановлення відношення сусідства та моніторингу їх доступності (keepalive).

LSR – пакети, за допомогою яких запитується повна інформація про LSA, яких бракує в LSDB локального маршрутизатора.

DBD – пакети, які описують вміст LSDB.

LSU – пакети, які передають повну інформацію, що міститься в LSA.

LSAck – пакети, за допомогою яких підтверджується отримання інших пакетів.

Необхідність подолання обмежень протоколів вектору відстаней призвела до розробки протоколів стану зв’язків. З використання оновлення стану зв’язків (LSA - Link State Advertisement), кожен маршрутизатор будує власний погляд на мережу, підтримує список сусідів, список всіх маршрутизаторів зони і перелік найкращих шляхів для кожного напрямку.

Протоколи стану зв’язків генерують оновлення тільки у випадку зміни мережевої топології. Коли зв'язок змінює свій стан, маршрутизатор виявляє це і створює LSA про цей зв'язок.

Процес роботи з протоколом можна описати такими етапами.

Після ввімкнення OSPF на маршрутизаторі він обирає Router ID. В залежності від реалізації, Router ID може обиратись за різними підходами: максимальна IP-адреса або мінімальна IP-адреса, яка назначена на інтерфейсах маршрутизатора; або ж використовується ручний спосіб задання Router ID, в цьому випадку, Router ID повинен бути унікальним в AS.

Після визначення Router ID, процес OSPF має бути перезавантажений, а всі LSA, які згенерував маршрутизатор, мають бути видалені з AS, до перезавантаження.

Виявлення сусідів за допомогою Hello-пакетів.

Маршрутизатори обмінюються hello-пакетами через усі OSPF інтерфейси (на яких OSPF активовано). Маршрутизатори, які знаходяться в одному широкомовному сегменті, визначаються як сусіди, коли вони приходять до домовленості про вказані в hello-пакетах параметри.

Для того щоб маршрутизатори стали сусідами повинні виконатись певні умови. Для цього необхідно щоб у hello-пакетах співпали значення таких полей:

- У маршрутизаторів мають співпадати мережа та маска мережі;

- Area ID – так як в OSPF границя зони проходить через маршрутизатор, то маршрутизатори в одному широкомовному сегменті, мають буть в одній зоні;
- Authentication – пароль, що використовується для автентифікації і тип автентифікації. Маршрутизатори не обов’язково мають використовувати автентифікацію, але якщо вона використовується, то паролі та тип мають співпадати;
- Hello Interval – частота відправки повідомлень Hello;
- Router Dead Interval – період часу, за проходженням якого, сусід рахується недоступним, якщо не було Hello;

1. Stub area flag – не обов’язковий флаг, що встановлюється на всіх маршрутизаторах, які належать тупіковій зоні (stub area).

Adjacency (відношення сміжності, відношення сусідства) це тип сусідства між маршрутизаторами, по якому вони синхронизують LSDB. Встановлення цих відношень залежить від типу мережі: якщо маршрутизатори знаходяться в мережі point-to-point, вони починають синхронизацію LSDB один з одним; якщо маршрутизатори знаходяться в мережі з множинним доступом, то вони обирають DR і виконують синхронизацію LSDB з ним.

Синхронизація LSDB виконується в декілька етапів, за сформованим відношенням сусідства проходить обмін пакетами.

DBD – за допомогою цих пакетів маршрутизатори інформують один одного про інформацію яку вони знають в стислому вигляді

LSR – після обміну DBD-пакетами, за допомогою LSR, маршрутизатори запитують у сусіда інформацію якої невистачає.

LSU (містить повний опис LSA). У відповідь на LSR, який йому надіслав сусід, маршрутизатор надсилає LSU, з повним описом інформації, якої не вистачає сусіду.

LSAck – після отримання LSU, маршрутизатор надсилає підтвердження, що інформація отримана.

Якщо обидва маршрутизатори мають запросити один у одного інформацію, то ця процедура повторюється і в інший напрямок.

Після цього, LSDB синхронизована, що означає ідентичність її для сусідів. Після синхронизації LSDB, маршрутизатор надсилає оновлення далі, своїм сусідам в інших широкомовних сегментах. Надсилаючи оголошення через зону, всі маршрутизатори будують ідентичну LSBD.

Коли база даних побудована, кожен маршрутизатор використовує алгоритм SPF для вираховування графу без петель, який описує найкоротший шлях до кожного відомого пункту призначення. Граф це дерево найкоротшого шляху. Кожен маршрутизатор будує таблицю маршрутизації, базуючись на своєму дереві.

OSPF використовує метрику вартості (cost). Вартість порівнюється у маршрутизаторів одного типу. Підрахунок вартості для кожного інтерфейсу не стандартизовано, на це слід звертати увагу в мультивендорному середовищі.

Для підрахунку вартості Cisco використовує наступну формулу (1.5)

cost = reference bandwidth/ link bandwidth, (1.5)

- де reference bandwidth це пропускна здатність, відносно якої вираховується, за замовчуванням вартість інтерфейса. За замовчуванням 100 Mb, може бути змінена.

Сумарна вартість маршруту – сума вартості вихідних інтерфейсів за шляхом передачі LSA.

Для позначення недоступної мережі, OSPF використовує метрику рівну 16777215(24^{24}-1).

Зонування домену OSPF.

При розділенні AS на зони, маршрутизаторам з однієї зони, невідома інформація про детальну топологію інших зон.

Розділення на зони використовується для:

2. зниження навантаження на CPU маршрутизаторів, за рахунок зменшення кількості перерахунку по алгоритму SPF;
- зменьшення розмір таблиць маршрутизації (за рахунок сумування маршрутів на границях зон);
- зменшення кількості пакетів оновлення станів каналу.

Для кожної зони призначається ідентифікатор (area ID). Ідентифікатор може бути як в десятковому форматі так і в форматі запису IP-адреси, але ідентифікатор зон не є IP-адресами, а отже, можуть співпадати з будь-якою використаною IP-адресою.

В OSPF взаємодія між зонами можлива лише через зону 0. У зоні 0 не має бути розривів, якщо ненульова зона має бути приєднана до іншої ненульової зони, використовуються: virtual-link або звичайний тунель налаштований вручну, наприклад, GRE.

Існують наступні типи зон:

1. Backbone (area 0) – магістральна зона. Дозволені всі типи маршрутів. Відповідальна за поширення маршрутизуючої інформації між

немагістральними зонами. Магістральна зона має бути сміжною з іншими зонами, але не обов’язково має бути фізично сміжною, з’єднання з магістральною зоною може бути втановлено за допомогою віртуальних каналів.

2. Normal. Звичайна зона, що створюється за замовчуванням. Також, дозволені всі типи маршрутів.
3. NSSA. Усі зовнішні маршрути повинні бути замінені на міжзональний маршрут за замовчуванням. В зоні може знаходитись ASBR
4. Totally NSSA. Всі маршрути інших зон та зовнішні маршрути для AS? Замінюються на маршрут за замовчуванням. В зоні може знаходитись ASBR.
5. Stub. Не приймає інформацію про зовнішні маршрути для автономної системи, але приймає маршрути інших зон. Якщо маршрутизаторам з тупикової зони необхідно передати інформацію за границю автономної системи, вони використовують маршрут за замовчуванням. ASBR не може знаходитись в зоні.
6. Totally Stub. Або «посилена» тупикова зона – в ній не тільки зовнішні маршрути, але й міжзональні замінені на маршрут за замовчуванням. Всі зовнішні маршрути замінені на міжзональний маршрут за замовчуванням. ASBR не може знаходитись в зоні.

LSA – одиниця даних, яка описує локальний стан маршрутизатора або мережі. Множина LSA створює базу даних стану каналів.

Сумарна інформація про LSA наведена в таблиці 1.2.

У кожного типу LSA такі функції:

3. Router LSA та Network LSA описують яким чином з’єднані маршрутизатори та мережі всередині зони.

4. Summary LSA призначені для зменшення кількості інформації про зони, що передається. Описують мережі інших зон для локальної.
5. ASBR Summary LSA описує для інших зон, як дійти до локального ASBR.
6. AS External LSA дозволяє передавати по автономній системі інформацію, яка отримана з зовнішніх джерел (наприклад, з іншого протоколу маршрутизації).

Таблиця 1.2 Сумарна інформації про LSA

Номер LSA	Назва LSA	Link-state ID	Джерело, що надсилає	Область поширення
LSA 1	Router LSA	Router ID відправника	Усі маршрутизатори	Всередині зони (IntraArea)
LSA 2	Network LSA	IP-адреса інтерфейса DR	DR (в мережах з множинним доступом)	Всередині зони (IntraArea)
LSA 3	Network Summary LSA	Мережі призначення і маска мережі	ABR	AS (InterArea)
LSA 4	ASBR Summary LSA	Router ID ASBR	ABR	AS (InterArea)
LSA 5	AS External LSA	Зовнішня мережа і маска	ASBR	AS (InterArea)
LSA 7	AS External LSA for NSSA	Зовнішня мережа і маска	ASBR у NSSA	NSSA

1.4 Постановка задачі

Проаналізувавши літературні джерела постановку задачі можна побудувати наступним чином:

- Необхідно проаналізувати якісні показники ефективності EIGRP та OSPF протоколів маршрутизації, що дозволить виявити їх недоліки та переваги.
- Використовуючи отриманні данні побудувати модель корпоративної мережі з використанням протоколів динамічної маршрутизації у середовищі GNS3 та виявити шляхи підвищення ефективності їх роботи.
- Розробити програмний додаток, що дозволить локалізацувати проблемні ділянки мережі у випадках відмови зв’язку на етапі моніторингу мережі.

2. ПРОТОКОЛИ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ ТА АНАЛІЗ ЇХ ПРОДУКТИВНОСТІ ЗАДОПОМОГОЮ OPNET

Вміння симулювати та моделювати продуктивність численних систем важливий інструмент для будь-якого IT фахівця. Інвестиції в дороге обладнання вимагає комплексної оцінки його продуктивності за допомогою моделей. Побудова моделі не є тривіальним завданням, це вимагає чіткого розуміння концепцій симуляції та моделювання, обширного знання властивостей змодельованої системи [5].

2.1 Використання OPNET та його функції

Головне питання на етапі побудови моделі це вибір інструментарію. При цьому важливими якостями для створення ефективної моделі є наступні:

1. детальна реалізація протоколів;
2. можливість зміни параметрів моделювання під час проведення експериментів;
3. платформенна незалежність;
4. розвинений графічний інтерфейс.

