

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 проекту (роботи)

магістра

(ступінь вищої освіти)

на тему МЕРЕЖЕВА СИСТЕМА ПІДПРИЄМСТВА З ЕЛЕМЕНТАМИ
ПІДВИЩЕНОЇ НАДІЙНОСТІ

Виконав: студент 2 курсу, групи КНТ-612м
спеціальності

123 Комп'ютерна інженерія

(код і найменування спеціальності)

Освітня програма (спеціалізація)

«Спеціалізовані комп'ютерні системи»

ГРИГОРЯН М.С.

(ПРИЗВИЩЕ та ініціали)

Керівник ЗЕЛЕНЬОВА І.Я.

(ПРИЗВИЩЕ та ініціали)

Рецензент ЄФИМЕНКО М.В.

(ПРИЗВИЩЕ та ініціали)

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) «Спеціалізовані комп'ютерні системи»
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

Зав. кафедри Кудерметов Р.К.

“12” листопада 2023 року

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

ГРИГОРЯН Марині Степанівні

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Мережева система підприємства з елементами підвищеної надійності

керівник проєкту (роботи) к.т.н., доцент, ЗЕЛЕНЬОВА Ірина Яківна

(науковий ступінь, вчене звання, ПРИЗВИЩЕ, ім'я, по батькові)

затверджені наказом закладу вищої освіти від «24» жовтня 2023 року №400

2. Строк подання студентом проєкту (роботи) 11 грудня 2023 року

3. Вихідні дані до проєкту (роботи) АТ «ТехКом», що складається з 5 філій; в мережі 5 маршрутизаторів та 5 комутаторів із використанням технологій mesh, Ethernet, стандарту 100BaseTX, VPN із застосуванням протоколу GRE, використання 5 бездротових точок доступу та технології WiFi стандарту 802.11ac, статичної адресації IPv4 та динамічної маршрутизації

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1) Надійність обчислювальних мереж

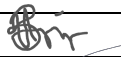
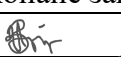
2) Вибір технологій, апаратних і мережних пристроїв

3) Дослідження впливу конфігурації мережі на показники її надійності

4) Розробка мережі з поліпшеною надійністю

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

6. Консультанти розділів проєкту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видала	прийняла виконане завдання
1-4	ЗЕЛЕНЬОВА І.Я., доцент		
нормоконтроль	ЩЕРБАК Н.В., ст. викл.		

7. Дата видачі завдання 01.10.2023 р.

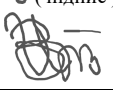
КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Аналіз наявних методів та алгоритмів пошуку об'єктів, перегляд отриманих результатів, виділення недоліків та переваг	05.09.2023 р.	
2	Розробка структури мережі	08.10.2023 р.	
3	Розробка алгоритму роботи мережі	04.10.2023 р.	
4	Використання роботи мережі	01.11.2023 р.	
5	Дослідження роботи мережі	09.11.2023 р.	
6	Оформлення отриманих результатів у ПЗ	10.11.2023 р.	
7	Оформлення графічного матеріалу	15.11.2023 р.	
8	Оформлення допоміжного матеріалу	20.11.2023 р.	

Студент(ка)


(підпис) Марина ГРИГОРЯН
(ім'я, ПРИЗВИЩЕ)

Керівник проєкту (роботи)


(підпис) Ірина ЗЕЛЕНЬОВА
(ім'я, ПРИЗВИЩЕ)

РЕФЕРАТ

ПЗ: 73 с., 28 рис., 3 табл., 28 посилань.

MESH, PACKET TRACER, КОНФІГУРАЦІЯ, КОМП'ЮТЕРНА МЕРЕЖА, КОМУТАТОР, МАРШРУТИЗАЦІЯ, МОДЕЛЬ, НАДІЙНІСТЬ, ПЕРЕДАЧА ДАНИХ, ПРИСТРІЙ

Об'єкт дослідження – засоби підвищення надійності мереж завдяки різним елементам, серед яких використання відмовостійкої конфігурації mesh.

Метою дослідження є підвищення надійності за допомогою технології mesh для створення мережі найкращої якості, яка діє на підприємстві, що займається збором та обробкою великої кількості даних.

У першому розділі розглядається надійність та доступність в інформаційних системах і бізнесі, основні аспекти підвищення готовності, важливість надійності в обчислювальних мережах.

У другому розділі міститься опис апаратної та кабельної частини проекту. Цей розділ містить вибір конкретних елементів реалізації логічної схеми.

У третьому розділі розглядається оцінка надійності роботи різних типів мереж за допомогою методу МШ та МП, побудова графів, що дає розбіг значень вірогідності безвідмовної роботи системи P_s , а також дає уявлення про точність розрахунків надійності.

У четвертому розділі розглянуто структуру АТ «ТехКом» в цілому та розроблено модель та граф-схему об'єднаної мережі АТ «ТехКом».

Робота має практичну цінність і може бути корисною для підвищення надійності та якості мережі АТ "ТехКом", що важливо для ефективного збору та обробки великих обсягів даних на підприємстві.

ABSTRACT

Explanatory note to the master's work: 73 p., 28 figures, 3 tables, 28 sources.

COMPUTER NETWORK, CONFIGURATION, DATA TRANSFER, DEVICES,
MODEL, MESH, PACKET TRACER, RELIABILITY, ROUTING, SWITCH

The object of research is the means of increasing the reliability of networks thanks to various elements, including the use of a fault-tolerant mesh configuration.

The purpose of the study is to improve reliability using mesh technology to create the best quality network operating in an enterprise that collects and processes a large amount of data.

The first chapter is about reliability and availability in information systems and business, the main aspects of increasing readiness, the importance of reliability in computer networks.

The second section contains a description of the hardware and cable part of the project. This section contains a selection of specific elements of the implementation of the logical scheme.

In the third section, the reliability assessment of the operation of various types of networks is considered using the MIII and MII method, the construction of graphs that gives the spread of the probability values of the failure-free operation of the Ps system, and also gives an idea of the accuracy of the reliability calculations.

In the fourth chapter, the structure of JSC "TechCom" as a whole is considered and a model (logical diagram) and graph diagram of the joint network of JSC "TechCom" is developed.

The work has practical value and can be useful for increasing the reliability and quality of the network of JSC TechCom, which is important for the effective collection and processing of large volumes of data at the enterprise.

ЗМІСТ

Перелік скорочень та умовних познач	7
Вступ	9
1 Надійність обчислювальних мереж	10
1.1 Надійність в інформаційних системах і бізнесі	10
1.2 Основні аспекти підвищення показників надійності	11
1.3 Актуальність підвищення надійності і аналіз факторів ризику	14
1.4 Постановка задачі розробки	18
2 Вибір технологій, апаратних і мережних пристроїв	19
2.1 Вибір системи моделювання локальної мережі	19
2.2 Вибір технологій і мережних пристроїв	22
2.3 Аналіз та вибір апаратних пристроїв	26
3 Дослідження впливу конфігурації мережі на показники її надійності	30
3.1 Основні типи конфігурації мереж та метод оцінки надійності	30
3.2 Оцінка надійності мереж «кільце» різної розмірності	35
3.3 Оцінка надійності мережі дерево	42
3.4 Оцінка надійності мережі зірка	44
3.5 Оцінка надійності mesh-мережі	47
3.6 Порівняльна характеристика різних топологій мереж	49
4 Розробка мережі з поліпшеною надійністю	53
4.1 Аналіз структури підприємства	53
4.2 Монтаж та налаштування мережі	56
4.3 Тестування працездатності мережі	67
4.4 Забезпечення мережевої безпеки та підключення до Інтернет	68
Висновки	70
Перелік джерел посилання	71

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАК

IP – Internet Protocol

LAN – Local Area Network

WAN – Wide Area Network

ПЗ – програмне забезпечення

ПК – персональний комп'ютер

ЦОД – центр обробки даних

МЗ – мережа зв'язку

IoT – Internet of Things

АТ – Акціонерне Товариство

FDDI – Fiber Distributed Data Interface

VPN – Virtual Private Network

VLAN – Virtual Local Area Network

OSPF – Open Shortest Path First

DHCP – Dynamic Host Configuration Protocol

OSI – Open Systems Interconnection

PDU – Power Distribution Unit

GRE – Generic Routing Encapsulation

PC – Personal Computer

LACP – Link Aggregation Control Protocol

MLT – Multi-link trunking

PAgP – Port Aggregation Protocol

IEEE – Institute of Electrical and Electronics Engineers

VRRP – Virtual Router Redundancy Protocol

HSRP – Hot Standby Router Protocol

PPP – Point-to-Point Protocol

HDLC – High-Level Data Link Control

МШ – мінімальні шляхи

МП – мінімальні перетини

CSMA/CA – Carrier-Sense Multiple Access with Collision Detection

UTP – Unshielded Twisted Pair

NIC – Network Interface Card

MDI – Medium Dependent Interface

ANSI – American National Standards Institute

ASNI TP-PMD – Twisted Pair Physical layer Medium Dependent

RJ45 – Registered jack-45

MLT-3 – Multi-Level Transmit-3

NRZI – NonReturn to Zero Inverted

STP – Spanning Tree Protocol

USB – Universal Serial Bus

Cisco IOS – Cisco Internetwork Operating System

IPS – in-plane switching

IPSEC – Internet Protocol Security

SSL – Secure Sockets Layer

DSP – Digital Signal Processor

PVC – Permanent Virtual Circuit

LSZH – Low Smoke Zero Halogen

S/FTP – Secure File Transfer Protocol

IPv4/ IPv6 – Internet Protocol version 4/6

GNS3 – Graphical Network Simulator-3

EVE-NG – Emulated Virtual Environment - Next Generation

VIRL – Virtual Internet Routing Lab

UNetLab – Unified Networking Lab

ВСТУП

У сьогоденні надійність комп'ютерних мереж відіграє дуже важливу роль для повноцінного та безвідмовного функціонування організації, компанії або підприємства. Тому надійність є актуальною темою, якщо хочеться, щоб була ідеальна робота мережі на підприємстві.

