МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітньо-професійна програма: «Комп'ютерна інженерія»

Група: 2БКС-29

КВАЛІФІКАЦІЙНА РОБОТА

здобувача освіти денної форми навчання

БКС.29.09.000.КРБ

ЄРОШЕНКО
МИКОЛИ СЕРГІЙОВИЧА

м. Одеса
2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітньо-професійна програма: **«Комп'ютерна інженерія»**

Група: **2БКС-28**

ПОЯСНЮВАЛЬНА ЗАПИСКА

До кваліфікаційної роботи бакалавра на тему: **Аналіз апаратних рішень відмовостійких комп'ютерних мереж**

Проектний матеріал складається з пояснювальної записки на 69 сторінках та графічного (презентаційного) матеріалу на 13 аркушах (слайдах)

Виконавець _____ (Єрошенко М.С)

Керівник проекту _____ (Кунуп Т. В.)

Консультанти:

з розділу охорони праці та техніки безпеки _____ (Чорновол Н.І.)

з нормоконтролю _____ (Петрашова В.І.)

старший консультант _____ (Кривченко Ю.В.)

До захисту допущений

Завідувач кафедри _____ (Іванова Л.В.)

Завідувач відділенням _____ (Краснокутська К.Г.)

Захист «12» 06 2025 р. Протокол ЕК № 2

Оцінка ЕК 4 (добре) / 80

Секретар ЕК _____

АНОТАЦІЯ

Цю кваліфікаційну роботу присвячено аналізу апаратних рішень, що забезпечують відмовостійкість комп'ютерних мереж в умовах зростання кількості користувачів та обсягів обробки даних.

Метою даної роботи є аналіз та оцінка ефективності сучасних апаратних рішень для забезпечення стабільної роботи систем при обробці запитів великої кількості користувачів та підвищення відмовостійкості систем в умовах часткових відмов компонентів.

Вивчено закономірності функціонування комп'ютерних мереж під навантаженням та особливості впливу часткових відмов вузлів системи, комутаторів та каналів на їхню працездатність.

Отримані кількісні оцінки ефективності застосування різних апаратних рішень в умовах високих навантажень та при симуляції сценаріїв часткової відмови компонентів мережі.

Створено моделі, що дозволяють оцінювати специфіку різних топологій, необхідний рівень швидкодії та відмовостійкості для прийняття оптимальних інженерних рішень.

Розглянуто питання з охорони праці та техніки безпеки.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення Комп'ютерних систем Кафедра Комп'ютерної інженерії

Спеціальність 123 «Комп'ютерна інженерія»

Освітньо-професійна програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР Бержань І.В.

"28" 05 2025р.

ЗАВДАННЯ

на кваліфікаційну роботу бакалавра

здобувачеві освіти Єрошенко Миколі Сергійовичу

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Аналіз апаратних рішень відмовостійкості комп'ютерних мереж*

затверджена наказом по коледжу від "14" листопада 20 24 р.№ 246

2. Термін здачі студентом кваліфікаційної роботи 20.06.2025

3. Вихідні дані до роботи 1.Проаналізувати сучасні апаратні рішення, які застосовуються для побудови відмовостійких комп'ютерних мереж, оцінити ефективність, надійність і доцільність використання в різних умовах експлуатації; 2. Дослідити відмовостійкість та критерії її оцінки в комп'ютерних мережах; 3. Розробити модель відмовостійкої мережі з використанням обраного обладнання; 4. Провести моделювання/аналіз (в середовищі GNS3, Packet Tracer або іншому ПЗ) сценаріїв збоїв та перевірити реакцію мережі.

4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити)

Вступ; Апаратні рішення для забезпечення відмовостійкості; Проєктування моделі відмовостійкої мережі; Опис використаного ПЗ для моделювання; Моделювання роботи мережі в умовах відмов; Сценарії тестування збоїв (вихід з ладу вузлів, комутаторів, каналів); Результати тестування; Оцінка ефективності апаратних рішень; Основні результати дослідження; Висновки; Питання з охорони праці і техніки безпеки

5. Перелік графічного матеріалу (слайдів мультимедійної презентації) Титульний слайд; Загальна схема відмовостійкої мережі з резервним маршрутизатором та комутатором; Моделювання роботи мережі з резервним маршрутизатором та комутатором та анімація трафіку (PacketTracer); Визначення пінгу між вузлами мережі у нормальному стані; Модель мережі з імітацією збою – відключення інтерфейсу; Модель мережі при відновленні з'єднання через резервний маршрут; Модель мережі після втрати одного з комутаторів; Конфігурація резервування шлюзу з використанням HSRP; Порівняльна таблиця апаратних рішень для відмовостійких мереж; Графіки порівняння ефективності моделей відмовостійкості мережі

6. Консультанти по кваліфікаційній роботі, із зазначенням розділів, що їх стосуються

Розділ	Консультант	ПІДПИС	
		Завдання видав	Завдання прийняв
Основний розділ	*Кунуп Т.В.*		
Розділ охорони праці	*Чорновол Н.І.*		
Нормоконтроль	*Петрашова В.І.*		
Старший консультант	*Кривченко Ю.В.*		

7. Дата видачі завдання 28.04.25

Керівник роботи *Кунуп Т.В.* _____
(підпис)

Завдання прийняв до виконання *Єрошенко М.С* _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	*Аналіз технічного завдання. Написання вступу*	28.04.25	виконав
2.	*Дослідження поняття відмовостійкості та критерії її оцінки*	05.05.25	виконав
3.	*Огляд апаратних рішень для забезпечення відмовостійкості*	08.05.25	виконав
4.	*Класифікація типів апаратної відмовостійкості*	15.05.25	виконав
5.	*Порівняння технічних характеристик популярних*	16.05.25	виконав
	рішень провідних виробників		
6.	*Розробка моделей відмовостійкої мережі з*	17.05.25	виконав
	використанням обраного обладнання		
7.	*Моделювання/аналіз (GNS3, Packet Tracer)*	20.05.25	виконав
	сценаріїв збоїв та перевірка реакції мережі		
8.	*Визначення ефективності використання апаратних*	05.06.25	виконав
	рішень залежно від масштабу і задач мережі		
9.	*Візуалізація результатів порівняння ефективності*	10.06.25	виконав
	моделей відмовостійкості мережі графіками		
10.	*Розробка питань з охорони праці та техніки безпеки*	14.06.25	виконав
11.	*Підготовка матеріалів мультимедійної презентації*	16.06.25	виконав
12.	*Підготовка доповіді для захисту*	18.06.25	виконав
13.	*Малий захист дипломного проєкту*	20.06.25	

Здобувач освіти _____
(підпис)

Керівник роботи _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			БКС 29. 09 000. 00 КРБ	Випускна робота		
А4			БКС 29. 09 000. 00 КРБ ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	БКС 28. ХХ 000. 00 КРБ		
Розробив		Єрошенко М.С.			Аналіз апаратних рішень відмовостійкості комп'ютерних мереж	Літ.	Аркуш 4 / Аркушів 69
Перевірив		Кунуп Т.В.		10.06		Н Д П	
Н. Контр.		Петрашова В.І.				ВСП "ОТФК ОНТУ" гр.2БКС-29	
Затверд.		Іванова Л.В.					

Зміст

ВСТУП

Сталий розвиток інформаційних технологій супроводжується зростанням кількості користувачів та обсягів обробки даних. Системи, що обробляють великі обсяги запитів, є значною частиною сучасної цифрової інфраструктури, що обслуговує мільйони користувачів одночасно. Оптимізація, шляхом використання сучасних апаратних рішень, є одним з важливих механізмів забезпечення стабільної роботи.

Апаратні рішення забезпечують доступність, надійність та продуктивність системи. Відсутність або їх неефективне використання може призвести до втрати даних, фінансових та репутаційних збитків.

Актуальність дослідження апаратних рішень, що забезпечують відмовостійкість комп'ютерних мереж, обумовлена необхідністю оптимізації роботи систем при обробці запитів великої кількості користувачів та забезпечення відмовостійкості систем в умовах часткових відмов компонентів.

Технічне завдання полягає у проведенні аналізу апаратних рішень, які є актуальними, застосованими та ефективними для вирішення проблем при обробці запитів великої кількості користувачів. Потрібно розглянути різні рішення, змоделювати різні сценарії роботи системи, оцінити ефективність в умовах високих навантажень та часткової відмови вузлів системи, комутаторів, каналів. Враховуючи, що немає єдиного вірного чи універсального рішення, яке ефективно у всіх випадках, необхідно буде оцінювати специфіку різних систем, потрібного рівня швидкодії, відмовостійкості та інших факторів. Можливо для простих систем буде достатньо рішень, що лежать на поверхні. В той же час для більш складних систем, де навантаження може бути нестабільним, непередбачуваним, більш ефективними можуть виявитися рішення, які є більш нетривіальними.

У результаті очікується отримати обґрунтовані рішення щодо вибору апаратних рішень для збереження стійкості роботи комп'ютерних систем, визначивши найбільш відповідні варіанти в залежності від можливостей та цілей.

1 ОСНОВНИЙ РОЗДІЛ

1.1 Апаратні рішення для забезпечення відмовостійкості

Почати огляд апаратних рішень для забезпечення відмовостійкості пропоную з найбільш вживаних та економічно вигідних рішень. Обґрунтувати їх найбільш легко, так як вони є дешевшими за інші рішення, їх можливо швидко змінити, якщо вони вийшли з ладу чи застаріли та вони не потребують поглиблення знань для інтеграції у існуючу систему.

Резервні джерела живлення

Дубльовані блоки живлення - використання кількох блоків живлення у одному серверному стенді або сервері дозволяє забезпечити безперебійну роботу, у разі відмови одного з блоків живлення, сервер одразу перейде на живлення з іншого блоку. Так як сучасні блоки живлення працюють паралельно. Сучасні сервери зазвичай оснащені двома або більше блоками живлення.

Джерела безперебійного живлення (UPS) - пристрої, що забезпечують тимчасове живлення у разі відключення основного джерела електропостачання. Вони можуть захищати прилади від перепадів напруги та інших проблем з мережею.

Рисунок 1.1. Приклад джерела безперебійного живлення

Резервні електрогенератори - можливо застосовувати дизельні або газові електрогенератори, що забезпечують тривале автономне електропостачання, у разі відключення електропостачання.

1.1.1 Відмовостійкі системи зберігання даних

RAID-масиви - технологія, що забезпечує об'єднання багатьох дисків в єдиний масив, що дає можливість підвищити надійність зберігання даних, шляхом запису даних одразу на декілька носіїв. Тому у разі відмови одного з дисків, можливо лише замінити його та система буде функціонувати так само, так як дані продубльовані на іншому носії.

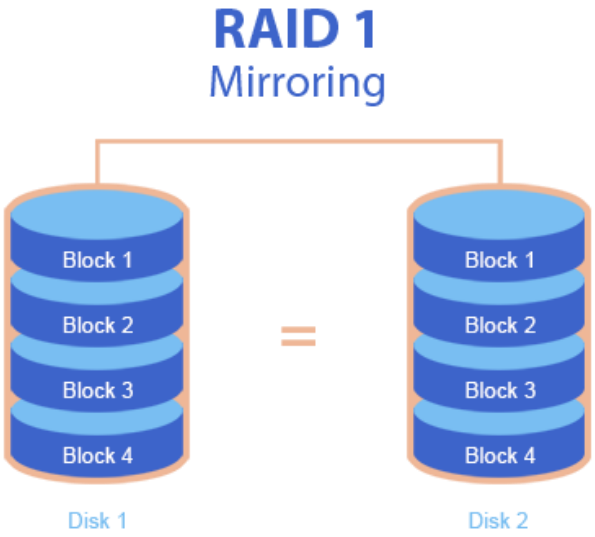


Рисунок 1.2. Приклад RAID 1 массиву

1.1.2 Відмовостійкі обчислювальні системи

Кластерні системи - це група незалежних пристроїв, що працюють разом для підвищення надійності, швидкості та доступності системи. У разі, якщо один з вузлів виходить з ладу, то система автоматично перерозподіляє навантаження на інші. Існують декілька типів кластерних систем. Активно-активні кластери - усі

вузли одночасно обробляють запити, розподіляючи таким чином навантаження та активно-пасивні кластери. Активно-пасивні кластери працюють за такою логікою: один вузол активний, інші очікують. Якщо з активним вузлом щось станеться, то інший вузол, що очікував, активується та бере на себе навантаження.

1.1.3 Спеціалізовані апаратні компоненти

ECC-пам’ять - пам’ять, що здатна виявляти та виправляти найпоширеніші пошкодження даних. Зазвичай використовують у системах, де критично важлива точність даних.

Відмовостійкі процесори - процесори, що працюють зазвичай одночасно та порівнюють свої дані для виявлення помилок. Навіть якщо один з процесорів повністю відключится, то інший все одно буде працювати. Такі процесори зазвичай використовують у системах, де потрібні надзвичайно високі показники доступності системи, на рівні 99,999%. Прикладами таких систем є банківська справа, торгівля на фондових біржах, служби екстреної допомоги, авіація.

1.1.4 Відмовостійкі мережеві рішення

Резервування мережевих з’єднань - рішення, що використовує декілька мережевих адаптерів та фізичних з’єднань задля забезпечення безперебійного зв’язку, навіть у разі відмови одного з компонентів мережі.

Відмовостійкі мережеві комутатори - можуть мати блоки резервного живлення, модулі управління та порти, що загалом забезпечують безперервну роботу мережі. Сучасні комутатори підтримують технології, що дозволяють з'єднати кілька окремих фізичних пристрої у один логічний.

1.1.5 Системи охолодження

Системи охолодження є критично важливими для забезпечення стабільної роботи. Вентилятори, кондиціонери та системи рідинного охолодження, всі вони забезпечують стабільну температуру при роботі обладнання. Саме обладнання оснащують датчиками температури, що дозволяє автоматично регулювати інтенсивність охолодження у разі зміни навантаження.

1.2 Проєктування моделі відмовостійкої мережі

1.2.1 Основні принципи відмовостійкості

Для проектування власної моделі відмовостійкої мережі, необхідно спочатку визначити принципи, яких ми будемо дотримуватися для забезпечення відмовостійкості. Я виділю основні принципи, що використовують зазвичай.

1. Надлишковість. Суть у дублюванні усіх компонентів для стабільної роботи навіть у випадку відмови частини з них.
2. Ізоляція відмов. Обмежити розповсюдження відмови до мінімального набору компонентів, задля уникнення каскадних збоїв
3. Швидке відновлення. Необхідно врахувати механізм швидкого опрацювання відмов і переключення на резервні системи, компоненти чи шляхи
4. Моніторинг та управління. Постійний контроль за станом мережі для виявлення можливих проблем, їх передбачення та швидкого реагування.

1.2.2 Рівні відмовостійкості в мережі

Принципи, що я зазначив вище, можливо використати на різних рівнях мережевої моделі. Розберемо кожен рівень та найвірогідніші рішення, що ми можемо застосувати на ньому.

1. Фізичний рівень

- Надлишковість кабелів. Ми можемо використати декілька різних фізичних кабелів, що будуть з’єднувати важливі пристрої

- Надлишковість обладнання. Ми можемо забезпечити резервні джерела живлення, мережеві інтерфейси, модули комутаторів/маршрутизаторів

- Географічна рознесеність. Можливо розмістити критично важливе обладнання у різних будівлях, дата-центрах, країнах.

2. Канальний рівень

- Link Aggregation (LAG/LACP/EtherChannel): Об'єднання кількох фізичних каналів в один логічний для підвищення пропускної здатності та забезпечення відмовостійкості. Якщо один фізичний канал виходить з ладу, трафік переходить на інші.

- Spanning Tree Protocol (STP/RSTP/MSTP): Запобігання петлям у мережі та забезпечення резервних шляхів. Хоча STP може бути повільним, RSTP та MSTP значно прискорюють конвергенцію.

- Virtual Router Redundancy Protocol (VRRP/HSRP/GLBP): Забезпечення відмовостійкості шлюзів за замовчуванням. Кілька маршрутизаторів працюють як єдиний віртуальний шлюз.

3. Мережевий рівень

- Динамічна маршрутизація. Використання протоколів, наприклад BGP, що дозволяють маршрутизаторам автоматично виявляти зміни у топології мережі та коригувати маршрути трафіку.

- Резервні маршрутизатори. Використання декількох маршрутизаторів у кожній критичній точці мережі

- Multi-homing. Підключення до декількох інтернет-провайдерів для забезпечення безперебійного доступу до інтернету, у разі відмови одного з них .

4. Транспортний та Прикладний рівень

- Балансування навантаження. Розподіл трафіку за допомогою балансувальника на пулу серверів, що опрацьовують запити користувачів. У разі відмови або перенавантаження окремих серверів, інші сервери можуть брати на себе більшу частку запитів (в залежності від налаштувань балансувальника).

- Кластеризація. Групування серверів у кластери, що дозволяє їм спільно працювати та заміняти один іншого, у разі виходу з ладу.

- Резервне копіювання та відновлення. Регулярне створення резервних копій даних та систем, щоб мати можливість завантажити їх на інше обладнання та швидко відновити роботу.

Рисунок 1.3. Візуалізація рівнів моделі OSI

1.2.3 Архітектурні моделі відмовостійкої мережі

Існують різні топології мереж, що мають свої переваги та недоліки. Розберемо найпоширеніші з них.

1. Зіркова топологія з резервуванням. Має у центрі два або більше маршрутизатори, які працюють у парі. Кожен кінцевий пристрій або сегмент підключається до обох центральних пристроїв. З переваг ми маємо

легкість та швидкість налаштування та розширення. Недоліком є те, що центральний вузол може стати точкою відмови, якщо немає належного резервування.

2. Кільцева топологія. Кожен вузол у цій топології має з’єднання з двома сусідніми вузлами, що утворює кільце з’єднань. З переваг ми маємо автоматичне відновлення шляху у випадку відмови одного каналу або вузла. До недоліків відносится те, що відмова може розділити мережу на дві частини, якщо немає вторинного кільця.
3. Сіткова топологія. Кожен вузол з’єднаний з декількома іншими вузлами, що надає високу відмовостійкість, але має дорогу та складну реалізацію, якщо працюємо з розгалуженою мережею. З переваг маємо високу відмовостійкість, за рахунок кількості резервних шляхів. До недоліків відносится висока вартість та складність реалізації та управління. Щоб знайти компроміс між відмовостійкістю та вартістю іноді використовують часткову сітку, коли лише деякі вузли з’єднані у сітку.
4. Деревоподібна топологія з резервуванням. Ознаками є кілька кореневих комутаторів/маршрутизаторів, кілька рівнів доступу/розподілу, кожен з яких має резервні з’єднання до вищих рівнів. Завдяки резервуванню забезпечує високу відмовостійкість, має високу масштабованість завдяки легкому розумінню продуктивності системи. Недоліками є вища вартість, через потребу в надлишковому обладнанні та може бути складною у конфігурації, так як потрібно врахувати усі вузькі місця та можливі мережеві петлі.

