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)

Дослідження процесів відмовостійкої маршрутизації із захистом шлюзу за замовчуванням на прикладі протоколу GLBP
(тема)

Виконала:
студентка 2 курсу, групи ТСМм-21-1
Журавльова А.С.
(прізвище, ініціали)
Спеціальність: 172 Телекомунікації та радіотехніка
(код і повна назва спеціальності)
Тип програми: освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма: Телекомунікаційні системи та мережі
(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)

2023р.

Атестаційна робота не містить відомостей заборонених до відкритого опублікування.

Студентка  *Журавльова А.С.*

(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 Телекомунікаційні системи та мережі

ЗАТВЕРДЖУЮ

Зав. кафедри

(підпис)

«_20_» ___травня_____2023р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентці Журавльовій Анні Станіславівні .
(прізвище, ім'я, по-батькові)

1. Тема роботи: Дослідження процесів відмовостійкої маршрутизації із захистом шлюзу за замовчуванням на прикладі протоколу GLBP затверджена наказом по університету від «13» березня 2023р. №1389Ст

2. Термін подання студентом роботи до екзаменаційної комісії 25.05.2023р.

3. Вихідні дані до роботи: математичної моделі щодо реалізації відмовостійкої маршрутизації.

4. Перелік питань, що потрібно опрацювати в роботі:

1) Аналіз відомих технологічних та теоретичних рішень щодо проблеми відмовостійкої маршрутизації в інфокомунікаційних мережах.

2) Моделювання процесів відмовостійкої маршрутизації та балансування навантаження в середовищі Matlab.

3) Дослідження процесів відмовостійкої маршрутизації та 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 відмовостійкої маршрутизації та 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		18.04

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	15.02.2023	Виконано
2	Збір матеріалів для дослідження	28.02.2023	Виконано
3	Розробка 1 розділу	19.03.2023	Виконано
4	Розробка 2 розділу	27.03.2023	Виконано
5	Розробка 3 розділу	18.04.2023	Виконано
7	Оформлення пояснювальної записки	15.05.2023	Виконано
8	Оформлення слайдів та презентації	16.05.2023	Виконано

Дата видачі завдання 15 січня 2023 року .

Студентка _____ Журавльова А.С.
(підпис) (прізвище, ініціали)

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

РЕФЕРАТ

Пояснювальна записка: 81 сторінки; 47 рисунків; 8 таблиці; 45 посилання.

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

Об’єкт дослідження – процес відмовостійкої маршрутизації із захистом шлюзу за замовчуванням на прикладі протоколу GLBP.

Предмет дослідження – математична модель відмовостійкої маршрутизації та балансування навантаження із реактивним 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 була розроблена та детально проаналізована математична модель, спрямована на забезпечення відмовостійкої маршрутизації та ефективного балансування навантаження в інфокомунікаційній мережі. Зокрема, модель передбачає реактивний захист маршрутизатора за замовчуванням.

Ця модель базується на ряді ключових принципів, включаючи одношляхову або багатошляхову маршрутизацію, балансування навантаження на стадії доступу, а також захист основного маршрутизатора. Важливими аспектами є забезпечення неперервності потоку даних на всіх рівнях мережі та уникнення перевантаження комунікаційних каналів.

В ході практичного експерименту, на основі цієї моделі було розроблено низку рекомендацій щодо удосконалення протоколу GLBP.

Також були налаштовані таймери на всіх маршрутизаторах мережі, що використовуються в протоколі балансування навантаження шлюзу.

ABSTRACT

Explanatory note: 81 pages; 47 drawing; 8 tables; 45 links.

FAULT-TOLERANT ROUTING, FLOW, QUALITY OF SERVICE, DEFAULT GATEWAY PROTECTION, INFOCOMMUNICATION NETWORK.

The object of research – the process of fault-tolerant routing with default gateway protection, exemplified by the GLBP protocol.

The subject of research – a mathematical model of fault-tolerant routing and load balancing with reactive protection of the default gateway in the infocommunication network, which adheres to the principles of the Traffic Engineering (TE) concept.

The purpose of the work is to improve the quality of service level in the infocommunication network using fault-tolerant routing.

Research methods include formalization and comparison, mathematical programming, and practical experimentation.

In the master's thesis, a mathematical model was developed and thoroughly analyzed, aimed at ensuring fault tolerance and effective load balancing in the infocommunication network. In particular, the model provides for reactive protection of the default router.

This model is based on a number of key principles, including single-path or multi-path routing, load balancing at the access stage, and protection of the main router. Important aspects are ensuring the continuity of data flow at all network levels and avoiding overloading of communication channels.

During a practical experiment, a series of recommendations for improving the GLBP protocol were developed based on this model.

Timers were also set on all network routers used in the load balancing protocol.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦ І ТЕРМІНІВ

ІКМ – інфокомунікаційна мережа;

ОС – операційна система;

ПЗ – програмне забезпечення;

Fault-tolerant routing – відмовостійка маршрутизація;

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

У сучасному світі технологічний прогрес не стоїть на місці, а особливо активно розвивається сфера телекомунікацій. Це породжує нові виклики для мережевих інфраструктур, що мають відповідати високим стандартам якості обслуговування (Quality of Service, QoS), та бути готовими до швидкого масштабування.

Оцінювати якість обслуговування мережі ми можемо за допомогою таких параметрів, як джиттер, втрати пакетів, швидкість передачі даних та середній час затримки. Всі ці показники в значній мірі залежать від використовуваних протоколів маршрутизації, а також від способу захисту шлюзу за замовчуванням.

Важливо розуміти, що розширення мережі і збільшення її складності вимагають нових підходів до маршрутизації та захисту. Потреба в розв'язаннях, що відповідають зростаючим вимогам, створює потребу в нових дослідженнях та розробках у цій сфері. Організаціям і компаніям потрібна стабільна мережа для захисту бізнесу від системних збоїв, втрати даних і відмов.

Побудова відмовостійкої мережевої інфраструктури є важливим етапом. Багато інтернет-провайдерів не можуть гарантувати неперервне підключення. З цієї причини, щоб забезпечити стабільність роботи мережі і зменшити ризик відмов, провайдери зазвичай використовують декілька підключень. У разі відмови основного підключення активується резервне. Така система передбачає наявність кількох мережевих шлюзів, що гарантує надійність мережі, навіть у випадку відмови одного з них.

Щоб забезпечити якісне обслуговування та мінімізувати мережеві збої, використовується протокол резервування першого переходу (FHRP). Багато сучасних пристроїв Cisco підтримують FHRP, включаючи Cisco Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP) та Gateway Load Balancing Protocol (GLBP).

Однак, не всі сучасні протоколи забезпечують автоматизацію роботи, це означає, що якість обслуговування може залежати від досвіду та навичок мережевого адміністратора. В цьому контексті, у роботі була розроблена удосконалена модель відмовостійкої маршрутизації, яка включає реактивний захист шлюзу за замовчуванням в інфокомунікаційній мережі. Дана модель

базується на протоколі GLBP, що значно покращує стабільність та надійність роботи мережі.

1 АНАЛІЗ ПРОТОКОЛІВ ВІДМОВОСТІЙКОЇ МАРШРУТИЗАЦІЇ В IP-МЕРЕЖАХ

У мережах з багатьма шлюзами за замовчуванням (default gateway), існує ризик втрати доступності мережі, коли один з шлюзів не працює. Щоб уникнути таких проблем, були розроблені протоколи FHRP. Ці протоколи дозволяють налаштувати віртуальну IP-адресу (Virtual IP, VIP) для групи шлюзів, яка буде використовуватися як головний шлюз. У випадку, коли головний шлюз не працює, інший шлюз з тієї ж групи може стати головним та продовжувати обслуговування мережі. Зазвичай ці протоколи використовують резервування ресурсів, таких як маршрутизатори та шлюзи, для підтримки мережевої роботи в разі відмови основних компонентів. На рисунку 1.1 наведена топологія фізичної мережі з відмовою маршрутизатора R1 та втратою доступу до Інтернету.

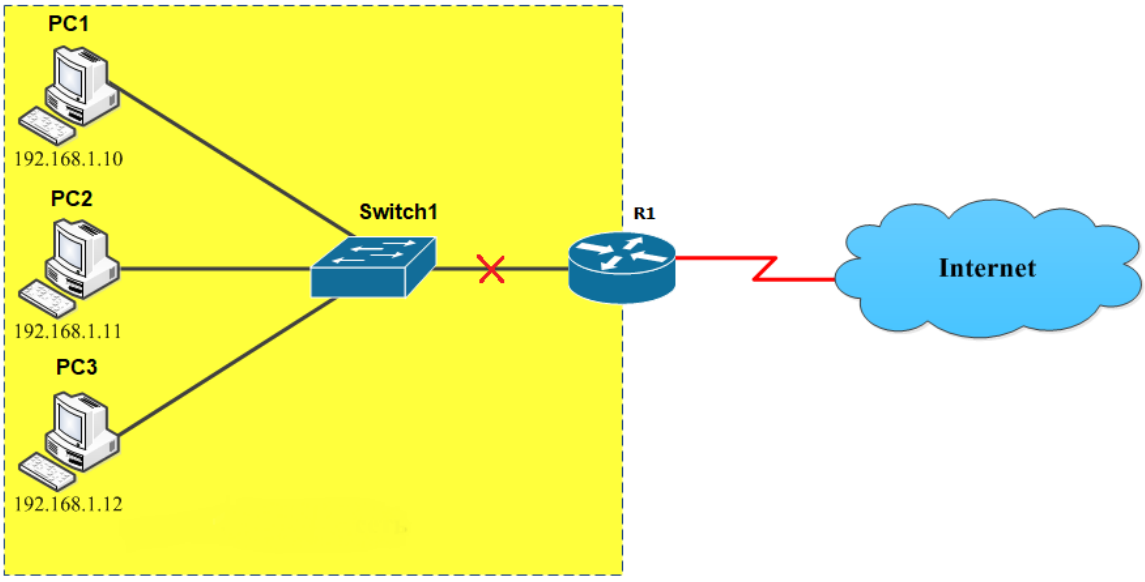

Рисунок 1.1 – Топологія фізичної мережі з R1

Якщо маршрутизатор R1 стає недоступним, то протоколи маршрутизації можуть динамічно змінювати свої маршрути. У такому разі R2 (рис. 1.2) приймає на себе відповідальність направляти пакети із зовнішніх мереж, які раніше проходили через R1. Але, не зважаючи на це, 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.

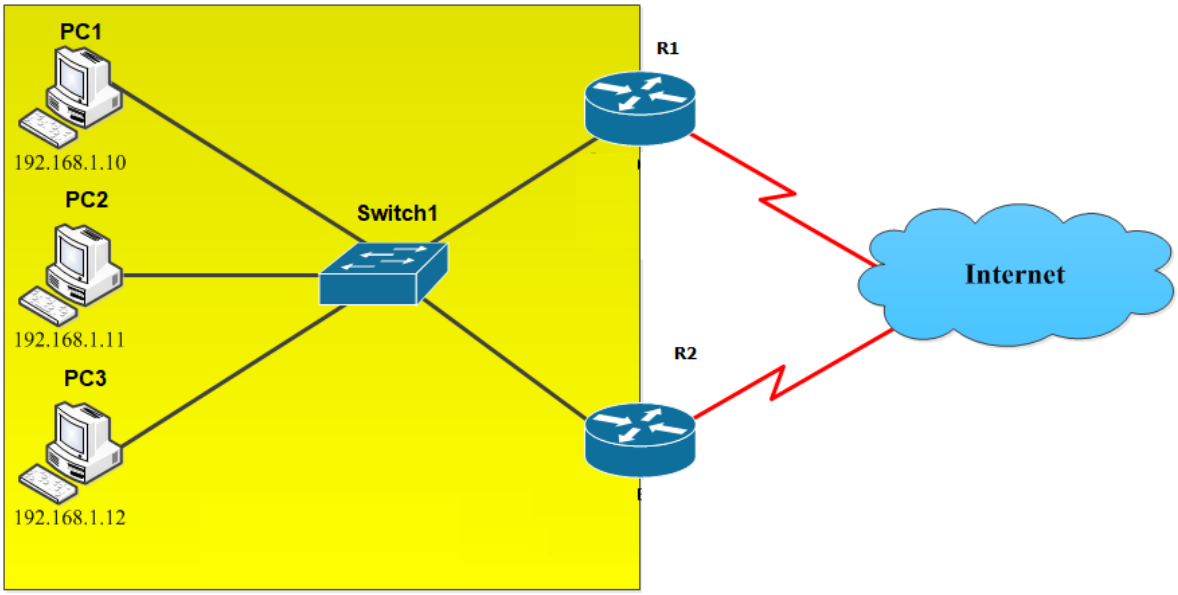

Рисунок 1.2 – Топологія фізичної мережі з R1 та R2

Протокол резервування забезпечує механізм для визначення маршрутизатора, який повинен відігравати активну роль у пересиланні трафіку та коли резервний маршрутизатор повинен прийняти роль пересилання. Перехід від одного маршрутизатора до іншого є неважливим для кінцевих пристроїв. Мережа може динамічно відновлюватися після збою пристрою, який виступає в якості шлюзу, завдяки здатності резервування першого переходу.

Основними протоколами FHRP є HSRP, VRRP та GLBP, які ми розглянемо в наступному розділі. Усі ці протоколи мають однакову мету - забезпечити високу доступність та надійність мережі шляхом створення віртуальних IP-адрес, які використовуються як маршрутизатори за замовчуванням.

При розгляді протоколів відмовостійкої маршрутизації в IP-мережах, важливо звернути увагу на фактори, які впливають на їхню ефективність. Деякі з цих факторів включають час відновлення після відмови, балансування навантаження, простоту впровадження та підтримки, а також сумісність з різними апаратними та програмними платформами. Перед тим, як випробувати GLBP, важливо розглянути деякі з базових протоколів відмовостійкої маршрутизації, які використовуються в IP-мережах.

Є два основних класи протоколів відмовостійкої маршрутизації, які часто використовуються: протоколи статичної маршрутизації та протоколи динамічної маршрутизації (табл.1.1). Статична маршрутизація базується на встановленій заздалегідь таблиці маршрутизації, яка не змінюється автоматично в реальному часі. Динамічна маршрутизація, з іншого боку, використовує протоколи, які адаптуються до змін у стані мережі.

Таблиця 1.1 – Порівняння статичної та динамічної маршрутизації [1]

Критерій порівняння	Статична маршрутизація	Динамічна маршрутизація
Складність конфігурування	Ускладнюється зі зростанням складності мережі	В загальному плані не залежить від складності мережі
Вимоги до знань адміністратора	Потрібен невисокий рівень знань	Потрібен невисокий рівень знань
Зміни Топології	Потрібне адміністративне втручання	Автоматично адаптується під зміни
Масштабування	Підходить лише для простих топологій	Підходить і для складних і для простих топологій
Ступінь безпеки	Більш безпечна, ніж динамічна маршрутизація	Не гарантує безпеки
Ступінь застосування ресурсів	Не потребує додаткових ресурсів	Застосовує процесор, оперативну пам'ять, смугу пропускання
Передбачуваність	Маршрут завжди постійний	Маршрут залежить від поточної топології

Ці два класи протоколів мають свої переваги та недоліки. Статична маршрутизація проста в реалізації, але може бути недостатньо гнучкою для сучасних динамічних мереж, особливо при високих вимогах до надійності. Динамічна маршрутизація гнучкіша, але також більш складна у плані конфігурації та управління.

Методи відмовостійкої маршрутизації, такі як протоколи VRRP, HSRP і GLBP, є прикладами протоколів динамічної маршрутизації. Вони адаптуються до

змін у мережі і можуть автоматично переключатися між різними шлюзами, що підвищує надійність мережі. Таким чином можна представити порівняльну характеристику протоколів.

1.1 Порівняльна характеристика протоколів VRRP, HSRP та GLBP

Розглянемо основні характеристики протоколів.

Протоколи VRRP, HSRP та GLBP є протоколами, що забезпечують високу доступність мережі. Ці протоколи дозволяють багатьом маршрутизаторам бути активними і забезпечувати резервний шлях маршрутизації в разі відмови головного шляху. Кожен з цих протоколів має свої особливості та переваги.

VRRP - це протокол відкритого стандарту IEEE 802.1Q, який дозволяє створювати віртуальний маршрутизатор, який буде виступати як резервний шлях маршрутизації в разі відмови головного шляху. VRRP дозволяє багатьом маршрутизаторам бути активними, але тільки один з них є віртуальним. VRRP використовує адресу IP віртуального маршрутизатора (Virtual IP, VIP) як шлюз за замовчуванням для клієнтів мережі. При відмові активного маршрутизатора, VRRP автоматично визначає нового активного маршрутизатора. VRRP також підтримує збереження стану маршрутизатора при зміні активного маршрутизатора та використовує алгоритм визначення приорітету для вибору активного маршрутизатора.

На рисунку 1.3 наведено приклад протоколу VRRP

N2 хоче зв’язатися N1. Якщо R1 з більшим пріоритетом, то він буде активним маршрутизатором, відповідно R2 з меншим пріоритетом буде резервним маршрутизатором. VRRP не достигає балансування навантаження автоматично[2].

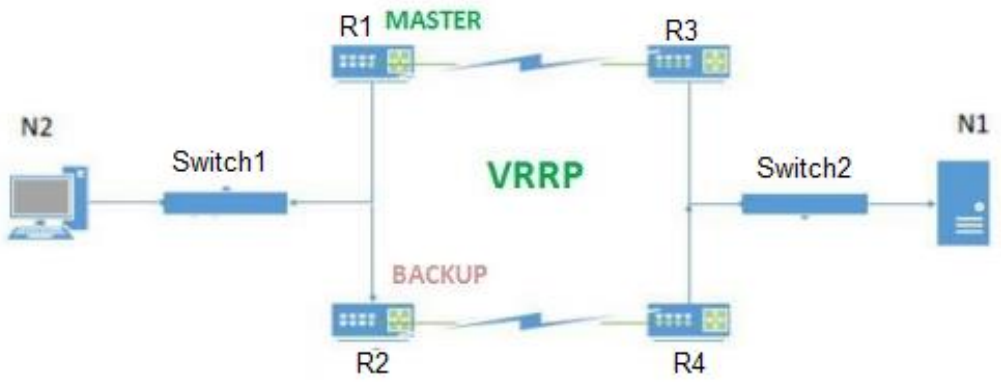

Рисунок 1.3 – Приклад протоколу VRRP

HSRP – це протокол Cisco, який дозволяє створювати віртуальний маршрутизатор, який буде виступати як резервний шлях маршрутизації в разі відмови головного шляху. HSRP дозволяє багатьом маршрутизаторам бути активними, але тільки один з них є активним за замовчуванням. HSRP використовує адресу IP віртуального маршрутизатора (Virtual IP, VIP) як шлюз за замовчуванням для клієнтів мережі. При відмові активного маршрутизатора, HSRP визначає нового активного маршрутизатора на основі пріоритету та додаткових параметрів, таких як інтервали перевірки доступності (hello) та інтервали переключення (hold). HSRP також підтримує збереження стану маршрутизатора при зміні активного маршрутизатора.

На рисунку 1.4 наведено приклад протоколу HSRP.

N2 у якості комп’ютера, який буде відправляти дані у пункт призначення N1. Налаштовуємо протокол HSRP на маршрутизаторах R1 та R2. Шлюз повинен бути вказаний на пристрої джерела, тому потрібно додати віртуальну IP-адресу як шлюз за замовчуванням. Якщо налаштувати R1 на найвищий пріоритет, то трафік буде проходити на R1, потім на R3 і потім на N1 через комутатор, але якщо з якоїсь причини маршрутизатор R1 вийде з ладу, то трафік піде на R1, потім на R3 і потім на N1 через комутатор. Маршрутизатор R2 зможе взяти на себе відповідальність, і надсилання повідомлень здійснюватиметься через R2. В HSRP інший маршрутизатор не зможе взяти на себе обов'язки першого маршрутизатора, доки в режимі конфігурації маршрутизатора не буде вимкнено функцію ***preemption***. Як тільки попередній розподіл увімкнено, він може пересилати трафік. Тут пріоритет R1 високий, тому він є активним маршрутизатором, а

маршрутизатор R2 буде резервним маршрутизатором. HSRP не виконує автоматичного балансування навантаження.

