Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

другий (магістерський)
(освітньо-кваліфікаційний рівень)

Розробка та дослідження методу відмовостійкої маршрутизації у IP-мережі з проактивним захистом шлюзу за замовчуванням
(тема)

Виконала:
студентка 2 курсу, групи ІКІм-21-1
Круглова А.О.
(прізвище, ініціали)
Спеціальність: 172 Телекомунікації та радіотехніка
(код і повна назва спеціальності)
Тип програми: освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма: Інфокомунікаційна інженерія
(повна назва освітньої програми)
Керівник: зав. кафедри ІКІ імені В.В. Поповського
Лемешко О.В.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2022р.

Атестаційна робота не містить відомостей заборонених до відкритого опублікування.

Студентка	_____	*Круглова А.О.*
	(підпис)	*(прізвище, ініціали)*
Керівник роботи	_____	*Лемешко О.В.*
	(підпис)	*(прізвище, ініціали)*

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 172 Телекомунікації і радіотехніка
(код і повна назва)
Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма Інфокомунікаційна інженерія

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)
«____» ___2022р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентці Кругловій Анастасії Олексіївні .
(прізвище, ім'я, по-батькові)

1. Тема роботи: Розробка та дослідження методу відмовостійкої маршрутизації у IP-мережі з проактивним захистом шлюзу за замовчуванням затверджена наказом по університету від «24» жовтня 2022р. №1389Ст
2. Термін подання студентом роботи до екзаменаційної комісії 15.12.2022р.
3.Вихідні дані до роботи: математичної моделі щодо реалізації маршрутизації з підтримкою балансування навантаження.
4. Перелік питань, що потрібно опрацювати в роботі:
1) Аналіз відомих технологічних та теоретичних рішень щодо проблеми балансування навантаження в інфокомунікаційних мережах.
2) Моделювання процесів балансування навантаження в середовищі Matlab.
3) Дослідження процесів балансування навантаження в інфокомунікаційній мережі.
4) Лабораторний експеримент.

5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій:

Демонстраційний матеріал у вигляді ppt-презентації: функціональна модель балансування навантаження в ІКМ; реалізація запропонованої математичної моделі в середовищі Matlab; результати дослідження; схема лабораторного експерименту.

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по-батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	Завідувач кафедри Лемешко Олександр Віталійович		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	01.09.2022	Виконано
2	Збір матеріалів для дослідження	05.10.2022	Виконано
3	Розробка 1 розділу	30.10.2022	Виконано
4	Розробка 2 розділу	10.11.2022	Виконано
5	Розробка 3 розділу	25.11.2022	Виконано
6	Розробка 4 розділу	05.12.2022	Виконано
7	Оформлення пояснювальної записки	15.12.2022	Виконано
8	Оформлення слайдів та презентації	15.12.2022	Виконано

Дата видачі завдання 01 вересня 2022 року .

Студентка _____ Круглова А.О.
(підпис) (прізвище, ініціали)

Керівник роботи _____ зав.каф Лемешко О.В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 80 сторінки; 57 рисунків; 7 таблиці; 48 посилання.

ВІДМОВОСТІЙКА МАРШРУТИЗАЦІЯ, ЯКІСТЬ ОБСЛУГОВУВАННЯ, ЗАХИСТ ШЛЮЗУ ЗА ЗАМОВЧУВАННЯМ, ІНФОКОМУНІКАЦІЙНА МЕРЕЖА.

Об’єкт дослідження – процес балансування навантаження із проактивним захистом шлюзу за замовчуванням в інфокомунікаційній мережі (ІКМ).

Предмет дослідження – математична модель балансування навантаження із проактивним захистом шлюзу за замовчуванням в інфокомунікаційній мережі, що відповідає принципам концепції Traffic Engineering (TE).

Мета роботи – покращення рівня якості обслуговування в інфокомунікаційній мережі засобами відмовостійкої маршрутизації.

Методи дослідження – формалізація та порівняння, математичне програмування, практичний експеримент.

У магістерській кваліфікаційній роботі було вдосконалено та досліджено математичну модель балансування навантаження з проактивним захистом шлюзу за замовчуванням в інфокомунікаційній мережі. В основі цієї моделі лежать умови реалізації одно або багатошляхової маршрутизації; балансування навантаження на рівні доступу; захист шлюзу за замовчуванням; збереження потоку на рівні доступу та самої мережі; запобігання перевантаження каналів зв’язку. Окрім того, обов’язковою вимогою до цих моделей та методів було забезпечення врахування рівня надійності приграничних маршрутизаторів, між якими балансується навантаження, що надходить від мережі доступу. Також, було порівняно та проаналізовано запропоновані моделі. Встановлено, що врахування показників надійності приграничних маршрутизаторів при балансуванні навантаження між ними, за допомогою рішень RATE або ResMetrTE дозволило підвищити поріг завантаженості каналів зв’язку мережі – у середньому від 15% до 27%

В процесі проведення практичного експерименту були сформульовані рекомендації з вдосконалення протоколу GLBP на основі запропонованої моделі.

ABSTRACT

Explanatory note: 80 pages; 57 drawing; 7 tables; 48 links.

FAILURE-RESISTANT ROUTING, QUALITY OF SERVICE, DEFAULT GATEWAY PROTECTION, INFOCOMMUNICATION NETWORK.

The object of research – the process of load balancing with default gateway protection in an infocommunication network.

The subject of research – a mathematical model of load balancing with default gateway protection in an information communication network, which corresponds to the principles of the Traffic Engineering (TE) concept.

The purpose of the work is to improve the level of service quality in the information communication network by means of fault-tolerant routing.

Research methods – formalization and comparison, mathematical programming, practical experiment.

In the master's qualification work, an improved mathematical model of load balancing with proactive protection of the default gateway in the information communication network was created and investigated. This model is based on the conditions for the implementation of single or multipath routing; load balancing at the access level; default gateway protection; flow preservation at the access level and the network itself; prevention of overloading of communication channels, which represent load balancing conditions in infocommunication network. In addition, a mandatory requirement for these models and methods is to ensure that the level of reliability of border routers, between which the load coming from the access network is balanced, is taken into account. Also, the proposed models were compared and analyzed. It was established that taking into account the reliability indicators of border routers when balancing the load between them, using RATE or ResMetrTE solutions, made it possible to increase the threshold of network communication channel load - on average from 15% to 27%

During the practical experiment, recommendations for improving the GLBP protocol were formulated based on the proposed model.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦ І ТЕРМІНІВ

ІКМ – інфокомунікаційна мережа;

ОС – операційна система;

ПЗ – програмне забезпечення;

ACL – Access Control List, лист контролю доступу

ARP – address resolution protocol, протокол визначення адрес;

AVF – active virtual forwarder, активний віртуальний пересилач;

AVG – active virtual gateway, активний віртуальний шлюз;

CARP – common address redundancy protocol, протокол дуплікації загальної адреси;

CSPF – Constrained Shortest Path First, найкоротший шлях з обмеженнями;

FHRP – first hop redundancy protocol, протокол резервування першого переходу;

GLBP – gateway load balancing protocol, протокол балансування навантаженням шлюзу за замовчуванням;

GNS3 – Graphical Network Simulator-3, емулятор програмного забезпечення мережі;

HSRP – hot standby router protocol, протокол резервування для забезпечення відмовостійкості шлюзу за замовчуванням;

IANA – Internet assigned numbers authority, адміністрація адресного простору Інтернет;

ICMP – Internet Control Message Protocol, протокол міжмережевих керуючих повідомлень;

IGRP – Interior Gateway Routing Protocol, протокол маршрутизації внутрішнього шлюзу;

IP – Internet protocol, протокол міжмережної взаємодії;

MAC – media access control, управління доступом до середовища;

NAT – network address translation, перетворення мережевих адрес;

OSPF – Open Shortest Path First, відкритий протокол маршрутизації за найкоротшим шляхом;

PC – personal computer, персональний комп'ютер;

QoS – Quality of Service, якість обслуговування;

RATE – Resilience Aware TE, інжиніринг трафіку з урахуванням стійкості;

ResMetrTE – Resilience Metrics TE, показники стійкості;

RIP – Routing Information Protocol, інформаційний протокол маршрутизації;

TCP – transmission control protocol, протокол керування передачею;

TE – Traffic Engineering, інжиніринг трафіку;

UDP – user datagram protocol, протокол датаграм користувача;

VRID – virtual Router Identifier, ідентифікатор віртуального маршрутизатора;

VRRP – virtual router redundancy protocol, протокол резервування віртуальних маршрутизаторів.

ВСТУП

Технології зв'язку, що швидко розвиваються, призводять до збільшення попиту на додатки та високошвидкісні мережі. Таким чином, від постачальників послуг очікується, що вони зможуть проектувати та розробляти ефективні рішення для підтримки вимог кінцевих користувачів [1]. Наявність належного рівня якості наданих послуг дуже потрібна в даний час епохи інформаційних технологій. Сучасним організаціям та компаніям потрібна мережа для захисту роботи бізнесу від пошкодження системи, втрати даних чи відмов.

При побудові мережної інфраструктури одним із найбільш важливим фактором є те, як мережа може впоратися із відмовами. Багато інтернет-провайдерів не можуть гарантувати 100% стабільне підключення до Інтернету. Тому, для того щоб мати можливість підтримувати інтернет-мережу стабільною і запобігати або знижувати ризик повної відмови, як правило, інтернет-провайдери мають два або більше підключень. Якщо основна мережа або первинне підключення перервано або відключено, одне з них використовується як вторинне або резервне підключення [2]. З цієї причини необхідно мати два або більше шлюзів, з'єднаних у мережу, тому що якщо один з шлюзів відмовить, інші шлюзи негайно замінять непрацюючі.

А для підтримки рівня якості мережевих послуг та зведення до мінімуму збоїв в мережі, необхідно впровадити систему протоколу резервування, також відому як FHRP (First Hop Redundancy Protocol, протокол резервування першого переходу) [3]. Багато сучасних пристроїв Cisco повністю підтримують протоколи резервування першого переходу. На ринку представлено кілька таких протоколів, і у даній роботі буде розглянуто протокол Cisco Hot Standby Router Protocol (HSRP), протокол надмірності віртуального маршрутизатора (VRRP) та протокол балансування навантаження шлюзу (GLBP).

Одним з суттєвих недоліків існуючих протоколів є відсутність автоматизації, тобто налаштування балансування навантаження в мережі повинно проводитися адміністратором мережі, а отже, якість обслуговування напряму залежить від досвіду та навичок адміністратора. Через це, в даній кваліфікаційній роботі пропонується вдосконалена модель балансування навантаження із проактивним захистом шлюзу за замовчуванням в інфокомунікаційній мережі.

1 АНАЛІЗ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКОСТІ IP-МЕРЕЖ

1.1 Визначення місця та ролі протоколів FHRP у забезпеченні відмовостійкості IP-мереж

Існує проблема відмови маршрутизатора, що є шлюзом за замовчуванням. У разі збою маршрутизатора або інтерфейсу маршрутизатора (який служить шлюзом за замовчуванням) вузли, налаштовані за допомогою цього шлюзу, ізолюються від зовнішніх мереж. У комутованої мережі кожен клієнт отримує тільки один шлюз за замовчуванням. Неможливо використовувати другий шлюз, навіть якщо існує другий шлях для передачі пакетів з локального сегмента. Жоден з хостів не зможе відправляти повідомлення за межі локальної мережі. Буде потрібно якийсь час, щоб цей шлюз знову запрацював.

Потрібен механізм для забезпечення альтернативних шлюзів за замовчуванням в комутованих мережах, де два або більше маршрутизатора підключені до одних і тих же віртуальних локальних комп'ютерних мереж. Цей механізм забезпечується протоколами резервування першого переходу –FHRPs.

Топологія фізичної мережі на рисунку 1.1 показує два комутатора, маршрутизатори, ПК (персональний комп'ютер) і сервер. Маршрутизатор R1 відповідає за маршрутизацію пакетів від ПК1. Якщо R1 стає недоступним, протоколи маршрутизації можуть динамічно сходитися. R2 тепер направляє пакети із зовнішніх мереж, які пройшли б через R1. Однак трафік з внутрішньої мережі, пов'язаної з R1, включаючи трафік з робочих станцій, серверів і принтерів, налаштованих з R1 в якості шлюзу, як і раніше відправляється на R1 і відкидається.

Кінцеві пристрої зазвичай настроюються з одною IPv4-адресою для шлюзу. Ця електронна адреса не змінюється при зміні топології мережі. Якщо цей IPv4-адрес шлюзу за замовчуванням не може бути досягнутий, локальний пристрій не може відправляти пакети з сегмента локальної мережі і відключається від інших мереж. Навіть якщо існує резервний маршрутизатор, який може служити шлюзом за замовчуванням для цього сегмента, не існує динамічного методу, за допомогою якого ці пристрої можуть визначати адресу нового шлюзу.

У протоколі FHRP як шлюз для робочих станцій в певному сегменті налаштований IPv4-адрес віртуального маршрутизатора. Коли пакети

відправляються з хост-пристроїв на шлюз за замовчуванням, хости використовують ARP (Address Resolution Protocol – протокол визначення адрес) для визначення MAC-адреси, пов'язаного з IPv4-адресою шлюзу. ARP повертає MAC-адресу віртуального маршрутизатора. Пакети, відправлені MAC-адресу віртуального маршрутизатора, можуть потім фізично оброблятися активним в даний момент маршрутизатором в групі віртуальних маршрутизаторів (рисунок 1.2).

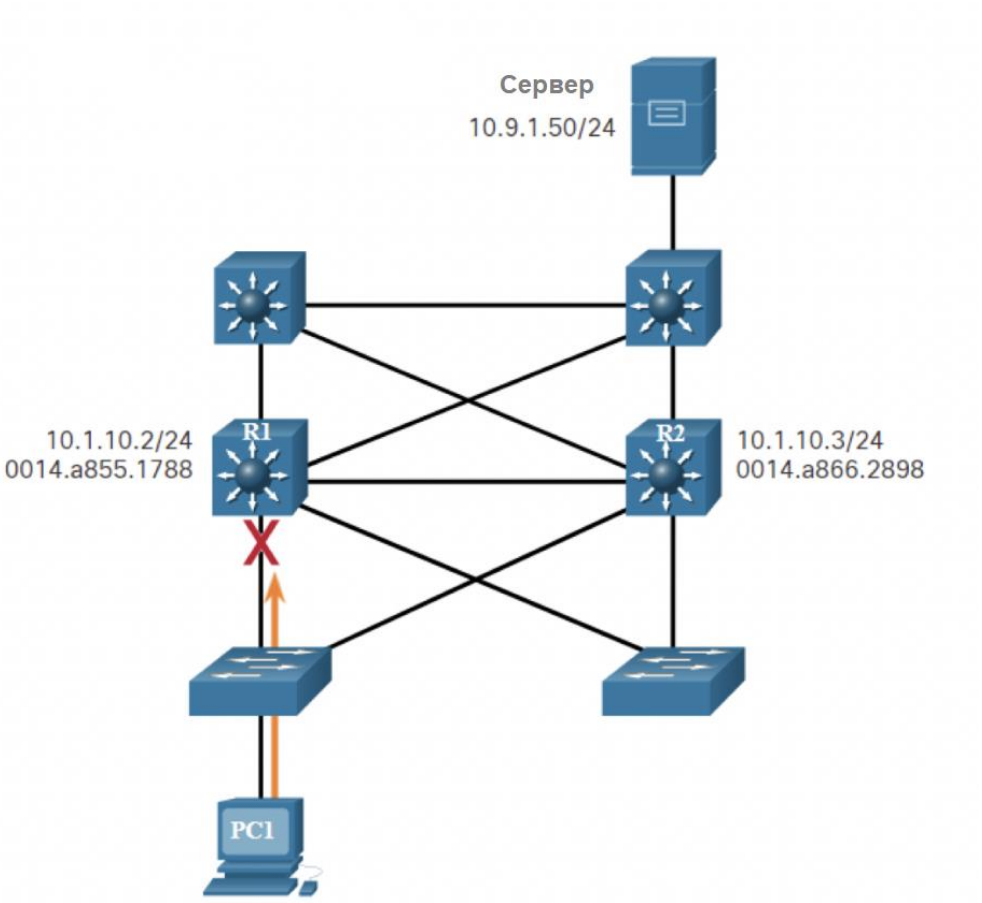


Рисунок 1.1 – Топологія фізичної мережі [9]

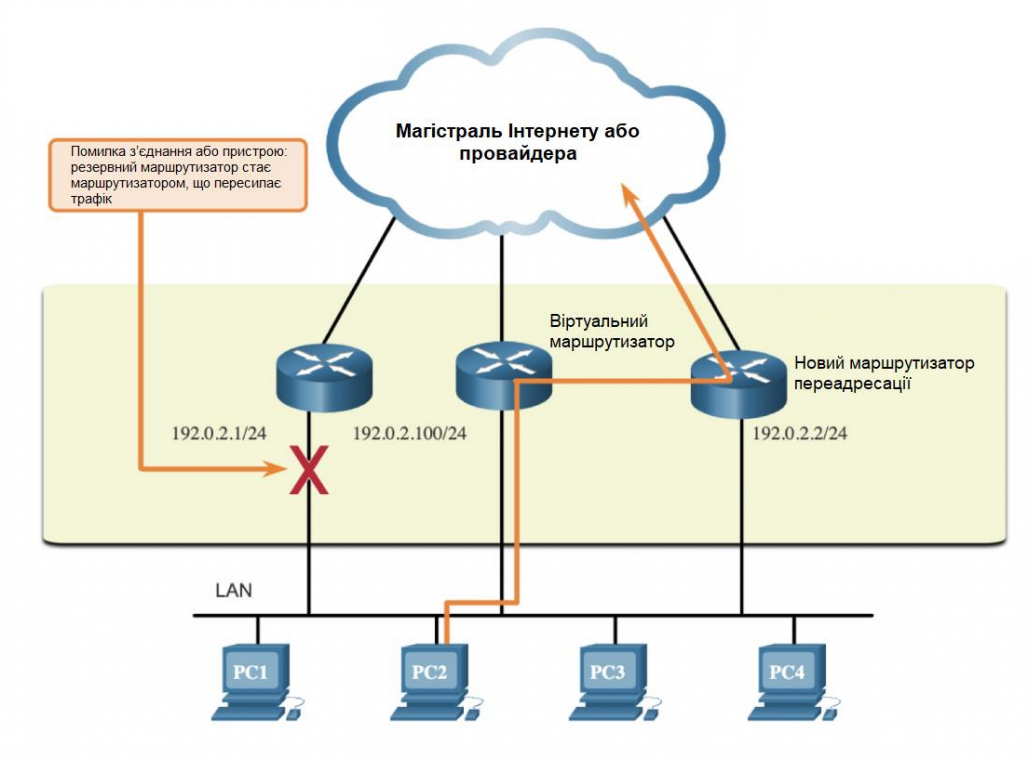


Рисунок 1.2 – Застосування віртуальних маршрутизаторів [9]

Протокол використовується для ідентифікації двох або більше маршрутизаторів як пристроїв, що відповідають за обробку пакетів, які відправляються на MAC-адресу або IP-адресу одного віртуального маршрутизатора. Хост-пристрої відправляють трафік на адресу віртуального маршрутизатора. Фізичний маршрутизатор, який пересилає цей трафік, не важливий для хост-пристроїв.

Протокол резервування забезпечує механізм для визначення, який маршрутизатор повинен відігравати активну роль в пересиланні трафіку. Він також визначає, коли роль переадресації повинен прийняти резервний маршрутизатор. Перехід від одного маршрутизатора пересилання до іншого неважливий для кінцевих пристроїв. Така здатність мережі динамічно відновлюватися після збою пристрою, який виступає в якості шлюзу, називається резервуванням першого переходу.

1.2 Огляд можливостей протоколів VRRP ТА HSRP

Протокол резервування віртуальних маршрутизаторів (Virtual Router Redundancy Protocol, VRRP) – це загальнодоступний протокол, який динамічно

розподіляє відповідальність за один або кілька віртуальних маршрутизаторів на маршрутизатори VRRP в локальній мережі IPv4. Це дозволяє декільком маршрутизаторам в каналі множинного доступу використовувати один і той самий віртуальний адрес IPv4. Маршрутизатор VRRP налаштований для запуску протоколу VRRP в поєднанні з одним або декількома іншими маршрутизаторами, підключеними до локальної мережі. У конфігурації VRRP один маршрутизатор вибирається в якості Master (головного) віртуального маршрутизатора, а інші маршрутизатори виступають в якості резервних копій на випадок збою віртуального маршрутизатора майстра.

Для групи маршрутизаторів налаштовується їхня належність віртуальному маршрутизатору. Фактично, віртуальний маршрутизатор – це група інтерфейсів маршрутизаторів, які знаходяться в одній мережі та поділяють Virtual Router Identifier (VRID) та віртуальну IP-адресу.

VRRP-маршрутизатор може перебувати у кількох віртуальних маршрутизаторах, кожен із унікальною комбінацією VRID/IP-адресу. Відповідності між VRID та віртуальною IP-адресою мають бути однаковими на всіх маршрутизаторах в одній мережі.

У будь-який момент часу лише один із фізичних маршрутизаторів виконує маршрутизацію трафіку, тобто стає VRRP Master маршрутизатор, решта маршрутизаторів у групі стає VRRP Backup router. Якщо поточний VRRP Master router стає недоступним, його роль бере на себе один з VRRP Backup маршрутизаторів, той у якого найвищий пріоритет. Завдання пріоритету дозволяє визначити пріоритетніші шляхи адміністративно.

Backup-маршрутизатор не намагатиметься перехопити на себе роль Master-маршрутизатора, якщо тільки він має не більш високий пріоритет, ніж у поточного Master-маршрутизатора. VRRP дозволяє адміністративно заборонити перехоплення ролі Master-маршрутизатора. Єдиний виняток із цього правила – VRRP-маршрутизатор завжди буде ставати Master, якщо він власник IP-адреси, яку присвоєно віртуальному маршрутизатору.

У кожному віртуальному маршрутизаторі тільки Master надсилає періодичні VRRP-оголошення на зарезервовану групову адресу 224.0.0.18. На канальному рівні як MAC-адреса (media access control, управління доступом до середовища) відправника VRRP-оголошень використовується віртуальна MAC-адреса.

HSRP (Hot Standby Router Protocol) є пропрієтарним FHRP, розробленим компаніє Cisco, який забезпечує прозоре перемикання при відмові пристрою IPv4

першого переходу. HSRP забезпечує високу доступність мережі, завдяки резервування маршрутизації на першому переході для вузлів IPv4 в мережах, налаштованих з адресою шлюзу IPv4. HSRP використовується в групі маршрутизаторів для вибору активного пристрою і резервного пристрою. У групі інтерфейсів пристроїв активний пристрій – це пристрій, який використовується для маршрутизації пакетів, резервний пристрій – це пристрій, який вступає в роботу при відмові активного пристрою або при виконанні встановлених умов. Функція резервного маршрутизатора HSRP полягає в тому, щоб відстежувати робочий стан групи HSRP і швидко брати на себе відповідальність за пересилку пакетів в разі збою активного маршрутизатора. Роль активного і резервного маршрутизаторів визначається під час процесу вибору HSRP. За умовчанням як активного маршрутизатора обраний маршрутизатор з найбільшим за чисельністю адресою IPv4. Однак завжди краще контролювати, як ваша мережа буде працювати в нормальних умовах, ніж залишати це на волю випадку.

Пріоритет HSRP (HSRP Priority) може використовуватися для визначення активного маршрутизатора. Маршрутизатор з найвищим пріоритетом HSRP стане активним маршрутизатором. За замовчуванням пріоритет HSRP дорівнює 100. Якщо пріоритети рівні, як активного маршрутизатора вибирається маршрутизатор з найвищим цифровим адресом IPv4.

Щоб налаштувати маршрутизатор як активний маршрутизатор, використовують команду інтерфейсу standby priority. Діапазон пріоритету HSRP становить від 0 до 255

HSRP протокол реалізований поверх стека протоколів TCP/IP, для доставки службової інформації використовується протокол UDP. Маршрутизатор або маршрутизовані комутатори, на яких налаштований і функціонує протокол HSRP, в рамках обміну службовою інформацією використовують так звані пакети вітання (hello packets). У свою чергу, дані пакети відправляються на IP-адреса групової розсилки 224.0.0.2 (HSRP Version 1) або на 224.0.0.102 (HSRP Version 2) по протоколу UDP на порт 1985.