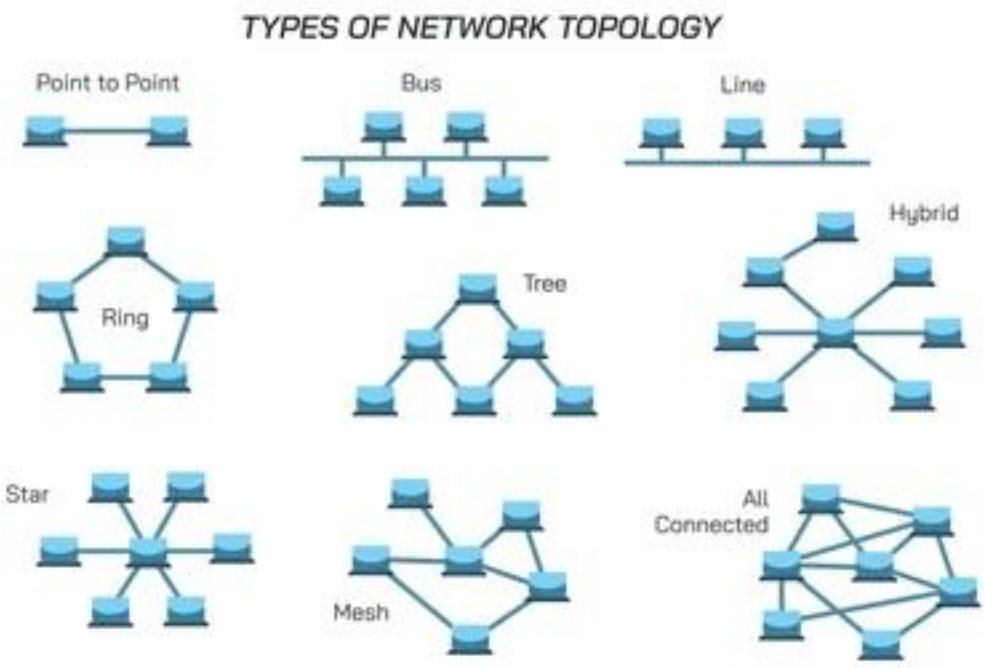


Рисунок 1.4. Мережеві топології

1.2.4 Власна модель відмовостійкої мережі

Для побудування власної моделі я керуюсь переліченими архітектурними рішеннями:

- Подвійне кільце. Основне та резервне кільце, що надає максимальну надлишковість.
- 5 вузлів, що з’єднані у кільцеву структуру.
- Автоматичне перемикання на резервні шляхи при відмовах.

Реалізовані принципи відмовостійкості:

- Надлишковість. Кожен вузол має 2 шляхи з’єднання.
- Ізолія відмов. Відмова одного з вузлів не вплине на роботу усієї мережі.
- Швидке відновлення. У разі відмови, трафік автоматично перенаправляется через альтернативні шляхи
- Моніторинг. Візуальний контроль стану всіх компонентів

1.3 Опис використаного ПЗ для моделювання

Для моделювання власної моделі мережі я використовував программу Packet Tracer. Я обрав це ПЗ, так як це ефективний спосіб моделювання мереж, який дозволяє експериментувати з різними конфігураціями, протоколами та пристроями без потреби у фізичному обладнанні.

Для моделювання мережі я використав комутатори Cisco 2960. Це багатофункціональний комутатор другого рівня моделі OSI, який чудово підходить для вивчення та моделювання мереж. Також я використав Комп'ютери, які є кінцевими пристроями, що генерують трафік та приймають його.

Я опрацював конфігурацію протоколу STP (Spanning Tree Protocol) та RSTP (Rapid Spanning Tree Protocol). Він є критичним для кільцевих топологій на комутаторах. Так як якщо би ми з'єднали комутатори у кільце без STP, то виникнув би широкомовний шторм, що призвев би до коллапсу мережі. STP блокує зайві шляхи, запобігаючи петлям та забезпечуючи єдиний основний шлях для передачі даних, при цьому дозволяючи мати резервний шлях, якщо щось вийде з ладу.

1.3.1 Переваги та недоліки Packet Tracer у порівнянні з GNS3

Packet Tracer є симулятором мережі, а GNS3 у свою чергу емулятором, вони мають різну природу розрахунку. Хоча і ці програми можуть здатися схожими, але вони мають різні цілі та переваги.

Переваги Packet Tracer:

1. Легкість використання. Packet Tracer має дуже інтуїтивно зрозумілий графічний інтерфейс. Ви можете швидко перетягувати пристрої, з'єднувати їх і починати конфігурувати. Для базових сценаріїв навчання мереж Packet Tracer не вимагає глибоких знань з віртуалізації чи операційних систем.

2. Низькі системні вимоги. Packet Tracer не запускає реальні образи операційних систем Cisco IOS. Він симулює їхню поведінку. Це означає, що він вимагає значно менше ресурсів процесора, оперативної пам'яті та дискового простору. Що надає можливість запустити досить велику мережу на відносно слабкому комп'ютері.
3. Візуалізація процесів. Packet Tracer має унікальний "Simulation Mode" (Режим симуляції), який дозволяє покроково відстежувати рух пакетів, їхні заголовки, зміни станів портів STP, роботу ARP та DNS. Це надзвичайно корисно для розуміння того, як саме працюють мережеві протоколи. GNS3 не має такої глибокої інтеграції на рівні візуалізації пакетів.
4. Підтримка широкого спектру пристроїв Cisco. Хоч це і симулятор, він підтримує більшість функцій маршрутизаторів, комутаторів, бездротових пристроїв та кінцевих пристроїв, які потрібні для вивчення основ мереж.

Чому GNS3 може бути менш зручним у цьому випадку:

1. Складність налаштування. GNS3 вимагає завантаження та інтеграції реальних образів Cisco IOS (IOS Images), що часто має проблему з ліцензуванням. Також потрібні знання з налаштування віртуальних машин (QEMU, VirtualBox, VMware) для запуску цих образів.
2. Високі системні вимоги. Оскільки GNS3 запускає реальні операційні системи, він споживає значно більше ресурсів комп'ютера. Запуск навіть кількох маршрутизаторів і комутаторів може сильно навантажити систему.
3. Обмежена підтримка комутаторів (на відміну від маршрутизаторів). Хоча GNS3 може емулювати деякі функції комутації через маршрутизатори з модулями комутації або інтеграцію з віртуальними комутаторами, це не завжди так повноцінно, як Packet Tracer для вивчення чисто комутаційних технологій, таких як STP, EtherChannel, наприклад на тих самих комутаторах 2960, що ми використовували. Packet Tracer імітує конкретну модель.

4. Менш візуальний. GNS3 є більш "інженерним" інструментом. Хоча він дозволяє будувати топології, у нього немає вбудованих інструментів для такої детальної візуалізації руху пакетів, як у Packet Tracer.

1.4 Моделювання роботи мережі в умовах відмов

Пропоную змоделювати дві варіації кільцевої топології, без подвійного кільця та з ним. Таким чином ми можемо отримати дані для порівняння апаратних рішень, оцінити кожен з варіантів, їх переваги та недоліки.

1.4.1 Моделювання роботи кільцевої топології без подвійного кільця в умовах відмов

Почнемо з кільцевої топології без подвійного кільця. Ось як виглядає топологія у програмі Packet Tracer

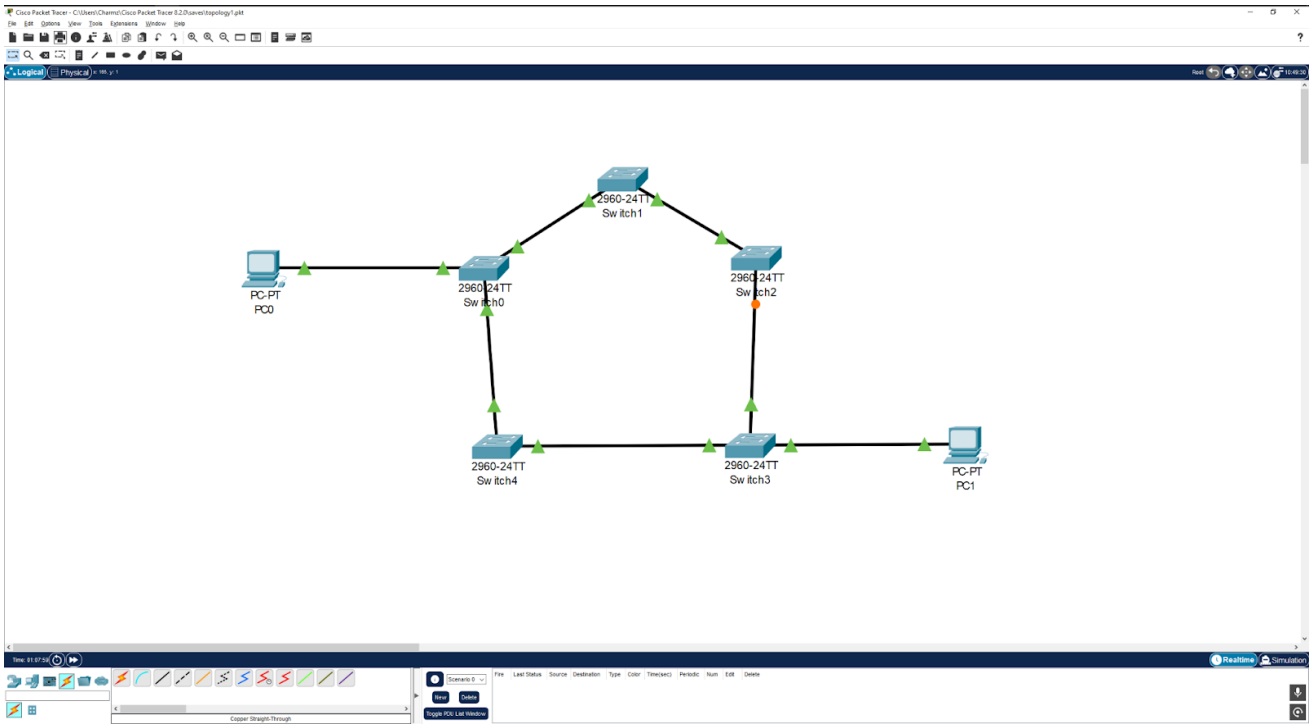


Рисунок 1.5. Кільцева топологія у Cisco Packet Tracer

Для тестування відмови ми будемо використовувати розділ симуляції, який дозволяє побачити як рухаються пакети протягом часу. Виконаємо команду ping 192.168.1.3 (PC1), щоб протестувати чи все працює.

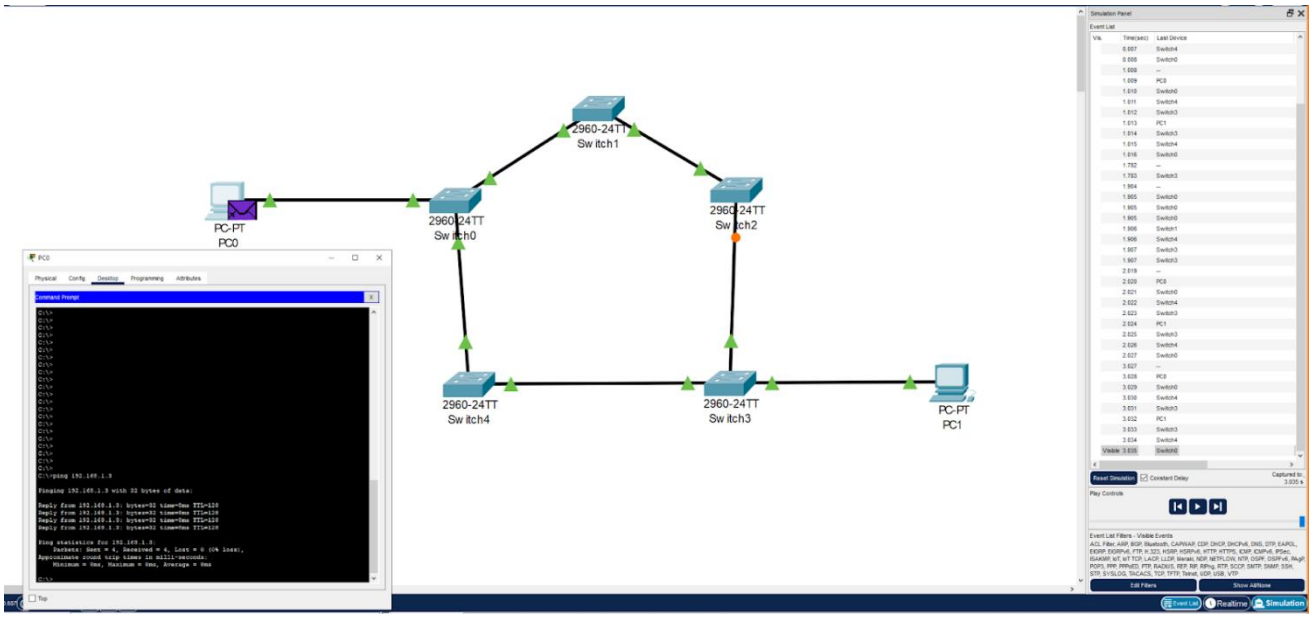


Рисунок 1.6. Виконання команди ping у Cisco Packet Tracer

Маємо такі результати у вікні командного рядку:

- Відправлено 4 пакети (Packets: Sent = 4, Received = 4, Lost = 0), що вказує на 100% успішність доставки.
- Час відповіді: Minimum = 8мс, Maximum = 8мс, Average = 8мс, що свідчить про дуже низьку затримку та стабільне з’єднання.
- Приклади відповідей: "Reply from 192.168.1.3: bytes=32 time<1ms TTL=128", що підтверджує коректну роботу мережі.

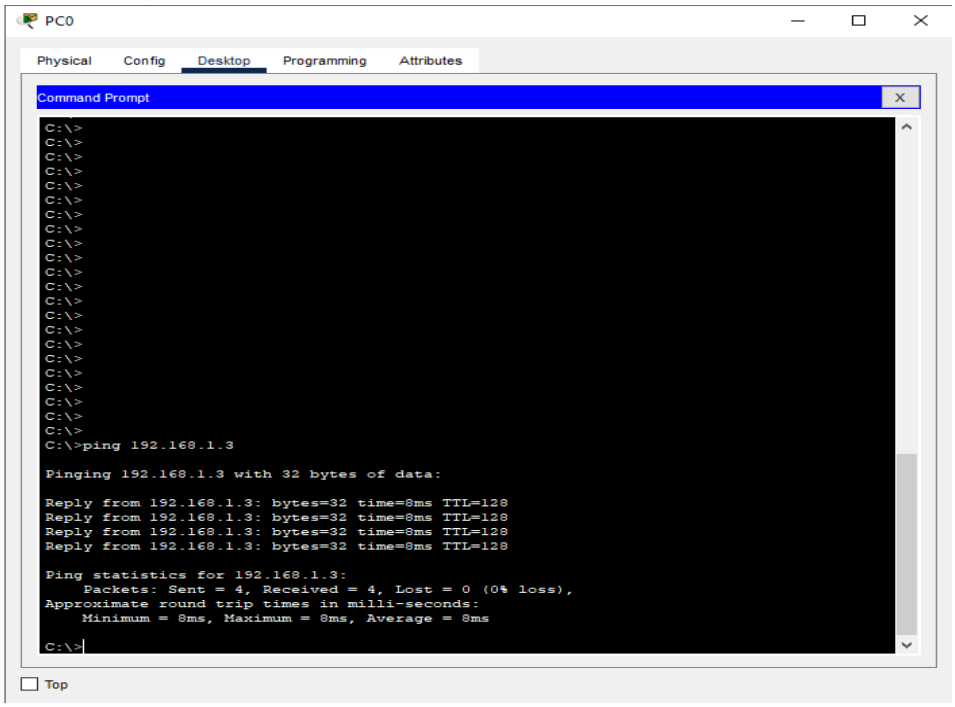


Рисунок 1.7. Командний рядок PC0 у Cisco Packet Tracer

Мережа функціонує коректно, оскільки немає втрати пакетів, а затримка мінімальна. Отже, тести показали, що мережа налаштована правильно, і між PC0 та PC1 існує стабільне з’єднання без збоїв.

Змоделюємо відмову одного з каналів, наприклад між Switch4 та Switch3, для цього оберемо інструмент видалення, який активізується за допомогою кнопки DEL, та натиснемо на лінію зв’язку між двома комутаторами.

Чому я обрав саме цей канал? Тому що, якщо звернути увагу на результати минулого тестування, то саме через маршрут Switch0 - Switch4 - Switch3 йшли запити, в той же час інший маршрут простоював. Якщо би ми видалили інший канал, який є надлишковим, то нічого би не змінилось. Тому зараз ми симулюємо обрив каналу та подивимось як реагує мережа.

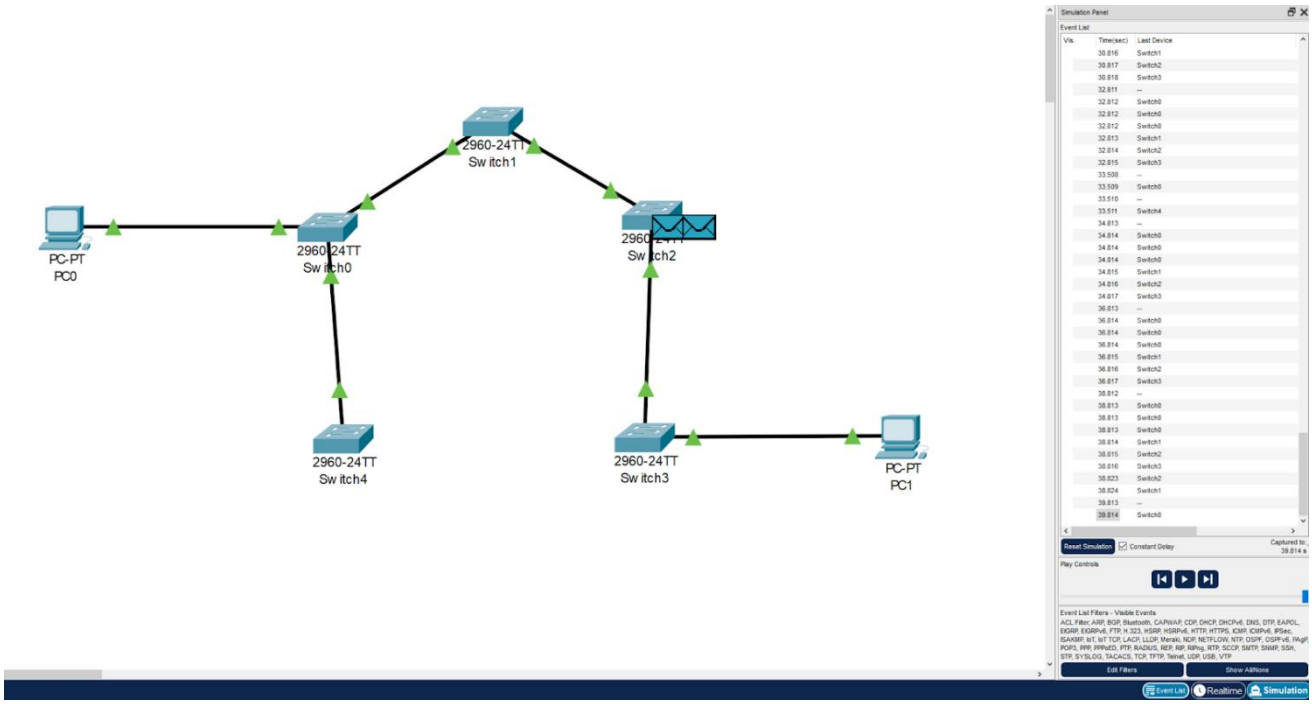


Рисунок 1.8. Топологія з видаленим каналом

Бачимо, що неактивний канал між Switch2 та Switch3 став активним протягом 40 секунд. Розберемо затримку та її причини

Час конвергенції STP: Затримка 40 секунд пов’язана з процесом конвергенції STP. За замовчуванням стандартний STP (IEEE 802.1D) має два ключові таймери:

- Hello Time (2 секунди): інтервал, з яким комутатори надсилають BPDU.
- Max Age (20 секунд): час, протягом якого комутатор чекає оновлення BPDU, перш ніж вважати зв’язок недійсним.
- Forward Delay (15 секунд): час, протягом якого порт перебуває в стані "Listening" і "Learning", перш ніж стати активним ("Forwarding").
- Загальна затримка може складатися з Max Age + 2 × Forward Delay ≈ 20 + 2 × 15 = 50 секунд у гіршому випадку.