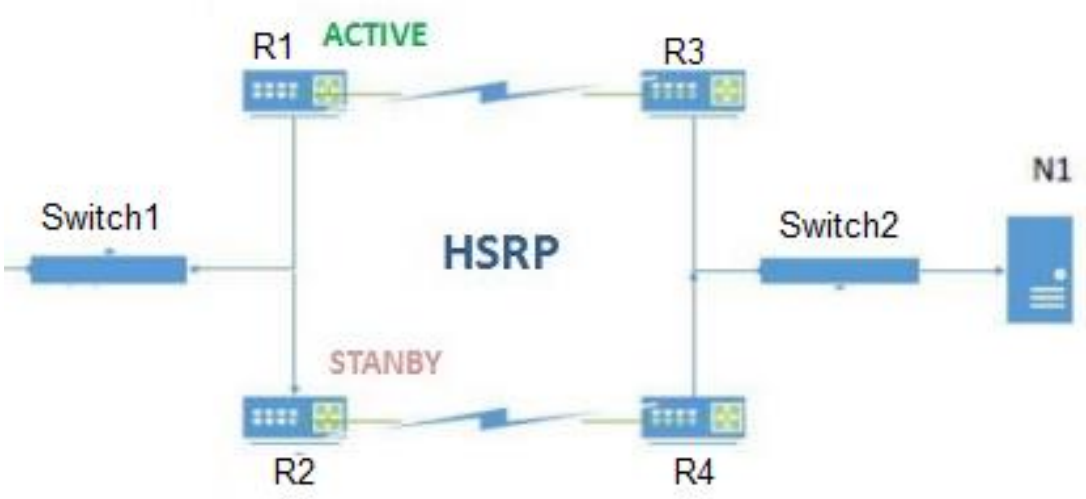

Рисунок 1.4 – Приклад протоколу HSRP

GLBP – це протокол Cisco, який дозволяє багатьом маршрутизаторам бути активними та роздавати навантаження між ними. GLBP використовує адресу IP віртуального маршрутизатора (Virtual IP, VIP) як шлюз за замовчуванням для клієнтів мережі, але замість того, щоб мати тільки одного активного маршрутизатора, GLBP дозволяє багатьом маршрутизаторам бути активними та роздавати навантаження між ними. GLBP використовує алгоритм вибору активного маршрутизатора на основі ваг (пріоритетів), які можуть бути налаштовані на кожному маршрутизаторі. Крім того, GLBP має можливість балансування навантаження з використанням алгоритму Round Robin або з використанням алгоритму виключення з розрахунку (Active/Passive), який відключає маршрутизатори, які не можуть обробити навантаження, від роздачі трафіку.

На рисунку 1.5 наведено приклад протоколу GLBP.

Система N2 хоче взаємодіяти з NI. Потрібно налаштувати протокол GLBP на маршрутизаторах R1 та R2. Якщо маршрутизатор R1 має найвищий пріоритет, цей маршрутизатор буде AVG, а маршрутизатор R2 буде AVF. Якщо система N2 хоче спілкуватися із системою N1, то трафік буде направлений через маршрутизатор AVG, який знаходиться через R1.

Якщо система N2 знову захоче взаємодіяти з системою NI, трафік пройде через маршрутизатор AVF, який знаходиться через маршрутизатор R2, оскільки

протокол GLBP автоматично балансує навантаження. Якщо трафік проходить через один маршрутизатор в одному циклі, то в другому циклі трафік проходитиме через інший маршрутизатор, оскільки маршрутизатор GLBP призначений для балансування навантаження, а також для FHRP [3].

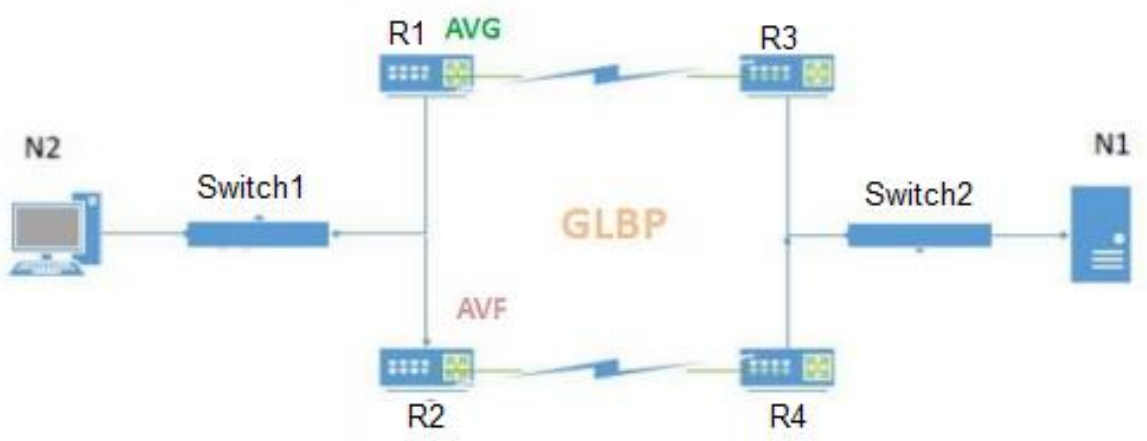

Рисунок 1.5 – Приклад протоколу GLBP

Наведені приклади дозволяють нам представити характеристику протоколів у вигляді таблиці 1.2.

Таблиця 1.2 – Характеристика протоколів FHRP

Характеристика	HSRP	VRRP	GLBP
Застосування	Cisco Proprietary	IEEE Standard	Cisco Proprietary
Стандарт	RFC 2281	RFC 5798	-
Рівень OSI	Мережний	Мережний	Мережний
Балансування навантаження	-	-	-
IPv6	Підтримується	Підтримується	Підтримується
Переваги	- легка конфігурація; - низьке навантаження мережі службовим трафіком.	- спрощене управління мережею; - висока адаптованість; - низьке навантеження мережі службовим трафіком; - балансування навантаження; - мінімізація витрат.	- ефективне використання мережних ресурсів; - висока доступність; - автоматичне балансування навантаження; - низькі витрати на адміністрування;

Продовження таблиці 1.2

Недоліки	- неефективний для передачі трафіку реального часу; - слабкий рівень безпеки;	- слабкий рівень безпеки	- пропрієтарний протокол Cisco; - висока складність управління мережею

У порівнянні з HSRP та VRRP, GLBP має перевагу у балансуванні навантаження між багатьма активними маршрутизаторами та використанні більш складного алгоритму вибору активного маршрутизатора на основі ваг. Однак, GLBP є протоколом Cisco та має обмежену сумісність з іншими виробниками обладнання. HSRP та VRRP, з іншого боку, є стандартами відкритого стандарту та можуть бути використані з різними виробниками обладнання.

Щодо безпеки, всі три протоколи дозволяють налаштовувати аутентифікацію між маршрутизаторами за допомогою різних методів (наприклад, за допомогою пароля або ключа).

Вибір між цими протоколами залежить від потреб мережі та вимог до безпеки, масштабованості та простоти налаштування. Якщо мережа має потребу в одному активному маршрутизаторі та простому налаштуванні, то VRRP або HSRP можуть бути кращим варіантом. Якщо мережа має потребу в багатьох активних маршрутизаторах та балансуванні навантаження, то GLBP може бути кращим вибором.

Незважаючи на те, що VRRP, HSRP та GLBP виконують схожу функцію, вони мають свої особливості та переваги, які слід враховувати при виборі протоколу для конкретної мережі. Деякі з цих особливостей та переваг включають:

- VRRP має підтримку IPv6, що робить його корисним для мереж, які використовують цей протокол;

- HSRP має можливість збереження стану маршрутизатора при зміні активного маршрутизатора, що забезпечує менший вплив на мережу під час переключення;

- GLBP може бути корисним для мереж, які мають потребу в багатьох активних маршрутизаторах та балансуванні навантаження, що забезпечує кращу продуктивність та доступність.

Отже, протоколи VRRP, HSRP та GLBP є протоколами відмовостійкої маршрутизації, які дозволяють забезпечити продуктивність та доступність мережі в разі відмови маршрутизатора. При виборі протоколу важливо врахувати також обмеження та особливості кожного з них, а також їхню сумісність з обладнанням, що використовується в мережі.

1.2 Аналіз параметрів, за допомогою яких можна управляти роботою протоколу GLBP

Аналіз параметрів GLBP дозволяє управляти роботою протоколу та забезпечувати розподіл навантаження між шлюзами. Вірно налаштовані параметри дозволяють досягти високої доступності та надійності мережі, забезпечити швидкий перехід на резервний шлюз у разі відмови основного, а також ефективно використовувати пропускну здатність мережі. Розуміння цих параметрів та їх вплив на роботу протоколу є важливим для проектування та налагодження високопродуктивних мереж, які забезпечують високу доступність та ефективне використання ресурсів.

Параметри GLBP вимагають належної конфігурації, щоб забезпечити оптимальну роботу протоколу. Нижче розглянемо детальніше кожен з них та команди для їх налаштування:

1. Вага шлюза – це числове значення, яке використовується для розподілу навантаження між шлюзами. За замовчуванням всі шлюзи мають однакову вагу. Налаштування ваги шлюза дозволяє адміністратору мережі керувати тим, який шлюз буде активним у будь-який момент часу.

Команда для налаштування ваги шлюза:

Router(config-if)# glbp group weight weight

де **group** – номер групи GLBP, **weight** – вага шлюза (від 1 до 255).

2. Пріоритет шлюза – це числове значення, яке використовується для визначення, який шлюз повинен бути активним у випадку, коли всі шлюзи мають однакову вагу. Шлюз з вищим пріоритетом стає активним шлюзом.

Команда для налаштування пріоритету шлюза:

Router(config-if)# glbp group priority priority

де **group** – номер групи GLBP, **priority** – пріоритет шлюза (від 1 до 255).

3. Таймери GLBP

Протокол GLBP використовує Hello та Hold таймери для визначення доступності партнерів мережі та керування обміном повідомленнями між ними.

Hello таймер вказує інтервал часу між відправленням Hello повідомлень між партнерами. По замовчуванню, значення Hello таймера в GLBP становить 3 секунди. Якщо партнер не отримує Hello повідомлення від іншого партнера протягом певного часу, він може вважати його недоступним.

Hold таймер вказує максимальний час очікування на отримання відповіді від партнера GLBP, після якого маршрутизатор вважатиме партнера недоступним. По замовчуванню, значення Hold таймера в GLBP становить 10 секунд. Якщо маршрутизатор не отримує жодного Hello повідомлення від партнера до закінчення таймера Hold, він вважає партнера недоступним.

Налаштування значень Hello та Hold таймерів дозволяє зменшити час відновлення послуги у випадку, якщо один з партнерів мережі стає недоступним. Наприклад, якщо партнер перестає відправляти Hello повідомлення, інший партнер може швидко відзначити його відсутність та зайняти його роль, щоб продовжити роботу мережі без перерви.

Для налаштування значень Hello та Hold таймерів в GLBP можна використовувати команду "**glbp timers**".

Наприклад, наступна команда встановлює значення Hello таймера на 5 секунд та Hold таймера на 20 секунд:

Router(config)# interface ethernet0/0
Router(config-if)# glbp 1 timers 5 20

У разі використання протоколу GLBP, правильне налаштування Hello та Hold таймерів може допомогти забезпечити надійну та стійку роботу мережі.

Розглянемо приклад використання таймерів Hello та Hold у GLBP.

Припустимо, що ми маємо мережу з двома маршрутизаторами, які підключені до групи GLBP, і ми хочемо налаштувати таймери Hello та Hold для

контролювання того, який маршрутизатор буде визначати віртуальну IP-адресу. Ми встановимо таймер Hello на 3 секунди і таймер Hold на 10 секунд.

Для цього можна виконати наступні команди на маршрутизаторах:

Router1(config)# interface gigabitethernet0/0
Router1(config-if)# glbp 1 timers 3 10
Router1(config-if)# exit

Router2(config)# interface gigabitethernet0/0
Router2(config-if)# glbp 1 timers 3 10
Router2(config-if)# exit

Тепер, коли мережа запущена, маршрутизатори будуть обмінюватись Hello-повідомленнями кожні 3 секунди, щоб узгодити стан кожної з них. Якщо маршрутизатор не отримує жодного Hello-повідомлення від іншого маршрутизатора протягом 10 секунд, то він вважає, що той маршрутизатор вийшов з ладу, і бере на себе обслуговування віртуальної IP-адреси.

Таким чином, таймери Hello та Hold дозволяють маршрутизаторам в групі GLBP взаємодіяти між собою та контролювати, який маршрутизатор буде відповідальним за віртуальну IP-адресу.

Hold timer – це таймер, який використовується в протоколах маршрутизації для визначення того, чи мережевий елемент (наприклад, маршрутизатор) є активним у мережі. Якщо маршрутизатор не отримує повідомлень від інших маршрутизаторів (через відсутність з'єднання або несправності), то він перестає брати участь у маршрутизації.

У протоколі GLBP, Hold timer використовується для визначення того, чи маршрутизатор ще обробляє віртуальну IP-адресу. Якщо маршрутизатор не отримує Hello-повідомлень від інших маршрутизаторів GLBP, то він перестає вважатись активним у роботі з віртуальною IP-адресою.

Таким чином, Hold timer відповідає за те, що маршрутизатори в групі GLBP регулярно обмінюються повідомленнями, щоб переконатись, що кожен маршрутизатор все ще працює. Якщо маршрутизатор не отримує жодного повідомлення від іншого маршрутизатора протягом Hold timer інтервалу, то він вважає, що той маршрутизатор вийшов з ладу.

Отже, параметри Hello та Hold є важливими для налаштування протоколу GLBP. Вони впливають на швидкість виявлення недоступності активного компонента та керування трафіком в мережі. Вірно налаштовані параметри можуть покращити ефективність роботи мережі і забезпечити надійність в роботі протоколу.

4. Призначення віртуальної IP-адреси – віртуальна IP-адреса використовується для забезпечення доступності мережі. Вона є адресою, яку користувачі використовують для звернення до мережі.

Команда для налаштування віртуальної IP-адреси:

Router(config-if)# glbp group ip ip-address

де **group** – номер групи GLBP, **ip-address** – віртуальна IP-адреса.

5. Налаштування пріоритету мережевого інтерфейсу – пріоритет мережевого інтерфейсу використовується для визначення того, який мережевий інтерфейс має бути використаний для входу трафіку в мережу.

Команда для налаштування пріоритету мережевого інтерфейсу:

Router(config-if)# glbp group forwarder-preemption [delay minimum],

де **group** – номер групи GLBP, **delay** – затримка, після якої пріоритет буде змінений, **minimum** – мінімальне значення затримки.

Отже, параметри GLBP дозволяють керувати роботою протоколу та забезпечити максимальну доступність мережі. Використання правильних команд допоможе налаштувати протокол GLBP для покращення продуктивності та забезпечення високої доступності мережі.

Використання цих параметрів може допомогти налаштувати GLBP для оптимальної роботи в конкретній мережі. Наприклад, налаштування ваги шлюзів може допомогти збалансувати навантаження, а перевірка доступності може допомогти уникнути проблем з доступністю шлюзів.

У підсумку, GLBP – це потужний протокол для розподілу навантаження між багатьма шлюзами. Використання параметрів, які відповідають конкретним потребам мережі, може допомогти забезпечити його оптимальну роботу.

1.3 Огляд існуючих наукових робіт по вдосконаленню моделей протоколів сімейства FHRP

Безперебійна та надійна робота мережі є важливою вимогою в сучасних IP-мережах. Якість обслуговування (QoS) залежить від стабільності та безперебійності мережі. Перші протоколи резервування FHRP були розроблені для підтримки цієї стабільності, забезпечуючи високий рівень доступності шлюзу за замовчуванням для кінцевих вузлів у локальних мережах.

Одним із напрямків вдосконалення є зменшення часу відновлення при відмові. Науковці працюють над методами, які зможуть зменшити час, необхідний для відновлення роботи мережі після відмови обладнання. Це допоможе мінімізувати перерви в роботі мережі, що, в свою чергу, позитивно позначиться на якості обслуговування.

У цьому розділі ми розглянемо деякі з останніх наукових робіт, що пропонують вдосконалення моделей протоколів сімейства FHRP:

При побудові мережної інфраструктури одним із найважливіших моментів є те, як мережа може реагувати на збої. Мережеві провайдери, оператори та інші виробники мережного обладнання задали доступність мережі до 99,999%, що означає, що мережа може відчувати перешкоди лише протягом 5 хвилин протягом одного року. З цієї причини необхідно мати два або більше шлюзів, підключених до мережі, тому що якщо один із шлюзів вийде з ладу, інші шлюзи негайно замінять мертві шлюзи. У цьому дослідженні [4] оцінюється продуктивність протоколу резервування першого переходу FHRP на VRRP, HSRP та GLBP, щоб визначити порівняння продуктивності з використанням параметрів QoS (пропускна здатність, джиттер, втрата пакетів, час простою). Метод збору даних полягав у вивченні літератури та методі моделювання з 8 етапами (постановка проблеми, концептуальна модель, вхідні та вихідні дані, моделювання, перевірка, експериментування та оцінка результатів). Результати цього дослідження показують, що GLBP має кращі параметри QoS, ніж VRRP та HSRP.

Продовжуючи огляд наукових робіт, які спрямовані на вивчення та вдосконалення HSRP, ми звертаємо увагу на наступну роботу:

У цій статті [5] автори поставили перед собою мету провести експериментальне дослідження та порівняти різні протоколи FHRP щодо їх відмовостійкої маршрутизації та ефективності використання ресурсів мережі. Для цього вони використали пакет моделювання мереж OPNET Modeler. Дослідження було проведено на прикладі великої корпоративної мережі з декількома підмережами та багатьма шлюзами мережі. Автори встановили різні протоколи FHRP (VRRP, HSRP та GLBP) на шлюзах мережі та провели експерименти для вимірювання різних параметрів, таких як час відновлення мережі після відмови головного шляху, кількість переданих пакетів, кількість пакетів, що втрачені та ін.

Результати експериментів показали, що GLBP має кращу ефективність в порівнянні з VRRP та HSRP, оскільки він забезпечує більш рівномірний розподіл трафіку між різними шлюзами мережі та може забезпечити відмовостійку маршрутизацію в разі відмови будь-якого з шлюзів. Крім того, GLBP виявився більш ефективним у використанні ресурсів мережі, оскільки дозволяє розподілити навантаження між різними шлюзами мережі. Отже, стаття допомагає зрозуміти особливості різних протоколів FHRP та їх взаємозв'язок з ефективністю мережі. У статті використано різноманітні методи, такі як моделювання мереж, вимірювання трафіку та часу відновлення мережі, статистичний аналіз даних.

В роботі [6] автори описують, що в цю епоху кожна сфера вимагає високої доступності мережі з найменшою ймовірністю втрати даних та що для проектування мережі слід якомога більше використовувати резервування. Висока доступність мережі вимагає вищих управлінських та експлуатаційних витрат. Вони описують, що вирішити проблему допомагають протоколи резервування, бо протоколи FHRP реалізовані для подолання втрати трафіку від джерела до пункту призначення в мережевих комунікаціях. Автори цієї роботи оцінюють три конкретні протоколи FHRP, а саме протокол HSRP, протокол VRRP і GLBP. Ці протоколи оцінюються за допомогою інструменту GNS3.

Після впровадження, оптимізації та тестування різних FHRP на додаток до вивчення та аналізу результатів втрати пакетів, часу перетворення і потоку трафіку; з експерименту чітко видно, що GLBP має вищу продуктивність, ніж HSRP і VRRP.

Для FHRP-v6 HSRP добре працює, оскільки кількість пакетів, втрачених після оптимізації часу, зменшилася, однак для цього потрібно збільшити використання CPU. VRRP є корисним, оскільки він швидше перемикається для резервного копіювання маршрутизаторів, які можна отримати за допомогою

стандартних механізмів IPv6 Neighbor Discover (RFC 4861); тим не менш, VRRP все ще демонструє більше втрат пакетів порівняно з GLBP без втрат через використання балансування навантаження в останньому протоколі.

Усі перспективи балансування навантаження роблять GLBP ефективним і надійним протоколом і забезпечують більшу доступність мережі. Єдиним недоліком GLBP є те, що він є власністю CISCO, тому він працює лише на пристроях CISCO.

Підводячи підсумок, автори визнали, що GLBP є кращим за HSRP і VRRP з точки зору продуктивності та досягнення вищої доступності в мережі.