Для створення та аналізу моделювання мережі OPNET Modeler пропонує графічне середовище. Це доволі зручне і якісне програмне забезпечення може використовуватися для великої кількості задач. Наприклад, створення та перевірка якості протоколів зв’язку, планування мережі та її оптимізація. Також, за допомогою пакету, можливо перевірити правильність аналітичної моделі та опис протоколів [6, 7].

У редакторі проекту можна створити палітру об’єктів мережі, якої користувач може задати різні форми вузлів та зв’язків. Доступне автоматичне створення мережевих топологій – зірки, кола, рандомної мережі. Редактор підтримується утилітами для імпорту мережевих топологій у різних форматах. Доступна автоматична генерація рандоиного трафіку що генерується за обраними алгоритмами.

Отримані результати моделі можуть використовуватися для подальшого аналізу, з використанням графів та анімації трафіку, які також можна згенерувати автоматично.

Є декілька середовищ редактора – по одному для кожного типу об’єкта. Організація об’єктів ієрархічна, мережеві об’єкти (моделі) зв’язані набором вузлів і об’єктів зв’язку, при цьому об’єкти вузла зв’язані набором об’єктів типу модулів черговості, модулів процесора, передатчиків і приймачів.

Виклик події моделі процесора впродовж моделювання управляється збудженням переривання, а кожне переривання відповідає події, яка повинна бути оброблена моделлю процесу. Основа зв’язку між процесами – структура даних, що називається пакетом. Можуть бути задані формати пакету, тобто вони визначають, які поля можуть містити такі стандартні типи даних, як цілі числа, числа з плаваючою точкою та вказівники на пакети (ця остання особливість дозволяє інкапсулювати моделювання пакету).

Структура даних, що викликає інформацію контролю інтерфейсу (interface control information - ICI), може бути розділена між двома подіями моделей процесу – це ще один механізм міжпроцесорного зв’язку, це дуже зручно для команд моделювання і відповідає архітектурі багаторівневого протоколу. Процес також може динамічно створювати дочірні процеси, які спростять функціональний опис таких систем як сервери.

Декілька основних моделей процесу входять у базову комплектацію пакету, моделюючи популярні протоколи роботи з мережами і алгоритми, наприклад, протокол шлюзу границі (border gateway protocol - BGP), протокол контролю передачі.

2.2 Збіжність протоколів динамічної маршрутизації

Основним критерієм для аналізу та порівняння ефективності протоколів динамічної маршрутизації використаємо показники збіжності. Цей параметр протоколу характеризує тривалість інтервалу ймовірної нестабільності у роботі мережі. За цей проміжок часу протокол виявляє «недоступний» маршрут, та обирає інший шлях та розповсюджує інформацію в мережі. При підтримці роботи важливих додатків дуже важлива швидкість з якою мережа реагує на зміну топології.

OSPF включає в себе такі часові затрати, що безпосередньо впливають на швидкість збіжності [8]:

- перш за все, час, який треба для визначення проблеми фізичного рівня. Цей параметр є найбільш важливим. Перевірки чи канал доступний виконується за рахунок пакеті - Hello. Пакет надсилається один раз на 10 секунд кожним маршрутизатором. Якщо сусіди не відповдають на 4 пакети Hello поспіль – то такий сусіл вважатися недоступним.
- час для поширення LSA пакетів у мережі.
- час для підрахунку SPF алгоритму, після оновлення даних.
- і нарешті час для оновлення таблиць маршрутизації.

За допомогою роботи в OPNET було виконано оцінку статистики за такими характеристиками [6, 9]:

- Тривалість збіжності (конвергенції) таблиць маршрутизації EIGRP в мережі - Network Convergence Duration. EIGRP. Та тривалість збіжності в OSPF.
- Network Convergence Activity - запис хвиль змін по осі ординат між 1 та 0. 1 – значення коли процес збіжності активний
  та значення 0 – проміжок часу коли відсутні будь-які активності збіжності в мережі.
- Та Protocol Traffic sent (вимірюється в bits/sec).

2.3 Показники збіжності OSPF та EIGRP та їх дослідження в OPNET

Розглядаємо модель мережі яка розділена на 5 підмереж: subnet_1...5, які з’єднані дуплексним способом PPP DS3 (44.736 Мб/с). У кожній підмережі 10 роутерів Cisco, маємо в сумі корпоративну мережу з 50 роутерами та 87 локальними мережами.

Загальний вигляд топології підмереж відображено на рисинку 2.1.

Розглянемо окремо сценарії з OSPF конфігурацією та EIGRP, на 300 секунді після запуску дослідження емулюємо відмову зв’язку між підмережою subnet_1 та підмережою subnet_2, зв’язок відновиться після 500 секунди. Час симуляцію – 1320 секунд.

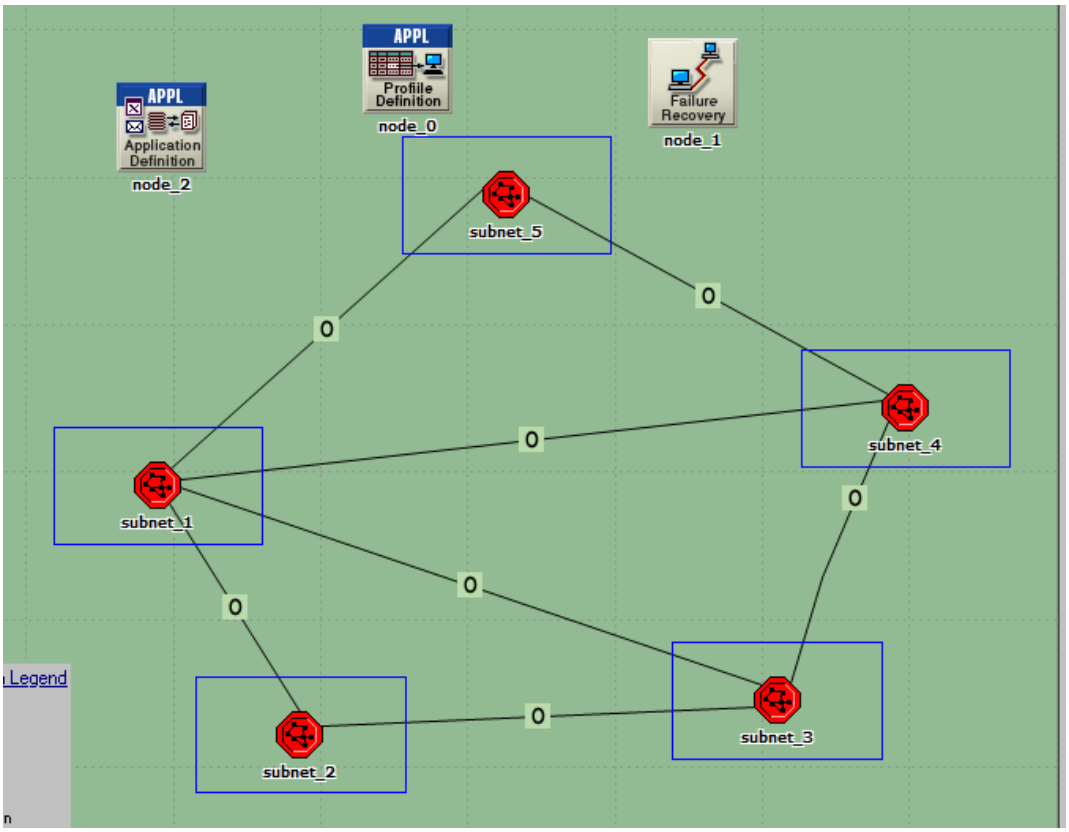


Рисунок 2.1 – Subnet_1...5

Топологія для всіх підмереж однакова, зображена на рисунку 2.2, на прикладі subnet_2.