Протестуємо чи проходить ping між комп’ютерами.

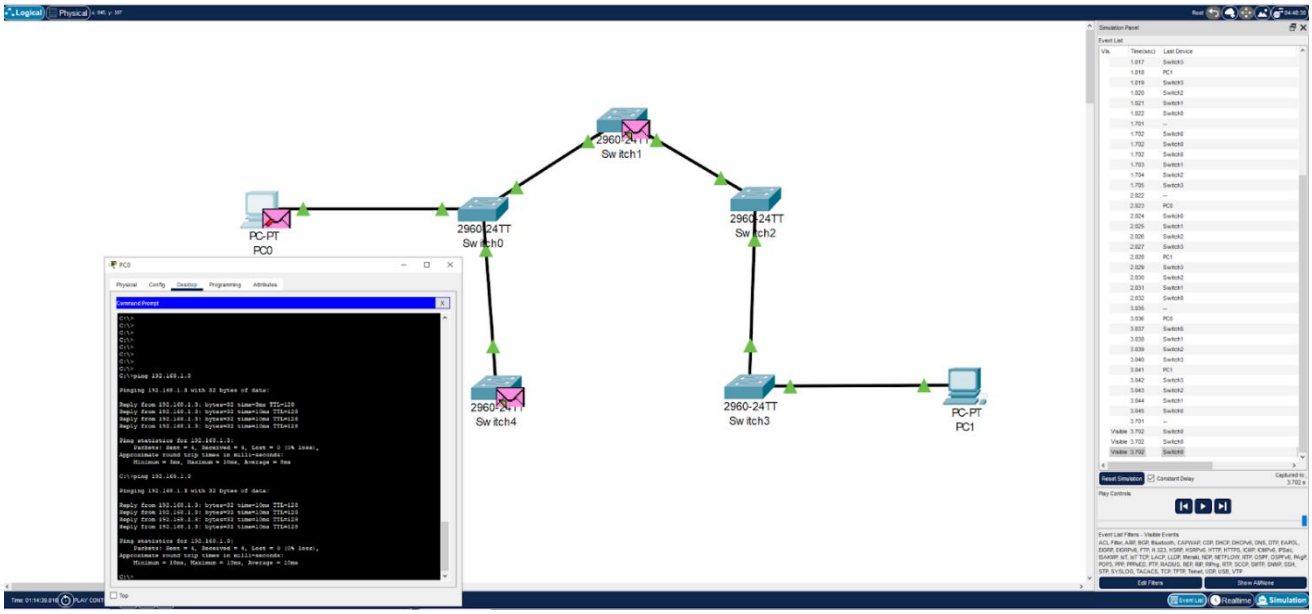


Рисунок 1.9. Успішна відповідь на ping

За результатами тесту бачимо, що ping проходить та втрати пакетів немає. Це свідчить про коректну роботу мережі.

1.4.2 **Моделювання роботи кільцевої топології з подвійним кільцем в умовах відмов**

Створимо друге кільце за допомогою кабелю “Cooper Straight-Through”, який ми обираємо на панелі керування. Тепер мережа у Packet Tracer виглядає ось так.

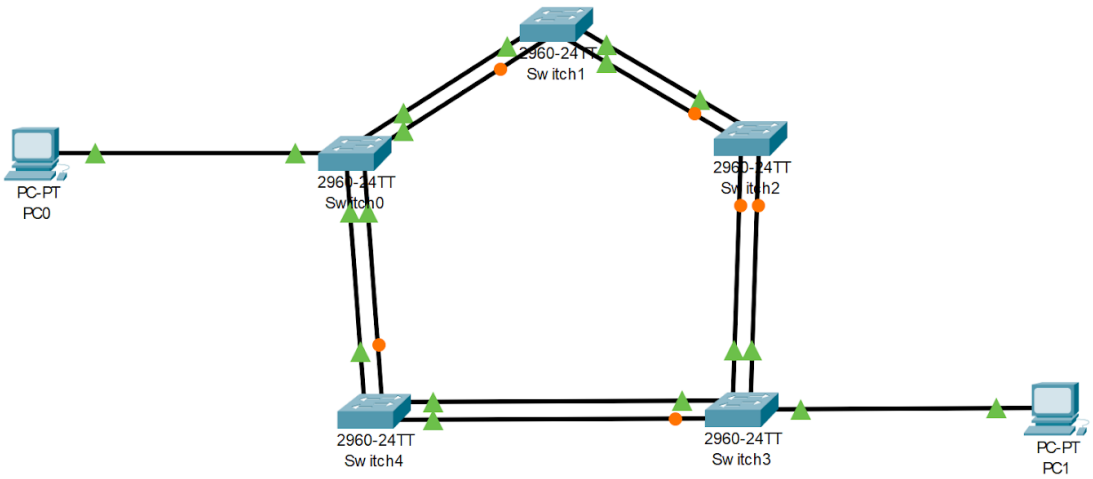


Рисунок 1.10. Топологія після додавання другого кільця

Маємо заблоковані надлишкові порти, що блокує STP. Це можливо перевірити за допомогою команди show spanning-tree на будь-якому комутаторі.

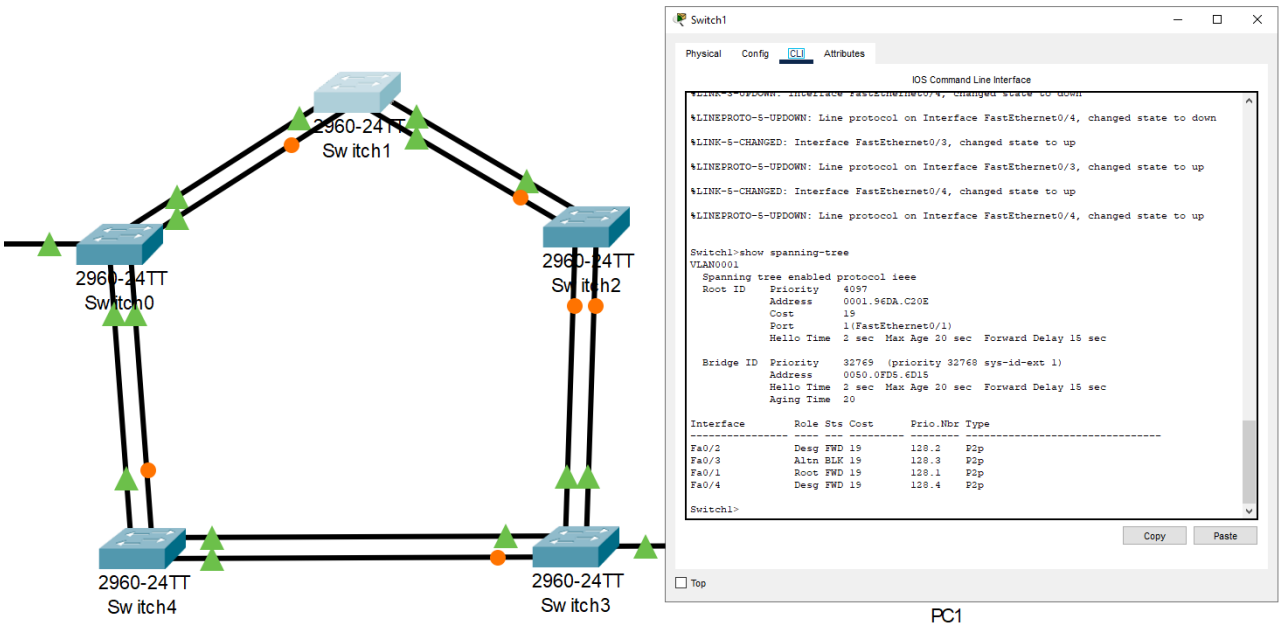


Рисунок 1.11. Заблоковані STP порти

Це відбувається так як мережа має петлі, STP автоматично виявляє їх та блокує порти щоб запобігти їм.

Почнемо тестування, наприклад приберемо той самий шлях між Switch4 та Switch3, щоб зафіксувати зміни.

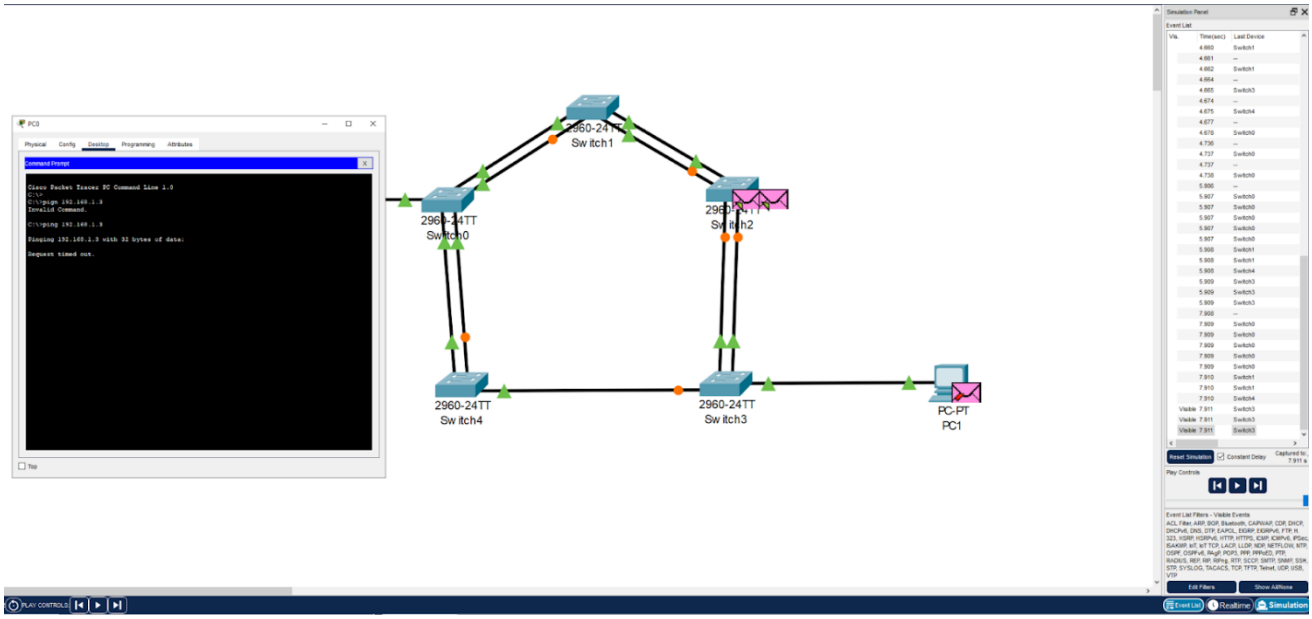


Рисунок 1.12. Топологія з імітацією втраченого каналу

Бачимо, що ping не пройшов, так як одразу після видалення каналу між комутаторами протокол STP ще не встиг оновити маршрут та активувати резервний канал. Якщо ж ми почекаємо 30-50 секунд, то все відновится та отримуємо результат як на рисунку № 1.13

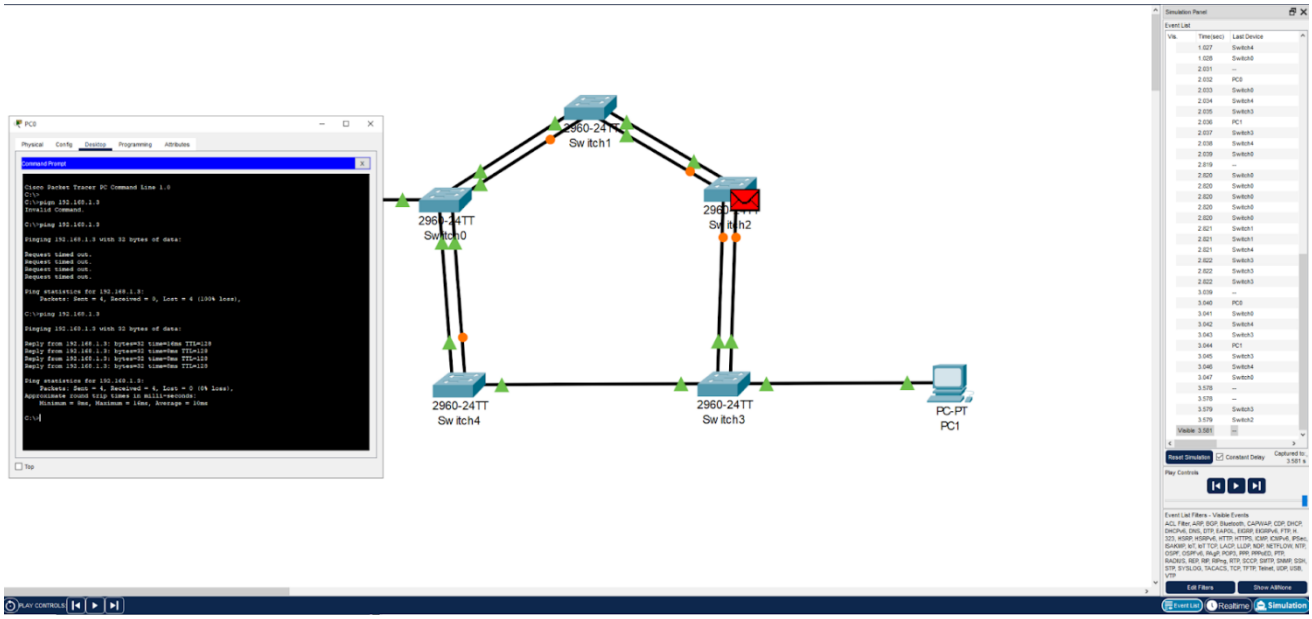


Рисунок 1.13. Мережа після відновлення

Тепер зробимо більш критичну ситуацію та подивимося як система буде працювати. Повністю видалимо Switch1, та приберемо перший канал між Switch0 та Switch4. Таким чином ми симулюємо відмову одного з вузлів та каналу зв’язку.

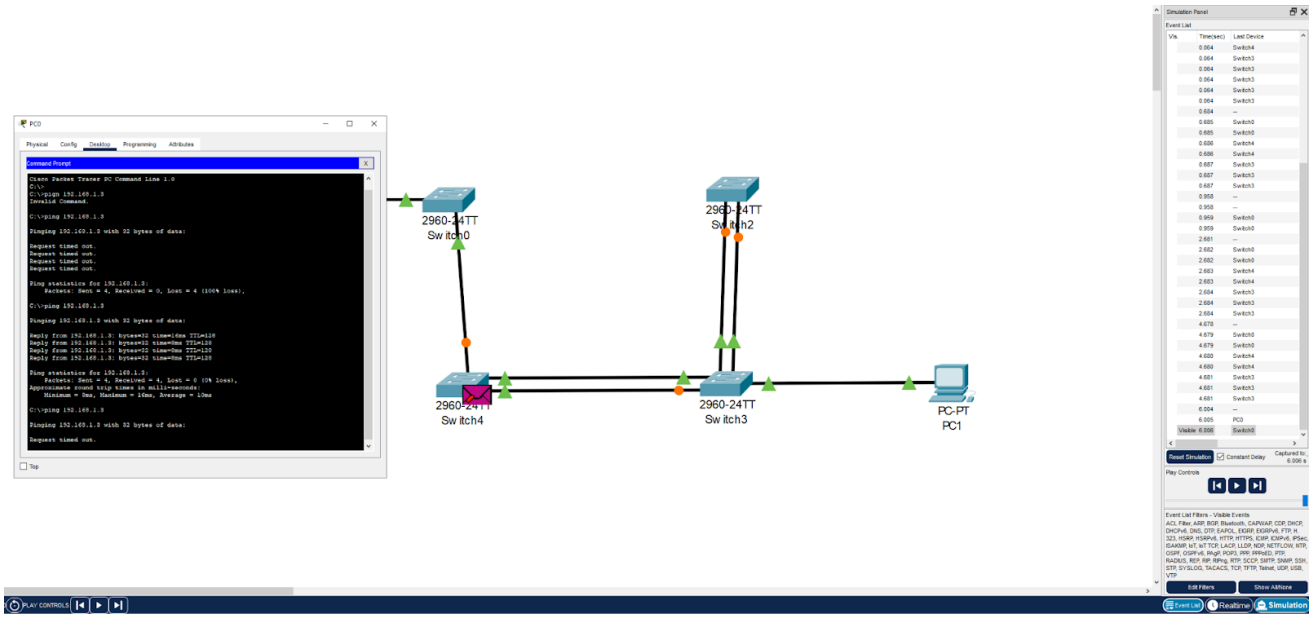


Рисунок 1.14. Топологія з видаленим Switch1

Бачимо ситуацію, як і з минулим видаленням каналу. STP не встиг опрацювати відмову та ping не пройшов. Якщо ж ми почекаємо, то мережа автоматично відновится.

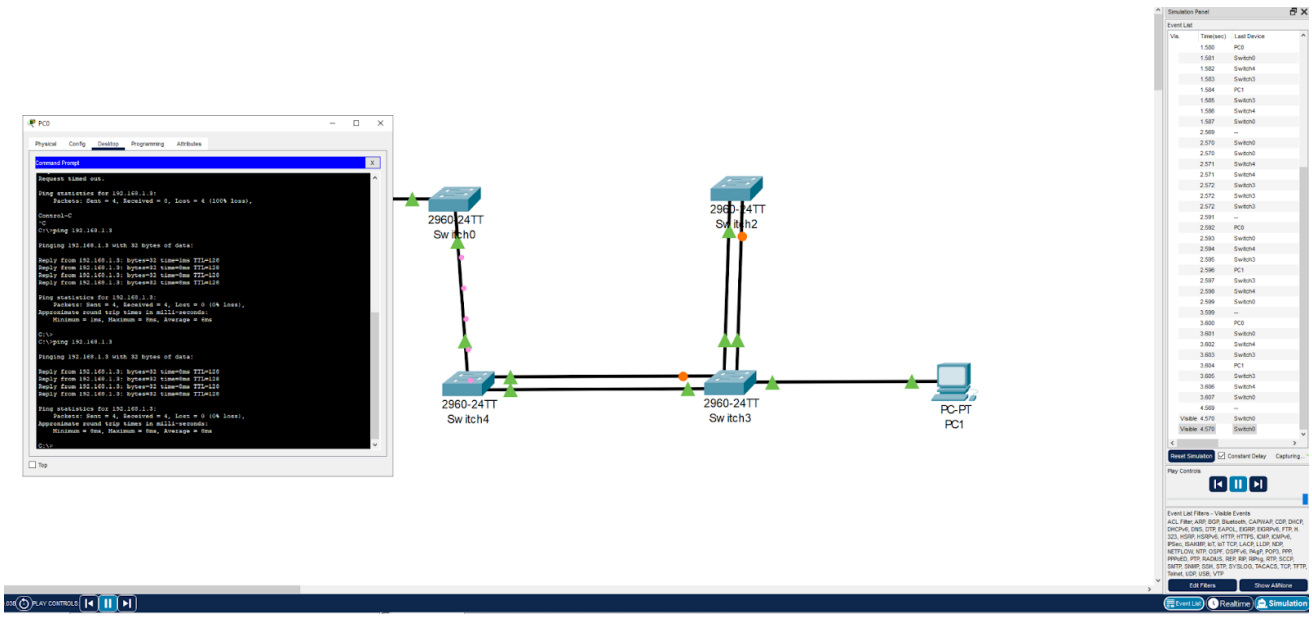


Рисунок 1.15. Відновлення мережі після видалення Switch1

1.4.3 Моделювання роботи кільцевої топології з подвійним кільцем в умовах відмов, використовуючи RSTP

Виходячи з минулих тестувань ми отримали інформацію, що у нашому випадку проблемою є час відновлення резервних каналів. Коренем цією проблеми є використання STP, що хоч і захищає від мережевих петель, але водночас спричиняє суттєві затримки під час перемикання каналів. У випадку відмови основного каналу, мережі потрібно занадто багато часу щоб відновити роботу, що має критичне значення при побудові відмовостійких мереж. Для вирішення цієї проблеми потрібно розглянути сучасну альтернативу STP, а саме RSTP (Rapid Spanning Tree Protocol).