На даний час організації напружено працюють, тому що відбувається збільшення даних, які необхідно якнайшвидше передати через велику кількість пристроїв, використовуючи Інтернет. З цієї причини дуже багато уваги звертається саме на забезпечення надійності.

Також дуже важливим фактором надійності є збереження конфіденційності, оскільки стрімко зростає загроза кібератак та комп'ютерних вірусів.

Не менш актуальним питанням є стійкість мережі до відмови. Особливо важливо це для галузей з охорони здоров'я, військових операцій та інших, де навіть одна відмова пристрою мережі може бути критичною. Відмова будь-якої частини мережі може призвести до втрати ключових даних, але це не загрожує mesh-мережам, тому що дослідження доводить, що сітчасті мережі займають перше місце за надійністю, тобто характеризуються безвідмовною роботою. І це зрозуміло, чому. У mesh-мереж особлива структура, завдяки якій, якщо один пристрій відмовить у роботі, завжди буде інший, що безвідмовно продовжить роботу мережі, оскільки всі пристрої взаємозв'язані між собою.

Отже, глибоке розуміння мережевих операцій і можливостей для розширення, без зайвої інфраструктури, є актуальними питаннями сучасних інформаційних технологій. Впровадження mesh-мереж та інших технологічних інновацій у мережевих системах може значно підвищити якість та доступність мережевих послуг.

1 НАДІЙНІСТЬ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ

1.1 Надійність в інформаційних системах і бізнесі

У сучасному світі Інтернет характеризується розгалуженою мережею з десятків мільйонів серверів і постійно зростаючою кількістю робочих станцій. Ця технологія знаходить широке застосування в інформаційних системах і бізнес-секторі, тим самим підкреслюючи актуальність вирішення питання надійності мережі.

В наш час дослідження надійності набули значного поширення, особливо в контексті критичних систем, таких як телекомунікації, транспорт, механічні системи та видобуток нафти/газу. Забезпечення того, щоб користувач постійно отримував своєчасну відповідь, будь то в банкоматі під час транзакції чи в системі ракетної навігації, залежить від правильності введення даних, підкреслюючи першочергову важливість надійності.

Досягнення високої надійності та доступності є надзвичайно складним завданням у складних системах. Отже, системні розробники повинні вивчити низку підходів до цієї проблеми, ретельно оцінюючи переваги та недоліки кожного, перш ніж рекомендувати певний курс дій. Висновки повинні ґрунтуватися на аналізі фактів, а не просто на припущеннях. Іноді найефективнішим рішенням є оптимізація дизайну шляхом усунення рідко використовуваних і складних функцій. Перекопати зацікавлених сторін у тому, що «менше — це більше», може бути складно, але часто це виявляється оптимальним підходом [1].

Надійність і доступність системи повинні завжди бути ключовими факторами, поряд із такими факторами, як вартість, продуктивність, терміни розробки, ризик відмови та інші відповідні змінні. Іноді для досягнення кількох проектних цілей може знадобитися пожертвувати певними бажаними характеристиками. Системний інженер повинен пам'ятати, що завдання проектування включають як обов'язкові вимоги, так і бажані функціональні можливості. Хоча дизайн повинен відповідати основним специфікаціям, компроміс

щодо деяких бажаних функцій часто є прагматичним підходом до досягнення досконалості [2].

При оцінці надійності мережі як сукупної здатності всіх компонентів функціонувати без збоїв, може здатися, що Інтернет демонструє відносно низьку надійність через потенційну можливість збоїв або ізоляції вузлів або робочих станцій. Однак, якщо ми оцінюємо надійність як потенціал для зв'язку через величезну кількість вузлів і робочих станцій, Інтернет демонструє вражаючий рівень надійності. Варто зазначити, що це не гарантує бездоганну продуктивність, особливо якщо ваша конкретна робоча станція не входить до рівняння.

Підвищення рівня надійності вимагає прийняття різних стратегій, включаючи використання високоінтегрованих електронних компонентів, мінімізацію перешкод, оптимізацію схем і оптимізацію температурних умов. Надійність можна кількісно визначити за допомогою таких показників, як середній час до відмови та частота відмов. Кабельні системи та комутаційне обладнання, наприклад з'єднувачі та крос-панелі, відіграють ключову роль у надійності мережі, забезпечуючи безперервне з'єднання між окремими вузлами.

Підвищення доступності мережі передбачає розгортання механізмів контролю та виправлення помилок у поєднанні з автоматичним відновленням потоку даних після виявлення несправностей. Цей підхід мінімізує час простою простої системи, сприяючи безперебійній роботі. Ці міркування разом сприяють створенню надійних комп'ютерних мереж, невід'ємного компонента сучасного інформаційного ландшафту [3].

1.2 Основні аспекти підвищення показників надійності

Оцінка продуктивності системи обертається навколо ретельної перевірки коефіцієнтів готовності, основного показника надійності і валідності. Коефіцієнт готовності забезпечує час, протягом якого система працює без збоїв і ініціює

виклик, безперебійну роботу системи. Це обчислюється шляхом порівняння середнього часу роботи із загальним часом безвідмовної роботи та стандартним часом оновлення. Системи, які демонструють підвищений рівень обслуговування, є надійними.

Одним із основних шляхів підвищення готовності є встановлення результативності ефективності. Цей принцип включає в себе включення в конструкцію надійних варіантів відмовостійкості, що активуються, коли виникає потреба. У комп'ютерних мережах, що містять різні елементи різного типу, створення кожного ключового компонента системи є обов'язковим. Це особливо вірно для магістральних маршрутів, які керують встановленою мережею клієнта. Як правило, ці маршрути ведуть до корпоративних серверів, таких як сервери баз даних, веб-сервери та поштові сервери. Щоб забезпечити відмовостійкість, усі компоненти мережі, через які проходять такі маршрути, повинні бути резервованими. Для цього потрібні додаткові кабельні з'єднання, готові до активації в разі виходу з ладу основного кабелю. Крім того, всі пристрої зв'язку на магістральних маршрутах повинні бути обладнані засобами для забезпечення резервного моніторингу окремих компонентів.

Перемикання з основного пристрою на резервний, незалежно від того, чи відбувається це автоматично або вимагає втручання адміністратора, має вирішальне значення. Важлива примітка: менше перемикань покращує ефективність системи, що значно обмежує час простою мережі, не пов'язаний з людьми. Реалізація процедур автоматичної реконфігурації залежить від інтелектуальних комунікаційних пристроїв у мережі та централізованої системи керування, яка контролює мережу та забезпечує зворотний зв'язок [4].

Важливу роль відіграє різна потужність комп'ютерних систем, особливо в регіонах комп'ютерних країн світу. Гра включає кілька важливих подій:

- висока готовність (high availability): цей термін можна відносити до систем, обладнаних пристроями в режимі очікування та автономними програмами, які можуть швидко вимкнутися через 2-20 хвилин після цього;

- відмовостійкість (fault tolerance): ці функції доступні автоматично для систем, які можуть мати надлишкове резервування без підключення до загального резервування для всіх функцій блоку, включаючи процесори, блоки живлення, підсистеми введення/виведення та підсистеми підключення дисків. Коли ви шукаєте практичні речі та позики за лічені секунди;

- постійна готовність (continuous availability): цей період підтримується в системі, що закриває збій не більше ніж за кілька секунд, сигналізуючи, що це не був збій, а досвід, викликаний оновленням систем або послуг, заплановано.

Теорія надійності в комп'ютерних системах включає фундаментальні аспекти, створені задля вирішення завдань, що з аналізом і синтезом надійності. Початковий аспект передбачає виконання розрахунків щодо визначення кількісних параметрів надійності існуючих або майбутніх систем, для забезпечення їх відповідності встановленим вимогам. Цей аспект відіграє у забезпеченні високої надійності системи.

