Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

Факультет комп'ютерних наук та технологій
Кафедра комп'ютерних систем та мереж

Пояснювальна записка

до дипломного проєкту (роботи)
магістра
(ступінь вищої освіти)

на тему **СИСТЕМА ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКОСТІ КОРПОРАТИВНИХ МЕРЕЖ ЗА ДОПОМОГОЮ ПРОТОКОЛІВ РЕЗЕРВУВАННЯ**

Виконав: студент 2 курсу, групи КНТ-514м
спеціальності
123 Комп'ютерна інженерія
(код і найменування спеціальності)

Освітня програма (спеціалізація)
Комп'ютерні системи та мережі

ШКОЛОВИЙ В. В.
(ПРІЗВИЩЕ та ініціали)
Керівник КИРИЧЕК Г.Г.
(ПРІЗВИЩЕ та ініціали)
Рецензент РОМАНОВСЬКИЙ О.В.
(ПРІЗВИЩЕ та ініціали)

2025

Форма № 25

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет Комп'ютерних наук і технологій
Кафедра «Комп'ютерні системи та мережі»
Ступінь вищої освіти магістерський
Спеціальність 123 Комп'ютерна інженерія
(код і найменування)

Освітня програма (спеціалізація) Комп'ютерні системи та мережі
(назва освітньої програми (спеціалізації)

ЗАТВЕРДЖУЮ
Зав. кафедри Кудерметов Р.К.
_____
"_15_" __жовтня__ 2025 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

ШКОЛОВОГО Владислава Вячеславовича
(ПРІЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Система забезпечення відмовостійкості корпоративних мереж за допомогою протоколів резервування
керівник проєкту (роботи) к. т. н., доцент, КИРИЧЕК Галина Григорівна
(науковий ступінь, вчене звання, ПРІЗВИЩЕ, ім'я, по батькові)
затверджені наказом вищого навчального закладу від " 30 " жовтня 2025 року № 491
2. Строк подання студентом проєкту (роботи) 23 грудня 2025 року
3. Вихідні дані до проєкту (роботи) Система забезпечення відмовостійкості корпоративних мереж за допомогою протоколів резервування. Наявні протоколи та механізми резервування. Середовище моделювання Cisco Packet Tracer.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Теоретичні основи побудови корпоративних мереж. Технології забезпечення відмовостійкості корпоративних мереж. Створення відмовостійкої мережі. Експериментальне дослідження параметрів відмовостійкої мережі.

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

6. Консультанти розділів проєкту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-4	КИРИЧЕК Г. Г., доцент		
нормоконтроль	ЩЕРБАК Н.В., ст. викл.		

7. Дата видачі завдання 01.10.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	**Примітка**
1	Огляд літературних джерел із забезпечення відмовостійкості корпоративних мереж	10.10.2025 р.	
2	Аналіз корпоративних мереж та методів резервування	25.10.2025 р.	
3	Дослідження протоколів резервування шлюзів (HSRP, VRRP, GLBP)	05.11.2025 р.	
4	Проєктування відмовостійкої мережі з використанням HSRP	12.11.2025 р.	
5	Реалізація мережі в Cisco Packet Tracer та базове тестування	18.11.2025 р.	
6	Моделювання аварійних режимів і порівняння конфігурацій HSRP	25.11.2025 р.	
7	Оформлення отриманих результатів у пояснювальній записці	30.11.2025 р.	
8	Оформлення графічного матеріалу	10.12.2025 р.	
9	Оформлення допоміжного матеріалу	15.12.2025 р.	

Студент _____ **Владислав ШКОЛОВИЙ**
(підпис) (ім'я, ПРІЗВИЩЕ)

Керівник проєкту (роботи) _____ **Галина КИРИЧЕК**
(підпис) (ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

ПЗ: 86 с., 36 рис., 14 табл., 21 джерел

HSRP, VRRP, GLBP, ВІРТУАЛЬНИЙ ШЛЮЗ, ВІДМОВОСТІЙКІСТЬ МЕРЕЖ, РЕЗЕРВУВАННЯ МАРШРУТИЗАТОРІВ, GATEWAY REDUNDANCY PROTOCOLS, КОРПОРАТИВНІ МЕРЕЖІ, БЕЗПЕРЕРВНІСТЬ РОБОТИ, FAILOVER

Метою роботи є реалізація системи забезпечення відмовостійкості корпоративних мереж за допомогою протоколів резервування, дослідження методів та механізмів, оцінка ефективності їх застосування у сучасних інформаційних системах.

Об’єктом дослідження є корпоративна мережа як інфраструктура передавання та обробки даних. Предметом дослідження виступають методи забезпечення відмовостійкості та протоколи резервування шлюзів (FHRP).

У роботі виконано аналіз архітектури корпоративних мереж, чинників, що впливають на їхню надійність, а також методів резервування і протоколів першого переходу. Для перевірки практичної придатності обраних рішень розроблено тестову відмовостійку мережу в середовищі Cisco Packet Tracer з використанням протоколу HSRP. Проведено моделювання роботи мережі без резервування, з HSRP зі стандартними таймерами та з оптимізованими параметрами.

Отримані результати показали суттєве скорочення простоїв мережі та зменшення втрат пакетів при використанні HSRP, особливо за умов оптимізації таймерів, що підтверджує доцільність застосування протоколів резервування під час проєктування та модернізації корпоративних мереж. Результати можуть бути використані для розроблення рекомендацій щодо побудови відмовостійкої інфраструктури та впровадження механізмів резервування в реальних корпоративних системах.

ABSTRACT

Explanatory note to the master's thesis: 86 p., 36 figures, 14 tables, 21 sources

HSRP, VRRP, GLBP, VIRTUAL GATEWAY, NETWORK REDUNDANCY, FAILOVER MECHANISMS, GATEWAY REDUNDANCY PROTOCOLS, ENTERPRISE NETWORKS, HIGH AVAILABILITY

The aim of this work is to implement a system for ensuring the fault tolerance of corporate networks using redundancy protocols, to investigate the corresponding methods and mechanisms, and to assess the effectiveness of their application in modern information systems.

The object of the research is the corporate network as an infrastructure for data transmission and processing. The subject of the research is the methods of ensuring fault tolerance and gateway redundancy protocols (FHRP).

The work includes an analysis of the architecture of corporate networks, the factors that affect their reliability, as well as redundancy methods and first-hop protocols. To verify the practical applicability of the chosen solutions, a test fault-tolerant network was designed in the Cisco Packet Tracer environment using the HSRP protocol. The operation of the network without redundancy, with HSRP using default timers, and with optimized parameters was simulated.

The obtained results showed a significant reduction in network downtime and packet loss when using HSRP, especially under timer optimization, which confirms the feasibility of applying redundancy protocols in the design and modernization of corporate networks. The results can be used to develop recommendations for building fault-tolerant infrastructures and implementing redundancy mechanisms in real corporate systems.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАК

FHRP - First Hop Redundancy Protocol;

HSRP - Hot Standby Router Protocol;

VRRP - Virtual Router Redundancy Protocol;

GLBP - Gateway Load Balancing Protocol;

VIP - Virtual IP Address;

LAN - Local Area Network;

WAN - Wide Area Network;

MTBF - Mean Time Between Failures;

MTTR - Mean Time To Repair;

QoS - Quality of Service;

HA - High Availability;

VLAN - Virtual Local Area Network.

ВСТУП

У сучасному цифровому середовищі корпоративні мережі відіграють ключову роль у функціонуванні інформаційних систем підприємств, установ та організацій. Вони забезпечують об’єднання різних структурних підрозділів у єдиний комунікаційний простір, що дозволяє ефективно обмінюватися даними, централізовано зберігати інформацію та реалізовувати корпоративні сервіси — від офісних додатків до хмарних обчислень і систем управління ресурсами. Завдяки корпоративним мережам стає можливим оперативне прийняття рішень, координація дій між віддаленими філіями та впровадження сучасних технологій кіберзахисту.

Разом із тим зростання масштабів корпоративних мереж, поява великої кількості розподілених сервісів, використання мобільних пристроїв, віртуалізації та хмарних технологій призводять до підвищення вимог до їхньої надійності, пропускної здатності та безпеки. Навіть короткочасна відмова мережевої інфраструктури може спричинити перебої в роботі бізнес-критичних систем, фінансові втрати, порушення регламентів обслуговування клієнтів та зниження репутації організації. У цих умовах забезпечення відмовостійкості та безперервності функціонування корпоративних мереж стає одним із пріоритетних напрямів розвитку інформаційних технологій.

Особливого значення набуває застосування протоколів резервування мережевих шлюзів та каналів зв’язку. Такі протоколи забезпечують автоматичне перемикання трафіку у разі відмови основного маршрутизатора або каналу, що дозволяє мінімізувати простої, знизити втрати даних та зберегти доступність критично важливих сервісів.

Актуальність даного дослідження зумовлена стрімким зростанням залежності бізнес-процесів від безперебійної роботи мережевої інфраструктури. Для більшості сучасних організацій простій мережі навіть протягом кількох хвилин є неприйнятним, оскільки може призвести до зупинки онлайн-сервісів, втрати

транзакцій, зриву договорів або порушення вимог до рівня сервісу (SLA). Тому розробка та дослідження систем забезпечення відмовостійкості корпоративних мереж на основі протоколів резервування є важливим завданням як з наукової, так і з практичної точки зору.

У першому розділі розглядаються теоретичні основи побудови корпоративних мереж. На основі цього формулюються загальні задачі дослідження та обґрунтовується необхідність використання систем резервування.

У другому розділі проводиться аналіз технологій забезпечення відмовостійкості корпоративних мереж. Розглядаються методи резервування каналів та мережевих пристроїв, протоколи резервування першого переходу (HSRP, VRRP, GLBP тощо), їхні переваги та обмеження

У третьому розділі здійснюється проєктування та реалізація відмовостійкої корпоративної мережі.

У четвертому розділі проводяться експериментальні дослідження параметрів роботи відмовостійкої мережі та порівняння різних конфігурацій. На основі отриманих результатів виконується порівняльний аналіз і формулюються висновки щодо ефективності застосованих механізмів резервування.

Результати роботи можуть бути використані при проєктуванні, модернізації та експлуатації корпоративних мереж у комерційних компаніях, державних установах, навчальних закладах, а також у центрах обробки даних та інфраструктурах, що надають хмарні й мережеві сервіси. Розроблені підходи до побудови та налаштування відмовостійких мережевих рішень можуть слугувати основою для створення практичних методичних рекомендацій для мережевих адміністраторів та інженерів, а також використовуватися у навчальному процесі при вивченні дисциплін, пов’язаних із комп’ютерними мережами та інформаційною безпекою.

1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Поняття та структура корпоративної мережі

Корпоративна мережа - це структурована система комунікації та обміну даними, яка включає апаратне забезпечення, кабельну інфраструктуру, мікропрограмне забезпечення, програмні засоби, логічну топологію тощо, що забезпечують наскрізну взаємодію корпоративних прикладних систем усередині організації.

Корпоративні мережі зазвичай використовують локальні (LAN) та глобальні (WAN) мережі для з'єднання персональних комп'ютерів, серверів та інших пристроїв, іноді розширюючи підключення до Інтернету або інтрамереж для внутрішньої комунікації та доступу до ресурсів. Інтрамережа (intranet) - це приватна вебмережа, доступна лише співробітникам, яка слугує платформою для ведення бізнес-операцій, отримання звітів і керування внутрішніми ресурсами. Доступ до неї мають лише користувачі, підключені до корпоративної мережі - безпосередньо на робочому місці або через захищені віртуальні приватні мережі (VPN). Корпоративна локальна мережа може бути як дротовою, так і бездротовою, а всередині неї можуть створюватися демілітаризовані зони (DMZ) для розмежування типів користувачів; адміністратори мережі можуть змінювати ці обмеження відповідно до наданих повноважень [1].

LAN (локальна мережа) є найчастіше використовуваним типом мережі. Це комп'ютерна мережа, яка з'єднує комп'ютери через спільний канал зв'язку, що знаходиться в межах обмеженої території, тобто локально. Локальна мережа охоплює два або більше комп'ютерів, підключених через сервер. Дві основні технології, що використовуються в цій мережі, - це Ethernet та Wi-Fi. Діапазон такої мережі сягає до 2 км, швидкість передачі даних дуже висока, а обслуговування просте та дешеве.

MAN (мережа міського масштабу) більша за LAN, але менша за WAN. Це тип комп'ютерної мережі, який з'єднує комп'ютери на географічній відстані через

спільний канал зв’язку в межах міста, містечка або метрополійної зони. У цій мережі переважно використовуються технології FDDI, CDDI та ATM, а діапазон покриття становить від 5 км до 50 км.

WAN (глобальна мережа) - це тип комп’ютерної мережі, яка з’єднує комп’ютери на великій географічній відстані через спільний канал зв’язку. Вона не обмежена однією локацією, а поширюється на багато місць. WAN також можна визначити як групу локальних мереж, що взаємодіють між собою на відстані понад 50 км. Тут використовуються технології Leased-Line та Dial-up. Швидкість передачі даних дуже низька, обслуговування дуже складне, а витрати дуже високі. Класифікація комп’ютерних мереж за масштабом (LAN, MAN, WAN), їхні характеристики та типові сценарії застосування детально розглянуті в класичних роботах [2-3].

В останні 10-20 років спостерігається значне зростання використання мобільних пристроїв, віртуалізації серверів та хмарних сервісів, і всі ці процеси потребують динамічної мережевої структури. Основна ідея мережевої взаємодії в корпоративних застосунках полягає у створенні з’єднання між численними системами та пристроями, яке забезпечує можливість ефективного обміну даними між ними.

Корпоративні мережі зазвичай будуються за модульним принципом, наприклад, за моделлю SAFE blueprint, яка структурно поділяє мережу на кілька зон: Campus Area, Edge Area та Service Provider Area. Campus Area (внутрішня зона) обслуговує внутрішніх користувачів організації, забезпечуючи стабільну комунікацію між підрозділами, тоді як Edge Area відповідає за взаємодію з зовнішніми сервісами, клієнтами та віддаленими користувачами.

Окрім цього, чіткий поділ на зони спрощує впровадження механізмів сегментації, таких як VLAN або VRF, які зменшують ризик поширення атак усередині мережі та допомагають ізолювати критичні сервіси. Завдяки модульності адміністратори можуть оперативно вносити зміни, модернізувати обладнання або додавати нові сервіси, не перериваючи роботу інших частин системи. Це робить корпоративну мережу більш керованою, надійною та стійкою до відмов.

Приклад побудови корпоративної мережі зображено на рисунку 1.1.

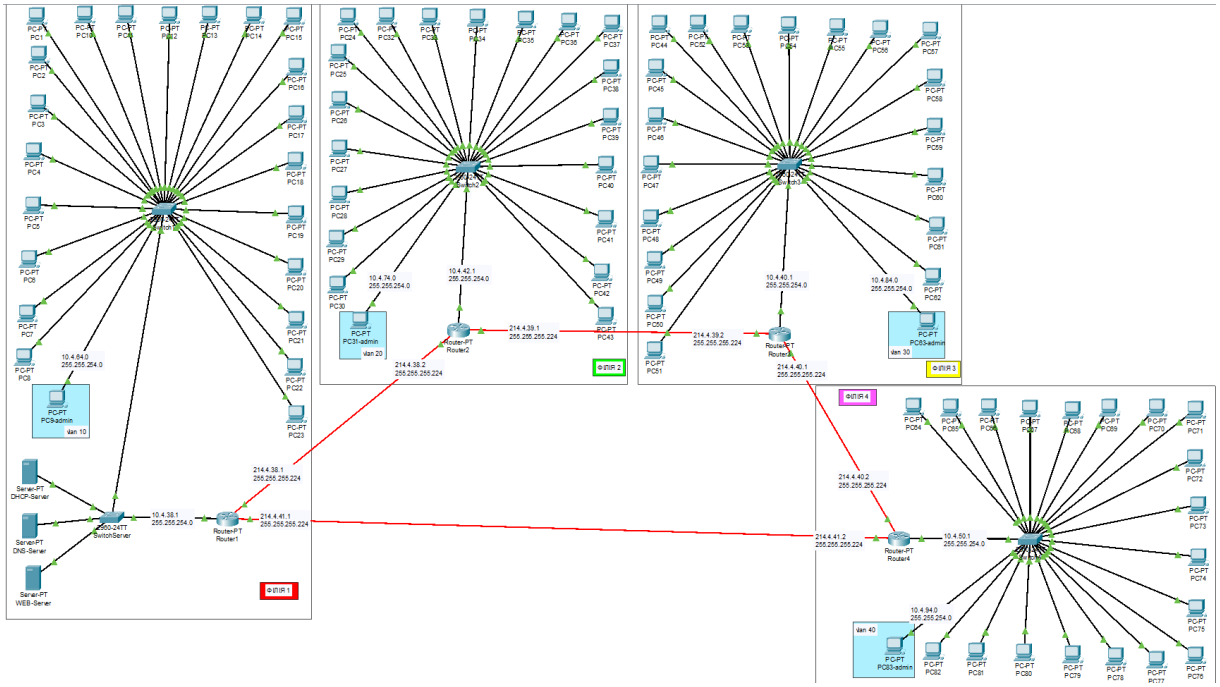


Рисунок 1.1 - Приклад схеми корпоративної мережі

Основними компонентами корпоративних мереж є маршрутизатори, комутатори (у тому числі рівня 3), міжмережеві екрани (firewalls), сервери, кінцеві пристрої та мережеві інтерфейсні карти (NIC) та кабелі для з’єднання компонентів.

Маршрутизатори використовуються для поділу локальних мереж (LAN) на підмережі, балансування трафіку та фільтрації даних відповідно до політик безпеки. Приклад маршрутизатора Cisco 2800 Series зображено ра рисунку 1.2.

Рисунок 1.2 – Маршрутизатор Cisco 2800 Series

Комутатори, зокрема комутатори третього рівня (Layer 3), забезпечують ефективну передачу даних і можуть здійснювати комутацію на швидкості лінії, що особливо важливо для підключення серверів у таких модулях, як E-Commerce Module. Приклад комутатора Cisco 2960 зображено ра рисунку 1.3.

Рисунок 1.3 – Комутатор Cisco 2960

Міжмережеві екрани розташовуються в різних точках мережі для контролю потоків трафіку, захисту від зовнішніх загроз і реалізації політик безпеки; вони можуть бути інтегрованими у маршрутизатори або існувати як окремі пристрої. Приклад апаратного міжмережевого екрану WatchGuard Firebox T15 зображено ра рисунку 1.4.

Рисунок 1.4 – Апаратний міжмережевий екран

Сервери забезпечують роботу прикладних систем, баз даних і вебсервісів, підтримуючи бізнес-процеси та доступ користувачів до ресурсів. Приклад серверу HP Proliant зображено ра рисунку 1.5.

Рисунок 1.5 - Сервер HP Proliant

Кінцеві пристрої (робочі станції, ноутбуки, мобільні пристрої) є точками доступу користувачів до мережевих сервісів, а мережеві інтерфейсні карти (NIC) забезпечують апаратне підключення пристроїв до корпоративної мережі. Приклад мережевої карти зображено ра рисунку 1.6.

Рисунок 1.6 – Мережева карта

1.2 Переваги та виклики використання корпоративних мереж

Корпоративні мережі сьогодні є фундаментальною складовою інформаційної інфраструктури будь-якої організації, незалежно від її масштабів чи галузевої специфіки. Вони забезпечують об’єднання розподілених ресурсів, ефективну взаємодію між підрозділами, захищений доступ до даних і можливість централізованого управління сервісами. Розвиток бізнес-процесів, зростання вимог до безпеки та цифрової трансформації організацій зумовлюють високі вимоги до гнучкості, масштабованості та надійності корпоративних мереж. У цьому контексті важливо розглядати як переваги, так і можливі виклики їх впровадження та експлуатації [4].

Однією з ключових переваг корпоративних мереж є централізація доступу до ресурсів. Працівники отримують єдину платформу для взаємодії з корпоративними сервісами - базами даних, файловими сховищами, бізнес-додатками та комунікаційними інструментами. Така централізація дозволяє оптимізувати управління обліковими записами, політиками доступу та правилами безпеки, зменшуючи ризик неконтрольованого розповсюдження інформації.

Суттєвою перевагою є також зниження операційних витрат і підвищення продуктивності персоналу. Налагоджені механізми маршрутизації, балансування навантаження та управління трафіком дозволяють ефективно використовувати доступні ресурси, покращувати швидкість доступу до сервісів та мінімізувати простої. Автоматизація мережевих процесів, яка активно впроваджується на базі сучасних SDN-рішень, додатково зменшує витрати на ручне адміністрування.

Корпоративні мережі також забезпечують високу надійність та відмовостійкість. Використання резервування каналів зв’язку, дублювання критичних елементів інфраструктури, протоколів швидкої конвергенції та механізмів failover дозволяє підтримувати неперервність бізнес-процесів навіть у випадку відмов обладнання або зовнішніх атак. Особливо важливо це у великих підприємствах, де простої можуть призвести до значних фінансових втрат.