В роботі [7] автори провели вимірювання трьох протоколів шлюзу резервування, а саме протоколу VRRP, протоколу HSRP і протоколу GLBP. Окрім надійності, продуктивність також є одним із факторів, що впливають на якість мережі Інтернет. Технологія потрібна для підтримки продуктивності в мережі Інтернет, наприклад технологія Etherchannel. Існує два протоколи etherchannel, а саме протокол LACP і протокол PAgP. Щоб з'ясувати продуктивність комбінації цих протоколів у мережі, потрібне дослідження. Дослідження було проведено шляхом вимірювання кількох сценаріїв з використанням протоколу FTP у мережі VLAN, що призвело до значень параметрів якості обслуговування, а саме пропускної здатності, затримки та втрати пакетів. Комбінація протоколів GLBP і PAGP є кращою за пропускною спроможністю та значеннями затримки в звичайних умовах і умовах відновлення після відмови, але має значення втрати пакетів, яке трохи не краще, ніж інші комбінації в кількох сценаріях.

В роботі [8] було впроваджено удосконалення до математичної моделі відмовостійкої маршрутизації, що забезпечує резервування шлюзу за замовчуванням та балансування навантаження між крайовими маршрутизаторами. Основою цих удосконалень є формулювання задачі відмовостійкої маршрутизації в рамках оптимізаційного підходу.

У цій моделі ключовим моментом є введення умов балансування навантаження, яке приходить від мереж доступу, між прикордонними маршрутизаторами. Важливо зазначити, що враховується надійність цих маршрутизаторів, вимірювана через коефіцієнт доступності.

Дослідження, проведені в цій роботі, демонструють ефективність мережевих рішень, базованих на пропонованій моделі відмовостійкої маршрутизації. Виявлено, що незначна різниця в надійності граничних маршрутизаторів не погіршує максимальний поріг використання мережевих

каналів. В той же час, в певних випадках було виявлено невелике збільшення (на 3%) максимального порогу при значній різниці в надійності маршрутизаторів, але такий сценарій є атиповим для сучасних інфокомунікаційних мереж.

Таким чином стає очевидно, що є потреба в розробці удосконаленої моделі, яка б більше враховувала фактори, такі як Traffic Engineering, пропускна спроможність каналів, надійність маршрутизаторів та інші мережеві метрики. Це допоможе забезпечити високі показники якості обслуговування.

Наступна робота [9] присвячена питанням безпеки в HSRP та розробці комплексного підходу до захисту мережі від атак та неправильних конфігурацій. Автори аналізують потенційні вразливості HSRP та розробляють набір методів та інструментів для їх виявлення та запобігання. Вони також досліджують можливість використання криптографічних механізмів для захисту мережевої інформації та забезпечення безпеки комунікацій між маршрутизаторами. Результати показують збільшення рівня безпеки HSRP та зменшення ризику атак та неправильних конфігурацій.

Усі ці наукові роботи представляють різні аспекти вдосконалення та покращення FHRP. Вони показують актуальність теми відмовостійкої маршрутизації та напрямки розвитку наукових досліджень у цій галузі. Усі розробки представлені у вищенаведених роботах можуть бути відмінною основою для подальшого аналізу та розробки нових рішень щодо забезпечення відмовостійкої маршрутизації в ІКМ.

1.4 Формулювання вимог до перспективних рішень у цій області

На основі аналізу існуючих протоколів відмовостійкої маршрутизації і огляду наукових робіт можна сформулювати декілька основних вимог до перспективних рішень в цій області:

- покращення відмовостійкої маршрутизації. Нові рішення повинні забезпечувати високий рівень доступності маршрутизаторів і здатність швидко відновлювати роботу при відмовах;
- ефективний розподіл навантаження. Чим краще розподіляється навантаження між маршрутизаторами в групі, тим вище загальна продуктивність мережі і тим більше користувачів може обслуговувати мережа без втрати якості обслуговування;

- гнучкість налаштувань. Кожна мережа має свої особливості і вимоги, тому нові рішення повинні бути достатньо гнучкими, щоб можна було адаптувати їх до будь-яких умов;
- простота впровадження і підтримки. Нові рішення повинні бути не тільки ефективними, але й простими у впровадженні і підтримці. Це забезпечить їх широке застосування і популярність серед спеціалістів в області мереж.

Враховуючи ці вимоги, можна стверджувати, що в області відмовостійкої маршрутизації є значний потенціал для подальших досліджень і інновацій.

З метою досягнення вищезазначених цілей пропонується розробка нового протоколу на основі існуючого протоколу GLBP, який би враховував пропускну здатність мережі, надійність мережевих пристроїв та ґрунтувався на новій потоковій математичній моделі для відмовостійкої маршрутизації, яка буде розглянута у наступному розділі.

Крім того, рекомендується забезпечити можливість автоматичного налаштування протоколу для уникнення помилок, пов'язаних з людським фактором. Традиційні протокольні і технологічні засоби часто не можуть гарантувати виконання всіх потреб сучасних мереж. Проблема полягає в тому, що багато з них базуються на графових моделях та методах пошуку найкоротшого шляху, що, на жаль, не дозволяє забезпечити всі вимоги до систем відмовостійкої маршрутизації.

2 ПОТОКОВА МОДЕЛЬ ВІДМОВОСТІЙКОЇ МАРШРУТИЗАЦІЇ В ІНФОКОМУНІКАЦІЙНІЙ МЕРЕЖІ

2.1 Опис обраної математичної моделі відмовостійкої маршрутизації з балансуванням навантаження

Структура ІКМ (рис. 2.1), буде представлена у вигляді графа $\Gamma = (M, L)$ (рис. 2.2). Множина вершин графа $M = R \bigcup V$, містить у собі дві підмножини: $R = \{R_i, i = \overline{1,m}\}$ – вершини, які відображають маршрутизатори, та $V = \{V_j, j = \overline{1,v}\}$ – вершини, що моделюють мережі доступу (МД). Множина вершин маршрутизаторів складається з двох підмножин – $R = R^+ \bigcup R^-$. Де R^+ – підмножина вершин, які є моделями прикордонних маршрутизаторів ІКМ, тобто маршрутизатори, до яких можуть підключатись мережі доступу, а $m^+ = |R^+|$ – кількість прикордонних маршрутизаторів; R^- – підмножина вершин, що відображають транзитні маршрутизатори, де $m^- = |R^-|$ – їх кількість в інфокомунікаційної мережі.

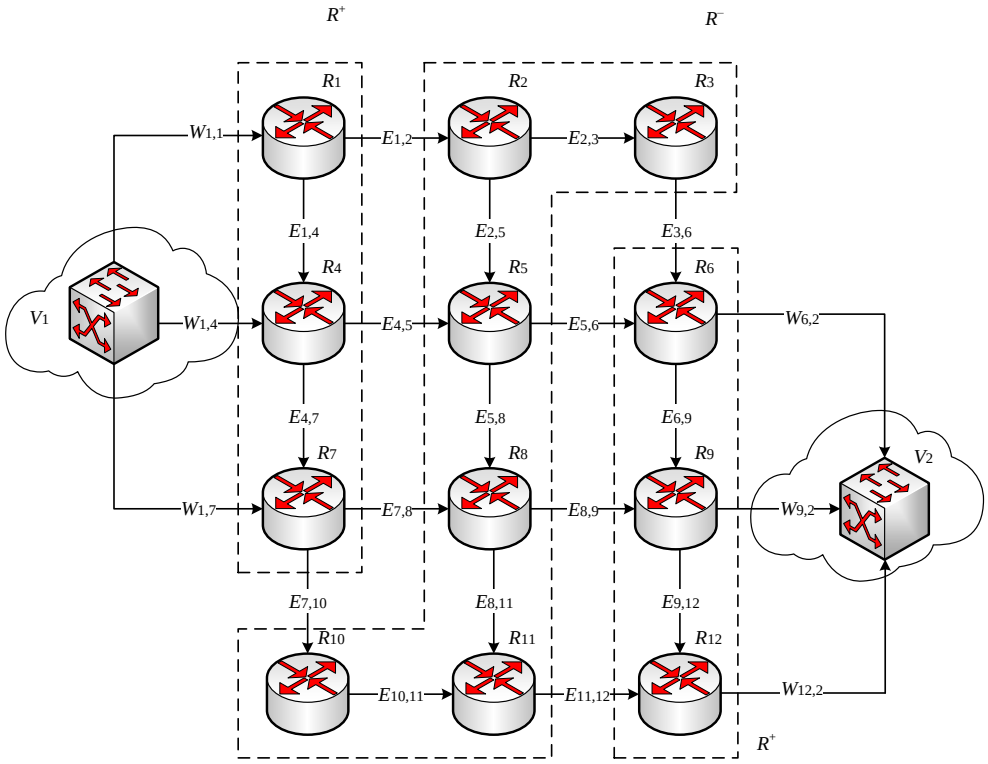

Рисунок 2.1 – Приклад структури ІКМ

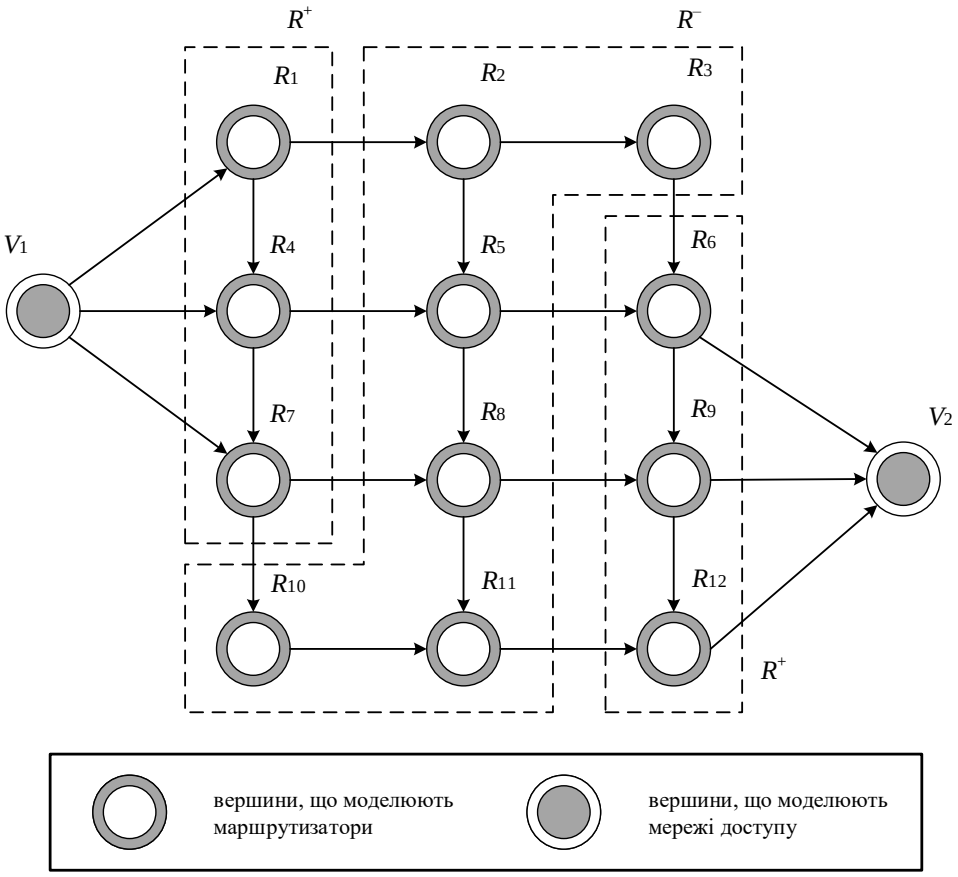

Рисунок 2.2 – Графова модель ІКМ

Припустимо, що R_j^+ – підмножина прикордонних маршрутизаторів R^+, яка включає маршрутизатори, що реалізують віртуальний маршрутизатор для мережі V_j. Визначимо $m_j^+ = \left|R_j^+\right|$ як кількість прикордонних маршрутизаторів, які реалізують віртуальний маршрутизатор для мережі доступу V_j . На рис. 2.1, наведено приклад, що для першої мережі доступу множина маршрутизаторів, представлених вершинами R_1, R_4 та R_7, є віртуальним маршрутизатором, тобто $m_1^+ = 2$.

Множина дуг $L = E \bigcup W$ графа Г (рис. 2.2) також містить дві підмножини: $E = \left\{E_{i,j}, i, j = \overline{1,m}, i \neq j\right\}$ – множина каналів зв'язку інфокомунікаційної мережі, $W = \left\{W_{i,j}, i = \overline{1,v}, j = \overline{1,m^+}\right\}$ – лінії доступу, що з'єднують прикордонні маршрутизатори та мережі доступу.

Припустимо, що в ІКМ передають пакети декількох потоків, які ми позначимо як K. Тоді кожний k-тий потік ($k \in K$) відповідає ряду параметрів:

V_s^k – мережа доступу, з якої походять пакети; V_d^k – мережа доступу, яка приймає цей потік пакетів; λ^k – середня пакетна інтенсивність k-го потоку (1/с). В процесі реалізації маршрутизації з балансуванням навантаження в ІКМ, потрібно визначити три типи управлінських змінних основного маршруту [10]:

$x_{i,j}^k$ – маршрутна змінна, яка визначає 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, що проходить через лінію доступу, представленій дугою $W_{i,j}$; $z_{j,i}^k$ – змінна доступу, яка характеризує частку k-го потоку, що проходить через лінію доступу, представленій дугою $W_{j,i}$.

При застосуванні одношляхового маршрутизаційного протоколу в мережі, на маршрутні змінні $x_{i,j}^k$ встановлюються наступні обмеження:

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

а у контексті багатошляхової маршрутизації:

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

Коли мережа доступу працює тільки з одним приграничним маршрутизатором ІКМ, всі доступні змінні підлягають обмеженню:

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

При реалізації балансування навантаження на рівні доступу, як, наприклад, в протоколах VRRP, GLBP та CARP, на ці змінні накладаються умови, схожі на (2.2):

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

Для забезпечення безпеки потоку на рівні доступу додаткові обмеження вводяться для керуючих змінних:

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

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

На рівні ІКМ загальні умови для збереження потоку будуть такі:

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

З виконанням умов (2.7) забезпечується взаємодія при обчисленні керуючих змінних трьох типів, і тепер можна координувати процеси балансування навантаження на рівні доступу та в цілому по ІКМ.

Для забезпечення балансування навантаження в мережі на основі принципів ТЕ, в модель вводяться такі обмеження для уникнення перевантаження:

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

де $\varphi_{i,j}$ – пропускна здатність каналу зв'язку, який представлений дугою $E_{i,j}$; α – верхня межа завантаженості каналів зв'язку ІКМ, яка є додатковою керуючою змінною, на яку накладаються такі обмеження:

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

Таким чином, задачу балансування навантаження в ІКМ можна сформувати в оптимізаційній формі. Критерій оптимальності виражається умовою:

$$\underset{x,y,z,x,y,z,\alpha}{min\, \alpha} \tag{2.10}$$

а обмеженнями є умови (2.1)-(2.9).

Відповідно до характеристик та вимог технологічних завдань балансування навантаження, оптимізаційна задача (2.10) відноситься до різних класів (табл. 2.1). Коли будь-які керуючі змінні мають логічний (булевий) характер, тобто при наявності умов (2.1) та (2.3), задача балансування навантаження стає оптимізаційною задачею змішаного цілочисельного лінійного програмування,

оскільки змінна приймає лише реальні значення. Якщо балансування навантаження реалізується як на рівні доступу (4), так і в цілому по ІКМ (2), то сформована оптимізаційна задача входить до класу задач лінійного програмування.

Таблиця 2.1. Оптимізаційні задачі 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
Модель 2		З балансуванням навантаження, багатошляхова маршрутизація (2)	Задача змішаного цілочисельного лінійного програмування
Модель 3	З балансуванням навантаження (4)		Задача лінійного програмування

2.2 Умови захисту елементів в ІКМ

Аби забезпечити стійкість до відмов ІКМ, потрібно встановити керуючі змінні, які визначають додаткові (резервні) маршрути в мережі [11]:

– $\overset{-k}{x}_{i,j}$ – змінна (маршрутна), яка вказує частку k–го потоку в каналі зв'язку $E_{i,j}$ резервного маршруту;

– $\overset{-k}{y}_{i,j}$ – змінна доступу, яка відображає частку k – го потоку, що протікає в резервній лінії доступу $W_{i,j}$;

– $\overset{-k}{z}_{i,j}$ – змінна доступу, яка характеризує частку k – го потоку, що протікає в резервній лінії доступу $W_{i,j}$.

Аналогічно до випадку створення основного маршруту, змінні доступу для резервного маршруту обмежені умовами, подібними до (2.2) та (2.4). Більше того, ті самі умови (2.3)-(2.4) мають відповідно запобігати втраті пакетів і забезпечити збереження потоку в транспортній мережі для резервного маршруту.

Для впровадження схеми захисту за замовчуванням з можливістю балансування навантаження по всім доступним інтерфейсам віртуального маршрутизатора в модель вводяться нелінійні умови [11]:

$$\sum_{i:V_i \in V} y_{i,j}^k \bar{y}_{i,j}^k + \sum_{n:E_{j,n} \in E} x_{j,n}^k \bar{x}_{j,n}^k = 0, R_j \in R^+. \quad (2.11)$$

Якщо ці умови виконуються, це забезпечує, що прикордонний маршрутизатор *Rj* (тобто всі канали зв'язку та лінії доступу, що виходять з цього вузла) використовується або основним, або резервним маршрутом.

Для відвернення потенційного перевантаження комунікаційних каналів ТМ вводяться такі умови [11]:

$$\begin{cases} x_{i,j}^k + \bar{x}_{i,j}^k \le 1; \\ y_{i,j}^k + \bar{y}_{i,j}^k \le 1; \\ z_{i,j}^k + \bar{z}_{i,j}^k \le 1; \end{cases} \quad (2.12)$$

Дотримання умов (2.12) гарантує, що прикордонний маршрутизатор *Rj* буде використано лише в одному маршруті – основному або резервному.

Отже, при вирішенні технологічного завдання щодо відмовостійкої маршрутизації в разі реалізації багатошляхової стратегії в ТМ та балансування навантаження на рівні прикордонних маршрутизаторів, оптимізаційне завдання прийме форму задачі нелінійного програмування з обмеженнями (2.2), (2.4)–(2.7).

2.3 Результати розрахунків по визначенню основних маршрутів в ІКМ

Припустимо, як це показано на рис. 2.3, джерелом потоку пакетів є мережа доступу V_1, тоді як мережа доступу V_2 приймає пакети цього потоку.

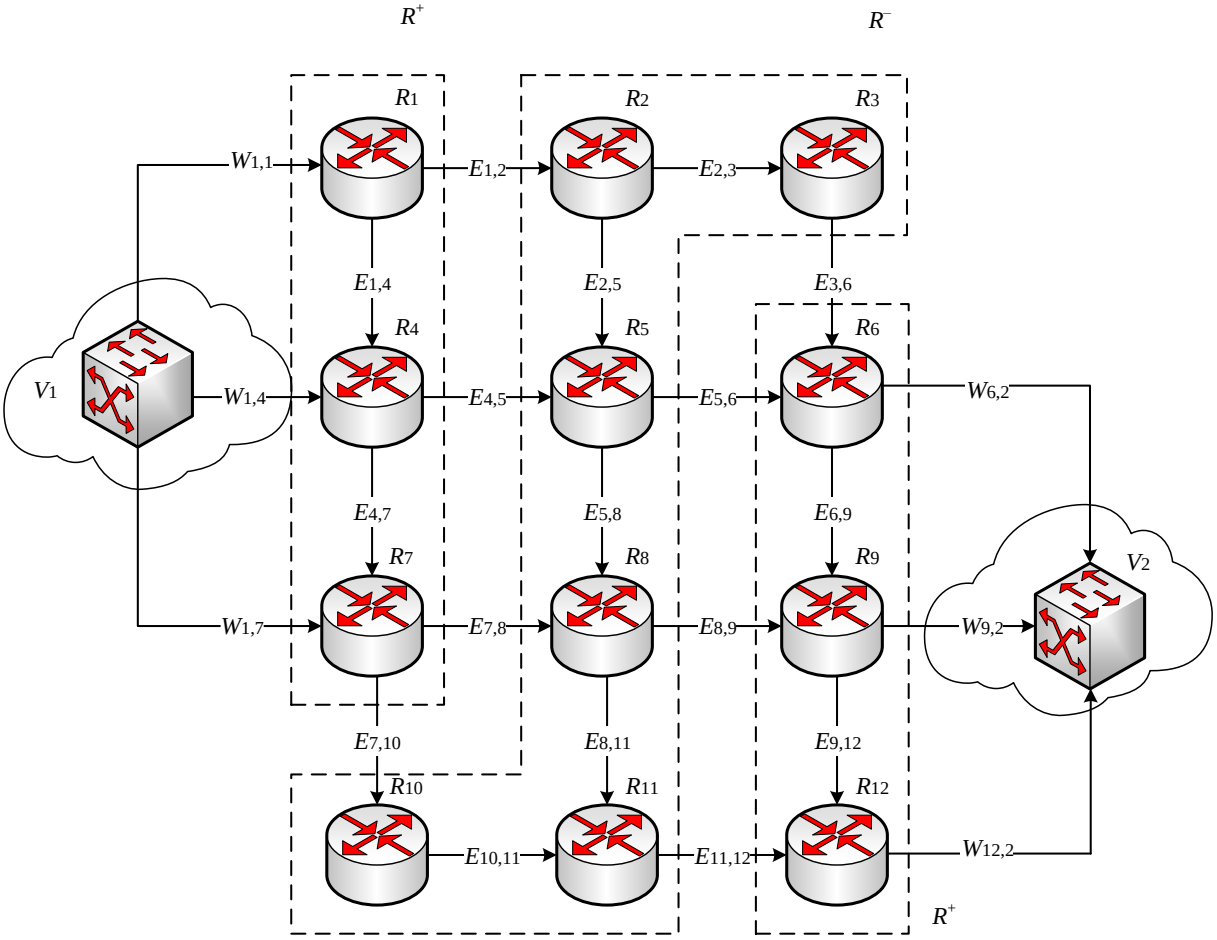

Рисунок 2.3 – Приклад структури ІКМ

В таблиці 2.2 наведені дані про пропускну здатність каналів зв'язку.