Другий важливий аспект спрямовано на створення надійної системи, покликаній забезпечити необхідний рівень надійності. Для оцінки надійності складних систем використовуються різні атрибути, зокрема:

- доступність: цей атрибут визначає час безвідмовної роботи системи. Підвищення доступності передбачає запровадження резервування в архітектуру системи. Це особливо актуально для мереж, де захист даних та захист від пошкодження мають вирішальне значення, забезпечуючи цілісність та доступність даних;

- безпека. Цей атрибут оцінює здатність системи захищати дані від несанкціонованого доступу. Підтримка високого рівня безпеки є важливим компонентом надійності системи, враховуючи потенційні ризики, пов'язані зі шкідливими загрозами, включаючи витік та пошкодження даних;

- відмовостійкість: цей аспект пов'язаний із здатністю системи приховувати від користувача відмову окремих компонентів. Хоча вихід з ладу одного елемента може погіршити продуктивність системи, він повинен призводити

до повного відключення. Система має продовжувати функціонувати, використовуючи наявні ресурси.

У контексті корпоративних мереж одним із основних елементів, що впливають на надійність, є мережа зв'язку (МЗ). Важливо наголосити, що надійність МЗ — це засіб досягнення максимальної ефективності мережі, а не самоціль.

Визначення оптимального рівня надійності МЗ залежить від багатьох факторів, у тому числі від призначення МЗ, її структури, ступеня пошкодження через втрату доступу, алгоритмів управління, що використовуються, надійності окремих компонентів МЗ та інших змінних. Оптимальний рівень надійності МЗ визначається стадії проектування верхнього рівня, де МЗ сприймається як підсистема. Цей підхід враховує конкретні випадки використання та вимоги до надійності, інтегруючи надійність МЗ із більш широкими цілями системи.

Загалом, теорія надійності та практичні підходи до забезпечення надійності корпоративних мереж є складними та багатоетапними завданнями, які вимагають уважного аналізу, розрахунків та керування для досягнення необхідних рівнів надійності та ефективності мережі [3, 5, 6].

1.3 Актуальність підвищення надійності і аналіз факторів ризику

Надійність мережі залишається актуальною та важливою темою у світі. Мережі відіграють центральну роль у сприянні передачі даних, уможливленні обміну інформацією та сприянні спілкуванню між людьми та пристроями. Незважаючи на постійний технологічний прогрес і вдосконалення мережевої інфраструктури, проблеми з надійністю все ще можуть виникати з серйозними наслідками.

Декілька факторів підкреслюють незмінну актуальність надійності мережі:

— власність бізнесу: багато організацій у своїй щоденній діяльності значною мірою покладаються на мережі. Збої в мережі можуть призвести до значних фінансових невдач, втрати даних, зниження продуктивності та шкоди репутації компанії;

— збільшення обсягу даних: обсяг даних, що передаються через мережу, продовжує зростати з кожним роком. У той же час зростає потреба в надійних мережевих інфраструктурах, які можуть ефективно обробляти та передавати значні обсяги даних без втрат і затримок;

— кібербезпека: із зростанням кількості кібератак і зловмисного програмного забезпечення захист мереж стає все більш критичним. Компанії та установи повинні вжити заходів для захисту своїх мереж від зовнішніх загроз і розгорнути механізми виявлення і попередження інцидентів;

— інтернет речей (IoT): поширення Інтернет-пристроїв, включаючи інтелектуальні пристрої, датчики та промислове обладнання, потребує надійних і послідовних мереж для безперебійного обміну даними. Збої в мережі можуть призвести до несправності інтернет-пристроїв і навіть створити ризики для безпеки та конфіденційності;

— мобільні мережі: еволюція мобільних технологій і мереж зв'язку ставить перед постачальниками послуг мобільного зв'язку завдання забезпечити надійність і якість зв'язку в різних областях і умовах. Користувачі очікують постійної доступності та стабільної швидкості з'єднання в мобільних мережах, підкреслюючи важливість надійності мережі для задоволення їхніх вимог;

— розподілені системи: сучасні програми та системи часто працюють у розподілених середовищах, використовуючи такі технології, як хмарні обчислення. В таких умовах особливого значення набуває надійність мережевих з'єднань. Збої або затримки можуть призвести до збою програм і значно порушити бізнес-процеси.

За своєю суттю надійність мережі є стрижнею безперебійного функціонування сучасного бізнесу та технологій, що розвиваються, які лежать в основі нашого взаємопов'язаного світу.

Зрештою, надійність мережі є критичною проблемою, яка має глибокий вплив на бізнес, суспільство та нестабільність загалом. Поява Інтернету речей, мобільних мереж і технологій розподілених систем додає цьому актуальності. Отже, підприємства та установи повинні активно вдосконалювати свою мережеву інфраструктуру та розробляти стратегії для забезпечення надійності та безпеки своїх мереж.

Дослідження надійності мережі в даний час займають чільне місце в глобальному ландшафті, намагаючись оцінити та підвищити стійкість і надійність мережевих систем. Він забезпечує всебічний аналіз різних аспектів мережевих компонентів і компонентів мережі та їх взаємодії.

Ось основні напрямки дослідження надійності мережі:

- аналіз відмовостійкості: у цій області можна визначити вразливі та слабкі місця в мережі, які можуть призвести до збоїв. Це включає оцінку надійності апаратного забезпечення, ресурсів резервного копіювання та налаштування параметрів резервного копіювання та аварійного відновлення;

- продуктивність. Дослідження в цій галузі спрямовані на вимірювання та покращення продуктивності мережі. Це включає вимірювання пропускної здатності, затримки даних, надійності з'єднання та інших функцій, які можуть впливати на продуктивність мережі;

- моделювання. Моделювання мережі та імітація дозволяє дослідникам ретельно вивчати різні сценарії та умови мережі. Це дозволяє оцінити його надійність і ефективність при різних навантаженнях, конфігураціях і стратегіях маршрутизації;

- безпека мережі: цей розділ присвячено аналізу та пом'якшенню загроз безпеці мережі, охоплюючи такі області, як пріоритетне програмне забезпечення, виявлення мережевого протоколу та вразливості системи. Дослідники також розробляють методи виявлення та пом'якшення таких загроз;

- управління мережею: Дослідження спрямовані на розробку методологій інтелектуального управління мережею, способів забезпечення

автоматичної трансформації, оптимізації та відновлення мережі. Ці зусилля зменшують ризики та підвищують надійність мережі.

Ці аспекти являють собою лише частину багатогранного дослідження надійності мережі. Ця величезна територія продовжує зростати з розвитком нових технологій і зростаючими потребами в ландшафті. Створення цих запитів для оцінки надійності мережі, виявлення вразливостей мережі та надання інформації, яка має вирішальне значення для розробки стратегій підвищення надійності мережі, покращення безпеки та оптимізації продуктивності.

Підвищення ефективності комп'ютерних мереж залишається тісно пов'язаним з оцінкою показників надійності та управлінням вибраними ризиками. Аналіз надійності базується на структурі мережі, надійності технічних рішень і програмного забезпечення. Для підвищення рівня надійності використовувалися різноманітні резервні копії, переважно структурного та тимчасового характеру.

Концепція ризику базується на кумулятивній ймовірності виникнення небезпечних подій і подальших наслідків, які можуть призвести до збою для користувачів і керівництва, покриваючи фінансові та матеріальні збитки. У комп'ютерних мережах інформація розглядається як нові знання від користувачів, що є критично важливим для прийняття обґрунтованих рішень. Однак завжди існує ризик неточностей в отриманих даних.

Під час перевірки надійності комп'ютерних мереж беруть участь кілька факторів. По-перше, комп'ютерні мережі стикаються з унікальними проблемами, такими як втрата даних, витік інформації, порушення конфіденційності та вплив вірусів та інших форм кібератак. У розрахунках надійності та оцінці ризиків у різних категоріях ці аспекти набувають першочергового значення.

Крім того, комп'ютерні мережі знаходяться в стані постійної еволюції: розширюється база даних, розширюється коло вирішуваних завдань, програмні та апаратні компоненти, а також архітектура піддаються постійній модернізації. Оцінка надійності та управління ризиками комп'ютерних мереж вимагає постійної адаптації до нових викликів і можливостей. Підтримка надійності та безпеки комп'ютерних мереж потребує постійного моніторингу показників надійності та

виявлення ризиків протягом усього часу їх експлуатації. Більшість проблем у комп'ютерних мережах демонструють складні та невизначені характеристики, які потребують ефективних рішень. Інформація в комп'ютерних мережах стає основним ресурсом для прийняття рішень, через що сфера комп'ютерних мереж переповнюється проблемами, пов'язаними з організаційною конкурентоспроможністю.

Ключовим аспектом ефективності рішень, пропонованих на терміналах комп'ютерної мережі, є ступінь інтелекту, яким володіють компоненти мережі. Аналіз ризиків залежить від співвідношення між ймовірністю виникнення неприємних подій і відкритими наслідками, які можуть завдати шкоди користувачам і адміністраторам. Цей аналіз враховує як суб'єктивні елементи, пов'язані з діями персоналу, так і об'єктивні фактори, такі як зміни зовнішнього середовища.