1.3 Огляд можливостей протоколу GLBP

GLBP працює аналогічно, але не ідентично іншим протоколам резервування шлюзу, такими як HSRP і VRRP.

Члени GLBP групи вибирають один шлюз який буде активним віртуальним шлюзом AVG (Active Virtual Gateway, активний віртуальний шлюз) для цієї групи. Інші члени групи забезпечують резервування для AVG в разі якщо AVG стане недоступним. AVG призначає віртуальний MAC адреса для кожного члена GLBP групи. Кожен член групи бере участь в передачі пакетів, використовуючи віртуальний MAC адресу, виданий AVG. Цих членів групи називають AVFs (Active Virtual Forwarders, активний віртуальний пересилач). AVG відповідальний за видачу відповідей по протоколу ARP (Address Resolution Protocol, протокол визначення адрес) на запити до віртуального IP-адресою. Розподіл навантаження досягається тим що AVG відповідає на ARP запити використовуючи різні віртуальні MAC-адреси.

GLBP підтримує такі режими балансування навантаження:

- None – режим, при якому комутатор не забезпечує балансування навантаження. На всі запити клієнтів він відповідає своїм MAC-адресою. Другий комутатор починає роботу тільки після того як основний комутатор (AVG) вийде з ладу або стане недоступним.

- Weighted load-balancing – балансування навантаження проводиться відповідно до ваги кожного комутатора. Вага комутатора призначається адміністратором на кожному комутаторі окремо. Наприклад якщо в GLBP групі два комутатора, у AVG вага 80, а у AVF 160 то навантаження буде розподілятися 1: 2. Іншими словами з трьох отриманих запитів на MAC-адресу AVG один раз відповість своїм MAC-адресою і двічі MAC-адресою AVF комутатора.

- Host-dependent load-balancing – цей режим використовується в разі якщо є необхідність в реалізації трансляції адрес Network Address Translation (NAT), так як цей режим гарантує повернення клієнту того ж MAC-адреси AVF комутатора, який він використовував раніше і отже NAT сесія у клієнта не переривається. Клієнти будуть отримувати ті ж MAC-адреси AVF до тих пір, поки кількість комутаторів в GLBP групі не зміниться.

- Round-robin load-balancing – режим використовується за замовчанням. В цьому режимі AVG видає MAC-адреси AVF поперемінно.

На рисунку 1.3 маршрутизатор A є AVG для GLBP групи, і відповідальний за віртуальний IP-адрес 10.24.0.1. Маршрутизатор A так само є AVF для віртуального MAC адреси 0007.b400.0204. Маршрутизатор B член тієї ж GLBP групи і призначений AVF для віртуального MAC адреси 0007.b400.0205. На клієнтах встановлюється шлюз з IP-адресою 10.24.0.1 і MAC адресою шлюзу

0007.b400.0204. У той час як на іншому клієнті MAC-адресу шлюзу за замовчуванням буде 4007.b400.0205 і таким чином маршрутизатор А буде розподіляти навантаження з маршрутизатором В.

GLBP підтримує до 4 маршрутизаторів в групі і до 1024 груп. Маршрутизатор відправляють один одному повідомлення hello кожні 3 секунди. Повідомлення відправляються на адресу 224.0.0.102, UDP порт 3222 (відправника і одержувача).

GLBP Gateway Priority визначає роль, яку кожен маршрутизатор AVF грає в групі. Тобто за допомогою цієї властивості можна визначити послідовність вибору нового AVG, якщо старий AVG стане недоступним. Пріоритет можна визначити на кожному маршрутизаторі значенням від 1 до 255 командою: glbp priority. Маршрутизатор з великим пріоритетом стає AVG.

За замовчуванням схема вибору AVG тільки на основі пріоритету вимкнена. Запасний AVF стане AVG тільки якщо поточний AVG стане недоступним. Що б дозволити вибори AVG на основі пріоритету потрібно ввести команду: gIbp preempt.

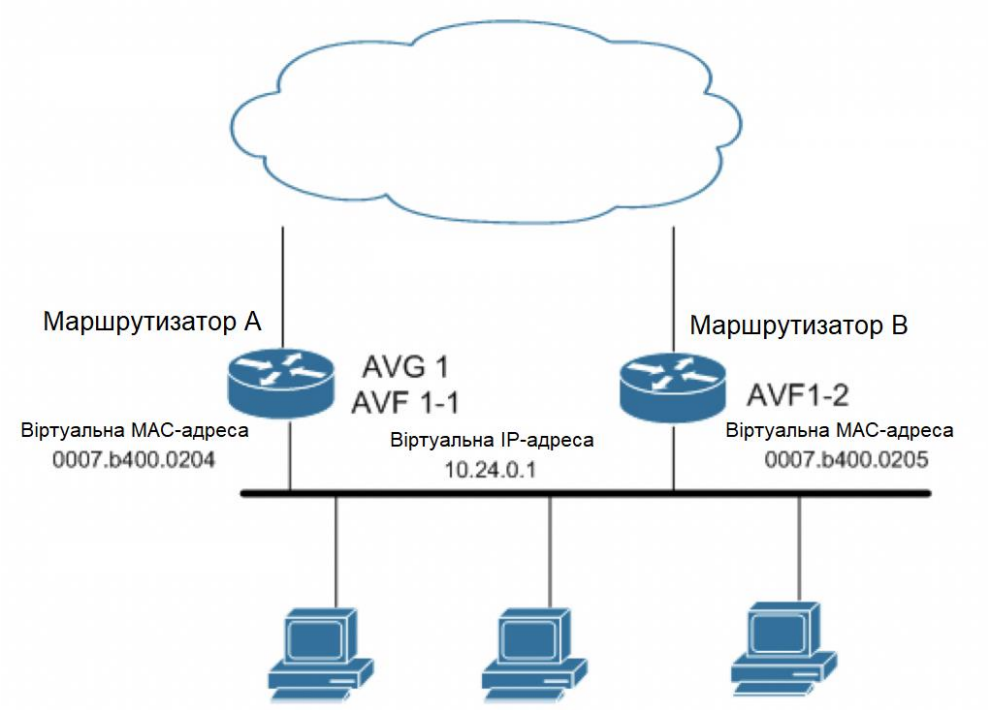


Рисунок 1.3 – Топологія мережі з балансуванням навантаження [9]

Балансування навантаження сприяє покращенню надійності мережі до того, як настануть відмови.

1.4 Характеристика переваг та недоліків проаналізованих протоколів відмовостійкої маршрутизації

Після детального розгляду протоколів резервування першого переходу можна сказати що кожен з них має свої переваги та недоліки.

До переваг протоколу VRRP можна віднести:

- надмірність – VRRP дає змогу налаштувати кілька маршрутизаторів як маршрутизатор шлюзу за замовчуванням, що зменшує можливість відмови в мережі;
- можливість розподіляти навантаження – можливо налаштувати VRRP таким чином, щоб трафік до та від клієнтів локальної мережі міг спільно використовуватися кількома маршрутизатори, тим самим рівномірно розподіляючи трафік між доступними маршрутизаторами;
- підтримка максимальної кількості віртуальних маршрутизаторів – VRRP підтримує до 255 віртуальних маршрутизаторів (груп VRRP) на фізичному інтерфейсі маршрутизатора, відповідно до платформи, що підтримує кілька MAC-адрес. Підтримка декількох віртуальних маршрутизаторів дозволяє реалізувати резервування та розподіл навантаження у топології локальної мережі;
- декілька IP-адрес – віртуальний маршрутизатор може управляти кількома IP-адресами, включаючи вторинні IP-адреси. Тому, якщо існує кілька підмереж, налаштованих на інтерфейсі Ethernet, можливо налаштувати VRRP для кожної підмережі;
- протокол оголошення – VRRP використовує спеціальну стандартну багатоадресну адресу для багатоадресної передачі Internet Assigned Numbers Authority (IANA). (224.0.0.18). Ця схема адресації мінімізує кількість маршрутизаторів, які повинні обслуговувати групову передачу та дозволяє тестовому обладнанню точно ідентифікувати пакети VRRP у сегменті. IANA присвоїла VRRP номер IP-протоколу 112;
- відстеження об'єктів VRRP – забезпечує спосіб переконатися, що найкращий маршрутизатор VRRP є головним віртуальним маршрутизатором для групи, шляхом зміни пріоритетів VRRP на статус відстежуваних об’єктів, таких як стани інтерфейсу або маршруту IP.

До недоліків протоколу VRRP можна віднести те, що він не підтримує балансування навантаження. До того ж, основним недоліком HSRP і VRRP є те, що активним вибирається тільки один шлюз, і використовується для пересилання

трафіку, в той час як інші не використовуються, поки активний не вийде з ладу. Також, недоліком VRRP є низький рівень безпеки, тому що у VRRP відсутні жодні методи захисту.

Для протоколу HSRP, до переваг можна віднести наступне:

- схема резервування – HSRP використовує перевірену часом і широко розгорнуту у великих мережах схему резервування;
- прозоре швидке відновлення після відмови маршрутизатора першого стрибка;
- алгоритм автентифікації message digest 5 (MD5) захищає від програмного забезпечення для підробки HSRP і використовує галузевий стандартний алгоритм MD5 для покращеної надійності та безпеки.

Існують деякі обмеження протоколу HSRP. Першим обмеженням, яке виникає, є відстеження, коли послідовне з'єднання, яке прямо під'єднано до ISP, виходить із ладу, HSRP не може визначити, чи потрібно змінити маршрутизатор за замовчуванням. HSRP – це власний протокол Cisco, його не можна запускати на маршрутизаторах інших постачальників. Також, HSRP не може забезпечити балансування навантаження на шлюзі за замовчуванням.

До переваг протоколу GLBP належать:

- розподіл навантаження – можливо налаштувати GLBP таким чином, щоб трафік від клієнтів локальної мережі міг спільно використовуватися кількома маршрутизаторами, тим самим рівномірніше розподіляючи трафік між доступними маршрутизаторами.
- кількість віртуальних маршрутизаторів – GLBP підтримує до 1024 віртуальних маршрутизаторів (груп GLBP) на кожному фізичному інтерфейсі маршрутизатора та до чотирьох віртуальних на групу.
- випередження – схема резервування GLBP дозволяє випереджати активний віртуальний шлюз із вищим пріоритетом резервний віртуальний шлюз, який став доступним. Випередження пересилання працює подібним чином, за винятком що пріоритетне пересилання використовує зважування замість пріоритету та ввімкнено за замовчуванням.
- аутентифікація – GLBP підтримує галузевий стандартний алгоритм дайджесту повідомлень 5 (MD5) для покращеної надійності, безпеки, і захисту від програмного забезпечення для підробки GLBP. Маршрутизатор у групі GLBP з іншим рядком автентифікації, ніж інші маршрутизатори, ігноруватиметься іншими членами групи. Можливо альтернативно використовувати просту схему

автентифікації текстового пароля між членами групи GLBP для визначення конфігурації помилки.

GLBP має певні обмеження, а саме: протокол належить Cisco не може бути розгорнутий на пристроях інших постачальників, а також він використовує автентифікацію простого тексту з надсиланням hello повідомлень один одному в одній групі. Під час обміну інформацією між протоколом балансування навантаження шлюзу (GLBP) та автентифікації один з одним у тій самій групі використовуючи hello повідомлення для обміну інформацією між собою, пакети повідомлень hello можуть бути захоплені та розшифровані. У майбутньому потрібно зосередитися на різних алгоритмах і різних методах для вирішення автентифікації між переходами в одній групі протоколу GLBP. Вони надсилають hello повідомлення у вигляді звичайного тексту, яке може бути легко захоплено та прочитано хакером, якщо хакер отримав доступ до нашого коду автентифікації або пароля, щоб він чи вона могли легко налаштувати власний маршрутизатор і зробити маршрутизатор членом нашої групи та створити свій маршрутизатор з найвищим пріоритетом для збирання даних та інформації. Також до недоліків протоколу можна віднести високу складність управління мережею.

1.5 Огляд можливостей протоколів маршрутизації в транспортній мережі – RIP, IGRP, OSPF

Відмовостійкість може бути забезпечена на границі мережі за допомогою таких протоколів як RIP (Routing Information Protocol, інформаційний протокол маршрутизації), IGRP (Interior Gateway Routing Protocol, протокол маршрутизації внутрішнього шлюзу), OSPF (Open Shortest Path First, відкритий протокол маршрутизації за найкоротшим шляхом). Також, відмовостійкість може бути забезпечена всередині транспортної мережі, наприклад, протоколами описаними вище – VRRP, HSRP, чи GLBP.

Протоколи динамічної маршрутизації протягом кількох секунд (а то й мілісекунд) дізнаються про проблеми в мережі та перебудовують свої таблиці маршрутизації, і у такому випадку пакети будуть надсилатися вже актуальним маршрутом. Далі, розглянемо докладніше кожен з протоколів.

Протокол RIP заснований на дистанційно-векторному алгоритмі та в більшості реалізацій використовує найпростішу метрику — кількість проміжних машрутизаторів до мережі призначення. Головною перевагою протоколу є

легкість конфігурування, яка не потребує високої кваліфікації обслуговуючого персоналу. Протокол є відкритим та підтримується практично всіма виробниками мережевого обладнання. Також є реалізації протоколу в ПЗ (наприклад, для Unix-подібних ОС - пакети Zebra, Quagga та ін) і підтримка в ряді ОС (наприклад, Windows, починаючи з Windows NT Server, Unix-подібних, Cisco IOS).

Основними недоліками протоколу є: повільна збіжність і великий обсяг службового трафіку (для адаптації змін у топології мережі маршрутизатори періодично розсилають повні копії своїх таблиць). Це обмежило сферу застосування протоколу для мереж з кількістю маршрутизаторів не більше п'ятнадцяти. У протокол RIP версії 2 додано підтримку маски змінної довжини, мультикастингова (багатоадресна) розсилка замість широкомовної та засоби захисту при обміні маршрутною інформацією у вигляді аутентифікації за ключом MD5 та відкритого (нешифрованого) тексту.

Протокол досить поширений у невеликих локальних мережах, які не прагнуть до розширення, з невисокими вимогами до надійності мережі та відсутністю кваліфікованого персоналу мережевих адміністраторів. У новій версії протоколу Riping організовано підтримку протоколу IPv6

Закритий дистанційно-векторний протокол IGRP компанії Cisco був спроектований для усунення ряду недоліків протоколу RIP, і мав на меті забезпечити кращу підтримку великих мереж (до 255 маршрутизаторів), які містять канали зв'язку з характеристиками смуги пропускання і величини затримки, що відрізняються. Протокол використовує комбіновану метрику, яка включає затримку, смугу пропускання, надійність та завантаженість маршруту. Вагові коефіцієнти, що визначають внесок цих характеристик у результуючу метрику, задаються користувачем, забезпечуючи гнучку адаптацію його конкретним завданням.

Показники затримки та смуги пропускання конфігуруються для кожної лінії зв'язку заздалегідь, а показники надійності та завантаженості можуть обчислюватися в процесі обробки реального трафіку в мережі. Для підтримки вимог QoS різних програм можна підготувати кілька маршрутних таблиць, побудованих на основі метрик з різними значеннями вагових коефіцієнтів. Протокол IGRP забезпечує швидшу збіжність, ніж RIP завдяки застосуванню пакетів оновлення з миттєвою розсилкою (інформація про зміни в мережі відправляється відразу, як стає доступною, не чекаючи чергового часу оновлення). Протокол підтримує балансування навантаження між кількома

маршрутами навіть у тому разі, якщо їх метрики не рівні, але перебувають у межах певного діапазону показників найкращого маршруту. При цьому співвідношення обсягів даних, що відправляються по кожному шляху даних буде пропорційне співвідношенню їх метрик.

До недоліків протоколу можна віднести відсутність підтримки масок підмереж змінної довжини та можливості об'єднання маршрутів. Періодичні розсилки маршрутної інформації сусіднім маршрутизаторам залишаються широкомовними. Засоби забезпечення безпеки обмежені. Відсутні засоби автентифікації під час обміну маршрутною інформацією. Непрямим засобом захисту є можливість прийому повідомлень про оновлення маршрутів тільки від маршрутизаторів, які даний визначає як «сусідні», а також можливість внесення змін до конфігурації маршрутизатора тільки на підставі пароля, який зберігається у зашифрованому вигляді. Протокол сумісний із RIP.

Найбільш універсальним та гнучким у налаштуванні протоколом динамічної маршрутизації в корпоративних мережах на сьогоднішній день є відкритий протокол вибору першого найкоротшого шляху (Open Shortest Path First Protocol – OSPF). Протокол спочатку був орієнтований на роботу у великих мережах (до 65 536 маршрутизаторів) зі складною топологією. Він заснований на алгоритмі стану каналів зв'язку і має високу стійкість до змін топології мережі та швидку збіжність.

При виборі маршруту використовується метрика пропускної спроможності складової мережі (тобто передача даних найбільш швидкісним каналам зв'язку). Протокол може підтримувати різні вимоги IP-пакетів на якість обслуговування (пропускна здатність, затримка та надійність) за допомогою побудови окремої таблиці маршрутизації для кожного з цих показників. Протокол має й інші переваги, корисні у великих сучасних мережах. До них відносяться можливість балансування навантаження між каналами з рівними метриками та засоби аутентифікації як по нешифрованому паролю, так і по шифрованому (шляхом додавання до пакету дайджеста ключа та тіла пакета за алгоритмом MD5). Нумерація пакетів виключає їх повторюваність і в такий спосіб можливість повторної атаки.

Відкритість протоколу визначає його підтримку практично всіма виробниками мережного обладнання, реалізації в ПЗ під усі популярні ОС (наприклад, для Unix-подібних ОС - пакети Zebra, Quagga та ін), а також безпосередню інтеграцію до ряду ОС (наприклад, Windows 2000 Server та вище,

OpenBSD, Cisco IOS, Solaris 10 тощо). До недоліків проколу слід віднести високу обчислювальну складність і, отже, високі вимоги до ресурсів маршрутизатора. Обчислювальна складність OSPF зростає із збільшенням розмірів мережі. Тому збільшення масштабованості протоколу застосовується поділ мережі на логічні області, з'єднані магістральною областю. Внутрішня топологічна інформація між областями не надається. Скорочення розмірів таблиць маршрутизації та зниження службового трафіку при оновленні топологічної інформації служить можливість об'єднання кількох адрес мереж в одну при виявленні у них загального префікса, і заміна широкомовних розсилок мультикастинговими. З метою економії IP-адрес у з'єднаннях типу «крапка – крапка» між маршрутизаторами призначати кінцевим точкам адреси не обов'язково. Платою за ці переваги є складність конфігурування та необхідність ретельного попереднього планування мережі для її оптимальної роботи (розбивка на області, виділення магістралі, розподіл функцій між маршрутизаторами з урахуванням їхньої обчислювальної потужності: рядові, виділені в зоні, прикордонні тощо).

Як перспективні функції OSPF слід назвати підтримку протоколу IPv6 і можливість вибору маршруту на підставі поточного коефіцієнта завантаженості каналів зв'язку (розширена версія OSPF отримала назву Constrained Shortest Path First — CSPF). Протокол сумісний із RIP.

1.6 Огляд існуючих наукових робіт у області забезпечення відмовостійкої маршрутизації

Багато сучасних науковців займаються вивчення проблеми вдосконалення та розробки нових рішень [18-23] щодо балансування навантаження та відмовостійкості в мережі. Тому, нещодавно було проведено та опубліковано кілька досліджень. Загальним у всіх роботах є оптимізаційний підхід. Так, наприклад у роботі [23] пропонується врахування рівня надійності приграничних маршрутизаторів, між якими балансується навантаження, що надходить від мереж доступу. Кількісні результати досліджень процесів відмовостійкої маршрутизації Traffic Engineering підтвердили ефективність запропонованої моделі щодо реалізації схеми захисту шлюзу за замовчуванням і балансування навантаження в мережі. Тим часом у [14] була запропонована та досліджена модель лише з урахуванням Traffic Engineering, без врахування надійності маршрутизаторів мережі.

Стаття [21] присвячена проблемам відмовостійкої маршрутизації як вирішального чинника для сучасних інфокомунікаційних мереж щоб досягнути високої доступності та надійності за допомогою механізмів маршрутизації. Математична модель відмовостійкої маршрутизації Traffic Engineering була досліджена в цій роботі для підтримки стратегій резервування шлюзу за замовчуванням і балансування мережевого навантаження за аналогією з механізмами протоколів FHRP. Модель охоплює різні варіанти балансування навантаження в ІКМ та на рівні доступу мережі. Результати дослідження показали ефективність запропонованої моделі. Вдалося знизити верхній поріг використання каналів зв'язку мережі, що сприяє покращенню критичних параметрів якості обслуговування, таких як продуктивність та втрата пакетів.

Робота [20] присвячена огляду останніх спроб подолання проблем відмовостійкості у площині керування програмно-визначеною мережею. Крім того, в цій роботі пропонується запозичення протоколів FHRP в структурі програмно-визначеної мережі. Стаття висвітлює майбутні напрямки для академічних дослідників та інженерів, щоб покращити стійкість програмно-визначеної мережі та надихнути на нові рішення. Отже, майбутні напрямки досліджень вбачаються в пропозиції потокових математичних моделей відмовостійкої маршрутизації та резервування. У той же час, порушені проблеми оптимізації та обізнаність про балансування навантаження, які допомагають ефективно використовувати доступні ресурси мережі.

У роботі [19] вдосконалено математичну модель відмовостійкої маршрутизації із захистом шлюзу за замовчуванням та забезпеченням балансування навантаження між пригранічними маршрутизаторами. У рамках запропонованої моделі в оптимізаційній формі сформульовано задачу відмовостійкої маршрутизації. Новизна запропонованої моделі відмовостійкої маршрутизації полягає у введенні умов, що відповідають за забезпечення балансування навантаження, що надходить від мереж доступу між пригранічними маршрутизаторами, з урахуванням їх надійності (коефіцієнта доступності). Проведені дослідження підтвердили ефективність мережевих рішень, отриманих через запропоновану відмовостійку модель маршрутизації. Встановлено, що при незначній різниці в надійності граничних маршрутизаторів отриманий порядок балансування не погіршував верхній поріг використання каналів мережі. Проте лише в окремих випадках відбувалося деяке підвищення (до 3%) верхнього порогу при різниці значень коефіцієнтів надійності

маршрутизаторів приблизно в два і більше разів, що не характерно для сучасних інфокомунікаційних мереж.

З цього витікає, що потрібно розробляти нову вдосконалену модель, яка б враховувала Traffic Engineering, надійність маршрутизаторів, пропускну здатність каналів, та інші мережні показники, для того, щоб покращити показники якості обслуговування.

1.7 Формулювання вимог до перспективних рішень у цій області

Велика кількість досліджень присвячена вивченню проблем балансування навантаження та відмов у мережі. Не зважаючи на всі, перелічені вище, переваги існуючих рішень, основним недоліком та полем для розвитку є те, що протоколи базуються на методі пошуку найкоротшого шляху та графовій моделі. Так як ефективність протоколу головним чином залежить від того математичного апарату, на якому його засновано, існуючі протоколи не можуть врахувати всі характеристики мережі. Це призводить до неможливості балансувати навантаження в мережі, а отже можливому перевантаженню мережі, відмовам та погіршенням показників якості обслуговування.

Вдосконалена модель має бути задана у формі оптимізаційної задачі на основі потокової моделі та реалізувати механізми балансування навантаження, для того щоб ефективно використовувати наявні мережні ресурси.

Також варто звернути увагу на те, що існуючи протоколи мають бути налаштовані адміністратором мережі вручну та потребують відповідної кваліфікації та часу для налаштування.

За для досягнення описаних вище цілей, пропонується створення нового протоколу на основі існуючого протоколу балансування навантаження GLBP, який би враховував пропускну здатність мережі, надійність пристроїв мережі та був оснований на потоковій математичній моделі. Також, пропонується зробити можливим автоматичне налаштування протоколу, для запобігання помилок зі сторони людського фактору.