Таблиця 2.2 – Пропускні здатності каналів зв’язку транспортної мережі

Канал зв’язку	$E_{1,2}$	$E_{2,3}$	$E_{1,4}$	$E_{2,5}$	$E_{3,6}$	$E_{4,5}$	$E_{5,6}$	$E_{4,7}$	$E_{5,8}$
Пропускна здатність, 1/с	950	300	900	400	600	700	600	450	600
Канал зв’язку	$E_{6,9}$	$E_{7,8}$	$E_{8,9}$	$E_{7,10}$	$E_{8,11}$	$E_{9,12}$	$E_{10,11}$	$E_{11,12}$	
Пропускна здатність, 1/с	700	400	600	800	500	900	700	800	

Під час дослідження оцінювалась ефективність вирішення задачі балансування навантаження в ІКМ, було використано три моделі (табл. 2.1). Варіювалась інтенсивність потоку від 10 до 950 1/с. Динаміку зміни максимального рівня навантаження на комунікаційні канали ІКМ відносно інтенсивності потоку пакетів, які надходили до мережі, можна побачити на рис. 2.4.

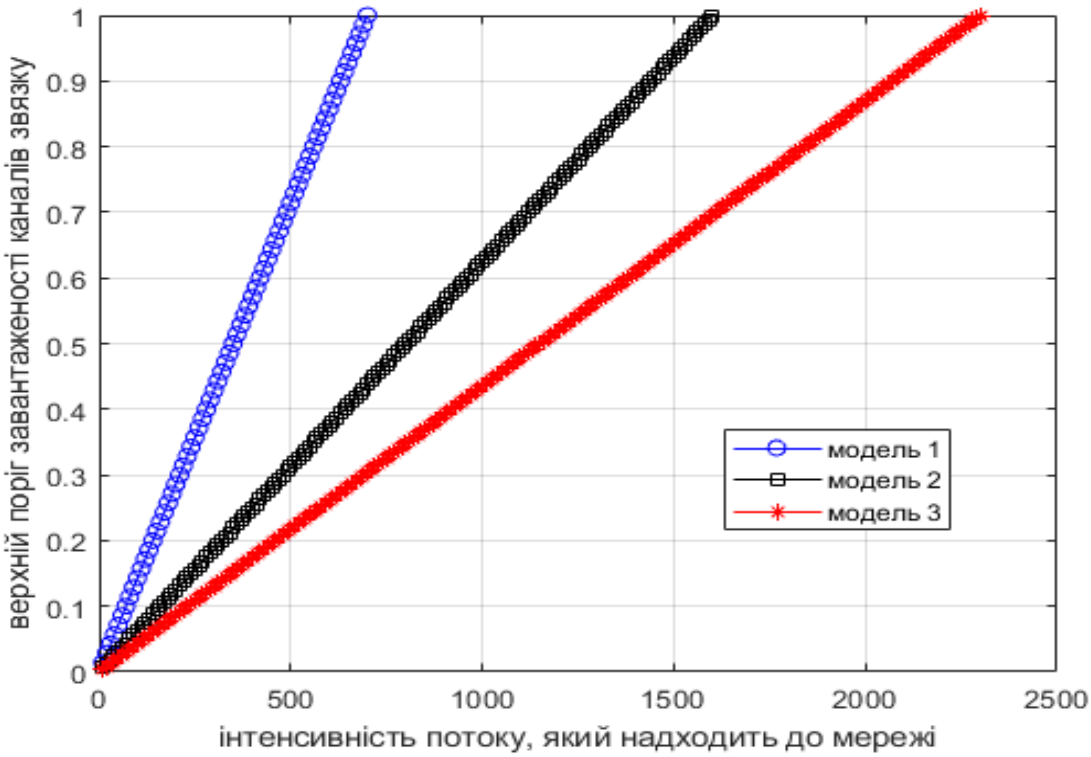

Рисунок 2.4 – Динаміка зміни верхнього порогу завантаженості каналів зв'язку ІКМ в залежності від інтенсивності потоку пакетів, який надходив до мережі

Як наведено на рис. 2.4, відсутність балансування навантаження на рівні доступу та в ІКМ загалом (модель 1) призводила до перевантаження мережі вже при $\lambda > 700$ 1/с. Рис. 2.5 демонструє розподіл трафіку без балансування навантаження на рівні доступу та при одношляховій маршрутизації на рівні ІКМ при $\lambda = 700$ 1/с. Весь потік пакетів в ІКМ з першої мережі доступу був спрямований на сьомий прикордонний маршрутизатор, а потім до другої мережі доступу передавався за маршрутом:

$R_7 \to R_{10} \to R_{11} \to R_{12}$.

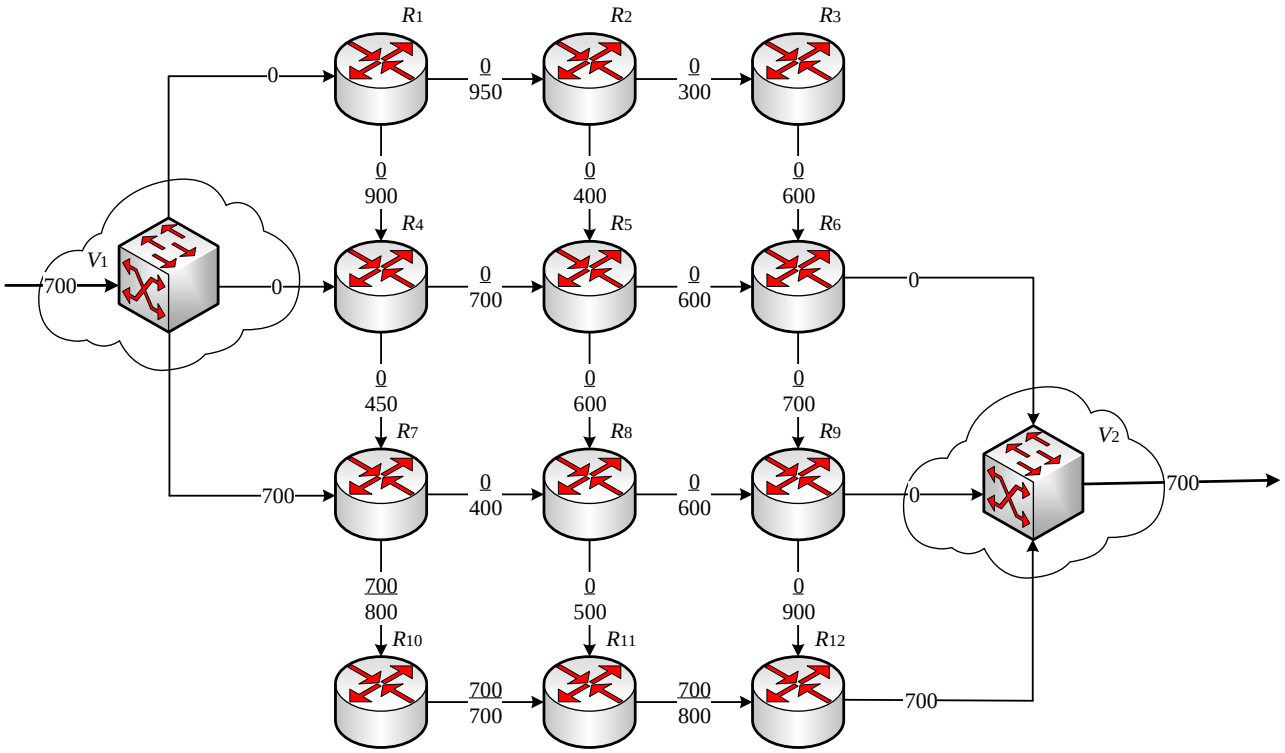

Рисунок 2.5– Порядок розподілу трафіка без балансування навантаження на рівні доступу та одношляхової маршрутизації та рівні ІКМ

У разі впровадження багатошляхової маршрутизації в ІКМ, без балансування навантаження між прикордонними маршрутизаторами (модель 2), мережа могла обслуговувати потік пакетів із максимальною інтенсивністю 1600 1/с, що в 2,28 рази більше, ніж у моделі 1. На рис. 2.6 зображено розподіл трафіку без балансування навантаження на рівні доступу та при багатошляхової маршрутизації на рівні ІКМ при $\lambda = 1600$ 1/с. Весь потік пакетів в ІКМ з першої мережі доступу був спрямований на перший прикордонний маршрутизатор, а потім до другої мережі доступу передавався по іншим маршрутам:

$R_1 \to R_2 \to R_3 \to R_6 \to R_9 \to R_{12}$ з інтенсивністю 300 1/с;

$R_1 \to R_2 \to R_5 \to R_8 \to R_{11} \to R_{12}$ з інтенсивністю 400 1/с;

$R_1 \to R_4 \to R_7 \to R_{10} \to R_{11} \to R_{12}$ з інтенсивністю 200 1/с;

$R_1 \to R_4 \to R_7 \to R_8 \to R_{11} \to R_{12}$ з інтенсивністю 100 1/с;

$R_1 \to R_4 \to R_7 \to R_8 \to R_9 \to R_{12}$ з інтенсивністю 150 1/с;

$R_1 \to R_4 \to R_5 \to R_6 \to R_9 \to R_{12}$ з інтенсивністю 250 1/с;

$R_1 \to R_4 \to R_5 \to R_8 \to R_9 \to R_{12}$ з інтенсивністю 200 1/с.

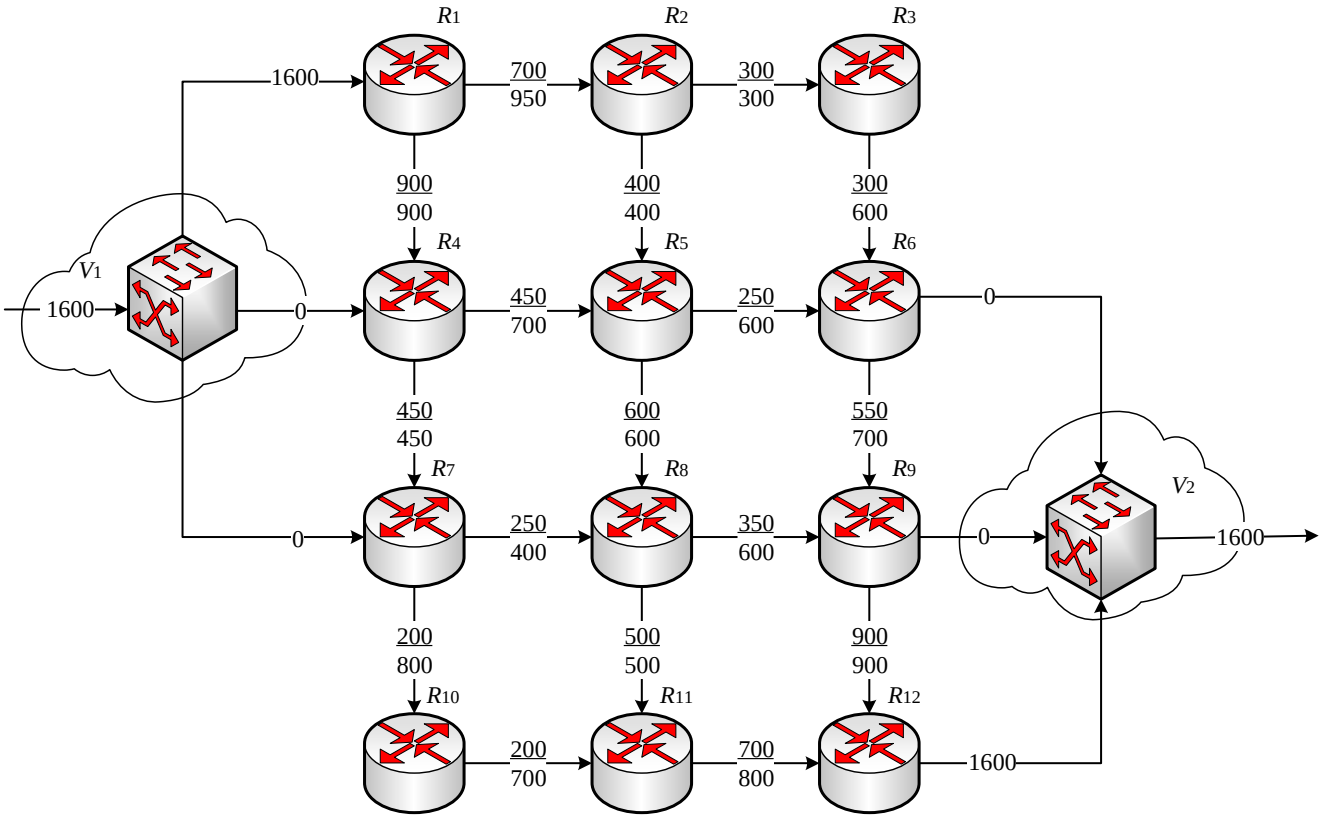

Рисунок 2.6 – Порядок розподілу трафіка без балансування навантаження на рівні доступу та багатошляхової маршрутизації та рівні ІКМ

Коли балансування навантаження відбувалося як на рівні доступу, так і на рівні ІКМ (модель 3), мережа змогла обслужити потік пакетів з максимальною інтенсивністю в 2300 1/с, що на 43,75% більше, ніж у моделі 2, та в 3,28 разів більше, ніж у моделі 1. На рис. 2.7 зображено балансування навантаження на рівні доступу та ІКМ при $\lambda = 2300$ 1/с. Балансування потоку пакетів, що надходив від першої мережі доступу, здійснювалося між першим, четвертим та сьомим маршрутизаторами у відношенні 21,7 на 30,4 на 47,8 %. Потім в ІКМ до другої мережі доступу трафік передавався за шістьома маршрутами:

$R_1 \to R_2 \to R_3 \to R_6$ з інтенсивністю 300 1/с;

$R_1 \to R_2 \to R_5 \to R_8 \to R_9$ з інтенсивністю 200 1/с;

$R_4 \to R_5 \to R_6$ з інтенсивністю 600 1/с;

$R_4 \to R_5 \to R_8 \to R_{11} \to R_{12}$ з інтенсивністю 100 1/с;

$R_7 \to R_8 \to R_9$ з інтенсивністю 400 1/с;

$R_7 \to R_{10} \to R_{11} \to R_{12}$ з інтенсивністю 700 1/с.

Трафік з ІКМ до другої мережі доступу надходив через шостий, дев'ятий та дванадцятий маршрутизатори у відношенні 39,1 на 34,7 на 26%.

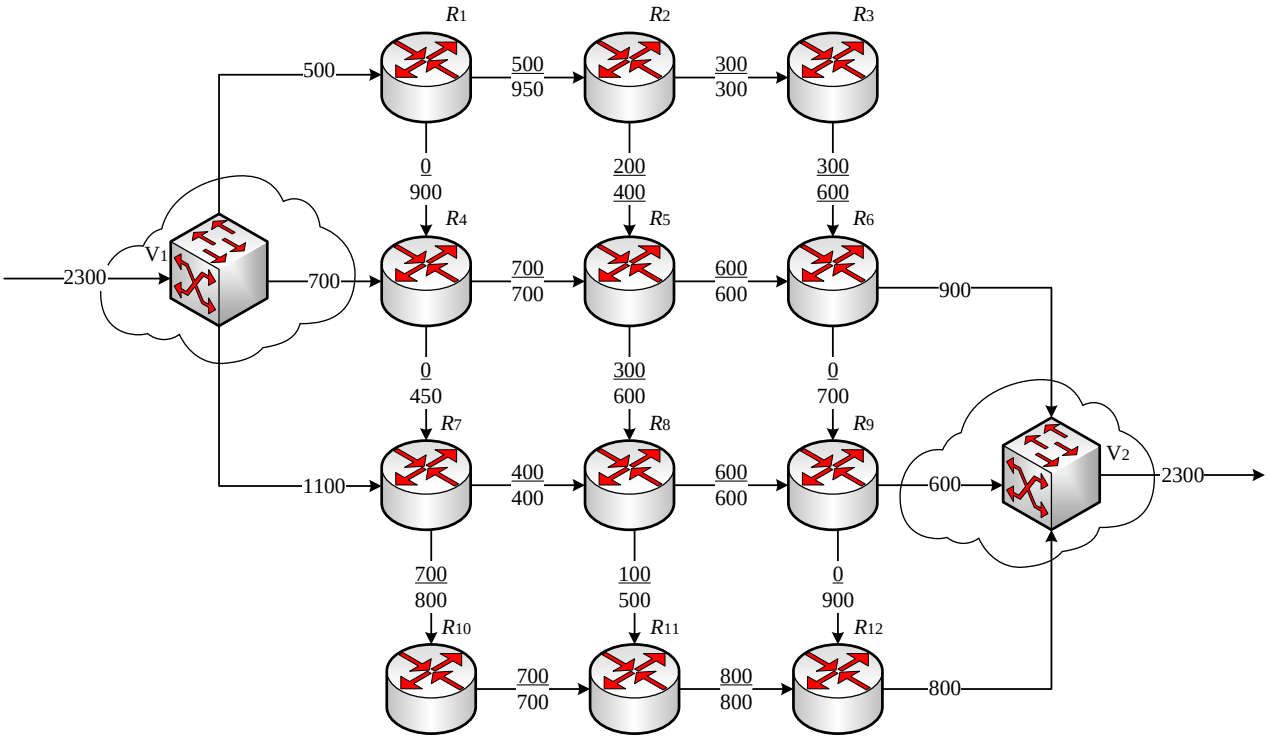

Рисунок 2.7 – Порядок балансування навантаження на рівнях доступу та ІКМ

Аналіз отриманих результатів (рис. 2.4) показав, що впровадження принципів балансування навантаження, передбачених в моделі 3, дозволило зменшити максимальний рівень використання каналів зв'язку мережі (12) в середньому на 69,57% порівняно з моделлю 1 та на 30,43% порівняно з моделлю 2. Використання моделі 2 сприяло покращенню показника (12) порівняно з моделлю 1 в середньому на 56,26%. Отримані результати представлені в таблиці 2.3.

Таблиця 2.3 – Результати аналізу 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	2,2	56,26%.
3-1	2,76	69,57%
3-2	1,2	30,43%

На основі проведеного аналізу (рис. 2.4), було з'ясовано, що модель, в якій балансування навантаження відбувається як на рівні доступу, так і на рівні ІКМ (модель 3), має переваги над моделями без балансування навантаження в плані продуктивності та максимального рівня використання каналів зв'язку (табл. 2.3). Саме через це майбутні рішення з резервними маршрутами будуть базуватися на моделі 3 (рис.2.7).

2.4 Дослідження процесів відмовостійкої маршрутизації при реалізації різних схем захисту елементів мережі

2.4.1 Реалізація схем захисту шлюзу за замовчуванням

У роботі проведено дослідження на прикладі захисту маршрутизаторів R_4 на вході та R_9 на виході транспортної мережі.

На рис.2.8 зображені результати захисту прикордонного маршрутизатора R_4. За основу була взята схема балансування навантаження, яка описана на рис. 2.7.