Одним із основних завдань у галузі надійності мереж є спрощення проектування мережі при збереженні високої надійності. Це передбачає побудову алгоритмів, які враховують характеристики компонентів мережі та критерії проектування. Точні аналітичні вирази можуть бути дуже складними, тому моделі для проектування вибирають заміники [3, 7].

1.4 Постановка задачі розробки

В процесі проектування мережі визначено основні задачі, які необхідно вирішити в ході проектування комп'ютерної мережі АТ «ТехКом», зробити:

- аналіз технічних характеристик;
- вибір мережевих пристроїв;
- аналіз апаратного забезпечення;
- вибір системи моделювання локальної мережі;
- аналіз та вибір технології LAN та WAN підключень для відділів;

- розміщення та налаштування мережевого обладнання;
- підвищення надійності мережі;
- вибір типу конфігурації мережі;
- граф-схему мережі;
- вибір принципу маршрутизації та адресації;
- забезпечення мережевої безпеки;
- підключення мережі до інтернету;
- налаштування мережі;
- тестування мереж.

Висновки: отже, надійність комп'ютерних мереж є невід'ємною складовою будь-якого підприємства, організації або бізнесу, тому важливо знати аспекти підвищення показників надійності завдяки різним методам, які буде використано для створення безпеки та надійних умов для мережі підприємства.

2 ВИБІР ТЕХНОЛОГІЙ, АПАРАТНИХ І МЕРЕЖНИХ ПРИСТРОЇВ

2.1 Вибір системи моделювання локальної мережі

Cisco Packet Tracer - це програмне забезпечення для створення моделей мережі, який надає студентам і професіоналам в області мережевої інфраструктури можливість використовувати віртуальні пристрої для експериментування, налаштування та відлагодження різних мережевих схем.

Основні функції Cisco Packet Tracer:

— створення мережі: у Cisco Packet Tracer є можливість створювати мережі з різними віртуальними пристроями, такими як маршрутизатори, комутатори, ПК (персональний комп'ютер), сервери, IP-телефони і інші. Ви можете конфігурувати ці пристрої та розташовувати їх у віртуальному середовищі для створення різних мережевих топологій;

— налаштування мережі: Cisco Packet Tracer дозволяє налаштовувати пристрої та виконувати тестування мережевих схем без необхідності фізичного доступу до обладнання. Ви можете використовувати різні інструменти, такі як ping, tracer, telnet, ssh і багато інших, для відлагодження проблем мережі та налаштування її роботи;

— навчальні можливості: Cisco Packet Tracer також є потужним засобом для навчання. Він містить безліч вправ і завдань, які допомагають студентам оволодіти роботою з мережевими пристроями і мережевими протоколами [8, 9].

Порівняємо Cisco Packet Tracer з аналогами та альтернативами для моделювання мереж:

а) GNS3 (Graphical Network Simulator-3):

- 1) Cisco Packet Tracer: основний фокус на освіті, спрощений інтерфейс, більш підходить для новачків;
- 2) GNS3: спрямований на професіоналів, дозволяє використовувати реальне обладнання та віртуальні машини для моделювання мереж. Має більше можливостей для налаштування.

б) EVE-NG (Emulated Virtual Environment - Next Generation):

- 1) Cisco Packet Tracer: простий у використанні, зручний для освіти, обмежений у функціональності;
- 2) EVE-NG: має більше функцій і підтримує різні типи віртуальних машин та обладнання, але складніший у використанні.

в) Boson NetSim:

- 1) Cisco Packet Tracer: безкоштовний для освіти, спеціалізований на Cisco-обладнанні, обмежений в можливостях моделювання;
- 2) Boson NetSim: має більше підтримуваного обладнання та підтримує інші виробники, але є комерційним продуктом.

г) VIRL (Virtual Internet Routing Lab):

- 1) Cisco Packet Tracer: простий у використанні, безкоштовний для освіти, обмежений в підтримці деякого обладнання;

- 2) VIRL: має більше підтримуваного Cisco-обладнання та більше можливостей для налаштування, але є комерційним продуктом.

г) Dynamips / Dynagen:

- 1) Cisco Packet Tracer: простий у використанні, спеціалізований на Cisco-обладнанні, обмежений в можливостях моделювання;
- 2) Dynamips / Dynagen: дозволяє використовувати реальні IOS-зображення Cisco для моделювання мереж. Складніший у використанні, але має більше можливостей.

д) UNetLab (Unified Networking Lab):

- 1) Cisco Packet Tracer: простий у використанні, безкоштовний для освіти, спеціалізований на Cisco-обладнанні;
- 2) UNetLab: дозволяє використовувати різні віртуальні машини та обладнання в одному середовищі. Має більше можливостей, але складніший у використанні.

Основними перевагами Cisco Packet Tracer є:

- навчання та освіта: Packet Tracer є важливим інструментом для навчання мережевої інфраструктури. Він використовується в багатьох академічних програмах і курсах, щоб надати студентам можливість навчатися практичним навичкам налаштування та управління мережами;
- безкоштовний доступ для освіти: Cisco надає безкоштовний доступ до Packet Tracer для освітніх закладів та студентів, що сприяє поширенню цього інструменту в освітньому середовищі;
- моделювання мереж: Packet Tracer дозволяє створювати та моделювати різноманітні мережеві сценарії, включаючи роботу з маршрутизаторами, комутаторами, ПК, IP-телефонами і іншим обладнанням;
- відлагодження мереж: Інструменти Packet Tracer дозволяють відлагоджувати мережеві проблеми, використовуючи команди ping, tracer, telnet, ssh та інші, що допомагає користувачам вирішувати проблеми мережі;

- багатомовність: Packet Tracer підтримує декілька мов інтерфейсу, що дозволяє користувачам з різних країн використовувати інструмент на своїй рідній мові;
- однією з найкращих переваг є режим Sim, який інакше недоступний у реальному спорядженні;
- дозволяє користувачам моделювати конфігурацію маршрутизаторів Cisco.

Недоліки Cisco Packet Tracer:

- обмежена функціональність: У порівнянні з більш складними програмами для моделювання мереж, Packet Tracer може бути обмеженим за функціональністю і можливостями моделювання;
- спрощена модель мережі: Packet Tracer використовує спрощену модель мережі, яка може не враховувати всі деталі та складності реальних мереж;
- обмежена підтримка деяких продуктів: Деякі продукти та пристрої, які підтримуються в реальних мережах, можуть бути відсутніми в Packet Tracer.

Кожен з цих інструментів має свої переваги і недоліки, і вибір залежить від конкретних потреб та рівня експертизи. Cisco Packet Tracer відмінно підходить для освіти та навчання, але, можливо, не надто підходить для складних професійних сценаріїв моделювання мережі. Загалом, Cisco Packet Tracer є потужним інструментом для навчання та моделювання мереж і корисним для освіти та практичних вправ [10].

2.2 Вибір технологій і мережних пристроїв

Під час аналізу вже існуючих LAN і WAN технологій в мережі АТ "ТехКом" розглядається основний механізм передачі інформації - магістраль. Магістраль виступає важливою частиною зв'язку між віддаленими вузлами корпоративної мережі та виконує одну з ключових функцій - транспортування даних між вузлами

мережі АТ "ТехКом". Давайте розглянемо різні мережеві архітектури, які використовуються при розробці магістральних мереж:

- Wide Area Networks (WAN): широко зонні мережі, які охоплюють великі географічні відстані і забезпечують зв'язок між віддаленими офісами чи об'єктами АТ "ТехКом";

- Local Area Networks (LAN): локальні мережі, які створюють мережеве оточення для групи комп'ютерів, що знаходяться близько один від одного, як правило, в одному приміщенні, офісі чи на невеликій відстані.

Якщо мова йде про LAN, цей вид підключення дозволяє об'єднати комп'ютери, розташовані в невеликій відстані один від одного в локальне мережеве середовище. Важливим аспектом є можливість підключення декількох комп'ютерів до однієї точки доступу, що реалізована за допомогою маршрутизатора.

Кожний LAN-порт на маршрутизаторі дозволяє об'єднати групу ПК в одній точці доступу, створюючи мережу, яка може охоплювати певну територію, наприклад, всередині одного будинку чи на невеликій відстані від нього. Для цього часто використовують високопропускні кабелі та мережеве обладнання.

WAN - цей вид підключення створює зовнішню мережу, що об'єднує велику кількість груп користувачів, незалежно від їх місцезнаходження. Основна відмінність полягає в тому, що попередній формат спрямований на внутрішнє об'єднання декількох ПК, тоді як цей тип зв'язку є зовнішнім.

Існують різні глобальні мережі, але найбільш відомою і широко використовуваною є Всесвітня павутина. Багато користувачів на різних відстанях віддають перевагу їй, оскільки вона не має географічних обмежень, створена за допомогою телефонних ліній і передових технологій.

Можливо, ви бачили роз'єм типу WAN, коли купували та налаштовували маршрутизатор. В нього підключається кабель від вашого інтернет-постачальника. Різні порти виконують різні функції, один з них передає сигнал до пристроїв, які підключені до роутера.