2 ОБҐРУНТУВАННЯ ТА ВИБІР МОДЕЛІ ДЛЯ ДОСЛІДЖЕННЯ ПРОЦЕСІВ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ

2.1 Опис математичної потокової моделі балансування навантаження в ІКМ

Нехай при описі маршрутних рішень, що порівнюються, використовуються позначення представлені у табл. 2.1. Під час дослідження була взята за основу потокова модель маршрутизації з балансуванням навантаження, що базується на принципах Traffic Engineering [6]. В межах цієї моделі було припущено структуру мережі (рис. 2.1), що описує граф $G = (M, L)$ (табл. 2.1). У такому випадку, K — це множина потоків, що циркулюють між мережами доступу за допомогою ресурсу транспортної мережі. З кожним k-м потоком пакетів ($k \in K$) пов'язані мережі доступу – джерело (V_s^k) та отримувач (V_d^k). Показник λ^k характеризує середню інтенсивність (швидкість) пакетів k-го потоку на вході в ІКМ, що вимірюється в пакетах за секунду (1/с).

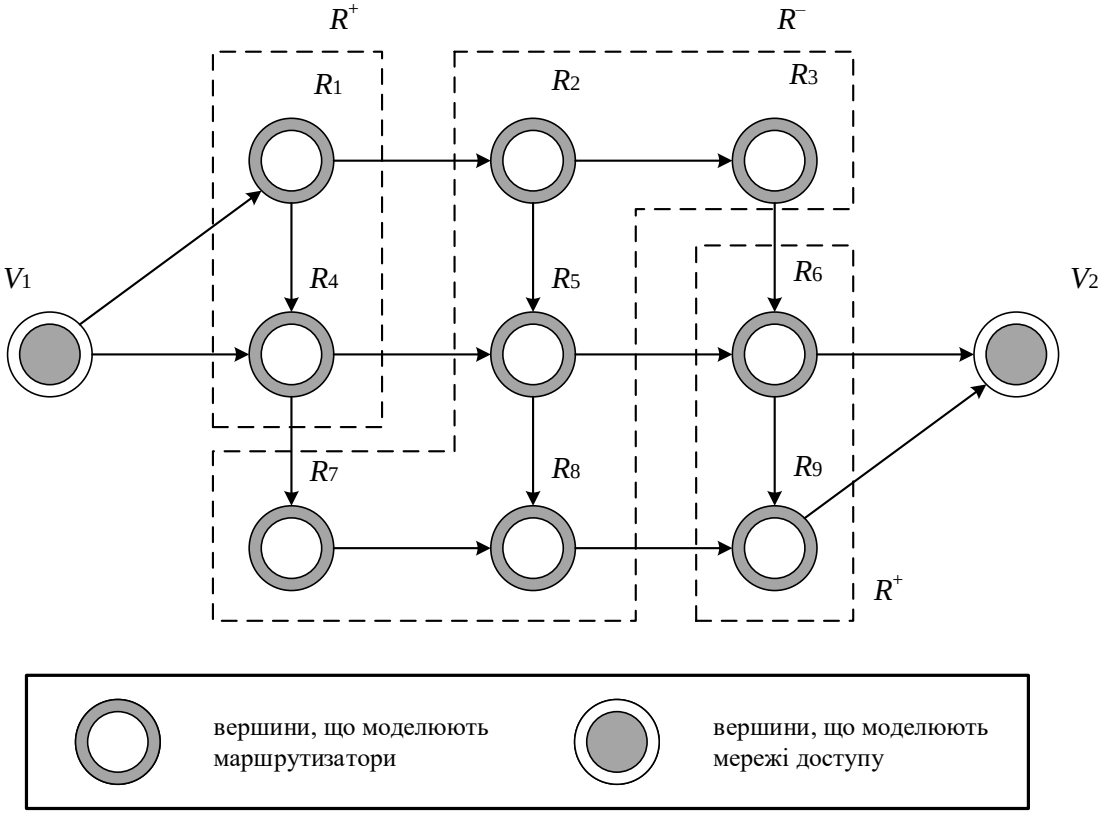


Рисунок 2.1 – Графова модель ІКМ

Таблиця 2.1 – Використані позначення

Позначення	Опис
$G = (M, L)$	Граф мережі
$M = R \cup V$	Множина вершин графа G ($R \cap V = \varnothing$)
$R = \{R_i, i = \overline{1,m}\}$	Підмножина вершин, які моделюють маршрутизатори
$V = \{V_j, j = \overline{1,v}\}$	Підмножина вершин, що описують мережі доступу
$R^+ \subset R$	Підмножина вершин, що моделюють пригранічні маршрутизатори ІКМ
$R^- \subset R$	Підмножина вершин, що моделюють транзитні маршрутизатори ІКМ
$R_j^+ \subset R^+$	Підмножина вершин графа , що моделює ті пригранічні маршрутизатори, які утворюють віртуальний маршрутизатор для мережі доступу V_j
$L = E \cup W$	Множина дуг графа G ($E \cap W = \varnothing$)
$E = \{E_{i,j}, i, j = \overline{1,m}, i \neq j\}$	Множина дуг, які моделюють канали зв'язку ІКМ, які з'єднують маршрутизатори
$W^+ = \{W_{i,j}^+, i = \overline{1,v}, j = \overline{1,m^+}\}$	Множина дуг, які описують лінії доступу, що з'єднують мережі доступу та пригранічні маршрутизатори
$W^- = \{W_{i,j}^-, i = \overline{1,m^+}, j = \overline{1,v}\}$	Множина дуг, які описують лінії доступу, що з'єднують пригранічні маршрутизатори ІКМ та мережі доступу
$\varphi_{i,j}$	Пропускна здатність каналу зв'язку, який моделюється дугою $E_{i,j} \in E$
K	Множина потоків пакетів, що циркулюють в ІКМ
K_i^+	Множина потоків, що надходять до ІКМ від мережі доступу V_i
K_i^-	Множина потоків, що виходять з ІКМ до мережі доступу V_i

Продовження таблиці 2.1

V_s^k	Мережа доступу, яка є джерелом *k*-го потоку пакетів
V_d^k	Мережа доступу, яка є отримувачем пакетів *k*-го потоку
λ^k	Середня інтенсивність пакетів *k*-го потоку
$x_{i,j}^k$	Маршрутна змінна, яка характеризує частку *k*-го потоку в каналі зв'язку, представленого дугою $E_{i,j}$
$y_{i,j}^k$	Змінна доступу, яка визначає частку *k*-го потоку, який протікає в лінії доступу, представленій дугою $W_{i,j}^+$
$z_{j,i}^k$	Змінна доступу, яка характеризує частку *k*-го потоку, що протікає в лінії доступу, представленій дугою $W_{j,i}^-$
α	Верхній поріг завантаженості каналів зв'язку ІКМ

У випадку використання одношляхової маршрутизації потоків в ІКМ, на маршрутні змінні $x_{i,j}^k$ накладаються такі обмеження:

$$x_{i,j}^k \in \{0;1\}, \tag{2.1}$$

а у випадку реалізації багатошляхової маршрутизації:

$$0 \le x_{i,j}^k \le 1. \tag{2.2}$$

При умові що мережа доступу взаємодіє лише з одним з приграничних маршрутизаторів ІКМ, на змінні доступу накладаються наступні обмеження:

$$y_{i,j}^k \in \{0;1\} \quad \text{та} \quad z_{j,i}^k \in \{0;1\}. \tag{2.3}$$

Якщо балансування навантаження підтримується на рівні доступу, як це реалізовано в протоколах VRRP, GLBP і CARP [7, 8, 9], на ці ж змінні накладаються умови, аналогічні до (2.2):

$$0 \le y_{i,j}^{k} \le 1 \text{ та } \ 0 \le z_{i,j}^{k} \le 1. \tag{2.4}$$

Щоб забезпечити збереження потоку на рівні доступу на відповідні керуючі змінні накладаються наступні умови-обмеження:

$$\sum_{R_j \in R_p^+} y_{p,j}^{k} = 1,\ V_p = V_s^k; \tag{2.5}$$

$$\sum_{R_j \in R_h^+} z_{j,h}^{k} = 1,\ \ V_h = V_d^k. \tag{2.6}$$

Для забезпечення збереження потоку на рівні транспортної мережі, накладаються наступні умови [12]:

$$\begin{cases} \sum\limits_{j:E_{i,j} \in E} x_{i,j}^{k} - \sum\limits_{j:E_{j,i} \in E} x_{j,i}^{k} = 0;\ \ k \in K\ , R_i \in R^{-}; \\ \sum\limits_{j:E_{i,j} \in E} x_{i,j}^{k} = y_{p,i}^{k};\ \ k \in K\ , R_i \in R^{+}, V_p = V_s^k; \\ \sum\limits_{j:E_{j,i} \in E} x_{j,i}^{k} = z_{i,h}^{k};\ \ k \in K\ , R_i \in R^{+}, V_h = V_d^k. \end{cases} \tag{2.7}$$

Дотримання умов (2.7) може забезпечити взаємозв’язок при розрахунку керуючих змінних різних типів, а отже і скоординувати процеси балансування навантаження на рівні доступу та ІКМ взагалі. Щоб забезпечити балансування навантаження в ІКМ на дотримуючись принципів ТЕ, в модель було введено умови [12]запобігання перевантаження наступного виду:

$$\sum_{k \in K} \lambda^{k} x_{i,j}^{k} \le \alpha \varphi_{i,j}, \tag{2.8}$$

де α – верхній поріг завантаженості каналів зв'язку ІКМ (табл. 2.1), який виступає додатковою керуючою змінною. На цю керуючу змінну накладаються обмеження виду:

$$0 \le \alpha \le 1. \tag{2.9}$$

У такому випадку, задача балансування навантаження в ІКМ може бути сформульована в оптимізаційній формі, де за аналогією до [12] критерієм оптимальності буде виступати умова:

$$\min_{x,y,z,\alpha} \alpha, \tag{2.10}$$

а обмеженнями – умови (2.1)-(2.9).

Залежно від конкретної постановки технологічної задачі балансування навантаження, задача оптимізації (2.10) буде належати до тієї чи іншої категорії (табл. 2.2). Якщо будь-яка з керуючих змінних $x_{i,j}^{k}$, $y_{i,j}^{k}$ та $z_{j,i}^{k}$ буде приймати булевий характер, тобто за виконання умов (2.1) та/або (2.3) задача балансування навантаження приймається як оптимізаційна задача змішаного цілочисельного лінійного програмування, тому що змінна α приймає дійсні значення. У випадку коли балансування навантаження буде підтримуватись і на рівні доступу (2.4), і на рівні ІКМ взагалі (2.2), тоді сформульована оптимізаційна задача буде належати до категорії задач лінійного програмування.

Таблиця 2.2 – Класифікація оптимізаційних задач балансування навантаження в ІКМ

№ моделі	Рівень доступу	Рівень ІКМ	Тип оптимізаційної задачі
Модель 1	Без балансування навантаження (3)	Без балансування навантаження, одношляхова маршрутизація (1)	Задача змішаного цілочисельного лінійного програмування

Продовження таблиці 2.2

Модель 2		З балансуванням навантаження, багатошляхова маршрутизація (2)	Задача змішаного цілочисельного лінійного програмування
Модель 3	З балансуванням навантаження (4)		Задача лінійного програмування

2.2 Розв’язок задачі маршрутизації з балансуванням навантаження за допомогою середовища Matlab

Для формулювання оптимізаційної задачі необхідно запрограмувати математичну модель, що описана в першому пункті даного розділу, з урахуванням усіх обмежень і умов. Щоб отримати результати оптимізаційної задачі було використано середовище MatLab, пакет Optimization Toolbox. Для розв’язання задач лінійної оптимізації було використано програму «linprog» та «intlinprog».

Реалізація цієї задачі в середовищі Matlab показана на рис. 2.2-2.5.

```
%clc;
clear all;
% r - інтенсивність потоку, який надходить до мережі
i = 0;
for r=500:10:500
    i = i + 1;
    lyambda(i) = r;
% c - вектор пропускних здатностей каналів зв'язку
c=[550; 620; 180; 170; 200; 350; 150; 250; 210; 290; 180; 260];
v = [0.9; 0.99; 0.98; 0.95];
% f - вектор метрик каналів зв'язку
f= [1/v(1); 1/v(2); 0; 0; 0;  0; 0;  0; 0; 0; 0; 0; 0; 0; 1/v(3); 1/v(4); 1000];
% формалізація у векторно-матричній формі обмежень у формі рівнянь
% Aeq*x=beq
Aeq = [-1  0    1  1  0  0  0  0  0  0  0  0  0  0    0  0    0
        0  0   -1  0  1  1  0  0  0  0  0  0  0  0    0  0    0
        0  0    0  0 -1  0  1  0  0  0  0  0  0  0    0  0    0
        0 -1    0 -1  0  0  0  1  1  0  0  0  0  0    0  0    0
        0  0    0  0  0 -1  0 -1  0  1  1  0  0  0    0  0    0
        0  0    0  0  0  0 -1  0  0 -1  0  1  0  0    1  0    0
        0  0    0  0  0  0  0  0 -1  0  0  0  1  0    0  0    0
        0  0    0  0  0  0  0  0  0  0 -1  0 -1  1    0  0    0
        0  0    0  0  0  0  0  0  0  0  0 -1  0 -1    0  1    0

        1  1    0  0  0  0  0  0  0  0  0  0  0  0    0  0   0
        0  0    0  0  0  0  0  0  0  0  0  0  0  0    1  1   0];
beq = [0; 0; 0; 0; 0; 0; 0; 0; 0; 1; 1];
```

Рисунок 2.2 – Перший фрагмент програми в середовищі Matlab

```
% формалізація у векторно-матричній формі обмежень у формі нерівностей
% A*x<=b
A = [0 0    r 0 0 0 0 0 0 0 0 0 0 0    0 0   -c(1)
     0 0    0 r 0 0 0 0 0 0 0 0 0 0    0 0   -c(2)
     0 0    0 0 r 0 0 0 0 0 0 0 0 0    0 0   -c(3)
     0 0    0 0 0 r 0 0 0 0 0 0 0 0    0 0    -c(4)
     0 0    0 0 0 0 r 0 0 0 0 0 0 0    0 0    -c(5)
     0 0    0 0 0 0 0 r 0 0 0 0 0 0    0 0    -c(6)
     0 0    0 0 0 0 0 0 r 0 0 0 0 0    0 0    -c(7)
     0 0    0 0 0 0 0 0 0 r 0 0 0 0    0 0    -c(8)
     0 0    0 0 0 0 0 0 0 0 r 0 0 0    0 0    -c(9)
     0 0    0 0 0 0 0 0 0 0 0 r 0 0    0 0    -c(10)
     0 0    0 0 0 0 0 0 0 0 0 0 r 0    0 0    -c(11)
     0 0    0 0 0 0 0 0 0 0 0 0 0 r    0 0    -c(12)];
b=[0 0 0 0 0 0 0 0 0 0 0 0];
% формалізація умов, щодо граничних значень координат вектора x
lb=zeros(17);
ub=ones(17);
```

Рисунок 2.3 – Другий фрагмент програми в середовищі Matlab

```
%intcon = [1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16]; % без балансування в транспортній мережі та на шлюхзах
intcon = [1 2 15 16]; % без балансування на шлюзах
%intcon = []; % з балансированням  в транспортній мережі та на шлюхзах
% розв'язання отпимізаційної задачі
%[x, fval] = linprog (f,A,b,Aeq,beq,lb,ub)
[x, fval] = intlinprog (f,intcon,A,b,Aeq,beq,lb,ub)
% Розрахунок інтенсивностей потоку в каналах зв'язку
y=r*x(3:14)
alpha(i) = x(17)
end
alpha'
```

Рисунок 2.4 – Третій фрагмент програми в середовищі Matlab

```
x =

    0.2754
    0.7246
    0.2754
         0
    0.2609
    0.0145
    0.2609
    0.5072
    0.2174
    0.3623
    0.1594
         0
    0.2174
    0.3768
    0.6232
    0.3768
    0.7246

fval =

  726.7081

y =

  137.6812
         0
  130.4348
    7.2464
  130.4348
  253.6232
  108.6957
  181.1594
   79.7101
         0
  108.6957
  188.4058

alpha =

    0.7246

ans =

    0.7246
```

Рисунок 2.5 – Фрагмент результатів програми в середовищі Matlab

2.3 Аналіз отриманих результатів дослідження процесів балансування навантаження в ІКМ

Як представлено на рис. 2.6, нехай джерелом потоку пакетів буде мережа доступу V_1, а отримувачем пакетів даного потоку буде мережа доступу V_2. У таблиці 2.3 представлені пропускні здатності каналів зв'язку.

Таблиця 2.3 – Пропускні здатності каналів зв'язку транспортної мережі

Канал зв'язку	$E_{1,2}$	$E_{2,3}$	$E_{1,4}$	$E_{2,5}$	$E_{3,6}$	$E_{4,5}$
Пропускна здатність, 1/с	550	180	620	170	200	350
Канал зв'язку	$E_{5,6}$	$E_{4,7}$	$E_{5,8}$	$E_{6,9}$	$E_{7,8}$	$E_{8,9}$
Пропускна здатність, 1/с	250	150	210	290	180	260

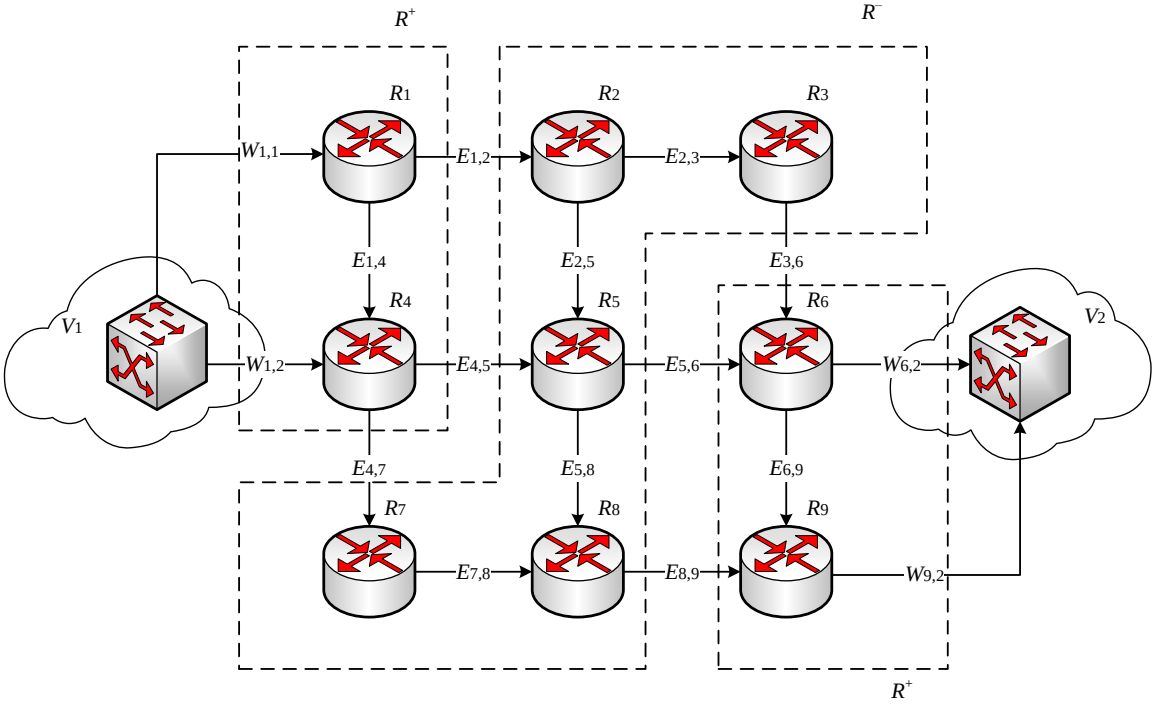


Рисунок 2.6 – Приклад структури ІКМ

Якщо балансування навантаження відсутнє на рівні доступу та на рівні ІКМ як це представлено у моделі 1, мережа досягала перенавантаження вже при $\lambda > 250$ 1/с. Порядок розподілу трафіка без балансування навантаження на рівні доступу та одношляхової маршрутизації на рівні ІКМ при $\lambda = 200$ 1/с показано на рис. 2.7. У цьому випадку, вест потік пакетів в ІКМ від мережі доступу V_1

надходив на четвертий приграничний маршрутизатор і передався до мережі доступу V_2 за наступним маршрутом: $R_4 \to R_5 \to R_6$.

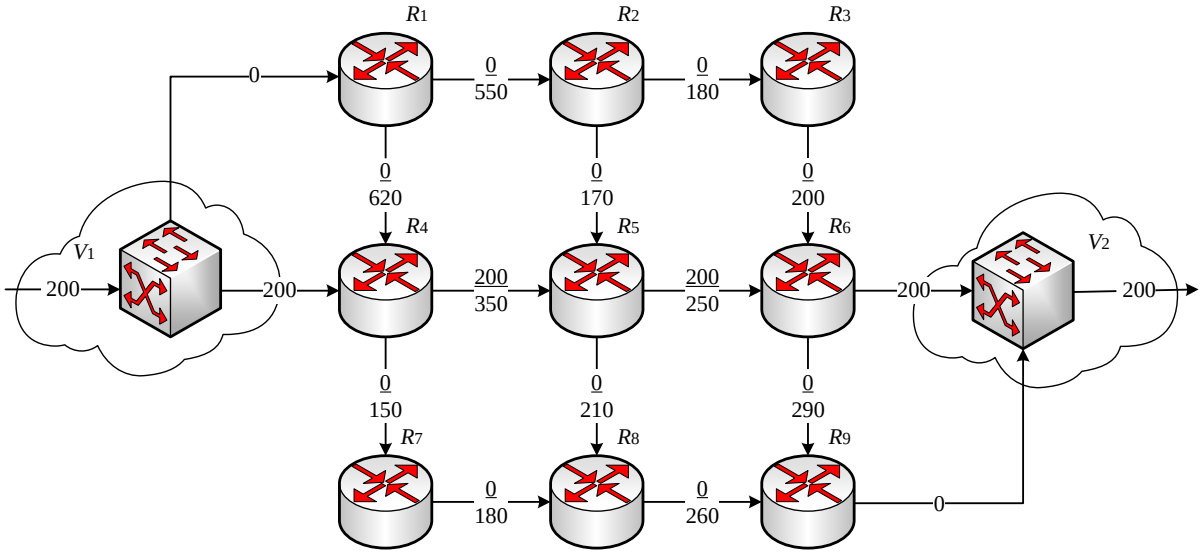


Рисунок 2.7 – Порядок розподілу трафіка без балансування навантаження на рівні доступу та одношляхової маршрутизації та рівні ІКМ

Якщо багатошляхова маршрутизація була реалізована на рівні ІКМ, але все ще була відсутня на рівні доступу між приграничними маршрутизаторами, як це представлено у моделі 2, максимальна інтенсивність потоку пакетів, яку могла обслужити мережа, була 550 1/с. Це є у 2,2 рази більше ніж могла обслужити модель 1. Як показано на рис.2.8 при інтенсивності $\lambda = 500$ 1/с потік пакетів в ІКМ від мережі доступу V_1 надходив на перший приграничний маршрутизатор і передавався до мережі доступу V_2 за наступними маршрутами:

$R_1 \to R_2 \to R_3 \to R_6 \to R_9$ з інтенсивністю 45,45 1/с;

$R_1 \to R_4 \to R_5 \to R_6 \to R_9$ з інтенсивністю 218,2 1/с;

$R_1 \to R_4 \to R_5 \to R_8 \to R_9$ з інтенсивністю 100 1/с;

$R_1 \to R_4 \to R_7 \to R_8 \to R_9$ з інтенсивністю 136,35 1/с;

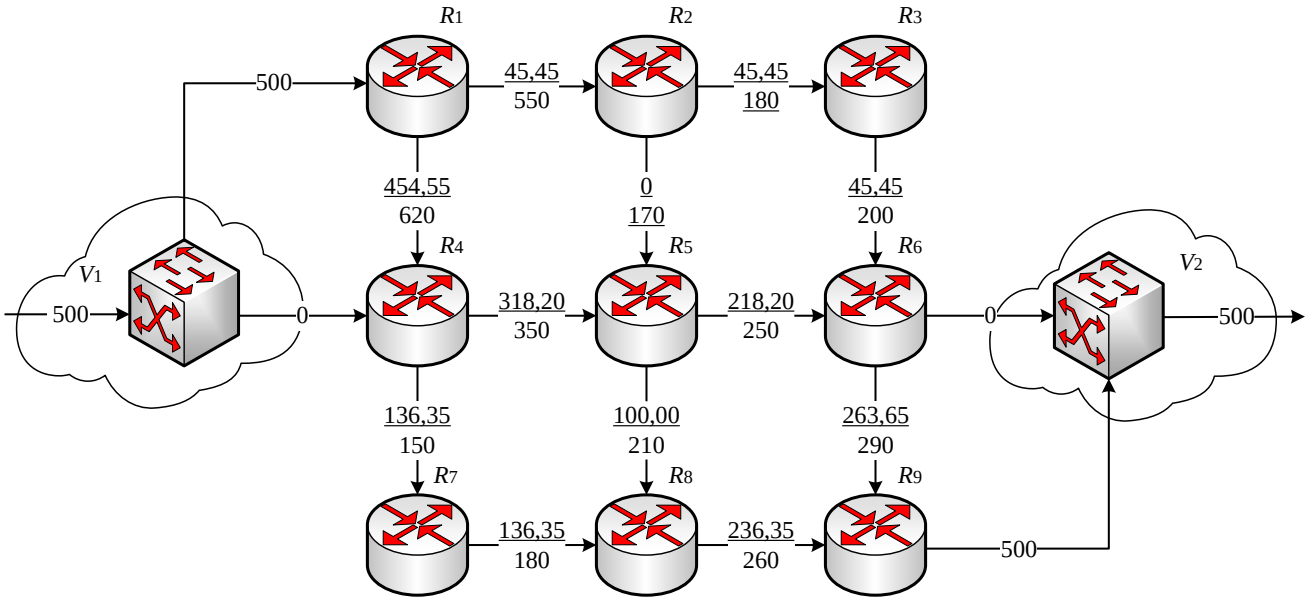


Рисунок 2.8 – Порядок розподілу трафіка без балансування навантаження на рівні доступу та багатошляхової маршрутизації та рівні ІКМ

У випадку якщо балансування навантаження підтримувалося і на рівні доступу і на рівні ІКМ, інтенсивність пакетів, яку мережа могла обслужити, зросла до 690 1/с, що на 25,45% більше ніж була спроможна обслужити модель 2 та в 2,76 рази більше, ніж могла обслужити модель 1. На рис. 2.9 представлено порядок балансування навантаження я на рівні доступу і на рівні ІКМ при $\lambda = 500$ 1/с. Потік пакетів, що надходив від мережі доступу V_1 було розподілено між першим і четвертим маршрутизаторами у пропорції 27,5% на 72,5 %. У ІКМ трафік передавався від мережі доступу V_1 до V_2 за п’ятьма маршрутами:

$R_1 \to R_2 \to R_3 \to R_6$ з інтенсивністю 130,43 1/с;

$R_4 \to R_5 \to R_6$ з інтенсивністю 181,17 1/с;

$R_1 \to R_2 \to R_5 \to R_8 \to R_9$ з інтенсивністю 7,25 1/с;

$R_1 \to R_4 \to R_7 \to R_8 \to R_9$ з інтенсивністю 72,46 1/с;

$R_4 \to R_7 \to R_8 \to R_9$ з інтенсивністю 108,69 1/с.