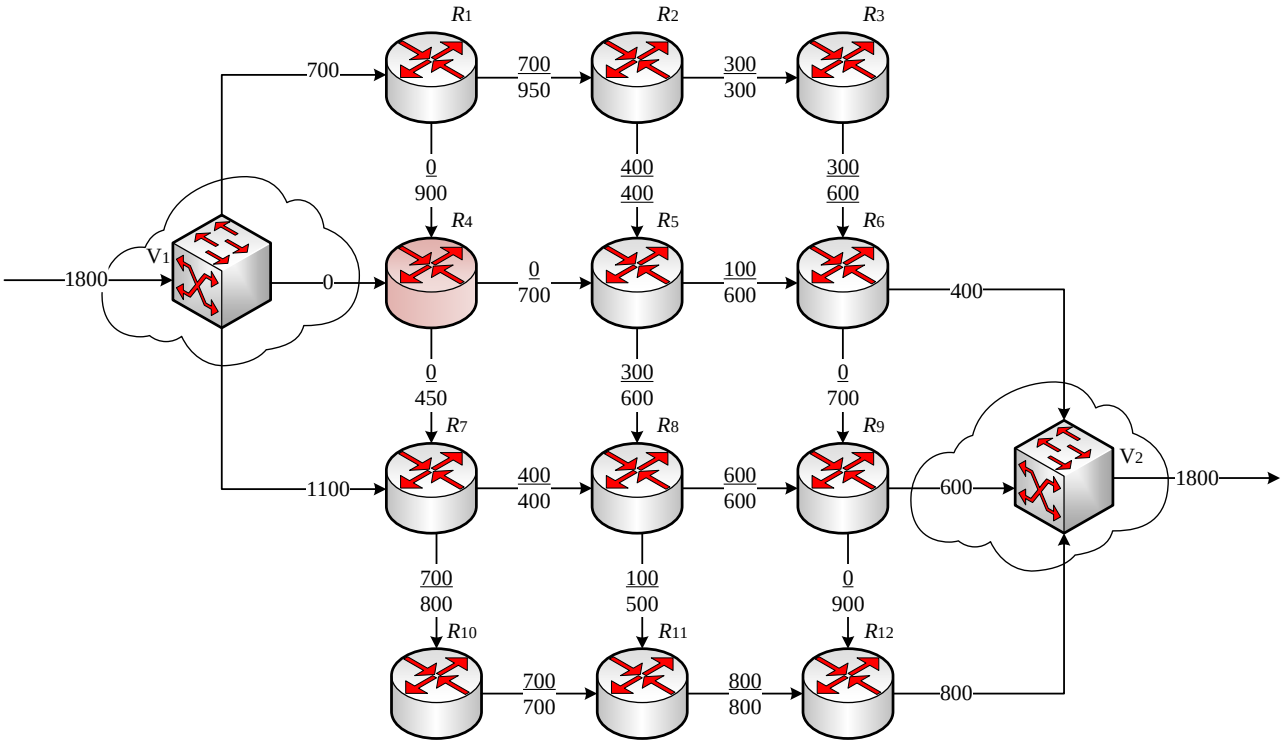

Рисунок 2.8 – Резервний маршрут балансування навантаження на рівнях доступу та ІКМ із захистом маршрутизатора R_4

Використовуючи захисні механізми маршрутизатора R_4 та балансування навантаження на обох рівнях - доступу та ІКМ, мережа демонструвала здатність обробляти потік пакетів з піковою інтенсивністю до 1800 пакетів за секунду. Це становить зростання на 12,5% порівняно з моделлю 2, та більш ніж вдвічі перевищує показники моделі 1.

Рисунок 2.8 демонструє процес балансування навантаження на різних рівнях при частоті $\lambda = 1800$ 1/с. Варто зазначити, що потік пакетів з першої мережі доступу був розподілений між першим та сьомим маршрутизаторами в співвідношенні 38,88% до 61,11%.

Від ІКМ, трафік був направлений до другої мережі доступу по шести маршрутам, що дозволило оптимізувати розподіл навантаження:

$R_1 \to R_2 \to R_3 \to R_6$ з інтенсивністю 300 1/с;

$R_1 \to R_2 \to R_5 \to R_6$ з інтенсивністю 100 1/с;

$R_1 \to R_2 \to R_5 \to R_8 \to R_9$ з інтенсивністю 200 1/с;

$R_1 \to R_2 \to R_5 \to R_8 \to R_{11} \to R_{12}$ з інтенсивністю 100 1/с;

$R_7 \to R_8 \to R_9$ з інтенсивністю 400 1/с;

$R_7 \to R_{10} \to R_{11} \to R_{12}$ з інтенсивністю 700 1/с.

Тобто з ІКМ до другої мережі доступу трафік надходив через шостий, дев’ятий та дванадцятий маршрутизатори у пропорції 22,2 на 33,3 на 44,5%.

Отже, при формуванні резервного маршруту прикордонний маршрутизатор R4 не використовували, а це означає, що умову захисту було виконано.

На рис. 2.9 представлено результат реалізації схеми захисту шлюзу за замовчуванням (маршрутизатора R_9).

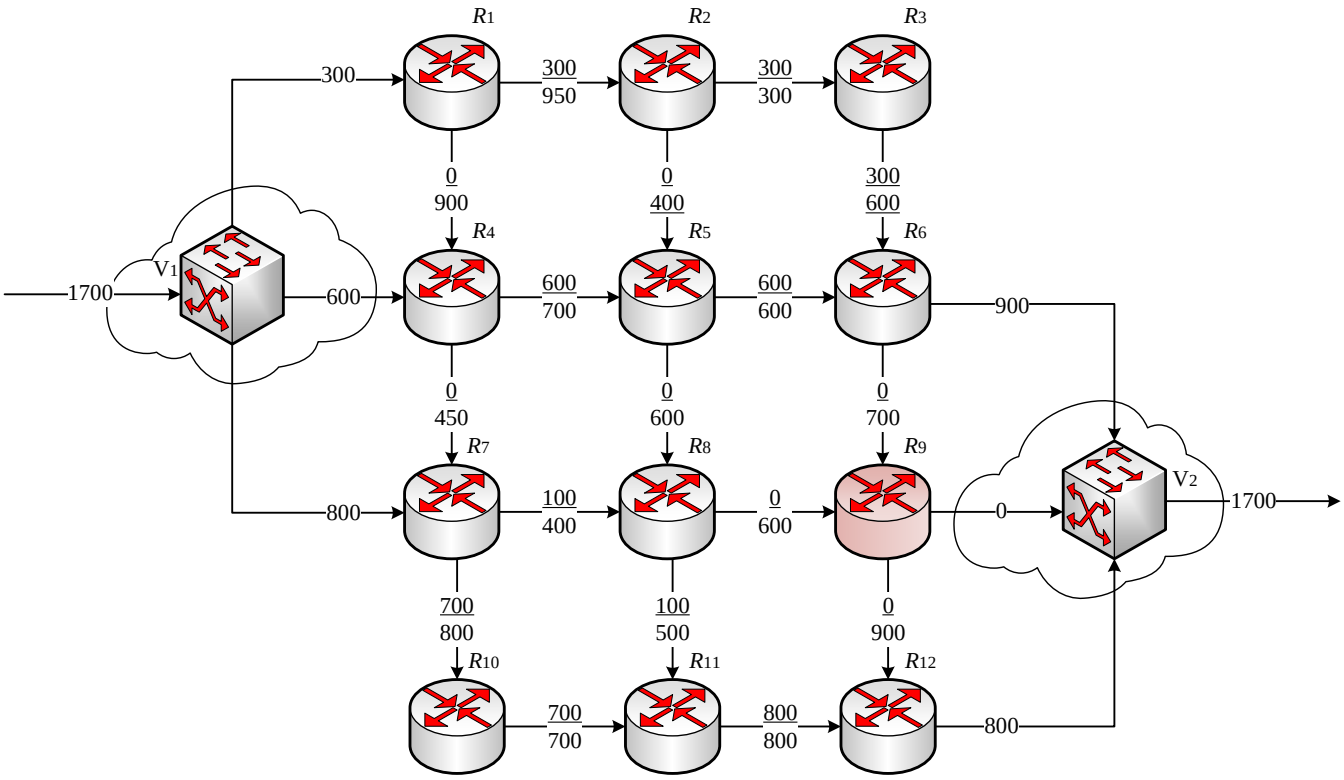

Рисунок 2.9 – Резервний маршрут балансування навантаження на рівнях доступу та ІКМ із захистом маршрутизатора R_9

Завдяки впровадженню захисту на маршрутизаторі R_9та балансуванню навантаження на двох рівнях - доступу та ІКМ, мережа впоралась з обробкою пікового потоку пакетів, що досягав 1700 пакетів за секунду. Це на 6,25% вище, ніж показники моделі 2, та більш ніж у два рази перевищує результати моделі 1.

Процес балансування навантаження на обох рівнях при частоті $\lambda = 1700$ 1/с ілюстровано на рисунку 2.9. Пакети, що прибувають від першої мережі доступу, розподілялися між першим, четвертим та сьомим маршрутизаторами у співвідношенні 17,65%, 35,29% та 47,06% відповідно.

Після цього, в ІКМ, трафік направлявся до другої мережі доступу по чотирьом визначеним маршрутам, що забезпечувало ефективне розподілення навантаження:

$R_1 \to R_2 \to R_3 \to R_6$ з інтенсивністю 300 1/с;

$R_4 \to R_5 \to R_6$ з інтенсивністю 600 1/с;

$R_7 \to R_{10} \to R_{11} \to R_{12}$ з інтенсивністю 700 1/с;

$R_7 \to R_8 \to R_{11} \to R_{12}$ з інтенсивністю 100 1/с.

Інформація з ІКМ була направлена до другої мережі доступу, використовуючи шостий та дванадцятий маршрутизатори, розподіл трафіку між якими склав 52,94% та 47,06% відповідно. Цей процес був здійснений без використання маршрутизатора R9, що свідчить про виконання умови захисту.

2.4.2 Дослідження схем захисту маршрутизаторів транспортної мережі

У випадку, коли балансування проводилось на обох рівнях - доступу та ІКМ, з додатковим захистом від маршрутизатора R_5, максимальний обсяг обслуговуваного трафіку досяг 1400 пакетів за секунду. Цей показник менший на 14,28% в порівнянні з моделлю 2, але удвічі перевищує ефективність моделі 1.

На рисунку 2.10 представлено деталі процесу балансування навантаження на обох рівнях при частоті $\lambda = 1400$ 1/с. Пакети від першої мережі доступу були розподілені між першим та сьомим маршрутизаторами у співвідношенні 21,43% проти 78,57%. Після цього, в ІКМ, трафік направлявся до другої мережі доступу через три маршрути:

$R_1 \to R_2 \to R_3 \to R_6$ з інтенсивністю 300 1/с;

$R_7 \to R_8 \to R_9$ з інтенсивністю 400 1/с;

$R_7 \to R_{10} \to R_{11} \to R_{12}$ з інтенсивністю 700 1/с.

Трафік з ІКМ до другої мережі доступу розподілявся між трьома маршрутизаторами: шостим, дев'ятим та дванадцятим. Цей розподіл був у пропорції 21,43%, 28,57% та 50% відповідно.

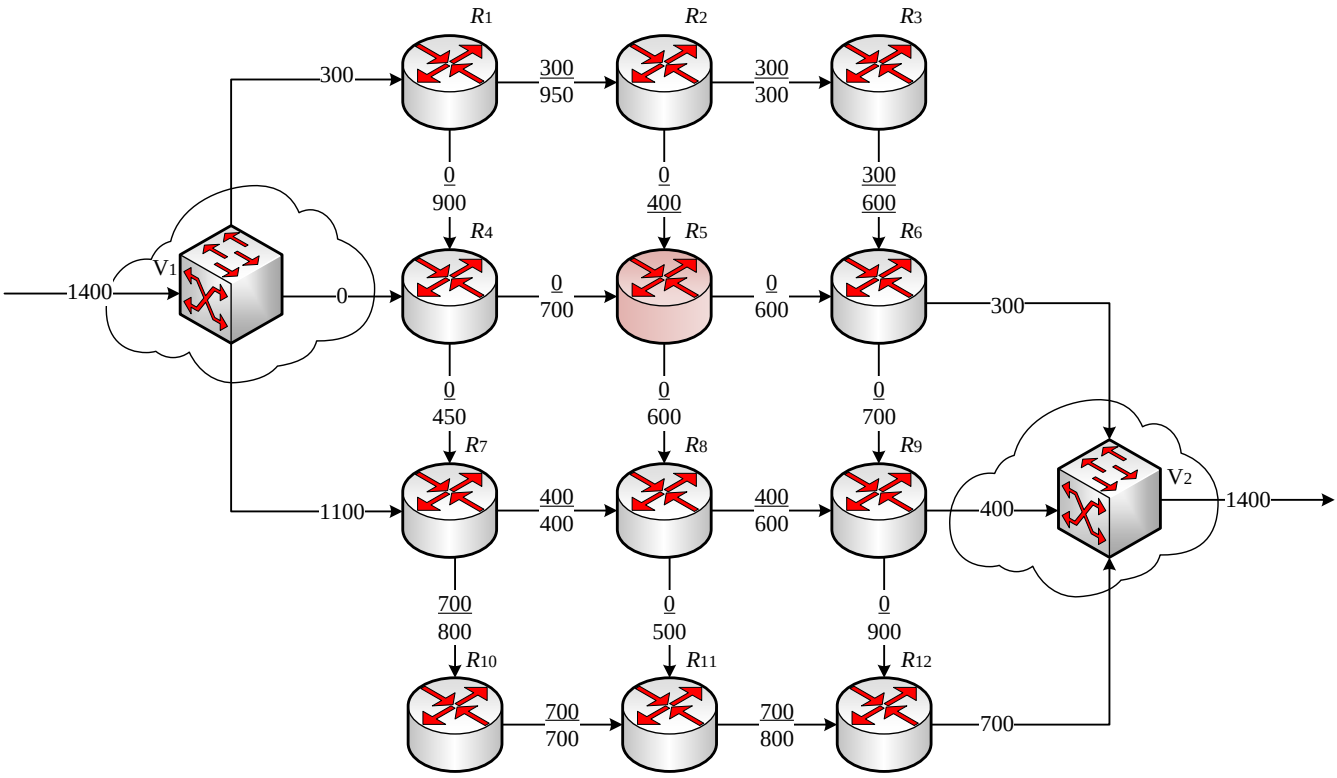

Рисунок 2.10 – Порядок балансування навантаження на рівнях доступу та ІКМ із захистом маршрутизатора R_5

В ситуації, коли балансування здійснювалось на обох рівнях - доступу та ІКМ, із додатковим захистом через маршрутизатор R_8, мережа забезпечувала обробку потоку даних з максимальною інтенсивністю 1600 пакетів за секунду. Це відповідає результатам для моделі 2 та у 2,28 рази перевищує ефективність моделі 1.

Детальну схему балансування навантаження на цих рівнях за даною інтенсивністю представлено на рисунку 2.11. Пакети даних, що надходили від першої мережі доступу, розподілялися між першим, четвертим та сьомим маршрутизаторами у відношенні 18,75%, 37,5% та 43,75% відповідно. Далі в ІКМ до другої мережі доступу трафік передавався за трьома маршрутами:

$R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_6$ з інтенсивністю 300 1/с;

$R_4 \rightarrow R_5 \rightarrow R_6$ з інтенсивністю 600 1/с;

$R_7 \rightarrow R_{10} \rightarrow R_{11} \rightarrow R_{12}$ з інтенсивністю 700 1/с.

Трафік з ІКМ до іншої мережі доступу надходив через шостий та дванадцятий маршрутизатори у пропорції 56,25 на 43,75%.

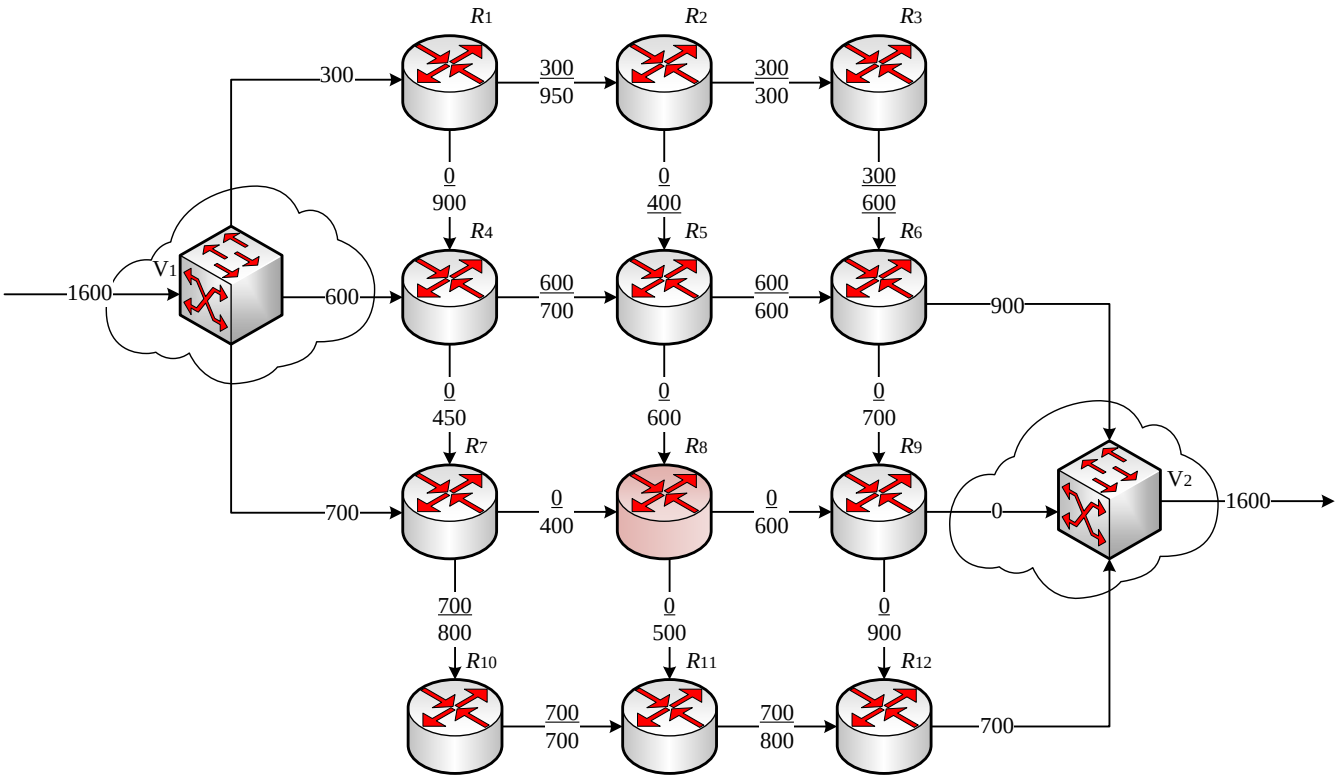

Рисунок 2.11 – Порядок балансування навантаження на рівнях доступу та ІКМ із захистом маршрутизатора R_8

У результаті аналізу було встановлено, що впровадження принципів відмовостійкої маршрутизації в моделі 3 призвело до зниження максимального навантаження на канали зв'язку мережі порівняно з моделями 1 і 2. Результати цього порівняння наведені у таблиці 2.4.

Таблиця 2.4 – Схема захисту маршрутизаторів

Схема захисту	Пропускна здатність			Виграш	
	Модель1	Модель 2	Модель 3	3-1	3-2
R_4	700	1600	1800	2,57 разів	12,5%
R_9	700	1600	1700	2,42 разів	6,25%
R_5	700	1600	1400	69,57%	30,43%
R_8	700	1600	1600	2,28 разів	-

Наведена математична модель була створена на основі комбінаторних графічних моделей, із метою поліпшення алгоритмів та механізмів для відмовостійкої маршрутизації. В ході проведення досліджень були отримані результати, які представлені на рис. 2.8-2.11 і направлені на відображення роботи багатошляхової відмовостійкої маршрутизації з балансуванням навантаження.

Аналіз представлених вище результатів вказує на те, що впровадження принципів відмовостійкої маршрутизації в моделі 3 дозволяє знизити максимальний рівень використання мережних комунікаційних каналів на 69,57% порівняно з моделлю 1 і на 30,43% порівняно з моделлю 2.

З огляду на це, в наступному розділі будуть висунути рекомендації щодо практичного застосування представленої математичної моделі та буде проведено аналіз протоколу GLBP метою якого є розширення його функціоналу.

3 ДОСЛІДЖЕННЯ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ДО ПРАКТИЧНОГО ЗАСТОСУВАННЯ ПРОТОКОЛУ GLBP

3.1 Приклад налаштування протоколу GLBP у режимі round robin з використанням пакету GNS3

Одним з ключових аспектів дослідницького процесу є розробка рекомендацій щодо практичного використання отриманих результатів у сучасних та майбутніх системах ІКМ. З цією метою було застосовано функціонал протоколу GLBP - протоколу маршрутизації, стійкого до відмов.