Технічні аспекти. Основні відмінності між цими форматами включають:

- перший вид допомагає створювати внутрішню мережу, в той час як WAN використовується для глобального об'єднання користувачів;
- локальна мережа має обмеження за кількістю клієнтів та територією, в той час як глобальна мережа не має цих обмежень;
- за швидкістю: передачі даних по мережі LAN швидше, ніж WAN;
- затримка передачі даних між пристроями в LAN менше, ніж в WAN мережах;
- ключова відмінність LAN від WAN криється на фізичному та каналному рівнях, різні порти використовують різні протоколи передачі даних: Ethernet і 802.11 для локальних мереж та PPP, HDLC, Frame Relay для глобальних.

Користувачам необхідно знати, в яких ситуаціях використовувати ці порти при підключенні домашнього роутера для інтернету. LAN-порт призначений для з'єднання комп'ютерів у випадку, коли їх кілька, тоді як WAN-порт дозволяє отримувати сигнал від постачальника послуг Інтернету [11].

Розглянемо мережеві архітектури, що використовуються при проектуванні мережі АТ «ТехКом». Враховуючи вимоги до них, описані в попередньому розділі, можна виділити дві основні технології побудови мереж:

- Fast Ethernet;
- Gigabit Ethernet.

У проектуванні мережі АТ «ТехКом» була використана технологія Fast Ethernet.

Fast Ethernet - це стандарт IEEE 802.3u, який був офіційно прийнятий 26 жовтня 1995 року. Ця специфікація визначає протокол каналного рівня для комп'ютерних мереж зі швидкістю передачі даних 100 Мбіт/с. Важливо зауважити, що стандарт Fast Ethernet є спадкоємцем попереднього стандарту Ethernet IEEE 802.3, і він зберіг формат кадру, механізм доступу до середовища CSMA/CD та топологію "зірка". Однак Fast Ethernet внесло певні зміни у конфігурацію фізичного рівня, що призвело до підвищення пропускної здатності мережі, включаючи використання різних типів кабелю, збільшення довжини сегментів і кількості концентраторів.

Стандарт Fast Ethernet описує три основних типи середовищ передачі сигналів Ethernet із швидкістю 100 Мбіт/с:

— 100Base-TX: даний стандарт використовує дві кручені пари проводів для передачі даних. Він дотримується стандартів ANSI для передачі даних у крученому фізичному середовищі. Кручений кабель може бути як екранованим, так і неекранованим. Для кодування даних використовується алгоритм 4В/5В та метод фізичного кодування MLT-3.

— 100Base-FX: цей стандарт використовує дві жилки оптоволоконного кабелю для передачі даних і також дотримується стандартів ANSI. Для кодування даних використовується алгоритм 4В/5В та метод фізичного кодування NRZI.

Ці два стандарти також відомі як 100Base-X. Передача даних в 100Base-TX використовує дві кручені пари, де одна пара використовується для передачі даних, а інша - для прийому. Це забезпечує сумісність із стандартами як екранованих, так і неекранованих кручених пар.

Серед інших особливостей, стандарт Fast Ethernet встановлює роз'єм MDI (Medium Dependent Interface), який залежить від середовища. Для кабелю на неекранованих кручених парах використовується восьми контактний роз'єм RJ45 категорії 5. Для кабелю на екранованих кручених парах використовується роз'єм STP типу 1.

Плата NIC для мереж 100Base-TX і 10Base-T використовує роз'єм RJ 45 для забезпечення сумісності з існуючими кабельними розведеннями категорії 5. Кабель UTP категорії 5(е) використовується для інтерфейсу середовища UTP 100Base-TX. Кабель має дві пари проводів, де чотири з них не використовуються для передачі даних, щоб уникнути перехресних наведень і спотворень сигналу. Пари проводів використовуються для передачі сигналів передачі та прийому і поляризовані, де один провід передає позитивний (+) сигнал, а інший - негативний (-).

Роз'єм RJ45 кабелю для мереж 100Base-TX і 10Base-T має змінені номери контактів для забезпечення сумісності. В стандарті ANSI TP-PMD контакти 7 і 9 використовуються для прийому даних. Однак у стандартах 100Base-TX і 10Base-T

ця функція призначена для контактів 3 і 6, що дозволяє забезпечити сумісність з попередніми версіями Ethernet.

Крім того, стандарт 100Base-TX також підтримує кабель STP типу 1 з опором 150 Ом. Цей кабель застосовується менше, і його основним призначенням є встановлення мереж Token Ring. Кабелі STP типу 1 мають дев'ятиконтактний роз'єм типу D з використанням контактів 1, 2 і 5, 9 у роз'ємі DB-9. Якщо плата мережевої карти (NIC) не має роз'єму DB-9, то до кінців кабелю STP можна підключити роз'єм RJ45 категорії 5 для забезпечення сумісності [12].

Загалом, стандарт Fast Ethernet був важливим кроком у розвитку комп'ютерних мереж, оскільки він дозволив підвищити швидкість передачі даних на старих кабельних системах, що вже були використані в попередніх версіях Ethernet. Це сприяло швидкому поширенню 100 Мбіт/с Ethernet і стало основою для подальшого розвитку мереж і переходу до стандартів Gigabit і 10 Gigabit Ethernet [13].

2.3 Аналіз та вибір апаратних пристроїв

Одним із ключових кроків у процесі проектування мережі АТ «ТехКом» є вибір маршрутизаторів та комутаторів, які будуть використовуватися у вузлах локальної мережі. Це обладнання відіграє ключову роль у функціонуванні мережі в цілому. Особливо важливо, щоб обрані комутатори та маршрутизатори дозволяли користувачам мережі передавати інформацію відповідно до стандартів без зайвих ускладнень.

Маршрутизатор Cisco 2901. Маршрутизатор Cisco 2901 відноситься до нового покоління модульних мережних маршрутизаторів, спеціально розроблених для роботи в конвергентних мережах. Це обладнання забезпечує надійне і безпечне підключення до Інтернету і є оптимальною платформою для розгортання різноманітних мережевих програм.

Маршрутизатори відрізняються високою рівнем надійності та продуктивності, а також мають гнучку апаратну платформу, що підтримує масштабування та можливість встановлення додаткових модулів інтерфейсу. Вони використовують оновлену операційну систему, яка включає в себе: широкий набір функціональних інструментів; підтримку всіх необхідних мережевих протоколів; функції аналізу мережевого трафіку; інструменти моніторингу та контролю роботи обладнання.

Маршрутизатор Cisco 2901 побудований на основі високопродуктивної архітектури, що забезпечує найкраще у своєму класі співвідношення між продуктивністю та ціною мережевого обладнання.

Просте керування. Для управління модульними маршрутизаторами використовується інтерфейс mini-USB. Це спрощує процедуру інсталяції та подальшого обслуговування мережного обладнання. При встановленні SEC-ліцензії користувачеві стають доступні функції апаратно підтримуваної технології IPSEC VPN.

Маршрутизатор Cisco 2901 працює під керуванням операційної системи Cisco IOS, яка має всі необхідні функції для виконання всіх завдань, покладених на нього. З обладнанням постачається набір повноцінних безкоштовних ліцензій для Firewall, захисту від вторгнень IPS, IPSEC VPN та IP-телефонії. Ліцензії є дійсними протягом 90 днів з моменту їх активації.

Високий рівень безпеки. Маршрутизатори Cisco 2901 використовують технологію IPS для захисту від вторгнень і мають вбудовану апаратну підтримку протоколів шифрування SSL і IPSEC. Вони також підтримують DSP і успішно впораються з завданнями безпеки інформаційного трафіку завдяки потужному багатоядерному процесору.

Завдяки модульній платформі, маршрутизатори можуть використовуватися як рішення для підтримки IPSEC VPN доступу та розгортання безпечної IP-телефонії та WI-FI зв'язку [14].

Комутатор Cisco Catalyst 2950-24. У рамках лінійки Cisco Catalyst 2950 Series виробник представив комутаційне обладнання з функцією автономної роботи, що

робить його ідеальним варіантом для будь-якого середовища. Моделі впевнено функціонують в інфраструктурі Ethernet, незалежно від протоколу (Fast або Gigabit). Користувачі мають можливість налаштовувати необхідну конфігурацію та отримувати продуктивність, враховуючи особливості середовища передачі. Системи постачаються з двома варіантами програмного забезпечення і кількома варіантами попередньої настройки, що спрощує адаптацію до потреб конкретної організації. Комутатори підходять для комерційних організацій, віддалених об'єктів та промислових середовищ.

Переваги обладнання:

- користувачам серійних моделей Cisco Catalyst 2950 Series пропонується зручна та зрозуміла панель адміністрування. Система автоматично виконує моніторинг та корекцію мережних неполадок;
- завдяки своїй гнучкості, комутатори швидко інтегруються в існуючі інфраструктури, що дозволяє користувачам уникнути додаткових витрат на обладнання та супутні послуги;
- усі пристрої, представлені в лінійці комутаторів, є неблокуючими, що означає відсутність раптової зупинки роботи портів або інших вузлів на каналі;
- обладнання має високий потенціал масштабування. Кількість каналів може збільшуватися за необхідності, і в ньому задіяні резервні джерела живлення [15].