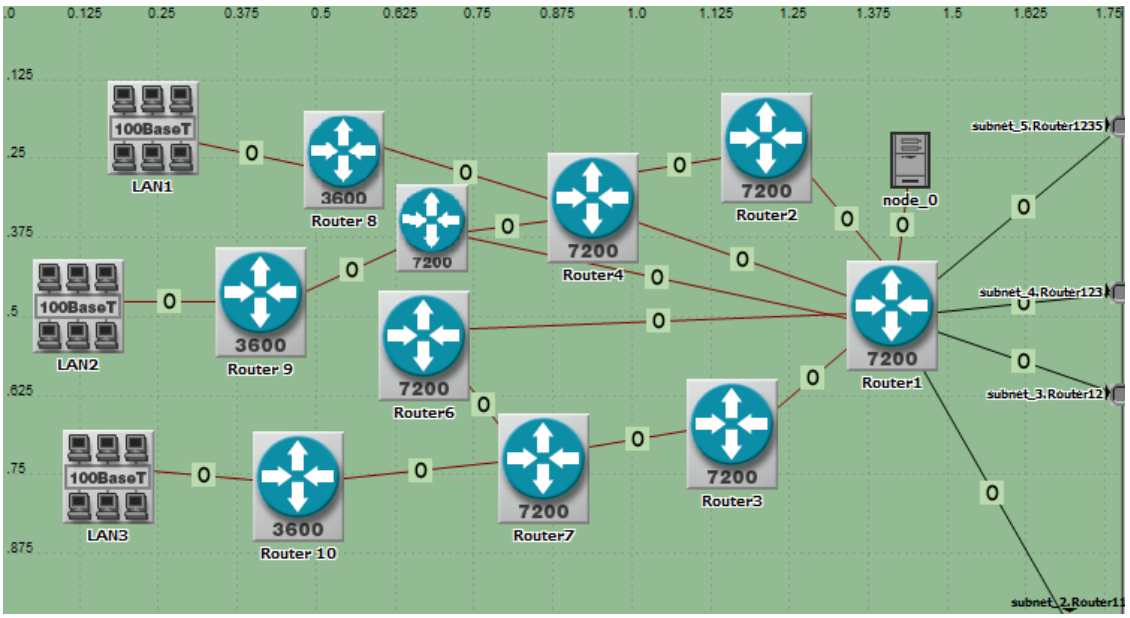


Рисунок 2.2 – OSPF. Топологія підмережі subnet_2

У результаті дослідження ми отримали наступні данні

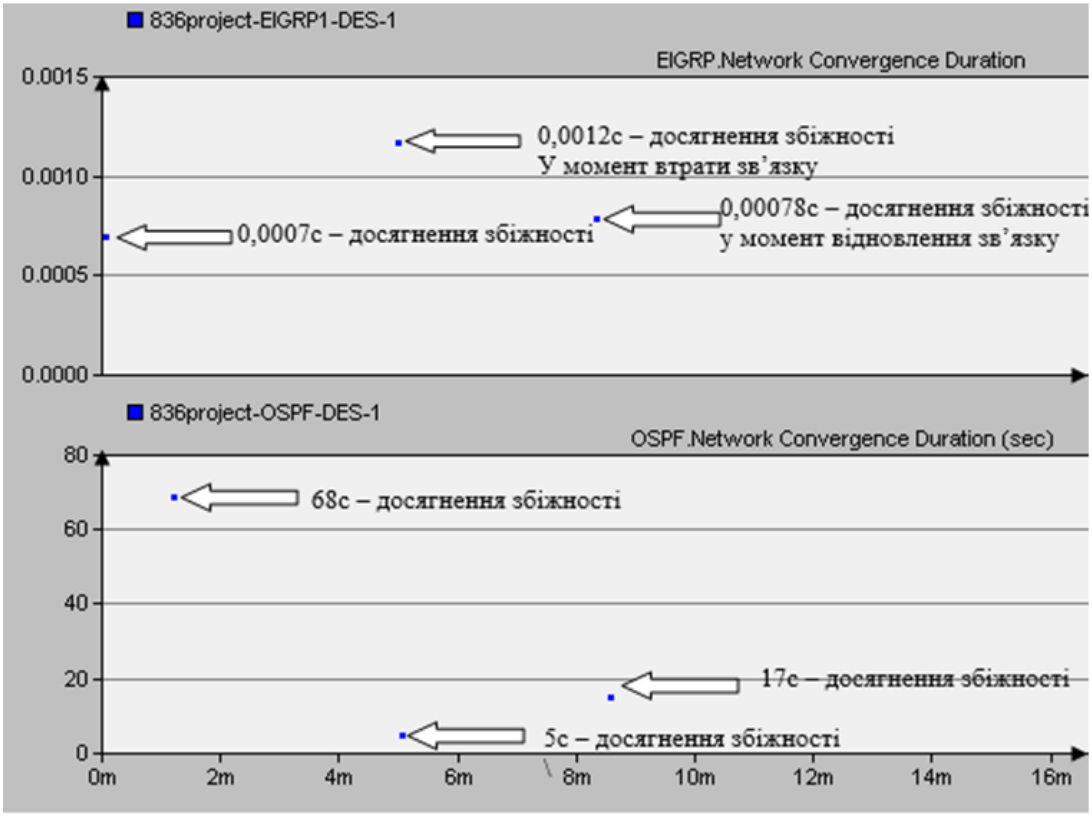
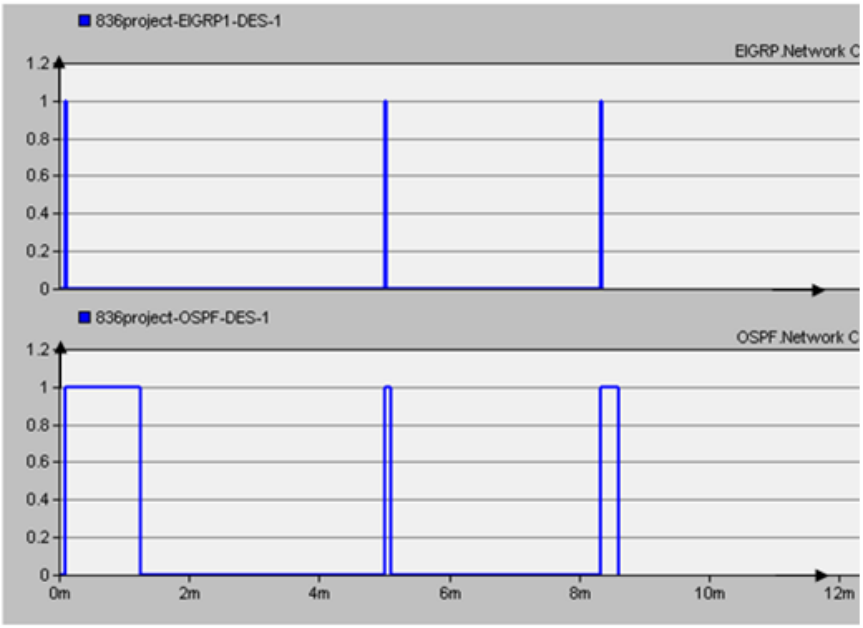


Рисунок 2.3 – Network Convergence Duration (sec) global statistic for EIRP and OSPF

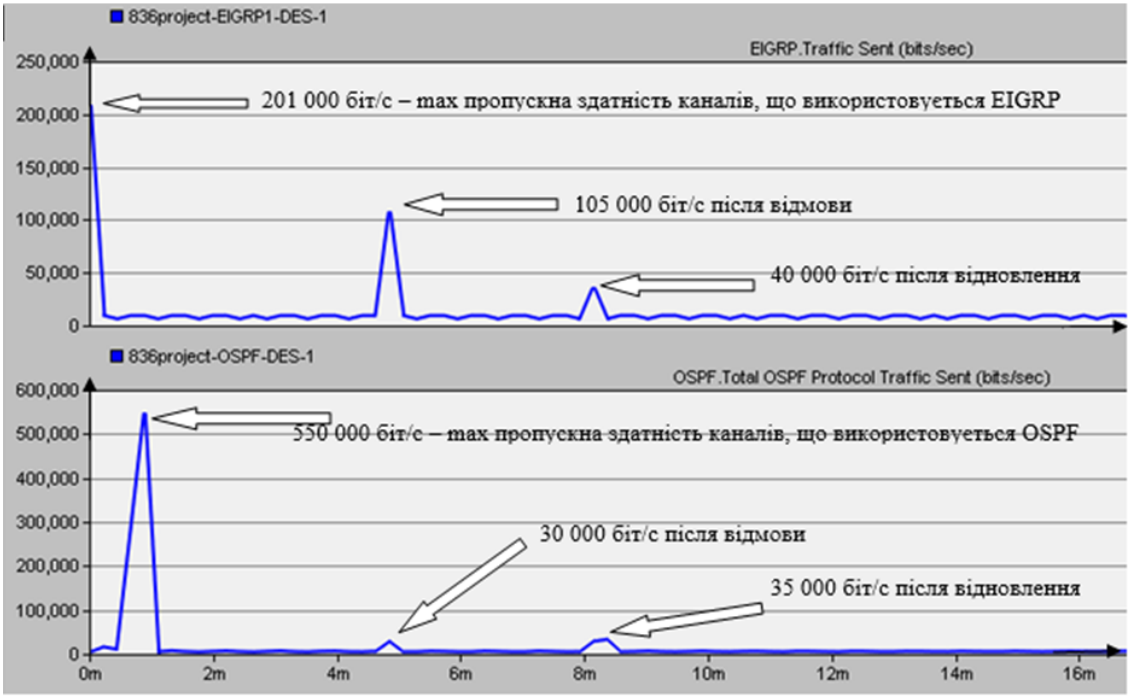
Як бачимо на рис. 2.3 час збіжність для EIGRP, коли кожен маршрутизатор має найактуальнішу інформацію, складає 0,0007 секунд при ініціалізації, у випадку виникненення розриву - 0,0012 секунд, а для відновлення - 0,00078 секунд. Для OSPF ці показники вищі: ініціалізація – 68 секунд, відмова – 5 секунд, відновлення – 17 секунд. Як бачимо, для актуалізації данних для OSPF найбільше часу необхідно при запуску, а для EIGRP при відновленні маршруту. Але в порівнянні один з одним час збіжності у OSPF набагато більший ніж у EIGRP.

Швидкість збіжності, також, відображається на рисунку 2.4.



OY: Активність протоколу по досягненню збіжності: 0 – процеси не активні, 1 - активні;
OX: Час емуляції роботи мережі (хвилини)

Рисунок 2.4 – Network Convergence Activity



OY: Пропускна здатність (біт/с); OX: Час емуляції роботи мережі

Рисунок 2.5 – Total OSPF Protocol Traffic Sent (bits/sec)

На підставі результатів дослідження, наведених на рисунку 2.4 трафік надісланий OSPF за ініціалізації дослідження (550 000 біт/с) перевищує

найбільше значення для EIGRP (200 000 біт/с) в два рази більше. В свою чергу при відмові одного каналу OSPF займає аж 30 000 біт/с в той час як для EIGRP показники значно нижчі – 105 біт/с.

Завдяки додатку Opnet Modeler немає потреби в ручному підрахунку та пошуку вразливостей мережі. Ми можемо спроектувати модель, симулювати необхідні для нас умови та на підставі отриманих результатів зробити висновки. Завдяки Opnet Modeler ми можемо проаналізувати збіжність мережі та об’ємів трафіку що був згенерований у мережах з різними протоколами маршрутизації, у нашому випадку OSPF та EIGRP.

3. МЕТОДИ ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ ТА ЇХ ПІДВИЩЕННЯ

За результатами проведеної симуляції можемо зробити висновок про якісні переваги EIGRP над OSPF. Незважаючи на такі очевидні плюси, головним недоліком EIGRP полягає в можливості його використання лише на Cisco обладнанні, оскільки цей фактор ускладнює, а подекуди унеможливлює його застосування у мультивендорних мережах. Тож зосередимо увагу на OSPF який э більш універсальним.

Існує декілька метожів використання ресурсів мережі за технології OSPF. Принцип яких полягає у скороченні обсягу згенерованого трафіку протоколом, в різних частинах мережі.

Серед таких методів можна виділити наступні [4]:

- Використання так званої мультизонової мережі;
- Визначення Backup Designated Router (BDR) та Designated Router (DR);
- Застосування підсумовувань підмережі на так називаємих Area Border Router (ABR).

Розглянемо ці функції у симуляторі GNS3, за допомогою моделювання.

3.1 Проектування топології

Спроектована мережа та її топологія відображена на рисунку 3.1.

Використаємо моделі роутера Cisco 7200, з інтерфейсами Gigabit Ethernet та Fast Ethernet.

Роутер ISP – обладнання Інтернет провайдеру, який встановлено за границями AS.