З огляду на необхідність скорочення часу відновлення резервних каналів, RSTP є оптимальним вибором. Порівнюючи його з STP, RSTP був розроблений з акцентом на швидку конвергенцію. Це дозволяє швидко відновлювати з’єднання, що є критичним для сучасних мереж.

Основні відмінності RSTP від STP:

1. Швидка конвергенція:

- STP: Використовує таймери (Listening, Learning), які можуть затримувати перехід порту в стан пересилання трафіку зазвичай на 30-50 секунд.
- RSTP: Значно прискорює цей процес, дозволяючи портам переходити в стан пересилання практично миттєво (зазвичай менше 1 секунди) у багатьох сценаріях. Це досягається завдяки новим типам портів та механізмам пропозиції/угоди (Proposal/Agreement).

2. Нові стани портів:

- STP: Має 5 станів портів (Blocking, Listening, Learning, Forwarding, Disabled).
- RSTP: Скорочує кількість станів до 3:

    - Discarding: Об'єднує стани Blocking, Listening та Learning, не пересилає дані, не вивчає MAC-адреси.

- Learning: Не пересилає дані, але вивчає MAC-адреси.

- Forwarding: Пересилає дані, вивчає MAC-адреси.

Таке спрощення та об'єднання дозволяє прискорити переходи між станами.

3. Типи портів RSTP:

- Root Port (Кореневий порт): Порт, що забезпечує найкоротший шлях до кореневого моста.

- Designated Port (Призначений порт): Порт, що пересилає трафік для сегмента мережі.

- Alternate Port (Альтернативний порт): Порт, який блокується, але має резервний шлях до кореневого моста. Готовий до негайного переходу в Forwarding стан у разі відмови основного шляху. Це ключова відмінність, що забезпечує швидке відновлення.

- Backup Port (Резервний порт): Використовується на сегментах, де один комутатор має декілька підключень до одного сегмента. Блокується, але також готовий до швидкого переходу.

4. Механізм Proposal/Agreement (Пропозиція/Угода): RSTP використовує цей механізм для швидкої конвергенції при змінах топології, якщо комутатор підключається до мережі або топологія змінюється, він може "запропонувати" сусіднім комутаторам швидко перейти в стан Forwarding, якщо вони згодні з цим шляхом. Це дозволяє уникнути очікування таймерів.

5. Edge Ports (Прикордонні порти): Порти, які підключаються безпосередньо до кінцевих пристроїв (ПК, сервери) і не повинні створювати петель. RSTP дозволяє налаштовувати такі порти як "edge ports". Ці порти переходять у стан Forwarding негайно, не чекаючи жодних таймерів. Це значно прискорює підключення нових пристроїв.

6. Швидке виявлення відмов: RSTP швидше виявляє відмову каналу або пристрою, оскільки використовує механізм "Hello" пакетів, що надсилаються частіше, і може швидше визначити втрату зв'язку.

Таблиця 1.1 Порівняння STP та RSTP

Характеристика	STP (802.1D)	RSTP (802.1w)
Стандартизація	IEEE 802.1D	IEEE 802.1w
Швидкість відновлення	Повільна (30-50 секунд)	Швидка (менше 1 секунди в ідеальних умовах)
Стани портів	Blocking, Listening, Learning, Forwarding, Disabled	Discarding, Learning, Forwarding
Виявлення збіжності	Таймери (Max Age, Forward Delay)	Повідомлення BPDU (proposal/agreement)
Типи портів	Root Port, Designated Port, Non-Designated Port	Root Port, Designated Port, Alternate Port, Backup Port
PortFast	Окрема функція/розширення	Інтегрована в протокол (Edge Port)
Використання BPDU	Періодична розсилка (Root Bridge)	Періодична розсилка (всіма комутаторами) та механізм heartbeat
Резервні шляхи	Не використовується активно для перемикання	Використовуються Alternate Port та Backup Port для миттєвого перемикання
Виявлення відмови	Залежить від тайм-аутів	Активне виявлення за допомогою BPDU та таймерів (hello timer)
Сумісність	Зворотна сумісність з RSTP	Сумісний зі STP (автоматично переходить в режим STP при виявленні STP-комутатора)
Призначення	Запобігання петлям у мережах Ethernet	Запобігання петлям зі швидшою збіжністю в сучасних мережах

Виходячи з проблеми, що полягає у тривалому часі відновлення каналі, що є надлишковими, резервними, RSTP є ідеальним рішенням. Архітектура цього протоколу та механізми його роботи спеціально розроблені щоб зменшити час простою.

Налаштуємо RSTP на всіх комутаторах, та зробимо необхідні тестування. Спочатку потрібно ввімкнути RSTP на кожному комутаторі (Switch0, Switch1, Switch2, Switch3, Switch4). Для цього використаємо команди:

- enable
- configure terminal
- spanning-tree mode rapid-pvst

Після цього можемо призначити головний та резервний комутатори, щоб ще оптимізувати мережу. Загалом це не є обов'язковим кроком у нашому випадку, так як мережа все одно обере головний комутатор самостійно, але якщо ми це зробимо вручну, то будемо мати більше контролю та розуміння мережі. Для цього ми виконаємо команду на головному та резервних комутаторах.

- spanning-tree vlan 1 priority 4096. На головному, наприклад Switch0.
- spanning-tree vlan 1 priority 8192. На резервному, наприклад Switch1.

Після виконання команд, можемо перевірити чи зміни запрацювали виконавши команду на Switch0 та Switch1

- show spanning-tree vlan 1

Як ми бачимо на малюнку №1.17, пріоритет у комутатора 4097, це свідчить про те, що налаштування успішно змінені.

Після вищевказаних змін, потрібно налаштувати порти, які пов'язують комутатори на режим point-to-point, щоб RSTP автоматично не намагався визначити який порт та не допустив помилку, що може спричинити затримки. Загалом налаштування портів є більш передбачуваним, так як ми самостійно все призначили. Ручне налаштування гарантує що все буде працювати швидко і стабільно. Для цього використовуємо команди:

- interface range fastethernet 0/1-9
- spanning-tree link-type point-to-point

Тепер подивимось, як це виглядає на комутаторі, використовуючи команду:

- show spanning-tree

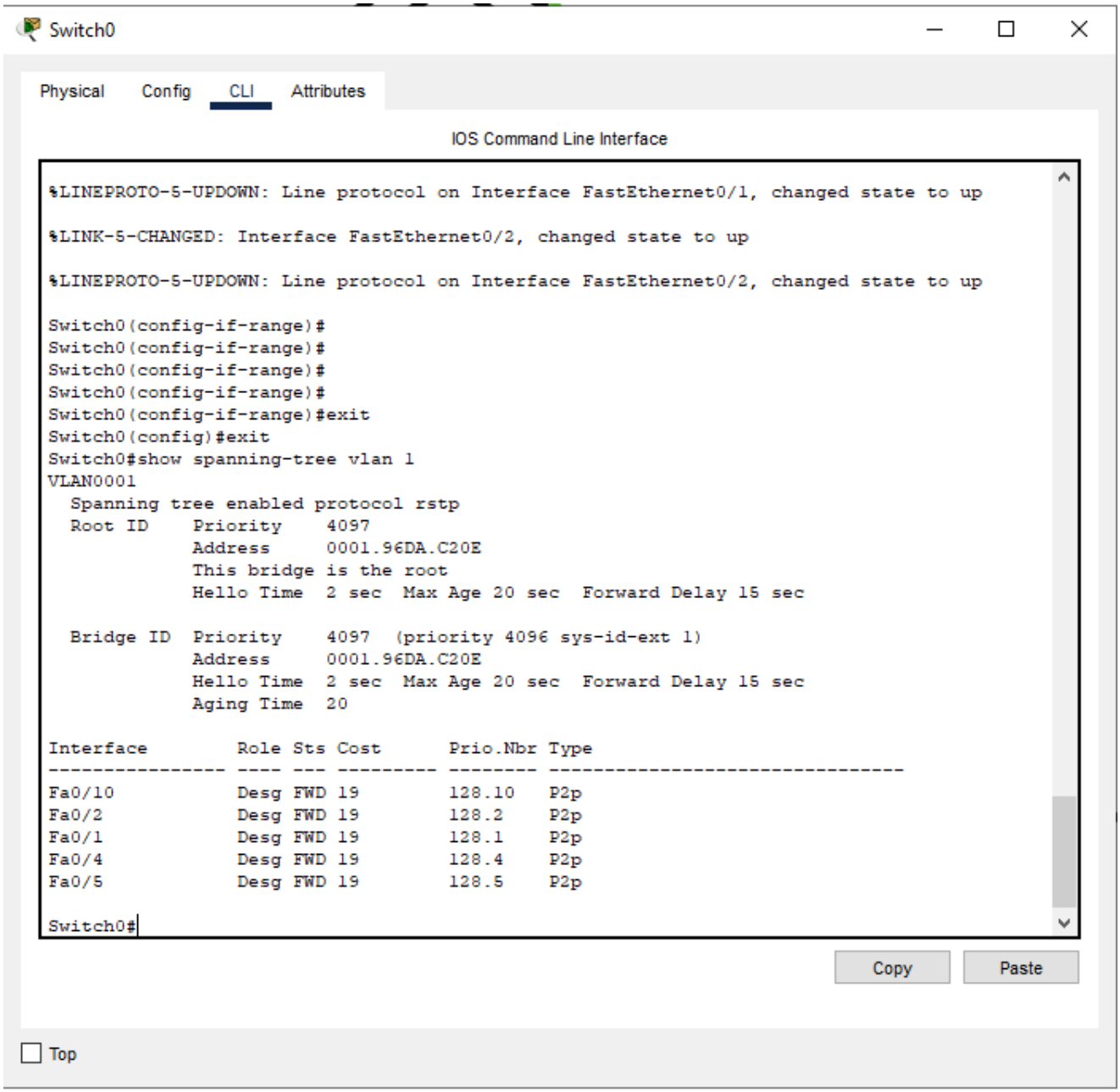


Рисунок 1.16. Налаштування spanning tree у комутатора Switch0

Бачимо, що всі порти мають Type P2p, що свідчить про те, що все добре. Також, для комп'ютера, що робить запити, що підключений у 10 порт, який не був вручну налаштован на P2p, ми бачимо, що RSTP також обрав тип P2p.

Після того, як ми зробили налаштування на інших комутаторах, почнемо тестування та фіксуємо що змінилося. Спочатку ми виконаємо команду ping, подивимося за яким маршрутом йшов запит та відключимо активні канали зв'язку. Зробимо це за допомогою режиму симуляції, метою тесту буде визначити чи змінилася швидкість активації резервних шляхів.

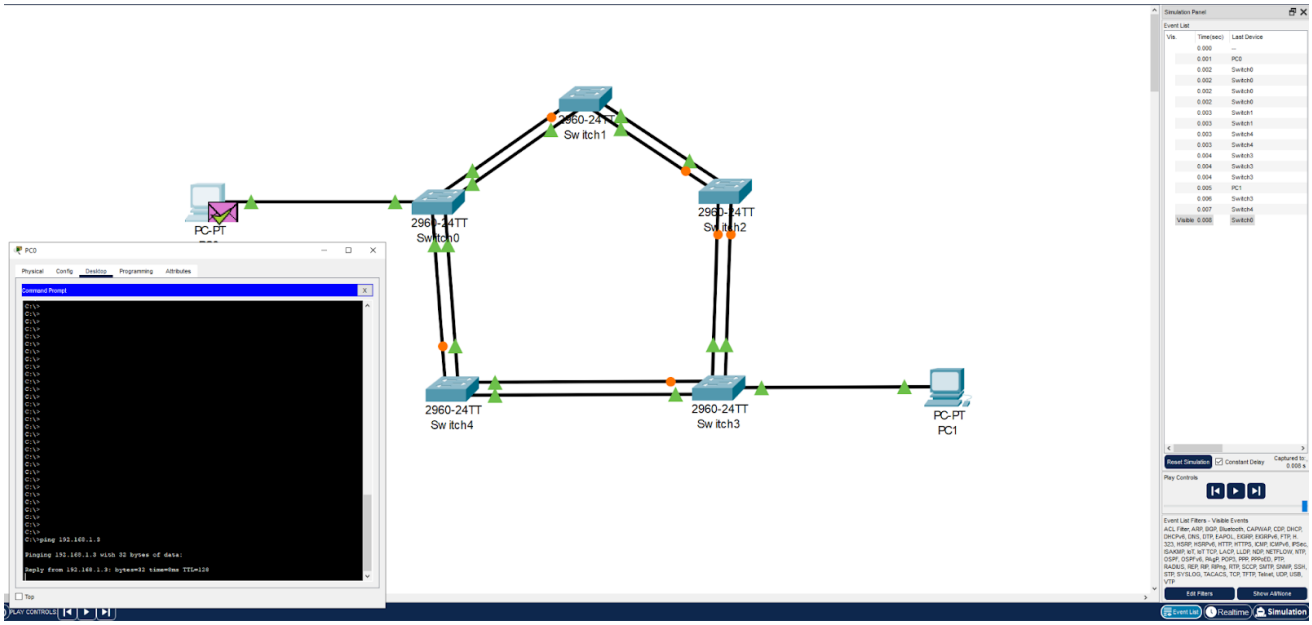


Рисунок 1.17. Надсилання запитів за допомогою ping на PC0

Відправлений ping з PC0 до PC1 пройшов по маршруту Switch0 - Switch4 - Switch3, вимкнемо порти на Switch4 та продовжимо симуляцію.

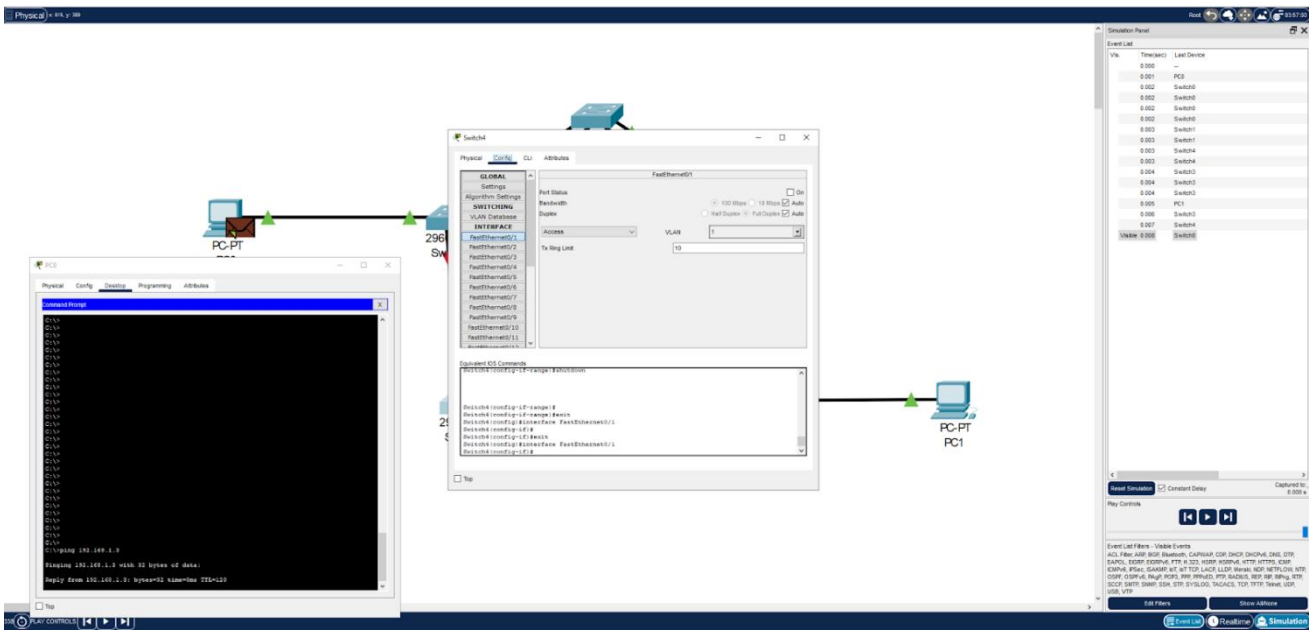


Рисунок 1.18. Вимкнені порти на Switch4 у налаштуваннях

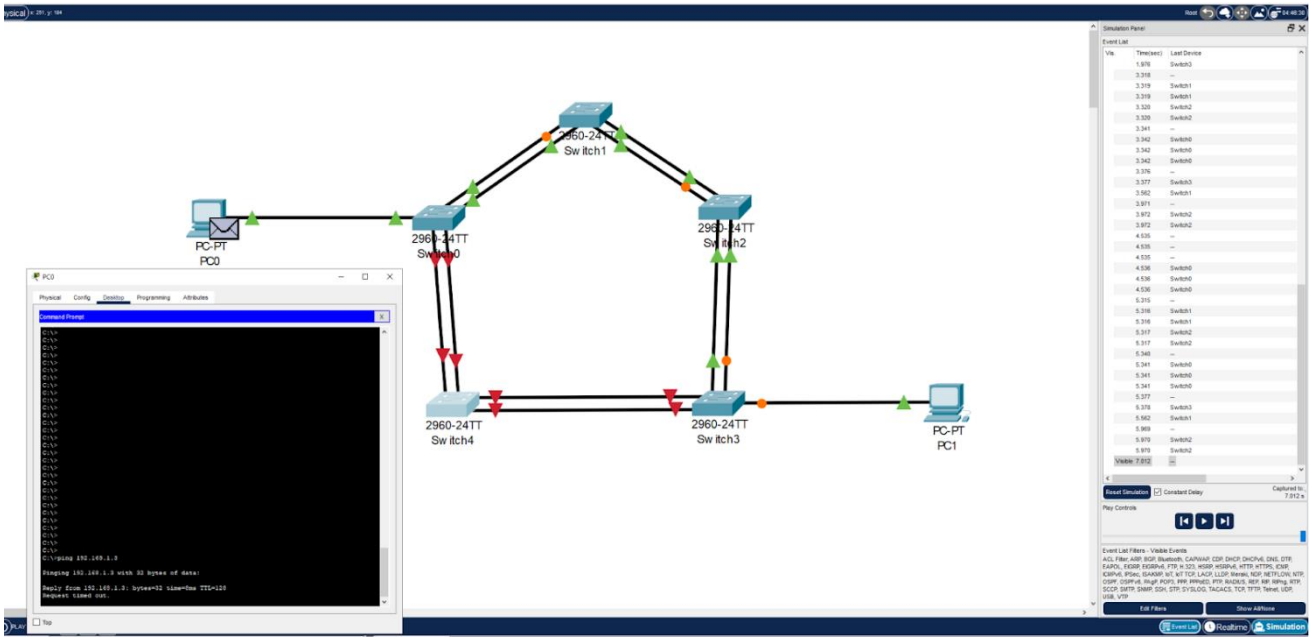


Рисунок 1.19. Вимкнені порти на топології

Бачимо, що за 7 секунд новий маршрут не вдалося встановити, тому час надсилання запитів сплинул. Повторимо надсилання запитів та фіксуємо коли відновиться зв’язок через резервний канал.