До другої мережі доступу з ІКМ трафік надходив через шостий та дев’ятий маршрутизатори у пропорції 62,3 на 37,7%.

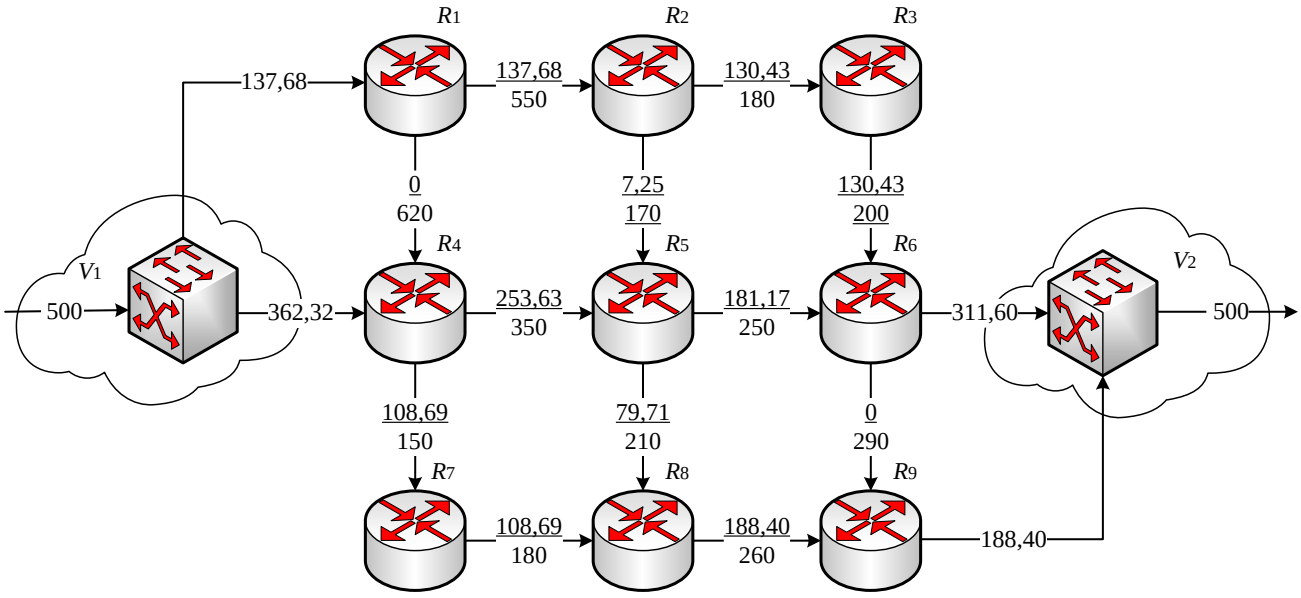


Рисунок 2.9 – Порядок балансування навантаження на рівнях доступу та ІКМ

За допомогою трьох варіантів моделі представлених у табл.2.1, було досліджена та порівняна ефективність рішення задачі балансування навантаження в ІКМ . Верхній поріг завантаженості каналів ІКМ змінювався в залежності від інтенсивності потоку пакетів, що надходив до мережі від 10 до 700 1/с як це показано за допомогою графіка на рис. 2.10.

Порівняння отриманих результатів показано у вигляді табл. 2.4.

Таблиця 2.4 – Результати виграшу по продуктивності та по верхньому порогу використання каналів зв’язку мережі

Моделі, що порівнювалися	Виграш по продуктивності	Виграш по верхньому порогу використання каналів зв’язку
2-1	у 2,2 рази	54,55%
3-1	у 2,76 рази	63,77%
3-2	у 1,2 рази	20,29%

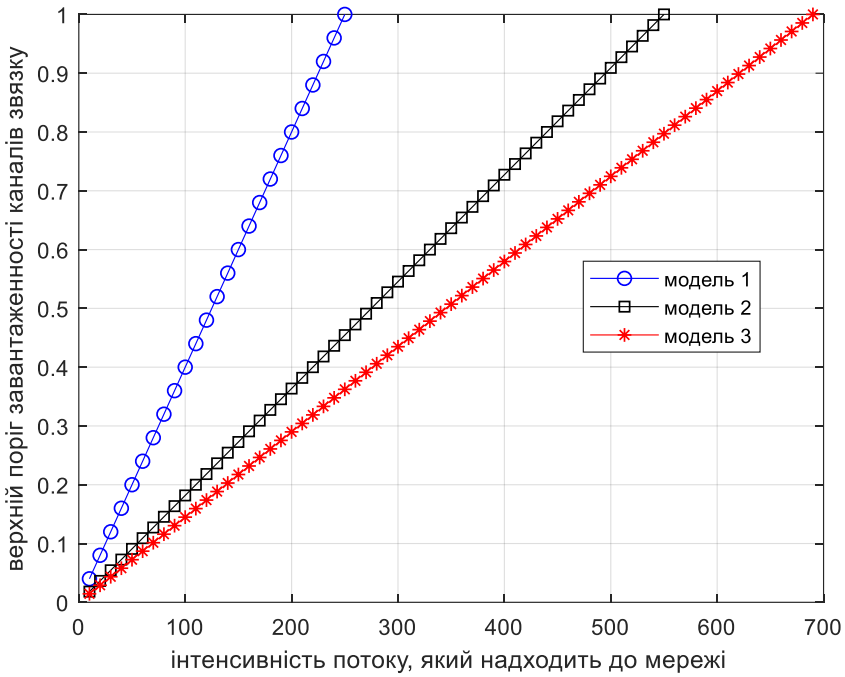


Рисунок 2.10 – Динаміка зміни верхнього порогу завантаженості каналів зв'язку ІКМ в залежності від інтенсивності потоку пакетів, який надходив до мережі

2.4 Висновки до другого розділу

У даному розділі описано вдосконалену математичну модель балансування навантаження в ІКМ, що заснована на принципах концепції Traffic Engineering. Описана модель (2.1)-(2.10) математично формалізує побудову ІКМ, де кожна мережа доступу комутується одночасно не до одного а до декількох приграничних маршрутизаторів для того, щоб підвисити відмовостійкість. Також було запропоновано забезпечити розподіл трафіка на рівні доступу між декількома приграничними маршрутизаторами, що створюють віртуальний шлюз за замовчуванням, для того щоб покращити рівень балансування навантаження в ІКМ за критерієм (2.10).

Досліджувана математична модель основана на умовах реалізації одно або багатошляхової маршрутизації (2.1) та (2.2); умовах балансування навантаження на рівні доступу (2.3) та (2.4); умовах збереження потоку на рівні доступу (2.5), (2.6) та ІКМ (2.7); умовах запобігання перевантаження каналів зв'язку (2.8) що виступають умовами балансування навантаження в ІКМ. Для описаної моделі задача балансування навантаження в ІКМ сформульована як оптимізаційна задача

змішаного цілочисельного лінійного програмування з критерієм оптимальності (2.10) та обмеженнями, що накладаються на керуючі змінні (2.1)-(2.9).

Проаналізувавши отримані результати, можна стверджувати, що реалізація покладених у модель принципів балансування навантаження може знизити верхній поріг використання каналів зв'язку мережі (2.9) у середньому на 63,77%, порівнюючи з моделлю 1 і на 20,29% порівнюючи з моделлю 2. Балансування навантаження на рівні ІКМ, як у моделі 2, покращує показник (2.9) у порівнянні з моделлю 1 у середньому на 54,55%. В ході дослідження було підтверджено, що балансування навантаження як на рівні ІКМ так і на рівні доступу, підвищує продуктивність мережі у середньому на 25%, порівнюючи з моделлю, де рішення було основане на багатошляховій маршрутизації, але без балансування навантаження на рівні доступу, і в 2,76 разів у порівнянні з рішенням де балансування навантаження на рівні ІКМ було відсутнє.

Загалом, можна зробити висновок, що підтримка балансування навантаження і на рівні доступу і на рівні ІКМ може підвищити показники якості обслуговування, такі як ймовірність втрат пакетів, середня міжкінцева затримка. Саме тому, дана модель була обрана для дослідження у цій роботі.

Одним з головних недоліків описаної вище моделі є неврахування таких мережних показників, як надійність маршрутизаторів. Тому, пропонується взяти модель 3 за основу для дослідження балансування навантаження та відмовостійкої маршрутизації в мережі з проактивним захистом шлюзу за замовчуванням, але при цьому враховувати надійність приграничних маршрутизаторів для підвищення відмовостійкості.

3 ДОСЛІДЖЕННЯ ПРОЦЕСІВ ВІДМОВОСТІЙКОЇ МАРШРУТИЗАЦІЇ З БАЛАНСУВАННЯМ НАВАНТАЖЕННЯ В ІНФОКОМУНІКАЦІЙНІЙ МЕРЕЖІ

3.1 Опис вдосконаленої потокової моделі відмовостійкої маршрутизації з балансуванням навантаження та врахуванням надійності в інфокомунікаційній мережі

У загальному випадку в межах моделі (2.1)-(2.10) балансування навантаження, що надходить в ІКМ з мережі доступу V_p через приграничний маршрутизатор R_j, реалізується шляхом виконання умов [23]:

$$\sum_{k \in K_p^+} \lambda^k y_{p,j}^k = m_{p,j}^+ \sum_{k \in K_p^+} \lambda^k, \tag{3.1}$$

де $m_{p,j}^+$ – метрики балансування, які визначають частку сумарного трафіку, що надходить в ІКМ від мережі доступу V_p через приграничний маршрутизатор R_j. Тобто при визначенні показників балансування повинна бути дотримана рівність

$$\sum_{R_j \in R_p^+} m_{p,j}^+ = 1. \tag{3.2}$$

Якщо балансування навантаження рівномірне (Round-Robin Load-Balancing) відповідна метрика балансування обернено пропорційна до кількості підключених до обраної мережі доступу приграничних маршрутизаторів:

$$m_{p,j}^+ = \frac{1}{\left| R_p^+ \right|}. \tag{3.3}$$

Таким чином, метрики балансування для окремих пригранічних маршрутизаторів, що створюють віртуальний шлюз за замовчуванням для мережі доступу V_p, будуть однаковими. У випадку коли мережа підтримує балансування не тільки на рівні окремих потоків (2.3), але й на рівні пакетів кожного потоку окремо (2.4), то для реалізації алгоритму RR необхідно забезпечити, щоб

$$y_{i,j}^{k} = \frac{1}{\left|R_i^{+}\right|}. \tag{3.4}$$

До того ж, протокол GLBP підтримує зважене балансування навантаження, що в моделі (3.1) відповідає адміністративному встановленню метрик балансування. У цьому дослідженні також пропонується впровадження зваженого балансування навантаження шляхом адаптації метрик балансування відповідно до рівня надійності пригранічних маршрутизаторів.

Нехай коефіцієнт готовності A_i характеризує кожен пригранічний маршрутизатор $R_i \in R^{+}$ відповідно до його рівня надійності. Значення коефіцієнту готовності маршрутизатора визначається як відношення часу, коли він знаходився у працездатному стані, до загального часу його роботи, тобто він приймає значення від нуля до одиниці. Таким чином, для реальзації балансування навантаження з урахуванням надійності пригранічних маршрутизаторів в системі (3.1), у роботі [23] пропонується визначати метрики балансування за такою формулою:

$$m_{p,j}^{+} = \frac{A_j}{\sum\limits_{R_i \in R_p^{+}} A_i},\ R_j \in R_p^{+}. \tag{3.5}$$

Таким чином, у випадку балансування навантаження між інтерфейсами віртуального маршрутизатора більше пакетів буде відправлено на більш надійний мережний пристрій.

Рішення, яке представлене виразами (3.1)-(3.5), відноситься до пригранічних маршрутизаторів, через які трафік надходить до ІКМ. Для випадку балансування навантаження на пригранічному маршрутизаторі R_j, через який

трафік виходить з ІКМ до мережі доступу V_p, застосовуються за аналогією з (3.1), (3.3) та (3.5) такі умови [23]:

$$\sum_{k \in K_p^-} \lambda^k z_{j,p}^k = m_{j,p}^- \sum_{k \in K_p^-} \lambda^k , \tag{3.6}$$

при застосуванні алгоритму Round-Robin:

$$m_{p,j}^- = \frac{1}{\left| R_p^- \right|}, \tag{3.7}$$

при врахуванні коефіцієнтів готовності:

$$m_{j,p}^- = \frac{A_j}{\sum\limits_{R_i \in R_p^+} A_i}, \; R_j \in R_p^+, \tag{3.8}$$

де $m_{j,p}^-$ – метрики балансування, які визначають частку сумарного трафіку, що виходить з ІКМ до мережі доступу V_p через пригранічний маршрутизатор R_j.

Метрики балансування та коефіцієнти готовності пропонується врахувати у процесі проактивної відмовостійкої маршрутизації двома способами. Перший спосіб заснований на тому, що критерій оптимальності маршрутних рішень (2.10) залишається незмінним, а на змінні доступу накладаються додаткові обмеження (3.1), (3.5), (3.6) та (3.8). Це рішення запропоноване у роботі [33] та носить назву RATE (Resilience Aware TE). Другий спосіб стосується перегляду критерія оптимальності (2.10), який приймає таку форму

$$\min_{x,y,z,\alpha} \left(\sum_{k \in K} \sum_{V_p \in V} \sum_{R_i \in R_p^+} (1 - A_i) y_{p,i}^k + \sum_{k \in K} \sum_{V_p \in V} \sum_{R_j \in R_p^-} (1 - A_j) z_{j,p}^k + c_\alpha \alpha \right), \tag{3.9}$$

де c_α – ваговий коефіцієнт, який регулює вплив на оптимальне рішення значення порогу α у порівнянні зі значеннями змінних доступу. При збільшенні вагового коефіцієнта c_α маршрутні рішення будуть наближатись за ефективністю балансування до рішень, які отримуються за допомогою критерія (2.10). Зменшення коефіцієнта c_α посилює вплив на балансування навантаження рівня надійності приграничних маршрутизаторів. Проактивне рішення щодо відмовостійкої маршрутизації, яке базується на моделі (2.1)-(2.9) та критерії оптимальності (3.9) буде мати назву ResMetrTE (Resilience Metrics TE).

Рішення RATE та ResMetrTE будуть порівнюватись з моделлю (2.1)-(2.10), яку скорочено позначимо через TE, а також з рішенням RRTE, при якому до моделі (2.1)-(2.10) додаються умови (3.1), (3.3), (3.6) та (3.7).

3.2 Порівняльний аналіз моделей відмовостійкої маршрутизації з балансуванням навантаження в інфокомунікаційній мережі

В ході роботи було досліджено та порівняно чотири рішення, перше рішення, реалізовано у моделі TE, було описано та досліджено у роботі [12], друге рішення, представлене моделлю RATE з врахуванням надійності, було запропоновано у роботі [23]. Також, було досліджено модель ResMetrTE з врахуванням метрик. У моделі RRTE відтворювався режим роботи протоколу GLBP з налаштуваннями щодо балансування навантаження за замовчуванням. За допомогою верхнього порогу завантаженості каналів зв'язку ІКМ (α) було оцінено ефективність процесу балансування навантаження. Модель TE (2.1)-(2.10) забезпечувала за визначенням мінімальний рівень, що максимально впливало на рівень якості обслуговування та покращувала такі показники як рівень втрат пакетів, продуктивність, середні затримки, та джитер.

Досліджувана структура ІКМ (рис. 3.1), складалась з дванадцяти маршрутизаторів ($R_1 \div R_{12}$), що були з'єднані між собою за допомогою сімнадцяти каналів зв'язку ($v = 17$). Пропускні здатності (1/с) каналів вказані у розривах каналів зв'язку (рис. 3.1). В ході роботи у ІКМ передавався один потік пакетів між першою (V_1) та другою (V_2) мережами доступу. Перша мережа доступу виступала як джерело потоку пакетів, віртуальний маршрутизатор (шлюз за замовчуванням) був представлений інтерфейсами приграничних маршрутизаторів R_1, R_4 та R_7. В свою чергу для другої мережі доступу, яка була

отримувачем потоку пакетів, віртуальний маршрутизатор представляли інтерфейси приграничних маршрутизаторів R_6, R_9 та R_{12}.

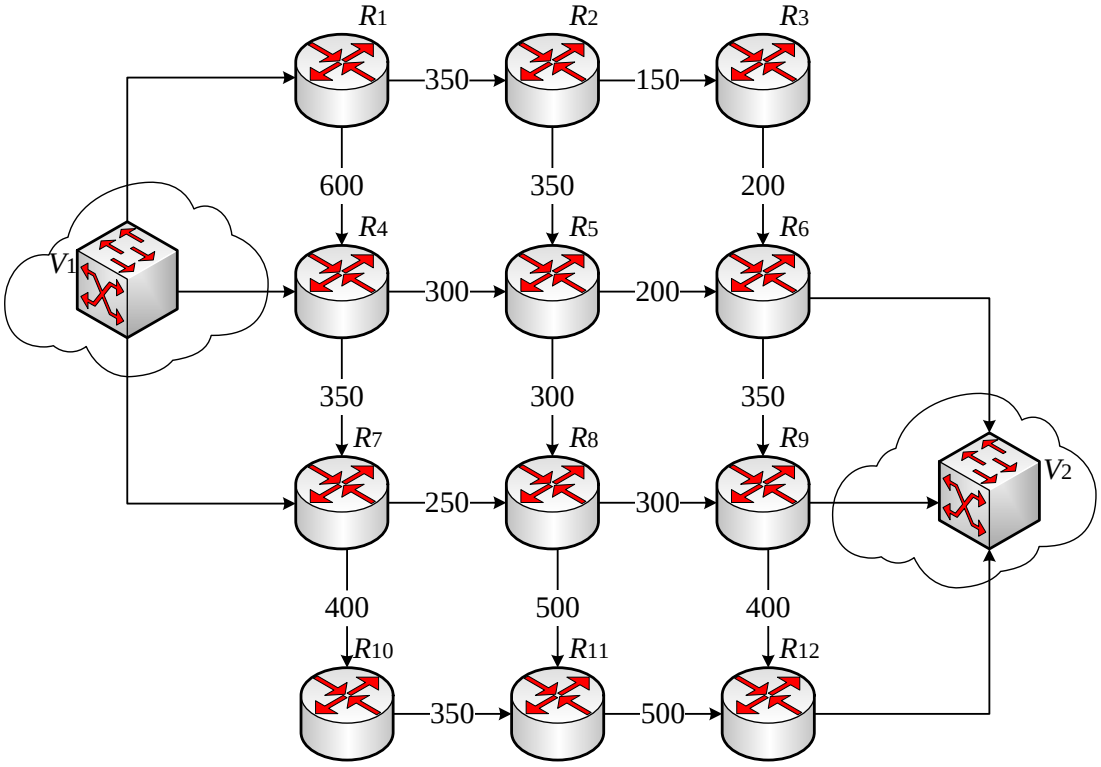


Рисунок 3.1 – Приклад структури ІКМ, яка досліджувалась

В ході дослідження порівнювались три варіанти щодо диференціації рівня надійності приграничних маршрутизаторів (табл. 3.1). Для першого варіанту коефіцієнти готовності приграничних маршрутизаторів приймали значення від 0,9 до 1; в межах другого варіанту – від 0,6 до 1; в межах третього варіанту – від 0,4 до 1.

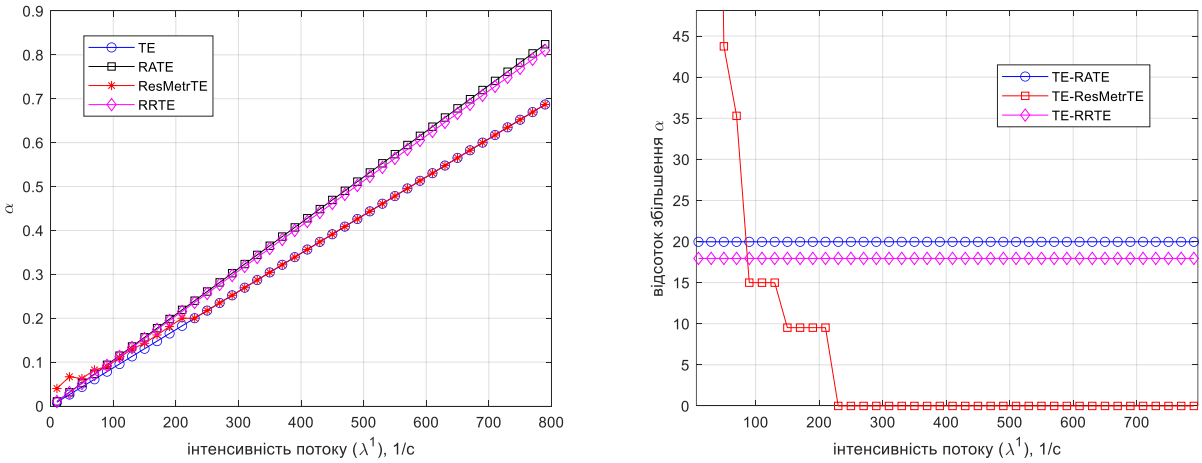
Таблиця 3.1 – Варіанти значень коефіцієнтів готовності приграничних маршрутизаторів ІКМ

Варіант / приграничні маршрутизатори	R_1	R_4	R_6	R_7	R_9	R_{12}
Варіант № 1	0,92	0,95	1	1	0,98	0,94
Варіант № 2	0,6	0,7	0,9	0,9	0,8	0,7
Варіант № 3	0,99	0,7	0,4	0,4	0,8	0,95

Звернемо увагу, що значення коефіцієнтів готовності маршрутизаторів та їх інтерфейсів залежать не тільки від номінальних характеристик, що стосуються заявленої експлуатаційної надійності від виробника, а і поточним станом пристрою, який залежить, наприклад від перевантажень, збоїв щодо електроживлення тощо, що теж впливає на рівень відмов в обслуговуванні.