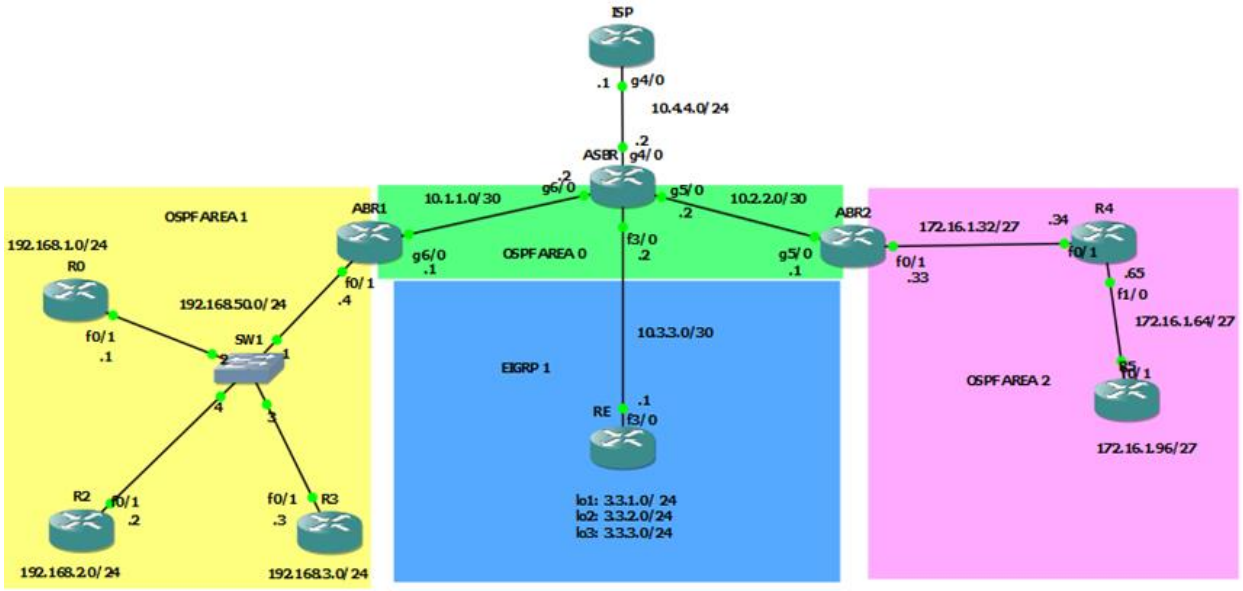


Рисунок 3.1 – Топологія моделі мультизонової корпоративної мережі з використанням OSPF та EIGRP

Роутер ASBR (AS boundary router) – маршрутизатор, який з'єднує автономну систему з зовнішньою мережею та знаходиться на її межі, має інтерфейси: Fast Ethernet та 3 Gigabit Ethernet. У нашому випадку EIGRP налаштовано для f3/0, а g6/0 та g5/0 належать до основної OSPF зони (назвемо її - Area 0).

ABR1 та ABR2 - граничні роутери зон, з портами які входять до основної зони: g6/0 (на ABR1) та g5/0 (на ABR2).

Домен EIGRP представлено з'єднанням ASBR-RE та loopback інтерфейсами на маршрутизаторі RE.

Зони 0, 1, 2 це дворівнева ієрархічна мережа: Area0 – зона, першого рівня, яка з'єднує Area1 та Area2 (зони другого рівня).

В Area1 сконфигуровано такі пристрої: Ethernet комутатор (SW1), ABR1 та роутери R0, R2, R3.

В Area2 сконфигуровані: ABR2 та роутери R2, R5.

Всередині зони, на граничних роутерах, необхідно спланувати IP-адресацію інтерфейсів, для подальшого підсумувування маршрутів. Для цього використаємо адреси підмереж з близьких діапазонів. Розробка легкорозширюванного та чіткого IP-плану дуже важлива на етапі планування (таблиця 3.1).

Таблиця 3.1 IP план корпоративної 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 1	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)
		R2	f0/1 (.2)
		R3	f0/1 (.3)

Продовження таблиці 3.1

Призначення	Адреса та маска мережі	Назва хосту	Інтерфейси (номер останнього октету)
OSPF Area 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 Підсумування маршрутів. Конфігурація

Головним пунктом на етапі проектування та моделювання є присвоєння адрес інтерфейсам, також дуже важливим пунктом є безпосередньо налаштування протоколів динамічної маршрутизації. Були використанні такі команди, для налаштування OSPF:

- router ospf 1 – команда вімкає OSPF, на роутері, з процесом номер 1
- network <ip address> <inverted subnet mask> area <X> – команда призначає мережі домен - OSPF та вказує номеру зони. Маска підмережі - інвертована або зворотня.
- default-information originate – перерозподіл маршрутів за замовчуванням, які визначаються граничним роутером AS роутерам під-рівнів. Задається на граничних роутерах Area1 та Area2.

Команди, які були використані для конфігурації EIGRP::

- router eigrp 1 – команда вімкнає EIGRP з процесом номер 1.

- network <ip address> <subnet mask> – команда присвоює домен EIGRP. Використання маски прямого формату.
- no auto-summary – команда вимкає авто-підсумувування адрес безкласових мереж.

Другим пунктом моделювання – для підсумувування маршрутів на пограничних роутерів зон використовуємо команди “area <X> range <summarized network ip address> <wildcard subnet mask>”,

де X – номер конкретної зони;

summarized network ip address – суммарна адреса підмереж;

wildcard subnet mask – зворотня маска підмережі.

На прикладі наступних адрес, розберемо, процес підрахунку суммарної адреси та маски підмереж:

- 192.168.50.0/24
- 192.168.3.0/24
- 192.168.2.0/24
- 192.168.1.0/24.

Переведемо адреси у бінарний вигляд:

- 192.168.50.0 - 11000000.10101000.00110010.00000000
- 192.168.1.0 - 11000000.10101000.00000001.00000000
- 192.168.2.0 - 11000000.10101000.00000010.00000000
- 192.168.3.0 - 11000000.10101000.00000011.00000000

Визначимо порядковий номер біту, після якого адреси відрізняються. У цьому прикладі це третій біт, третього октету.

Замінимо на одиниці біти що співпадають, а неспівпадіння на нулі, для того щоб визначити маску сумарного маршруту, отримаємо такий запис - 11000000.10101000.11000000.00000000. Перведемо це значення до десяткового вигляду - 255.255.192.0.

Підставимо нулі усі значення після другого біту третього октету, для визначення адреси сумарного маршруту - 11000000.10101000.00000000.00000000. переведемо до десяткового вигляду - 192.168.0.0. Отже сумарним маршрутом є:

192.168.0.0 255.255.192.0 (192.168.0.0/18).

Отже маємо один запис сумарного маршруту у таблиці маршрутизації роутерів, що не належать до зони 1, замість чьотирьох. Перевіримо наші підрахунки за допомогою команди, яку виконаємо на ASBR:

show ip route (Рис 3.2).

```
ASBR#show ip route
Codes: 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

Gateway of last resort is not set

     3.0.0.0/24 is subnetted, 3 subnets
D       3.3.1.0 [90/156160] via 10.3.3.1, 00:18:58, FastEthernet3/0
D       3.3.2.0 [90/156160] via 10.3.3.1, 00:18:58, FastEthernet3/0
D       3.3.3.0 [90/156160] via 10.3.3.1, 00:18:58, FastEthernet3/0
     172.16.0.0/25 is subnetted, 1 subnets
O IA    172.16.1.0 [110/2] via 10.2.2.1, 02:57:13, GigabitEthernet5/0
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.4.4.0/24 is directly connected, GigabitEthernet4/0
C       10.3.3.0/30 is directly connected, FastEthernet3/0
C       10.2.2.0/30 is directly connected, GigabitEthernet5/0
C       10.1.1.0/30 is directly connected, GigabitEthernet6/0
O IA 192.168.0.0/18 [110/2] via 10.1.1.1, 03:01:57, GigabitEthernet6/0
ASBR#
```

Рисунок 3.2 – Таблиця маршрутизації роутера ASBR зі зазначенням сумарних маршрутів зон 1 та 2

Зменьшення кількості записів у таблиці маршрутизації – зменьшує кількість інформації, що передається LSA за межами зони.

Цей метод, спрямований на зменьшення розмірів LSA пакетів, раціональний для мереж з великою кількістю зон та пристроїв, в яких можна знехтувати детальною топологією зон другого рівня на роутерах.

3.3 DR та BDR, їх призначення в областях з множинним доступом

Третім пунктом при моделюванні мережі є конфігурація виділеного роутеру (DR) та резервного виділеного роутеру (BDR). У мережі з множинними доступами, доцільно контролювати те, який саме маршрутизатор треба використовувати для обробки LSA, при оновленні в області. У нашому прикладі така мережа представлена як Area1, в якій 4 маршрутизатори з'єднані однією мережею - 192.168.50.0/24 (Рис 3.1).

У випадку зміни топології в цих мережах спільний канал перенавантажується надмірними LSU та LSA пакетами. Виділений роутер забезпечує одну точку, яку використовують, під час оновлення при визначенні найкоротших маршрутів, данний підхід зберігає ресурси інших роутерів в цій зоні.

При виборі DR та BDR враховується одне з трьох значень:

- Пріоритет інтерфейсу
- Ідентифікатор роутеру (Router ID)
- Найбільша IP адреси, на інтерфейсах

Пріоритет інтерфейсу є важливішим параметром при визначені DR ніж інші параметри, тому цей спосіб ми обрали при конфігурації моделі.

Налаштування інтерфейсу, що знаходиться у розділеній мережі, виконується за допомогою команди:

- `ip ospf priority <0-255>`

Число від 0 до 255 визначає пріоритетність маршрутизатора в якості DR, у мережах з множинним доступом. Дуже важливо зберігати

послідовність при першому запуску, оскільки присвоєння статусу DR чи BDR маршрутизаторам може змінитися при перезавантаження інтерфейсів. Для перевірки виконаємо команду «show ip ospf neighor» (рис. 3.3).

```
R3#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.1.1     100   FULL/DR         00:00:38    192.168.50.1    FastEthernet0/1
192.168.2.1      50   FULL/BDR        00:00:39    192.168.50.2    FastEthernet0/1
192.168.50.4      1   2WAY/DROTHER    00:00:30    192.168.50.4    FastEthernet0/1
R3#
```

Рисунок 3.3 – Таблиця OSPF сусідів R3

3.4 Перерозподіл маршрутів в OSPF та EIGRP

Маштабування мережі, може викоикати необхідність сконфігурувати комунікацію між сегментами, що використовують різні протоколи динамічної маршрутизації.

На нашому прикладі, маршрутизатор ASBR використовує OSPF на двох інтерфейсах, та з’єднаний з мережею EIGRP - 10.3.3.0/30. За допомогою двонаправленного перерозподілу маршрутів, можна досягти передачу даних з таблиць маршрутизації. У нашій моделі маршрутизатор ASBR стане ключовим.

За допомогою таких команд, можна настроїти перерозподіл маршрутів з мережі OSPF до мережі EIGRP:

- `router ospf 1`
- `redistribute eigrp 1 subnets`

Для мереж з безкласовою IP-адресацією необхідно обов’язково вказувати опцію subnets. Результати такого налаштування розглянемо на

рисунку 3.4 – маршрути, які раніше були відомі лише в домені EIGRP також поширились динамічно до мережі з OSPF.