Вита пара представляє собою кабель, всередині якого містяться декілька скручених у пучок ізольованих провідників. Зазвичай кабель має 2 або 4 пари внутрішніх жил. Скрутка провідників забезпечує надійний захист кабелю від перешкод. Додатковий екран служить для захисту витой пари від радіочастотних перешкод. Тому екранований витий кабель часто використовується там, де є джерело потужного електромагнітного випромінювання.

Основні конструктивні елементи витой пари включають:

- провідники з міді або біметалу;
- ізоляцію провідників;
- захисний екран з алюмінієвої фольги;

- дренажний провід;
- зовнішню оболонку з PVC (ПВХ).

Оболонкою витой пари, в основному, є такі матеріали:

- PVC (ПВХ) – полівінілхлорид, який застосовується для внутрішньої прокладки;
- PE-поліетилен, використовується головним чином у кабелях для зовнішньої прокладки;
- LSZH (Low Smoke Zero Halogen) - оболонка з низьким викидом диму і нульовим вмістом галогенів. Цей тип кабелю є пожежобезпечним і призначений для прокладки в місцях, де можливе масове скупчення людей.

Вита пара широко використовується в телекомунікаційних системах, зокрема в телефонних лініях для передачі голосу і даних, а також в локальних мережах.

Основними перевагами використання витой пари на основі мідного кабелю порівняно з оптичними технологіями є її доступність і простота монтажу. Монтажнику достатньо мати необхідний інструмент для обтиску (крімпер) та конектори типу RJ45. Кабелі на основі мідного кабелю виявляються менш вразливими до механічних пошкоджень і вимагають менше зусиль для ремонту. У разі пошкодження конектора витой пари його можна легко та економічно замінити.

Щодо видів захисного екрану кабелю вита пара, то існують два основних типи: одинарний, який включає металізовану полімерну плівку, і подвійний, що містить фольгу і плетіння з міді. Пари в кабелі зазвичай оточені одинарними екранами з фольги або плівки. Подвійні екрани витой пари можуть зустрічатися в кабельній техніці, але в комп'ютерних мережах вони рідко використовуються.

Структура загальних кабельних екранів може відрізнятися залежно від типу. У випадку, коли екран виконаний з фольгової плівки, вона зазвичай розташована з алюмінієвою стороною всередині, спрямованою до серцевини кабелю, і по тій же стороні прокладається дренажний провід. У разі, якщо над фольговою плівкою є додаткове плетіння, то шар алюмінію часто звертається назовні, і обплетення контактує з ним.

За стандартом ІЕС61156-5 розрізняються дві групи виробів: рівень 1 та рівень 2 (кабель з плівковим екраном). Згідно цього стандарту, кабель UTP повинен мати ступінь придушення зовнішнього впливу на рівні 40 дБ, тоді як в конструкціях витої пари S/FTP ця величина становить 85 дБ [16].

Висновки: було проведено аналіз вибору системи моделювання локальної мережі та встановлено, що для даної розробки мережі підійде Cisco Packet Tracer, який є безкоштовним та потужним інструментом для створення будь-яких мереж, як для студентів, так і для просунутих користувачів. Обрана технологія Fast Ethernet пропонує такі переваги, як збільшена пропускна здатність мережі, універсальна сумісність з різними типами кабелів, збільшена довжина сегментів і підвищена ємність концентратора, що сприяє ефективній передачі даних у комп'ютерних мережах на швидкості 100 Мбіт/с. Маршрутизатор Cisco 2901 і комутатор серії Catalyst 2950 пропонують такі переваги, як висока надійність, безпечне підключення до Інтернету та гнучка апаратна платформа, що підтримує масштабованість, додаткові інтерфейсні модулі та повний набір функціональних інструментів, а використання мідних кабелів з витотою парою забезпечує економічність та легко ремонтні рішення з доступністю та простотою встановлення, що робить його широко використовуваним вибором для телекомунікацій та локальних мереж.

3 ДОСЛІДЖЕННЯ ВПЛИВУ КОНФІГУРАЦІЇ МЕРЕЖІ НА ПОКАЗНИКИ ІІ НАДІЙНОСТІ

3.1 Основні типи конфігурації мереж та метод оцінки надійності

В термінології комп'ютерних мереж, конфігурація (також топологія) означає структуру та розташування комп'ютерів у мережі, а також засоби їхнього з'єднання. Важливо підкреслити, що концепція топології найбільше застосовується в локальних мережах, де структура зв'язків легко спостерігати. У глобальних мережах, структура зв'язків, як правило, прихована і не відіграє

суттєвої ролі для користувачів, оскільки кожний зв'язок може виконуватися по різних шляхах.

Топологія мережі визначає вимоги до обладнання, типу кабелю, методів керування обміном даних, надійності роботи та можливостей розширення мережі. Існують п'ять основних типів мережевих топологій:

- топологія "шина" (bus): у цій топології всі комп'ютери підключаються паралельно до одного спільного каналу зв'язку, і дані від кожного комп'ютера передаються всім іншим. Топологія "Шина" передбачає ідентичність обладнання комп'ютерів і рівноправність усіх користувачів. Комп'ютери мають передавати дані послідовно через загальний канал, оскільки в іншому випадку можуть виникнути конфлікти та колізії даних. Ця топологія підтримує напівдуплексний обмін даним;

- топологія "зірка" (star): у цій топології кожен комп'ютер підключається до центрального вузла (найчастіше це комутатор або концентратор), і кожен комп'ютер використовує окремий кабель для з'єднання з центральним вузлом. Центральний вузол відповідає за керування обміном даних. Конфлікти в цій топології практично виключені завдяки централізованому керуванню;

- топологія "кільце" (ring): у топології "Кільце" кожен комп'ютер передає дані лише одному наступному комп'ютеру в ланцюжку і отримує дані від попереднього комп'ютера в ланцюжку. Ця топологія утворює закрите "кільце," і всі комп'ютери працюють як ретранслятори. Керування обміном зазвичай відбувається за допомогою спеціального керуючого вузла. Така топологія має свої особливості та переваги, але вразлива до відмов центрального керуючого вузла.

Крім цих основних топологій, існують комбіновані топології, такі як "дерево," яке є поєднанням декількох зірок або інших комбінацій. Топологія "Дерево" може бути як активною, так і пасивною. В активній версії топології "Дерево," в центрах об'єднання декількох ліній зв'язку розташовані центральні комп'ютери. У пасивній версії - це концентратори (хаби). Крім того, існують комбіновані топології, такі як зірково-шинна або зірково-кільцева [17, 18].

Особливим видом мережевої топології є mesh-мережі, відомі також як сітчасті мережі. У таких мережах кожен вузол, який називається вузлом меш, функціонує як комутатор і бере участь у передачі даних мережею. Всі вузли співпрацюють для розподілу даних по мережі, і кожен вузол бере активну участь у передачі і отриманні даних [19].

Mesh-мережі мають численні переваги, які роблять їх привабливими для різних сфер використання. Деякі з основних переваг включають в себе:

- низькі витрати інвестицій: Mesh-мережі вимагають менших фінансових витрат при встановленні та розгортанні;
- значне покриття користувачів: Вони можуть обслуговувати велику кількість користувачів;
- швидке розгортання та масштабованість: Mesh-мережі дозволяють легко збільшувати мережу за потребою;
- висока живучість: Mesh-мережі мають високий рівень надійності та стійкості до відмов;
- висока пропускна спроможність: Вони можуть передавати великі обсяги даних з високою швидкістю;
- інтелектуальність: Mesh-мережі здатні до інтелектуального керування трафіком та оптимізації роботи [20].

Для широкого впровадження mesh-мереж на сучасному ринку мережевих технологій важлива сумісність з існуючими мережевими стандартами та протоколами, такими як Ethernet, VPN, VLAN, OSPF і інші. Ця здатність дозволяє різним мережам mesh, виробниками яких є різні компанії, ефективно співпрацювати на рівнях каналу та мережі за моделлю OSI, включаючи протоколи IPv4 та IPv6. Окрім цього, для оптимальної роботи мережі важливо забезпечити сумісність пристроїв з різними бездротовими інтерфейсами, і наразі, корпорація Intel веде дослідження та розробку механізмів, що дозволять це досягти. Цей підхід має потенціал значної економічної вигоди порівняно з реалізацією кількох бездротових інтерфейсів у кожному пристрої.

Завдяки цим характеристикам, mesh-мережі можуть бути успішно використані у різних галузях, включаючи широкосмуговий доступ в Інтернет, міські та офісні мережі, мережі комунальних служб, транспортні мережі, військове використання для забезпечення громадської безпеки та інші застосування. Mesh-мережі виявляються надзвичайно корисними в області комунікацій і зв'язку завдяки їхнім унікальним можливостям.

Обираючи топологію для мережі, варто враховувати вимоги до мережі, її розмір і складність, а також можливості розширення та надійності. Кожен тип топології має свої переваги та обмеження, і вибір залежить від конкретних вимог проекту [21].