В ході дослідження інтенсивність потоку між першою та другою мережами доступу змінювалась від 10 до 800 1/с з кроком 20 1/с . На рис. 3.2 зображені результати розрахунків щодо моделювання чотирьох порівнюваних рішень для відмовостійкої маршрутизації та балансування навантаження для вихідних варіантів першого варіанта (табл. 3.1) при c_α=0,4. На рис. 3.2 а показано динаміку зміни верхнього порогу завантаженості каналів зв'язку ІКМ залежності від значення інтенсивності потоку, що надходить від мереж доступу. На рис. 3.2 б продемонстровано, на скільки відсотків збільшиться значення порогу α за використання рішень RATE, ResMetrTE та RRTE у порівнянні з рішенням TE.

З отриманих результатів розрахунків (рис. 3.2) можна зробити висновок, що врахування рівня надійності приграничних маршрутизаторів в межах рішень RATE та ResMetrTE призводить до підвищення порогу завантаженості каналів зв'язку ІКМ, що є нібито платне за підвищення рівня відмовостійкості ІКМ. В межах моделі ResMetrTE врахування рівня надійності маршрутизаторів забезпечувалось при невисокому навантаженні на ІКМ (до 200 1/с включно). Коли ж навантаження на ІКМ зростало (рис. 3.2 б) моделі ResMetrTE та TE давали однаковий результат. До того ж, моделі RATE та RRTE забезпечували приблизно однаковий результат, тому що для першого варіанту вихідних даних (табл. 3.1), коефіцієнти готовності приграничних маршрутизаторів приймали максимально високі значення, і їх значення майже співпадали. Це призводило до того, що метрики балансування (3.3) та (3.5), (3.7) та (3.8) майже не відрізнялись між собою.



а) б)

Рисунок 3.2 – Результати розрахунків щодо реалізації чотирьох порівнюваних рішень щодо відмовостійкої маршрутизації та балансування навантаження для першого варіанта вихідних даних (табл. 3.1)

У табл. 3.2 представлені результати балансування навантаження в ІКМ для чотирьох порівнюваних моделей за умови, що інтенсивність потоку складала 200 1/с. Результати представлені у табл. 2.3 показують чутливість маршрутних рішень RATE та ResMetrTE до рівня надійності приграничних маршрутизаторів. На маршрутизатори з більшим значенням надійності надходило більше навантаження, а на маршрутизатори з меншим значенням надійності приходило менше навантаження. До того ж, у цьому прикладі показано, що рішення RATE забезпечувало диференціацію в завантаженості приграничних маршрутизаторів в залежності від рівня диференціації їх коефіцієнтів готовності. Модель ResMetrTE забезпечувала пропорційний розподіл навантаження в залежності від ранжування маршрутизаторів за рівнем надійності. На маршрутизатор R_7 з найбільшою надійністю надходило вдвічі більше навантаження, ніж на наступний за надійністю маршрутизатор R_4. За тим же принципом, на четвертий маршрутизатор надходило вдвічі вище навантаження ніж на найменш надійний маршрутизатор R_1. Тим часом, на вихідних маршрутизаторах R_6, R_9 та R_{12} в межах моделі ResMetrTE порядок балансування не завжди залежав від рівня їх надійності, що пояснювалось впливом оптимальності маршрутних рішень також порогу α у критерії (3.9). При подальшому збільшенні навантаження, його вплив ставав визначальним, а рішення ResMetrTE зовсім втрачало чутливість до рівня надійності мережного обладнання. У разі зменшення вагового коефіцієнта c_α

вплив порогу α у критерії (3.9) стає слабкішим, а при c_α=0 в межах рішення ResMetrTE будуть використовуватись лише найбільш надійні маршрутизатори з тих, що утворюють віртуальний шлюз за замовчуванням для тієї чи іншої мережі доступу. Маршрутизатори з меншою надійністю почнуть використовуватись тільки за умови перевантаження маршрутів, якщо починаються з найбільш надійного приграничного маршрутизатора.

Таблиця 3.2 – Результати балансування навантаження в ІКМ для чотирьох порівнюваних рішень за умови, що інтенсивність потоку складала 200 1/с

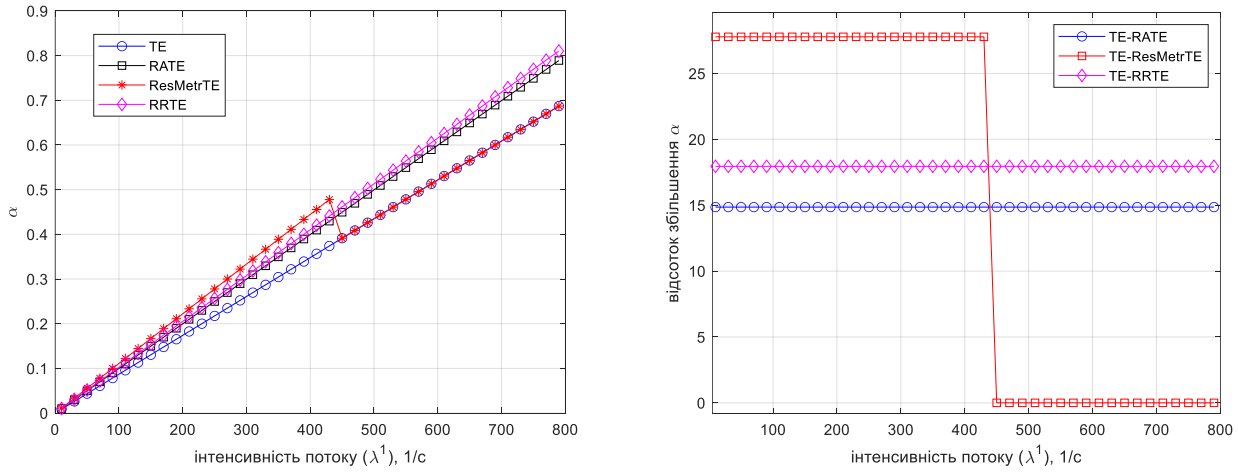
Зв'язки	$\varphi_{i,j}$	Інтенсивності потоку пакетів для різних рішень			
		TE	RATE	ResMetrTE	RRTE
$W_{1,1}^{+}$		60,87	64,11	28,57	66 ⅔
$W_{1,4}^{+}$		52,17	66,20	57,14	66 ⅔
$W_{1,7}^{+}$		86,96	69,69	114,29	66 ⅔
$E_{1,2}$	350	60,87	31,30	28,57	30,77
$E_{2,3}$	150	26,09	31,30	28,57	30,77
$E_{1,4}$	600	0	32,81	0	35,90
$E_{2,5}$	350	34,78	0	0	0
$E_{3,6}$	200	26,09	31,30	28,57	30,77
$E_{4,5}$	300	52,17	52,16	57,14	51,28
$E_{5,6}$	200	34,78	41,73	38,10	41,02
$E_{4,7}$	350	0	46,85	0	51,28
$E_{5,8}$	300	52,17	10,43	19,04	10,26
$E_{6,9}$	350	0	4,53	0	5,13
$E_{7,8}$	250	43,48	52,16	47,62	51,28
$E_{8,9}$	300	52,17	62,59	57,14	61,54
$E_{7,10}$	400	43,48	64,38	66,67	66 ⅔
$E_{8,11}$	500	43,48	0	9,52	0
$E_{9,12}$	400	0	0	0	0

Продовження таблиці 3.2

$E_{10,11}$	350	43,48	64,38	66,67	66 ⅔
$E_{11,12}$	500	86,96	64,38	76,19	66 ⅔
$W_{6,2}^{-}$		60,87	68,50	66,67	66 ⅔
$W_{9,2}^{-}$		52,17	67,12	57,14	66 ⅔
$W_{12,2}^{-}$		86,96	64,38	76,19	66 ⅔

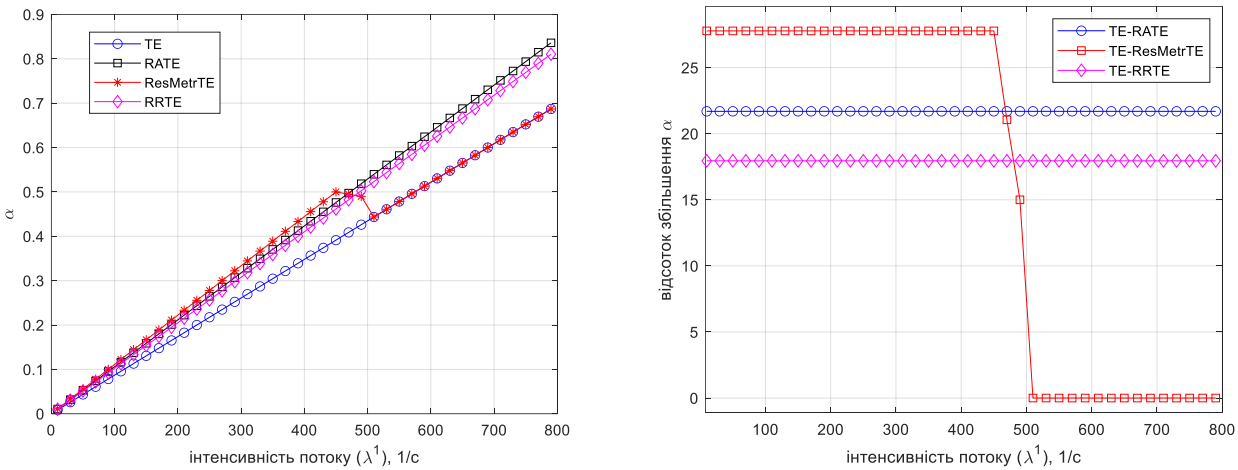
Результати розрахунків щодо реалізації чотирьох порівнюваних рішень щодо відмовостійкої маршрутизації та балансування навантаження для другого варіанта вихідних даних (табл. 3.1) при c_α=15 показано на рис 3.3. У разі реалізації рішень RATE та ResMetrTE, що направлені на врахування рівня надійності приграничних маршрутизаторів, поріг завантаженості каналів зв'язку ІКМ зростав приблизно на 15% та 27,8%. За умови навантаження на мережу в 450 1/с і вище рішення ResMetrTE за наведених вихідних даних втрачало свою чутливість до рівня надійності мережного обладнання.

Для третього варіанта вихідних даних (табл. 3.1) при c_α=15 результати розрахунків щодо реалізації чотирьох порівнюваних рішень щодо відмовостійкої маршрутизації та балансування навантаження представлені на рис. 3.4. При реалізації рішень RATE та ResMetrTE, направлених на врахування рівня надійності приграничних маршрутизаторів, поріг завантаженості каналів зв'язку ІКМ підвищувався приблизно на 21,7% та 27,8%. За умови коли навантаження на мережу вище 500 1/с рішення ResMetrTE за наведених вихідних даних також втрачало свою чутливість до рівня надійності мережного обладнання.



а) б)

Рисунок 3.3 – Результати розрахунків щодо реалізації чотирьох порівнюваних рішень щодо відмовостійкої маршрутизації та балансування навантаження для другого варіанта вихідних даних (табл. 3.1)



а) б)

Рисунок 3.4 – Результати розрахунків щодо реалізації чотирьох порівнюваних рішень щодо відмовостійкої маршрутизації та балансування навантаження для третього варіанта вихідних даних (табл. 3.1)

3.3 Висновки до третього розділу

В ході дослідження було підтверджено, що одним з важливих критеріїв проактивного забезпечення відмовостійкої маршрутизації в ІКМ є підтримка балансування навантаження як на рівні транспортної мережі, так і а рівні доступу за допомогою FHRP.

Так як сучасні протоколи маршрутизації використовують алгоритми пошуку найкоротшого шляху та графові моделі, при розрахунку неможливо задовільнити вимоги, які висуваються до якості обслуговування, такі як пропускна здатність, джитер, середня затримка, ймовірність втрат пакетів. Тому, за основу було взято вдосконалену модель [12], описану у другому розділі цієї роботи.

Однак, для того, щоб забезпечити та підвищити відмовостійкість мережі, потрібно враховувати рівень надійності приграничних маршрутизаторів, між якими балансується навантаження, що надходить від мереж доступу. Тому, було запропоновано вдосконалення існуючих математичних моделей та методів, що складають алгоритмічну основу протоколів відмовостійкої маршрутизації, шляхом врахування надійності приграничних маршрутизаторів мережі.

У розділі було досліджено чотири математичні моделі задачі проактивної відмовостійкої маршрутизації. Всі розглянуті моделі підтримують вимоги концепції Traffic Engineering, і два з розглянутих рішень враховують у явному вигляді рівень надійності приграничних маршрутизаторів, що кількісно характеризується їх коефіцієнтами готовності.

В ході роботи було розв’язано задачі проактивної відмовостійкої маршрутизації на мережній топології (рис. 3.1). Результати досліджень підтвердили чутливість маршрутних рішень RATE та ResMetrTE до рівня надійності приграничних маршрутизаторів, так як саме ці моделі забезпечували такий порядок балансування навантаження, що на найменш надійний приграничний маршрутизатор надходило трафіку менше, а, відповідно, на приграничний маршрутизатор з найбільшим показником надійності приходило трафіку більше.

4 РЕКОМЕНДАЦІЇ ДО ПРАКТИЧНОГО ЗАСТОСУВАННЯ ДОСЛІДЖУВАНИХ РІШЕНЬ НА БАЗІ ПРОТОКОЛУ GLBP

4.1 Приклад налаштування протоколу GLBP з балансуванням навантаження у режимі round robin з використанням пакету GNS3

Створення рекомендацій щодо практичного застосування отриманих рішень у сучасних та перспективних ІКМ є важливим моментом процесу дослідження. Для цього, пропонується задіяти функціонал протоколу відмовостійкої маршрутизації GLBP , у якому керуючі параметри, які відповідають за балансування навантаження, будуть задаватись не емпіричним шляхом, а теоретично обґрунтовано, керуючись результатами розрахунків в межах досліджуваних та проаналізованих у попередніх розділах рішень.

Для перевірки та застосування на практиці отриманих результатів, проведемо експеримент, використовуючи пакет GNS3. Досліджуваний фрагмент мережі складається з трьох маршрутизаторів R1-R3 та двох комутаторів, підключених між собою через порти Fast Ethernet. До першого комутатора підключено сім робочих станцій PC1-PC7. До другого комутатора підключена одна робоча станція PC8. Схема мережі, для дослідження протоколу GLBP наведена на рис. 4.1.

На рис 4.2. Наведено приклад налаштування для робочої станції PC1. Віртуальний маршрутизатор, що виконує функції шлюзу за замовчуванням для семи робочих станцій PC1-PC7, створений у межах 192-ї GLBP групи, та має IP-адресу 192.168.0.254/24 (див. табл. 4.1).

Таблиця 4.1 – Дані для налаштування кінцевих станцій

Параметр/кінцева станція	IP-адреса	Маска мережі	Шлюз за замовчуванням
PC1	192.168.0.1	255.255.255.0	192.168.0.254
PC2	192.168.0.2	255.255.255.0	192.168.0.254
PC3	192.168.0.3	255.255.255.0	192.168.0.254
PC4	192.168.0.4	255.255.255.0	192.168.0.254
PC5	192.168.0.5	255.255.255.0	192.168.0.254

Продовження таблиці 4.1

PC6	192.168.0.6	255.255.255.0	192.168.0.254
PC7	192.168.0.7	255.255.255.0	192.168.0.254
PC8	10.0.2.1	255.255.255.0	10.0.2.254

Для того, щоб налаштувати протокол GLBP на маршрутизаторах мережі, були прописані наступні команди для маршрутизаторів R1-R3 відповідно, як показано на рис 4.3-4.5. На інтерфейсах маршрутизаторів R1-R3 Fast Ethernet 0/0 була налаштована 192-а GLBP група у режимі round robin, і відповідно на інтерфейсах Fast Ethernet 0/1 було налаштовано 10-ту GLBP група у режимі round robin, що означає, що трафік повинен розподілятися між маршрутизаторами порівну.

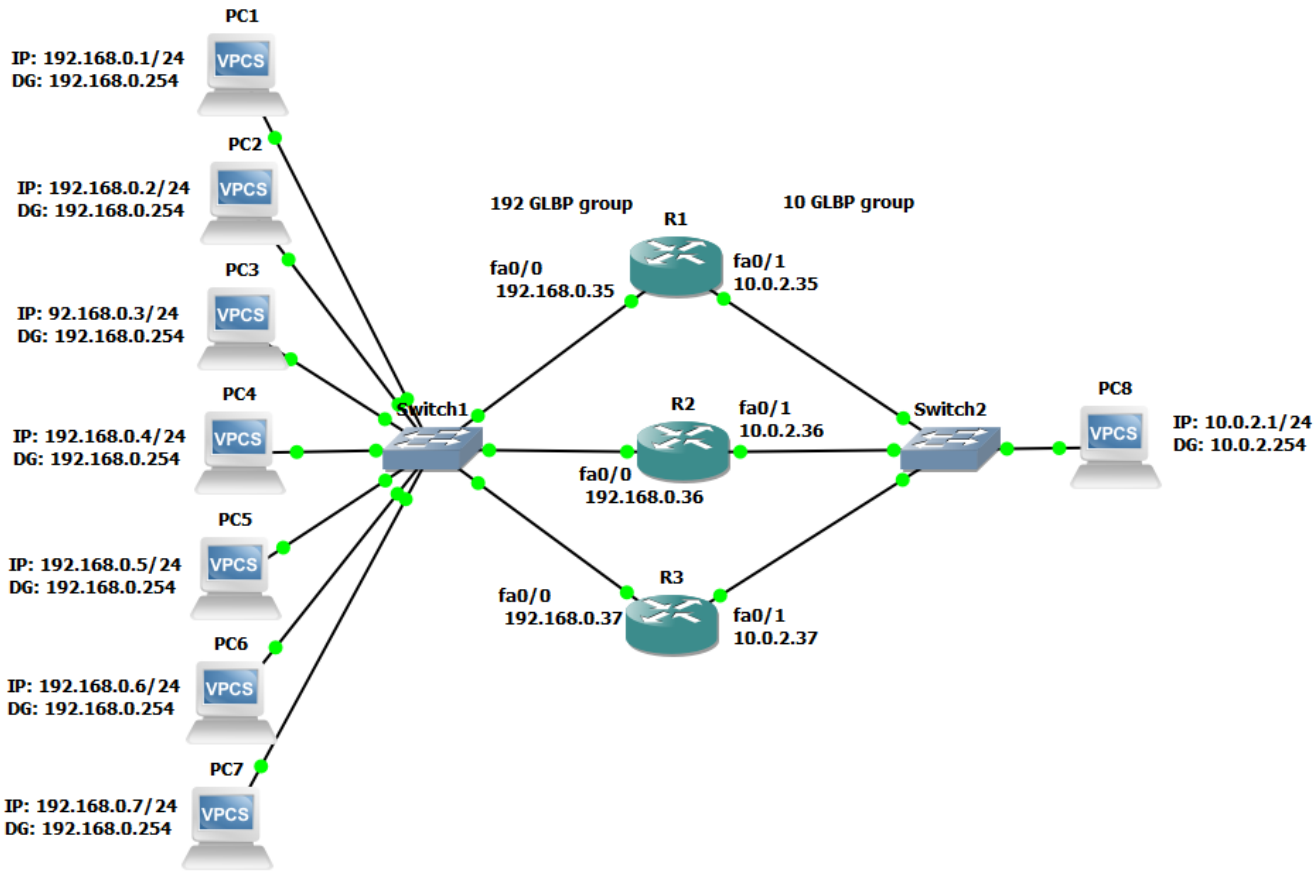


Рисунок 4.1 – Схема для дослідження протоколу GLBP

```
PC1> ip 192.168.0.1/24 192.168.0.254
Checking for duplicate address...
PC1 : 192.168.0.1 255.255.255.0 gateway 192.168.0.254

PC1> show

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC1    192.168.0.1/24       192.168.0.254     00:50:79:66:68:00  10042  127.0.0.1:10043
       fe80::250:79ff:fe66:6800/64

PC1>
```

Рисунок 4.2 – Приклад налаштування IP-адреси, маски та шлюзу за замовчуванням PC1

На інтерфейсах маршрутизатора R1 Fast Ethernet 0/0 та Fast Ethernet 0/1 було прописано IP адреси 192.168.0.35 та 10.0.2.35 відповідно за допомогою команди «ip address». Також, було присвоєно маску 255.255.255.0. Для того щоб налаштувати віртуальний шлюз за замовчуванням для маршрутизатора R1 були використані команди «glbp 192 ip 192.168.0.254» та «glbp 10 ip 10.0.2.254».

На інтерфейсах маршрутизатора R1 Fast Ethernet 0/0 та Fast Ethernet 0/1 було прописано IP адреси 192.168.0.35 та 10.0.2.35 відповідно за допомогою команди «ip address». Також, було присвоєно маску 255.255.255.0. Для того щоб налаштувати віртуальний шлюз за замовчуванням для маршрутизатора R1 були використані команди «glbp 192 ip 192.168.0.254» та «glbp 10 ip 10.0.2.254».

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int fa 0/0
R1(config-if)#ip address 192.168.0.35 255.255.255.0
R1(config-if)#glbp 192 ip 192.168.0.254
R1(config-if)#glbp 192 load-balancing round-robin
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
R1(config)#int fa 0/1
R1(config-if)#ip address 10.0.2.35 255.255.255.0
R1(config-if)#glbp 10 ip 10.0.2.254
R1(config-if)#glbp 10 load-balancing round-robin
R1(config-if)#no shutdown
R1(config-if)#exit
```

Рисунок 4.3 – Приклад налаштування протоколу GLPB на маршрутизаторі R1

На інтерфейсах маршрутизатора R2 Fast Ethernet 0/0 та Fast Ethernet 0/1 було прописано IP адреси 192.168.0.36 та 10.0.2.36 відповідно за допомогою команди

«ip address». Також, було присвоєно маску 255.255.255.0. Для того щоб налаштувати віртуальний шлюз за замовчуванням для маршрутизатора R2 були використані команди «glbp 192 ip 192.168.0.254» та «glbp 10 ip 10.0.2.254»

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int fa 0/0
R2(config-if)#ip address 192.168.0.36 255.255.255.0
R2(config-if)#glbp 192 ip 192.168.0.254
R2(config-if)#glbp 192 load-balancing round-robin
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
R2(config)#int fa 0/1
R2(config-if)#ip address 10.0.2.36 255.255.255.0
R2(config-if)#glbp 10 ip 10.0.2.254
R2(config-if)#glbp 10 load-balancing round-robin
R2(config-if)#no shutdown
R2(config-if)#exit
```

Рисунок 4.4 – Приклад налаштування протоколу GLPB на маршрутизаторі R2

На інтерфейсах маршрутизатора R3 Fast Ethernet 0/0 та Fast Ethernet 0/1 було прописано IP адреси 192.168.0.37 та 10.0.2.37 відповідно за допомогою команди «ip address». Також, було присвоєно маску 255.255.255.0. Для того щоб налаштувати віртуальний шлюз за замовчуванням для маршрутизатора R2 були використані команди «glbp 192 ip 192.168.0.254» та «glbp 10 ip 10.0.2.254»

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int fa 0/0
R3(config-if)#ip address 192.168.0.37 255.255.255.0
R3(config-if)#glbp 192 ip 192.168.0.254
R3(config-if)#glbp 192 load-balancing round-robin
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#
R3(config)#int fa 0/1
R3(config-if)#ip address 10.0.2.37 255.255.255.0
R3(config-if)#glbp 10 ip 10.0.2.254
R3(config-if)#glbp 10 load-balancing round-robin
R3(config-if)#no shutdown
R3(config-if)#exit
```

Рисунок 4.5 – Приклад налаштування протоколу GLPB на маршрутизаторі R3

Для перевірки налаштувань інтерфейсів маршрутизаторів була використана команда «show ip interface brief». Результати перевірки представлено на рис. 4.6-

4.8. З отриманих даних можна зробити висновок, що інтерфейси маршрутизаторів було налаштовано правильно.