Одностороннього перепрозподілу недостатньо. Перевіримо стан зв'язку між ABR1 - source 192.168.50.4 та RE - 3.3.1.1, за допомогою команди ping. Як ми бачимо на рис. 3.5 – з'єднання не встановлено.

```
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
```

Рисунок 3.4 – Таблиця маршрутизації роутера ABR1

```
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)
```

Рисунок 3.5 – Ping RE lo1

Аналогічним чином налаштовуємо перерозподіл маршрутів з мережі OSPF до мережі EIGRP. Зробити це можна за допомогою таких команд на ASBR:

- `router eigrp 1`

- `redistribute ospf 1 metric 1 1 1 1 1`

Як ми бачимо на рис. 3.6 таблиця маршрутизації RE доповнилася данними з мережі OSPF.

Важливо, враховувати, що при додаванні нової мережі до ASBR є вірогідність втратити дані при перерозподілі маршрутів, які під'єднані до ASBR напряму

Розберемо схожу ситуацію з використанням нового інтерфейсу - loopback22, маршрутизатором ASBR, коли цей інтерфейс представляє нове з'єднання до домену OSPF.

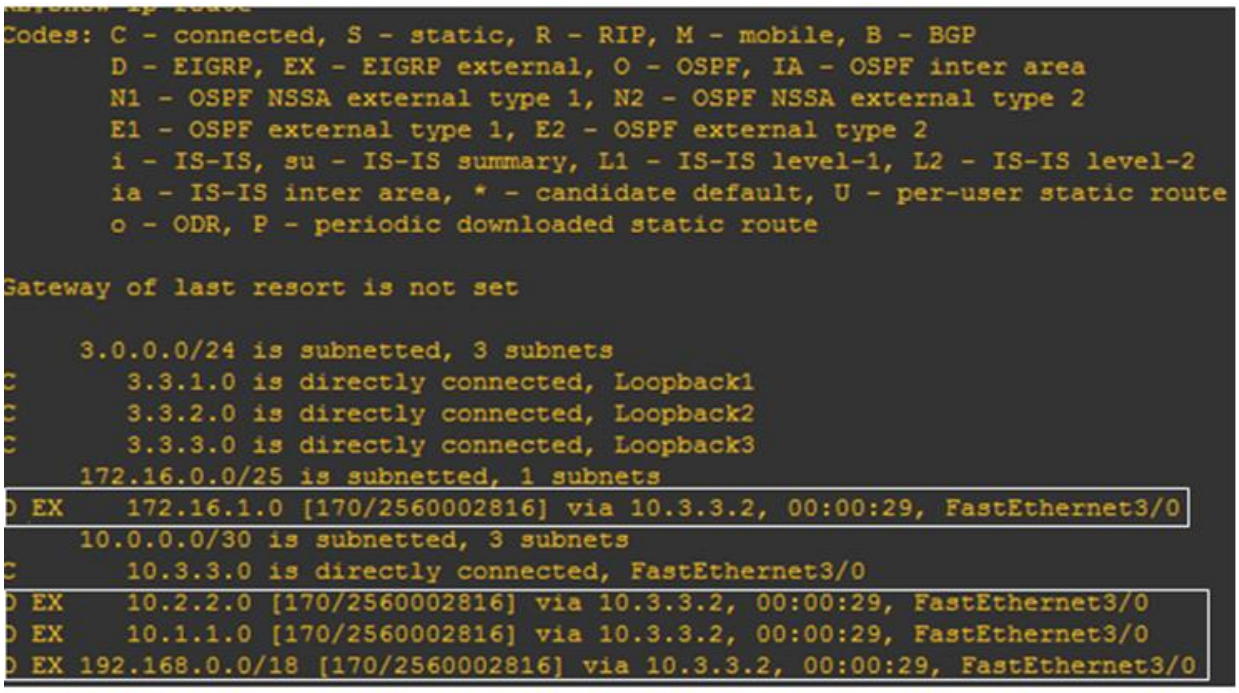


Рисунок 3.6 – Таблиця маршрутизації RE

Перерозподіл нового маршруту буде здійснюватися за допомогою використання route-map:

- `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`

На рис. 3.7 можемо побачити таблицю маршрутизації ABR1, з цих данних ми бачимо, що попередньо отримана про мережу 10.3.3.0/30 - втрачена.

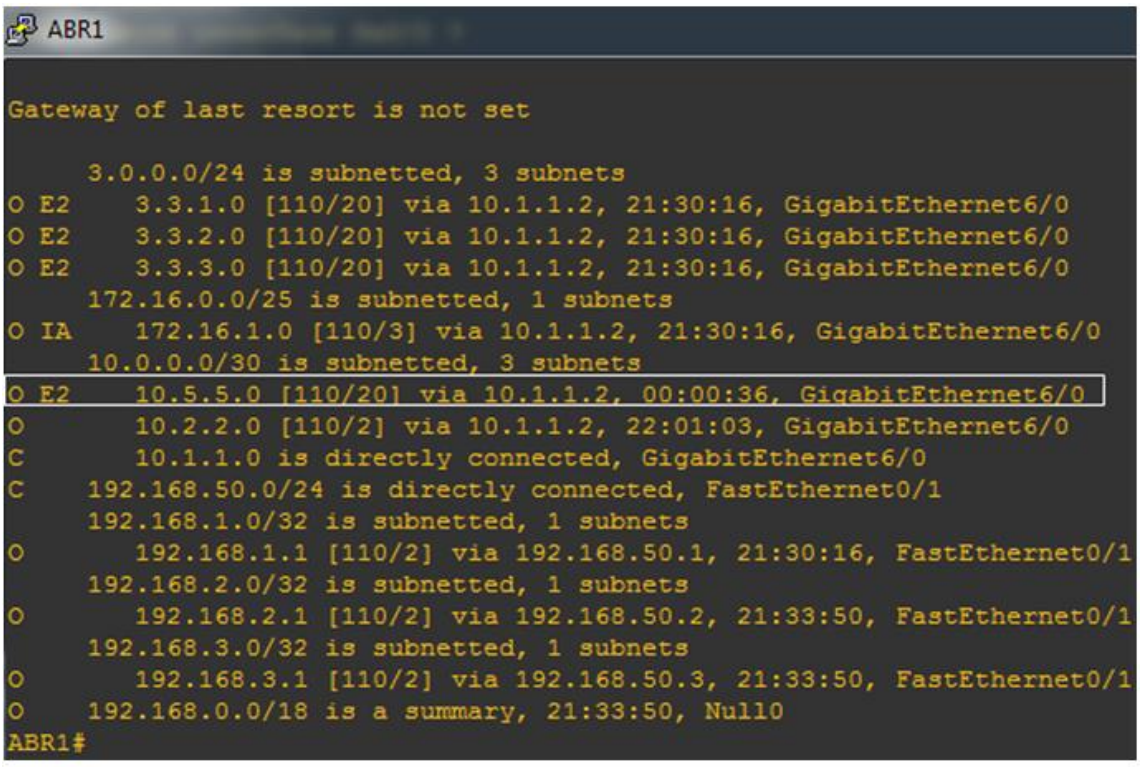


Рисунок 3.7 – Результат перерозподілу додаткової мережі – таблиця маршрутизації ABR1

За допомогою лінкування потрібного інтерфейсу на ASBR (fa0/3) з route-map, ми можемо вирішити проблему з обробкою даних про напряму під’єднані мережі інших доменів:

- `route-map CONN>OSPF`
- `match interface fa3/0`

Знову перевіримо таблицю маршрутизації ABR1 і переконаємося що мережа 10.3.3.0/30 перерозподілилась коректно (рис. 3.8).

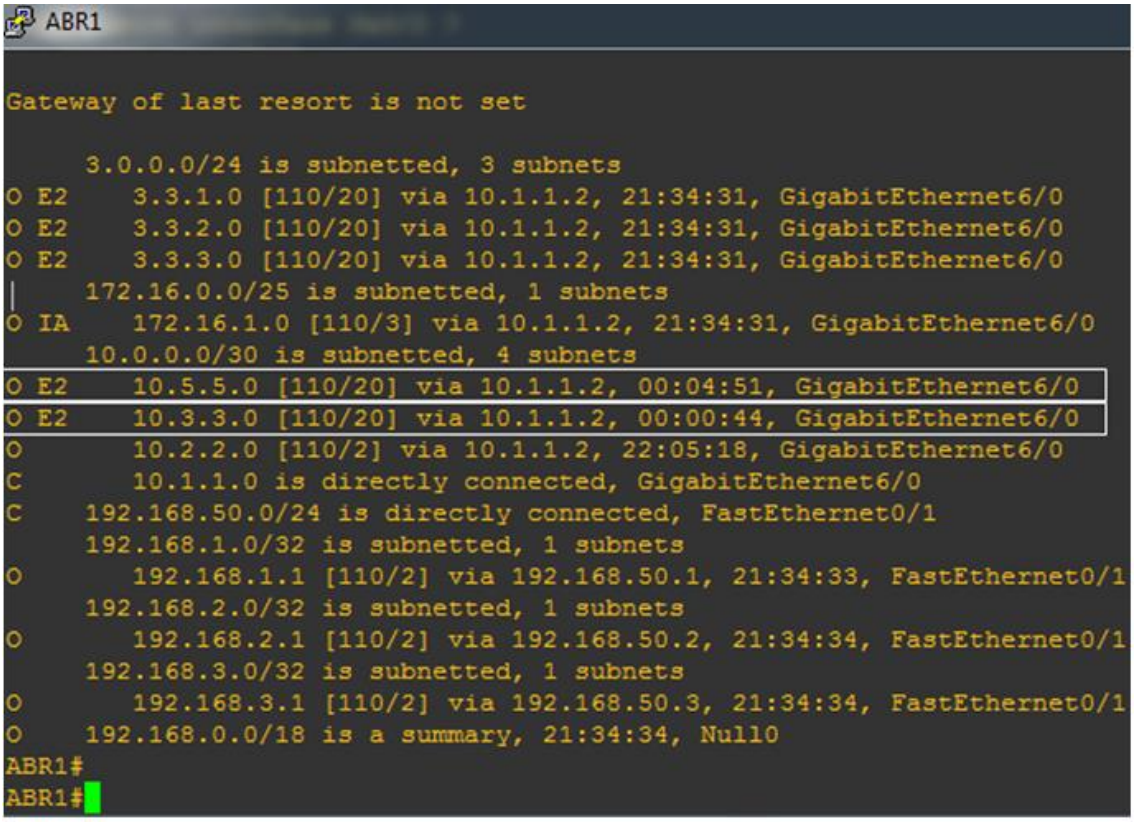


Рисунок 3.8 – Результат перерозподілу – таблиця маршрутизації ABR1

В Додатку А наведено приклади налаштування маршрутизаторів R0, ABR1, ASBR, RE.