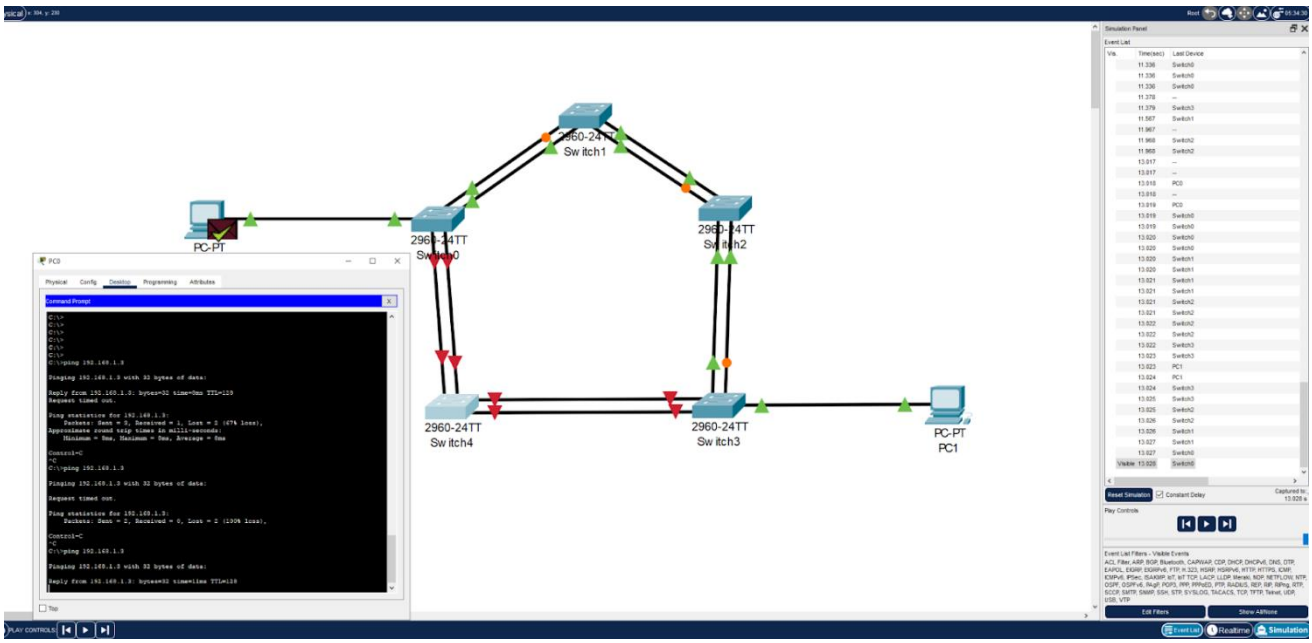


Рисунок 1.20. Відновлений зв’язок через 13 секунд

Як ми бачимо, зв’язок відновився через 13 секунд після втрати з’єднання з Switch4. Що свідчить про пришвидшення активації резервного каналу, але не є очікуваним. Провевши ще 3 тести у режимі симуляції, я отримав схожі результати.

Враховуючи, що RSTP не повинен так повільно працювати, я провів додаткові тестування та виявив, що режим симуляції має помилку, коли будь-який з пакетів викликає затримку, тому що “зависає” на непрацюючому комутаторі і наступний пакет чомусь не надсилається. Довести існування такої помилки можливо, якщо провести тестування у режимі Realtime у Packet Tracer, так як можливо побачити суттєву різницю у швидкості. Почнемо тестування у режимі Realtime:

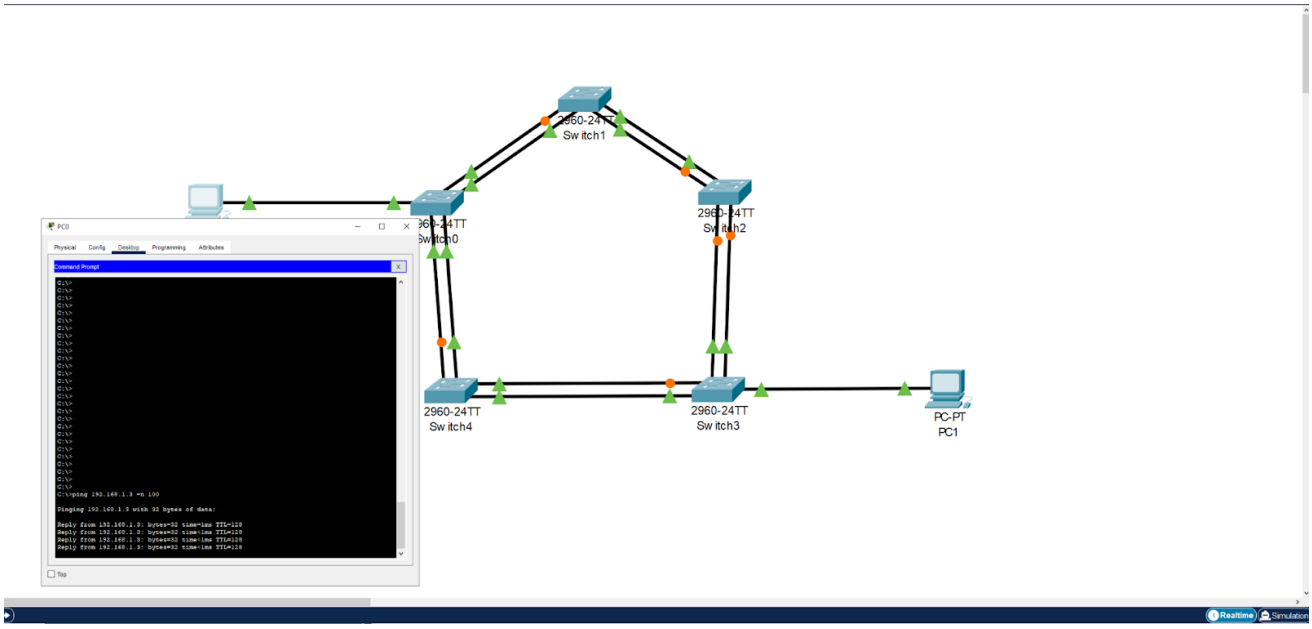


Рисунок 1.21. Симуляція у режимі Realtime

Після чого відключимо порти коммутатору Switch4:

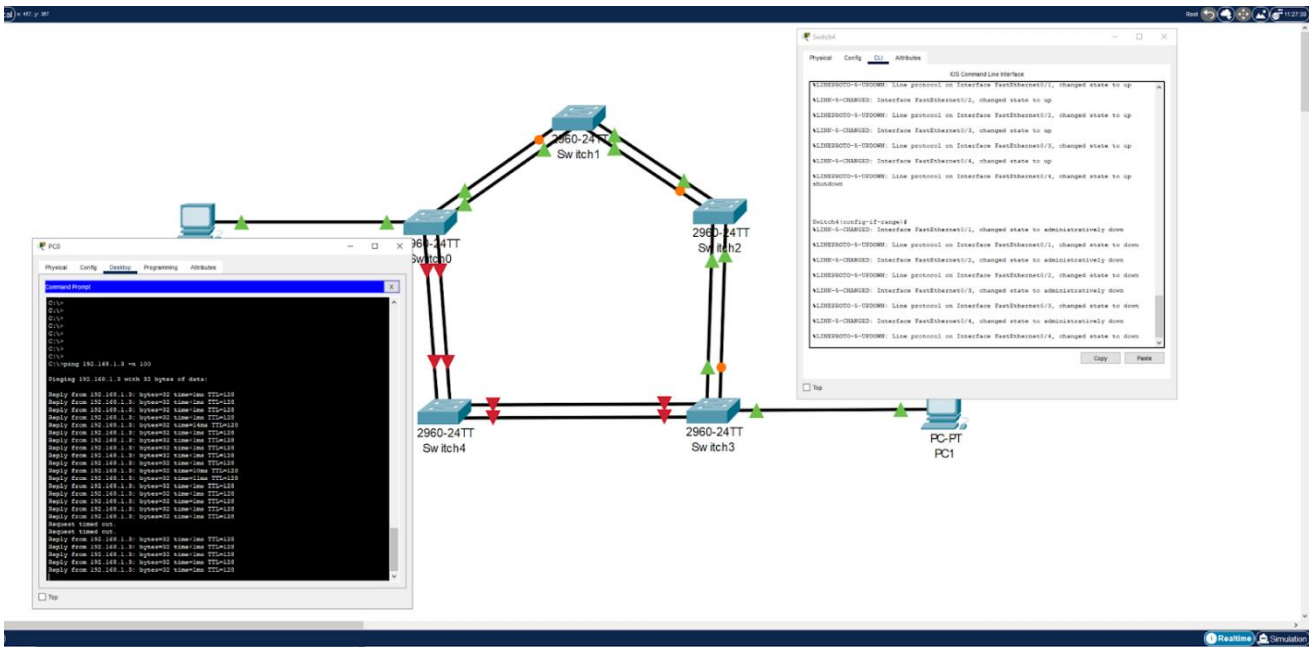


Рисунок 1.22. Відключення портів Switch4

Як ми бачимо, то усього 2 запити було втрачено. Враховуючи, що ми знаємо стандартну швидкість відправки запитів - 1 раз на секунду, то отримаємо результат у 2 секунди простою мережі. Проведемо контрольне тестування. Під час нього відключимо порти та підключимо їх обратно, щоб подивитися як працює мережа під час відновлення після збою.

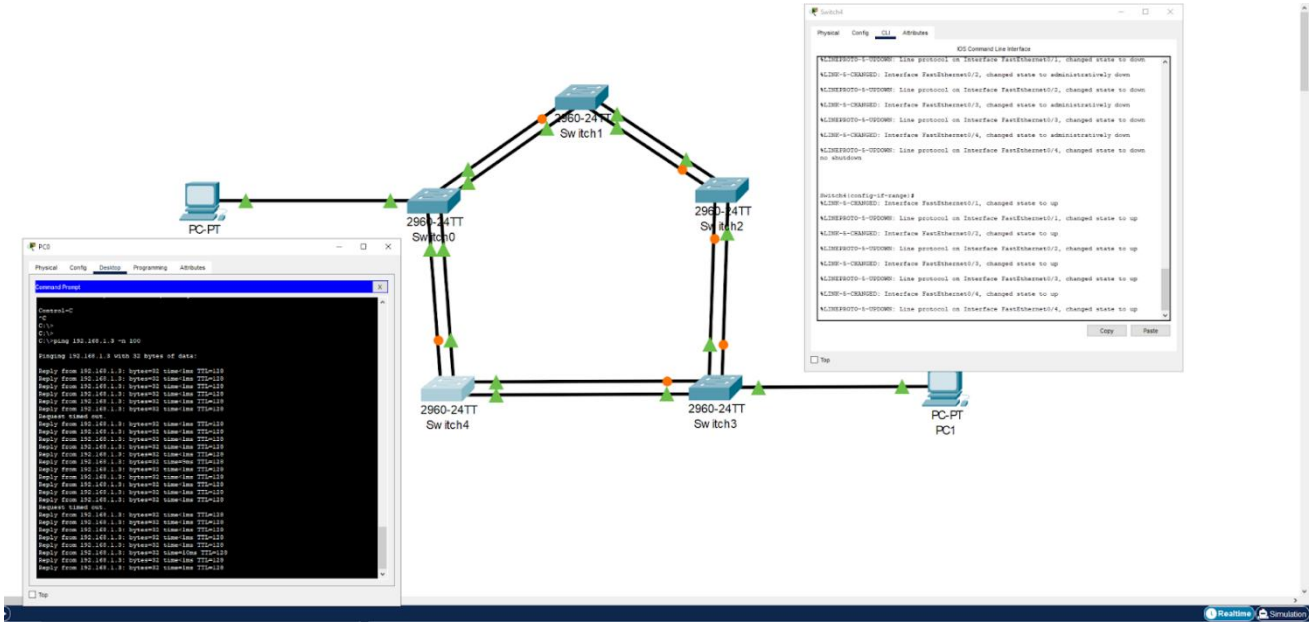


Рисунок 1.23. Втрата двох пакетів за період тестування

Отримали 2 втрачених пакету. Один з них при відключенні портів комутатору, інший при відновленні. Що свідчить про середній час відновлення у ~1 секунду.

Це підтверджує мою твердження про наявність проблеми у Packet Tracer. Так як дані різняться суттєво, що викликає питання. Ці помилки можливо пояснити так як:

1. Відмінності в обробці часу. Режим реального часу працює синхронно з годинником комп'ютера. Процеси, такі як розсилка оновлень протоколами маршрутизації, відбуваються у фоновому режимі з певними інтервалами, як і в реальній мережі. У той же час режим симуляції працює на основі подій (event-driven). Час просувається не лінійно, а від однієї значущої події до іншої (наприклад, відправка пакета, отримання пакета, оновлення таблиці маршрутизації). Такий підхід дозволяє наочно показати кожен крок, але

може спотворювати реальну картину для протоколів, що чутливі до часових затримок.

2. Програмні помилки Packet Tracer. Як і будь-яке складне програмне забезпечення, Packet Tracer має власні помилки. Деякі з них можуть проявлятися саме в режимі симуляції через його специфічну логіку обробки подій та пакетів, користувачі на форумах та інших ресурсах часто повідомляють про дивну поведінку, яка виникає лише при покроковому аналізі.

Враховуючи, що Packet Tracer є симулятором, а не емулятором, нам не потрібно використовувати його як 100-відсотковий еталон для перевірки конфігурацій мережі. Його справжня цінність полягає у наочності та доступності, перевірці загальних тез.

1.4.4 Моделювання роботи топології “Шина” в умовах відмов

Принцип функціонування: У цій топології всі пристрої підключаються до єдиного центрального кабелю, відомого як шина. Дані, що передаються одним пристроєм, поширюються по всій шині в обох напрямках. Кожен пристрій моніторить шину та обробляє лише ті дані, що адресовані йому. Для запобігання відбиття сигналу та інтерференції на кінцях шини встановлюються термінатори.

Уявимо такі сценарії збоїв:

- Обрив кабелю: Пошкодження центрального кабелю призводить до повного розриву мережі на два або більше ізольованих сегменти, що унеможливлює зв'язок між ними. Відсутність термінації в точці розриву спричиняє відбиття сигналу та виникнення колізій, паралізуючі навіть локальні сегменти.

- Вихід з ладу вузла: Несправність окремого вузла не впливає на функціонування інших пристроїв у мережі, оскільки вони продовжують використовувати спільну шину для зв'язку

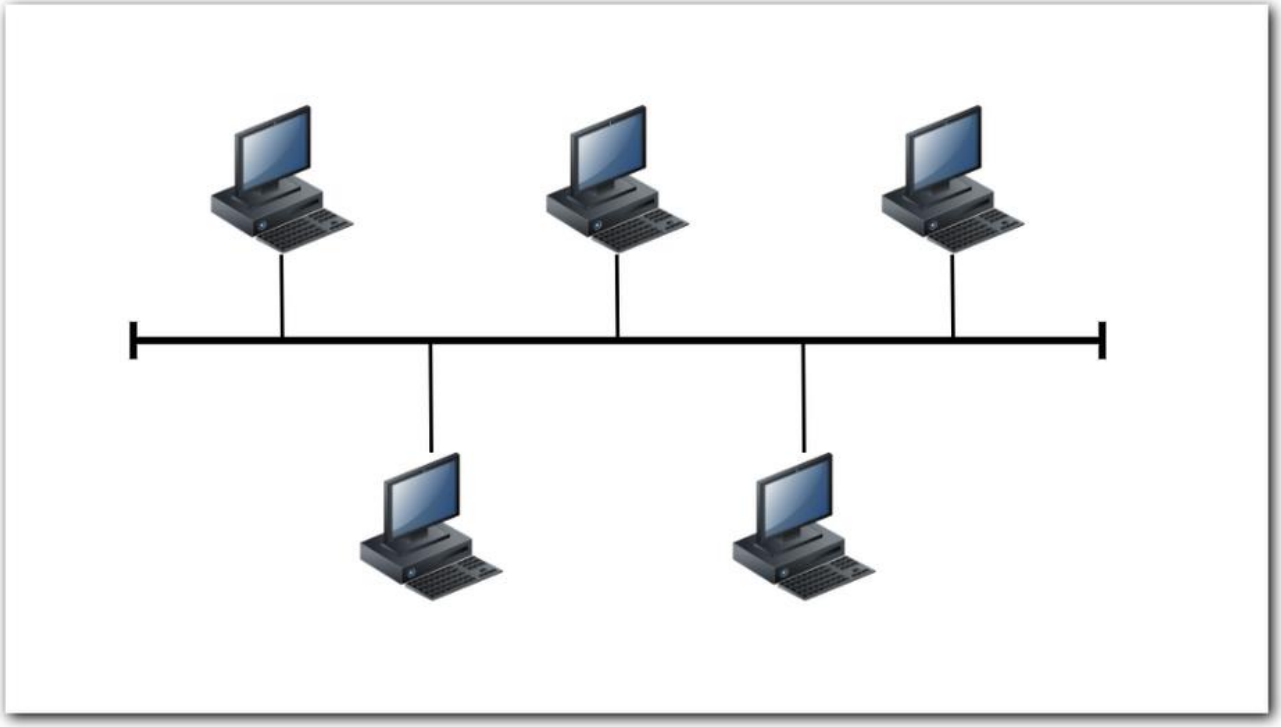


Рисунок 1.24. Топологія шина

1.4.5 Моделювання роботи зіркової топології в умовах відмов

Принцип функціонування: У цій топології всі пристрої підключаються до центрального пристрою, такого як комутатор або концентратор (хаб), за допомогою окремих кабелів, передача даних від одного пристрою до іншого відбувається через цей центральний вузол, який спрямовує трафік лише до призначеного одержувача.

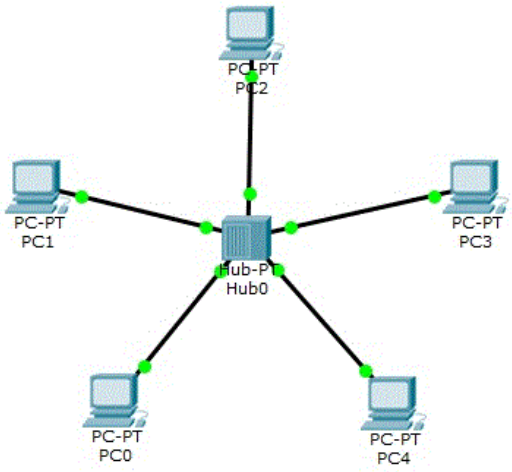


Рисунок 1.25. Зіркова топологія

Уявимо такі сценарії збоїв:

- Обрив кабелю: Пошкодження кабелю, що з'єднує окремий вузол з центральним пристроєм, ізолює лише цей конкретний вузол. Інші пристрої мережі продовжують функціонувати безперебійно, оскільки їхні з'єднання залишаються цілими.