```
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.0.35    YES NVRAM  up                    up
FastEthernet0/1            10.0.2.35       YES NVRAM  up                    up
R1#
```

Рисунок 4.6 – Приклад перевірки налаштованих IP адрес на маршрутизаторі R1

```
R2#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.0.36    YES NVRAM  up                    up
FastEthernet0/1            10.0.2.36       YES NVRAM  up                    up
R2#
```

Рисунок 4.7 – Приклад перевірки налаштованих IP адрес на маршрутизаторі R2

```
R3#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.0.37    YES NVRAM  up                    up
FastEthernet0/1            10.0.2.37       YES NVRAM  up                    up
R3#
```

Рисунок 4.8 – Приклад перевірки налаштованих IP адрес на маршрутизаторі R3

Для перевірки роботи балансування навантаження було використано протокол ICMP, а саме повідомлення Echo Request. Для підрахунку (реєстрації) пакетів ICMP, які надійшли на обраний інтерфейс маршрутизатора, було створено списки контролю доступу (Access Control List, ACL), як показано на рис. 4.9-4.11.

Для того, щоб налаштувати списки контролю доступу було використано наступні команди: «access-list *номер* permit icmp *адреса мережі відправника обернена маска підмережі адреса мережі отримувача обернена маска підмережі*».

Команда «access-list *номер* permit ip any any» (рис. 4.9-4.11) була використана з метою запобігання блокування трафіка, який передається не за допомогою протоколу ICMP.

Надалі, на відповідних вхідних інтерфейсах Fast Ethernet 0/0 маршрутизаторів R1-R3 було сконфігуровано налаштовані списки контролю доступу.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 111 permit icmp 192.168.0.1 0.0.0.0 10.0.2.0 0.0.0.255
R1(config)#access-list 111 permit icmp 192.168.0.2 0.0.0.0 10.0.2.0 0.0.0.255
R1(config)#access-list 111 permit icmp 192.168.0.3 0.0.0.0 10.0.2.0 0.0.0.255
R1(config)#access-list 111 permit icmp 192.168.0.4 0.0.0.0 10.0.2.0 0.0.0.255
R1(config)#access-list 111 permit icmp 192.168.0.5 0.0.0.0 10.0.2.0 0.0.0.255
R1(config)#access-list 111 permit icmp 192.168.0.6 0.0.0.0 10.0.2.0 0.0.0.255
R1(config)#access-list 111 permit icmp 192.168.0.7 0.0.0.0 10.0.2.0 0.0.0.255
R1(config)#access-list 111 permit ip any any
R1(config)#
R1(config)#int fa 0/0
R1(config-if)#ip access-group 111 in
R1(config-if)#exit
R1(config)#
```

Рисунок 4.9 – Приклад налаштування листів контролю доступу на маршрутизаторі R1

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 111 permit icmp 192.168.0.1 0.0.0.0 10.0.2.0 0.0.0.255
R2(config)#access-list 111 permit icmp 192.168.0.2 0.0.0.0 10.0.2.0 0.0.0.255
R2(config)#access-list 111 permit icmp 192.168.0.3 0.0.0.0 10.0.2.0 0.0.0.255
R2(config)#access-list 111 permit icmp 192.168.0.4 0.0.0.0 10.0.2.0 0.0.0.255
R2(config)#access-list 111 permit icmp 192.168.0.5 0.0.0.0 10.0.2.0 0.0.0.255
R2(config)#access-list 111 permit icmp 192.168.0.6 0.0.0.0 10.0.2.0 0.0.0.255
R2(config)#access-list 111 permit icmp 192.168.0.7 0.0.0.0 10.0.2.0 0.0.0.255
R2(config)#access-list 111 permit ip any any
R2(config)#
R2(config)#int fa 0/0
R2(config-if)#ip access-group 111 in
R2(config-if)#exit
R2(config)#
```

Рисунок 4.10 – Приклад налаштування листів контролю доступу на маршрутизаторі R2

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 111 permit icmp 192.168.0.1 0.0.0.0 10.0.2.0 0.0.0.255
R3(config)#access-list 111 permit icmp 192.168.0.2 0.0.0.0 10.0.2.0 0.0.0.255
R3(config)#access-list 111 permit icmp 192.168.0.3 0.0.0.0 10.0.2.0 0.0.0.255
R3(config)#access-list 111 permit icmp 192.168.0.4 0.0.0.0 10.0.2.0 0.0.0.255
R3(config)#access-list 111 permit icmp 192.168.0.5 0.0.0.0 10.0.2.0 0.0.0.255
R3(config)#access-list 111 permit icmp 192.168.0.6 0.0.0.0 10.0.2.0 0.0.0.255
R3(config)#access-list 111 permit icmp 192.168.0.7 0.0.0.0 10.0.2.0 0.0.0.255
R3(config)#access-list 111 permit ip any any
R3(config)#
R3(config)#int fa 0/0
R3(config-if)#ip access-group 111 in
R3(config-if)#exit
R3(config)#
```

Рисунок 4.11 – Приклад налаштування листів контролю доступу на маршрутизаторі R3

Після підключення списків контролю доступу до відповідних інтерфейсів, можна переглядати кількість спрацьовувань правил згідно ACL під час прибуття на інтерфейси ICMP-пакетів, що направляються до мережі призначення.

Щоб перевірити роботу протоколу GLBP у режимі round robin, було проведено два однакові експерименти. В ході перевірки балансування навантаження, за допомогою команди ping, було надіслано по 5 пакетів з кожного комп'ютера PC1-PC7 на комп'ютер PC8 як показано на рис. 4.12.

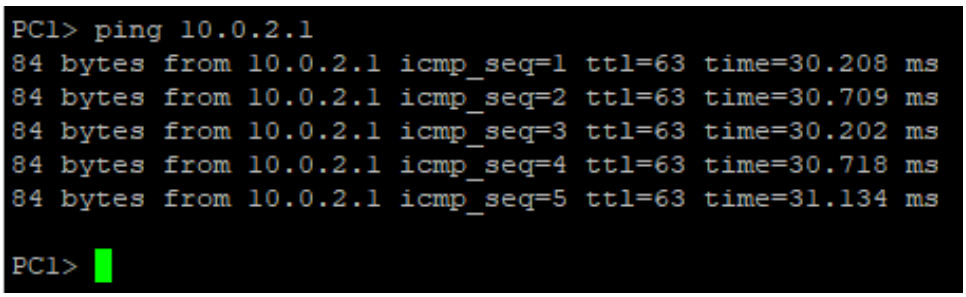


Рисунок 4.12 – Приклад команди ping на робочий станції PC1

Для перевірки налаштованих списків контролю доступу, було використано команду «show access-lists» для всіх маршрутизаторів, як показано на рис. 4.13-4.18. Щоб очистити списки контролю доступу, використано команду «clear ip access-list counters».

З отриманих результатів можна зробити висновок, що балансування навантаження налаштовано у режимі round-robin вірно. Під час першого експерименту пакети були розподілені у такому порядку між маршрутизаторами:

З комп’ютерів PC1, PC4, PC7 –> на маршрутизатор R1 (рис. 4.13);

З комп’ютерів PC2, PC5 –> на маршрутизатор R2 (рис. 4.14);

З комп’ютерів PC3, PC6 –> на маршрутизатор R3 (рис. 4.15).

Під час другого експерименту трафік був розподілений таким чином:

З комп’ютерів PC3, PC6 –> на маршрутизатор R1 (рис. 4.16);

З комп’ютерів PC1, PC4, PC7 –> на маршрутизатор R2 (рис. 4.17);

З комп’ютерів PC2, PC5 –> на маршрутизатор R3(рис. 4.18).

```
R1#show access-lists
Extended IP access list 111
    10 permit icmp host 192.168.0.1 10.0.2.0 0.0.0.255 (5 matches)
    20 permit icmp host 192.168.0.2 10.0.2.0 0.0.0.255
    30 permit icmp host 192.168.0.3 10.0.2.0 0.0.0.255
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255 (5 matches)
    50 permit icmp host 192.168.0.5 10.0.2.0 0.0.0.255
    60 permit icmp host 192.168.0.6 10.0.2.0 0.0.0.255
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255 (5 matches)
    80 permit ip any any (246 matches)
R1#clear ip access-list counters
```

Рисунок 4.13 – Приклад перевірки списків контролю доступу на маршрутизаторі R1 при першому експерименті

```
R2#clear ip access-list counters

R2#show access-lists
Extended IP access list 111
    10 permit icmp host 192.168.0.1 10.0.2.0 0.0.0.255
    20 permit icmp host 192.168.0.2 10.0.2.0 0.0.0.255 (5 matches)
    30 permit icmp host 192.168.0.3 10.0.2.0 0.0.0.255
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255
    50 permit icmp host 192.168.0.5 10.0.2.0 0.0.0.255 (5 matches)
    60 permit icmp host 192.168.0.6 10.0.2.0 0.0.0.255
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255
    80 permit ip any any (246 matches)
R2#clear ip access-list counters
```

Рисунок 4.14 – Приклад перевірки списків контролю доступу на маршрутизаторі R2 при першому експерименті

```
R3#clear ip access-list counters

R3#show access-lists
Extended IP access list 111
    10 permit icmp host 192.168.0.1 10.0.2.0 0.0.0.255
    20 permit icmp host 192.168.0.2 10.0.2.0 0.0.0.255
    30 permit icmp host 192.168.0.3 10.0.2.0 0.0.0.255 (5 matches)
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255
    50 permit icmp host 192.168.0.5 10.0.2.0 0.0.0.255
    60 permit icmp host 192.168.0.6 10.0.2.0 0.0.0.255 (5 matches)
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255
    80 permit ip any any (246 matches)
R3#clear ip access-list counters
```

Рисунок 4.15 – Приклад перевірки списків контролю доступу на маршрутизаторі R3 при першому експерименті

```
R1#show access-lists
Extended IP access list 111
    10 permit icmp host 192.168.0.1 10.0.2.0 0.0.0.255
    20 permit icmp host 192.168.0.2 10.0.2.0 0.0.0.255
    30 permit icmp host 192.168.0.3 10.0.2.0 0.0.0.255 (5 matches)
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255
    50 permit icmp host 192.168.0.5 10.0.2.0 0.0.0.255
    60 permit icmp host 192.168.0.6 10.0.2.0 0.0.0.255 (5 matches)
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255
    80 permit ip any any (93 matches)
R1#clear ip access-list counters
```

Рисунок 4.16 – Приклад перевірки списків контролю доступу на маршрутизаторі R1 при другому експерименті

```
R2#show access-lists
Extended IP access list 111
    10 permit icmp host 192.168.0.1 10.0.2.0 0.0.0.255 (5 matches)
    20 permit icmp host 192.168.0.2 10.0.2.0 0.0.0.255
    30 permit icmp host 192.168.0.3 10.0.2.0 0.0.0.255
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255 (5 matches)
    50 permit icmp host 192.168.0.5 10.0.2.0 0.0.0.255
    60 permit icmp host 192.168.0.6 10.0.2.0 0.0.0.255
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255 (5 matches)
    80 permit ip any any (102 matches)
R2#clear ip access-list counters
```

Рисунок 4.17 – Приклад перевірки списків контролю доступу на маршрутизаторі R2 при другому експерименті

```
R3#show access-lists
Extended IP access list 111
    10 permit icmp host 192.168.0.1 10.0.2.0 0.0.0.255
    20 permit icmp host 192.168.0.2 10.0.2.0 0.0.0.255 (5 matches)
    30 permit icmp host 192.168.0.3 10.0.2.0 0.0.0.255
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255
    50 permit icmp host 192.168.0.5 10.0.2.0 0.0.0.255 (5 matches)
    60 permit icmp host 192.168.0.6 10.0.2.0 0.0.0.255
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255
    80 permit ip any any (102 matches)
R3#clear ip access-list counters
```

Рисунок 4.18 – Приклад перевірки списків контролю доступу на маршрутизаторі R3 при другому експерименті

Розподіл трафіку показано графічно на рис. 4.19-4.20.

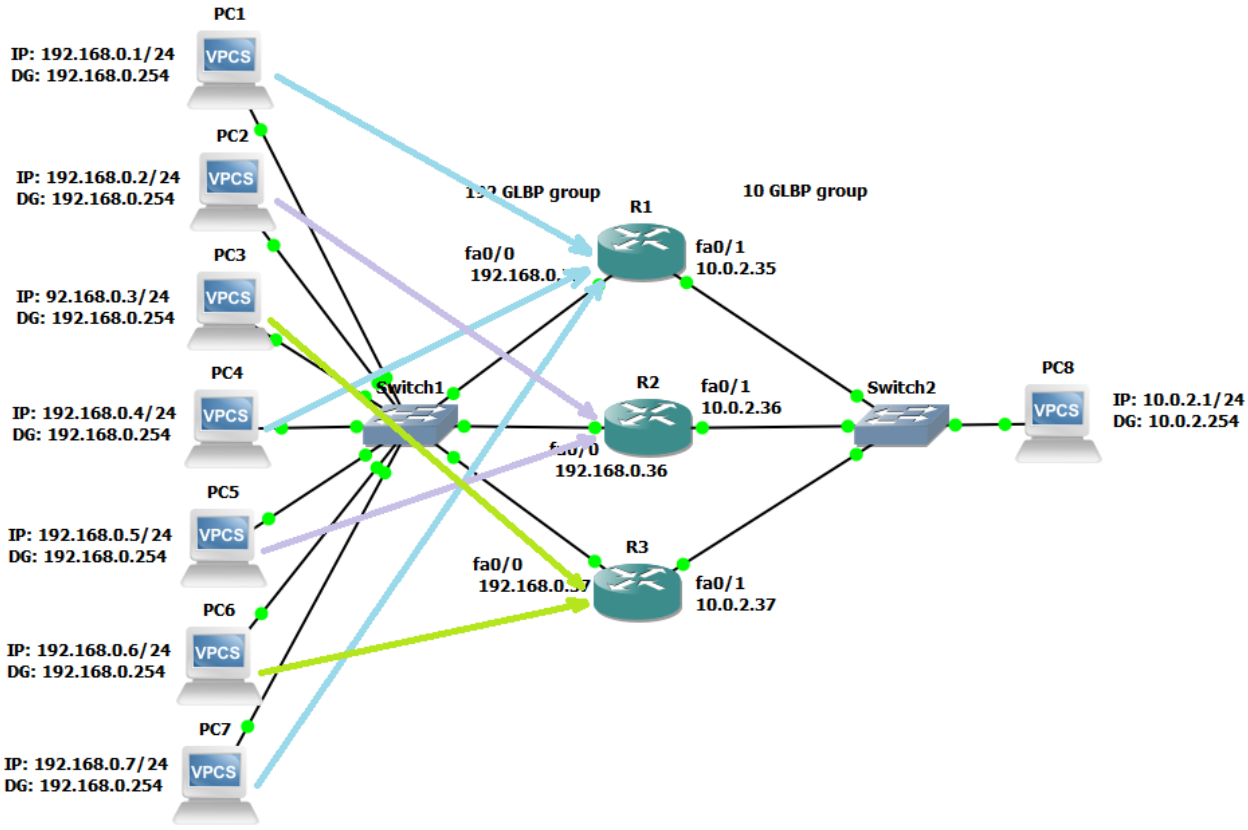


Рисунок 4.19 – Схема мережі з розподілом трафіку для першого експерименту

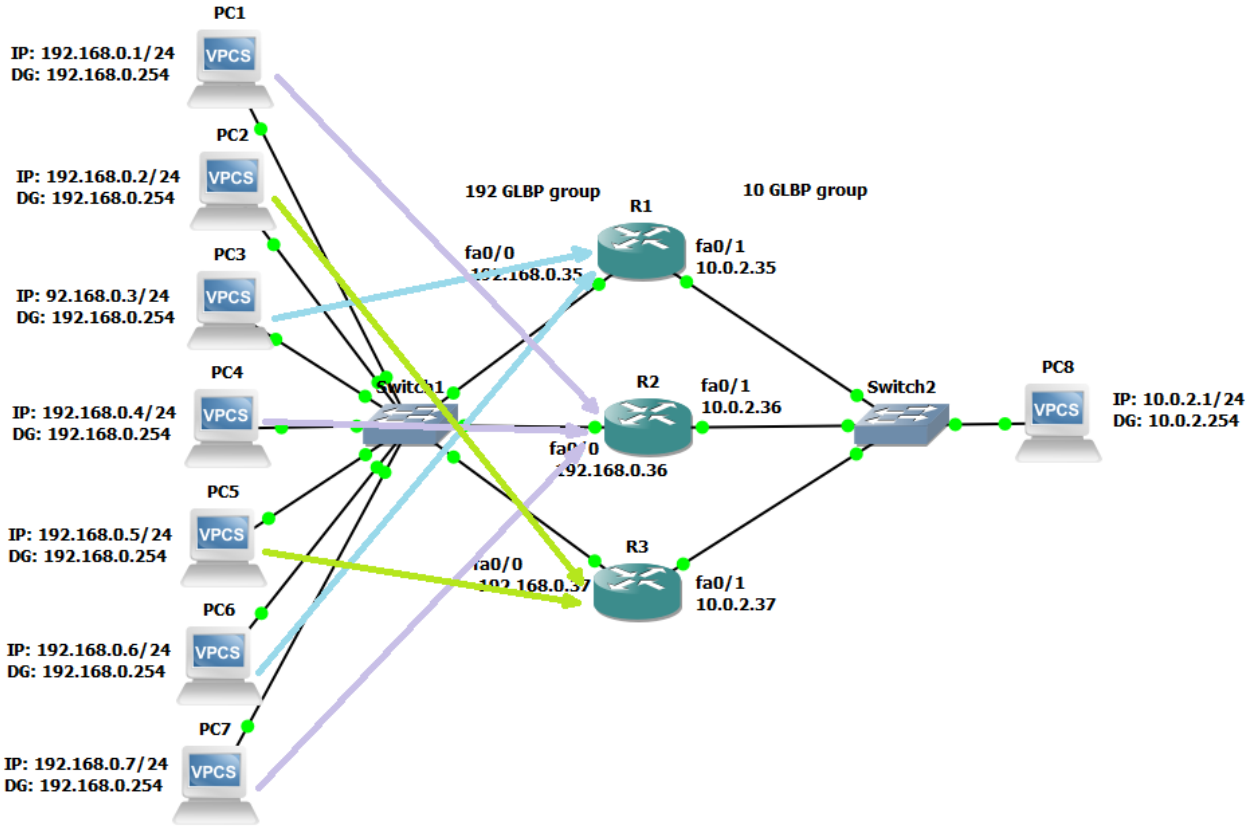


Рисунок 4.20 – Схема мережі з розподілом трафіку для другого експерименту

Щоб перевірити налаштування протоколу GLBP, було використано команду «show glbp» як показано на рис. 4.21-4.23.

На рис. 4.16 наведені такі позначення: 1 – назва GLBP групи; 2 – Роутер R1 має статус «Listen»; 3 – налаштований віртуальний адрес; 4 – режим балансування навантаження; 5 – Forwarder R1 має налаштований статус «Listen»; 6 – R2 має статус «Listen»; : 7 – R3 має статус «Active»; 8 – назва GLBP групи; 9 –R1 має налаштований статус «Listen»; 10 – налаштований віртуальний адрес; 11 – режим балансування навантаження; 12 – Forwarder R1 має налаштований статус «Listen»; 13 – R2 має статус «Listen»; 14 – R3 має статус «Active».

На рис. 4.17 наведені такі позначення: 1 – назва GLBP групи; 2 – Роутер R1 має статус «Listen»; 3 – налаштований віртуальний адрес; 4 – режим балансування навантаження; 5 – Forwarder R1 має налаштований статус «Listen»; 6 – R2 має статус «Active»; : 7 – R3 має статус «Listen»; 8 – назва GLBP групи; 9 –R1 має налаштований статус «Listen»; 10 – налаштований віртуальний адрес; 11 – режим балансування навантаження; 12 – Forwarder R1 має налаштований статус «Listen»; 13 – R2 має статус «Active»; 14 – R3 має статус «Listen».

На рис. 4.18 наведені такі позначення: 1 – назва GLBP групи; 2 – Роутер R1 має статус «Listen»; 3 – налаштований віртуальний адрес; 4 – режим балансування навантаження; 5 – Forwarder R1 має налаштований статус «Active»; 6 – R2 має статус «Listen»; : 7 – R3 має статус «Listen»; 8 – назва GLBP групи; 9 –R1 має налаштований статус «Listen»; 10 – налаштований віртуальний адрес; 11 – режим балансування навантаження; 12 – Forwarder R1 має налаштований статус «Active»; 13 – R2 має статус «Listen»; 14 – R3 має статус «Listen».

```
R1#show glbp
FastEthernet0/0 - Group 192   1
  State is Listen   2
  Virtual IP address is 192.168.0.254   3
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.888 secs
  Redirect time 600 sec, forwarder timeout 14400 sec
  Preemption disabled
  Active is 192.168.0.37, priority 100 (expires in 7.176 sec)
  Standby is 192.168.0.36, priority 100 (expires in 8.080 sec)
  Priority 100 (default)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin   4
  Group members:
    c001.33a0.0000 (192.168.0.35) local
    c002.4948.0000 (192.168.0.36)
    c003.44ec.0000 (192.168.0.37)
  There are 3 forwarders (1 active)
  Forwarder 1
    State is Listen   5
    MAC address is 0007.b400.c001 (learnt)
    Owner ID is c003.44ec.0000
    Time to live: 14397.164 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 192.168.0.37 (primary), weighting 100 (expires in 8.252 sec)
  Forwarder 2
    State is Listen   6
    MAC address is 0007.b400.c002 (learnt)
    Owner ID is c002.4948.0000
    Time to live: 14399.392 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 192.168.0.36 (primary), weighting 100 (expires in 9.392 sec)
  Forwarder 3
    State is Active   7
      1 state change, last state change 00:08:13
    MAC address is 0007.b400.c003 (default)
    Owner ID is c001.33a0.0000
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100
FastEthernet0/1 - Group 10   8
  State is Listen   9
  Virtual IP address is 10.0.2.254   10
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.124 secs
  Redirect time 600 sec, forwarder timeout 14400 sec
  Preemption disabled
  Active is 10.0.2.37, priority 100 (expires in 8.232 sec)
  Standby is 10.0.2.36, priority 100 (expires in 9.596 sec)
  Priority 100 (default)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin   11
  Group members:
    c001.33a0.0001 (10.0.2.35) local
    c002.4948.0001 (10.0.2.36)
    c003.44ec.0001 (10.0.2.37)
  There are 3 forwarders (1 active)
  Forwarder 1
    State is Listen   12
    MAC address is 0007.b400.0a01 (learnt)
    Owner ID is c003.44ec.0001
    Time to live: 14398.508 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 10.0.2.37 (primary), weighting 100 (expires in 8.508 sec)
  Forwarder 2
    State is Listen   13
    MAC address is 0007.b400.0a02 (learnt)
    Owner ID is c002.4948.0001
    Time to live: 14399.580 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 10.0.2.36 (primary), weighting 100 (expires in 9.576 sec)
  Forwarder 3
    State is Active   14
      1 state change, last state change 00:08:20
    MAC address is 0007.b400.0a03 (default)
    Owner ID is c001.33a0.0001
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100
R1#
```