4. OSPF ПРОТОКОЛ ТА ЙОГО ДОСЛІДЖЕННЯ ЗА ДОПОМОГОЮ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Однією з основних задач мережевого інженера або адміністратора після планування та реалізації мережевої топології є діагностування несправностей. Повна або часткова автоматизація процесу дозволяє зберегти трудозатрати та забезпечити швидшу реакцію на проблему. Тому з метою виявлення такої критичної ситуації як недоступність каналу зв'язку або мережевого обладнання у автономній системі з підтримкою динамічної маршрутизації у рамках даної роботи створено програмне забезпечення. А саме додаток, що дозволяє дослідити топологію мережі з OSPF за допомогою SNMP запитів до мережевих пристроїв.

Програма забезпечує наступні опції:

1. можливість моніторингу стану мережі у режимі реального часу віддалено без повного переліку IP адрес пристроїв;
2. локалізацію наслідків невірної конфігурації OSPF, відмови окремого інтерфейсу або обладнання вцілому.

Як результат даний додаток може використовуватися як у навчальних цілях при вивченні технологій динамічної маршрутизації так і в реальних системах адміністраторами.

Додаток реалізовано мовою програмування Python версії 2.7 з використанням стандартних та спеціалізованих програмних модулів.

Кореневий функціонал програми працює на основі технологій протоколу SNMP (Simple Network Management Protocol), який є стандартним Інтеренет-протоколом для управління пристроями у IP-мережах на базі архітектур TCP/UDP. До пристроїв, що підтримують SNMP належать

маршрутизатори, комутатори, сервери, робочі станції, принтери, модемні стійки та інші.

SNMP дозволяє станції управління звертатися до мережі як до розподіленої бази даних про стан, конфігурацію, та багато іншого. Протокол стандартизовано IETF, дані, що отримуються та оброблюються також стандартизовані у MIB (Management Information Base) [10].

Стандартні операції SNMP наведено у таблиці 4.1.

Таблиця 4.1 Функції протоколу SNMP

Назва	Призначення
GET	Отримання даних від мережевої ноди
GETNEXT	Отримання даних про наступний елемент після мережевої ноди
SET	Надсилання конфігурацій або команд контролю до мережевої ноди
TRAP	Забезпечення нотифікацій від мережевої ноди до станції управління
INFORM	Забезпечення асинхронних нотифікації від станції управління та у зворотному напрямку

4.1 Алгоритм програмного забезпечення

Розглянемо алгоритм програмного забезпечення. На рисунку 4.1 відображено етапи роботи додатку у вигляді

Необхідно розглянути головні імпортовані пакети необхідні для роботи нашої програми [11].

Завдяки класу CommandGenerator([snmpEngine]) та модулю pysnmp ми можемо використовувати функціонал протоколу SNMP.

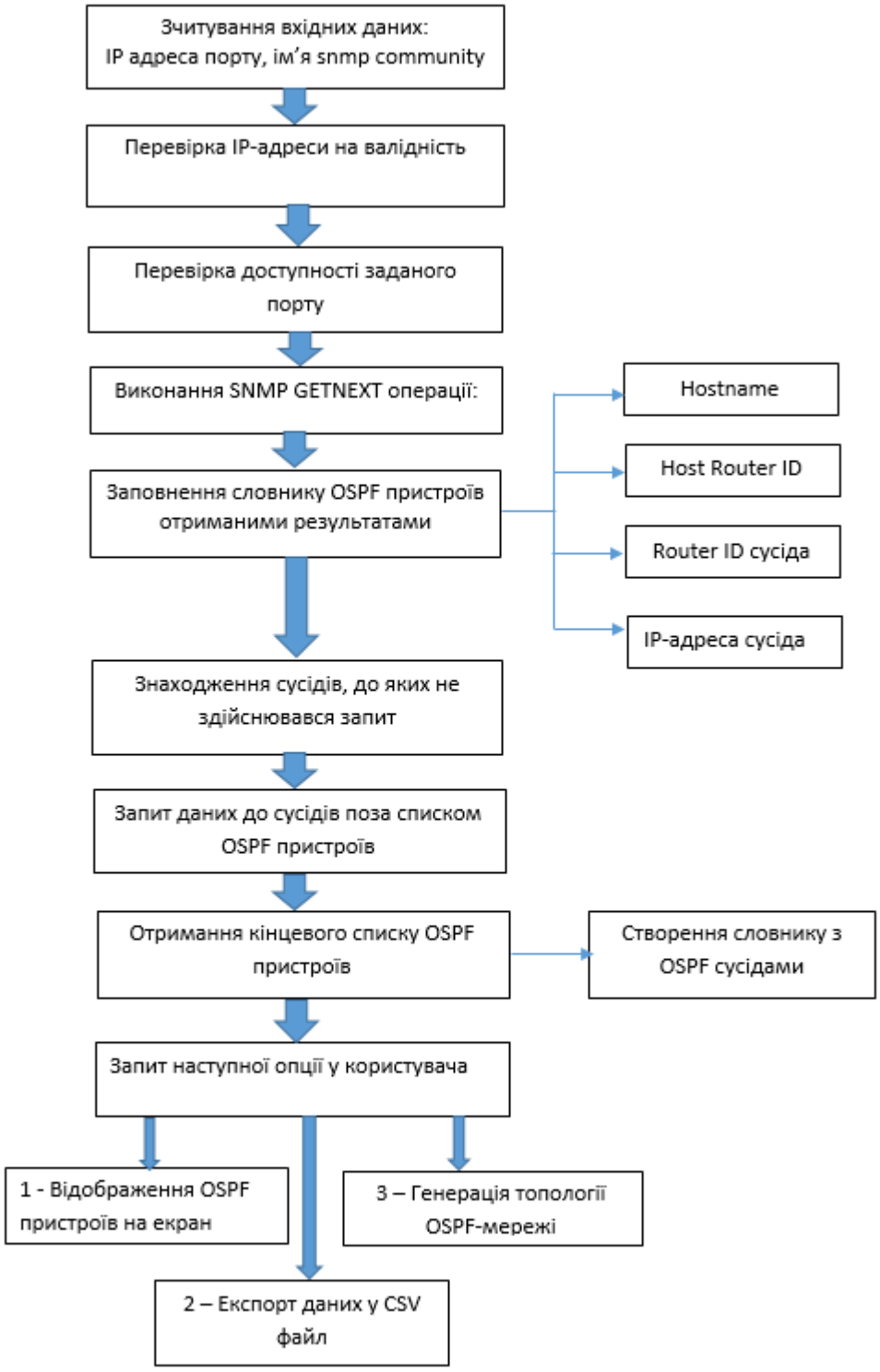


Рисунок 4.1 – Етапи роботи програми дослідження OSPF топології

Для отримання інформації щодо доступності вказанної адреси ми імпортували функцію call() та модуль subprocess.

Для того щоб результат був зрозумілим та читабельним, ми можемо конвертувати значення у десятковий формат які ми отримали за допомогою SNMP з OID, використовуємо binascii модуль.

Для доступу до змінних, функцій, які співпрацюю з python інтерпритатором, використовуємо sys модуль.

За допомогою бібліотеки matplotlib ми можемо створити якісні малюнки в різних форматах. Це по суті модуль-пакет. В рамках цієї роботи використаємо matplotlib.pyplot інтерфейс. Що включає в себе набір функцій та команд, для синтаксису графчних команд matplotlib.

Для створення та конфігурації, аналізу функціонування комп'.терної мережі імпортуємо networkx модуль. Пакет використовується для генерації графу мережі.

Опис перемінних та функцій, що використовуються для забезпечення основного функціоналу, розглянимо у таблицях 4.2 та 4.3 відповідно.

Таблиця 4.2 Основні перемінні програми

Назва	Призначення
ip	IP-адреса, що задана користувачем при запуску програми у вигляді символьного рядку
comm	Ідентифікатор SNMP community, що налаштовано на маршрутизаторах автономної системи

Продовження таблиці 4.3

Назва	Призначення
ping_reply	Цілочисельна змінна, що ідентифікує значення відповіді на запит ping
ospf	Список словників з даними про сусідів та хост
nbridlist	Список router id сусідів
nbriplist	Список IP-адрес сусідів
ospf_devices	Словник даних зі значеннями для Host, HostID, NbrRtrId, NbrRtrIp
ospf_host	Ім'я хосту
ospf_host_id	Router ID хосту
all_host_ids	Список усіх ідентифікаторів хостів
all_nbr_ids	Список усіх ідентифікаторів сусідів
all_outsiders	Список сусідів які на даний момент не зазначені як хост у списку хостів

Таблиця 4.3 Характеристика основних функцій програми дослідження топології OSPF мережі

Назва функції	Призначення	Користувацька/ Пакетна
ip_is_valid()	Слугує для перевірки введеної користувачем IP-адреси	Користувацька
split('delimiter')	Призначена для розділення символьного рядку за зазначеним роздільником.	Стандартна вбудована ф-я python

Продовження таблиці 4.2

Назва функції	Призначення	Користувацька/ Пакетна
call(args, *, stdin=None, stdout=None, stderr=None, shell=False, timeout=None)	Виконує мережеву команду, що описана у аргументі. Очікує завершення команди та повертає код повернення. У поточній програмі використана для відправки запиту ping за вказаною IP-адресою.	subprocess
snmp_get(ip)	Функція, що оперує змінними для отримання даних безпосередньо від пристрою за допомогою запиту SNMP.	Користувацька
cmdgen.CommandGenerator()	Виклик конструктура класу генерації команд	pysnmp
cmdGen.nextCmd()	Виконання SNMP GETNEXT операції для вказаних OSPF OID. Функція повертає кортеж значень errorIndication, errorStatus, errorIndex, varBindTable Як аргументи використані дані про snmp community, UDP порт та OID даних з таблиці сусідів.	pysnmp
add_edges_from()	Функція класу Graph, що ініціалізує ребра графа	networkx

Продовження таблиці 4.2

Назва функції	Призначення	Користувацька/ Пакетна
hexlify(string)	Функція конвертації рядку у бінарному форматі до шістнадцяткового з метою подальшого переведення у десятковий формат. Оперує даними, що отримані у результаті snmp запиту	binascii
find_unqueried_neighbors()	Функція для визначення маршрутизаторів зі списку сусідів від яких ще не було отримано дані за допомогою snmp getnext	Користувацька
nx.Graph()	Ініціалізація об'єкту класу Graph	networkx
spring_layout ()	Позиціонує ноди графу	networkx
nx.draw()	Функція для створення рисунку графу мережі	networkx

У Додатку Б повний лістинг програмного коду.