Ще однією перевагою є масштабованість, тобто можливість поступового розширення мережі без значних змін у її архітектурі. Сучасні модульні мережеві моделі (наприклад, Cisco SAFE або моделі зонування Campus-Edge-Data Center) дозволяють нарощувати кількість користувачів, серверів, сервісів чи географічних локацій без порушення стабільності та безпеки існуючої інфраструктури.

Також важливою є підтримка різних типів трафіку - від даних і голосового зв'язку до відеоконференцій і специфічних додатків, що вимагають низької затримки. Використання QoS-механізмів дозволяє пріоритизувати критичні для бізнесу сервіси, забезпечуючи стабільну роботу навіть при максимальному навантаженні мережі. Особливості підтримки мультимедійного трафіку, QoS та вимоги до затримок і втрат пакетів для КМ детально описано в [4].

Попри численні переваги, корпоративні мережі супроводжуються низкою викликів, які важливо враховувати під час проєктування та експлуатації. Одним із головних є підвищена складність управління. Сучасні мережі включають велику кількість взаємопов'язаних елементів: маршрутизаторів, комутаторів, міжмережевих екранів, серверів, точок доступу та систем забезпечення безпеки. Управління такою системою потребує високої кваліфікації персоналу та застосування спеціалізованих інструментів моніторингу й автоматизації.

Другим важливим викликом є забезпечення кібербезпеки. Зростання кількості атак на корпоративні мережі - включаючи DoS-атаки, фішинг, несанкціонований доступ, експлуатацію вразливостей обладнання та програмного забезпечення — вимагає впровадження багаторівневих систем захисту. Для цього необхідні міжмережеві екрани, системи виявлення вторгнень, сегментація трафіку, Zero Trust-архітектури та регулярний аудит безпеки. Розбудова такої багаторівневої системи може бути фінансово й технічно складною.

Ще однією проблемою є масштабування інфраструктури. Хоча сучасні корпоративні мережі проєктуються модульно, реальне розширення ресурсів може вимагати заміни обладнання, оновлення прошивок, налаштування нових політик маршрутизації та безпеки. Це ускладнює інтеграцію застарілих систем із новими технологіями та може призводити до тимчасових перерв у роботі сервісів.

Не менш критичним викликом є забезпечення відмовостійкості та безперервності сервісів. Навіть за наявності механізмів резервування, зміни маршрутизації або перемикання на резервні канали можуть супроводжуватися затримками, короткочасними перервами чи некоректною роботою окремих додатків. Крім того, неправильне налаштування протоколів HSRP, VRRP, GLBP або STP може спричинити петлі в мережі та повне її перезавантаження. Особливості взаємодії протоколів резервування шлюзів із протоколами комутації другого рівня (STP, RSTP, VLAN) та вплив архітектури комутованої мережі на загальну відмовостійкість докладно описано в [5-6].

До викликів також належить висока вартість впровадження та модернізації. Корпоративна мережа потребує інвестицій у надійне обладнання, ліцензії, спеціалізоване програмне забезпечення, резервні канали зв’язку та засоби безпеки. Додаткові витрати пов’язані з навчанням IT-персоналу, регулярним оновленням систем і проведенням аудитів.

Важливо згадати й людський фактор, оскільки помилки адміністраторів залишаються однією з найпоширеніших причин збоїв у корпоративних мережах. Неправильні налаштування VLAN, ACL, протоколів маршрутизації чи правил безпеки можуть створювати критичні вразливості або навіть спричинити повний вихід мережі з ладу.

1.3 Проблеми надійності та безперервності роботи

Як було описано раніше забезпечення надійності мереж та захист інформації стало одним із першочергових завдань у контексті цифрової трансформації та зростання кіберзагроз. Дослідники наголошують, що сучасні інформаційні системи повинні не лише протистояти зовнішнім атакам, але й зберігати стійкість під час внутрішніх збоїв та інфраструктурних несправностей [7].

Вихід мережі з ладу - це серйозна проблема, яка може порушити зв’язок у мережі, і включає збій каналу, зміну конфігурації, відмову сайту та відмову будь-якого мережевого компонента, такого як маршрутизатор або комутатор. Для перевірки того, чи працює вузол і відповідає, можна використовувати такі методи, як пінгування та тайм-аут. Коли машини з різних мереж із їхніми унікальними конфігураціями та політиками беруть участь, будь-яка зміна цих конфігурацій може створити проблеми для додатків, які використовують ресурси цих машин.

Несправність виникає тоді, коли система не здатна виконати очікуване завдання через ненормальний стан одного або кількох її компонентів. Несправність може спричинити появу помилки, яка, у свою чергу, призводить до часткової або повної відмови системи. Таким чином, помилки є проявами несправностей, а несправності - їхньою першопричиною.

У розподілених системах несправності класифікують за причиною, місцем виникнення та типом. Серед них виділяють часові помилки, що виникають, коли відповіді надходять раніше (рання часова помилка) або пізніше (пізня часова помилка), ніж визначено допустимим інтервалом. Окремим різновидом часової помилки є пропускна відмова (omission failure), коли сервер узагалі не надсилає відповідь на вхідний запит.

Апаратні відмови охоплюють усі проблеми, пов’язані з фізичним обладнанням: вихід з ладу серверів і робочих станцій, дисків, пам’яті, процесорів, периферійних пристроїв, а також збої, спричинені перегрівом чи іншими фізичними чинниками. Програмні відмови стосуються не лише прикладних програм, а й операційної системи та проміжного програмного забезпечення. До них належать збої ОС, критичні помилки додатків, некоректний ввід даних, користувацькі та необроблені винятки, а також збої, пов’язані з виконанням конкретних задач. У разі відмови операційної системи робота всіх програм і сервісів на відповідному вузлі повністю припиняється [8].

Простої мережі мають суттєві економічні наслідки, що проявляються у втраті прибутку, зниженні продуктивності та погіршенні ділової репутації. Рівень збитків залежить від масштабу підприємства: для малого бізнесу втрати можуть становити

приблизно 427 доларів за хвилину, тоді як для великих корпорацій - до 100 000 доларів і більше за годину простою.

Економічні наслідки поділяються на прямі та непрямі (приховані) витрати.

Прямі фінансові втрати:

- втрачений дохід. Компанії, що залежать від онлайн-операцій, втрачають гроші з кожною хвилиною простою, адже клієнти не можуть здійснити покупку, оплату чи бронювання;

- витрати на відновлення. Простої часто потребують дорогого ремонту або заміни обладнання й програмного забезпечення, а також залучення зовнішніх фахівців для відновлення роботи систем.

Непрямі та приховані витрати:

- зниження продуктивності. Під час простою працівники не можуть виконувати завдання, отримувати доступ до файлів чи спілкуватися між собою, що спричиняє затримки проєктів і зрив термінів. За дослідженнями, після переривання роботи співробітнику потрібно в середньому 23 хвилини, щоб знову зосередитися;

- пошкодження репутації. Часті або тривалі перебої можуть зменшити довіру клієнтів і спричинити негативні відгуки, що у довгостроковій перспективі шкодить бренду;

- втрата клієнтської довіри. Користувачі можуть перейти до конкурентів, якщо їхні сервіси доступніші або стабільніші;

- підвищені ризики безпеки. У період простою мережа часто стає більш вразливою до кіберзагроз - зокрема витоку даних чи атак зловмисників;

- зниження вартості акцій. Для публічних компаній значні простої можуть негативно впливати на показники біржової вартості.

Зрештою, усе схильне до зносу - від масштабних IT-систем із кількома майданчиками до звичайних лампочок. Незапланований простій може мати серйозні, а подекуди й катастрофічні наслідки. Тому інженери та технічні фахівці з обслуговування повинні заздалегідь розробляти плани дій, щоб у разі відмови оперативно усунути проблему. Основна мета полягає в мінімізації часу простою,

що дозволяє скоротити втрати, пов’язані зі зниженням продуктивності, прибутку чи задоволеності клієнтів.

1.3.1 Показники надійності мережі та їх вплив на якість обслуговування

Існує багато способів зменшити час простою. Наприклад, компанія може скоротити тривалість ремонту обладнання, забезпечивши наявність необхідних запасних частин безпосередньо на місці. Інший підхід - аналіз процесів ремонту для пошуку швидших методів виконання робіт або ефективніших способів сповіщення техніків. Крім того, доцільно інвестувати у високоякісне обладнання з довшим терміном служби, що дозволяє рідше здійснювати ремонт.

Однак, щоб покращити надійність систем і компонентів, спершу потрібно вміти її вимірювати. Серед найпоширеніших показників надійності у сфері технічного обслуговування є середній час відновлення (MTTR, Mean Time To Repair), також відомий як середній час відновлення працездатності, та середній час між відмовами (MTBF, Mean Time Between Failures). Хоча ці показники взаємопов’язані, вони мають різне призначення і відповідають на різні питання щодо надійності систем або продуктів [9].

MTBF - це ключовий показник ефективності (KPI), який відображає середній час між двома послідовними відмовами системи або пристрою. Цей показник використовується для оцінки надійності й часто застосовується під час планування технічного обслуговування, розробки продуктів та визначення гарантійних термінів. Варто зазначити, що MTBF стосується відновлюваних об’єктів, тобто тих, які можна відремонтувати. Його не слід плутати з близьким за змістом показником MTTF, який використовується для невідновлюваних пристроїв, що підлягають заміні після виходу з ладу.

Розрахунок MTBF здійснюється за формулою 1.1:

$$MTBF = \frac{T_{\text{заг}}}{N_{\text{відм}}} \qquad (1.1)$$

Наприклад, якщо пристрій працював 1000 годин і за цей час вийшов з ладу тричі, то MTBF становитиме:

$$\frac{1000}{3} = 333.3$$

Це означає, що в середньому пристрій можна очікувати до відмови після приблизно 333 годин роботи.

Показник MTBF допомагає оцінити очікувану тривалість роботи продукту та спланувати своєчасне технічне обслуговування або заміну компонентів. Водночас MTBF не враховує час, необхідний на ремонт після відмови - а це може мати суттєве значення для багатьох систем.

Саме для цього застосовується показник MTTR (Mean Time To Repair).

MTTR - це показник, який відображає середній час, необхідний для відновлення працездатності системи або пристрою після відмови. Він характеризує надійність обладнання з точки зору ремонтопридатності та ефективності обслуговування.

До складу MTTR зазвичай входить час, витрачений на повідомлення технічної команди про інцидент, охолодження або підготовку обладнання до ремонту, усунення несправності, повторне складання елементів системи, а також тестування перед відновленням роботи або виробничого процесу.

Основна мета використання MTTR - мінімізувати простої, спричинені відмовами, і, відповідно, знизити витрати, пов’язані з ремонтами та втраченою продуктивністю.

Розрахунок MTTR здійснюється за формулою 1.2:

$$MTTR = \frac{T_{\text{рем}}}{N_{\text{відм}}} \qquad (1.2)$$

Наприклад, якщо за останній рік система виходила з ладу 5 разів, а сумарний час простою (включно з ремонтом) становив 10 годин, то:

$$\frac{10}{5} = 2$$

Це означає, що в середньому на відновлення системи після кожної відмови потрібно близько двох годин.

Показник MTTR є корисним інструментом для оцінки ефективності ремонтних процесів і допомагає визначити напрямки, у яких можна підвищити продуктивність технічного обслуговування [10].

Висока надійність мережі безпосередньо впливає на якість обслуговування (QoS) - набір інструментів і методів, які використовуються для керування та покращення продуктивності мережі. Він потрібен для встановлення пріоритетів трафіку (рис. 1.7), розподілу ресурсів і забезпечення своєчасної доставки пакетів даних. За допомогою QoS можна підвищити продуктивність таких програм, як VoIP, потокове відео та онлайн-ігри [11].

Рисунок 1.7 - Схема прикладу встановлення пріоритетів трафіку

Параметри QoS - це параметри, які визначають продуктивність мережі. Вони дуже важливі, оскільки за допомогою них можна зрозуміти, як добре функціонує мережа та яку кількість даних можна без проблем передавати по ній.

Основні параметри QoS включають:

- пропускна здатність (Throughput) - обсяг даних, що передається мережею за одиницю часу;

- затримка (Latency) - час переміщення пакету від джерела до одержувача;

- тремтіння (Jitter) - нерівномірність затримки пакетів, критична для VoIP та потокового відео;

- втрати пакетів (Packet Loss) - відсоток пакетів, що не досягли отримувача.

Взаємозв’язок надійності та QoS полягає в наступному:

- зменшення часу простою та відмов (збільшення MTBF та зменшення MTTR) забезпечує стабільну пропускну здатність і зменшує втрати пакетів;

- швидке відновлення систем після відмови мінімізує затримки та тремтіння, що покращує роботу критичних сервісів;

- низька надійність проявляється у деградації параметрів QoS, навіть якщо обладнання відповідає стандартам швидкості та пропускної здатності.

Як показано в класичних роботах з комп’ютерних мереж, деградація показників QoS майже завжди є наслідком зниження надійності інфраструктури, що підтверджує необхідність впровадження механізмів резервування.

1.4 Постановка завдань проведення досліджень

У попередніх підпунктах 1.1-1.3 було розглянуто теоретичні основи побудови корпоративних мереж, їхню структуру, основні компоненти, переваги та виклики впровадження, а також проблеми надійності та безперервності роботи. Окремо проаналізовано економічні наслідки простоїв, поняття MTBF та MTTR, а також взаємозв’язок надійності інфраструктури з параметрами якості обслуговування (QoS). На основі цих положень формуються цілі та завдання даного дослідження, а також концепція реалізації системи забезпечення відмовостійкості корпоративної мережі.

Для досягнення поставленої мети необхідно розв’язати такі основні завдання дослідження:

- проаналізувати структуру та особливості функціонування корпоративних мереж, виділити їхні ключові компоненти та вузли, від надійності яких залежить безперервність роботи інформаційних систем;

- дослідити проблеми надійності та безперервності функціонування корпоративних мереж, виявити основні причини відмов і простоїв, а також їхні технічні та економічні наслідки;

- розглянути існуючі методи та механізми резервування мережевих ресурсів, зокрема протоколи HSRP, VRRP, GLBP, Spanning Tree Protocol та інші засоби забезпечення відмовостійкості;

- виконати порівняльний аналіз протоколів резервування за критеріями сумісності з обладнанням, підтримки балансування навантаження, складності налаштування, часу перемикання та масштабованості, обґрунтувати вибір протоколу для практичної реалізації;

- розробити модель відмовостійкої корпоративної мережі з урахуванням різнорідності обладнання (маршрутизатори, комутатори, сервери, канали зв’язку) та можливостей програмного резервування;

- реалізувати тестову схему мережі в середовищі моделювання (Cisco Packet Tracer), налаштувати протокол резервування (HSRP) та перевірити базову працездатність мережі;

- розробити методику експериментальних досліджень, що включає сценарії відмов вузлів та каналів, вимірювання часу автоматичного перемикання (failover), часу відновлення активної ролі маршрутизатора, втрат пакетів та зміни затримки;

- провести серію експериментів для різних конфігурацій мережі (без резервування, з HSRP зі стандартними та оптимізованими таймерами), виконати аналіз отриманих результатів та порівняння альтернативних підходів до забезпечення відмовостійкості;

- сформулювати практичні рекомендації щодо налаштування протоколів резервування та побудови відмовостійких корпоративних мереж.

Реалізація поставлених завдань здійснюється поетапно, відповідно до структури дипломної роботи.

Ці завдання охоплюють усі етапи дослідження - від аналізу надійності мережевої інфраструктури до розробки та перевірки системи відмовостійкості. У результаті передбачається створення функціональної системи, що забезпечує безперервність роботи, високий рівень надійності та оптимальну ефективність корпоративних мереж.

2 ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКОСТІ КОРПОРАТИВНИХ МЕРЕЖ

2.1 Огляд методів резервування та відмовостійкості мереж

Виходячи з мети дослідження розглянемо методи, завдяки яким можна створити надійну мережу, яка не втратить своєї функціональності навіть під час збоїв. Для узагальнення усіх технологій використовують поняття «Висока доступність (high availability, HA)» – це здатність системи працювати безперервно без збоїв протягом заданого періоду часу. В інформаційних технологіях (IT) прийнято використовувати для позначення HA стандартний показник «п’ять дев’яток», що означає, що система має бути доступною 99,999% часу протягом року. Високодоступні системи ретельно проєктуються та тестуються перед введенням в експлуатацію. При плануванні кожної з таких систем підбираються компоненти, які відповідають вимогам стандарту доступності. Питання математичного опису високої доступності, моделі розрахунку загальної готовності системи та впливу різних видів відмов детально висвітлено в [12], де наведені практичні приклади побудови високодоступних мережевих рішень.

Методи для забезпечення високої доступності:

- балансування навантаження;
- усунення єдиної точки відмови;

- моніторинг;
- відмовостійкість;
- аварійне відновлення.

Балансування навантаження (load balancing) забезпечує автоматичний розподіл робочих запитів між серверами чи іншими ресурсами з метою рівномірного завантаження інфраструктури та запобігання перевантаженням. Під час надходження користувацького запиту балансувальник визначає оптимальний ресурс для його обробки, що дозволяє підтримувати стабільну роботу сервісів та підвищувати їх доступність. У сучасних інформаційних системах балансування навантаження реалізується як за допомогою програмних рішень (reverse proxy, спеціалізовані балансувальники), так і засобами хмарних платформ.

Важливою складовою побудови надійної інфраструктури є усунення єдиних точок відмови (Single Point of Failure, SPOF). Єдина точка відмови - це компонент, збій якого може призвести до зупинки всієї системи або викликати каскадні збої в залежних елементах. Для зменшення подібних ризиків на кожному рівні інфраструктури впроваджують механізми надмірності: кластеризацію серверів, високодоступні платформи віртуалізації, кластерні системи керування контейнерами, а також реплікацію даних у базах даних. У мережевій інфраструктурі надмірність забезпечується, зокрема, за рахунок використання кількох маршрутизаторів, дубльованих комутаторів, резервних лінків та протоколів динамічної маршрутизації (OSPF, BGP), що дозволяють автоматично переключатися на альтернативні маршрути у разі відмови одного з сегментів.

Для підтримання стабільної роботи системи важливим є постійний моніторинг її працездатності та продуктивності. Сучасні системи моніторингу й збору логів дозволяють своєчасно виявляти відхилення в роботі обладнання і сервісів, прогнозувати потенційні проблеми та оперативно реагувати на позаштатні ситуації. Вони надають аналітику щодо завантаження мережі, часу відповіді, кількості помилок і збоїв, що значно підвищує загальну надійність інфраструктури.

Відмовостійкість (fault tolerance, FT) - це властивість системи забезпечувати безперервність роботи навіть у разі відмови одного або кількох її компонентів.

Іншими словами, це здатність мережі продовжувати функціонувати без суттєвого зниження продуктивності чи втрати даних при виникненні збоїв у її елементах. Одним із ключових способів досягнення відмовостійкості є резервування (redundancy), тобто створення дублюючих елементів, які замінюють основні компоненти у випадку їх відмови [13]. Резервування може стосуватися різних рівнів системи: фізичної інфраструктури, маршрутизаторів, каналів зв'язку, сервісів та даних.

Резервування на рівні фізичної інфраструктури передбачає дублювання апаратних елементів - серверів, джерел живлення, мережевих карт, комутаторів і кабельних ліній. Використання двох і більше фізичних каналів або пристроїв забезпечує наявність альтернативного шляху для передачі даних у разі пошкодження чи виходу з ладу основного обладнання [14].

Резервування маршрутизаторів (шлюзів) реалізується за допомогою технологій, які забезпечують автоматичне перемикання між активним і резервним шлюзами. Серед найбільш поширених рішень - протоколи резервування першого переходу (FHRP, First Hop Redundancy Protocols). Вони дозволяють створювати віртуальний шлюз, до якого підключаються клієнти, тоді як реальні маршрутизатори працюють у режимі активного або резервного, забезпечуючи безперервний доступ до мережі.

Резервування каналів зв'язку полягає у використанні кількох незалежних каналів передачі даних, що з'єднують локальні та віддалені сегменти мережі. У разі відмови одного каналу інший автоматично бере на себе трафік. Для цього використовуються механізми динамічної маршрутизації (OSPF, BGP), балансування навантаження або технології агрегації каналів (Link Aggregation, EtherChannel). Такий підхід дозволяє знизити ймовірність втрати зв'язку та забезпечити стабільну пропускну здатність.

Резервування сервісів і даних реалізується на рівні програмного забезпечення - за допомогою кластеризації серверів, реплікації баз даних, механізмів знімків (snapshot) і систем резервного копіювання. Це дозволяє зберегти цілісність

інформації та забезпечити доступність критичних сервісів навіть у разі відмови окремих вузлів.

Залежно від способу активації резервних ресурсів розрізняють активне та пасивне резервування. Активне резервування (active redundancy) передбачає одночасну роботу основного і резервного елементів із розподілом навантаження між ними, що забезпечує високу продуктивність і швидке перемикання у разі збою. Пасивне резервування (passive redundancy) означає, що резервні елементи перебувають у режимі очікування і активуються лише після виходу з ладу основних, що є більш економічним, але зазвичай супроводжується більшим часом відновлення.