Для оцінки надійності мереж різної топології буде використано метод мінімальних шляхів і мінімальних перетинів.

Метод мінімальних шляхів і мінімальних перетинів, відомий як метод Езар-Прошана, є інструментом, призначеним для надання верхніх та нижніх наближених оцінок надійності систем складної структури.

У цьому методі термін "шлях" визначається як будь-яка сукупність елементів, працездатність яких забезпечує працездатність системи. "Перетин" (або "розріз") означає будь-яку сукупність елементів, відмова яких призводить до непрацездатності системи.

Мінімальний шлях - це така сукупність елементів системи, де працездатність кожного з них необхідна і достатня для того, щоб система залишалася працездатною. Іншими словами, мінімальний шлях включає елементи, працездатність яких обов'язкова для забезпечення працездатності системи.

Для мінімального шляху:

- якщо всі елементи, які входять до мінімального шляху, залишаються працездатними, то система залишається працездатною;
- мінімальний перетин визначається як сукупність елементів системи, відмова яких є необхідною і достатньою для відмови всієї системи;
- якщо всі елементи, що входять до мінімального перетину, виходять з ладу, то вся система також виходить з ладу.

Якщо всі мінімальні шляхи в системі працюють, система залишається працездатною. Отже, система буде працювати, якщо працює хоча б один із мінімальних шляхів. Уявлення системи як паралельного з'єднання всіх мінімальних шляхів надає верхню (завищену, оптимістичну) оцінку її надійності.

Для отримання верхньої оцінки надійності системи на основі мінімальних шляхів слід виконати наступні кроки:

- знайти всі мінімальні шляхи системи;
- послідовно з'єднати елементи кожного мінімального шляху;
- паралельно з'єднати всі отримані послідовні ланцюжки.

Оптимістичний характер оцінки методом мінімальних шляхів виявляється в тому, що відмова елемента, що входить до декількох мінімальних шляхів (наприклад, першого), призводить лише до втрати одного з цих шляхів. Але в цій системі відмова цього елемента може призвести до відмови також у малому шляху.

Система вважається ненадійною, якщо відмовляють усі елементи хоча б одного малого перетину. Іншими словами, для всіх мінімальних зв'язків системи хоч один елемент повинен залишитися працездатним.

Таким чином, для оцінки методом мінімальних перетинів необхідно виконати такі кроки:

- знайти усі мінімальні перетини системи;
- паралельно поєднати елементи кожного малого перетину;
- послідовно з'єднати всі мінімальні перетини.

Метод мінімальних перетинів особливо цікавий для інженерних розрахунків, оскільки він надає нижню, обережну оцінку надійності системи. Крім того, цей метод може бути використаний для оцінки похибки розрахунку надійності, оскільки він призводить до оптимістичних результатів, які можуть бути корисними в інженерних практиках [22, 23, 24].

3.2 Оцінка надійності мереж «кільце» різної розмірності

У рамках графу надійності, який показано на рисунку 3.2, інформація передається як від вершини А до вершини В, так і в зворотньому напрямку. На рисунку 3.1 зображено логічну схему мережі кільце у Packet Tracer.

За допомогою цього графа надійності можливо визначити наступні важливі параметри:

- мінімальні перетини: 1-4, 3-6, 1-6, 2-5, 3-4, 1-2, 2-3, 5-6, 4-5;
- мінімальні шляхи: 1-2-3, 4-5-6.

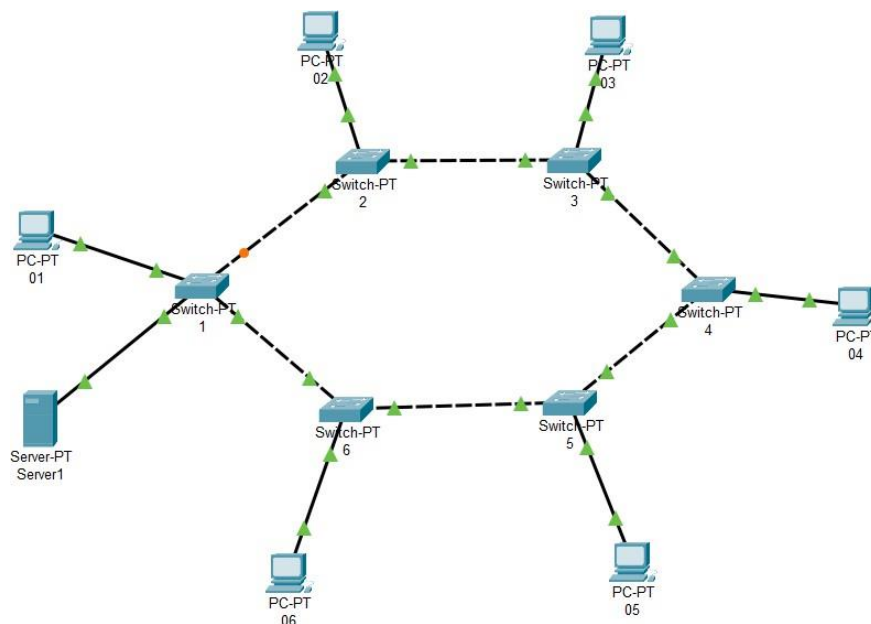


Рисунок 3.1 - Схема мережі кільце у Packet Tracer

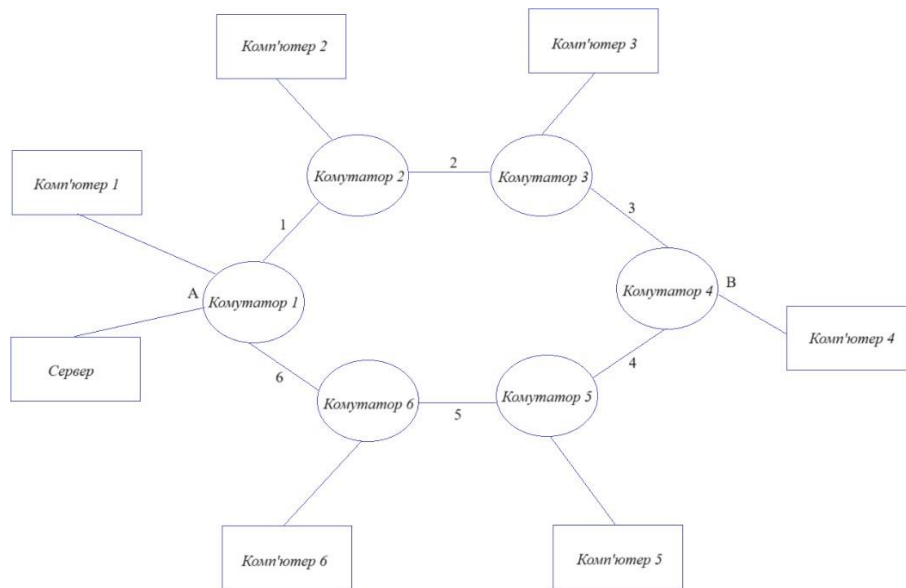
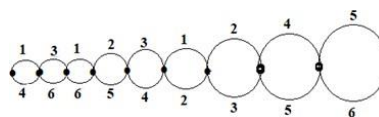


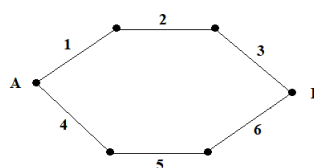
Рисунок 3.2 - Граф надійності мережі кільце

Далі побудовано два еквівалентні графи надійності для оцінки надійності системи: граф для нижньої оцінки (P_n): цей граф включає послідовно встановлені групи мінімальних перетинів; граф для верхньої оцінки (P_v): цей граф включає паралельно встановлені групи мінімальних шляхів (див. рис. 3.3).

Це допомагає визначити надійність системи і забезпечує дві різні оцінки, одна з них - консервативна (нижня оцінка), а інша - оптимістична (верхня оцінка) надійності системи передачі інформації від вершини А до вершини В та в зворотному напрямку.