4.2 Використання програмного забезпечення та його тестування на моделі

В рамках виконання роботи було змодельовано мережу у GNS середовищі, для перевірки функціонування додатку. На рисунку 4.2 наведена топологія змодельованої мережі.

Динамічна OSPF маржрутизація була налаштована на кожній ноді. Всі роутери розміщені в одній зоні - area id 50.

Виконаємо запуск додатку на Linux Debian 7, що встановлена на віртуальній машині.

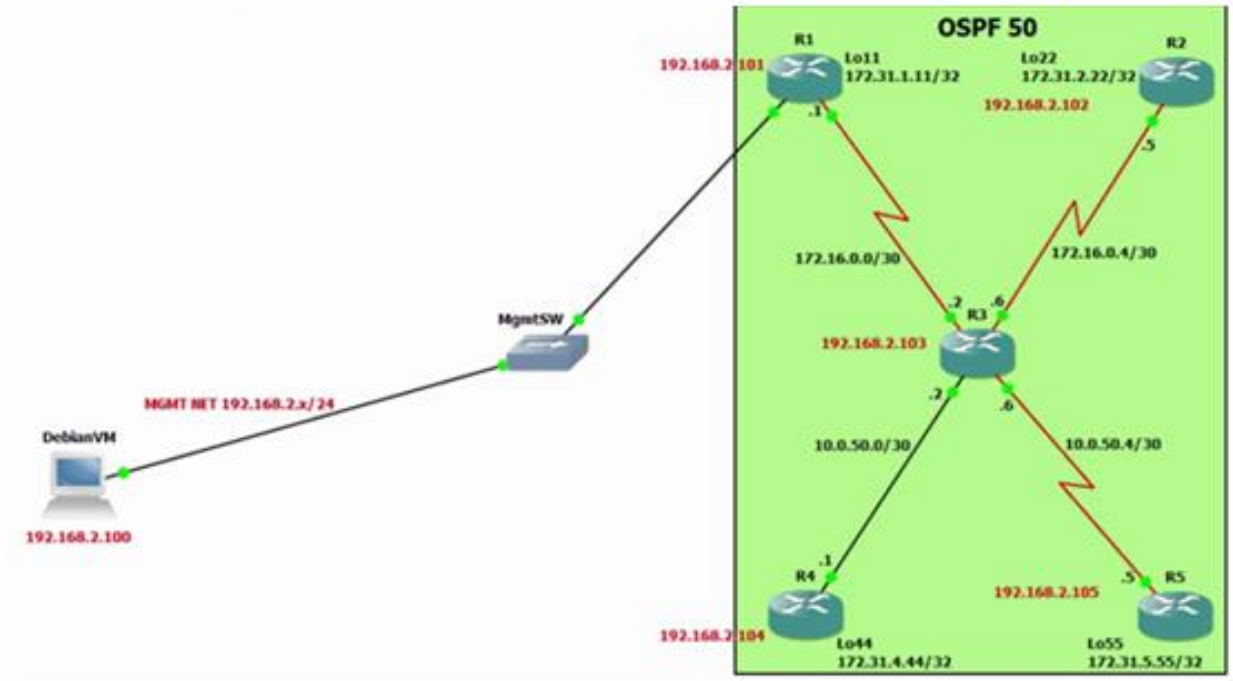


Рисунок 4.2 – Топологія тестової мережі

Для запуску додатку на кожному маршрутизаторі налаштуємо автономну систему snmp community string, це забезпечить автентифікацю при звернені до пристроїі за допомогою SNMP.

- `snmp-server community public RO`

в нашому випадку public – рандомний ідентифікатор/пароль.

На рис. 4.3 выдображено інтерфейс додатку, консольний інтерфейс було обрано задля економії ресурсів на віртуальній машині.

При виборі опції 3 додаток побудує граф нашої мережі з зазначеними IP адресами интерфейсів (відображаються на ребрах) та Router ID що є назвою нод. На рис.4.4 ми можемо побачити приклад відображення графу в додатку для змодельованної топології.

Завдяки модулю matplotlib ми можемо зберегти файли у різноманітних форматах.

Рисунок 4.3 – Запит опції представлення даних

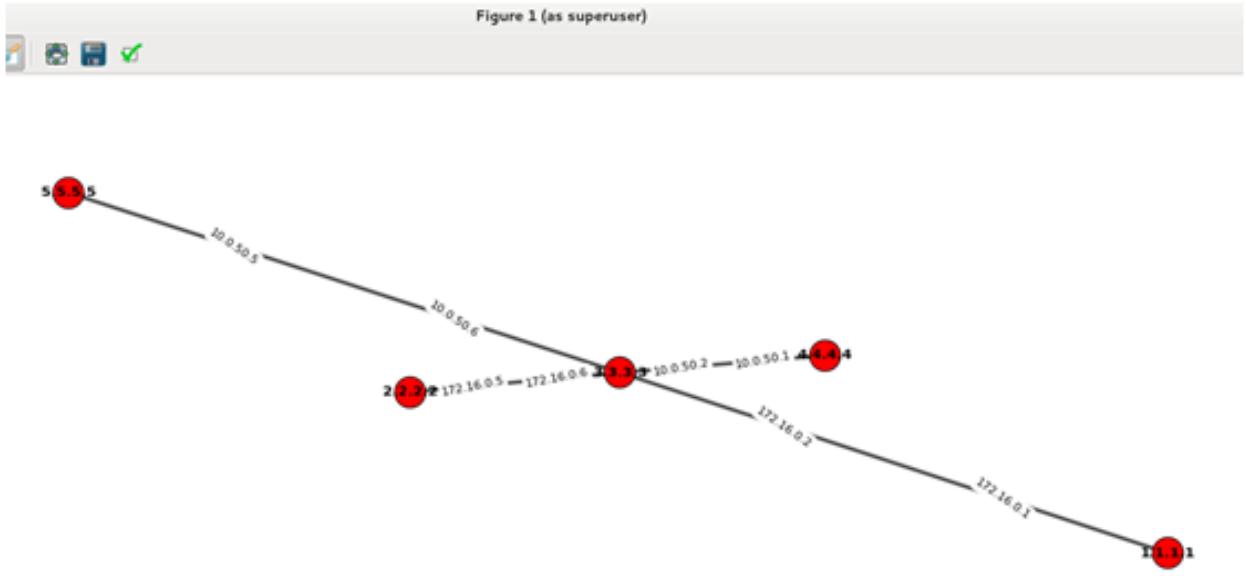


Рисунок 4.4 – Граф тестової мережі

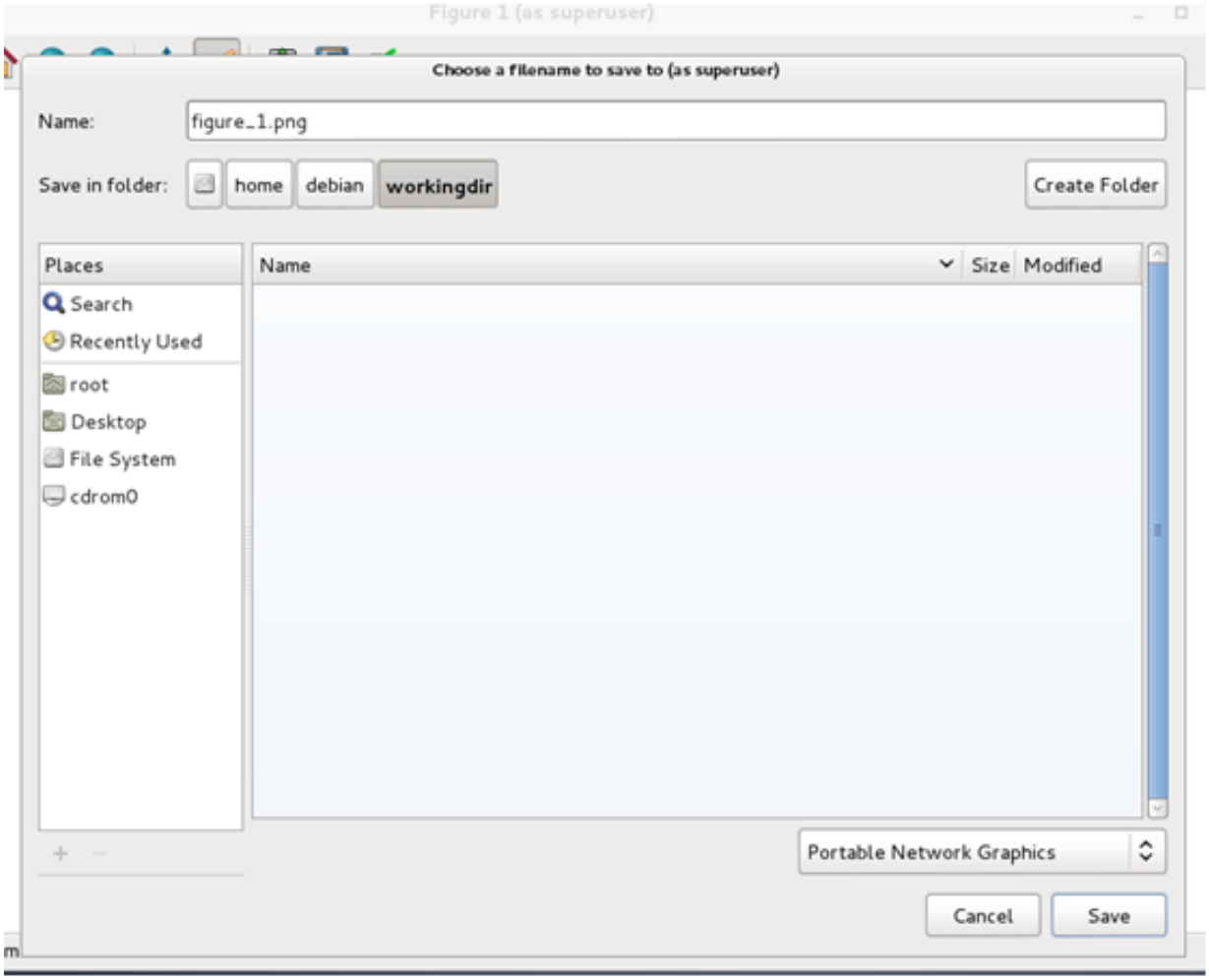


Рисунок 4.5 – Діалогове вікно збереження зображення

Щоб продемонструвати роботу додатку, земулюємо ситуацію з втратою зв’язку між нодами в досліджуванній мережі, для цього відключимо один з інтерфейсів, наприклад - se0/0 на маршрутизаторі - R5. Здійснимо повторний запуск для перерахунку даних. Як бачимо на рис.4.6. ми отрималємо нову топологію.