Аварійне відновлення (disaster recovery, DR) є завершальним та критично важливим елементом забезпечення безперервності роботи системи. DR-процедури охоплюють резервне копіювання, реплікацію критичних даних, перемикання на резервні майданчики та відновлення після техногенних або природних катастроф. У практиці використовуються як локальні, так і хмарні рішення для резервного копіювання й реплікації. Сукупність цих технологій забезпечує швидке відновлення системи та мінімізацію простоїв у критичних ситуаціях, гарантуючи високу доступність сервісів навіть за умов масштабних збоїв.

Підсумовуючи, слід зазначити, що високодоступна мережа ґрунтується на поєднанні резервування обладнання, каналів зв’язку, сервісів і даних, а також на розвинених механізмах моніторингу та аварійного відновлення [15]. У межах даної дипломної роботи основний акцент робиться саме на мережевих механізмах забезпечення відмовостійкості, зокрема на резервуванні шлюзів доступу за допомогою протоколів першого переходу (FHRP). Саме ці протоколи визначають безперервність доступу користувачів до мережевих ресурсів і стануть предметом детального аналізу та практичної реалізації в подальших розділах.

2.1.1 Захист інформації як компонент надійності

Безпека мережі є невід’ємною складовою її надійності, оскільки успішні атаки або несанкціонований доступ можуть призвести до відмови сервісів не менш критичної, ніж фізичний збій обладнання. Тому в комунікаційних системах

застосовуються різноманітні засоби захисту інформації, які доповнюють механізми резервування та відмовостійкості й у комплексі забезпечують безперервність роботи корпоративної мережі.

Для блокування атак із зовнішнього середовища використовують міжмережеві екрани (firewall), які керують проходженням мережевого трафіку відповідно до встановлених правил. Зазвичай їх встановлюють на вході мережі, на «прикордонних» маршрутизаторах, що дозволяє розділити мережу на внутрішні (приватні) та зовнішні (загального доступу) сегменти.

Системи виявлення втручань (Intrusion Detection System, IDS) призначені для своєчасного виявлення спроб несанкціонованого доступу як із зовнішніх джерел, так і всередині мережі, а також для захисту від атак типу «відмова в обслуговуванні» (DoS).

Засоби створення віртуальних приватних мереж (VPN, Virtual Private Network) дозволяють організувати захищені канали передачі даних через незахищене середовище. Технологія VPN забезпечує прозоре для користувача об’єднання локальних мереж, водночас зберігаючи конфіденційність і цілісність інформації завдяки динамічному шифруванню.

Засоби аналізу захищеності застосовуються для оцінки рівня безпеки корпоративних мереж, виявлення потенційних каналів загроз і контролю стану захищеності. Це дозволяє своєчасно отримувати інформацію про можливі атаки, оптимізувати втрати та підвищувати ефективність захисту інформації.

Для забезпечення безпечного обміну даними між корпоративними мережами застосовують фільтри доступу (ACL-списки), формують захищені тунелі на основі технології VPN, а також реалізують аутентифікацію та криптографічний захист інформації в граничних маршрутизаторах.

Як підсумок, розглянемо ключові технології та рішення для створення відмовостійкої мережі. У таблиці 2.1 наведено основні засоби та методи, що забезпечують безперервність роботи, резервування компонентів та захист даних.

Таблиця - 2.1 Технології для створення відмовостійкої мережі

Категорія	Призначення	Технології / Приклади
Балансування навантаження	Рівномірний розподіл трафіку між серверами/ресурсами, забезпечення безперервної роботи при відмові вузлів	Програмні балансувальники (reverse proxy), хмарні load balancer-и
Усунення єдиної точки відмови (SPOF)	Створення надмірності на всіх рівнях інфраструктури, автоматичне переключення при збоях	Кластеризація серверів, високодоступні платформи віртуалізації, реплікація БД
Динамічна маршрутизація	Забезпечення альтернативних маршрутів у разі відмови каналу чи маршрутизатора	OSPF, BGP
Протоколи резервування шлюзів (FHRP)	Автоматичне перемикання між активним і резервним маршрутизаторами, збереження доступу до мережі	VRRP, HSRP, GLBP
Резервування фізичної інфраструктури	Захист від відмов обладнання, дублювання ключових компонентів	Резервні сервери, подвійні БЖ, дубльовані NIC, резервні комутатори
Агрегація та резервування каналів	Забезпечення сталого зв’язку й підвищення пропускної здатності	Link Aggregation, LACP, EtherChannel
Моніторинг працездатності	Раннє виявлення проблем, запобігання збоям, аналітика роботи системи	Системи збору метрик і логів, платформи моніторингу (Zabbix, Prometheus тощо)
Резервування сервісів і даних	Захист інформації від втрати, забезпечення доступності критичних даних	Кластеризація сервісів, реплікація БД, резервне копіювання
Аварійне відновлення (DR)	Відновлення роботи після критичних збоїв, катастроф, втрати даних	Системи резервного копіювання, реплікація на резервні майданчики
Мережевий захист	Захист від атак, забезпечення безпечної передачі даних	Фаєрволи, IDS/IPS, ACL, VPN
Шифрування та тунелювання	Забезпечення конфіденційності та цілісності при передачі даних	VPN-технології, TLS, IPsec

2.2 Огляд протоколів резервування

Розглянемо резервування маршрутизаторів більш детально. Якщо існує тільки один маршрутизатор, ми створюємо єдину точку відмови (рис. 2.1). Якщо цей маршрутизатор або лінія зв’язку виходить з ладу - мережа не працюватиме.

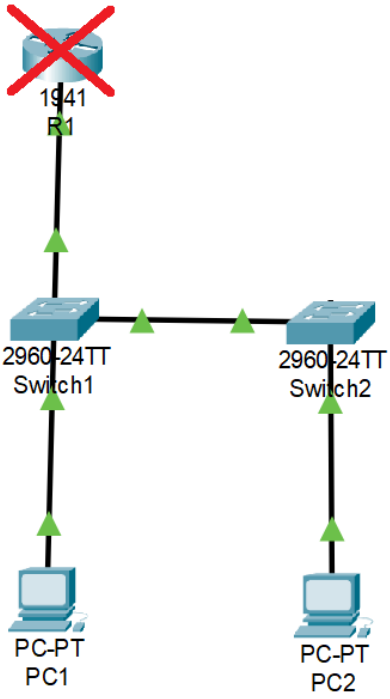


Рисунок 2.1 - Вихід з ладу маршрутизатора

Щоб уникнути цього, ми додаємо другий резервний маршрутизатор. Кожен маршрутизатор підключається до Інтернету або корпоративної WAN-мережі. Ми також підключаємо їх до різних комутаторів, щоб уникнути єдиної точки відмови (рис. 2.2).

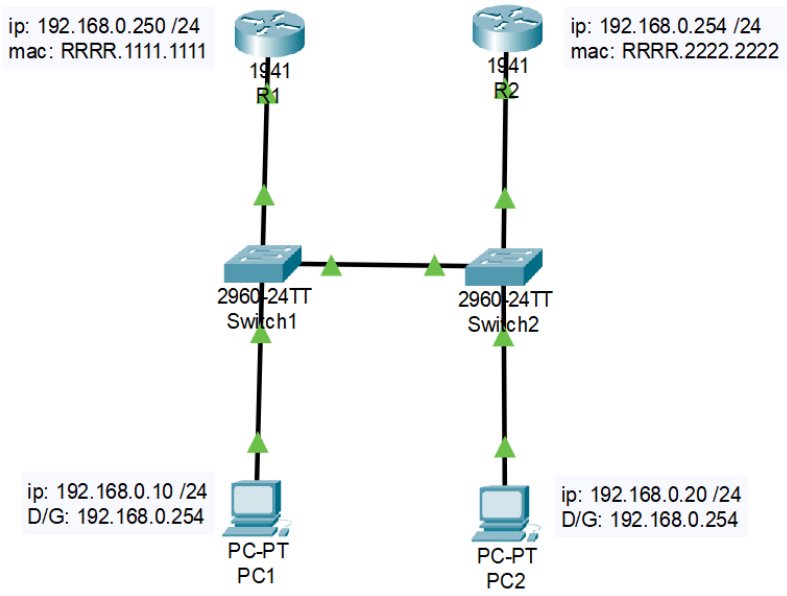


Рисунок 2.2 - Підключення резервного маршрутизатора

Однак у такій схемі є проблема. Коли пристрій хоче надіслати дані до вузла поза своєю мережею, він надсилає їх шлюзу за замовчуванням (default geteway, D/G). І ось тут є проблема: кожен хост має вказаний як шлюз маршрутизатор R2. Якщо маршрутизатор R2 виходить з ладу, хости все одно намагаються надсилати трафік до нього, навіть якщо маршрутизатор R1 повністю працездатний. Немає способу автоматично змінити шлюз за замовчуванням на всіх хостах у разі відмови маршрутизатора.

Ось де на допомогу приходять протоколи резервування першого переходу (First Hop Redundancy Protocol, FHRP).

Протоколи резервування - це системи, які забезпечують надійність мережі шляхом створення альтернативних шляхів передачі даних на випадок відмови основного каналу. Вони працюють шляхом безперервного моніторингу мережевих компонентів та автоматичного перенаправлення трафіку на резервні маршрути, якщо первинне з'єднання виходить з ладу [16].

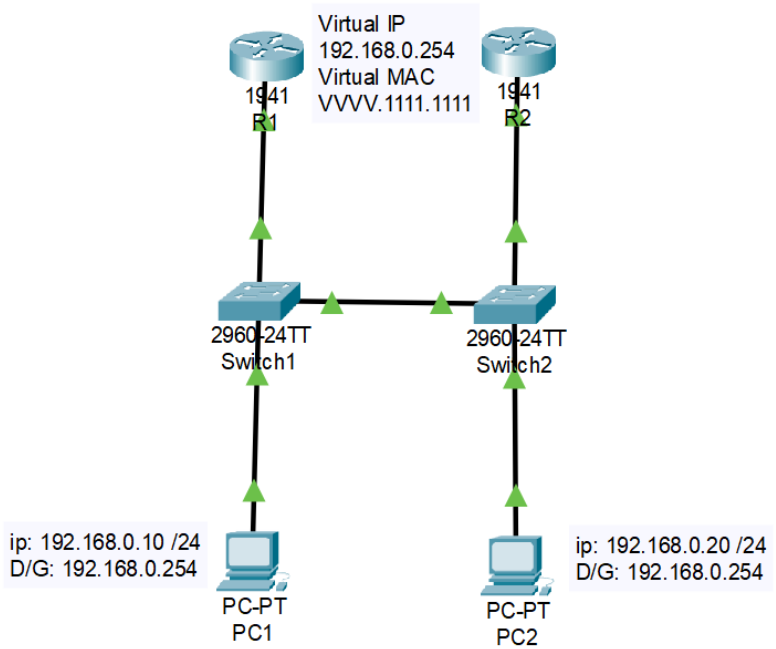


Рисунок 2.3 - Впровадження протоколів резервування

Впровадження протоколів резервування дозволяє мінімізувати час простою та підвищити загальну ефективність і продуктивність мережі. Протоколи FHRP

дозволяють хостам автоматично використовувати резервний маршрутизатор без жодних змін на самих хостах. Маршрутизатори об’єднуються в групу, яка має віртуальну IP-адресу і віртуальну MAC-адресу (рис. 2.3).

Хост надсилає ARP-запит до віртуальної IP-адреси. Обидва маршрутизатори отримують запит, але лише один відповідає, і він надсилає віртуальну MAC-адресу, а не власну. Якщо цей маршрутизатор виходить з ладу, інший починає відповідати на ARP-запити, знову використовуючи ту саму віртуальну MAC-адресу. Хост навіть не знає, що маршрутизатор змінився.

Якщо ARP-запит не надходить (бо хост використовує кеш ARP), новий активний маршрутизатор надсилає gratuitous ARP, щоб комутатори оновили свої MAC-таблиці. Таким чином, усі пристрої тепер використовуватимуть новий маршрутизатор. Це загальний погляд на те, як працюють FHRP. Тепер розглянемо кожен з них детальніше.

2.2.1 HSRP (Hot Standby Router Protocol)

HSRP - це протокол, розроблений компанією Cisco. Він працює майже так само, як описано в загальному принципі FHRP.

Маршрутизатори, що працюють з HSRP, надсилають і отримують multicast hello-повідомлення кожні три секунди. Вони використовуються для обміну інформацією та моніторингу стану один одного. Multicast-адреса залежить від версії протоколу:

- HSRP v1: 224.0.0.2;
- HSRP v2: 224.0.0.102.

Маршрутизатори визначають, який з них буде active (активний), а який - standby (резервний). Активний маршрутизатор «володіє» віртуальною IP-адресою та віртуальною MAC-адресою. Резервний лише чекає, поки активний вийде з ладу.

Вибір активного маршрутизатора базується на:

- найвищому пріоритеті HSRP;
- якщо пріоритети рівні - на найвищій IP-адресі інтерфейсу.

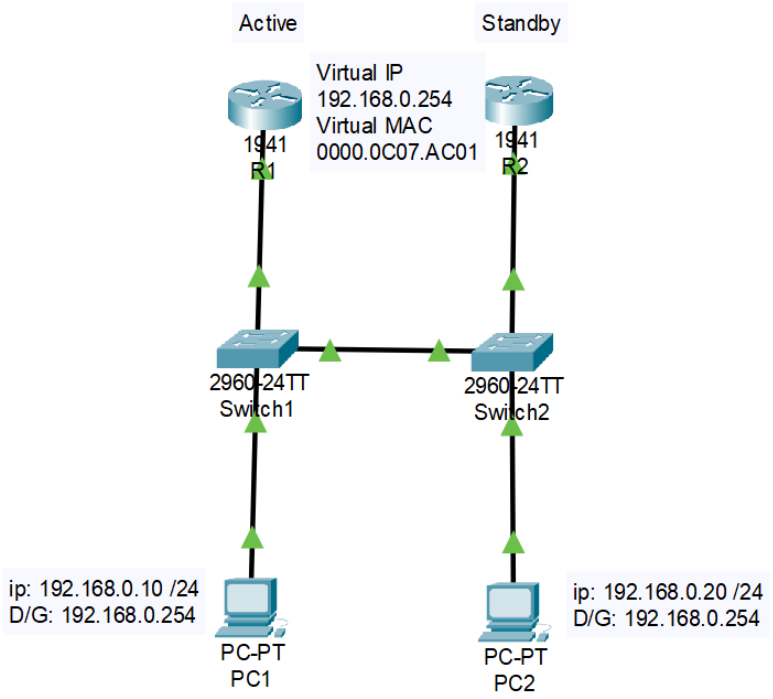


Рисунок 2.4 - Налаштування HSRP

Під час налаштування HSRP (рис. 2.4) адміністратор задає віртуальну IP-адресу, яку потім вказують як шлюз за замовчуванням на хостах. Віртуальна MAC-адреса генерується автоматично та має стандартний формат. Початкова частина MAC завжди однакова (ідентифікатор HSRP), а кінцеві байти показують ID групи:

- HSRP v1:0000.0C07.ACXX;

- HSRP v2: 0000.0C9F.FXXX.

Після запуску протоколу маршрутизатори регулярно обмінюються hello-пакетами. Це дозволяє переконатися, що активний маршрутизатор працює.

Якщо активний маршрутизатор виходить з ладу (рис. 2.5):

- резервний перестає отримувати hello-повідомлення;

- очікує завершення hold timer (10 секунд за замовчуванням);

- стає активним і надсилає повідомлення в мережу, щоб комутатори оновили свої MAC-таблиці (рис. 2.6).

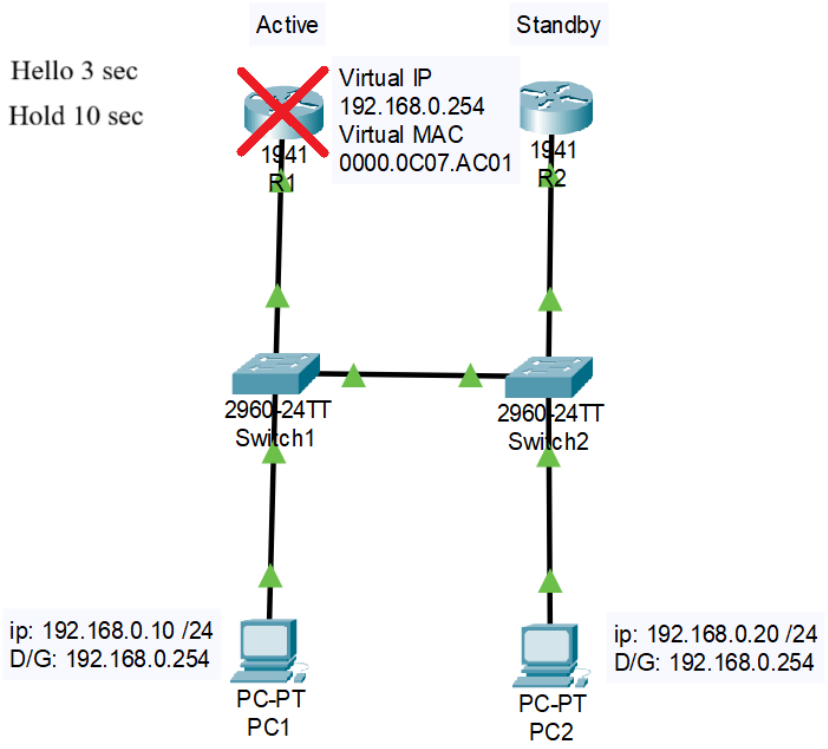


Рисунок 2.5 - Вихід з ладу активного маршрутизатора

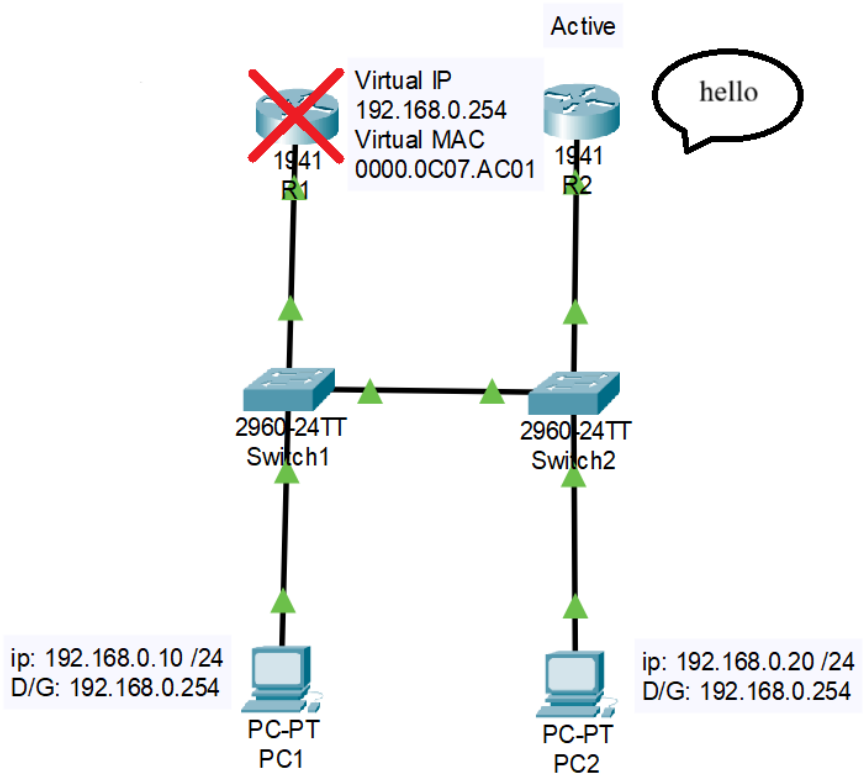


Рисунок 2.6 - Резервний маршрутизатор стає активним

За замовчуванням, коли «старий» активний маршрутизатор повертається до роботи, він не стає активним автоматично, а переходить у standby. Щоб змусити його завжди повертати собі роль активного, вмикають функцію standby preempt.

2.2.2 VRRP (Virtual Router Redundancy Protocol)

VRRP працює дуже схоже на HSRP. Є лише кілька незначних відмінностей. У VRRP маршрутизатори мають ролі: Master (основний) та Backup (резервний).

Однією з особливостей VRRP є те, що один з маршрутизаторів може мати реальну IP-адресу, яка одночасно є віртуальною IP-адресою (рис. 2.7). Такий маршрутизатор називається IP adress owner («власник IP-адреси»).