Рисунок 4.21 – Перевірка налаштувань протоколу GLBP на маршрутизаторі R1

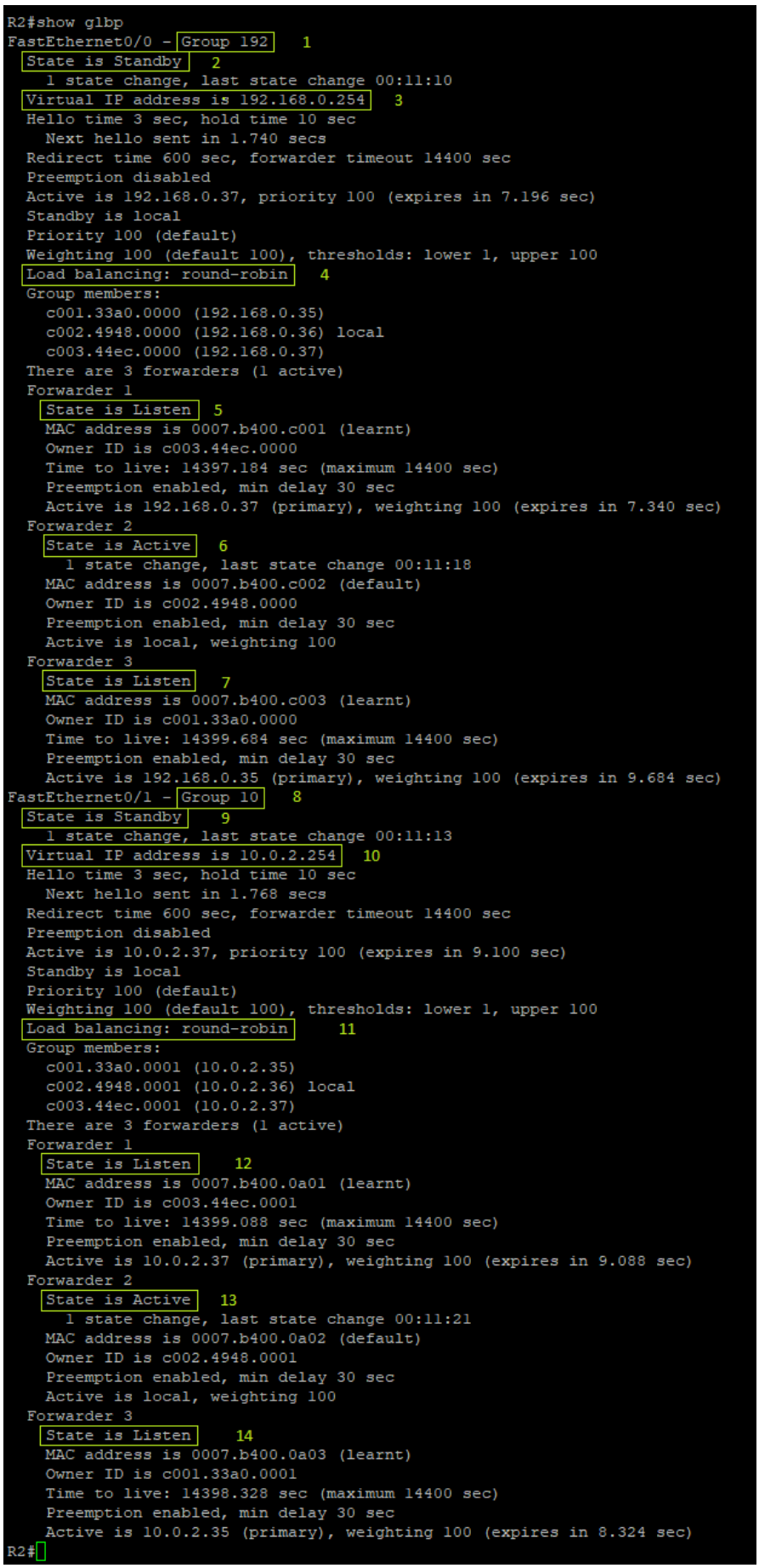


Рисунок 4.22 – Перевірка налаштувань протоколу GLBP на маршрутизаторі R2

```
R3#show glbp
FastEthernet0/0 - Group 192   1
  State is Active   2
    2 state changes, last state change 00:14:12
  Virtual IP address is 192.168.0.254    3
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.512 secs
  Redirect time 600 sec, forwarder timeout 14400 sec
  Preemption disabled
  Active is local
  Standby is 192.168.0.36, priority 100 (expires in 8.984 sec)
  Priority 100 (default)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin   4
  Group members:
    c001.33a0.0000 (192.168.0.35)
    c002.4948.0000 (192.168.0.36)
    c003.44ec.0000 (192.168.0.37) local
  There are 3 forwarders (1 active)
  Forwarder 1
    State is Active   5
      1 state change, last state change 00:14:02
    MAC address is 0007.b400.c001 (default)
    Owner ID is c003.44ec.0000
    Redirection enabled
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100
  Forwarder 2
    State is Listen   6
    MAC address is 0007.b400.c002 (learnt)
    Owner ID is c002.4948.0000
    Redirection enabled, 596.668 sec remaining (maximum 600 sec)
    Time to live: 14396.668 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 192.168.0.36 (primary), weighting 100 (expires in 6.664 sec)
  Forwarder 3
    State is Listen   7
    MAC address is 0007.b400.c003 (learnt)
    Owner ID is c001.33a0.0000
    Redirection enabled, 598.132 sec remaining (maximum 600 sec)
    Time to live: 14398.128 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 192.168.0.35 (primary), weighting 100 (expires in 8.128 sec)
FastEthernet0/1 - Group 10    8
  State is Active    9
    2 state changes, last state change 00:14:14
  Virtual IP address is 10.0.2.254    10
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.524 secs
  Redirect time 600 sec, forwarder timeout 14400 sec
  Preemption disabled
  Active is local
  Standby is 10.0.2.36, priority 100 (expires in 7.844 sec)
  Priority 100 (default)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin   11
  Group members:
    c001.33a0.0001 (10.0.2.35)
    c002.4948.0001 (10.0.2.36)
    c003.44ec.0001 (10.0.2.37) local
  There are 3 forwarders (1 active)
  Forwarder 1
    State is Active    12
      1 state change, last state change 00:14:07
    MAC address is 0007.b400.0a01 (default)
    Owner ID is c003.44ec.0001
    Redirection enabled
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100
  Forwarder 2
    State is Listen   13
    MAC address is 0007.b400.0a02 (learnt)
    Owner ID is c002.4948.0001
    Redirection enabled, 599.260 sec remaining (maximum 600 sec)
    Time to live: 14399.256 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 10.0.2.36 (primary), weighting 100 (expires in 9.252 sec)
  Forwarder 3
    State is Listen    14
    MAC address is 0007.b400.0a03 (learnt)
    Owner ID is c001.33a0.0001
    Redirection enabled, 596.688 sec remaining (maximum 600 sec)
    Time to live: 14396.684 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 10.0.2.35 (primary), weighting 100 (expires in 6.680 sec)
R3#
```

Рисунок 4.23 – Перевірка налаштувань протоколу GLBP на маршрутизаторі R3

4.2 Приклад налаштування протоколу GLBP з балансуванням навантаження у зваженому режимі з використанням пакету GNS3

Для того щоб налаштувати розподіл трафіку в мережі згідно отриманим розрахункам, будемо використовувати вагові коефіцієнти, а саме налаштуємо маршрутизатори у зваженому режимі таким чином: R1 – 29, R2 – 57, R3 – 114. В ході налаштування були використані команди «glbp *номер GLBP групи* load-balancing weighted» та «glbp *номер GLBP групи* weighting *ваговий коефіцієнт*» як показано на рис. 4.24-4.26.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int fa 0/0
R1(config-if)#glbp 192 load-balancing weighted
R1(config-if)#glbp 192 weighting 29
R1(config-if)#exit
```

Рисунок 4.24 – Приклад налаштування протоколу GLPB на маршрутизаторі R1

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int fa 0/0
R2(config-if)#glbp 192 load-balancing weighted
R2(config-if)#glbp 192 weighting 57
R2(config-if)#exit
```

Рисунок 4.25 – Приклад налаштування протоколу GLPB на маршрутизаторі R2

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int fa 0/0
R3(config-if)#glbp 192 load-balancing weighted
R3(config-if)#glbp 192 weighting 114
R3(config-if)#exit
```

Рисунок 4.26 – Приклад налаштування протоколу GLPB на маршрутизаторі R3

Щоб перевірити розподіл трафіку між маршрутизаторами, було проведено два експерименти. За допомогою команди ping було надіслано по 5 пакетів з кожного комп'ютера PC1-PC7 на комп'ютер PC8. Правильність розподілу трафіку можна перевірити за допомогою списків контролю доступу як показано на рис. 4.27-4.32.

За результатами перевірки, можна зробити висновок, що балансування навантаження налаштовано вірно у зваженому режимі. Розподіл трафіку між маршрутизаторами є у таких пропорціях: 1/7, 2/7, та 4/7. У першому випадку пакети були розподілені у такому порядку між маршрутизаторами:

З комп'ютера PC3 –> на маршрутизатор R1 (рис. 4.27);

З комп'ютерів PC2, PC6 –> на маршрутизатор R2 (рис. 4.28);

З комп'ютерів PC1, PC4, PC5, PC7 –> на маршрутизатор R3 (рис. 4.29).

У другому випадку трафік був розподілений нступним чином:

З комп'ютера PC1 –> на маршрутизатор R1 (рис. 4.30);

З комп'ютерів PC3, PC6 –> на маршрутизатор R2 (рис. 4.31);

З комп'ютерів PC2, PC4, PC5, PC7 –> на маршрутизатор R3 (рис. 4.32).

```
R1#show access-lists
Extended IP access list 111
    10 permit icmp host 192.168.0.1 10.0.2.0 0.0.0.255
    20 permit icmp host 192.168.0.2 10.0.2.0 0.0.0.255
    30 permit icmp host 192.168.0.3 10.0.2.0 0.0.0.255 (5 matches)
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255
    50 permit icmp host 192.168.0.5 10.0.2.0 0.0.0.255
    60 permit icmp host 192.168.0.6 10.0.2.0 0.0.0.255
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255
    80 permit ip any any (93 matches)
R1#clear ip access-list counters
```

Рисунок 4.27 – Приклад перевірки списків контролю доступу на маршрутизаторі R1 при першому експерименті

```
R2#show access-lists
Extended IP access list 111
    10 permit icmp host 192.168.0.1 10.0.2.0 0.0.0.255
    20 permit icmp host 192.168.0.2 10.0.2.0 0.0.0.255 (5 matches)
    30 permit icmp host 192.168.0.3 10.0.2.0 0.0.0.255
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255
    50 permit icmp host 192.168.0.5 10.0.2.0 0.0.0.255
    60 permit icmp host 192.168.0.6 10.0.2.0 0.0.0.255 (5 matches)
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255
    80 permit ip any any (93 matches)
R2#clear ip access-list counters
```

Рисунок 4.28 – Приклад перевірки списків контролю доступу на маршрутизаторі R2 при першому експерименті

```
R3#show access-lists
Extended IP access list 111
    10 permit icmp host 192.168.0.1 10.0.2.0 0.0.0.255 (5 matches)
    20 permit icmp host 192.168.0.2 10.0.2.0 0.0.0.255
    30 permit icmp host 192.168.0.3 10.0.2.0 0.0.0.255
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255 (5 matches)
    50 permit icmp host 192.168.0.5 10.0.2.0 0.0.0.255 (5 matches)
    60 permit icmp host 192.168.0.6 10.0.2.0 0.0.0.255
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255 (5 matches)
    80 permit ip any any (87 matches)
R3#clear ip access-list counters
```

Рисунок 4.29 – Приклад перевірки списків контролю доступу на маршрутизаторі R3 при першому експерименті

```
R1#show access-lists
Extended IP access list 111
    10 permit icmp host 192.168.0.1 10.0.2.0 0.0.0.255 (5 matches)
    20 permit icmp host 192.168.0.2 10.0.2.0 0.0.0.255
    30 permit icmp host 192.168.0.3 10.0.2.0 0.0.0.255
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255
    50 permit icmp host 192.168.0.5 10.0.2.0 0.0.0.255
    60 permit icmp host 192.168.0.6 10.0.2.0 0.0.0.255
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255
    80 permit ip any any (126 matches)
R1#clear ip access-list counters
```

Рисунок 4.30 – Приклад перевірки списків контролю доступу на маршрутизаторі R1 при другому експерименті

```
R2#show access-lists
Extended IP access list 111
    10 permit icmp host 192.168.0.1 10.0.2.0 0.0.0.255
    20 permit icmp host 192.168.0.2 10.0.2.0 0.0.0.255
    30 permit icmp host 192.168.0.3 10.0.2.0 0.0.0.255 (5 matches)
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255
    50 permit icmp host 192.168.0.5 10.0.2.0 0.0.0.255
    60 permit icmp host 192.168.0.6 10.0.2.0 0.0.0.255 (5 matches)
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255
    80 permit ip any any (129 matches)
R2#clear ip access-list counters
```

Рисунок 4.31 – Приклад перевірки списків контролю доступу на маршрутизаторі R2 при другому експерименті

```
R3#show access-lists
Extended IP access list 111
    10 permit icmp host 192.168.0.1 10.0.2.0 0.0.0.255
    20 permit icmp host 192.168.0.2 10.0.2.0 0.0.0.255 (5 matches)
    30 permit icmp host 192.168.0.3 10.0.2.0 0.0.0.255
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255 (5 matches)
    50 permit icmp host 192.168.0.5 10.0.2.0 0.0.0.255 (5 matches)
    60 permit icmp host 192.168.0.6 10.0.2.0 0.0.0.255
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255 (5 matches)
    80 permit ip any any (132 matches)
R3#clear ip access-list counters
```

Рисунок 4.32 – Приклад перевірки списків контролю доступу на маршрутизаторі R3 при другому експерименті

Розподіл трафіку показано графічно на рис. 4.33-4.34.

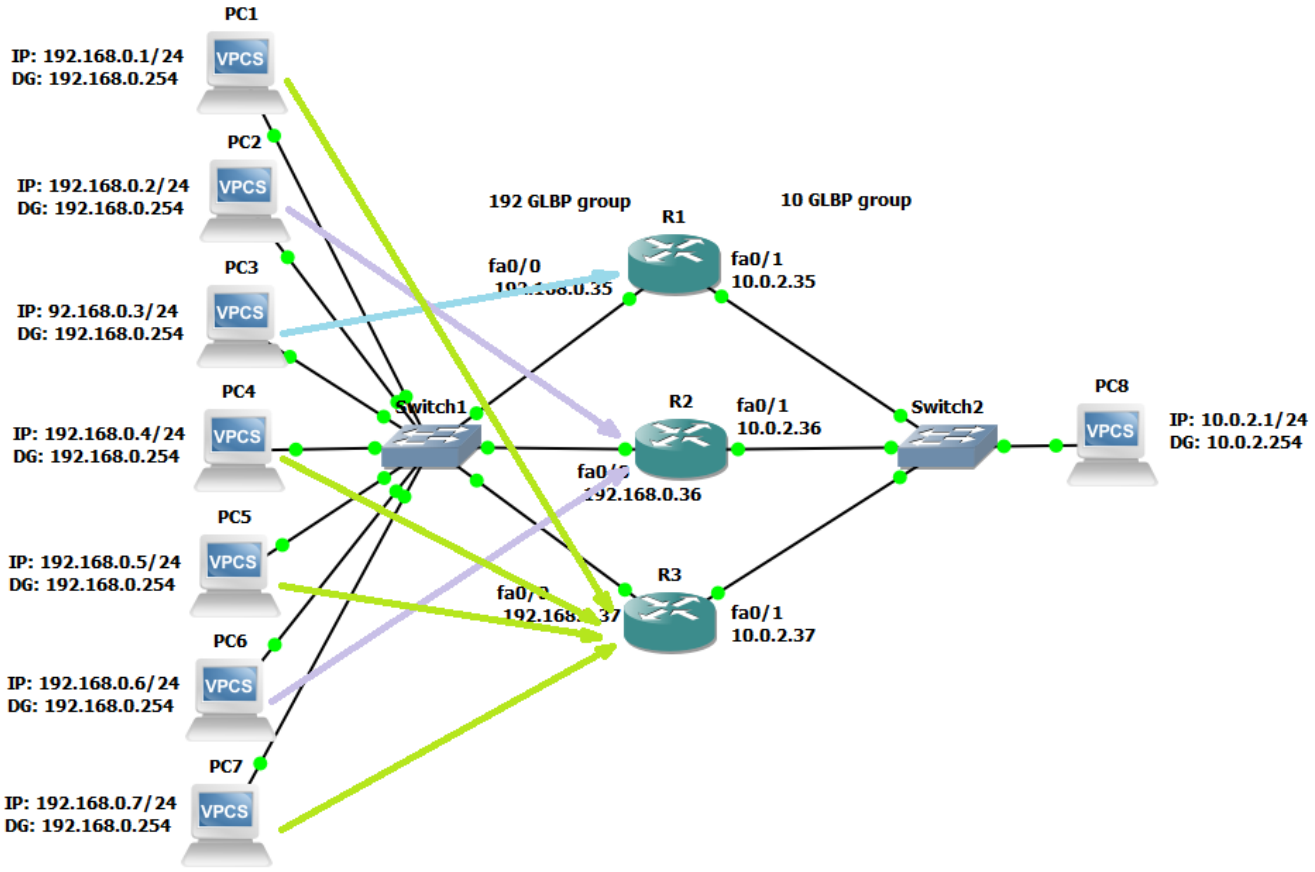


Рисунок 4.33 – Схема мережі з розподілом трафіку для другого експерименту

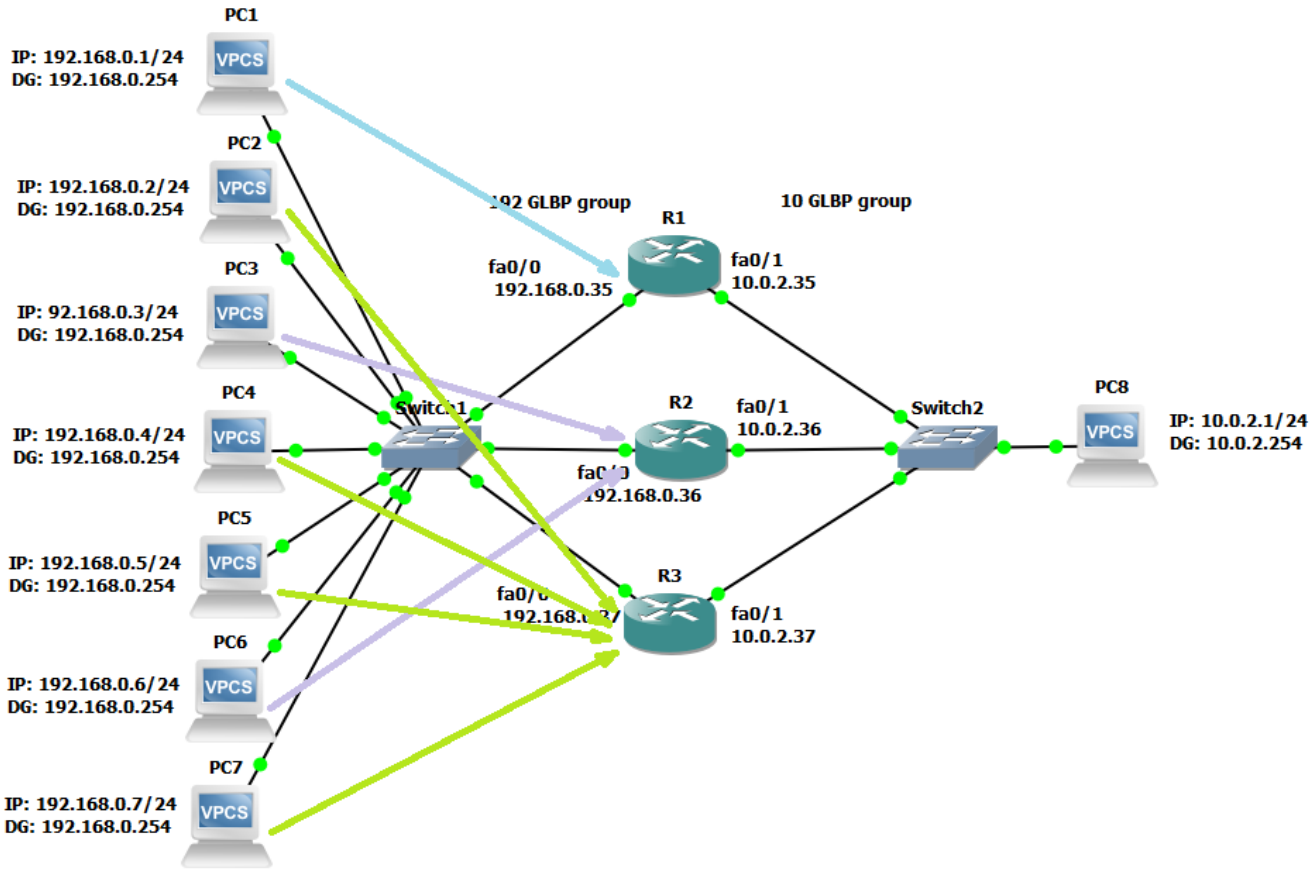


Рисунок 4.34 – Схема мережі з розподілом трафіку для другого експерименту

Щоб перевірити налаштування протоколу GLBP, було використано команду «show glbp» як показано на рис. 4.35-4.37.

На рис. 4.28 наведені такі позначення: 1 – назва GLBP групи; 2 – Роутер R1 має статус «Listen»; 3 – налаштований віртуальний адрес; 4 – значення вагового коефіцієнту; 5 – режим балансування навантаження; 6 – Forwarder R1 має налаштований статус «Listen»; 7 – R2 має статус «Listen»; : 8 – R3 має статус «Active»; 9 – назва GLBP групи; 10 –R1 має налаштований статус «Listen»; 11 – налаштований віртуальний адрес; 12 – режим балансування навантаження; 13 – Forwarder R1 має налаштований статус «Listen»; 14 – R2 має статус «Listen»; 15 – R3 має статус «Active».

На рис. 4.29 наведені такі позначення: 1 – назва GLBP групи; 2 – Роутер R1 має статус «Listen»; 3 – налаштований віртуальний адрес; 4 – значення вагового коефіцієнту; 5 – режим балансування навантаження; 6 – Forwarder R1 має налаштований статус «Listen»; 7 – R2 має статус «Active»; : 8 – R3 має статус «Listen»; 9 – назва GLBP групи; 10 –R1 має налаштований статус «Listen»; 11 – налаштований віртуальний адрес; 12 – режим балансування навантаження; 13 –

Forwarder R1 має налаштований статус «Listen»; 14 – R2 має статус «Active»; 15 – R3 має статус «Listen».

На рис. 4.30 наведені такі позначення: 1 – назва GLBP групи; 2 – Роутер R1 має статус «Listen»; 3 – налаштований віртуальний адрес; 4 – значення вагового коефіцієнту; 5 – режим балансування навантаження; 6 – Forwarder R1 має налаштований статус «Active»; 7 – R2 має статус «Listen»; : 8 – R3 має статус «Listen»; 9 – назва GLBP групи; 10 –R1 має налаштований статус «Listen»; 11 – налаштований віртуальний адрес; 12 – режим балансування навантаження; 13 – Forwarder R1 має налаштований статус «Active»; 14 – R2 має статус «Listen»; 15 – R3 має статус «Listen».