- Вихід з ладу вузла: Несправність окремого кінцевого вузла не впливає на роботу мережі. Однак, вихід з ладу центрального пристрою (комутатора/концентратора) призводить до повного припинення функціонування всієї мережі, оскільки він є єдиною точкою зв'язку.

1.4.6 Моделювання роботи сітчастої топології в умовах відмов

Принцип функціонування: У повній топології "сітка" кожен пристрій у мережі має пряме з'єднання з кожним іншим пристроєм. Це створює численні надлишкові шляхи для передачі даних, забезпечуючи високу надійність

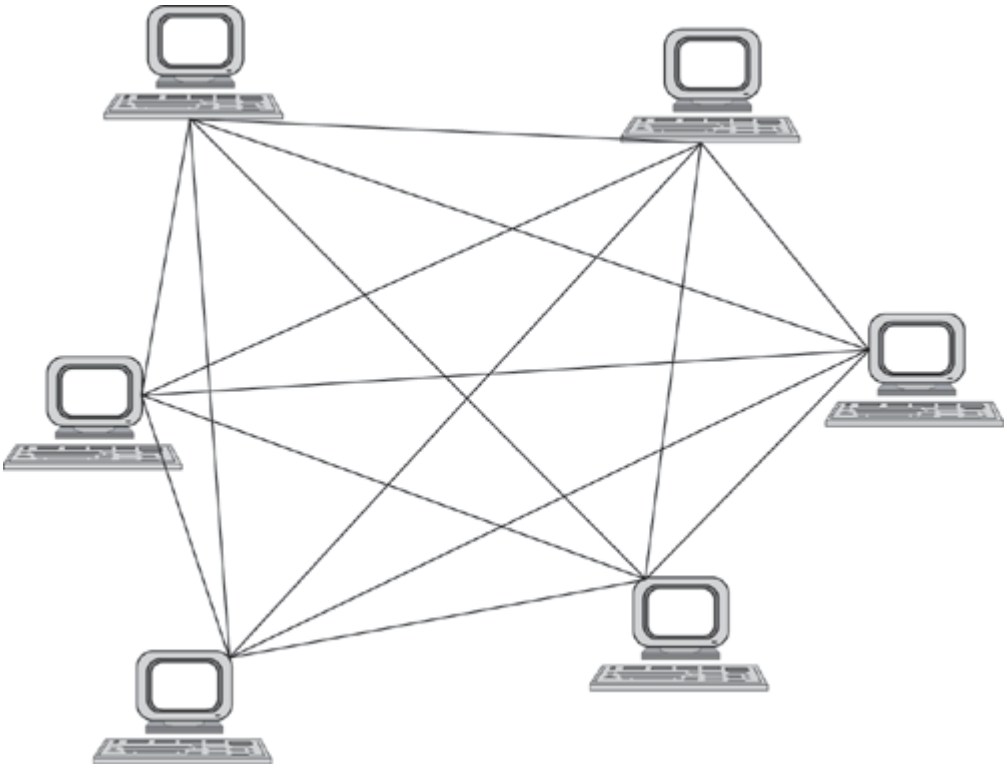


Рисунок 1.26. Сітчаста топологія

Уявимо такі сценарії збоїв:

- Обрив кабелю: Пошкодження одного або навіть кількох кабелів не призводить до втрати зв'язку між вузлами, оскільки дані можуть бути перенаправлені через альтернативні шляхи. Мережа автоматично адаптується, використовуючи доступні з'єднання.

- Вихід з ладу вузла: Вихід з ладу одного або декількох вузлів не перешкоджає функціонуванню решти мережі. Система маршрутизації автоматично обходить несправні вузли, підтримуючи зв'язок між іншими пристроями.

1.4.7 Моделювання роботи деревоподібної топології в умовах відмов

Принцип функціонування: Топологія "Дерево" є гібридною формою, що поєднує елементи топології "Шина" і "Зірка", створюючи ієрархічну структуру. Вона складається з центрального кореневого вузла, зазвичай комутатора або маршрутизатора, до якого підключаються вторинні вузли, які, у свою чергу, слугують центральними точками для кінцевих пристроїв таких як робочих станцій, серверів. Ця структура нагадує розгалужене дерево, де кореневий вузол є "стовбуром", комутатори середнього рівня – "гілками", а кінцеві пристрої – "листям".

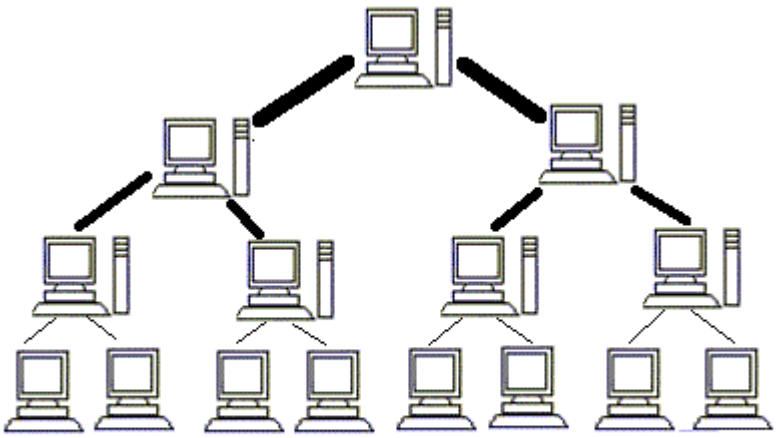


Рисунок 1.27. Деревоподібна топологія

Уявимо такі сценарії збоїв:

- Вихід з ладу кінцевого вузла: Відмова окремого кінцевого пристрою (наприклад, комп'ютера або його кабелю) ізолює лише цей пристрій. Робота решти мережі, включно з іншими кінцевими вузлами та усіма сегментами, залишається незмінною

- Вихід з ладу проміжного вузла: Відмова комутатора середнього рівня. Наприклад, комутатора на поверсі, призводить до ізоляції всього сегмента мережі, який до нього підключений. Усі кінцеві пристрої цього сегмента втрачають зв'язок між собою та з рештою мережі. Однак, інші сегменти та їхні з'єднання з кореневим вузлом продовжують функціонувати безперебійно.

- Вихід з ладу кореневого вузла: Несправність центрального, кореневого комутатора є найбільш критичною подією для топології "Дерево". Це призводить до повного розриву зв'язку між усіма підключеними гілками. Хоча окремі сегменти (наприклад, комп'ютери на одному поверсі) можуть зберігати локальний зв'язок через свої проміжні комутатори, зв'язок між сегментами стає неможливим, фактично розділяючи мережу на ізольовані "острови".

1.5 Результати тестування

За результатами тестування та моделювання роботи різних топологій мережі в умовах відмов ми отримали дані щодо відмовостійкості різних підходів. Оцінимо кожен з них по чотирьох критеріях відмов та по шкалі в 5 балів, де:

- 1 - мережа повністю не працює.
- 2-3 - мережа має значне зниження доступності, але частина мережі працює.
- 4 - деградація, але мережа майже повністю працює.
- 5 - відмова непомітна або дуже малопомітна, не завдає значних наслідків.

Таблиця 1.2. Оцінка топологій мереж

Топологія мережі	Відмова одного каналу	Відмова одного вузла	Відмова кількох каналів	Відмова кількох вузлів

Продовження таблиці 1.2. Оцінка топологій мереж

Шина	1	4	-	4
Кільце	4	5	2	1
Подвійне кільце	5	5	4	1
Зірка	4	3	3	1
Дерево	3	3	2	2
Сітчаста	5	5	4	4

1. Шина:

- Відмова одного каналу: оцінка 1 (мережа повністю не працює). Оскільки в шинній топології один канал є єдиним шляхом передачі даних, його відмова повністю паралізує мережу.

- Відмова одного вузла: оцінка 4 (деградація, але мережа майже повністю працює). Відмова одного вузла не впливає на роботу інших вузлів, оскільки вони продовжують використовувати спільну шину.

- Відмова кількох вузлів: оцінка 4 (деградація, але мережа майже повністю працює). Як і з одним вузлом, відмова кількох вузлів не критична для роботи решти мережі.

Загальний висновок по шині: дуже вразлива до відмови каналу, але відносно стійка до відмов окремих вузлів.

2. Кільце:

- Відмова одного каналу: оцінка 4 (деградація, але мережа майже повністю працює). Якщо один канал виходить з ладу, дані можуть передаватися в іншому напрямку по кільцю.

- Відмова одного вузла: оцінка 5 (відмова непомітна або дуже малопомітна). Якщо один вузол виходить з ладу, дані можуть передаватися по кільцю.

- Відмова кількох каналів: оцінка 2 (значне зниження доступності, але частина мережі працює). При відмові кількох каналів можуть утворитися розриви в кільці, що призведе до ізоляції частин мережі.

- Відмова кількох вузлів: оцінка 1 (мережа повністю не працює). Відмова кількох вузлів у кільці може призвести до його розриву та непрацездатності.

Загальний висновок по кільцю: добре справляється з відмовою одного каналу/вузла завдяки можливості альтернативного шляху, але вразливе до відмови кількох вузлів або каналів.

3. Подвійне кільце:

- Відмова одного каналу: оцінка 5 (відмова непомітна або дуже малопомітна). Завдяки наявності двох кілець, відмова одного каналу в одному кільці компенсується іншим кільцем.

- Відмова одного вузла: оцінка 5 (відмова непомітна або дуже малопомітна). Якщо один вузол виходить з ладу, дані можуть передаватися по кільцю.

- Відмова кількох каналів: оцінка 4 (деградація, але мережа майже повністю працює). Навіть при відмові кількох каналів (за умови, що вони не повністю перекривають обидва кільця), мережа продовжує функціонувати.

- Відмова кількох вузлів: оцінка 1 (мережа повністю не працює). Хоча і стійкіша за одинарне кільце, відмова кількох вузлів може порушити обидва кільця, призводячи до повного збою.

Загальний висновок по подвійному кільцю: висока стійкість до відмов окремих каналів та вузлів. Однак, як і звичайне кільце, може повністю вийти з ладу при масштабних відмовах вузлів.

4. Зірка

- Відмова одного каналу: оцінка 4 (деградація, але мережа майже повністю працює). Відмова каналу до одного з периферійних пристроїв ізолює лише цей пристрій.

- Відмова одного вузла: оцінка 3 (значне зниження доступності, але частина мережі працює). Якщо відмовляє центральний вузол (хаб або комутатор), вся

мережа виходить з ладу. Якщо відмовляє периферійний вузол, це впливає лише на нього.

- Відмова кількох каналів: оцінка 3 (значне зниження доступності, але частина мережі працює). Відмова кількох каналів призводить до ізоляції відповідних пристроїв.

- Відмова кількох вузлів: оцінка 1 (мережа повністю не працює). Якщо відмовляє центральний вузол, це може призвести до повного збою.

Загальний висновок по зірці: вразлива до відмов центрального вузла, але відносно стійка до відмов окремих периферійних каналів та вузлів.

5. Деревоподібна:

- Відмова одного каналу: оцінка 3 (значне зниження доступності, але частина мережі працює). Залежно від місця відмови, може ізолювати цілу гілку мережі.

- Відмова одного вузла: оцінка 3 (значне зниження доступності, але частина мережі працює). Відмова вузла, може призвести до ізоляції великих частин мережі.

- Відмова кількох каналів: оцінка 2 (значне зниження доступності, але частина мережі працює). Кілька відмов можуть розірвати мережу на значні ізольовані фрагменти.

- Відмова кількох вузлів: оцінка 2 (значне зниження доступності, але частина мережі працює). Відмова кількох вузлів також може призвести до значної фрагментації мережі.

Загальний висновок по деревоподібній: середня стійкість до відмов. Стійкість залежить від розташування відмови – чим ближче до кореня, тим більший вплив.

6. Сітчаста (Mesh):

- Відмова одного каналу: оцінка 5 (відмова непомітна або дуже малопомітна). Завдяки множинним шляхам між вузлами, відмова одного каналу легко компенсується іншими шляхами.

- Відмова одного вузла: оцінка 5 (відмова непомітна або дуже малопомітна). Аналогічно, відмова одного вузла компенсується іншими шляхами через інші вузли.
- Відмова кількох каналів: оцінка 4 (деградація, але мережа майже повністю працює). Навіть при відмові кількох каналів, висока надмірність дозволяє підтримувати зв'язок.
- Відмова кількох вузлів: оцінка 4 (деградація, але мережа майже повністю працює). Навіть при відмові кількох вузлів, якщо залишаються альтернативні шляхи, мережа продовжує функціонувати, хоча і з деградацією.

Загальний висновок по сітчастій топології: найвища стійкість до відмов серед топологій завдяки високій надмірності з'єднань.

Основні результати:

- Найвища відмовостійкість. Сітчаста топологія демонструє найкращі показники за всіма критеріями відмов. Подвійне кільце також дуже добре показує себе при відмовах окремих елементів.

- Найнижча відмовостійкість. Шина є найменш відмовостійкою, особливо до відмов каналів.

- Чутливість до центрального елемента. Топології "зірка" та "дерево" дуже чутливі до відмов центральних вузлів або вузлів ближче до кореня, що може призвести до ізоляції значних частин мережі.

- Надмірність є ключовою. Топології з більшою кількістю альтернативних шляхів (сітчаста, подвійне кільце) значно стійкіші до відмов.

- Вплив відмови. Важливо розрізняти вплив відмови каналу та відмови вузла, а також одиничних та множинних відмов. Деякі топології добре справляються з одиничними відмовами, але повністю виходять з ладу при множинних.

1.6 Оцінка ефективності апаратних рішень

Результати чітко показують, що наявність надмірних шляхів, як у "Сітчастій" та "Подвійному кільці", є ключовим фактором для забезпечення відмовостійкості, особливо в умовах множинних відмов. Топології з єдиними точками відмови, наприклад, центральний вузол у "Зірці" або основний канал у "Шині", є вкрай вразливими. Це підкреслює, що надійна система повинна бути спроєктована таким чином, щоб усунути єдині точки відмови та включати стратегічну надмірність, що відповідає найкращим практикам для забезпечення високої доступності.

Вища відмовостійкість "Сітчастої" та "Подвійного кільця" топологій, хоча й є технічно бажаною, часто пов'язана зі значно вищими витратами. Це пов'язано зі збільшеними вимогами до апаратного забезпечення, такими як більше кабелів, комутаторів та надлишкових компонентів, а також потенційно вищою складністю впровадження та обслуговування, наприклад, повністю дзеркальна система, хоча й відмовостійка, є дорогим і іноді громіздким рішенням. Це вимагає проведення ретельного аналізу загальної вартості, що дозволить збалансувати початкові інвестиції з довгостроковими перевагами, такими як скорочення часу простою, підвищення безперервності бізнесу та покращення задоволеності клієнтів. Потрібно зважувати ці компроміси, враховуючи специфічну критичність своїх операцій та бюджетні обмеження

Роль CPU та GPU:

- CPU (Центральний процесор). Процесори є основою обчислювальних систем і відіграють ключову роль у виконанні послідовних операцій. Їхня продуктивність визначається такими параметрами, як тактова частота (кількість циклів, які CPU може виконати за секунду), кількість ядер та потоків (здатність обробляти кілька завдань одночасно), інструкції за цикл (IPC – ефективність виконання роботи за цикл) та розмір кешу (швидкий доступ до даних). Новіші архітектури CPU можуть значно покращити показник IPC, забезпечуючи кращу загальну продуктивність

навіть при тій же тактовій частоті. Для ефективної багатозадачності та паралельної обробки критично важливою є достатня кількість ядер та потоків.

- GPU (Графічний процесор): На відміну від CPU, графічні процесори оптимізовані для масивного паралелізму, що робить їх надзвичайно ефективними для обробки великих обсягів даних одночасно. Вони оснащені тисячами ядер та власною високошвидкісною пам'яттю (VRAM), що робить їх незамінними для високопродуктивних обчислень (HPC), завдань штучного інтелекту (AI) та машинного навчання (ML). Показник TFLOPS (терафлопс) є ключовим для вимірювання продуктивності GPU з плаваючою комою.

- Вплив на топології: У високопродуктивних мережах, таких як сітчасті, ефективність CPU та GPU вузлів безпосередньо впливає на загальну пропускну здатність та здатність системи обробляти складні розподілені навантаження. Оптимальне поєднання цих компонентів на кожному вузлі мережі максимізує її обчислювальний потенціал.

Ієрархія пам'яті: Ієрархія пам'яті, включаючи регістри, кеш-пам'ять, основну пам'ять та віртуальну пам'ять, є фундаментальною для оптимізації продуктивності комп'ютерної системи, оскільки вона мінімізує середній час доступу до даних. Швидші рівні пам'яті, наприклад, кеш L1, L2, L3, мають меншу ємність, але забезпечують набагато швидший доступ, тоді як повільніші рівні, як основна пам'ять, мають більшу ємність. Ефективне управління кешем, включаючи політики заміщення та забезпечення когерентності, а також роль віртуальної пам'яті у наданні більшого адресного простору та покращенні багатозадачності, можуть значно покращити загальну продуктивність системи.

Вплив на мережеві топології: У розподілених системах, де дані часто переміщуються між вузлами або обробляються локально, ефективна ієрархія пам'яті на кожному вузлі допомагає зменшити затримки обробки та забезпечити швидкий доступ до даних. Це є критичним для підтримки високої пропускної здатності та продуктивності мережі, особливо в умовах відмов, коли система повинна швидко перерозподіляти завдання.

Компоненти мережі. Шини, комутатори, кабелі та інші компоненти мережі, забезпечують зв'язок між різними компонентами системи. Їхня продуктивність критично впливає на загальну затримку, пропускну здатність та енергоспоживання системи.

Вплив на мережеві топології: У сітчастих та подвійних кільцевих топологіях, де дані можуть переміщуватися різними шляхами, високопродуктивні компоненти мережі є життєво важливими для ефективного використання надмірності та мінімізації затримок, особливо під час перенаправлення трафіку після відмови. Вони забезпечують швидке та надійне сполучення, що дозволяє системі підтримувати продуктивність навіть при деградації.

Паралелізм та Розподіл Навантаження:

Паралельна обробка революціонізувала обчислення, дозволяючи кільком процесорам одночасно працювати над однією проблемою, розділяючи складні завдання на менші, незалежні підзадачі, що виконуються паралельно. Це значно скорочує час обробки та підвищує обчислювальну потужність, дозволяючи додаткам обробляти більші набори даних та швидко вирішувати складні проблеми.

Оптимізація паралелізму. Ступінь паралелізму має бути оптимізований для конкретного апаратного забезпечення, а не просто максимізований. Надмірний паралелізм може збільшити накладні витрати через зростання кількості процесів і фактично погіршити продуктивність. Важливо зважувати переваги додаткового паралелізму проти потенційних втрат ефективності обробки.

Розподіл навантаження: Розподіл вхідного трафіку та завдань рівномірно між кількома серверами є критично важливим для управління навантаженням. Це запобігає перевантаженню будь-якого окремого сервера, забезпечуючи кращу продуктивність, надійність та час безвідмовної роботи. Балансування навантаження допомагає підтримувати оптимальну ефективність сервера, скорочувати час відгуку та покращувати користувацький досвід, а також забезпечує плавну обробку пікових навантажень.