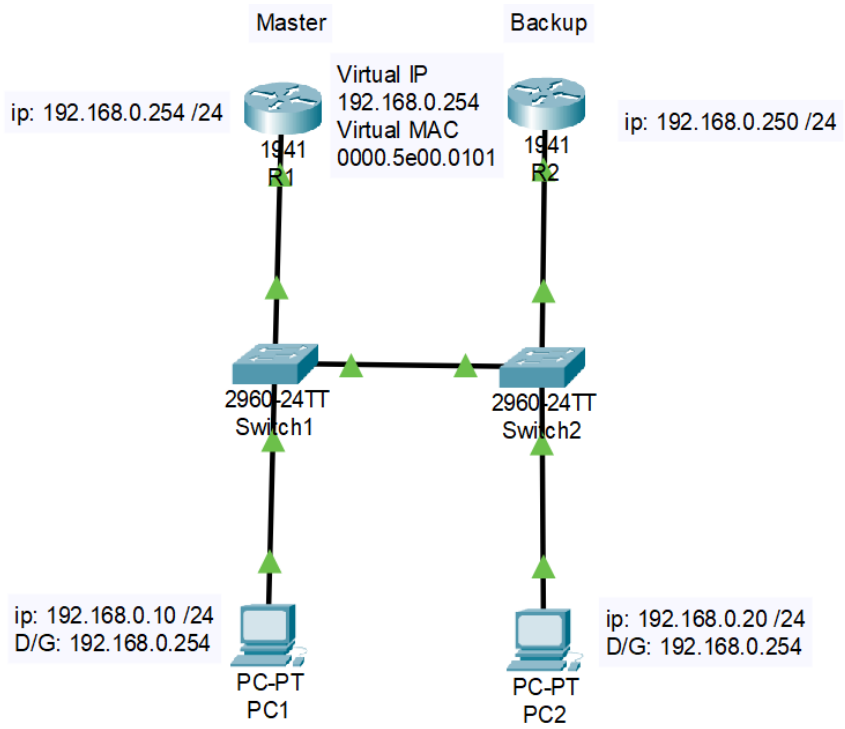


Рисунок 2.7 - Налаштування VRRP

«Власник IP» завжди обирається майстром, якщо він доступний. Якщо IP-власник недоступний, вибір здійснюється за такими ж правилами, як і в HSRP:

- найвищий пріоритет (діапазон 1-254, за замовчуванням 100);
- потім найвища IP-адреса.

Віртуальна MAC-адреса VRRP має інший формат, але також містить ідентифікатор та номер групи: 0000.5e00.01XX.

VRRP надсилає повідомлення лише від master, а не від усіх маршрутизаторів, як у HSRP. Master надсилає advertisement-повідомлення на multicast-адресу 224.0.0.18 щосекунди.

Якщо master виходить з ладу (рис. 2.8):

- Backup чекає завершення master down timer,

- Це приблизно три секунди за замовчуванням (3 × advertisement timer + невеликий додатковий інтервал),

- Після цього backup стає новим master і надсилає оголошення в мережу (рис. 2.9).

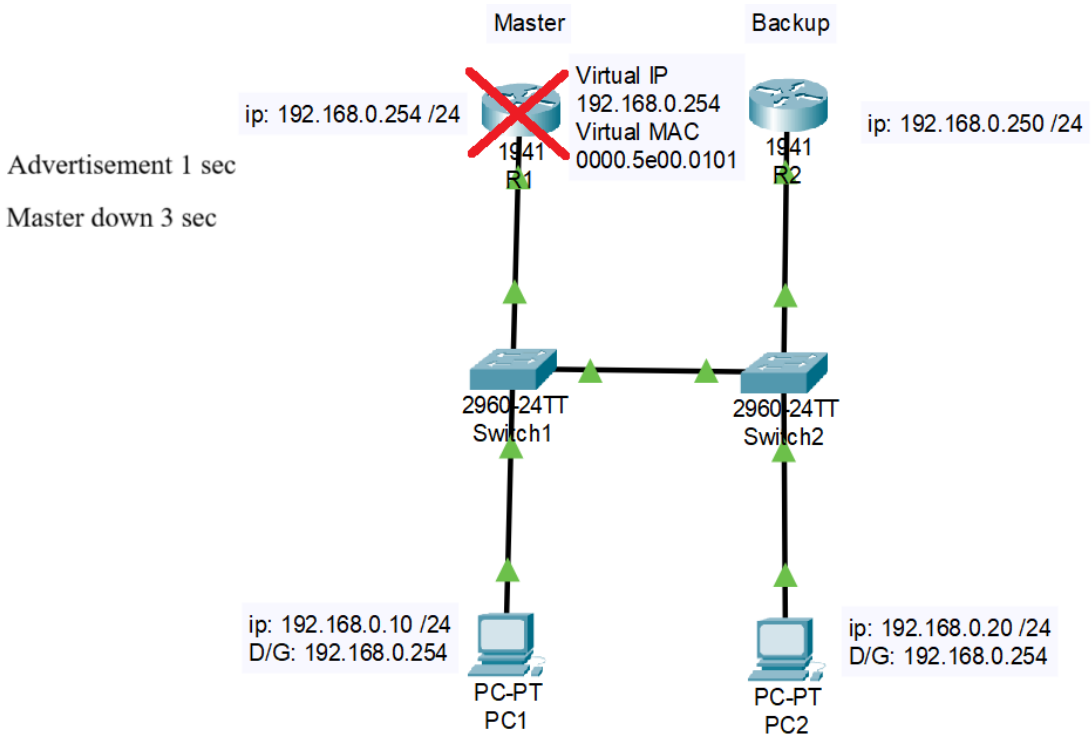


Рисунок 2.8 – Вихід з ладу master

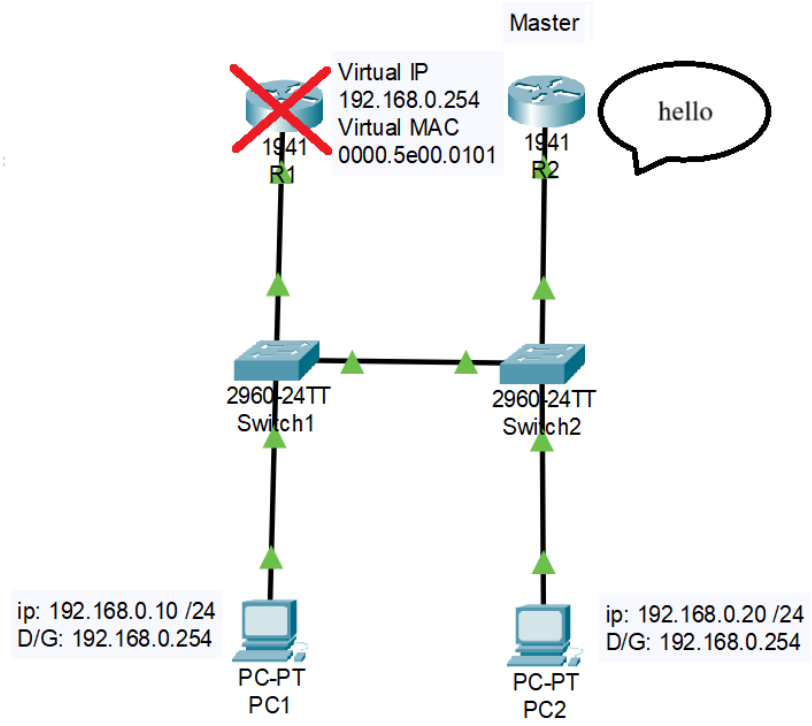


Рисунок 2.9 - Backup стає новим master

На відміну від HSRP, у VRRP коли старий master повертається, він автоматично повертає собі роль master . Практичні рекомендації щодо вибору протоколів резервування першого переходу в залежності від топології, вимог до доступності та типу трафіку наведені в, де розглянуто реальні сценарії впровадження HSRP та VRRP в корпоративних мережах [17].

2.2.3 GLBP (Gateway Load Balancing Protocol)

Після випуску VRRP, Cisco створила новий протокол, який називається GLBP. Оскільки цей протокол був розроблений Cisco, він має чимало спільного з HSRP, але з деякими суттєвими відмінностями. Де найбільш важлива перевага - балансування навантаження між кількома маршрутизаторами.

Маршрутизатори, що працюють з GLBP, надсилають hello-повідомлення кожні три секунди до multicast-адреси 224.0.0.102. Маршрутизатори обирають AVG - Active Virtual Gateway.

Вибір відбувається так само, як у HSRP:

- найвищий пріоритет;

- найвища IP-адреса при рівності пріоритетів.

GLBP використовує одну віртуальну IP-адресу, але кілька віртуальних MAC-адрес - по одній для кожного маршрутизатора (рис. 2.10).

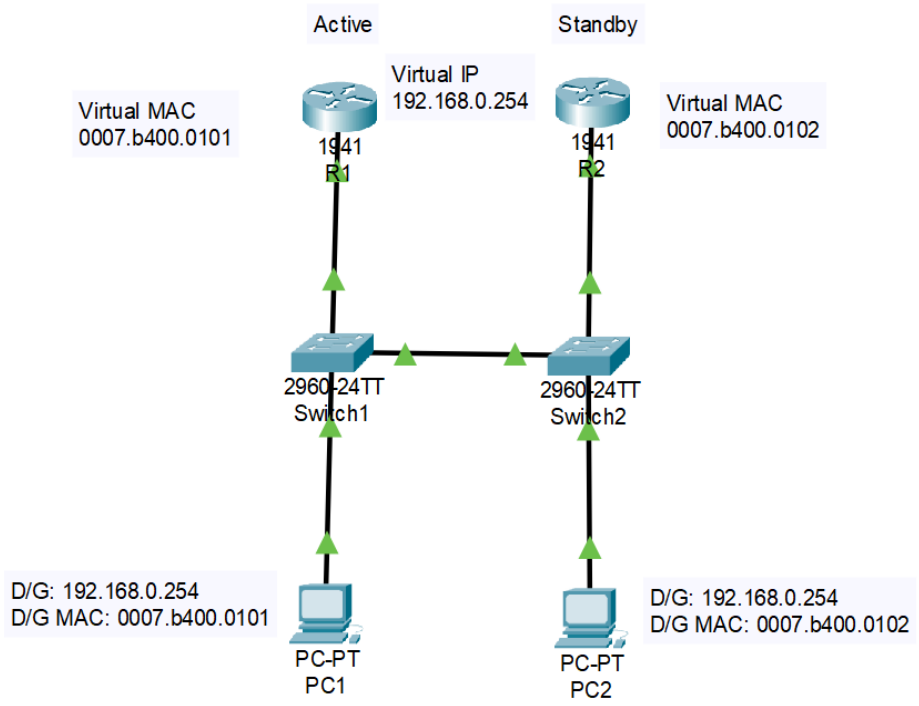


Рисунок 2.10 - Налаштування GLBP

Розглянемо формат віртуальної MAC-адреси:

0007.b400.XXYY,

- де перша частина представляє віртуальну MAC-адресу GLBP; X показують номер групи, а Y позначають те, що називається AVF ID.

Це означає, що кожен маршрутизатор отримує свою віртуальну MAC-адресу і може використовуватися хостами як шлюз. Це дозволяє розподіляти трафік:

- один хост отримує MAC маршрутизатора №1;

- інший хост - MAC маршрутизатора №2;

- вони використовують один і той самий віртуальний IP, але різні MAC, що дає справжнє балансування навантаження.

Якщо активний маршрутизатор виходить з ладу (рис. 2.11), резервний бере на себе керування та всі віртуальні MAC-адреси (рис. 2.12).

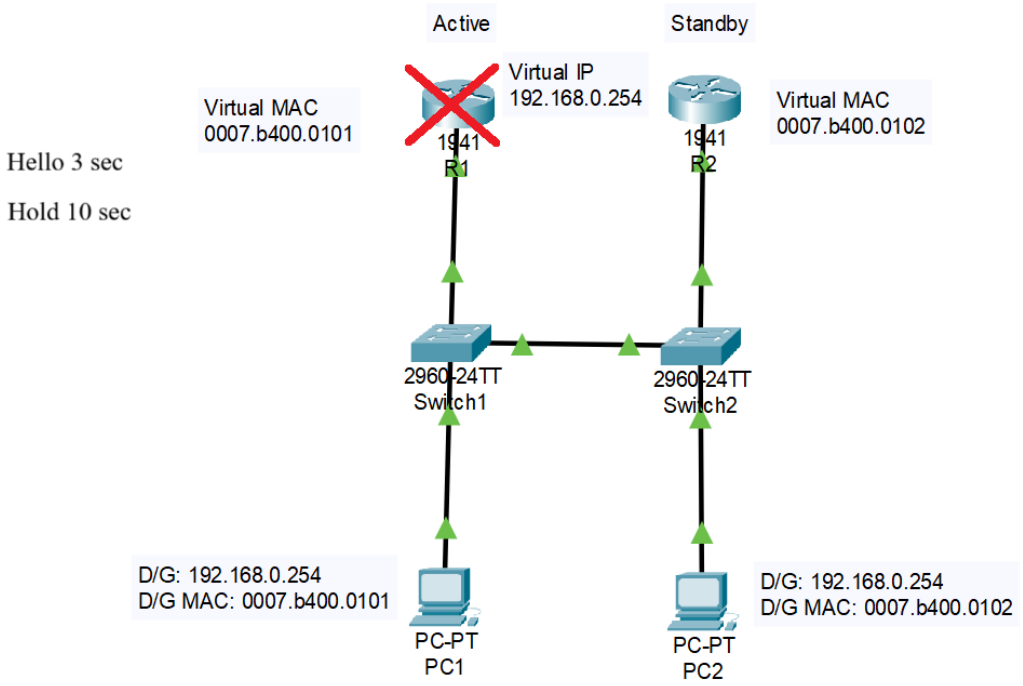


Рисунок 2.11 - Вихід з ладу активного маршрутизатора

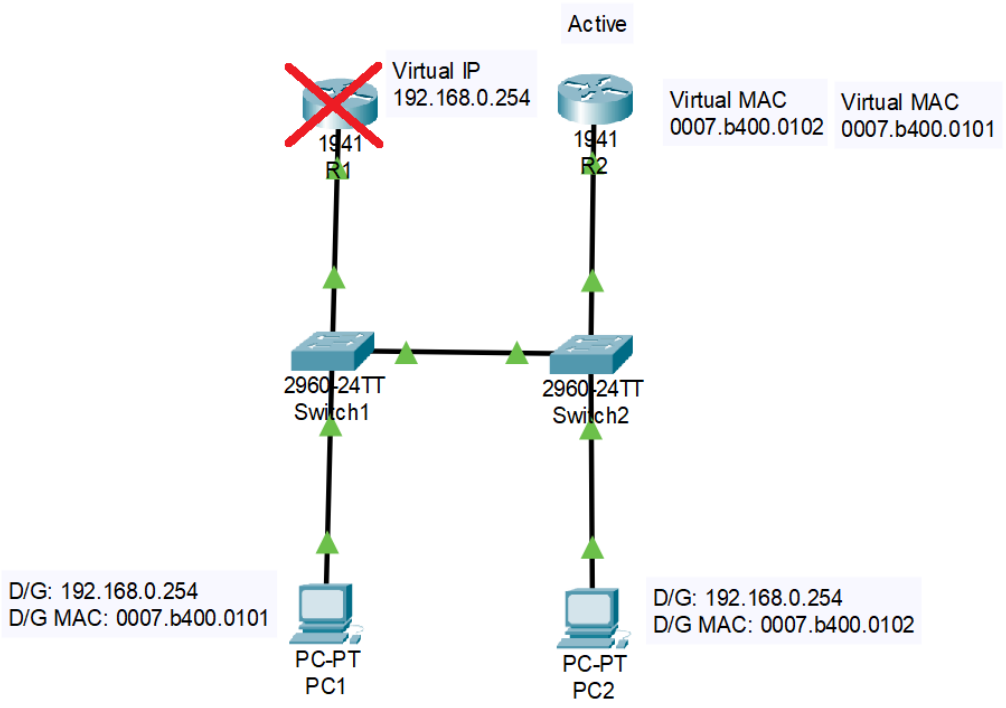


Рисунок 2.12 - Резервний маршрутизатор стає активним

Коли старий маршрутизатор повертається, він знову бере на себе відповідальність за свою власну MAC-адресу. Перемикання між

маршрутизаторами виконується автоматично і безперервно, забезпечуючи як резервування, так і збереження балансу навантаження [18].

2.3 Порівняльний аналіз протоколів резервування

Виходячи з огляду протоколів стає зрозумілим, що вони вирішують спільну задачу - забезпечення безперервного доступу до мережі при відмові шлюзу, проте кожен із них має власні особливості. В межах даного підпункту виконаємо порівняння протоколів, але перед цим розглянемо переваги та недоліки кожного з них. В таблиці 2.2 наведено переваги та недоліки протоколу HSRP.

Таблиця 2.2 - Переваги та недоліки HSRP

Переваги	Недоліки
Забезпечує безперервний доступ до мережі при відмові маршрутизатора	Cisco-пропрієтарний протокол, не сумісний з обладнанням інших виробників
Проста реалізація і налаштування	Обмежена масштабованість у великих мережах
Можливість налаштування пріоритетів для вибору активного маршрутизатора	Витрачає ресурси на підтримку Hello-повідомлень
Сумісність з моделями маршрутизаторів Cisco	Не забезпечує балансування навантаження

В таблиці 2.3 наведено переваги та недоліки протоколу VRRP.

Таблиця 2.3 - Переваги та недоліки VRRP

Переваги	Недоліки
Є відкритим стандартом (RFC 5798), підтримується різними виробниками	Дещо менше функцій порівняно з деякими реалізаціями HSRP
Забезпечує сумісність у мультивендорних середовищах	Не всі виробники реалізують усі розширення стандарту однаково
Просте налаштування і стабільна робота	Може потребувати ручної синхронізації таймінгів у гетерогенних мережах
Забезпечує швидке автоматичне перемикання між маршрутизаторами	Не реалізує балансування навантаження (як і HSRP)

В таблиці 2.4 наведено переваги та недоліки протоколу GLBP.

Таблиця 2.4 - Переваги та недоліки GLBP

Переваги	Недоліки
Поєднує резервування шлюзів і балансування навантаження	Пропрієтарний Cisco-протокол (не підтримується іншими виробниками)
Забезпечує ефективне використання ресурсів кількох маршрутизаторів	Складніша конфігурація порівняно з HSRP та VRRP
Автоматичний перерозподіл трафіку у разі відмови маршрутизатора	Може вимагати більше системних ресурсів
Підтримує кілька алгоритмів балансування навантаження	Обмежена масштабованість у великих мережах

Основні критерії порівняння включають: швидкість перемикання на резервний канал, складність налаштування, сумісність з існуючим обладнанням, маштабованість та підтримка балансування навантаження. В таблиці 2.5 наведено порівняння протоколів резервування, а на основі таблиці створено радарний графік (рис. 2.13).

Таблиця 2.5 - Порівняння протоколів резервування

Критерій порівняння	HSRP	VRRP	GLBP
Сумісність із обладнанням	Висока (переважно Cisco)	Середня (багато виробників)	Середня (Cisco та сумісні)
Підтримка балансування навантаження	Низька (один активний маршрутизатор)	Низька (один Master маршрутизатор)	Висока (кілька активних маршрутизаторів одночасно)
Складність налаштування	Середня	Середня	Середня
Час відновлення після відмови (failover time)	Дуже швидкий	Швидкий	Швидкий
Масштабованість	Висока	Висока	Висока

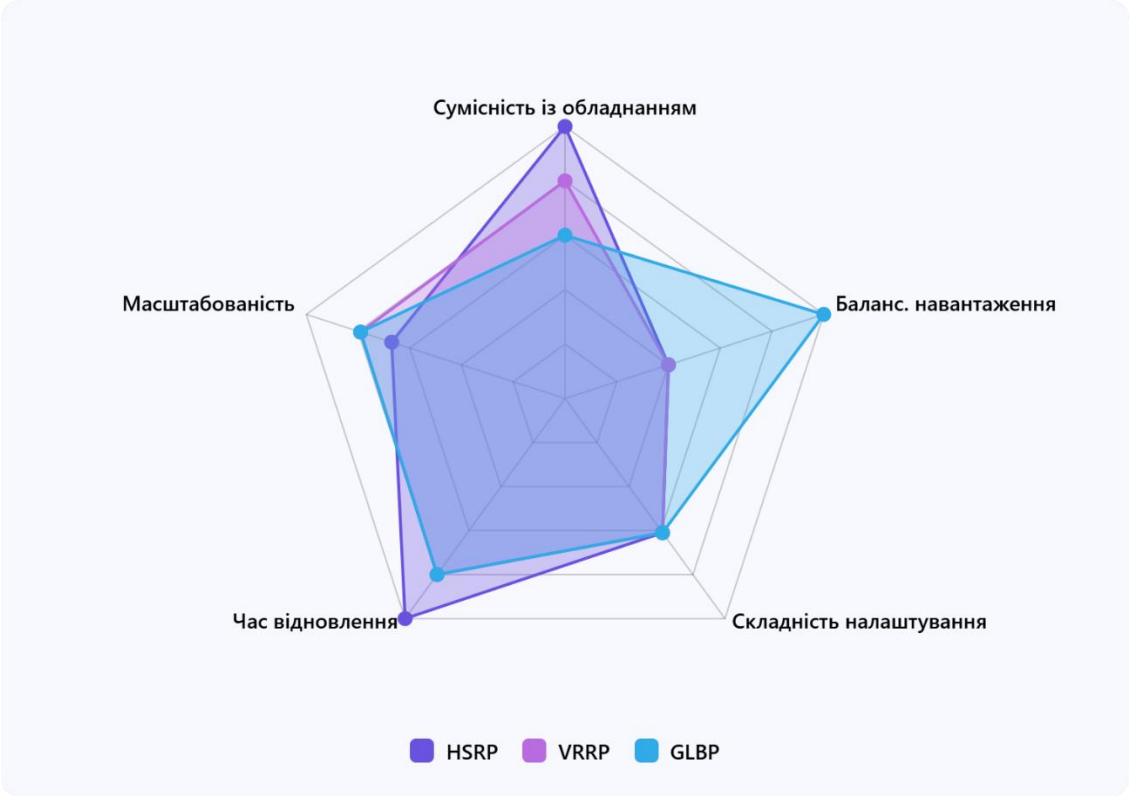


Рисунок 2.13 - Графік порівняння протоколів резервування

На основі виконаного порівняльного аналізу можна зробити висновок, що всі розглянуті протоколи FHRP вирішують спільну задачу - забезпечення безперервного доступу до мережі при відмові шлюзу, проте мають різні сфери доцільного застосування. HSRP є надійним рішенням для мереж, побудованих на обладнанні Cisco, та вирізняється простотою конфігурації й широкою підтримкою в мережевих пристроях цього виробника. VRRP, як відкритий стандарт, забезпечує сумісність у мультивендорних середовищах і часто використовується в змішаних корпоративних інфраструктурах. GLBP поєднує резервування шлюзів і балансування навантаження, що робить його доцільним у високонавантажених Cisco-мережах. З огляду на орієнтацію даної роботи на корпоративні мережі на базі обладнання Cisco, а також на необхідність експериментального дослідження часу перемикання та параметрів відмовостійкості, для практичної реалізації в подальших розділах обрано протокол HSRP, тоді як VRRP і GLBP розглядаються як альтернативні рішення на теоретичному рівні [19].