```
R1#show glbp
FastEthernet0/0 - Group 192   1
  State is Listen  2
  Virtual IP address is 192.168.0.254   3
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.244 secs
  Redirect time 600 sec, forwarder timeout 14400 sec
  Preemption disabled
  Active is 192.168.0.37, priority 100 (expires in 8.876 sec)
  Standby is 192.168.0.36, priority 100 (expires in 9.648 sec)
  Priority 100 (default)
  Weighting 29 (configured 29), thresholds: lower 1, upper 29   4
  Load balancing: weighted    5
  Group members:
    c001.33a0.0000 (192.168.0.35) local
    c002.4948.0000 (192.168.0.36)
    c003.44ec.0000 (192.168.0.37)
  There are 3 forwarders (1 active)
  Forwarder 1
    State is Listen    6
    MAC address is 0007.b400.c001 (learnt)
    Owner ID is c003.44ec.0000
    Time to live: 14398.864 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 192.168.0.37 (primary), weighting 114 (expires in 6.444 sec)
  Forwarder 2
    State is Listen    7
    MAC address is 0007.b400.c002 (learnt)
    Owner ID is c002.4948.0000
    Time to live: 14397.216 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 192.168.0.36 (primary), weighting 57 (expires in 7.212 sec)
  Forwarder 3
    State is Active    8
      1 state change, last state change 01:45:02
    MAC address is 0007.b400.c003 (default)
    Owner ID is c001.33a0.0000
    Preemption enabled, min delay 30 sec
    Active is local, weighting 29
FastEthernet0/1 - Group 10    9
  State is Listen    10
  Virtual IP address is 10.0.2.254    11
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.792 secs
  Redirect time 600 sec, forwarder timeout 14400 sec
  Preemption disabled
  Active is 10.0.2.37, priority 100 (expires in 6.420 sec)
  Standby is 10.0.2.36, priority 100 (expires in 8.096 sec)
  Priority 100 (default)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin    12
  Group members:
    c001.33a0.0001 (10.0.2.35) local
    c002.4948.0001 (10.0.2.36)
    c003.44ec.0001 (10.0.2.37)
  There are 3 forwarders (1 active)
  Forwarder 1
    State is Listen    13
    MAC address is 0007.b400.0a01 (learnt)
    Owner ID is c003.44ec.0001
    Time to live: 14396.992 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 10.0.2.37 (primary), weighting 100 (expires in 6.988 sec)
  Forwarder 2
    State is Listen    14
    MAC address is 0007.b400.0a02 (learnt)
    Owner ID is c002.4948.0001
    Time to live: 14398.076 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 10.0.2.36 (primary), weighting 100 (expires in 8.076 sec)
  Forwarder 3
    State is Active    15
      1 state change, last state change 01:45:08
    MAC address is 0007.b400.0a03 (default)
    Owner ID is c001.33a0.0001
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100
R1#
```

Рисунок 4.35 – Перевірка налаштувань протоколу GLBP на маршрутизаторі R1

```
R2#show glbp
FastEthernet0/0 - Group 192   1
  State is Standby   2
    1 state change, last state change 01:47:19
  Virtual IP address is 192.168.0.254   3
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.284 secs
  Redirect time 600 sec, forwarder timeout 14400 sec
  Preemption disabled
  Active is 192.168.0.37, priority 100 (expires in 8.736 sec)
  Standby is local
  Priority 100 (default)
  Weighting 57 (configured 57), thresholds: lower 1, upper 57    4
  Load balancing: weighted    5
  Group members:
    c001.33a0.0000 (192.168.0.35)
    c002.4948.0000 (192.168.0.36) local
    c003.44ec.0000 (192.168.0.37)
  There are 3 forwarders (1 active)
  Forwarder 1
    State is Listen   6
    MAC address is 0007.b400.c001 (learnt)
    Owner ID is c003.44ec.0000
    Time to live: 14398.728 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 192.168.0.37 (primary), weighting 114 (expires in 6.588 sec)
  Forwarder 2
    State is Active   7
      1 state change, last state change 01:47:26
    MAC address is 0007.b400.c002 (default)
    Owner ID is c002.4948.0000
    Preemption enabled, min delay 30 sec
    Active is local, weighting 57
  Forwarder 3
    State is Listen   8
    MAC address is 0007.b400.c003 (learnt)
    Owner ID is c001.33a0.0000
    Time to live: 14396.472 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 192.168.0.35 (primary), weighting 29 (expires in 6.472 sec)
FastEthernet0/1 - Group 10    9
  State is Standby   10
    1 state change, last state change 01:47:22
  Virtual IP address is 10.0.2.254   11
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.112 secs
  Redirect time 600 sec, forwarder timeout 14400 sec
  Preemption disabled
  Active is 10.0.2.37, priority 100 (expires in 7.676 sec)
  Standby is local
  Priority 100 (default)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin   12
  Group members:
    c001.33a0.0001 (10.0.2.35)
    c002.4948.0001 (10.0.2.36) local
    c003.44ec.0001 (10.0.2.37)
  There are 3 forwarders (1 active)
  Forwarder 1
    State is Listen    13
    MAC address is 0007.b400.0a01 (learnt)
    Owner ID is c003.44ec.0001
    Time to live: 14397.664 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 10.0.2.37 (primary), weighting 100 (expires in 7.660 sec)
  Forwarder 2
    State is Active    14
      1 state change, last state change 01:47:29
    MAC address is 0007.b400.0a02 (default)
    Owner ID is c002.4948.0001
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100
  Forwarder 3
    State is Listen    15
    MAC address is 0007.b400.0a03 (learnt)
    Owner ID is c001.33a0.0001
    Time to live: 14398.848 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 10.0.2.35 (primary), weighting 100 (expires in 8.844 sec)
R2#
```

Рисунок 4.36 – Перевірка налаштувань протоколу GLBP на маршрутизаторі R2

```
R3#show glbp
FastEthernet0/0 - Group 192  1
  State is Active  2
    2 state changes, last state change 01:49:44
  Virtual IP address is 192.168.0.254  3
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.548 secs
  Redirect time 600 sec, forwarder timeout 14400 sec
  Preemption disabled
  Active is local
  Standby is 192.168.0.36, priority 100 (expires in 7.348 sec)
  Priority 100 (default)
  Weighting 114 (configured 114), thresholds: lower 1, upper 114  4
  Load balancing: weighted  5
  Group members:
    c001.33a0.0000 (192.168.0.35)
    c002.4948.0000 (192.168.0.36)
    c003.44ec.0000 (192.168.0.37) local
  There are 3 forwarders (1 active)
  Forwarder 1
    State is Active  6
      1 state change, last state change 01:49:34
    MAC address is 0007.b400.c001 (default)
    Owner ID is c003.44ec.0000
    Redirection enabled
    Preemption enabled, min delay 30 sec
    Active is local, weighting 114
    Client selection count: 12
  Forwarder 2
    State is Listen  7
    MAC address is 0007.b400.c002 (learnt)
    Owner ID is c002.4948.0000
    Redirection enabled, 598.892 sec remaining (maximum 600 sec)
    Time to live: 14398.892 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 192.168.0.36 (primary), weighting 57 (expires in 8.888 sec)
    Client selection count: 6
  Forwarder 3
    State is Listen  8
    MAC address is 0007.b400.c003 (learnt)
    Owner ID is c001.33a0.0000
    Redirection enabled, 596.788 sec remaining (maximum 600 sec)
    Time to live: 14396.788 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 192.168.0.35 (primary), weighting 29 (expires in 6.784 sec)
    Client selection count: 3
FastEthernet0/1 - Group 10  9
  State is Active  10
    2 state changes, last state change 01:49:49
  Virtual IP address is 10.0.2.254  11
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.620 secs
  Redirect time 600 sec, forwarder timeout 14400 sec
  Preemption disabled
  Active is local
  Standby is 10.0.2.36, priority 100 (expires in 5.708 sec)
  Priority 100 (default)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin  12
  Group members:
    c001.33a0.0001 (10.0.2.35)
    c002.4948.0001 (10.0.2.36)
    c003.44ec.0001 (10.0.2.37) local
  There are 3 forwarders (1 active)
  Forwarder 1
    State is Active  13
      1 state change, last state change 01:49:39
    MAC address is 0007.b400.0a01 (default)
    Owner ID is c003.44ec.0001
    Redirection enabled
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100
    Client selection count: 3
  Forwarder 2
    State is Listen  14
    MAC address is 0007.b400.0a02 (learnt)
    Owner ID is c002.4948.0001
    Redirection enabled, 598.476 sec remaining (maximum 600 sec)
    Time to live: 14398.476 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 10.0.2.36 (primary), weighting 100 (expires in 8.472 sec)
    Client selection count: 3
  Forwarder 3
    State is Listen  15
    MAC address is 0007.b400.0a03 (learnt)
    Owner ID is c001.33a0.0001
    Redirection enabled, 596.660 sec remaining (maximum 600 sec)
    Time to live: 14396.656 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 10.0.2.35 (primary), weighting 100 (expires in 6.652 sec)
    Client selection count: 3
R3#
```

Рисунок 4.37 – Перевірка налаштувань протоколу GLBP на маршрутизаторі R3

4.3 Висновки до четвертого розділу

В ході роботи було налаштовано та перевірено на практиці роботу протоколу GLBP як у зваженому режимі (Load-Balancing Weighted) так і у режимі (Load-Balancing Round-Robin).

За результатами практичного дослідження було доведено, що засобами протоколу GLBP можливо розподіляти трафік між кількома маршрутизаторами як порівну, так і у зваженому режимі за коефіцієнтами.

Вагові коефіцієнти для налаштування зваженого режиму були визначені не емпірично, а на основі результатів розрахунків в межах рішень RATE або ResMetrTE. За результатами, отриманими в ході дослідження у розділі 3, було налаштовано наступні вагові коефіцієнти: для маршрутизатора R1 – 29, для маршрутизатора R2 – 57, і для маршрутизатора R3 – 114.

Так як в протоколі GLBP трафік розподіляється за хостами, за результатами дослідження, розподіл навантаження у зваженому режимі роботі протоколу GLBP, було організовано наступним чином: для маршрутизатора R1 – 1/7 трафіку, для маршрутизатора R2 – 2/7 трафіку, та для маршрутизатора R3 – 4/7 трафіку. Тобто, можна зробити висновок, що навантаження між маршрутизаторами мережі було розподілено у відповідності до налаштованих вагових коефіцієнтів.

Для пришвидшення та автоматизації процесу налаштування, пропонується зробити автоматичну конфігурацію, щоб протокол мав змогу визначати та налаштовувати вагові коефіцієнти на основі розрахунків запропонованої у даній роботі моделі. У випадку коли протокол буде налаштовуватися самостійно, тобто автоматично, можливо виключити будь який людський фактор, і робота протоколу не буде залежати від досвіду та рівня кваліфікації адміністратора мережі.

ВИСНОВКИ

Використовуючи отриманий, в ході дослідження матеріал, можна зробити висновок, що одним з головних факторів при проектуванні та роботі мережної інфраструктури є те, як мережа може впоратися з балансуванням навантаження та відмовами. З цієї причини, з'являється необхідність враховувати надійність мережевих пристроїв та пропускні здатності для того, щоб ефективно управляти трафіком в мережі. Цього можна досягнути за допомогою протоколів маршрутизації, які є одним з найважливіших засобів забезпечення якості обслуговування.

Однак, через те, що існуючі рішення не задовольняють в повному обсязі потреби сучасної мережної інфраструктури, було запропоновано створення нового протоколу на основі існуючого протоколу балансування навантаження GLBP. Для того, щоб покращити якість обслуговування в мережі, було запропоновано та досліджено вдосконалену математичну модель, яка б враховувала надійність мережних пристроїв, а саме пригранічних маршрутизаторів, пропускну здатність.

У даній роботі було описано чотири математичні рішення задачі проактивної відмовостійкої маршрутизації. Для того щоб забезпечити високий рівень якості обслуговування, всі чотири рішення враховують вимоги концепції Traffic Engineering, а два з запропонованих рішення враховують у явному вигляді рівень надійності пригранічних маршрутизаторів, що кількісно характеризується їх коефіцієнтами готовності.

Отримані результати підтвердили чутливість маршрутних рішень RATE та ResMetrTE до рівня надійності пригранічних маршрутизаторів. Саме за допомогою цих рішень, у більшості випадків, можна було забезпечити такий порядок балансування навантаження, щоб на більш надійні пригранічні маршрутизатори трафік надходив з більшою інтенсивністю. Для розглянутого прикладу було встановлено, що врахування рівня надійності пригранічних маршрутизаторів, при організації балансування навантаження між ними за допомогою рішень RATE або ResMetrTE, призводить до деякого підвищення порогу завантаженості каналів зв'язку ІКМ – у середньому від 15% до 27%.

Для підтвердження можливості балансування навантаження, за отриманими чисельними коефіцієнтами було налаштовано та перевірено роботу мережі за

допомогою протоколу GLBP у зваженому режимі. В ході дослідження було підтверджена можливість балансувати навантаження враховуючи вагові коефіцієнти маршрутизаторів, а також було рекомендовано створення нового протоколу на основі GLBP та запропонованої у даній роботі моделі. Також, рекомендовано зробити конфігурацію протоколу автоматичною, для того щоб, робота мережі на залежала від кваліфікації адміністратора мережі. Це дозволить покращити кількісні значення таких показників як ймовірність втрат пакетів, продуктивність, середня затримка та джитер.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Global Information Infrastructure - Global Information Society (GIIGIS). // OECD Publishing. – 1997. – №25.

2. Janevski T. QoS for Fixed and Mobile Ultra-Broadband / Tony Janevski., 2019. – (First Edition).

3. Ioan F. Network Performance Evaluation for RIP, OSPF and EIGRP Routing Protocols / F. Ioan, T. Gavril., 2013.

4. Yeremenko O., Tariki N., Hailan A.M. Fault-tolerant IP routing flow-based model. Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET): Proceedings of the 13th International Conference, viv, Ukraine, 23–26 February, 2016. IEEE, 2016. P. 655–657. DOI: 10.1109/TCSET.2016.7452143.

5. Lemeshko O.V., Yeremenko O.S., Tariki N., Hailan A.M. Fault-Tolerance Improvement for Core and Edge of IP Network. Computer Sciences and Information Technologies (CSIT): Proceedings of the XIth International Scientific and Technical Conference, Lviv, Ukraine, 6–10 Sept. 2016. IEEE, 2016. P. 161–164. DOI: 10.1109/STC-CSIT.2016.7589895.

6. Lemeshko O., Yeremenko O., Tariki N. Solution for the Default Gateway Protection within Fault-Tolerant Routing in an IP Network. International Journal of Electrical and Computer Engineering Systems. 2017. Vol. 8, No. 1. P. 19–26.

7. Pavlik J., Komarek A., Sobeslav V., Horalek J. Gateway redundancy protocols. Computational Intelligence and Informatics (CINTI) 2014: Proceedings of 142 the IEEE 15th International Symposium. Budapest, Hungary, 19–21 November, 2014. IEEE, 2014. P. 459–464. DOI: 10.1109/CINTI.2014.7028719.

8. RFC 5798. Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6. March 2010. 40 p. URL: https://tools.ietf.org/pdf/rfc5798.pdf.

9. First Hop Redundancy Protocol comparison (HSRP, VRRP, GLBP) with the diagram (2013). Cisco Networking Center. URL: http:// cisconetworkingcenter. blogspot.com/2013/01/first-hop-redundancy-protocol.html.

10. Tiso J., Teare D. Designing Cisco Network Service Architectures (ARCH): Foundation Learning Guide. Cisco press. 2011. 733 p.

11. ITU-T Rec. Y.1540. Internet protocol data communication service – IP packet transfer and availability performance parameters. July 2016. 57 p. URL: https://www.itu.int/rec/T-REC-Y.1540-201607-I/en.

12. Лемешко О.В., Круглова А.О., Крепко А.В. Порівняльний аналіз проактивних рішень з відмовостійкої маршрутизації в інфокомунікаційній мережі // Проблеми телекомунікацій. 2022. 2(31). С. 3-22.

13. Лемешко О. В. Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість / О. В. Лемешко, О. С. Єременко, О. С. Невзорова. – Харків, 2020. – 307 с.

14. Круглова А. О. Потокова модель балансування навантаження в інфокомунікаційній мережі / А. О. Круглова, А. С. Журавльова // Міжнародна науково-технічна конференція студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» ПРІТС 2021: Збірник тез конференції. К.: КПІ ім. Ігоря Сікорського / А. О. Круглова, А. С. Журавльова. 2021. – 402 с.

15. Круглова А.О., Журавльова А.С. Дослідження впливу таймерів у протоколі GLBP на відмовостійкість мережі / А.О. Круглова, А.С. Журавльова // Матеріали восьмої Міжнародної науково-технічної конференції «Проблеми електромагнітної сумісності перспективних безпроводових мереж зв'язку (EMC-2022)». Харків, ХНУРЕ, 2022. С. 54-55.

16. Vegesna S. IP Quality of Service (Cisco networking fundamentals).Cisco press. 2001. 232 p.

17. Телекомунікаційні системи та мережі. Структура та основні функції / В.В. Поповський та ін. Вид. 2-ге, випр. та допов. Харків: СМІТ. 2018. Т. 1. URL: http://www.znanius.com/3534.html.

18. Лемешко О.В., Єременко А.С., Журавльова А.С., Круглова А.О. Результати дослідження методу відмовостійкої маршрутизації в IP-мережі з використанням протоколу GLBP // Матеріали XXI Міжнародної науково – практичної конференції "Інформаційно-комунікаційні технології та сталий розвиток", 14 – 16 листопада 2022 р., Національна академія наук України. Інститут телекомунікацій і глобального інформаційного простору. Науковий центр аерокосмічних досліджень Землі Інституту геологічних наук. Державна установа "Науковий гідрофізичний центр НАНУ". - Київ, 2022, - С. 1-3.

19. Resilience Aware Traffic Engineering FHRP Solution / O.Lemeshko, O. Yeremenko, A. Mersni, M. Yevdokymenko. // IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo). – 2021. – С. 88–93.

20. Application Prospects of First Hop Redundancy Protocols for Fault-Tolerant SDN Controllers: A Survey / [O. Lemeshko, A. Mersni, O. Yeremenko та ін.]. // IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T). – 2021. – С. 58–63.

21. Lemeshko O. Investigation of Enhanced Mathematical Model For Traffic Engineering Fault-Tolerant Routing / O. Lemeshko, O. Yeremenko, A. Mersni. // International Conference on Engineering and Emerging Technologies (ICEET). – 2021. – С. 98–106.

22. Usman A. Performance Analysis and Functionality Comparison of FHRP Protocols / A. Usman, T. Jing, A. Hafiz. // IEEE 11th International Conference on Communication Software and Networks (ICCSN). – 2019. – С. 46–53.

23. Resilience Improvement by Traffic Engineering Fault-Tolerant Routing in Programmable Networks / [O. Lemeshko, O. Yeremenko, M. Yevdokymenko та ін.] // Progress in Advanced Information and Communication Technology and Systems / [O. Lemeshko, O. Yeremenko, M. Yevdokymenko та ін.]., 2022. – С. 235–255.

24. Szigeti T., Hattingh C., Barton R., Briley K. End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks, 2nd Edition. Cisco Press. Part of the Networking Technology series, 2013.

25. Medhi D., Ramasamy K. Network Routing, Second Edition: Algorithms, Protocols, and Architectures (The Morgan Kaufmann Series in Networking) 2nd Edition. Cambridge, MA, USA: Elsevier Inc., 2018. 1018 p.

26. Wibowo F.X.A. et al. Multi-domain software defined networking: research status and challenges. Journal of Network and Computer Applications, 2017, Vol. 87. P. 32-45.

27. Katsalis K. et al. Implementation experience in multi-domain SDN: Challenges, consolidation and future directions. Computer Networks, 2017, Vol. 129. P. 142-158.

28. Blial O., Mamoun M. Ben, Benaini R. An Overview on SDN Architectures with Multiple Controllers. Journal of Computer Networks and Communications. 2016. Vol. 2, P. 1-8. DOI: 10.1155/2016/9396525.

29. Misra S., Goswami S. Network Routing: Fundamentals, Applications, and Emerging Technologies 1st Edition. Wiley, 2017. 536 p.

30. Szigeti T., Zacks D., Falkner M., Arena S. Cisco Digital Network Architecture: Intent-based Networking for the Enterprise. Cisco Press, 2018. 800 p.

31. Wójcik R., Domżał J., Duliński Z. A survey on methods to provide interdomain multipath transmissions. Computer Networks. 2016. Vol. 108. P. 233-259.

32. Eun J.S., Jung H. The implementation of domain routing protocol in hierarchical domain network model // 2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS) (Busan, South Korea, 19-21 Aug. 2015). Busan, 2015. P. 396-399.

33. Lemeshko, O., Nevzorova O., Hailan A.M. Hierarchical Method of Routing and Resource Allocation in DiffServ-TE Network. Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET'2018): 14th International Conference (Lviv-Slavske, Ukraine, 20-24 Feb. 2018). Lviv, 2018. P. 1-5.

34. Lemeshko O., Yeremenko O., Nevzorova O. Hierarchical Method of Inter-Area Fast Rerouting. Transport and Telecommunication Journal. 2017 18(2). P. 155-167.

35. Nevzorova Ye.S., Arous K.M., Salakh M.T.R. Method for hierarchical coordinated multicast routing in a telecommunication network. Telecommunication and Radio Engineering. 2016. Vol. 75. P. 1137- 1151.

36. Лемешко А.В., Невзорова Е.С., Ильяшенко А.Е. Разработка и анализ метода иерар-хическо-координационной междоменной маршрутизации в телекоммуникационной се-ти. Наукові записки Українського науково-дослідного інституту зв'язку. 2016. №4 (44). С. 49- 67.

37. White R., Tantsura J. E. Navigating Network Complexity: Next-generation routing with SDN, service virtualization, and service chaining. AddisonWesley Professional, 2015. 320 p.

38. Lin S.C., Akyildiz I.F., Wang P., Luo M. QoS-aware Adaptive Routing in Multi-Layer Hierarchical Software Defined Networks: A Reinforcement Learning Approach. 2016 IEEE International Conf. on Services Computing (San Francisco, CA, USA, 27 June-2 July 2016). San Francisco, 2016. P. 25-33.

39. Amin R., Reisslein M., Shah N. Hybrid SDN Networks: A Survey of Existing Approaches. IEEE Communications Surveys & Tutorials. 2018. 48 p. DOI: 10.1109/COMST.2018.2837161.

40. Yeremenko O., Lemeshko O. QoS Ensuring over Probability of Timely Delivery in Multipath Routing. In: Hu Z., Petoukhov S., Dychka I., He M. (eds) Advances in Computer Science for Engineering and Education. ICCSEEA 2018. Advances in Intelligent Systems and Computing, Springer, Cham. 2018. Vol. 754. P. 244-254. DOI: https://doi.org/10.1007/978-3-319-91008-6_25.

41. Lemeshko O.V. Policy-based QoS management model for multiservice networks / O.V. Lemeshko, S.V. Garkusha, O.S. Yeremenko , A.M. Hailan. International Siberian Conference on Control and Communications (SIBCON), 21-23 May 2015, Omsk, Russia. Publisher: IEEE. P. 1-4.

42. Lemeshko A.V., Evseeva O.Yu., Garkusha S.V. Research on Tensor Model of Multipath Routing in Telecommunication Network with Support of Service Quality by Greate Number of Indices. Telecommunications and RadioEngineering, 2014, Vol.73, No 15. P. 1339-1360.

43. Lemeshko O., Yeremenko O. Dynamic Presentation of tensor model for multipath QoS-routing. Modern Problems of Radio Engineering, Telecommunications and Computer Science. Proceedings of the international Conference TCSET'2016. – Lviv-Slavske, Ukraine, February 23 - 26, 2016: Publishing House of Lviv Polytechnic, 2016. P. 601-604.

44. Lemeshko O., Yevdokymenko M., Naors Y. Anad Alsaleem. Development of the tensor model of multipath QoE-routing in an infocommunication network with providing the required Quality Rating // Eastern-European Journal of Enterprise Technologies. 2018. Vol. 5, Issue 2 (95). P. 40–46. DOI: https://doi.org/10.15587/1729-4061.2018.141989.

45. Yevdokymenko M. Routing Tensor Model with Providing Multimedia Quality. Problems of Infocommunications. Science and Technology" (PICS&T-2019): International Scientific-Practical Conference–Kyiv, 2019. P. 819 - 824.

46. Lemeshko O.V., Yeremenko O. S., Hailan A. M. QoS solution of traffic management based on the dynamic tensor model in the coordinate system of interpolar paths and internal node pairs. Radio Electronics & Info Communications (UkrMiCo): Proceedings of the International Conference, Kiev, Ukraine, 11-16 Sept. 2016. IEEE, 2016. P. 1–6. DOI: 10.1109/UkrMiCo.2016.7739625.

47. Yeremenko O. Development of the dynamic tensor model for traffic management in a telecommunication network with the support of different classes of service. Eastern-European Journal of Enterprise Technologies. 2016. Vol. 6, Issue 9 (84). P. 12–19. DOI: 10.15587/1729-4061.2016.85602.

48. Бачинський В. А. Вибір протоколу динамічної маршрутизації у корпоративній IP-мережі / В. А. Бачинський, В. Ш. Гіоргізова-Гай. // Міжнародний науково-технічний журнал "Системні дослідження та інформаційні технології". – 2011. – №1.