Вплив на мережеві топології: Топології з високою надмірністю, такі як сітчаста, ідеально підходять для розподілених систем, що використовують паралелізм, оскільки вони можуть ефективно розподіляти навантаження та забезпечувати безперервність роботи навіть при відмові окремих вузлів або каналів. Це дозволяє системі використовувати весь свій обчислювальний потенціал, мінімізуючи вплив локальних збоїв.

Вплив Типів Робочих Навантажень. Різні типи робочих навантажень мають різні вимоги до ресурсів і значно впливають на вибір оптимальних апаратних рішень та їхню ефективність.

- HPC (High-Performance Computing): Вимагає масивно паралельних обчислень, часто з використанням десятків тисяч або мільйонів процесорів/ядер. Для HPC критичні висока пропускна здатність, низька затримка та ефективне управління пам'яттю. Оптимізація архітектури HPC включає вибір правильного поєднання CPU, GPU, а також мережеву оптимізацію для мінімізації затримки.

- AI/ML (Artificial Intelligence/Machine Learning): Характеризується інтенсивними завданнями, що потребують великих обсягів обробки даних для розробки, навчання та розгортання моделей AI. GPU є особливо ефективними для AI/ML завдяки своїй паралельній архітектурі, яка дозволяє прискорювати навчання нейронних мереж та обробку великих обсягів даних. Розвиток спеціалізованого обладнання, такого як Google TPUs, також оптимізує продуктивність робочих навантажень ML.

- Бази даних: Продуктивність баз даних значною мірою залежить від швидкості та ємності апаратного забезпечення (CPU, пам'ять, система зберігання, пропускна здатність мережі). Висока кількість одночасних користувачів або процесів, що звертаються до бази даних, збільшує потребу в ресурсах CPU та ризик вузьких місць. Оптимізація запитів та індексації, а також балансування навантаження є ключовими для ефективної роботи.

- Веб-сервіси: Навантаження на веб-сервери вимірюється використанням CPU, споживанням пам'яті, дисковою активністю та мережевим трафіком. Високе навантаження може призвести до повільного часу завантаження та недоступності.

Для веб-сервісів важливі кешування, оптимізація запитів, стиснення файлів та балансування навантаження.

Вплив на мережеві топології: Вибір топології повинен відповідати вимогам робочого навантаження. Наприклад, для HPC та AI/ML, де критична висока пропускна здатність та низька затримка між обчислювальними вузлами, сітчаста топологія може бути ідеальною, незважаючи на її складність. Для менш критичних веб-сервісів з меншими вимогами до відмовостійкості, зіркова або деревовидна топологія може бути більш економічно вигідною.

Загальна ефективність апаратного рішення визначається не лише відмовостійкістю мережевої топології, а й глибокою взаємодією між базовою архітектурою апаратного забезпечення та специфічними вимогами робочого навантаження. Наприклад, хоча сітчаста топологія пропонує вищу відмовостійкість, її повний потенціал для робочих навантажень AI/ML або HPC може бути реалізований лише за умови, що вузли оснащені потужними GPU. Це забезпечує ефективну паралельну обробку та передачу даних. І навпаки, розгортання високопродуктивного, відмовостійкого обладнання для простих веб-сервісів може призвести до надмірного забезпечення та непотрібних витрат. Це підкреслює необхідність цілісного підходу до проєктування, де компоненти апаратного забезпечення вибираються та конфігуруються відповідно до обчислювальних потреб, потоку даних, доступних коштів.

Робочі навантаження є динамічними і можуть значно коливатися з часом. Ця динамічність вимагає, щоб апаратні рішення, окрім їхньої вбудованої відмовостійкості, також володіли адаптивністю та механізмами для динамічного розподілу ресурсів. Такі функції, як автомасштабування , які автоматично налаштовують ресурси сервера відповідно до попиту, стають критично важливими для підтримки оптимальної продуктивності та економічної ефективності під час пікових періодів або несподіваних стрибків попиту. Це зміщує фокус зі статичних проектних рішень на безперервний моніторинг та гнучке управління інфраструктурою, гарантуючи, що система може не тільки витримувати збої, а й ефективно масштабуватися для задоволення потреб бізнесу.

1.7 Основні результати дослідження

Забезпечення відмовостійкості мереж вимагає комплексного підходу, який значною мірою спирається на впровадження надмірності на різних рівнях апаратного забезпечення. Це включає дублювання фізичних компонентів, використання спеціалізованих масивів зберігання даних та застосування протоколів, що дозволяють автоматичне перемикання між пристроями.

Надлишковість фізичних компонентів є основою апаратної відмовостійкості. Вона передбачає дублювання критично важливих елементів інфраструктури для усунення єдиних точок відмови.

Дублювання серверів та мережевих пристроїв, таких як маршрутизатори, комутатори, є поширеною та працюючою практикою. Наприклад, сервер може бути зроблений відмовостійким шляхом використання ідентичного резервного сервера, який паралельно дзеркалює всі операції. У разі збою основного сервера, резервний негайно бере на себе навантаження, забезпечуючи безперервність роботи. Цей принцип застосовується до всіх критичних мережевих пристроїв, оскільки будь-яка одиночна точка відмови на фізичному рівні може звести нанівець ефективність програмних механізмів відмовостійкості.

Надлишкові джерела живлення є ще одним критично важливим аспектом апаратної відмовостійкості. Вони гарантують безперебійне живлення обладнання, автоматично перемикаючись на альтернативні джерела у разі збою основного. Багато сучасних мережевих комутаторів підтримують функцію гарячої заміни (hot-swapping) блоків живлення, що дозволяє замінювати несправні компоненти без відключення пристрою та переривання роботи мережі. Існують різні схеми резервування живлення: повна надмірність (1:1 або 1+1), де кожен комутатор підключений до двох джерел живлення, і часткова (1:N), де одне додаткове джерело живлення обслуговує кілька комутаторів. Повна надмірність забезпечує нульовий час простою у разі відмови одного джерела живлення, оскільки інше миттєво компенсує повну потужність.

Надлишкові мережеві з'єднання передбачають використання кількох мережевих підключень або шляхів для запобігання єдиній точці відмови. Це може бути реалізовано через агрегацію каналів, яка об'єднує кілька фізичних з'єднань в одне логічне, збільшуючи не тільки пропускну здатність, але й надійність. Повсюдне застосування надмірності на всіх рівнях апаратного забезпечення (обчислювальні ресурси, мережа, живлення) демонструє фундаментальний принцип: будь-яка одиночна точка відмови на фізичному рівні може звести нанівець програмну відмовостійкість. Ця систематична дублікація є основою надійності.

RAID-масиви є ключовим апаратним рішенням для забезпечення відмовостійкості зберігання даних. Він дозволяє об'єднувати кілька жорстких дисків в єдиний логічний блок, забезпечуючи захист даних та/або підвищення продуктивності.

Різні рівні RAID пропонують різні компроміси між продуктивністю, ємністю та рівнем відмовостійкості:

- RAID 0 не забезпечує відмовостійкості, оскільки дані розподіляються (страйпуються) по дисках без надмірності. Відмова одного диска призводить до втрати всіх даних, але цей рівень значно підвищує швидкість читання/запису.

- RAID 1 дзеркалює дані на кількох дисках, створюючи точну копію. Це забезпечує відмовостійкість до відмови одного диска, але зменшує корисну ємність сховища вдвічі.

- RAID 5 використовує блокове страйпування з розподіленим паритетом. Він дозволяє системі витримати відмову одного диска без втрати даних, забезпечуючи хороший баланс між продуктивністю, ємністю та відмовостійкістю.

- RAID 6 схожий на RAID 5, але використовує подвійний розподілений паритет, що дозволяє системі витримати відмову до двох дисків без втрати даних. Це забезпечує вищий рівень захисту, але вимагає мінімум чотирьох дисків.

- RAID 10 (RAID 1+0) комбінує дзеркалювання (RAID 1) та страйпінг (RAID 0). Цей рівень є дорогим, вимагає мінімум чотирьох дисків, але забезпечує високу

продуктивність та відмовостійкість, дозволяючи системі продовжувати роботу без втрати даних, якщо збої відбуваються в різних підгрупах.

Апаратний RAID зазвичай підтримує більше рівнів RAID та забезпечує кращу продуктивність порівняно з програмним RAID, оскільки обробка даних виконується спеціалізованим контролером, а не центральним процесором. Вибір рівня RAID є яскравим прикладом того, як апаратна надмірність адаптується для забезпечення цілісності та доступності даних. Вибір конкретного рівня RAID безпосередньо відображає можливість та потребу бізнесу до зберігання даних та вимоги до продуктивності, підкреслюючи, що "відмовостійкість" не є монолітним поняттям, а скоріше спектром рішень.

Протоколи надмірності першого хопу (FHRP) є ключовими для забезпечення відмовостійкості на рівні маршрутизації в локальних мережах. Ці протоколи, такі як HSRP (Hot Standby Router Protocol), VRRP (Virtual Router Redundancy Protocol) та GLBP (Gateway Load Balancing Protocol), створюють ілюзію єдиного віртуального маршрутизатора, забезпечуючи безперебійну роботу навіть у разі відмови фізичного шлюзу за замовчуванням.

- HSRP (Hot Standby Router Protocol) є пропрієтарним протоколом Cisco. Він дозволяє двом або більше маршрутизаторам функціонувати як єдиний віртуальний маршрутизатор. В групі HSRP один маршрутизатор призначається активним і пересилає весь трафік, тоді як інші перебувають у режимі очікування (standby). У разі відмови активного маршрутизатора, резервний маршрутизатор автоматично бере на себе його роль, забезпечуючи безперебійну маршрутизацію.

- VRRP (Virtual Router Redundancy Protocol) - це відкритий стандарт IEEE (RFC 5798), який виконує схожу функцію, усуваючи єдину точку відмови, притаманну статичному маршрутизованому середовищу. Група маршрутизаторів діє як віртуальний логічний маршрутизатор, де один маршрутизатор є "майстром", а інші - "резервними". Якщо майстер виходить з ладу, один з резервних маршрутизаторів стає майстром.

- GLBP (Gateway Load Balancing Protocol) також є пропрієтарним протоколом Cisco, але, на відміну від HSRP та VRRP, він надає не тільки надмірність, але й

функціональність балансування навантаження. GLBP дозволяє розподіляти трафік між кількома маршрутизаторами, використовуючи одну віртуальну IP-адресу та кілька віртуальних
MAC-адрес. Це означає, що всі маршрутизатори в групі можуть активно пересилати трафік, оптимізуючи використання ресурсів.

Хоча ці протоколи є програмними компонентами, їх функція нерозривно пов'язана з апаратним забезпеченням, а саме маршрутизаторами, на яких вони працюють. Вони є критично важливими для забезпечення апаратної відмовостійкості на периферії мережі. Здатність GLBP балансувати навантаження між кількома активними маршрутизаторами перетворює суто відмовостійкий механізм на той, що одночасно підвищує продуктивність, демонструючи, як апаратна надмірність, керована інтелектуальним програмним забезпеченням, може надавати подвійні переваги.

Таблиця 1.3 Порівняння HSRP, VRRP, GLBP

Характеристика	HSRP (Hot Standby Router Protocol)	VRRP (Virtual Router Redundancy Protocol)	GLBP (Gateway Load Balancing Protocol)
Стандарт	Пропрієтарний Cisco	Відкритий стандарт IEEE (RFC 5798)	Пропрієтарний Cisco
Ролі Маршрутизаторів	Активний, Резервний	Майстер, Резервний	Активний Віртуальний Шлюз (AVG), Активні Віртуальні Форвардери (AVF)
Балансування Навантаження	Не підтримується (можливе через кілька груп)	Не підтримується	Підтримується

Продовження таблиці 1.3 Порівняння HSRP, VRRP, GLBP

Віртуальна IP/MAC	Одна віртуальна IP, одна віртуальна MAC	Одна віртуальна IP, одна віртуальна MAC	Одна віртуальна IP, кілька віртуальних MAC
Переваги/Недоліки	Швидке перемикання, широке використання в середовищах Cisco	Сумісність між вендорами, відкритий стандарт	Надмірність + балансування навантаження, ефективніше використання ресурсів

Таблиця 1.3 надає чіткий та швидкий огляд ключових атрибутів цих протоколів. Вона дозволяє легко ідентифікувати їхні сильні та слабкі сторони, наприклад, унікальну здатність GLBP до балансування навантаження порівняно з активно-резервним характером HSRP та VRRP. Це має вирішальне значення для розуміння того, чому той чи інший протокол буде обраний у конкретному сценарії проектування мережі.

2 РОЗДІЛ ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

2.1 Вступ до охорони праці

Охорона праці — це комплекс заходів, спрямованих на захист життя та здоров'я працівників під час виконання ними службових обов'язків. Ці заходи охоплюють широкий спектр аспектів, включаючи норми освітлення, рівень шуму, мікроклімат, розмір робочого місця та багато інших значущих факторів. Нормативно-правові акти, закони та положення регулюють комфортні та безпечні умови праці. Неналежні умови праці, вплив негативних факторів або дискомфортне середовище можуть призвести до швидкої втоми працівників, збільшення кількості помилок, а також до розвитку професійних захворювань або виробничих травм

У контексті цього дипломного проєкту питання охорони праці розглядається у зв'язку з безпекою робочого місця програміста, який працює з персональним комп'ютером.

2.2 Аналіз умов та безпеки праці на робочому місці програміста

На робочому місці програміста існують потенційні шкідливі фактори, перелік яких наведено в Таблиці 2.1.

Таблиця 2.1. Шкідливі та небезпечні фактори

Категорія фактору	Фактор	Деталі
Шкідливі фактори	Мікроклімат	Підвищена або знижена температура повітря, підвищена або знижена рухливість повітря, підвищена або знижена іонізація повітря.
	Фізичні перевантаження	Статичні перевантаження опорно-рухового апарату, динамічні локальні перевантаження м'язів кистей рук.
	Навантаження на зір	Перенапруження очей.

Продовження таблиці 2.1. Шкідливі та небезпечні фактори

	Особливості праці	Монотонність праці.
Небезпечні фактори	Електричний струм	Підвищена напруга в електричному ланцюзі, ураження якою може статися через тіло людини.

Робота не передбачає значних фізичних навантажень і належить до категорії 1а. Основний інструмент праці – персональний комп'ютер.

2.3 Організація робочого місця

Робочий стіл повинен бути достатнього розміру, щоб зручно розмістити монітор (дисплей), клавіатуру, інше обладнання та документи. Поверхня столу повинна мати низьку відбивну здатність. Клавіатуру слід розміщувати так, щоб перед нею був достатній простір (щонайменше 300 мм від краю столу) для опори рук працівника. Рекомендується розміщувати екран монітора нижче рівня очей працівника, бажано перпендикулярно до нормальної лінії погляду (приблизно 15° вниз від горизонталі), для забезпечення зручності зорового спостереження та точного зчитування інформації. Для мінімізації впливу електромагнітних випромінювань відстань між екраном монітора та працівником повинна бути не менше 500 мм (оптимально 600-700 мм).

2.4 Мікроклімат

Мікроклімат у приміщенні повинен відповідати нормативам, встановленим ДСН 3.3.6.042-99. Оптимальні умови для підтримання комфортного теплового балансу та терморегуляції організму людини включають:

- У холодну пору року температура повітря повинна становити 22-24°С, відносна вологість повітря 40-60%, а швидкість руху повітря — 0,1 м/с.

- У теплу пору року температура повітря повинна бути 23-25°С, відносна вологість повітря 40-60%, а швидкість руху повітря — 0,1 м/с.

Висока температура розширює кровоносні судини, збільшуючи тепловіддачу, тоді як низька — звужує їх, зменшуючи приплив крові та тепловіддачу. Вологість повітря також впливає на терморегуляцію. Надмірно висока вологість (понад 85%) ускладнює її, а занадто низька (менше 20%) призводить до пересихання слизових оболонок, зокрема дихальних шляхів та очей. Оптимальна вологість у приміщенні важлива також для зниження впливу електростатичних та електромагнітних полів, рівень випромінювання яких у приміщеннях з комп'ютерами завжди підвищений.

Рівень іонів у повітрі має відповідати санітарно-гігієнічним нормам № 2152-80. Мінімальна кількість позитивних іонів (n+) становить 400 на см³, а негативних іонів (n-) — 600 на см³. Оптимальний діапазон для n+ — 1500-3000 на см³, а для n- — 3000-5000 на см³. Максимальна кількість для обох типів іонів становить 50000 на см³.

Для підтримки оптимального мікроклімату рекомендується використовувати кондиціонери, зволожувачі повітря або інші відповідні прилади.

2.5 Освітлення

Робоче місце з ПК слід розміщувати так, щоб природне світло падало збоку, бажано зліва. Для зменшення яскравості природного освітлення в полі зору можна використовувати регульовані жалюзі або щільні штори. Світильники загального та місцевого освітлення повинні забезпечувати необхідний рівень освітленості та контраст між екраном і навколишнім середовищем, враховуючи характер роботи та вимоги до видимості. Освітленість поверхні столу в зоні робочого документа має становити 300-500 люкс**.**

Можливі відблиски на екрані монітора та іншому обладнанні, що заважають відображенню, слід усувати шляхом належного розташування екрану, обладнання та світильників місцевого освітлення. При рядному розташуванні робочих столів

забороняється розміщувати екрани відеомоніторів назустріч один одному через взаємне відображення.

Для штучного освітлення рекомендується використовувати люмінесцентні лампи. Допускається використання металогалогенних ламп потужністю до 250 Вт. Лампи розжарювання дозволяються для місцевих світильників. Використання будь-яких світильників без розсіювачів заборонено.

2.6 Електробезпека

Конструктивні заходи електробезпеки включають захист від випадкового дотику до струмопровідних частин за допомогою захисних оболонок та ізоляції. Схемно-конструктивні заходи спрямовані на запобігання ураженню електричним струмом при дотику до металевих корпусів, які можуть опинитися під напругою внаслідок аварії. У даному приміщенні для комп'ютерів застосовується занулення, а біля монітора передбачена подвійна ізоляція.

Необхідно суворо дотримуватися правил техніки безпеки при роботі з високою напругою та наступних запобіжних заходів:

- Монтаж, обслуговування, ремонт та налагодження ЕОМ, заміна деталей, пристосувань, блоків повинні здійснюватися лише при повному відключенні живлення.

- Заземлення конструкції приміщення має бути надійно захищене діелектричними щитками або сітками від випадкового дотику.

2.7 Пожежна безпека

Пожежна безпека є невід'ємною частиною комплексу заходів з охорони праці. Організаційна робота в цій сфері на об'єктах господарювання охоплює широкий спектр заходів, зокрема:

- Створення безпечних умов праці.

- Мінімізація ризику виникнення пожеж.

- Своєчасне та повноцінне забезпечення технічними засобами для запобігання займанням та ліквідації пожеж і їх наслідків.

- Контроль за дотриманням протипожежних вимог і норм законодавства.

- Розробка та впровадження регламентів з гасіння пожеж, евакуації та порятунку людей і майна (матеріальних цінностей) з місць пожежі та задимлення.

- Внутрішнє та зовнішнє навчання співробітників.

Джерелами займання у виробничих приміщеннях з ПЕОМ можуть бути: іскра при розряді статичної електрики; іскри від електрообладнання; іскри від удару та тертя; відкрите полум'я.

Первинні засоби пожежогасіння застосовуються для боротьби з пожежами на початковій стадії. До них належать: пожежні кран-комплекти, вогнегасники, пожежний інвентар (резервуари з водою, ящики з піском, пожежні відра, лопати), а також різний переносний пожежний інструмент (кирки, сокири, багри, ломи тощо).