3 СТВОРЕННЯ ВІДМОВОСТІЙКОЇ МЕРЕЖІ

3.1 Постановка завдання

На основі аналізу технологій та протоколів резервування, наведених у розділі 2, для практичної реалізації системи забезпечення відмовостійкості корпоративної мережі було обрано протокол HSRP. Такий вибір зумовлений його широким використанням у корпоративних інфраструктурах на базі обладнання Cisco, простотою конфігурації та підтримкою механізмів автоматичного перемикання трафіку у разі відмови основного шлюзу.

Практична частина роботи виконується у середовищі Cisco Packet Tracer, яке є програмним інструментом для моделювання мережевих інфраструктур [20]. Використання Packet Tracer обумовлено такими чинниками:

- доступність та простота використання - середовище дозволяє швидко створювати й змінювати мережеві топології без потреби у фізичному обладнанні, що знижує витрати та спрощує проведення експериментів;

- повна підтримка HSRP у моделях маршрутизаторів Cisco - це дає змогу досліджувати поведінку активного та резервного маршрутизаторів у різних сценаріях відмови;

- можливість імітації корпоративної інфраструктури - за допомогою комутаторів, VLAN та маршрутизаторів можна відтворити типову структуру корпоративної мережі та дослідити її відмовостійкість;

- наявність засобів моніторингу - Packet Tracer надає інструменти для перегляду стану інтерфейсів, таблиць маршрутизації та процесів HSRP у режимі реального часу, що спрощує аналіз результатів.

У межах даного розділу ставиться завдання спроєктувати та реалізувати відмовостійку мережу, в якій забезпечується автоматичне перемикання між двома маршрутизаторами-шлюзами без втрати доступу користувачів до мережі.

3.2 Проєктування схеми відмовостійкої мережі

Для моделювання мережі використано таке обладнання Cisco Packet Tracer:

- маршрутизатори Cisco 1941- для конфігурації HSRP та забезпечення шлюзу за замовчуванням для користувацьких VLAN;

- комутатори Cisco 2960 - для організації VLAN та підключення кінцевих пристроїв;

- персональні комп'ютери (PC) - для перевірки доступності мережевих ресурсів через віртуальний шлюз HSRP.

Логічна схема мережі наведена на рисунку 3.1.

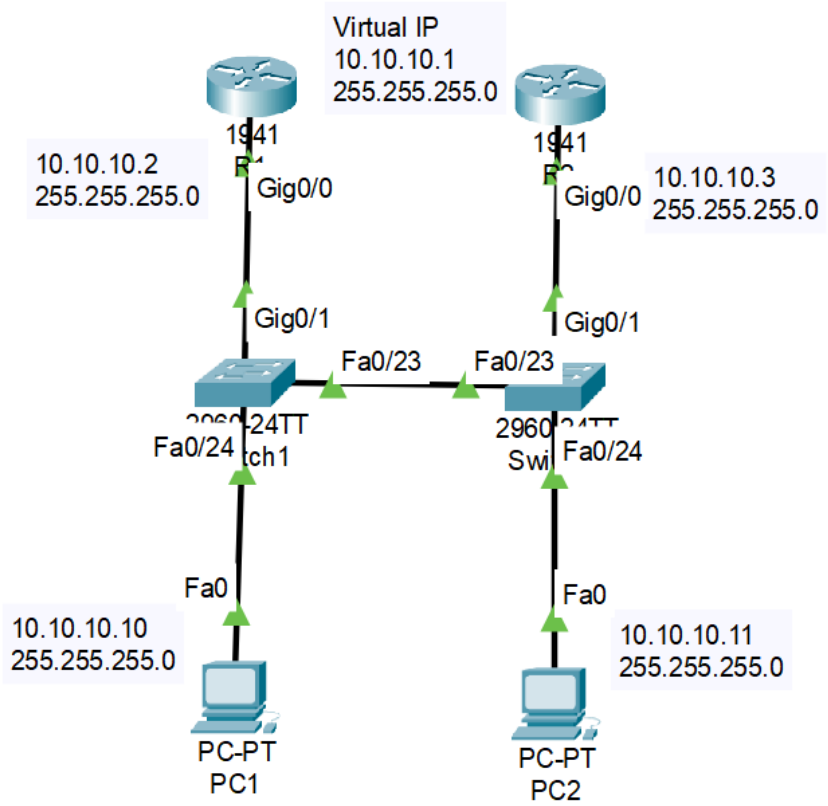


Рисунок 3.1 - Логічна схема мережі

Логічна структура створеної мережі відображає принципи побудови відмовостійкої інфраструктури, у якій ключовим механізмом забезпечення

безперервності роботи є протокол HSRP. В мережі виділено окремий VLAN 10, призначений для користувацьких пристроїв. Використання VLAN дозволяє ізолювати трафік кінцевих станцій і забезпечити коректну роботу HSRP у межах спільного широкомовного домену.

Кожен маршрутизатор має власну фізичну IP-адресу в межах VLAN 10, а також спільну віртуальну IP-адресу, яку використовують кінцеві пристрої як шлюз за замовчуванням:

- R1 - основний маршрутизатор, що в нормальному режимі виконує роль Active Router;

- R2 - резервний маршрутизатор, що перебуває у стані Standby Router і готовий автоматично перебрати функції активного у разі відмови R1;

- Virtual IP - віртуальна IP-адреса HSRP, яка налаштовується як стандартний шлюз на всіх користувацьких ПК.

У таблиці 3.1 наведено схему IP-адресації для VLAN 10.

Таблиця 3.1 - Схема адресації IP

Пристрій / Інтерфейс	IP-адреса	Маска підмережі	Примітка
R1 - g0/0	10.10.10.2	255.255.255.0	Основний маршрутизатор (Active)
R2 - g0/0	10.10.10.3	255.255.255.0	Резервний маршрутизатор (Standby)
HSRP Virtual IP	10.10.10.1	255.255.255.0	Віртуальний шлюз VLAN 10
PC1	10.10.10.10	255.255.255.0	Користувацька станція
PC2	10.10.10.11	255.255.255.0	Користувацька станція
Gateway (для ПК)	10.10.10.1	-	Проксі-адреса HSRP

Фізичні з’єднання між пристроями наведені в таблиці 3.2.

Таблиця 3.2 - Фізичне з’єднання пристроїв

Пристрій 1	Порт	Пристрій 2	Порт	Тип з’єднання
PC1	FastEthernet0	SW1	FastEthernet0/24	Прямий (Straight-through)
PC2	FastEthernet0	SW2	FastEthernet0/24	Прямий (Straight-through)
SW1	FastEthernet 0/23	SW2	FastEthernet0/23	Прямий (Straight-through)
R1	GigabitEthernet0/0	SW1	GigabitEthernet0/1	Прямий (Straight-through)
R2	GigabitEthernet0/0	SW2	GigabitEthernet0/1	Прямий (Straight-through)

Така схема дозволяє змоделювати ситуацію, коли обидва маршрутизатори підключені до користувацького сегмента через окремі комутатори, але при цьому залишаються в одному широкомовному домені VLAN 10. Це відповідає типовому фрагменту корпоративної мережі з резервуванням шлюзів.

3.3 Налаштування HSRP

Для забезпечення відмовостійкості мережі виконано конфігурацію протоколу HSRP на маршрутизаторах R1 та R2, а також налаштовано комутатори SW1 і SW2 та користувацькі станції PC1 і PC2.

Конфігурація включає такі кроки:

- створення VLAN 10 на комутаторах та призначення портів у режим access;
- налаштування IP-адрес інтерфейсів G0/0 маршрутизаторів R1 і R2;
- створення HSRP-групи з віртуальною IP-адресою 10.10.10.1;
- налаштування пріоритетів HSRP (R1 - вищий пріоритет, R2 - нижчий);
- увімкнення механізму preempt для коректного повернення активної ролі після відновлення маршрутизатора;
- налаштування IP-адрес та шлюзу за замовчуванням на користувацьких ПК.

Лістинг 3.1 - Налаштування SW1

```
Switch1(config)#vlan 10
Switch1(config)#Exit
Switch1(config)#interface range fa0/1 – 24
Switch1(config-if-range)#switchport mode access
Switch1(config-if-range)#switchport access vlan 10
Switch1(config-if-range)#exit
Switch1(config)#interface g0/1
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 10
Switch1(config-if)#exit
```

Лістинг 3.2 - Налаштування SW2

```
Switch2(config)#vlan 10
Switch2(config)#Exit
Switch2(config)#interface range fa0/1 – 24
Switch2(config-if-range)#switchport mode access
Switch2(config-if-range)#switchport access vlan 10
Switch2(config-if-range)#exit
Switch2(config)#interface g0/1
Switch2(config-if)#switchport mode access
Switch2(config-if)#switchport access vlan 10
Switch2(config-if)#exit
```

Лістинг 3.3 - Налаштування R1

```
R1(config)# interface g0/0
R1(config-if)#ip address 10.10.10.2 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)#standby 10 ip 10.10.10.1
R1(config-if)#standby 10 priority 120
R1(config-if)#standby 10 preempt
```

Лістинг 3.4 - Налаштування R2

```
R2(config)# interface g0/0
R2(config-if)#ip address 10.10.10.3 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)#standby 10 ip 10.10.10.1
R2(config-if)#standby 10 priority 100
R2(config-if)#standby 10 preempt
```

Налаштування користувацьких ПК (рис. 3.2 та 3.3) включає призначення IP-адрес із підмережі 10.10.10.0/24 та вказання шлюзу за замовчуванням 10.10.10.1 (віртуальна адреса HSRP).

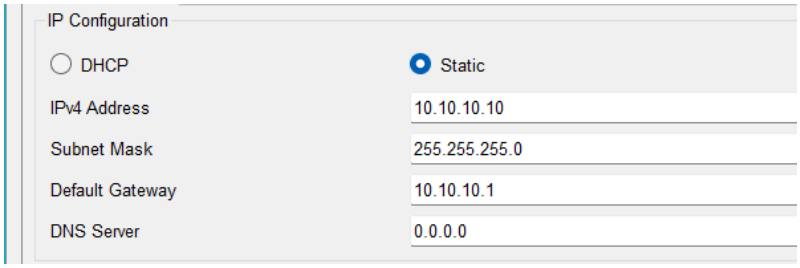


Рисунок 3.2 - Налаштування PC1

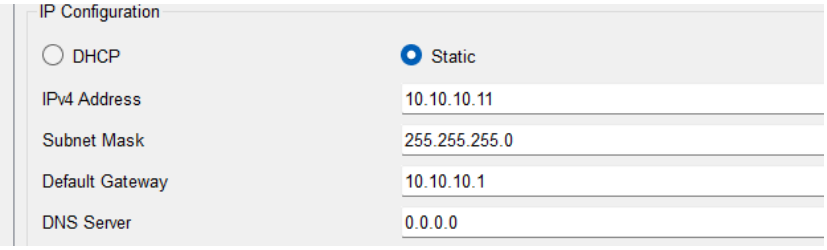


Рисунок 3.3 - Налаштування PC2

Для більш повного ознайомлення та можливості розширеної конфігурації наведено таблицю всіх основних команд HSRP (табл. 3.3), які застосовуються для управління протоколом, контролю стану та оптимізації роботи мережі.

Таблиця 3.3 - HSRP-команди

Команда	Призначення
standby <group> ip <virtual-ip>	Призначає віртуальну IP-адресу для HSRP-групи
standby <group> priority <value>	Встановлює пріоритет маршрутизатора у групі
standby <group> preempt	Дозволяє маршрутизатору з вищим пріоритетом стати Active
standby <group> timers <hello> <hold>	Встановлює інтервал відправки HSRP-повідомлень та час очікування
standby <group> authentication <string>	Встановлює пароль для обміну HSRP-повідомленнями
standby <group> track <interface> [priority-decrement]	Відстежує стан інтерфейсу або маршруту і змінює пріоритет
standby <group> preempt delay minimum <seconds>	Затримка активації preempt для плавного переходу
show standby	Перевірка стану HSRP, ролі Active/Standby
show standby brief	Коротка інформація про всі HSRP-групи на маршрутизаторі
shutdown / no shutdown	Симуляція відмови інтерфейсу або відновлення

3.4 Перевірка працездатності мережі

Після завершення налаштування HSRP було проведено початкове тестування працездатності мережі. Метою цього етапу є перевірка коректності конфігурації, доступності віртуального шлюзу та правильного розподілу ролей між маршрутизаторами R1 і R2 у нормальному режимі роботи.

Спочатку була проведена перевірка доступності маршрутизаторів і віртуального шлюзу з користувацької станції (наприклад, з PC1):

ping 10.10.10.2

ping 10.10.10.3

ping 10.10.10.1

Успішне проходження ICMP-запитів (рис. 3.4, 3.5) свідчить про коректну IP-адресацію в межах VLAN 10, доступність обох маршрутизаторів та працездатність віртуального шлюзу HSRP.

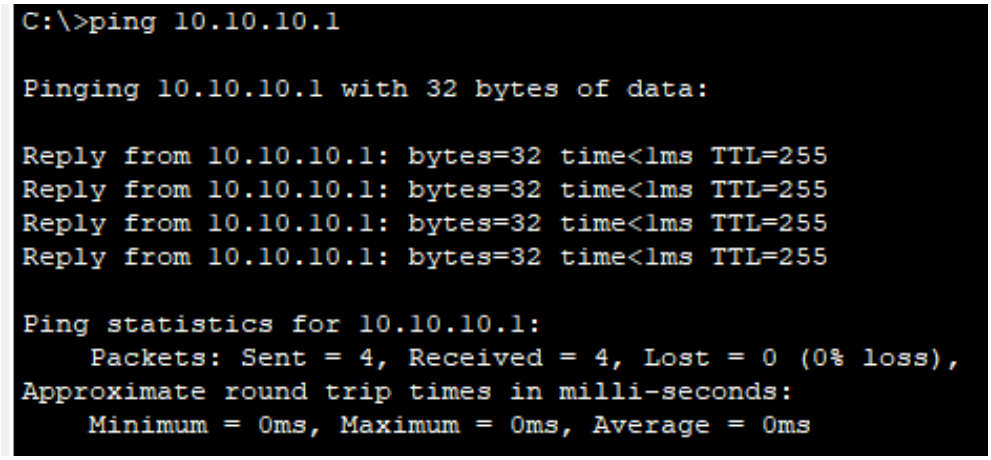


Рисунок 3.4 - Перевірка роботи віртуального IP

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data:

Reply from 10.10.10.2: bytes=32 time<1ms TTL=255
Reply from 10.10.10.2: bytes=32 time<1ms TTL=255
Reply from 10.10.10.2: bytes=32 time<1ms TTL=255
Reply from 10.10.10.2: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.10.10.3

Pinging 10.10.10.3 with 32 bytes of data:

Reply from 10.10.10.3: bytes=32 time<1ms TTL=255
Reply from 10.10.10.3: bytes=32 time<1ms TTL=255
Reply from 10.10.10.3: bytes=32 time<1ms TTL=255
Reply from 10.10.10.3: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 3.5 - Перевірка базової доступності маршрутизаторів

На рисунку 3.6 показано, що для IP-адреси 10.10.10.1 клієнт отримує віртуальну MAC-адресу HSRP, що підтверджує коректну роботу віртуального шлюзу та прозорість механізму для користувача.

```
C:\>arp -a
  Internet Address      Physical Address      Type
  10.10.10.1            0000.0c07.ac0a        dynamic
  10.10.10.2            0001.420c.2401        dynamic
  10.10.10.3            0010.118e.a501        dynamic
```

Рисунок 3.6 - Перевірка MAC-адреси HSRP у таблиці ARP

Виконаємо перевірку стану HSRP та переглянемо коротку інформацію про всі HSRP-групи на маршрутизаторах R1 та R2. На рисунках 3.7 і 3.8 наведено приклади виводу команд:

show standby

show standby brief

для R1 та R2. З них видно, що R1 виконує роль Active, R2 - Standby, обидва маршрутизатори належать до однієї HSRP-групи з віртуальною IP-адресою 10.10.10.1, а обмін Hello-повідомленнями відбувається штатно.

```
R1#show standby
GigabitEthernet0/0 - Group 10
  State is Active
    5 state changes, last state change 00:00:27
  Virtual IP address is 10.10.10.1
  Active virtual MAC address is 0000.0C07.AC0A
    Local virtual MAC address is 0000.0C07.AC0A (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.389 secs
  Preemption enabled
  Active router is local
  Standby router is 10.10.10.3
  Priority 120 (configured 120)
  Group name is hsrp-Gig0/0-10 (default)
R1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0      10   120 P Active   local           10.10.10.3      10.10.10.1
R1#
```

Рисунок 3.7 - Перевірка HSRP на R1

```
R2#show standby
GigabitEthernet0/0 - Group 10
  State is Standby
    6 state changes, last state change 00:00:39
  Virtual IP address is 10.10.10.1
  Active virtual MAC address is 0000.0C07.AC0A
    Local virtual MAC address is 0000.0C07.AC0A (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.846 secs
  Preemption enabled
  Active router is 10.10.10.2
  Standby router is local
  Priority 100 (default 100)
  Group name is hsrp-Gig0/0-10 (default)
R2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0      10   100 P Standby  10.10.10.2      local           10.10.10.1
R2#
```

Рисунок 3.8 - Перевірка HSRP на R2

Проведені перевірки підтвердили коректність базової конфігурації та працездатність відмовостійкої схеми з використанням HSRP. У четвертому розділі

на основі цієї мережі буде виконано детальне експериментальне дослідження параметрів failover і часу відновлення, а також порівняння роботи мережі в різних режимах.

3.5 Практичні рекомендації щодо налаштування HSRP в корпоративних мережах Cisco

Результати аналітичних досліджень та моделювання в середовищі Cisco Packet Tracer показали, що протокол HSRP забезпечує необхідний рівень відмовостійкості навіть у відносно простій топології. Однак під час впровадження цього протоколу в реальних корпоративних мережах доцільно враховувати низку практичних аспектів, які впливають на швидкість перемикання, стабільність роботи та безпеку всієї інфраструктури. У даному підпункті наведено рекомендації щодо проєктування й налаштування HSRP, базовані на результатах експериментів, аналізі документації Cisco та типовому досвіді застосування протоколів резервування.

3.5.1 Вибір схеми розподілу ролей Active/Standby

У найпростішому випадку один маршрутизатор виконує роль Active, а другий - Standby для всіх VLAN/підмереж. Такий підхід є достатнім для невеликих мереж, але в більших інфраструктурах він призводить до нерівномірного використання ресурсів: активний пристрій несе основне навантаження, тоді як резервний більшість часу простоює.

Тому на практиці часто застосовують схему розподілу ролей (active/standby per VLAN), коли:

- в одних підмережах маршрутизатор R1 є Active, а R2 - Standby;
- в інших, навпаки, R2 призначається Active, а R1 - Standby.

Такий підхід дозволяє:

- рівномірніше розподілити трафік між маршрутизаторами;

- зменшити ризик перевантаження одного вузла;

- підвищити загальну ефективність використання обладнання.

Навіть у разі відмови одного з маршрутизаторів HSRP забезпечить автоматичне перемикання всіх груп на працездатний пристрій, зберігаючи безперервність роботи мережі.

3.5.2 Налаштування таймерів та механізмів відстеження стану

У теоретичній частині та під час експериментів було показано, що значення таймерів hello/hold безпосередньо впливають на час автоматичного перемикання (failover). Стандартні параметри standby timers 3 10 забезпечують прийнятний баланс між часом реакції та обсягом службового трафіку, однак для сервісів із жорсткими вимогами до доступності доцільно використовувати зменшені значення, наприклад standby timers 1 3.