Щоб перевірити та використати отримані результати на практиці, проведено експеримент, з використанням програмного пакету GNS3.

Фрагмент мережі, що досліджується, складається з трьох маршрутизаторів (R1-R3) та двох комутаторів, які з'єднані між собою через порти Fast Ethernet. Шість робочих станцій (PC1-PC6) підключено до першого комутатора, а одна робоча станція (PC7) - до другого комутатора. Схема мережі для дослідження протоколу GLBP представлена на рис. 3.1.

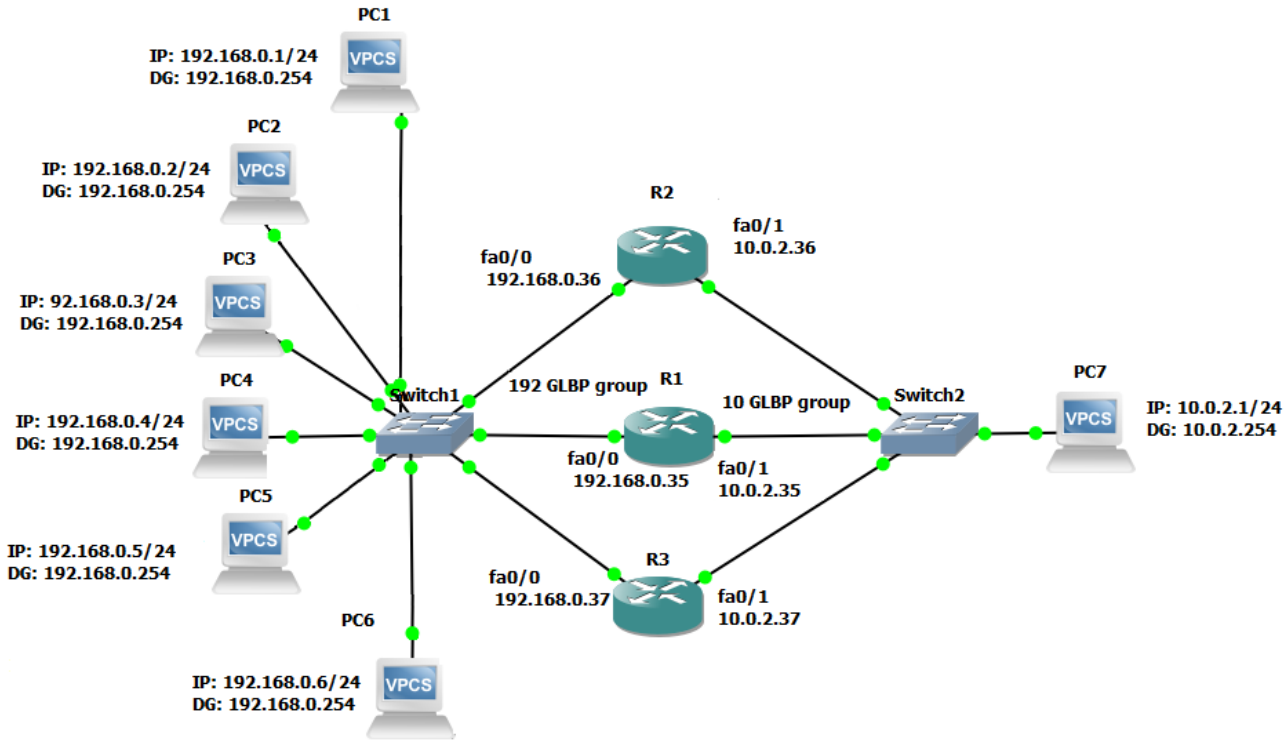

Рисунок 3.1 – Схема для дослідження протоколу GLBP

На рисунку 3.2 представлено приклад налаштування для робочої станції PC1. Віртуальний маршрутизатор, який служить шлюзом за замовчуванням для шести робочих станцій (PC1-PC6), створений в рамках 192-ї групи GLBP та має IP-адресу 192.168.0.254/24. Дані для налаштування кінцевих станцій представлено в таблиці 3.1.

Таблиця 3.1 – 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
PC6	192.168.0.6	255.255.255.0	192.168.0.254
PC7	10.0.2.1	255.255.255.0	10.0.2.254

Для конфігурації протоколу GLBP на маршрутизаторах мережі, були використані команди для маршрутизаторів R1-R3 [14]. Ці команди представлені на рисунках 3.3-3.5. Інтерфейси Fast Ethernet 0/0 маршрутизаторів R1-R3 були налаштовані на 192-у групу GLBP у режимі "round robin". Також було налаштовано 10-у групу GLBP у режимі "round robin" на інтерфейсах Fast Ethernet 0/1. "Round robin" означає, що трафік буде рівномірно розподілятися між маршрутизаторами.

```
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 3.2 – Приклад налаштування IP-адреси, маски та шлюзу за замовчуванням PC1

Маршрутизатор R1 було налаштовано шляхом встановлення IP-адрес на його інтерфейсах Fast Ethernet 0/0 та Fast Ethernet 0/1. За допомогою команди "ip

address", ми присвоїли цим інтерфейсам IP-адреси 192.168.0.35 та 10.0.2.35 відповідно. До кожної з цих адрес ми присвоїли маску підмережі 255.255.255.0.

Наступним кроком було налаштування віртуального шлюзу за замовчуванням для маршрутизатора R1. Для цього ми використали команди "glbp 192 ip 192.168.0.254" та "glbp 10 ip 10.0.2.254", що дозволило нам присвоїти IP-адреси шлюзу відповідним групам GLBP.

```
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 3.3 – Приклад налаштування протоколу GLPB на маршрутизаторі R1

Налаштування маршрутизатора R2 було проведено аналогічно до R1. Задали IP-адреси для інтерфейсів Fast Ethernet 0/0 та Fast Ethernet 0/1, використовуючи команду "ip address". Інтерфейсам було присвоєно адреси 192.168.0.36 та 10.0.2.36 відповідно, з маскою підмережі 255.255.255.0.

Далі було налаштувано віртуальний шлюз за замовчуванням для маршрутизатора R2. Для цього було використано команди "glbp 192 ip 192.168.0.254" та "glbp 10 ip 10.0.2.254". Це дозволило нам налаштувати відповідні IP-адреси шлюзу для груп GLBP.

```
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 3.4 – Приклад налаштування протоколу GLPB на маршрутизаторі R2

Для маршрутизатора R3, налаштування було проведено за тим же принципом. Інтерфейсам Fast Ethernet 0/0 та Fast Ethernet 0/1 було задано IP-адреси 192.168.0.37 та 10.0.2.37 відповідно, за допомогою команди "ip address". Маска підмережі була встановлена як 255.255.255.0.

Для налаштування віртуального шлюзу за замовчуванням для R3, були використані команди "glbp 192 ip 192.168.0.254" та "glbp 10 ip 10.0.2.254". Ці команди дозволили налаштувати IP-адреси шлюзу для відповідних груп GLBP.

```
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 3.5 – Приклад налаштування протоколу GLPB на маршрутизаторі R3

Щоб перевірити налаштування інтерфейсів маршрутизаторів, була використана команда "show ip interface brief".

Результати цієї перевірки можна побачити на рисунках 3.6-3.8.

```
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 3.6 – 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 3.7 – 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 3.8 – Приклад перевірки налаштованих IP адрес на маршрутизаторі R3

З аналізу отриманих даних можна побачити, що налаштування інтерфейсів маршрутизаторів було виконано правильно.

Використовуючи протокол ICMP та специфічно Echo Request повідомлення, перевіряється ефективність балансування навантаження. Для слідкування ICMP пакетів, що надходять на визначений інтерфейс маршрутизатора, було використано механізм списків контролю доступу (Access Control List, ACL), які відображені на рисунках 3.9-3.11.

Налаштування ACL здійснювалось через виконання команди: «access-list *номер* permit icmp *адреса мережі відправника обернена маска підмережі адреса мережі отримувача обернена маска підмережі*».

Щоб впевнитися, що інший трафік, крім ICMP, не буде заблоковано, була введена команда «access-list *номер* permit ip any any» , як показано на рисунках 3.9-3.11.

Останнім кроком було прикріплення цих налаштованих ACL до відповідних вхідних інтерфейсів Fast Ethernet 0/0 маршрутизаторів R1-R3. Таким чином, забезпечити ефективне слідкування та управління ICMP трафіком.

```
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 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 3.9 – 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 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 3.10 – 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 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 3.11 – Приклад налаштування листів контролю доступу на маршрутизаторі R3

Після активації списків контролю доступу на відповідних інтерфейсах, можемо спостерігати, як кількість спрацьовувань ACL розподіляється при приході ICMP-пакетів, що надсилаються до мережі призначення.

Для оцінки роботи протоколу GLBP у режимі round robin, було проведено експеримент. Використовуючи команду ping, було відправлено по 5 пакетів з кожного з комп'ютерів PC1-PC6 до комп'ютера PC7 для перевірки балансування навантаження. Деталі цього процесу можна переглянути на рисунку 3.12.

```
PC1> ping 10.0.2.1
84 bytes from 10.0.2.1 icmp_seq=1 ttl=63 time=30.208 ms
84 bytes from 10.0.2.1 icmp_seq=2 ttl=63 time=30.709 ms
84 bytes from 10.0.2.1 icmp_seq=3 ttl=63 time=30.202 ms
84 bytes from 10.0.2.1 icmp_seq=4 ttl=63 time=30.718 ms
84 bytes from 10.0.2.1 icmp_seq=5 ttl=63 time=31.134 ms

PC1>
```

Рисунок 3.12 – Приклад команди ping на робочий станції PC1

Для перевірки конфігурації списків контролю доступу, була використана команда "show access-lists" на кожному з маршрутизаторів, як видно на рисунках 3.13-3.15. Щоб скинути лічильники списків контролю доступу, була застосована команда "clear ip access-list counters".

У ході експерименту пакети були розподілені між маршрутизаторами в наступному порядку:

З комп’ютерів PC1, PC4 –> на маршрутизатор R1 (рис. 3.13);

З комп’ютерів PC2, PC5 –> на маршрутизатор R2 (рис. 3.14);

З комп’ютерів PC3, PC6 –> на маршрутизатор R3 (рис. 3.15).

```
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 (5 matches)
    70 permit ip any any (246 matches)
R1#clear ip access-list counters
```

Рисунок 3.13 – Приклад перевірки списків контролю доступу на маршрутизаторі R1

```
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 ip any any (246 matches)
R2#clear ip access-list counters
```

Рисунок 3.14 – Приклад перевірки списків контролю доступу на маршрутизаторі R2

```
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 ip any any (246 matches)
R3#clear ip access-list counters
```

Рисунок 3.15 – Приклад перевірки списків контролю доступу на маршрутизаторі R3

Висновок з отриманих результатів свідчить про правильне налаштування у режимі round-robin.

Схема мережі з розподілом трафіку для експерименту показано графічно на рисунку 3.16.

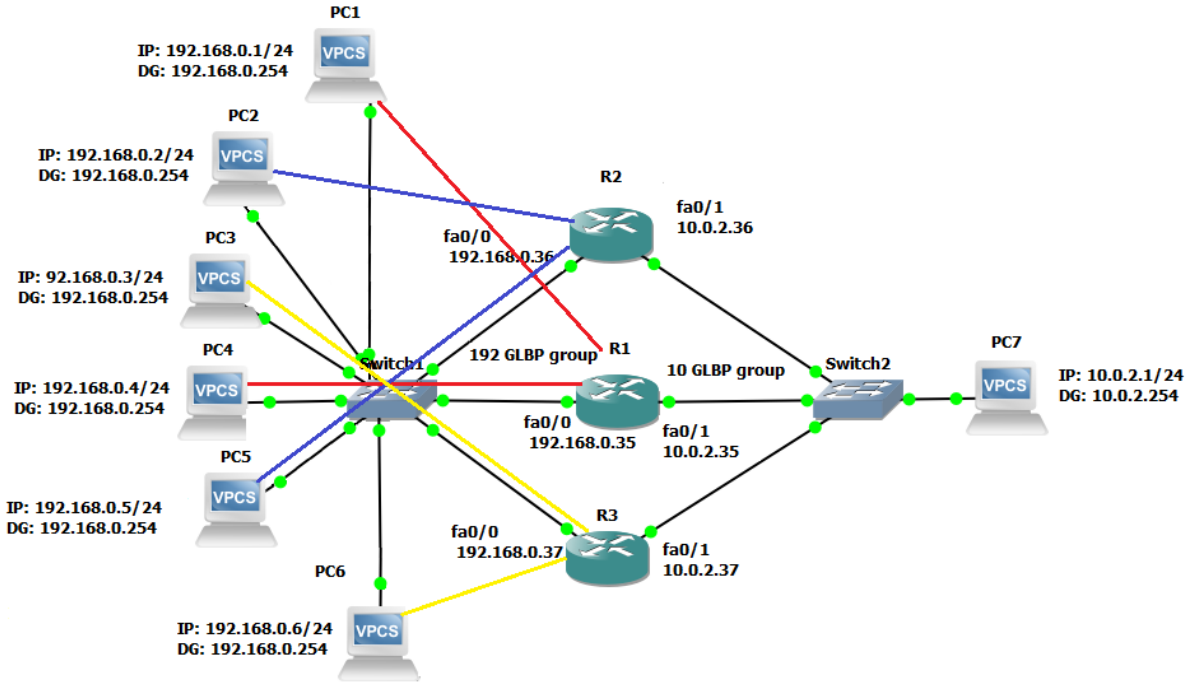

Рисунок 3.16 – Схема мережі з розподілом трафіку для експерименту

Для перевірки налаштувань протоколу GLBP була використана команда "show glbp", результати якої можна побачити на рисунках 3.17-3.19.