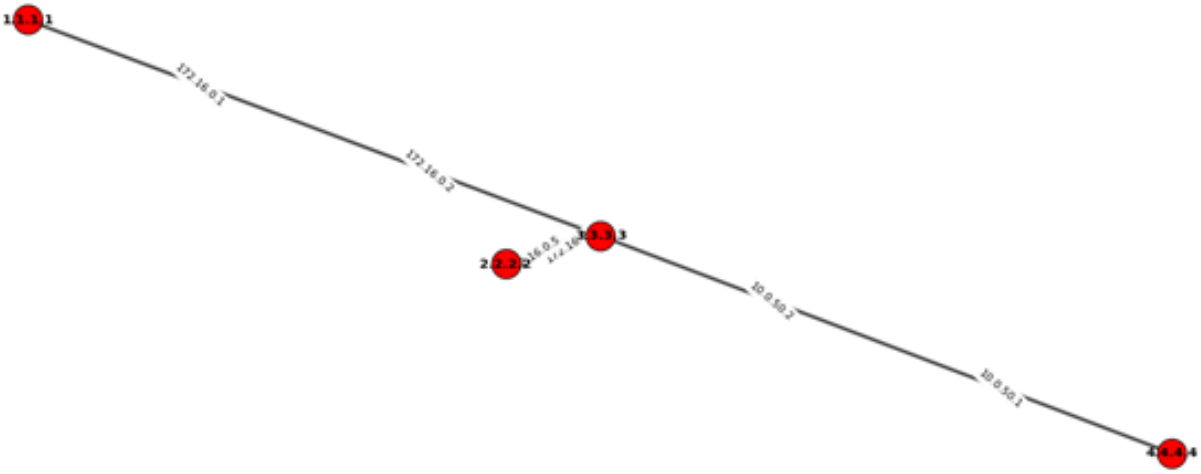


Рисунок 4.6 - Граф з урахуванням відсутності даних про R5

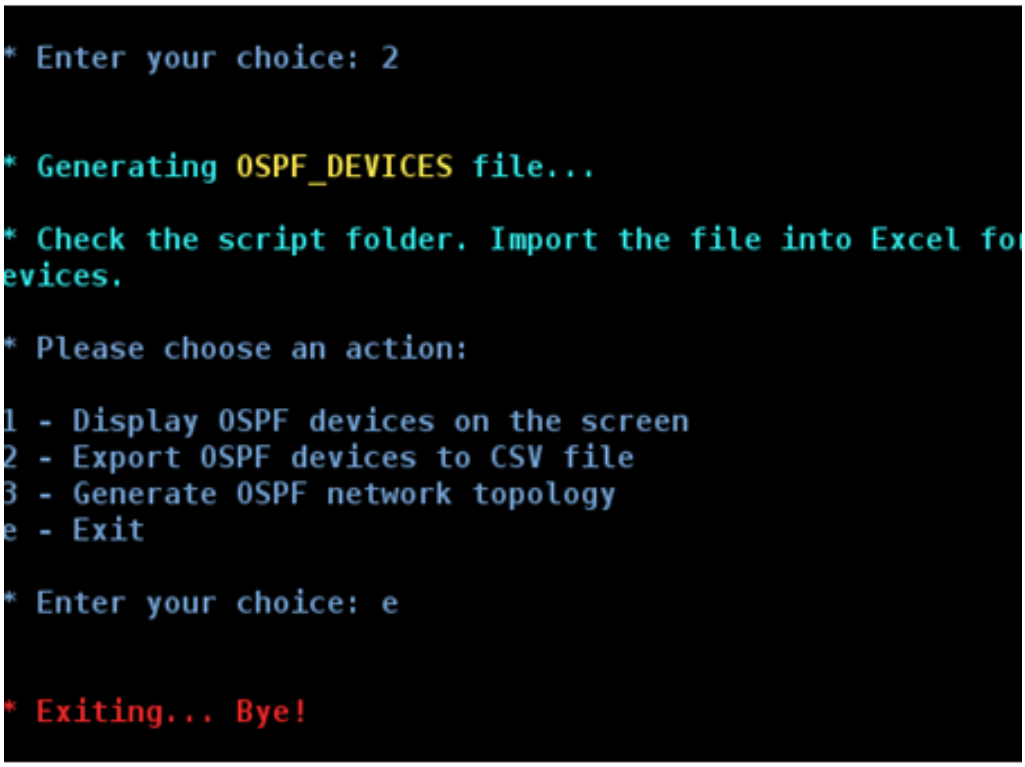


Рисунок 4.7 – Діалогове вікно виходу з програми

За допомогою додатку ми також можемо данні у CSV форматі, це дозволяє провести подальший аналіз у Microsoft Excel. CSV файл включатиме в себе інформацією про Hostname, Host Router ID, Neighbors Router ID, Neighbors Router IP.

ВИСНОВКИ

У рамках данної магістерської ми дослідили OSPF та EIGRP протоколи динамічної маршрутизації. Визначили якісні характеристики протоколів та їх відмінності, за допомогою моделювання мережі в додатку OPNET Modeler. EIGRP протокол проявив себе доволі ефекти і показав дуже швидкий час збіжності, але через його пропрієтарність, його можна використовувати в мережах виключно на Cisco обладнанні, в таких мережах гарантована доставка пакету з мінімізацією втрат при відмовах.

В той час як OSPF можливо використовувати в мережах які постійно маштабуються, що ставить його на першу позицію для мультивендрних великих корпоративних мереж.

Ми побудували корпоративну мережу, для підвищення ефективності роботи мережі з OSPF протоколом. Було запропоновано низка рекомендацій для скорочення об’ємів трафіку, задля збереження пропускної здатності каналів для користувачів.

Було розроблено програмне забезпечення, для моніторингу на підтримки цілісності топології мережі у разі відмови каналів зв’язку або обладнання.

Данні результати корисні для адміністраторів мережі, в проектуванні та конфігурації, та вивченні технології протоколів.

СПИСОК ЛІТЕРАТУРИ

1. Бачинский В.А., Гіоргізова-Гай В.Ш., Вибір протоколу динамічної маршрутизації в корпоративній IP-мережі // Системні дослідження та інформаційні технології, №1, 2015 – 100с.
2. Don Xu and Ljiljana Trajković, Performance Analysis of RIP, EIGRP, and OSPF using OPNET // Simon Fraser University, Canada, 2015
3. Enhanced Interior Gateway Routing Protocol // Cisco [електронний ресурс] - http://docwiki.cisco.com/wiki/Enhanced_Interior_Gateway_Routing_Protocol
4. Керівництво з управління OSPF, Cisco [електронний ресурс] - www.cisco.com/c/ru_ru/support/docs/ip/open-shortest-path-first-ospf/7039-1.pdf
5. Овсяннікова М.І., Замятіна О.М., Методичні рекомендації з використання програмного продукту OPNET для моделювання комп'ютерних мереж // збірник статей Молодіжний науковий форум: Технічні та математичні науки. №4, 2015 - 56с.
6. 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
7. Антонова О.А., Оцінка ефективності протоколів динамічної маршрутизації при передачі потокового відео // Автоматизація і управління у техничних системах, №4.2, 2015
8. Макаренко С.І., Час збіжності протоколів маршрутизації при відмові в мережі // Системи управління, зв'язку і безпеки №2, 2015 – 49 с.
9. Navita Komal, Rajan Vohra, Ravinder Singh Sawhney, Behavioral Analysis of Dymanic Routing Protocols under Incrementing Workstations // Int. J. on Recent Trends in Engineering and Technology, Vol. 11, No. 1, July 2015 – 1p.
10. Євстропов Д. Е., Добржінскій Ю. В., SNMP - Протокол управління і спостереження ЛОС // Вологдинське читання №73, 2015 – 69с.
11. Documentation Python Tutorials – Modules // Python [електронний ресурс] - https://docs.python.org/2/tutorial/modules.html

12. 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.

13. І. М. Єхриєль, Р. Д. Рерле, Тестування і аналіз телекомунікаційних протоколів // ФГУП ЛОНИИС, 2002

14. Поповский В. В., Волотка В. С. Методи аналізу динамічної структури телекомунікацийних систем // Північно-Європейский журнал передових технологій. № 5/2 (65), 2016 – 18-22с.

15. Протокол EIGRP (удосконалений внутрішній протокол маршрутизації шлюзів) // Cisco Systems, Inc., 2015 [електронний ресурс] - http://www.cisco.com/cisco/web/support/RU/9/92/92088_eigrp-toc.html

16. Тарасов В.Н., Коннов А.Л., Ушаков Ю.А., Аналіз і оптимізація локальних мереж і мереж зв’язку за допомогою програмної системі OPNET Moduler. // Вісник ОГУ№6/Червень, 2016. – 197 с.

17. Фадеев А.Н., Аналітичний огляд пакетів імітаційного моделювання // Матеріали Міжнародної науково-техничної конференції, МИРЕА, Москва, 2017 – 24-26с.

ДОДАТКИ

ДОДАТОК А

- Конфігурація ASBR:
  - hostname ASBR
  - interface Loopback22
  - ip address 10.5.5.1 255.255.255.252
  - interface FastEthernet3/0
  - ip address 10.3.3.2 255.255.255.252
  - interface GigabitEthernet4/0
  - ip address 10.4.4.2 255.255.255.0
  - interface GigabitEthernet5/0
  - ip address 10.2.2.2 255.255.255.252
  - interface GigabitEthernet6/0
  - ip address 10.1.1.2 255.255.255.252
  - router eigrp 1
  - redistribute ospf 1 metric 1 1 1 1 1
  - network 10.3.3.0 0.0.0.3
  - no auto-summary
  - router ospf 1
  - log-adjacency-changes
  - redistribute connected subnets route-map CONN>OSPF
  - redistribute eigrp 1 subnets
  - network 10.1.1.0 0.0.0.3 area 0
  - network 10.2.2.0 0.0.0.3 area 0
  - route-map CONN>OSPF permit 10
  - match interface Loopback22 FastEthernet3/0
- Конфігурація ABR1:
  - hostname ABR1
  - 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

ДОДАТОК Б

net_state.txt