При цьому важливо дотримуватися таких рекомендацій:

- однакові значення таймерів мають бути налаштовані на всіх маршрутизаторах, що входять до HSRP-групи;

- не слід встановлювати занадто малі інтервали (менше 1 с), якщо мережа містить повільні або перевантажені ділянки - це може призвести до хибних спрацьовувань і «флапання» ролей Active/Standby;

- бажано узгоджувати таймери HSRP з параметрами протоколів динамічної маршрутизації (якщо вони використовуються), щоб уникнути ситуацій, коли шлюз уже перемкнувся, а маршрути ще не оновилися.

Окремий напрямок оптимізації - застосування механізму track. Типовий приклад:

```
interface g0/0
standby 10 ip 10.10.10.1
standby 10 priority 120
standby 10 preempt
standby 10 track g0/1 20
```

У цьому випадку, якщо інтерфейс G0/1 (наприклад, uplink до провайдера або ядра мережі) переходить у стан down, пріоритет HSRP зменшується на 20. Це

дозволяє швидше передати роль Active тому маршрутизатору, який зберіг доступ до зовнішніх ресурсів, навіть якщо локальний інтерфейс VLAN 10 формально залишається працездатним. Таким чином, користувачі не «застрягають» за шлюзом, який не має робочого виходу з мережі.

3.5.3 Забезпечення безпеки протоколу HSRP

За замовчуванням HSRP не використовує захищену автентифікацію, і будь-який пристрій у спільному широкомовному сегменті, що підтримує цей протокол, потенційно може приєднатися до групи або впливати на її роботу. У невеликих лабораторних топологіях це не є критичним, але в реальних корпоративних мережах такий підхід створює ризики:

- можливість спуфінгу HSRP-повідомлень і захоплення ролі Active зловмисником;

- порушення стабільності роботи групи через некоректно налаштовані пристрої.

Для зниження цих ризиків рекомендується:

- використовувати автентифікацію HSRP: standby 10 authentication MD5 key-string SECRET_KEY; або, у простішому варіанті: standby 10 authentication cisco. Це дозволяє відхиляти HSRP-пакети від маршрутизаторів, які не мають коректного ключа;

- обмежувати широкомовний домен VLAN лише тими комутаторами й інтерфейсами, де справді необхідна участь у HSRP;

- застосовувати додаткові засоби захисту другого рівня (Port Security, DHCP Snooping, Dynamic ARP Inspection), щоб зменшити ймовірність ARP- та MAC-спуфінгу в сегменті користувачів.

3.5.4 Взаємодія HSRP з іншими протоколами та сервісами

У корпоративних мережах HSRP рідко використовується ізольовано. Зазвичай він працює спільно з протоколами:

- STP/RSTP - забезпечують відсутність петель на рівні 2;

- VLAN - розділяють трафік між різними сегментами;

- OSPF/EIGRP/BGP - маршрутизація між підмережами та зовнішніми доменами;

- механізми QoS та фаєрволами.

Під час проєктування відмовостійкої мережі важливо:

- уникати ситуації, коли активний шлюз для VLAN фізично підключений до комутатора, що має заблокований STP-порт. У такому разі навіть за коректної роботи HSRP трафік від користувачів може не досягати маршрутизатора через блокування лінка на другому рівні;

- забезпечити узгодженість пріоритетів STP і HSRP. Практично часто реалізують правило: root-комутатор STP знаходиться в тому ж сегменті, де підключено Active-шлюз. Це зменшує ймовірність асиметричних маршрутів і «обходу» трафіку по неоптимальних шляхах;

- враховувати, що зміна ролі Active впливає на напрямок трафіку для всіх сервісів, включно з політиками фільтрації, NAT та QoS. Тому списки доступу (ACL), правила NAT і політики маркування трафіку мають бути симетрично налаштовані на обох маршрутизаторах, які беруть участь у HSRP.

3.5.5 Типові помилки конфігурації та рекомендації щодо тестування

Під час налаштування HSRP адміністратори часто припускаються типових помилок, які не заважають мережі працювати в нормальному режимі, але проявляються саме при відмовах:

- неконсистентна IP-адресація: різні маски на маршрутизаторах та клієнтах, або віртуальна адреса HSRP поза межами підмережі;

- різні номери групи на маршрутизаторах (наприклад, standby 1 на R1 та standby 10 на R2), через що пристрої фактично не утворюють спільної HSRP-групи;

- відсутність або некоректні параметри preempt, у результаті чого після відновлення первинного маршрутизатора роль Active не повертається, що може суперечити запланованій схемі розподілу навантаження;

- неправильна конфігурація track (відстежується не той інтерфейс, що справді впливає на доступність сервісів).

Щоб виявити такі проблеми до моменту введення мережі в експлуатацію, рекомендується:

1) Створити набір тестових сценаріїв, аналогічних до тих, що реалізовані в розділі 4: відмова активного маршрутизатора, відновлення його роботи, відмова окремих інтерфейсів.

2) Для кожного сценарію фіксувати:

- доступність віртуального шлюзу з клієнтських ПК;
- час відсутності відповідей на ICMP-запити;
- зміни в таблицях ARP і MAC-таблицях комутаторів;
- стан HSRP-груп за допомогою команд show standby та show standby brief.

3) Аналізувати результати не лише з точки зору часу перемикання, але й з погляду прозорості процесу для користувача: чи потребує сценарій ручного втручання, чи зберігаються активні сесії, чи не виникає нестандартних затримок.

Окрему увагу слід приділяти документуванню конфігурації. Наявність зрозумілих схем, таблиць адресації та опису HSRP-груп значно спрощує подальший супровід мережі, пошук несправностей і планування модернізації.

3.6 Висновки до розділу 3

У третьому розділі було спроєктовано та реалізовано тестову відмовостійку корпоративну мережу, яка слугує базою для подальших експериментальних досліджень. На основі аналізу протоколів резервування першого переходу обрано протокол HSRP, що зумовлено його поширеним використанням в інфраструктурах на базі обладнання Cisco, підтримкою механізмів автоматичного перемикання шлюзу та відносною простотою конфігурації.

Для практичної реалізації системи обрано середовище моделювання Cisco Packet Tracer, яке дає можливість відтворити типову структуру корпоративної мережі, налаштувати протоколи резервування й відстежувати їхню роботу в режимі

реального часу. Було розроблено логічну та фізичну схеми мережі з виділеним VLAN 10 для користувацьких пристроїв, налаштовано IP-адресацію, віртуальний шлюз HSRP та взаємозв’язки між маршрутизаторами, комутаторами й кінцевими станціями.

У процесі налаштування виконано конфігурацію HSRP на маршрутизаторах R1 та R2, створено HSRP-групу з віртуальною IP-адресою, визначено пріоритети й увімкнено механізм preempt для коректного повернення активної ролі. Початкові тести (ping до фізичних і віртуального адрес, перевірка ARP-таблиць, аналіз виводу команд show standby та show standby brief) підтвердили правильність схеми адресації, коректний розподіл ролей Active/Standby та прозорість роботи віртуального шлюзу для користувачів.

Окремо сформульовано практичні рекомендації щодо застосування HSRP у корпоративних мережах: вибір схеми розподілу ролей Active/Standby між VLAN, налаштування таймерів hello/hold з урахуванням вимог до часу перемикання, використання механізму track для відстеження стану критичних інтерфейсів, застосування автентифікації HSRP та узгодження роботи протоколу з STP, VLAN і динамічною маршрутизацією. Також наведено типові помилки конфігурації та підходи до їх виявлення під час тестування.

Таким чином, у розділі 3 створено повноцінну модель відмовостійкої корпоративної мережі з використанням HSRP, перевірено її базову працездатність та визначено ключові параметри, що впливають на надійність і швидкість перемикання. Одержані результати та розроблена тестова інфраструктура стали основою для подальших експериментальних досліджень часових характеристик failover та preemption, викладених у розділі 4.

4 ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ПАРАМЕТРІВ ВІДМОВОСТІЙКОЇ МЕРЕЖІ

4.1 Мета та методика експериментальних досліджень

У третьому розділі було спроєктовано та налаштовано відмовостійку корпоративну мережу з використанням протоколу резервування HSRP, а також перевірено її базову працездатність: усі вузли коректно взаємодіють, пінгування проходять успішно, доступ до мережевих ресурсів забезпечується. Однак факт працездатності мережі ще не дає кількісної оцінки її відмовостійкості та якості функціонування в аварійних режимах.

Метою даного розділу є експериментальне дослідження параметрів роботи відмовостійкої мережі, побудованої у розділі 3, а також порівняння ефективності різних варіантів конфігурації протоколів резервування та базового (нерезервованого) рішення. Особливу увагу приділено часовим характеристикам перемикання, втратам пакетів і доступності мережевих сервісів під час відмови та відновлення вузлів.

У межах дослідження розв’язуються такі основні задачі:

- визначення часу перемикання (failover time) при відмові активного маршрутизатора;

- вимірювання часу відновлення роботи мережі при поверненні маршрутизатора в експлуатацію;

- оцінка кількості втрачених пакетів і зміни затримки (RTT) під час аварійних подій;

- порівняння отриманих результатів для різних конфігурацій мережі.

Експериментальні дослідження проводяться в середовищі Cisco Packet Tracer на основі тестової топології, наведеної в розділі 3. Як основний інструмент контролю доступності використовується безперервне пінгування (ICMP echo) критичних вузлів (віртуального шлюзу, серверів), а для детального аналізу подій -

Simulation Mode, що дозволяє відстежувати часові мітки відправлення та отримання пакетів, зміни станів протоколу HSRP та інтерфейсів маршрутизаторів.

Для підвищення достовірності результатів кожен сценарій випробувань (відмова активного маршрутизатора, його відновлення, зміна конфігурації таймерів) виконується серією з кількох прогонів. За підсумками серії розраховуються:

- середній час перемикання та відновлення;
- середня кількість втрачених ICMP-пакетів;
- характерні значення затримки до та після аварійної події.

Отримані експериментальні дані систематизуються у вигляді таблиць та графіків, що дозволяє виконати порівняльний аналіз різних конфігурацій та зробити висновки щодо доцільності використання тих чи інших параметрів протоколів резервування у корпоративних мережах з підвищеними вимогами до відмовостійкості.

4.2 Дослідження базової мережі без протоколів резервування

Першим етапом експериментальних досліджень є аналіз роботи мережі без використання протоколів резервування шлюзів. Такий варіант розглядається як базовий, оскільки він відповідає типовій конфігурації корпоративної мережі, в якій існує єдиний маршрутизатор-шлюз для доступу до зовнішніх ресурсів, а відмова цього вузла призводить до повної втрати зв’язку.

У тестовій топології, розробленій у розділі 3, для базового сценарію були виконані такі зміни:

- з конфігурації маршрутизаторів вилучено налаштування протоколу HSRP;
- для хостів локальної мережі як шлюз за замовчуванням встановлено IP-адресу єдиного активного маршрутизатора;

- резервний маршрутизатор у цьому сценарії не використовується як шлюз і не бере участі в обробці трафіку користувачів.

У базовій конфігурації (рис. 4.1) робочі станції PC1 та PC2 використовують єдиний шлюз - маршрутизатор R1 з адресою 10.10.10.1. Протоколи резервування першого переходу не використовуються, віртуальна IP-адреса відсутня, тому відмова маршрутизатора R1 призводить до повної втрати доступу до зовнішніх ресурсів.

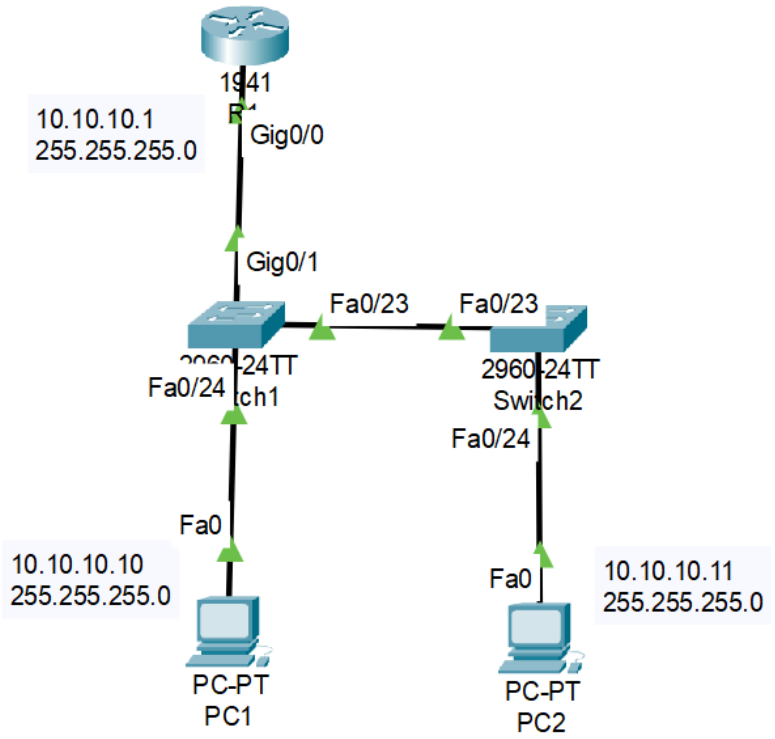


Рисунок 4.1 - Схема базової мережі без протоколів резервування

4.2.1 Сценарій моделювання відмови

Для оцінки впливу відмови єдиного шлюзу на роботу мережі застосовано такий сценарій:

а) У режимі RealTime перевіряється коректність роботи мережі:

1) виконується пінгування з робочих станцій до шлюзу;

2) фіксується, що втрат пакетів немає, затримка стабільна.

б) Далі мережа переводиться в режим Simulation, активується безперервне пінгування маршрутизатора.

в) На моменті часу $t_{\text{відм}}$ виконується штучна відмова маршрутизатора-шлюзу:

1) переведення основного інтерфейсу в стан shutdown.

г) У Simulation Mode фіксується:

1) момент часу, коли перестають надходити відповіді на ICMP-запити;

2) загальна тривалість періоду, протягом якого мережа недоступна для користувачів;

3) кількість втрачених ICMP-пакетів.

д) Після певного часу маршрутизатор знову вмикається, однак без зміни конфігурації хостів (шлюз залишається тим самим). Вимірюється час відновлення зв’язку після повернення маршрутизатора до роботи.

Кожен експеримент проводиться не менше ніж у п’яти прогонах, що дозволяє врахувати можливі варіації часу реакції та стабільності роботи симулятора.

4.2.2 Результати випробувань базової мережі

За підсумками серії експериментів для базової (нерезервованої) конфігурації фіксуються такі показники:

- час повної втрати доступності мережі після відмови маршрутизатора-шлюзу;

- кількість втрачених пакетів під час простою;

- характер зміни затримки (RTT) до моменту відмови та після відновлення;

- необхідність ручного втручання адміністратора для відновлення працездатності (зміна шлюзу, перезапуск пристрою тощо).

Результати подані у вигляді узагальненої таблиці (табл. 4.1):

Таблиця 4.1 - Параметри роботи базової мережі без протоколів резервування

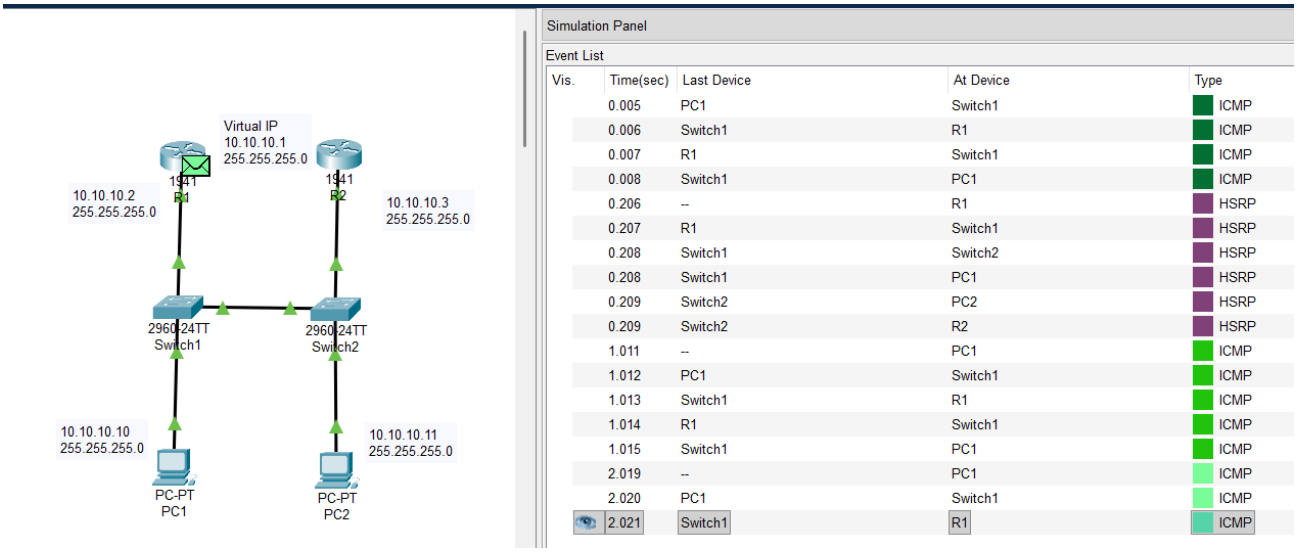
№ прогону	Час відмови шлюзу, s	Час відновлення зв’язку, s	Тривалість недоступності, s	Кількість втрачених ICMP-пакетів
1	10	70	60	60
2	10	71	61	61
3	10	69	59	59
4	10	72	62	62
5	10	70	60	60
Середнє	–	–	60,4	60,4

Аналіз отриманих даних показує, що у разі відмови єдиного маршрутизатора-шлюзу мережа стає повністю недоступною для користувачів, а відновлення зв’язку можливе лише після повернення пристрою в робочий стан або внесення змін до мережевих налаштувань. Це підтверджує критичну залежність базової конфігурації від одного мережевого вузла та обґрунтовує необхідність впровадження протоколів резервування, розглянутих у наступних підрозділах.

4.3 Дослідження параметрів мережі з використанням HSRP

На наступному етапі було досліджено роботу відмовостійкої мережі, у якій на маршрутизаторах R1 та R2 налаштовано протокол резервування першого переходу HSRP з параметрами за замовчуванням (standby 10 timers 3 10). Топологія мережі відповідає схемі, наведеної у розділі 3, а віртуальна IP-адреса використовується як єдиний шлюз для робочих станцій.

Експериментальні випробування проводилися в режимі симуляції Cisco Packet Tracer (рис. 4.2). Для контролю доступності мережі з робочої станції здійснювалося безперервне пінгування віртуального шлюзу (рис. 4.3), а у вікні Simulation Mode фіксувалися часові мітки ICMP-пакетів та службових повідомлень HSRP. На основі зібраних даних було сформовано вибірки для аналізу часу автоматичного перемикання (failover) та часу повернення активної ролі маршрутизатора R1 (preemption).



Vis.	Time(sec)	Last Device	At Device	Type
	0.005	PC1	Switch1	ICMP
	0.006	Switch1	R1	ICMP
	0.007	R1	Switch1	ICMP
	0.008	Switch1	PC1	ICMP
	0.206	--	R1	HSRP
	0.207	R1	Switch1	HSRP
	0.208	Switch1	Switch2	HSRP
	0.208	Switch1	PC1	HSRP
	0.209	Switch2	PC2	HSRP
	0.209	Switch2	R2	HSRP
	1.011	--	PC1	ICMP
	1.012	PC1	Switch1	ICMP
	1.013	Switch1	R1	ICMP
	1.014	R1	Switch1	ICMP
	1.015	Switch1	PC1	ICMP
	2.019	--	PC1	ICMP
	2.020	PC1	Switch1	ICMP
	2.021	Switch1	R1	ICMP

Рисунок 4.2 - Режим симуляції

```
C:\>arp -a
  Internet Address      Physical Address      Type
  10.10.10.1            0000.0c07.ac0a        dynamic

C:\>ping -t 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data:

Reply from 10.10.10.1: bytes=32 time=4ms TTL=255
Reply from 10.10.10.1: bytes=32 time=4ms TTL=255
Reply from 10.10.10.1: bytes=32 time=4ms TTL=255
Reply from 10.10.10.1: bytes=32 time=4ms TTL=255
Reply from 10.10.10.1: bytes=32 time=4ms TTL=255
Reply from 10.10.10.1: bytes=32 time=4ms TTL=255
Reply from 10.10.10.1: bytes=32 time=4ms TTL=255
Reply from 10.10.10.1: bytes=32 time=4ms TTL=255
Reply from 10.10.10.1: bytes=32 time=4ms TTL=255
Reply from 10.10.10.1: bytes=32 time=4ms TTL=255
Request timed out.
Request timed out.
Reply from 10.10.10.1: bytes=32 time=6ms TTL=255
```

Рисунок 4.3 - Пінг до віртуального шлюзу

На рисунку 4.4 показано, що після відмови R1 маршрутизатор R2 коректно переймає на себе роль активного шлюзу.

```
R2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gig0/0      10   100 P Active  local           unknown         10.10.10.1
```

Рисунок 4.4 - R2 став Active

4.3.1 Аналіз параметрів failover.