На рис. 3.17 наведені позначення:

```
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 3.17 – Перевірка налаштувань протоколу GLBP на маршрутизаторі R1

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. 3.18 наведені такі позначення:

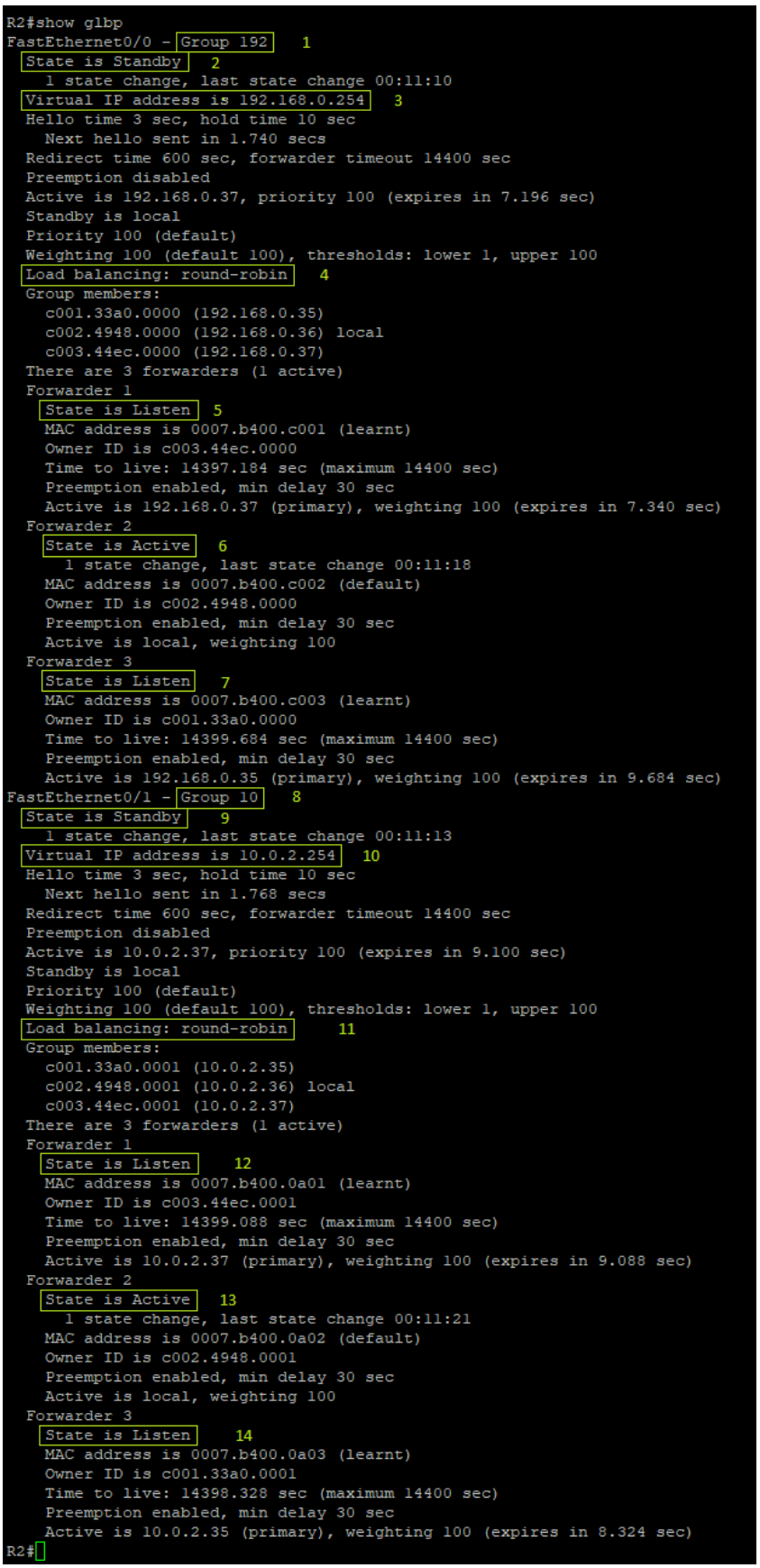

Рисунок 3.18 – Перевірка налаштувань протоколу GLBP на маршрутизаторі R2

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. 3.19 наведені такі позначення:

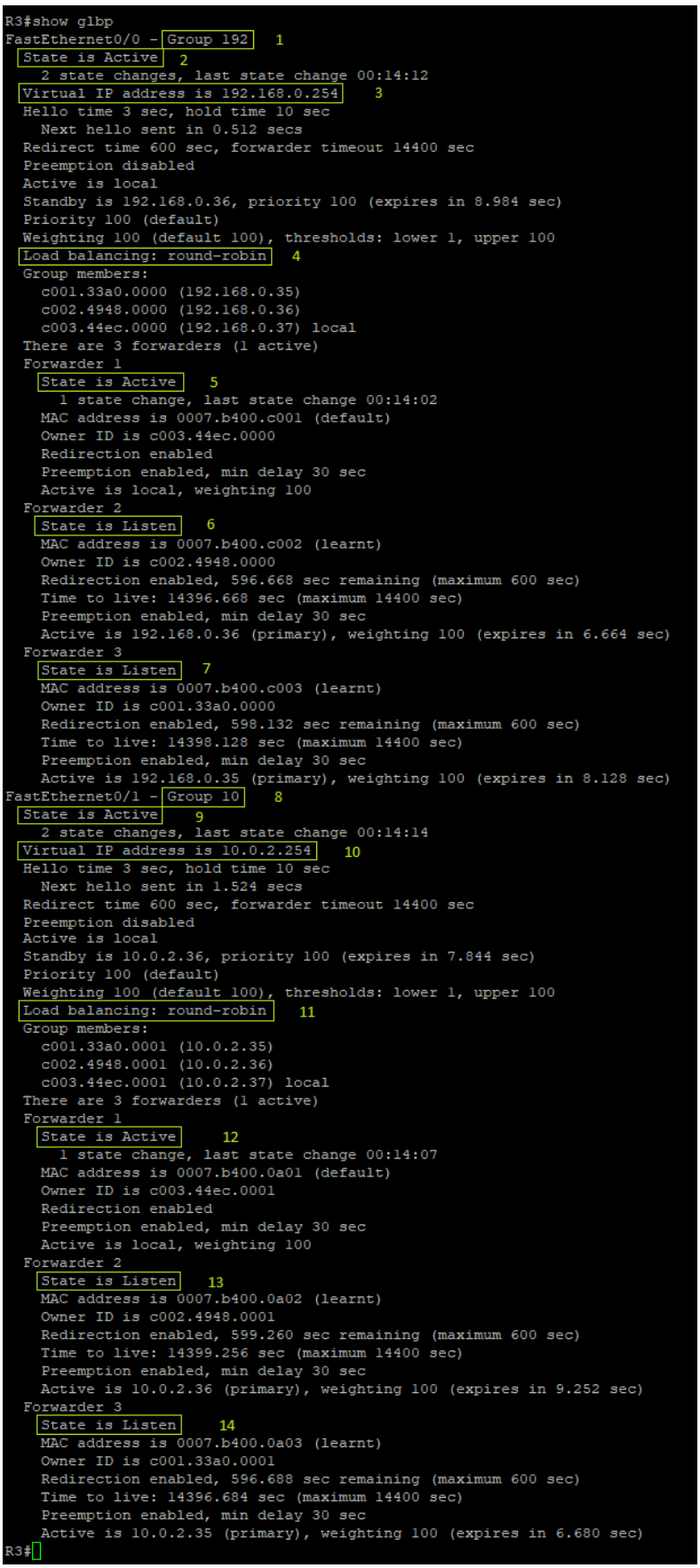

Рисунок 3.19 – Перевірка налаштувань протоколу GLBP на маршрутизаторі R3

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».

3.2 Дослідження впливу таймерів на процес роботи протоколу GLBP

У відповідь на швидкі темпи технологічного розвитку та впровадження новітніх додатків та сервісів, стандарти обслуговування постійно підвищуються. Вимоги до таких параметрів як ймовірність втрати пакетів, пропускна здатність та джитер зростають. Оскільки ці показники відображають рівень завантаженості комунікаційних каналів та маршрутів, важливо впровадити принципи Traffic Engineering (TE) для балансування використання мережевих ресурсів.

Для оптимізації використання мережевих ресурсів, ми пропонуємо використовувати стратегію захищеної маршрутизації за замовчуванням. Вона передбачає одночасне комутування доступних мереж до кількох крайових маршрутизаторів, замість одного. Це можливо завдяки використанню протоколу GLBP.

GLBP використовує спеціальні таймери - Hello та Hold, для моніторингу стану пристроїв GLBP. Для налаштування цих таймерів ми користуємося командою "glbp timers" у режимі налаштування інтерфейсу. Hello таймер регулює період часу між відправками hello-пакетів від активного маршрутизатора до інших маршрутизаторів у групі GLBP. За замовчуванням цей інтервал становить 3 секунди. Hold таймер встановлює проміжок часу, протягом якого резервний маршрутизатор очікує перед відправкою повідомлення про відмову активного маршрутизатора та переходу до активного статусу. За замовчуванням цей час складає 10 секунд.

Важливо відмітити, що таймери, які налаштовані на активному віртуальному шлюзу (AVG), мають вищий пріоритет над іншими налаштуваннями. Всі маршрутизатори в межах групи GLBP повинні використовувати однакові налаштування цих таймерів. Зазвичай, тривалість Hold

таймера в три рази перевищує тривалість Hello таймера (тривалість hold > 3 * тривалість hello-таймера).

Для дослідження змінювалося значення hello-та hold-таймерів. Під час передачі пакетів з однієї мережі в іншу, були створені умови для відмови одного з маршрутизаторів, щоб визначити кількість пакетів, які були втрачені до відновлення роботи мережі. Для налаштування інтенсивності передачі пакетів від кожного комп'ютера PC1-PC6 до PC7, була використана команда — ***ping 10.0.2.1 -c 500 -i 100***, де ***-c*** вказує на кількість переданих пакетів, а ***-i*** вказує на інтенсивність (10 пакетів за секунду). Схема мережі для дослідження таймерів протоколу GLBP представлена в попередньому підрозділі на рисунку 3.1

В процесі експерименту змінювалися значення hold- та hello-таймерів, щоб визначити їх вплив на кількість втрачених пакетів при відмові маршрутизатора R1. (рис. 3.20).

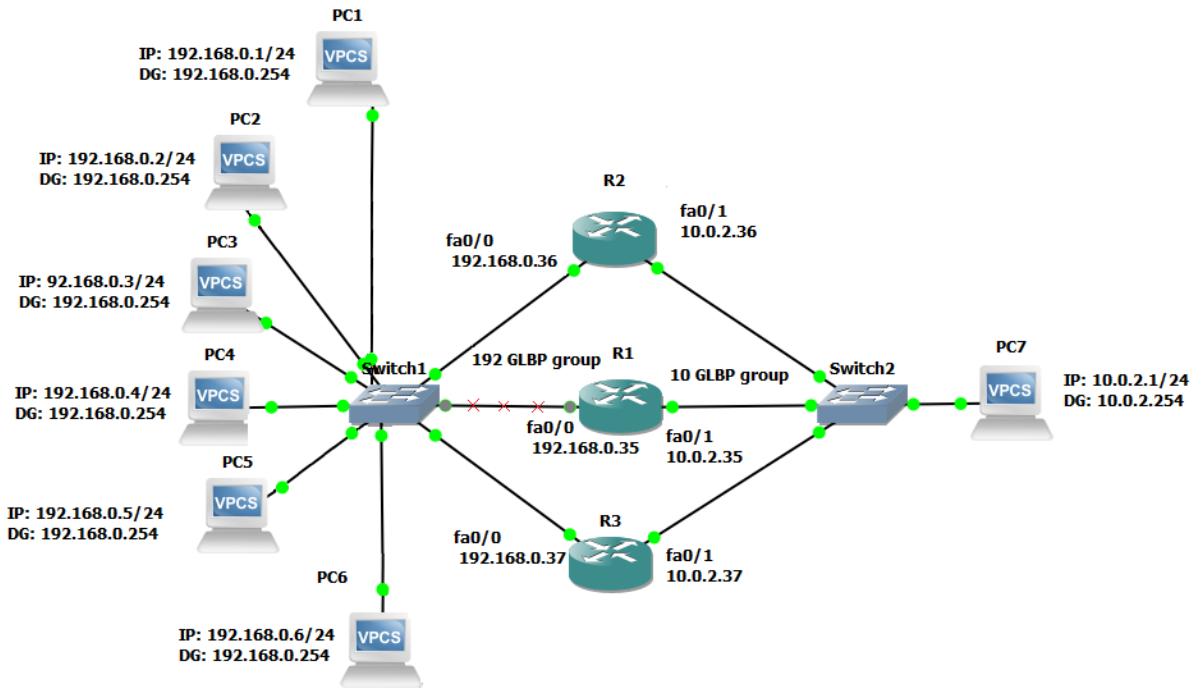

Рисунок 3.20 – Схема для дослідження таймерів протоколу GLBP при відмові маршрутизатора R1

Отримані в процесі експерименту дані наведено в таблиці 3.2.

Таблиця 3.2 – Результати експерименту

Hello time	Hold time	Кількість переданих пакетів через маршрутизатор R1	Кількість переданих пакетів через маршрутизатор R2	Кількість переданих пакетів через маршрутизатор R3	Кількість втрачених пакетів
3	10	1000	1864	112	24
3	9	1000	1839	145	16
3	8	1000	1884	103	13
3	7	1026	1864	98	12
3	6	1000	1880	111	9
3	5	1018	1895	79	8
3	4	1000	1902	92	6
2	5	1000	1900	90	10
1	4	1000	1886	106	8
2	10	1000	1897	83	20
1	10	1000	1867	115	18

Списки контролю доступу були налаштовані для перевірки розподілення пакетів між маршрутизаторами.

Для перевірки цих списків на маршрутизаторах, було застосовано команду «show access-lists», як показано на рис. 3.20-3.35.

Під час експерименту пакети були розподілені таким чином:

При тривалості hold-таймеру в 10 секунд, а hello-таймеру в 3 секунди, з 1000

відправлених пакетів через маршрутизатор R1, 1864 відправлених пакетів через маршрутизатор R2 та 112 пакетів через маршрутизатор R3, кількість втрачених пакетів дорівнює 24 (рис.3.20).

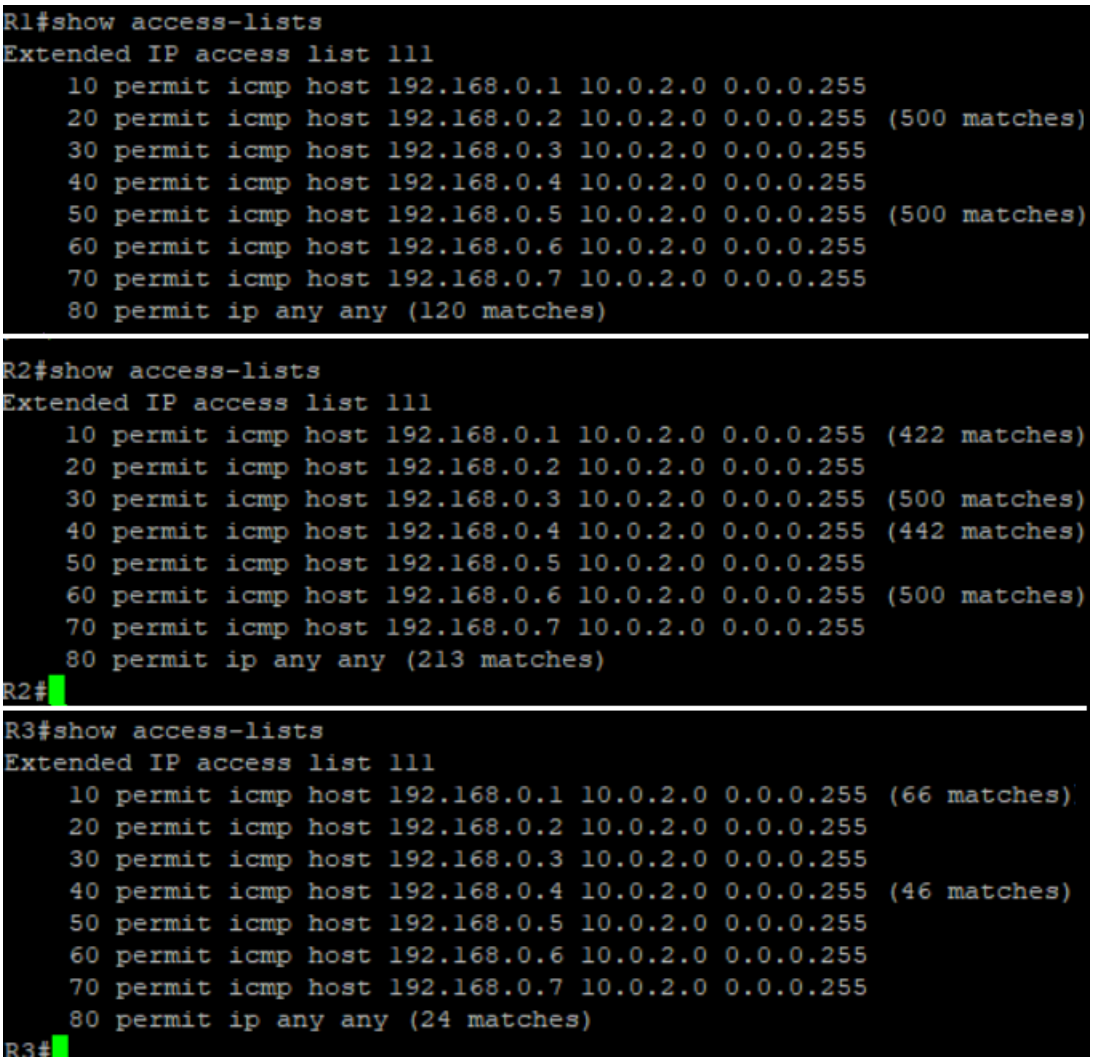

Рисунок 3.20 – Приклад перевірки списків контролю доступу на маршрутизаторах R1, R2 та R3

При тривалості hold-таймеру в 9 секунд, а hello-таймеру в 3 секунди, з 1000 відправлених пакетів через маршрутизатор R1, 1839 відправлених пакетів через маршрутизатор R2 та 145 пакетів через маршрутизатор R3, кількість втрачених пакетів дорівнює 16 (рис.3.21).

```
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 (500 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 (500 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 (108 matches)
R1#
```

```
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 (409 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 (500 matches)
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255 (430 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 (500 matches)
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255
    80 permit ip any any (153 matches)
R2#
```

```
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 (83 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 (62 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
    80 permit ip any any (51 matches)
R3#
```

Рисунок 3.21 – Приклад перевірки списків контролю доступу на маршрутизаторах R1, R2 та R3

При тривалості hold-таймеру в 8 секунд, а hello-таймеру в 3 секунди, з 1000 відправлених пакетів через маршрутизатор R1, 1884 відправлених пакетів через маршрутизатор R2 та 103 пакетів через маршрутизатор R3, кількість втрачених пакетів дорівнює 13 (рис.3.22).

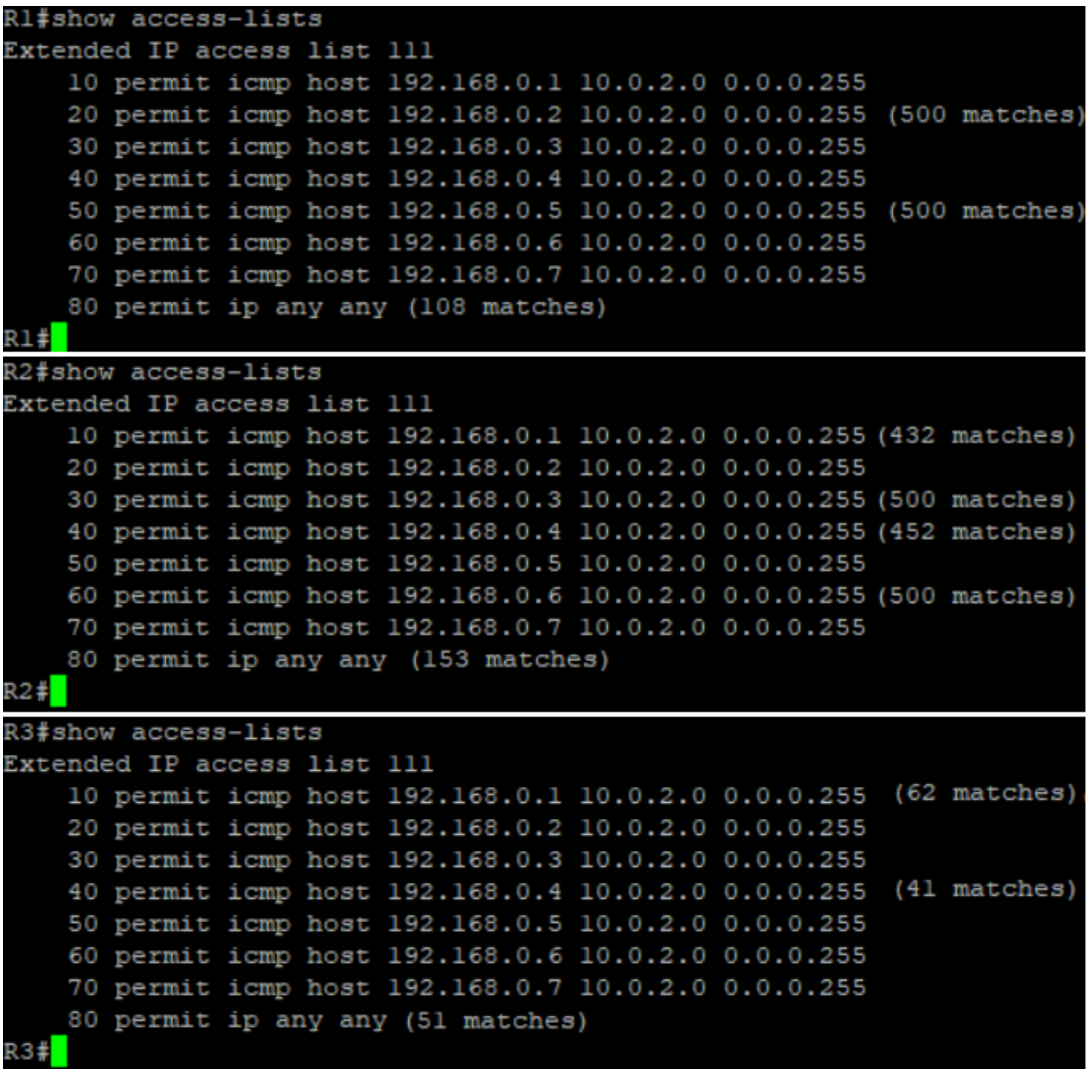

Рисунок 3.22 – Приклад перевірки списків контролю доступу на маршрутизаторах R1, R2 та R3

При тривалості hold-таймеру в 7 секунд, а hello-таймеру в 3 секунди, з 1026 відправлених пакетів через маршрутизатор R1, 1864 відправлених пакетів через маршрутизатор R2 та 98 пакетів через маршрутизатор R3, кількість втрачених пакетів дорівнює 12 (рис.3.23).

```
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 (13 matches)
    20 permit icmp host 192.168.0.2 10.0.2.0 0.0.0.255 (500 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 (13 matches)
    50 permit icmp host 192.168.0.5 10.0.2.0 0.0.0.255 (500 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 (108 matches)
R1#
```

```
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 (420 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 (500 matches)
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255 (444 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 (500 matches)
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255
    80 permit ip any any (153 matches)
R2#
```