При захисті приміщень з персональними комп'ютерами від пожежі слід враховувати специфіку вогнегасних речовин у вогнегасниках, які можуть пошкодити обладнання під час гасіння. Ці приміщення рекомендується оснащувати вуглекислотними вогнегасниками, враховуючи гранично допустиму концентрацію вогнегасної речовини. Забороняється гасити електроустановки в закритих приміщеннях без належної вентиляції. Вуглекислота не залишає слідів після випаровування і водночас не пошкоджує загоріле електрообладнання. Це особливо важливо при гасінні комп'ютерної техніки або телевізора, що загорівся. Вуглекислотними вогнегасниками можна гасити електроустановки під напругою до 10 000 Вольт (10 кВ).

Також при роботі з ПЕОМ на робочому місці забороняється зберігати вогненебезпечні речовини. Насамперед, не можна допускати накопичення паперових відходів поблизу ПЕОМ та їх несвоєчасного прибирання.

У приміщеннях забороняється: розпалювати вогонь; вмикати електрообладнання, якщо в приміщенні відчувається запах газу; курити; сушити будь-що на опалювальних приладах; закривати вентиляційні отвори в електроапаратурі.

Висновки

Дослідження апаратних рішень для забезпечення відмовостійкості мереж виявляє їхню фундаментальну роль у підтримці безперервності бізнесу та надійності критично важливих систем.

Основним принципом апаратної відмовостійкості є надмірність, яка реалізується через дублювання фізичних компонентів, таких як сервери, мережеві пристрої (маршрутизатори, комутатори) та джерела живлення. Це усуває фізичні точки відмови. RAID-масиви забезпечують відмовостійкість зберігання даних, пропонуючи різні рівні захисту та продуктивності. Протоколи надмірності першого хопу (HSRP, VRRP, GLBP) дозволяють автоматичне перемикання шлюзів за замовчуванням, а архітектури центрів обробки даних (N+1, 2N, Spine-Leaf) забезпечують системну надмірність на масштабі інфраструктури.

Переваги впровадження апаратної відмовостійкості є значними: вона мінімізує час простою, що може коштувати організаціям не тільки у грошах, а і у репутаційних ризиках, та значно підвищує надійність системи. Крім того, надмірність може покращити продуктивність через балансування навантаження, підвищує масштабованість та гнучкість для майбутніх оновлень, а також забезпечує стійкість до кібератак та природних катастроф.

Проте, реалізація апаратної відмовостійкості не позбавлена викликів. Вона вимагає значних початкових інвестицій та постійних експлуатаційних витрат. Збільшення складності проектування, впровадження та управління може призвести до нових джерел збоїв, таких як помилки конфігурації. Також можливий вплив на продуктивність, зокрема збільшення затримки через накладні витрати на надмірність.

Оцінка ефективності відмовостійких рішень здійснюється за допомогою таких метрик, як час безвідмовної роботи (Uptime) та доступність (Availability), а також середній час до відмови (MTTF), середній час між відмовами (MTBF) та середній час відновлення (MTTR).

Розвиток програмно-визначених мереж (SDN) та віртуалізації мережевих функцій (NFV) також сприятиме створенню більш гнучких та самовідновлюваних

мережевих інфраструктур. Нарешті, хмарні архітектури та розподілені системи за своєю суттю використовують принципи відмовостійкості, що вимагає подальших досліджень для управління їхньою складністю та забезпечення високої надійності в динамічних середовищах.

Отже, аналіз апаратних рішень для забезпечення відмовостійкості мереж підкреслює необхідність збалансованого підходу, що поєднує надійне апаратне забезпечення, інтелектуальне програмне управління, ретельне проектування та безперервний моніторинг для досягнення бажаного рівня стійкості та безперервності операцій.

ПЕРЕЛІК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Євсеєв С. П., Дженюк Н. В., Толкачов М. Ю. та ін. "Комп’ютерні мережі. Книга 1. Технології комп’ютерних мереж" Харків–Львів: "Новий Світ – 2000", 2025. - 471 с

2. Микитишин А.Г., Митник М.М., Стухляк П.Д. "Комп’ютерні мережі. Книга 1. Навчальний посібник для технічних спеціальностей ВНЗ" Рекомендовано МОН України, 2023. - 256 с

3. Задерейко О.В., Логінова Н.І., Толокнов А.А. "Комп’ютерні мережі: навчальний посібник"

4. PayPro Global. Що таке відмовостійкість і резервування в SaaS? [Електронний ресурс]. - Режим доступу: https://payproglobal.com/uk/відповіді/що-таке-відмовостійкійскість-і-надмірність-у-saas/

5. AlexHost. Що таке мережевий бондинг? Типи мережевих зв'язків [Електронний ресурс]. - Режим доступу: https://alexhost.com/uk/faq/shho-take-merezhevyj-bondyng-typy-merezhevyh-zvyazkiv/

6. Гаврилюк О. Дослідження управління надійністю та відмовостійкістю в інфокомунікаційних мережах // Науковий вісник ХНУРЕ. — 2023. - № 2. - С. 42–48.

7. Вісник Харківського національного університету ім. В. Н. Каразіна. Актуальні проблеми побудови комп'ютерних мереж // Серія: Математика, прикладна математика та інформатика. - 2024. - № 1307. - С. 110–120.

8. MyBook.biz.ua. Комп'ютерні мережі, книга.1. Навчальний посібник для технічних спеціальностей ВНЗ [Електронний ресурс]. - Режим доступу: https://mybook.biz.ua/ua/eom-informaciyni-ta-kompyuterni-mereji/kompyuterni-mereji-kniga1-navchalniy-posibnik-dlya-tehnichnih-specialnostey-vnz-rekomendovano-mon/

9. PayPro Global. Що таке балансування навантаження в хмарних обчисленнях? [Електронний ресурс]. - Режим доступу: https://payproglobal.com/uk/відповіді/що-таке-балансування-навантаження-в-хмарних-обчисленнях/

ДОДАТОК А. Слайди мультимедійної презентації

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

За спеціальністю: 123 «Комп'ютерна інженерія»

на тему: «Аналіз апаратних рішень відмовостійких комп'ютерних мереж»

м. Одеса
2025 р.

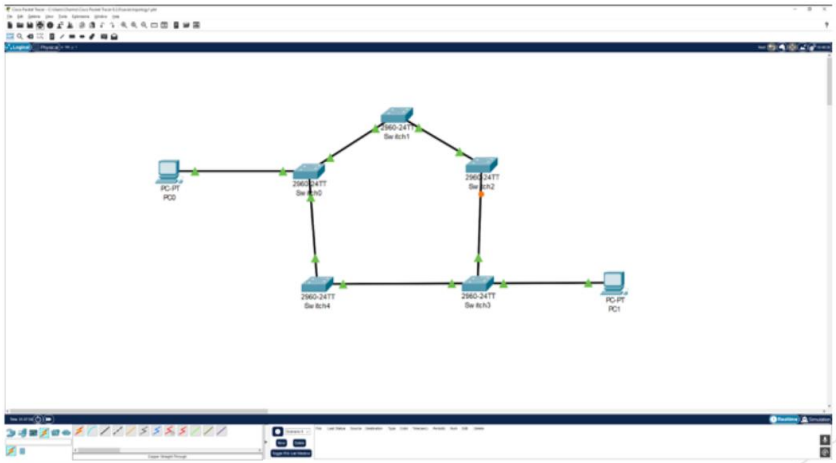
Розробив: Єрошенко М.С.
гр.2БКС-29
Керівник роботи: Кунуп Т.В.

Вступ

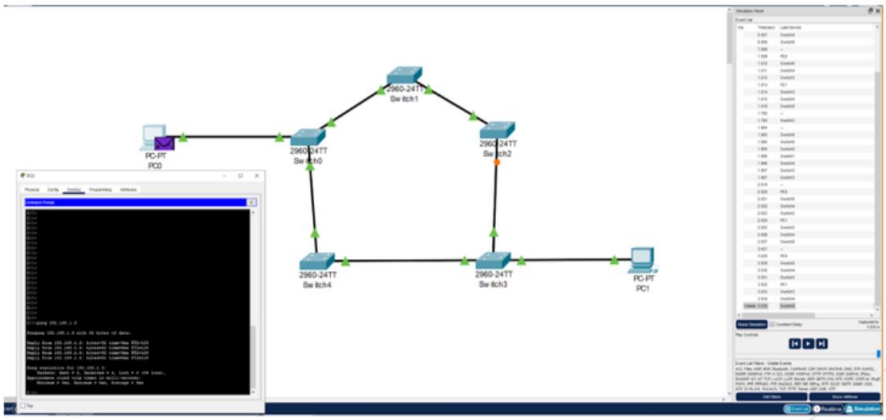
Сталий розвиток інформаційних технологій супроводжується зростанням кількості користувачів та обсягів обробки даних. Системи, що обробляють великі обсяги запитів, є значною частиною сучасної цифрової інфраструктури, що обслуговує мільйони користувачів одночасно. Оптимізація, шляхом використання сучасних апаратних рішень, є одним з важливих механізмів забезпечення стабільної роботи.

Актуальність дослідження апаратних рішень, що забезпечують відмовостійкість комп'ютерних мереж, обумовлена необхідністю оптимізації роботи систем при обробці запитів великої кількості користувачів та забезпечення відмовостійкості систем, в умовах часткових відмов компонентів.

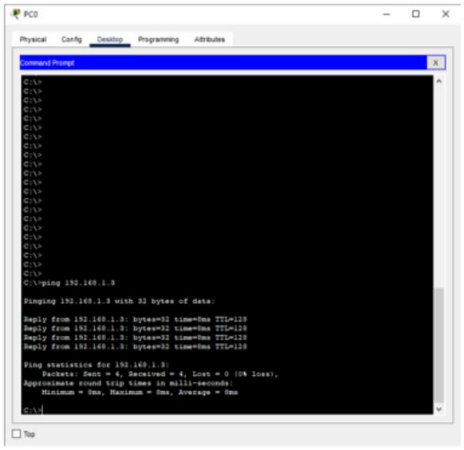
Загальна схема відмовостійкої мережі з резервними комутаторами



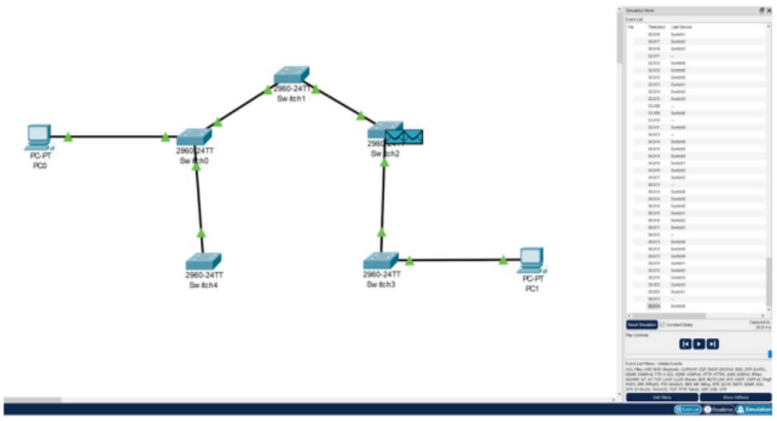
Моделювання роботи мережі з резервними комутаторами та анімація трафіку (PacketTracer)



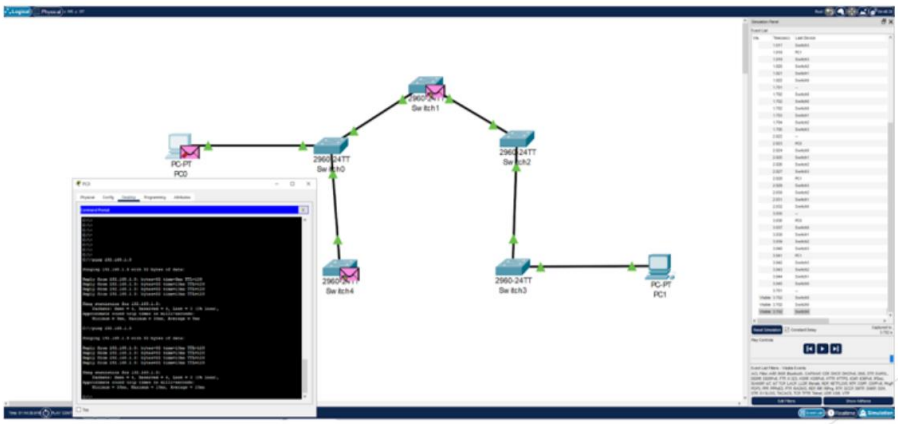
Визначення пінгу між вузлами мережі у нормальному стані



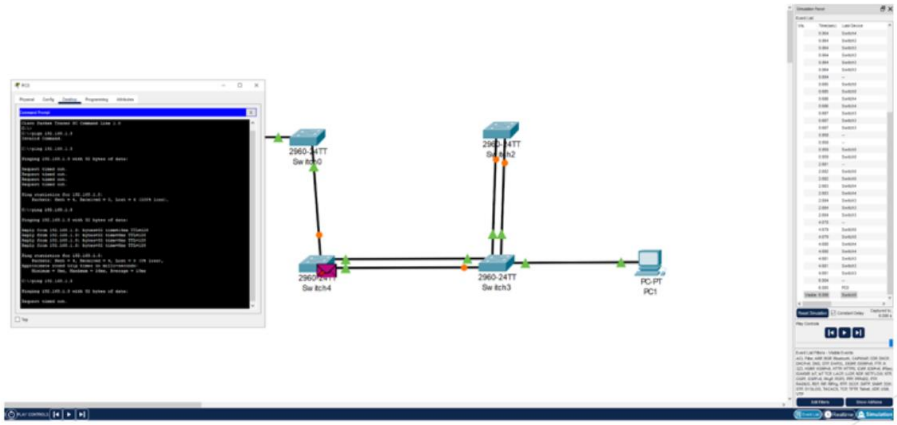
Модель мережі з імітацією збою - відключення інтерфейсу



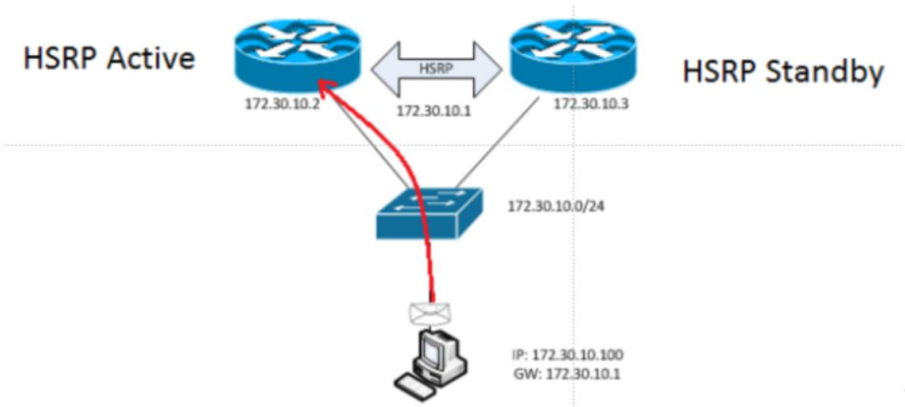
Модель мережі при відновленні з’єднання через резервний маршрут



Модель мережі після втрати одного з комутаторів



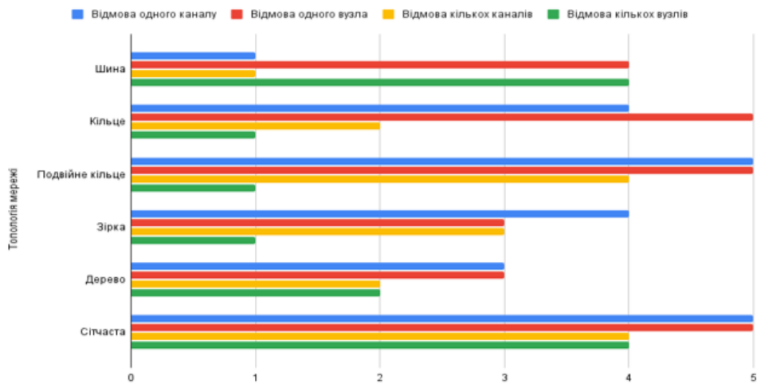
Конфігурація резервування шлюзу з використанням HSRP



Порівняльна таблиця апаратних рішень для відмовостійких мереж

Рішення	Опис	Основні переваги	Основні недоліки	Типове застосування
HSRP / VRRP	Протоколи резервування першого хопу (FHRP). Кілька фізичних маршрутизаторів об'єднуються у віртуальну групу з однією IP-адресою. Один маршрутизатор є активним, а інший перебуває в режимі очікування (standby).	Відносна простота налаштування; VRRP є відкритим стандартом; широка підтримка виробниками.	Зазвичай працює в режимі "активний/пасивний", що означає простій ресурсів резервного пристрою; є невеликий час на перемикання.	Забезпечення відмовостійкості шлюзу за замовчуванням для кінцевих пристроїв у мережах.
Стекування комутаторів (Switch Stacking)	Об'єднання кількох фізичних комутаторів (зазвичай до 8-9) в один логічний пристрій за допомогою спеціальних високошвидкісних портів та кабелів (напр., Cisco StackWise, Juniper Virtual Chassis).	Спрощене управління (один інтерфейс); висока пропускна здатність між комутаторами; швидке відновлення (sub-second failover).	Зазвичай вимагає обладнання одного вендора та однієї серії; обмежена відстань між комутаторами.	Рівень доступу або агрегації у мережах; комутатори Top-of-Rack (ToR) у невеликих центрах обробки даних (ЦОД).
Агрегація на рівні шасі (MLAG / vPC / VSS)	Технологія, що дозволяє підключати пристрій (сервер, інший комутатор) до двох окремих фізичних комутаторів, які для підключеного пристрою виглядають як єдине ціле.	Усуває блокування портів протоколом STP; повне використання пропускної здатності всіх каналів (активний/активний); високий рівень відмовостійкості.	Складніше в налаштуванні; переважно є пропрієтарною технологією конкретного вендора (напр., vPC у Cisco Nexus, VSS у Catalyst).	Ядро мережі ЦОД; підключення серверів та систем зберігання даних, що вимагають максимальної доступності та пропускної здатності.
Агрегація каналів (LACP / EtherChannel)	Об'єднання кількох фізичних портів в один логічний канал для збільшення пропускної здатності та резервування. Якщо один фізичний канал виходить з ладу, трафік продовжує йти через інші.	LACP є відкритим стандартом; збільшує пропускну здатність; забезпечує резервування на рівні порту/кабелю.	Не захищає від відмови всього комутатора, якщо всі порти підключені до одного пристрою.	З'єднання між комутаторами ("транки"); підключення серверів, мережевих сховищ (NAS/SAN), що потребують високої пропускної здатності.
Резервні компоненти в шасі	Використання модульних пристроїв з дублюючими компонентами: два або більше блоки живлення, змінні вентилятори, резервні модулі керування.	Захист від відмови окремого компонента (блок живлення, вентилятор) без простою всього пристрою; можливість "гарячої" заміни.	Значно збільшує вартість та складність обладнання; не захищає від збою програмного забезпечення.	Модульні комутатори та маршрутизатори ядра мережі, високопродуктивне обладнання для ЦОД та критично важливої інфраструктури.

Графіки порівняння ефективності моделей відмовостійкості мережі



Дякую за увагу