Для оцінки часу перемикання активного шлюзу імітувалася відмова маршрутизатора R1 у фіксований момент часу (10-та секунда симуляції). У кожному прогоні вимірювалися:

- момент вимкнення R1;

- час надходження першого HSRP-повідомлення від резервного маршрутизатора R2;

- час першої успішної ICMP-відповіді після переключення на резервний шлюз;

- кількість втрачених ICMP-пакетів під час події.

Результати п’яти прогонів узагальнено в таблиці 4.2.

Таблиця 4.2 - Результати вимірювання часу автоматичного перемикання (failover) при стандартних таймерах HSRP

Прогін	Час вимкнення R1 (s)	Перший HSRP-пакет від R2 (s)	Перший успішний ICMP (s)	Failover time (s)	Втрачено ICMP
1	10.0	12.5	22.0	12.0	2
2	10.0	12.3	21.8	11.8	1
3	10.0	12.7	22.2	12.2	2
4	10.0	12.1	22.5	12.5	2
5	10.0	12.9	21.9	11.9	1
Середнє (прибл.)	-	12.5 ± 0.2	22.08 ± 0.2	12.08 ± 0.2	1.6

Середній час автоматичного перемикання склав приблизно 12,1 с, при цьому в середньому втрачалося 1,6 ICMP-пакета. На графіку зміни часу failover (рис. 4.5) видно, що розкид значень між окремими прогонами не перевищує 0,7 с, що свідчить про стабільність роботи HSRP за стандартних налаштувань таймерів.

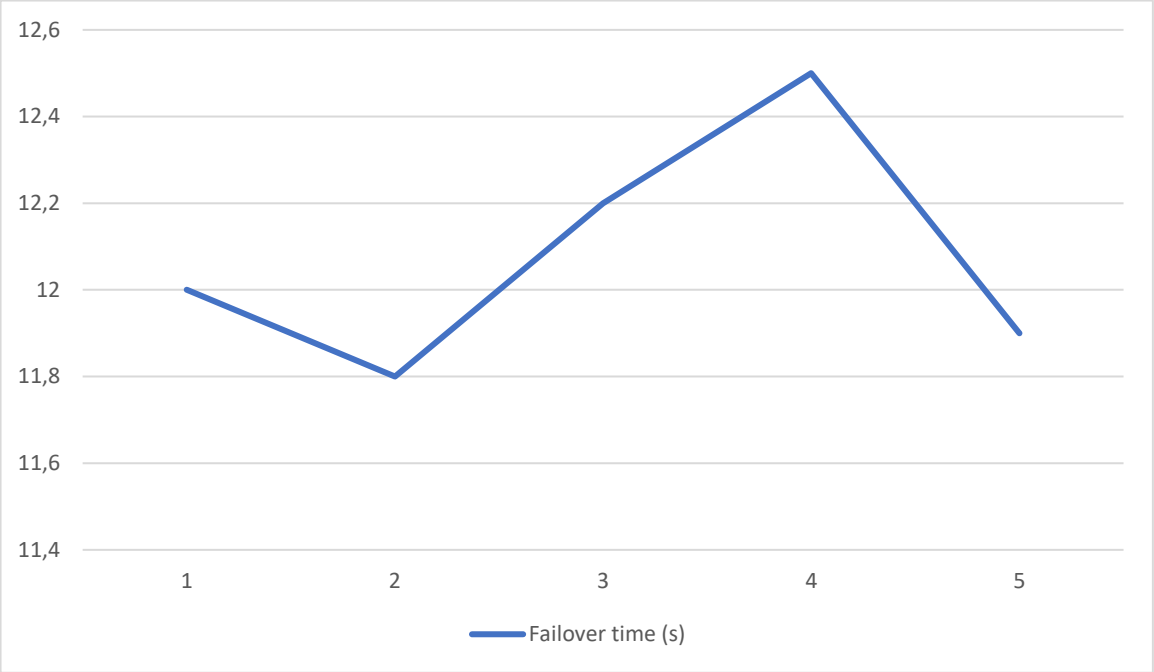


Рисунок 4.5 - Графік автоматичного відновлення

Порівняно з базовою конфігурацією без протоколів резервування (підпункт 4.2), де тривалість повної недоступності мережі після відмови шлюзу перевищувала 60 с, використання HSRP дозволило зменшити час простою більш ніж у п’ять разів. Крім того, відновлення зв’язку відбувається автоматично, без участі адміністратора, що є критично важливим для корпоративних мереж із підвищеними вимогами до безперервності роботи.

4.3.2 Аналіз параметрів відновлення активної ролі (preemption)

Окремо було досліджено процес повернення активної ролі маршрутизатора R1 після його відновлення. У цьому сценарії R2 тимчасово виконує роль активного шлюзу, а після ввімкнення R1 (за умови більш високого пріоритету та параметра preempt) відбувається зворотне перемикання активного шлюзу на R1.

Під час експерименту вимірювалися:

- момент подачі живлення на R1;

- час появи першого HSRP-повідомлення від R1 після завантаження;

- час першої успішної ICMP-відповіді після повернення R1 до ролі активного маршрутизатора;

- кількість втрачених ICMP-пакетів у процесі перемикання.

Результати випробувань зведено у таблицю 4.3.

Таблиця 4.3 - Результати вимірювання часу відновлення активної ролі маршрутизатора R1 (preemption)

Прогін	Час увімкнення R1	Час появи першого HSRP від R1 після відновлення (s)	Перший успішний ICMP після відновлення (s)	Час від HSRP до пінг (s)	Втрачено ICMP
1	0.1	27.0	35.0	8.0	1
2	0.1	26.8	34.5	7.7	1
3	0.1	27.5	35.6	8.1	1
4	0.1	27.9	35.2	7.3	1
5	0.1	26.9	34.3	7.4	1
Середнє (прибл.)		-	-	7.7 ± 0.2	1

Побудований на основі отриманих даних графік (рис. 4.6) демонструє незначний розкид значень часу відновлення, що підтверджує передбачуваність роботи механізму preemption в умовах стандартних таймерів HSRP.

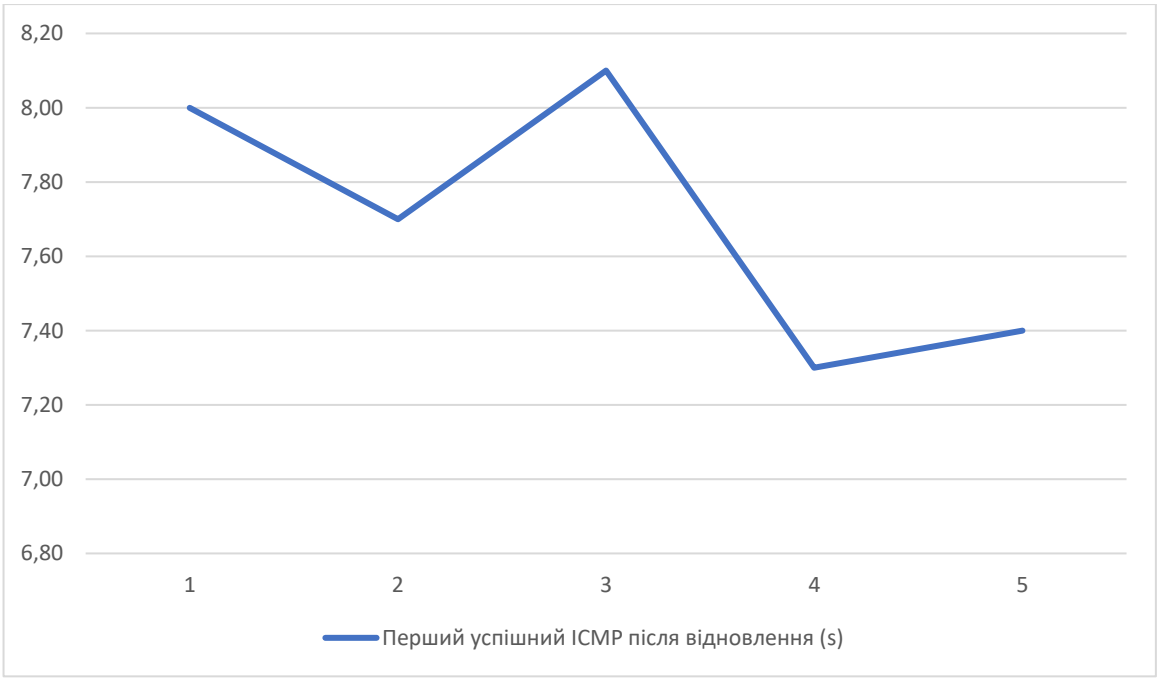


Рисунок 4.6 - Графік вимірювання часу відновлення R1

Середній час від моменту надходження першого HSRP-повідомлення від R1 до відновлення успішних ICMP-відповідей становив близько 7,7 с. У кожному

прогоні фіксувалася втрата лише одного ICMP-пакета, що є прийнятним показником для більшості корпоративних застосунків, особливо з урахуванням того, що процес переключення є повністю прозорим для користувачів.

4.3.3 Узагальнення результатів для HSRP з таймерами за замовчуванням

Проведені експериментальні дослідження показали, що використання протоколу HSRP зі стандартними значеннями таймерів дозволяє істотно підвищити відмовостійкість корпоративної мережі порівняно з базовим варіантом без резервування:

- час простою при відмові основного шлюзу скорочується з десятків секунд до ~12 с;

- відновлення активної ролі первинного маршрутизатора відбувається за ~7-8 с із мінімальними втратами пакетів;

- процес перемикання та повернення активного шлюзу повністю автоматизований і не потребує ручного втручання адміністратора.

Водночас отримані значення failover time можуть бути недостатніми для сервісів із жорсткими вимогами до безперервності (VoIP, відеоконференції тощо). Це обґрунтовує доцільність подальшої оптимізації параметрів HSRP, зокрема зменшення значень таймерів hello/hold, що розглядається в наступному підрозділі.

4.4 Дослідження параметрів мережі з HSRP та оптимізованими таймерами

Як показали результати підрозділу 4.3, використання HSRP зі стандартними таймерами вже дає суттєвий виграш порівняно з базовою конфігурацією без резервування. Водночас середній час перемикання на резервний шлюз на рівні ≈12 с може бути недостатнім для сервісів, чутливих до затримок (VoIP, відеоконференції, інтерактивні застосунки). Тому наступним кроком є дослідження можливості зменшення часу простою за рахунок оптимізації параметрів HSRP.

Для цього було змінено значення таймерів:

standby 10 timers 1 3,

що відповідає інтервалу надсилання hello-повідомлень 1 с і часу утримання (hold time) 3 с. Інші параметри (номер групи, пріоритети, preempt) залишалися такими самими, як у попередньому експерименті, що дозволяє коректно порівнювати результати.

4.4.1 Аналіз параметрів failover при зменшених таймерах

Сценарій моделювання відмови активного маршрутизатора R1 залишався незмінним: у фіксований момент часу (10-та секунда симуляції) виконувалося вимкнення R1, а далі фіксувалися:

- час відмови R1;
- час надходження першого HSRP-повідомлення від R2;
- час першої успішної ICMP-відповіді після переключення;
- кількість втрачених ICMP-пакетів.

Результати п’яти прогонів наведено в таблиці 4.4.

Таблиця 4.4 - Результати вимірювання часу автоматичного перемикання (failover) при таймерах HSRP 1/3

Прогін	Час вимкнення R1 (s)	Перший HSRP-пакет від R2 (s)	Перший успішний ICMP (s)	Failover time (s)	Втрачено ICMP
1	10.0	11.0	13.2	3.2	1
2	10.0	11.1	13.0	3.0	1
3	10.0	10.9	13.4	3.4	2
4	10.0	11.2	13.3	3.3	1
5	10.0	10.8	13.1	3.1	1
Середнє (прибл.)	–	11.0 ± 0.2	13.2 ± 0.2	3.2 ± 0.2	≈1.2

На основі зібраних даних середній час перемикання становив приблизно 3,2 с, тобто був у 3-4 рази меншим, ніж при використанні стандартних таймерів. Кількість втрачених ICMP-пакетів при цьому не перевищувала 1-2 за прогін, що можна вважати прийнятним значенням для більшості типів трафіку.

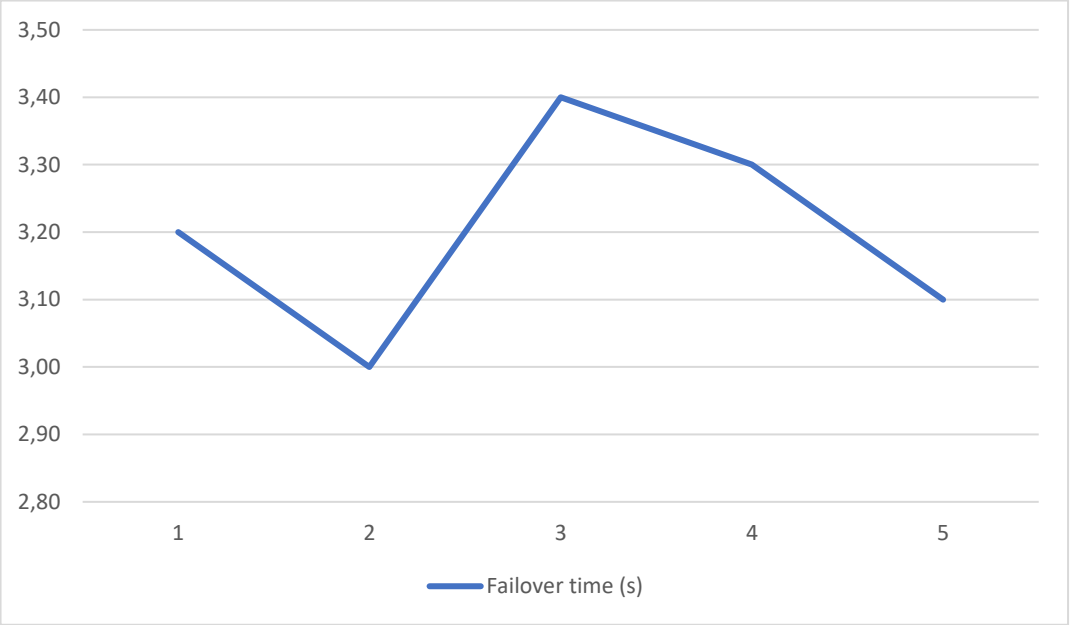


Рисунок 4.7 - Графік автоматичного відновлення

Графік зміни часу failover для окремих прогонів (рис. 4.7) демонструє невеликий розкид значень, що свідчить про стабільність роботи протоколу HSRP навіть за зменшених таймерів.

4.4.2 Аналіз параметрів відновлення активної ролі R1

Аналогічно до попереднього підрозділу, було досліджено процес повернення активної ролі маршрутизатора R1 (preemption) після його відновлення. У конфігурації залишався увімкнений параметр preempt, а таймери 1/3 використовувалися як для активного, так і для резервного маршрутизаторів.

Під час експерименту вимірювалися:

- момент появи першого HSRP-повідомлення від R1 після ввімкнення;
- час першої успішної ICMP-відповіді після повернення R1 до ролі активного шлюзу;
- проміжок часу між цими подіями;
- кількість втрачених ICMP-пакетів.

Результати п’яти прогонів зведено у таблицю 4.5.

Таблиця 4.5 - Результати вимірювання часу відновлення активної ролі маршрутизатора R1 при таймерах HSRP 1/3

Прогін	Час увімкнення R1 (s)	Час появи першого HSRP від R1 після відновлення (s)	Перший успішний ICMP після відновлення (s)	Час від HSRP до пінг (s)	Втрачено ICMP
1	0.1	40.0	42.0	2.0	1
2	0.1	39.8	41.9	2.1	0
3	0.1	40.2	42.3	2.1	1
4	0.1	39.9	42.1	2.2	1
5	0.1	40.1	42.2	2.1	0
Середнє (прибл.)	–	–	–	2.1 ± 0.1	≈0.6

У середньому час від моменту надходження першого HSRP-повідомлення від R1 до відновлення відповіді на ICMP-запити становив близько 2,1 с, що істотно менше, ніж значення ≈7,7 с, отримане при стандартних таймерах. Кількість втрачених ICMP-пакетів у кожному прогоні дорівнювала 0-1, тобто негативний вплив на прикладні сервіси є мінімальним.

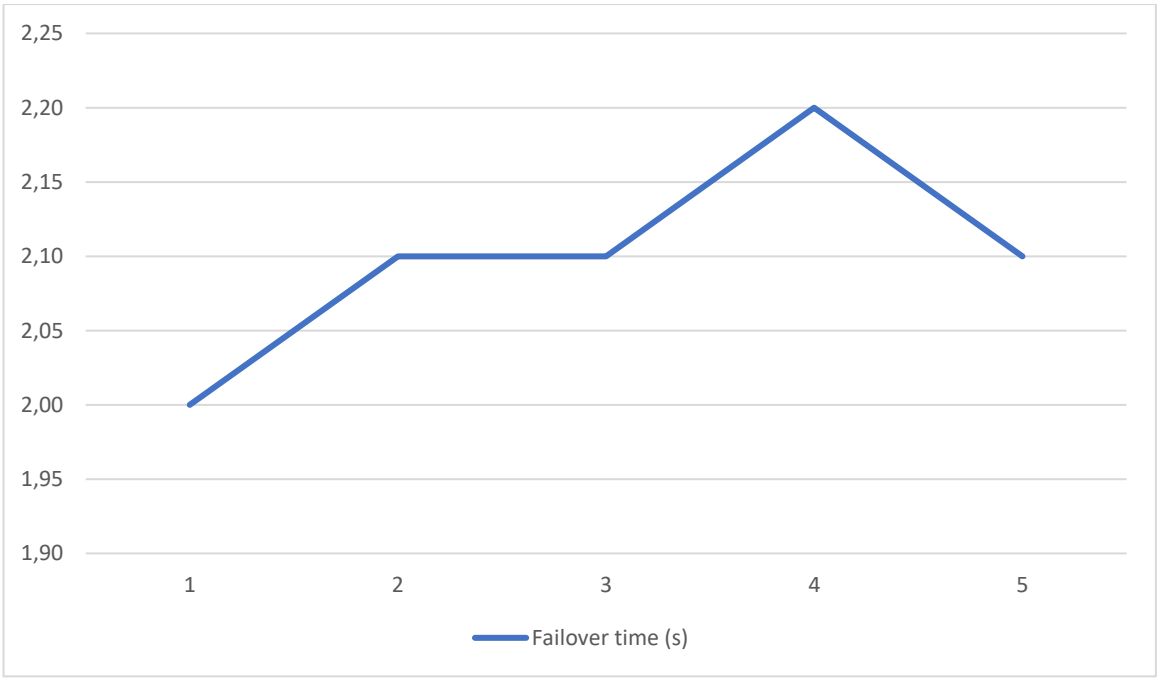


Рисунок 4.8 - Графік автоматичного відновлення

Побудований графік (рис. 4.8) підтверджує, що зменшення таймерів дозволяє досягти стабільного та прогнозованого скорочення часу відновлення активної ролі без суттєвого збільшення кількості втрат пакетів.

4.4.3 Узагальнення для оптимізованих таймерів

Оптимізація параметрів HSRP за рахунок зменшення інтервалів hello/hold дозволила:

- скоротити час автоматичного перемикання з ≈12,1 с до ≈3,2 с;
- зменшити час повернення активної ролі маршрутизатора R1 з ≈7,7 с до ≈2,1 с;
- зберегти низький рівень втрат ICMP-пакетів (0-2 за подію).

Таким чином, конфігурація з таймерами 1/3 забезпечує значно вищу оперативність реакції на відмову та відновлення вузлів, що робить її доцільною для застосування в мережах із жорсткими вимогами до доступності та мінімальних простоїв. Водночас зменшення таймерів збільшує частоту службових повідомлень у мережі, тому вибір конкретних значень має здійснюватися з урахуванням навантаження та особливостей інфраструктури.

4.5 Порівняння конфігурацій мережі та аналіз результатів

Для узагальнення отриманих результатів було проведено порівняння трьох основних варіантів конфігурації мережі:

- базова мережа без протоколів резервування (єдиний шлюз);
- мережа з HSRP та стандартними таймерами (timers 3 10);
- мережа з HSRP та оптимізованими таймерами (timers 1 3).

У табл. 4.6 наведено зведені показники для кожного зі сценаріїв.

Таблиця 4.6 - Порівняння параметрів роботи мережі для різних конфігурацій

Конфігурація мережі	Середній час простою при відмові шлюзу (failover), с	Середній час відновлення активної ролі R1, с	Середня кількість втрачених ICMP-пакетів	Необхідність ручного втручання
Без протоколів резервування	≈60 і більше	залежить від дій адміністратора	висока	так
HSRP, таймери 3/10	≈12,1	≈7,7	низька (1-2 за подію)	ні
HSRP, таймери 1/3	≈3,2	≈2,1	дуже низька (0-1 за подію)	ні

Аналіз таблиці показує, що впровадження протоколу резервування першого переходу HSRP радикально підвищує відмовостійкість мережі: час простою скорочується з десятків секунд до одиниць секунд, а процес відновлення стає повністю автоматизованим. Додаткова оптимізація таймерів дозволяє ще більше зменшити час реакції на відмову та відновлення, практично не погіршуючи інших показників.