```
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 (61 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 (37 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
    80 permit ip any any (51 matches)
R3#
```

Рисунок 3.23 – Приклад перевірки списків контролю доступу на маршрутизаторах R1, R2 та R3

При тривалості hold-таймеру в 6 секунд, а hello-таймеру в 3 секунди, з 1000 відправлених пакетів через маршрутизатор R1, 1880 відправлених пакетів через маршрутизатор R2 та 111 пакетів через маршрутизатор R3, кількість втрачених пакетів дорівнює 9 (рис.3.24).

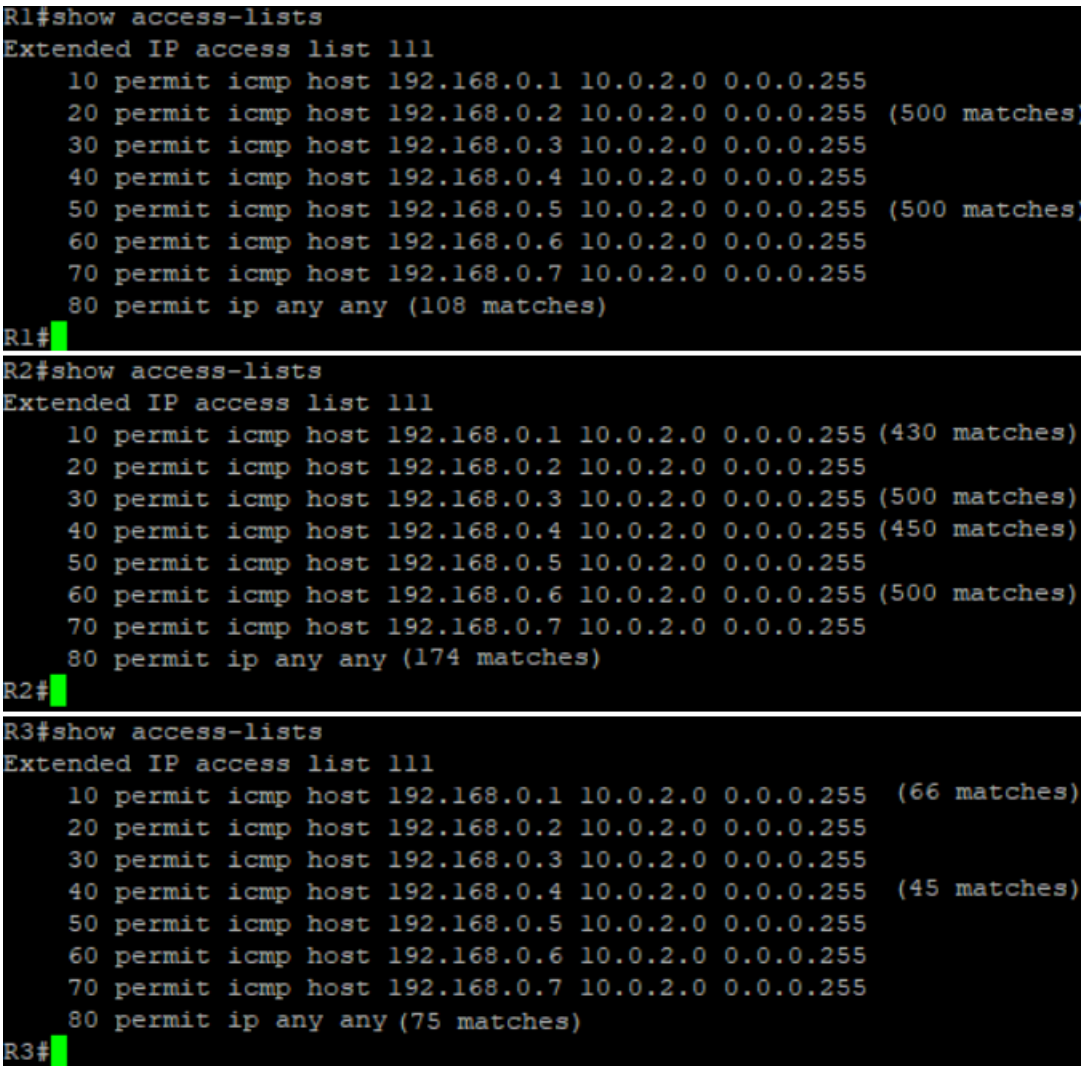

Рисунок 3.24 – Приклад перевірки списків контролю доступу на маршрутизаторах R1, R2 та R3

При тривалості hold-таймеру в 5 секунд, а hello-таймеру в 3 секунди, з 1018 відправлених пакетів через маршрутизатор R1, 1895 відправлених пакетів через маршрутизатор R2 та 79 пакетів через маршрутизатор R3, кількість втрачених пакетів дорівнює 8 (рис.3.25).

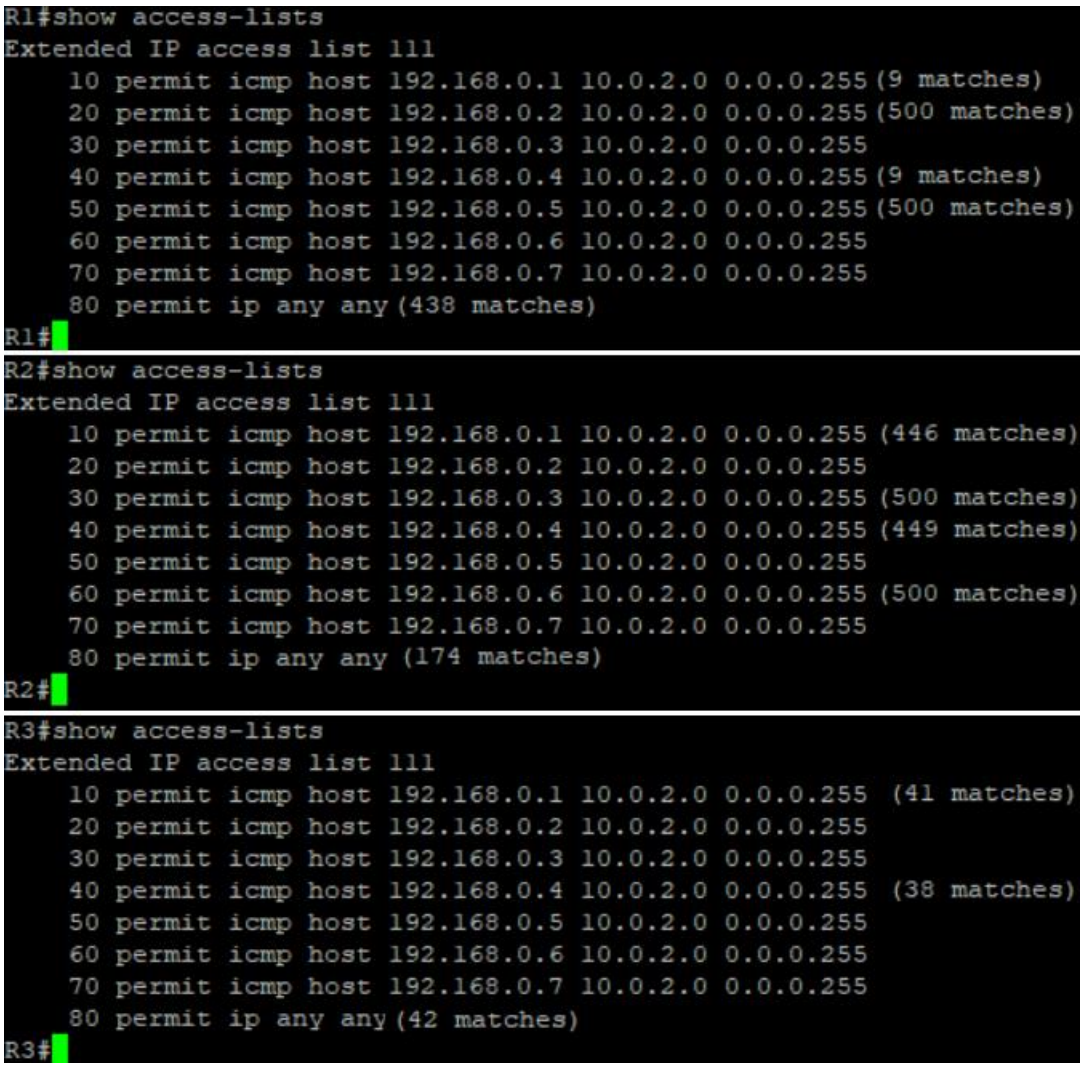

Рисунок 3.25 – Приклад перевірки списків контролю доступу на маршрутизаторах R1, R2 та R3

При тривалості hold-таймеру в 4 секунд, а hello-таймеру в 3 секунди, з 1000 відправлених пакетів через маршрутизатор R1, 1902 відправлених пакетів через маршрутизатор R2 та 92 пакетів через маршрутизатор R3, кількість втрачених пакетів дорівнює 6 (рис.3.26).

```
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 (500 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 (500 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
    80 permit ip any any (138 matches)
R1#
```

```
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 (442 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 (500 matches)
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255 (460 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 (500 matches)
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255
    80 permit ip any any (132 matches)
R2#
```

```
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 (55 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 (37 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
    80 permit ip any any (33 matches)
R3#
```

Рисунок 3.26 – Приклад перевірки списків контролю доступу на маршрутизаторах R1, R2 та R3

При тривалості hold-таймеру в 5 секунд, а hello-таймеру в 2 секунди, з 1000 відправлених пакетів через маршрутизатор R1, 1900 відправлених пакетів через маршрутизатор R2 та 90 пакетів через маршрутизатор R3, кількість втрачених пакетів дорівнює 10 (рис.3.27).

```
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 (500 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 (500 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
    80 permit ip any any (138 matches)
R1#
```

```
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 (440 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 (500 matches)
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255 (460 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 (500 matches)
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255
    80 permit ip any any (204 matches)
R2#
```

```
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 (55 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 (35 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
    80 permit ip any any (60 matches)
R3#
```

Рисунок 3.27 – Приклад перевірки списків контролю доступу на маршрутизаторах R1, R2 та R3

При тривалості hold-таймеру в 4 секунд, а hello-таймеру в 1 секунди, з 1000 відправлених пакетів через маршрутизатор R1, 1886 відправлених пакетів через маршрутизатор R2 та 106 пакетів через маршрутизатор R3, кількість втрачених пакетів дорівнює 8 (рис.3.28).

```
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 (500 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 (500 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
    80 permit ip any any (462 matches)
R1#
```

```
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 (435 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 (500 matches)
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255 (451 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 (500 matches)
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255
    80 permit ip any any (204 matches)
R2#
```

```
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 (61 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 (45 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
    80 permit ip any any (84 matches)
R3#
```

Рисунок 3.28 – Приклад перевірки списків контролю доступу на маршрутизаторах R1, R2 та R3

При тривалості hold-таймеру в 10 секунд, а hello-таймеру в 2 секунди, з 1000 відправлених пакетів через маршрутизатор R1, 1897 відправлених пакетів через маршрутизатор R2 та 83 пакетів через маршрутизатор R3, кількість втрачених пакетів дорівнює 20 (рис.3.29).

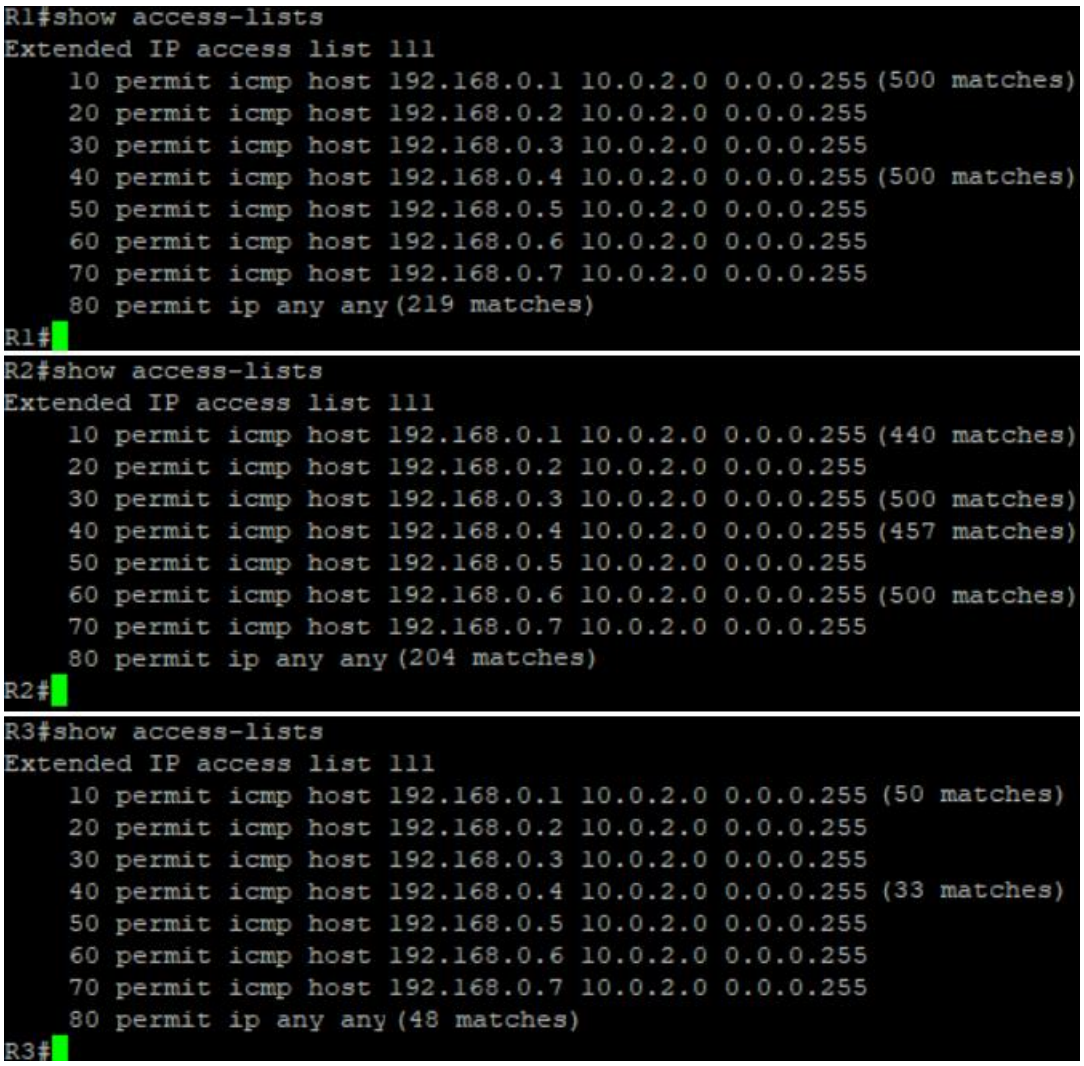

Рисунок 3.29 – Приклад перевірки списків контролю доступу на маршрутизаторах R1, R2 та R3

При тривалості hold-таймеру в 10 секунд, а hello-таймеру в 1 секунди, з 1000 відправлених пакетів через маршрутизатор R1, 1867 відправлених пакетів через маршрутизатор R2 та 115 пакетів через маршрутизатор R3, кількість втрачених пакетів дорівнює 18 (рис.3.30).

```
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 (500 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 (500 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
    80 permit ip any any (429 matches)
R1#
```

```
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 (425 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 (500 matches)
    40 permit icmp host 192.168.0.4 10.0.2.0 0.0.0.255 (442 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 (500 matches)
    70 permit icmp host 192.168.0.7 10.0.2.0 0.0.0.255
    80 permit ip any any (429 matches)
R2#
```

```
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 (66 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 (49 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
    80 permit ip any any (150 matches)
R3#
```

Рисунок 3.30 – Приклад перевірки списків контролю доступу на маршрутизаторах R1, R2 та R3

Якщо змінити тривалість hold-таймеру з 10 до 4 секунд або менше, втрати скоротяться з 24 до 6. Таким чином, було знижено кількість втрачених пакетів з 0,8% до 0,2% та прискорено процес відновлення роботи мережі після відмови одного з маршрутизаторів. Як показано в таблиці 3.2.

Важливо відзначити, що процес відновлення мережі після відмови одного з маршрутизаторів вимагає точного і правильного налаштування hello- та hold-таймерів. Їх значення впливають на швидкість відновлення мережі та кількість втрачених пакетів під час періоду відмови.

Даний експеримент підтверджує важливість правильного налаштування таймерів в групі GLBP, щоб оптимізувати роботу мережі та забезпечити її високу відмовостійку маршрутизацію.

Також під час даного дослідження була успішно реалізована та випробувана робота протоколу GLBP у режимі Round-Robin. Протокол GLBP, за результатами експерименту демонструє здатність до ефективного балансування трафіку між декількома маршрутизаторами, розподіляючи навантаження порівну або використовуючи зважені коефіцієнти.

Оскільки протокол GLBP ділить трафік за хостами, було вирішено організувати розподіл навантаження у зваженому режимі наступним чином: маршрутизатор R1 обробляє 1/6 трафіку, R2 – 2/6, а R3 – 4/6. Таким чином, навантаження між маршрутизаторами було розподілено відповідно до встановлених вагових коефіцієнтів. З метою оптимізації та автоматизації налаштування було запропоновано використовувати автоматичну конфігурацію. Такий підхід дозволяє протоколу самостійно визначати та налаштовувати вагові коефіцієнти, базуючись на розрахунках моделі, запропонованої в даному дослідженні. Це виключає можливість впливу людського фактору і забезпечує, що робота протоколу не залежить від досвіду або рівня кваліфікації адміністратора мережі.

ВИСНОВКИ

У процесі дослідження стало очевидним, що однією з ключових вимог до сучасної мережної інфраструктури є здатність до ефективного балансування навантаження та реагування на відмови. Відтак, важливо враховувати надійність мережевих пристроїв та їх пропускні здатності, щоб керувати трафіком в мережі. У реалізації цього завдання значну роль відіграють протоколи маршрутизації, які допомагають забезпечити якість обслуговування.

З урахуванням актуальності потреб сучасної мережної інфраструктури та існуючих обмежень у рішеннях, пропонується розробка нового протоколу на базі вже використовуваного протоколу балансування навантаження GLBP.

Ця ініціатива має на меті вдосконалити якість обслуговування мережі шляхом розробки та дослідження нової математичної моделі, яка бере до уваги надійність мережних пристроїв, зокрема прикордонних роутерів та їх пропускні здатності.

У роботі запропоновано вдосконалену математичну модель балансування навантаження в ІКМ, яка відповідає принципам концепції Traffic Engineering. Модель (2.1)-(2.10) математично формалізує випадок побудови ІКМ, де кожна мережа доступу для забезпечення відмовостійкої маршрутизації може одночасно комутуватись до декількох приграничних маршрутизаторів. Тому пропонується покращити рівень балансування навантаження в ІКМ за критерієм (2.10) шляхом забезпечення розподілу трафіка на рівні доступу між декількома приграничними маршрутизаторами, які створюють віртуальний шлюз за замовчуванням.

Результати проведеного дослідження підтвердили ефективність запропонованого рішення. За допомогою проведеного аналізу, було виявлено, що удосконалена модель відмовостійкої маршрутизації, яка здійснює балансування навантаження як на рівні доступу, так і на рівні ІКМ, має переваги за продуктивністю і рівнем завантаженості комунікаційних каналів порівняно з моделями без балансування навантаження (табл. 2.3).

В ході дослідження було підтверджена можливість балансувати навантаження враховуючи вагові коефіцієнти маршрутизаторів. Рекомендовано зробити конфігурацію протоколу автоматичною, для того щоб, робота мережі на залежала від кваліфікації адміністратора мережі. Це дозволить покращити числові

показники таких метрик, як ймовірність втрати пакетів, продуктивність, середня затримка та джитер.

Для дослідження відмовостійкої маршрутизації, були налаштовані таймери в GLBP групі та проведено експеримент з імітацією відмови одного з маршрутизаторів. Результати показали, що правильне налаштування цих таймерів може суттєво зменшити втрати пакетів і прискорити відновлення мережі. У ході експерименту було визначено, що при відмові маршрутизатора, з 3000 відправлених пакетів втрачається 24 пакетів. При тривалості hold-таймеру в 10 секунд втрачається 24 пакетів, а при зменшенні цього часу до 4 секунд - лише 6 пакетів.

Таким чином, ми змогли знизити втрати пакетів з 0,8% до 0,2% і прискорити процес відновлення роботи мережі після відмови одного з маршрутизаторів (табл. 3.2). Це підкреслює важливість відповідного налаштування мережевих параметрів для забезпечення оптимальної роботи і відмовостійкої маршрутизації.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Лемешко О. В. Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість: монографія / за ред. О. В. Лемешко, О. С. Єременко, О. С. Невзорова. Харків : ХНУРЕ, 2020. 308 с.

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

3. Tate, Jon, et al. IBM Flex System and PureFlex System Network Implementation. IBM, International Technical Support Organization. 2013. P. 80 – 89.

4. Imelda J., Hendra S., Luh W., Dewi K., Khodijah H. Performance Evaluation of First Hop Redundancy Protocol (FHRP) on VRRP, HSRP, GLBP with Routing Protocol BGP and EIGRP. 8th International Conference on Cyber and IT Service Management (CITSM). 2020. P 37.

5. Thompson, M., & Garcia, N. Adaptive Load Balancing in HSRP Environments: A Machine Learning Approach. Journal of Computer Networks and Communications. January 15. Vol. 44, No. 1. P. 10-21.

6. Usman A., Jing T., Hafiz U., Ammar S. Performance Analysis and Functionality Comparison of FHRP Protocols. IEEE 11th International Conference on Communication Software and Networks (ICCSN). 2019. P. 19-27.

7. Rak J. Resilient Routing in Communication Networks (Computer Communications and Networks), 1st edition. Springer, 2015. P. 181.

8. Lemeshko O., Yeremenko O., Mersni A., Investigation of Enhanced Mathematical Model For Traffic Engineering Fault-Tolerant Routing. International Conference on Engineering and Emerging Technologies (ICEET). Istanbul, Turkey, 27-28 October, 2021. P. 98–106. DOI: 10.1109/ICEET53442.2021.9659606

9. 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.

10. 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”. м. Київ, 2022. С. 1-3.

11. 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.

12. 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. С. 402.

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

14. 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.

15. 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.

16. Lemeshko O.V., 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.

17. 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.

18. Mauthe A., Hutchison D., Cetinkaya E.K., Ganchev I., Rak J., Sterbenz J.P., Gunkelk M., Smith P., Gomes T. Disaster-resilient communication networks: Principles and best practices. Resilient Networks Design and Modeling (RNDM) 2016:

Proceedings of the 8th International Workshop. Halmstad, Sweden, 13-15 September, 2016. IEEE, 2016. P. 1-10. DOI: 10.1109/RNDM.2016.7608262.

19. Лемешко О. В., Євсєєва О. Ю. Конспект лекцій з дисципліни «Алгоритми управління та адаптації в ТКС» для студентів денної форми навчання спеціальності 7.092401 – Телекомунікаційні системи та мережі. Харків: ХНУРЕ, 2008. С. 164.

20. O. Lemeshko, O. Yeremenko, M. Yevdokymenko. Resilience Improvement by Traffic Engineering Fault-Tolerant Routing in Programmable. Progress in Advanced Information and Communication Technology and Systems. 2022. С. 235–255.

21. 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. P. 129-140.

22. 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. P. 1018.

23. 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.

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

25. 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.

26. Beshley M., Klymash M., Strykhalyuk B., Shpur O., Bugil B., Kagalo I. SOA quality management subsystem on the basis of load balancing method using fuzzy sets. International Journal of Computer Science and Software Engineering (IJCSSE). 2015. January 15. Vol. 44, No. 1. P. 10-21.

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

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

29. 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.

30. 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.

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

32. 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.

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

34. 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.

35. 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.

36. 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.

37. 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.

38. 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.

39. 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.

40. 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.

41. 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.

42. 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.

43. Лемешко А.В. Модель отказоустойчивой маршрутизации многоадресных и широковещательных потоков в MPLS-сети / А.В. Лемешко, К.М. Арус // Системи обробки інформації. – 2013. – Вип. 9. – С. 160-163. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2013_9_34

44. 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.

45. 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.