Отримані результати підтверджують доцільність використання протоколів резервування у корпоративних мережах та демонструють, що правильний вибір параметрів HSRP має суттєвий вплив на показники доступності та якості мережевих сервісів. Діапазони значень часу перемикання та втрат пакетів, отримані в експерименті, узгоджуються з результатами досліджень продуктивності протоколів FHRP, наведеними в роботах [18-21].

4.6 Висновки до розділу 4

У четвертому розділі було виконано експериментальне дослідження параметрів роботи корпоративної мережі в різних режимах функціонування: без протоколів резервування, з використанням HSRP зі стандартними таймерами та з оптимізованими параметрами роботи протоколу.

Аналіз базової конфігурації без резервування показав критичну залежність мережі від єдиного маршрутизатора-шлюзу: у разі його відмови доступ до ресурсів повністю втрачається, тривалість простою становить порядку 60 с і більше, а відновлення роботи можливе лише після ручного втручання адміністратора. Такий підхід є неприйнятним для сучасних корпоративних мереж із підвищеними вимогами до безперервності сервісів.

Використання протоколу HSRP зі стандартними таймерами (timers 3 10) дозволило істотно підвищити відмовостійкість системи. Середній час автоматичного перемикання на резервний маршрутизатор становив близько 12 с, час повернення активної ролі R1 - близько 7,7 с, при цьому втрати пакетів були незначними (1-2 ICMP-пакети на подію), а весь процес відновлення відбувався без участі адміністратора. Уже на цьому етапі було досягнуто багаторазове скорочення простою порівняно з базовою конфігурацією.

Подальша оптимізація налаштувань HSRP за рахунок зменшення таймерів до timers 1 3 і використання механізму preempt дала змогу ще більше зменшити час реакції мережі на відмову. Середній час failover скоротився до ≈3,2 с, а час відновлення активної ролі R1 - до ≈2,1 с, при цьому кількість втрачених пакетів не перевищувала 0-1 на подію. Отже, така конфігурація є придатною для застосування в середовищах із жорсткими вимогами до мінімізації перерв у наданні послуг.

Зведене порівняння трьох розглянутих варіантів підтвердило, що впровадження протоколів резервування першого переходу є необхідною умовою для забезпечення високої доступності корпоративних мереж. Вибір конкретних значень таймерів HSRP повинен здійснюватися з урахуванням компромісу між швидкістю реагування на відмови та додатковим службовим навантаженням на мережу, однак результати експериментів показують, що навіть помірне зменшення таймерів дає суттєвий виграш у відмовостійкості без помітного погіршення інших характеристик.

ВИСНОВКИ

У ході виконання магістерської роботи було реалізовано поставлену мету - розроблено та досліджено систему забезпечення відмовостійкості корпоративної мережі на основі протоколів резервування, а також оцінено ефективність їх застосування в сучасних інформаційних системах.

У першому розділі було проаналізовано поняття та структуру корпоративних мереж, їхні переваги та виклики, а також проблеми надійності та безперервності роботи.

У другому розділі досліджено технології забезпечення відмовостійкості. Окрему увагу приділено протоколам резервування першого переходу (FHRP). Проаналізовано їх принципи роботи, а також переваги й обмеження в контексті корпоративних мереж.

У третьому розділі було спроєктовано та реалізовано відмовостійку тестову мережу в середовищі Cisco Packet Tracer із використанням протоколу HSRP.

У четвертому розділі проведено експериментальні дослідження параметрів роботи мережі у трьох конфігураціях:

- базова мережа без протоколів резервування (єдиний шлюз);
- мережа з HSRP та стандартними таймерами (timers 3 10);
- мережа з HSRP та оптимізованими таймерами (timers 1 3, preempt).

Практичні результати роботи підтверджують, що використання протоколів резервування першого переходу є доцільним та необхідним для корпоративних мереж із підвищеними вимогами до безперервності сервісів. Розроблена тестова мережа та отримані експериментальні дані можуть бути використані як основа для подальшого масштабування рішень, впровадження аналогічних механізмів у реальних інфраструктурах, а також для навчальних цілей під час підготовки фахівців у галузі комп’ютерних мереж та кібербезпеки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Corporate Network. URL: https://www.sciencedirect.com/topics/computer-science/corporate-network (дата звернення 15.09.2025).

2. Тарнавський, Ю. А., & Кузьменко, І. М. (2018). Організація комп'ютерних мереж. - Київ : КПІ ім. Ігоря Сікорського, 2018. - 259 с.

3. Tanenbaum A. S., Wetherall D. J. Computer Networks. - 5th ed. - Pearson, 2011.

4. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. - 7th ed. - Pearson, 2017. - 864 p.

5. Seifert R., Edwards J. The All-New Switch Book: The Complete Guide to LAN Switching Technology. - 2nd ed. - Wiley, 2008. - 928 p.

6. Киричек Г.Г., Тягунова М.Ю., Школовий В.В. Протокол RSTP в сучасній розподіленій мережі. Науково-практична конференція «Теорія та практика актуальних наукових досліджень», 26-27 вересня 2025 року, м. Полтава, Україна, С.106-110.

7. Bhagwan, Ranjita, Stefan Savage, and Geoffrey M. Voelker. "Understanding availability." International Workshop on Peer-to-Peer Systems. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003.

8. Network Failure. URL: https://www.sciencedirect.com/topics/computer-science/network-failure (дата звернення 18.09.2025).

9. MTTR vs. MTBF: What’s the difference? URL: https://www.ibm.com/think/topics/mttr-vs-mtbf (дата звернення 19.09.2025).

10. Koren I., Krishna C. M. Fault-tolerant systems. - Morgan Kaufmann, 2020.

11. Що таке якість обслуговування? URL: https://fiberroad.com/uk/resources/glossary/what-is-quality-of-service-qos/ (дата звернення 20.09.2025).

12. Oggerino C. High Availability Network Fundamentals. - Cisco Press, 2001.

13. Чи така важлива висока доступність для інфраструктури? URL: https://onbiz.biz/is-high-availability-important-for-infrastructure/ (дата звернення 20.09.2025).

14. Fault Tolerance in Network Design. URL: https://www.siberoloji.com/fault-tolerance-in-network-design-data-communications/ (дата звернення 24.09.2025).

15. Oppenheimer P. Top-Down Network Design. - 3rd ed. - Cisco Press, 2011. - 432 p.

16. What are Redundancy Protocols? URL: https://lightyear.ai/tips/what-are-redundancy-protocols (дата звернення 25.09.2025).

17. Єременко, О. С., Мерсні, А. Підвищення відмовостійкості елементів сучасних інфокомунікаційних мереж із застосуванням протоколів резервування шлюзу за замовчуванням. Проблеми телекомунікацій, № 2(27), 2020, с. 68–81. URL: https://science.lpnu.ua/ictee/all-volumes-and-issues/volume-5-number-1-2025/study-reliability-and-fault-tolerance-management (дата звернення 25.09.2025).

18. Rahman Z. U. et al. Performance Evaluation of First Hop Redundancy Protocols //J. Appl. Environ. Biol. Sci. - 2017. - Т. 7. - №. 3. - С. 268-278.

19. Agarwal, Aayush, and Shilpi Sharma. "Performance evaluation of hsrp, glbp and vrrp with interior gateway routing protocol and exterior gateway routing protocol." 2022 12th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE, 2022.

20. What is Cisco Packet Tracer? URL: https://www.netacad.com/cisco-packet-tracer (дата звернення 15.11.2025).

21. Simanjuntak, Imelda Uli Vistalina, Junas Haidi, and Lukman Medriavin Silalahi. "Simulation and Performance Analysis of Network Backup Systems Using Hot Standby Router Protocol (HSRP) Method on Real-Time Networks." International Journal of Electronics and Telecommunications (2023): 763-768.

ДОДАТОК А

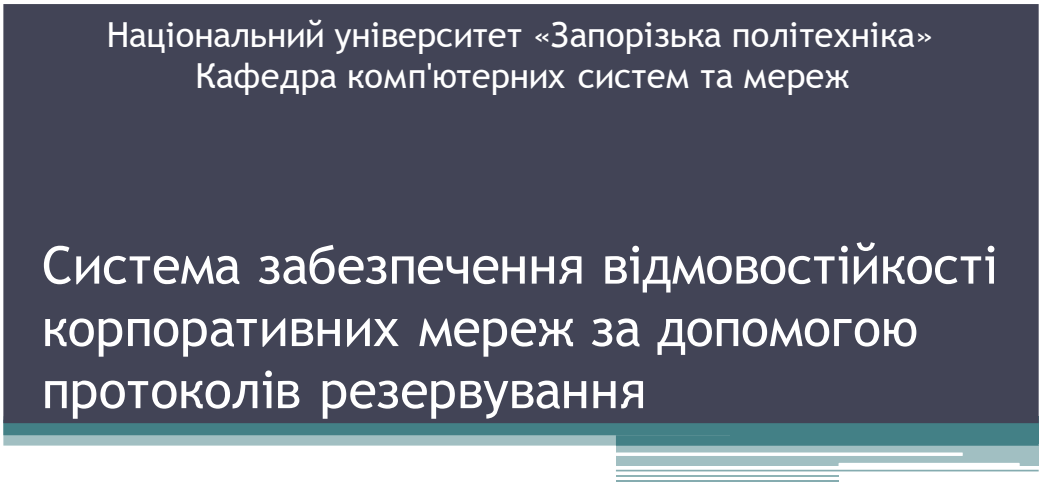


Рисунок А.1 - Слайд перший

Метою дослідження є реалізація системи забезпечення відмовостійкості корпоративних мереж за допомогою протоколів резервування, дослідження методів та механізмів, оцінка ефективностіїх застосуванняу сучасних інформаційних системах.

Об'єктом дослідження є корпоративна мережа як інфраструктурапередаваннята обробки даних.

Предметом дослідження є методи забезпечення відмовостійкості та протоколи резервування шлюзів (FHRP: HSRP, VRRP, GLBP).

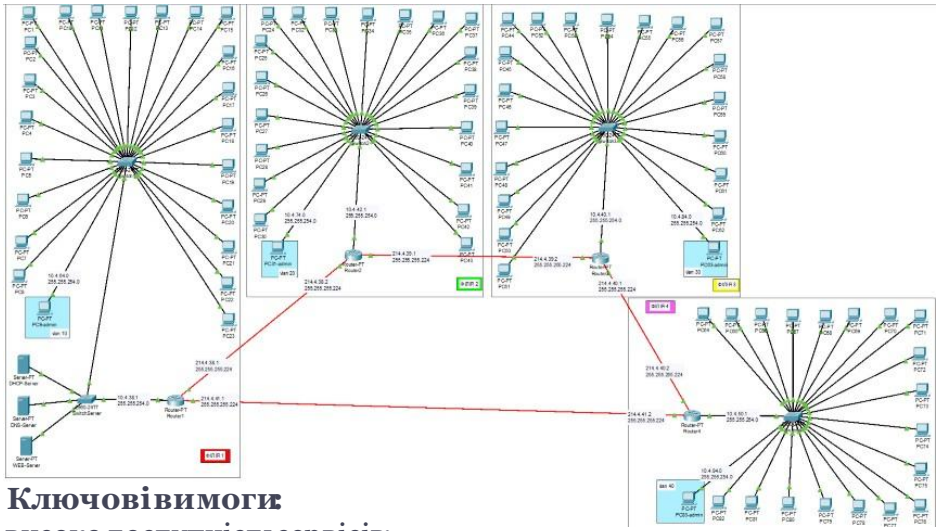
Рисунок А.2 - Слайд другий

Основнізадачі:

- проаналізувати структуру корпоративних мереж та фактори, що впливають на їх надійність;
- дослідитиметоди резервування та протоколи FHRP;
- спроєктувати відмовостійку мережу з HSRP у Cisco Packet Tracer;
- експериментальнопорівняти роботу мережі без резервування, з HSRP 3/10 та HSRP 1/3;
- сформулювати рекомендації щодо налаштування відмовостійкихмереж.

Рисунок А.3 - Слайд третій

Корпоративна мережа: структура та вимоги



Ключовівимоги:

- висока доступністьсервісів;
- масштабованістьі модульність;
- безпека та сегментація;
- керованістьта моніторинг.

Рисунок А.4 - Слайд четвертий

5

Проблеми надійності та методи їх вирішення

Причини відмов:
- апаратні збої (маршрутизатори, комутатори, канали зв'язку);
- програмні помилки;
- людський фактор;
- кіберінциденти.

Ключові підходи:
- резервування обладнання (маршрутизатори, комутатори, сервери);
- резервування каналів (Link Aggregation, динамічна маршрутизація OSPF/BGP);
- протоколи FHRP: HSRP, VRRP, GLBP;
- моніторинг та аварійне відновлення;
- інформаційна безпека: firewall, IDS/IPS, VPN.

Рисунок А.5 - Слайд п'ятий

6

Аналіз протоколів резервування (FHRP)

Розглянуті протоколи першого переходу:
- **HSRP** (Hot Standby Router Protocol) - пропрієтарний протокол Cisco;
- **VRRP** (Virtual Router Redundancy Protocol) - відкритий стандарт (RFC 5798);
- **GLBP** (Gateway Load Balancing Protocol) - пропрієтарний протокол Cisco з балансуванням навантаження.

Для кожного протоколу було проаналізовано:
- принцип роботи та ролі маршрутизаторів (Active/Standby, Master/Backup, AVG/AVF);
- механізм вибору активного шлюзу (пріоритет, IP-адреса, «IP address owner»);
- особливості таймерів та часу перемикання (failover);
- можливість балансування навантаження між кількома шлюзами;
- переваги, недоліки та сфери доцільного застосування в корпоративних мережах.

Рисунок А.6 - Слайд шостий

7

Порівняння FHRP

Критерій порівняння	HSRP	VRRP	GLBP
Сумісність із обладнанням	Висока (переважно Cisco)	Середня (багато виробників)	Середня (Cisco та сумісні)
Підтримка балансування навантаження	Низька (один активний маршрутизатор)	Низька (один Master маршрутизатор)	Висока (кілька активних маршрутизаторів одночасно)
Складність налаштування	Середня	Середня	Середня
Час відновлення після відмови (failover time)	Дуже швидкий	Швидкий	Швидкий
Масштабованість	Висока	Висока	Висока

Рисунок А.7 - Слайд сьомий

8

Порівняння FHRP

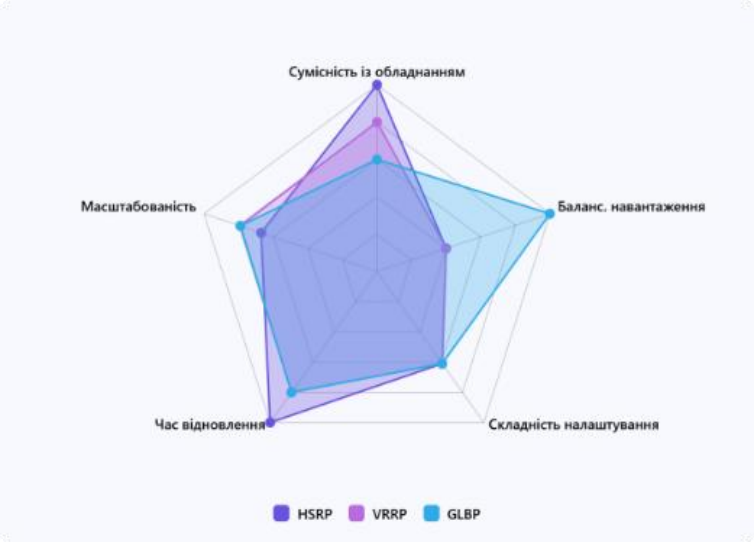


Рисунок А.8 - Слайд восьмий

Тестова мережа з HSRP

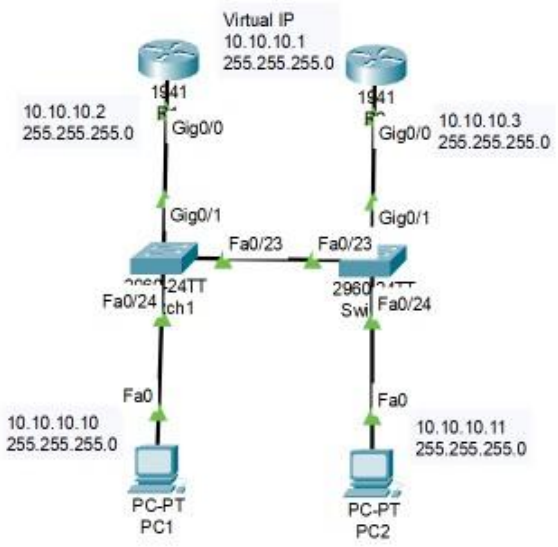


Рисунок А.9 - Слайд дев’ятий

Конфігурація HSRP

На R1:
ip address 10.10.10.2 255.255.255.0
standby 10 ip 10.10.10.1
standby 10 priority 120
standby 10 preempt
На R2:
ip address 10.10.10.3 255.255.255.0
standby 10 ip 10.10.10.1
standby 10 priority 100
standby 10 preempt

Рисунок А.10 - Слайд десятий

11

Сценарії експерименту

Три конфігурації

1. **Без резервування** єдиний шлюз R1.
2. **HSRP, таймери 3/10** - стандартні налаштування
3. **HSRP, таймери 1/3** - оптимізовані таймери.

Для кожної конфігурації:

- моделювання відмови R1 (shutdown інтерфейсу);
- безперервний ping до шлюзу;
- вимірюються:
  - час failover;
  - час відновлення активної ролі R1 (preemption);
  - кількість втрачених ICMP-пакетів.

Рисунок А.11 - Слайд одинадцятий

12

Результати

Рисунок А.12 - Слайд дванадцятий

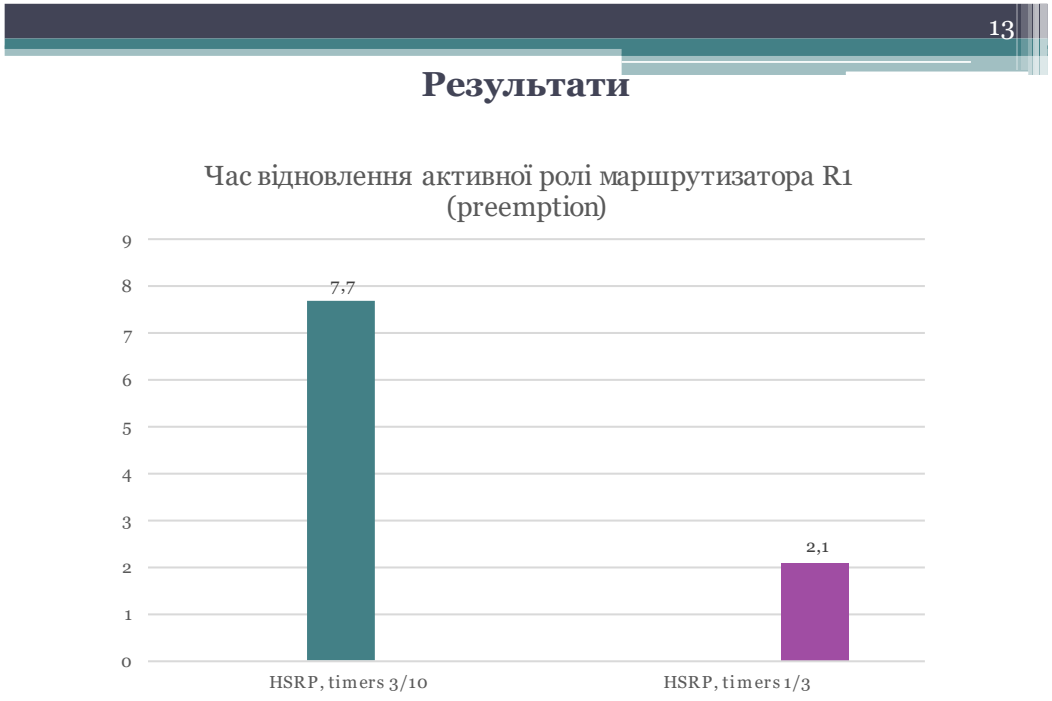


Рисунок А.13 - Слайд тринадцятий

Рисунок А.14 - Слайд чотирнадцятий

15

ВИСНОВКИ

Розроблено та досліджено систему забезпеченнявідмовостійкості корпоративної мережі з використанням HSRP.

Показано, що:

- без резервування мережа критично залежить від єдиного шлюзу;
- HSRP зі стандартними таймерами суттєво зменшує простої;
- оптимізація таймерів до 1/3 дає додатковe 3–4-разове скорочення часу перемикання.

Отримані результати підтверджують доцільність застосування FHRP у корпоративних мережах з високими вимогами до доступності.

Розроблена тестова мережа та методика вимірювань можуть бути використані:

- для проєктуваннята модернізації корпоративних мереж,
- у навчальному процесі при підготовці фахівців з комп'ютерних мереж.

Рисунок А.15 - Слайд п'ятнадцятий

16

Публікації

Киричек Г.Г., Тягунова М.Ю., Школовий В.В. Протокол RSTP в сучасній розподіленій мережі. Науково-практична конференція «Теорія та практика актуальних наукових досліджень», 26-27 вересня 2025 року, м. Полтава, Україна, С.106-110.

Рисунок А.16 - Слайд шістнадцятий