а)



б)

Рисунок 3.3 - Еквівалентні графи надійності для оцінки нижнього P_n (а) та верхнього P_v (б) рівнів імовірності безвідмовної роботи системи

Нехай імовірності відмови пристроїв однакові і дорівнюють 0,2, тоді:

$$q_{zy} = q_c = q_{\pi} = 0,2$$

Імовірність безвідмовної роботи розраховано за формулою:

$$P_{\text{посл}} = \prod_{i=1}^n p_i ; \quad (3.1)$$

$$P_{\text{парал}} = 1 - \prod_{i=1}^n (1 - p_i), \text{ де } p_i = 1 - q \quad (3.2)$$

$$p_H = p_{14} * p_{36} * p_{16} * p_{25} * p_{34} * p_{12} * p_{23} * p_{56} * p_{45}$$

$$p_{45} = 1 - q^2 = p_{14} = p_{36} = p_{16} = p_{25} = p_{34} = p_{12} = p_{23} = p_{56} = 1 - 0,04 = 0,96$$

Якщо підставити відповідні значення, отримаємо:

$$p_H = 0,96 * 0,96 * 0,96 * 0,96 * 0,96 * 0,96 * 0,96 * 0,96 * 0,96 = 0,692$$

Імовірність безвідмовної роботи приладу пам'яті буде $P_{zy} = 1 - q_{zy}$, приладу сполучення - через $p_c = 1 - q_c$, процесорів - через $p_{\pi} = 1 - q_{\pi}$. Згідно графу Мінімальних Шляхів (МШ), для послідовно включених шляхів ми отримаємо:

$$P_{123} = P_{456} = (1 - q)^3 = (1 - 0,2)^3 = 0,512$$

Після обчислень для декількох послідовно включених імовірностей безвідмовної роботи за допомогою графу мінімальних шляхів, визначимо загальну верхню імовірність відмови Q_v при паралельній структурі за формулою:

$$Q = \prod_{i=1}^n Q_i, \quad (3.3)$$

Таким чином, отримаємо:

$$Q_v = Q_{123} Q_{456} = (1 - 0,512)^2 = 0,238$$

На основі цього визначимо верхній рівень імовірності безвідмовної роботи системи:

$$P_v = 1 - Q_v = 1 - 0,238 = 0,762$$

Загальна імовірність безвідмовної роботи системи знаходиться в інтервалі:

$$0,692 < P_c < 0,762$$

Граф-схему надійності мережі кільце з 8 пристроями показано на рисунку 3.5, а логічну схему на рисунку 3.4:

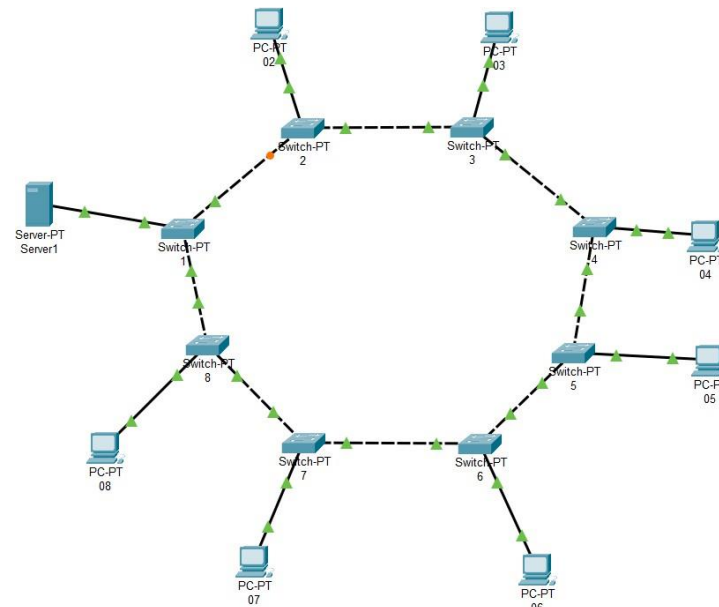


Рисунок 3.4 - Схема мережі кільце у Packet Tracer

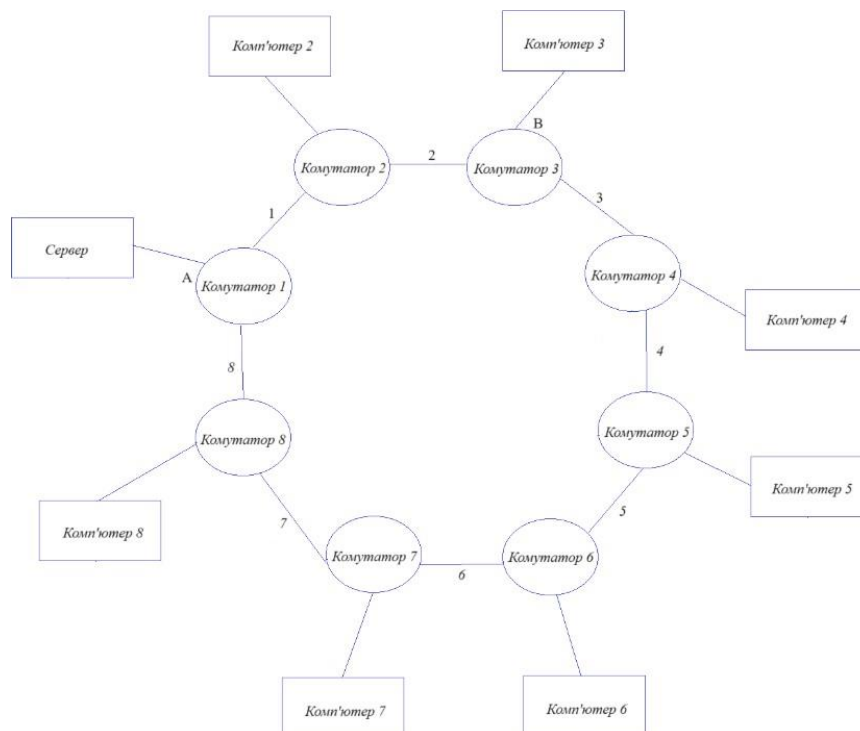
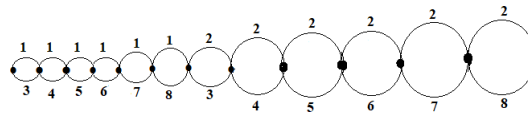


Рисунок 3.5 - Граф надійності мережі кільце

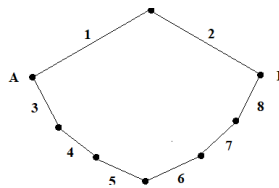
По графу надійності визначимо:

- мінімальні перетини – 1-3, 1-4, 1-5, 1-6, 1-7, 1-8, 2-3, 2-4, 2-5, 2-6, 2-7, 2-8;
- мінімальні шляхи – 1-2, 3-4-5-6-7-8.

Еквівалентні графи надійності на рисунку 3.6:



а)



б)

Рисунок 3.6 - Еквівалентні графи надійності для оцінки нижнього R_H (а) та верхнього R_B (б) рівнів імовірності безвідмовної роботи системи

$$q_{zy} = q_c = q_n = 0,2$$

Імовірність безвідмовної роботи розраховано за формулами 3.1 та 3.2:

$$r_H = p_{13} * p_{14} * p_{15} * p_{16} * p_{17} * p_{18} * p_{23} * p_{24} * p_{25} * p_{26} * p_{27} * p_{28}$$

$$p_{28} = 1 - q^2 = p_{13} = p_{14} = p_{15} = p_{16} = p_{17} = p_{18} = p_{23} = p_{24} = p_{25} = p_{26} = p_{27} = 1 - 0,04 = 0,96$$

Підставим значення та отримаємо:

$$r_H = 0,96^{12} = 0,612$$

По графу МШ, для послідовно включених шляхів одержимо:

$$R_{12} = (1 - q)^2 = (1 - 0,2)^2 = 0,64$$

$$R_{345678} = (1 - q)^6 = (1 - 0,2)^6 = 0,262$$

Визначимо загальну верхню імовірність відмови Q_B при паралельній структурі:

$$Q_B = Q_{12} Q_{345678} = (1 - 0,64) * (1 - 0,262) = 0,266$$

Отже, можна визначити верхній рівень імовірності безвідмовної роботи системи:

$$R_B = 1 - Q_B = 1 - 0,266 = 0,734$$

Загальна імовірність безвідмовної роботи системи знаходиться в інтервалі:
 $0,612 < P_c < 0,734$

У графі надійності мережі кільце з 10 пристроями на рисунку 3.8 інформація також передається як від вершини А до вершини В, так і в зворотньому напрямку. Логічну схему зображено на рисунку 3.7:

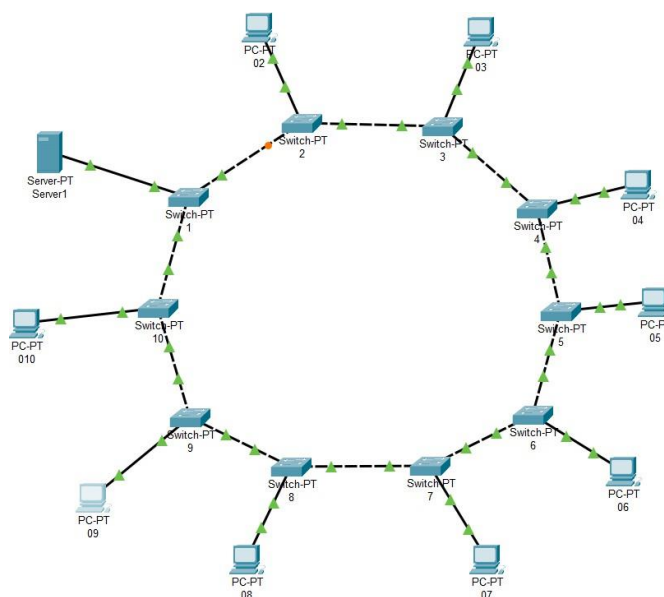


Рисунок 3.7 - Схема мережі кільце у Packet Tracer

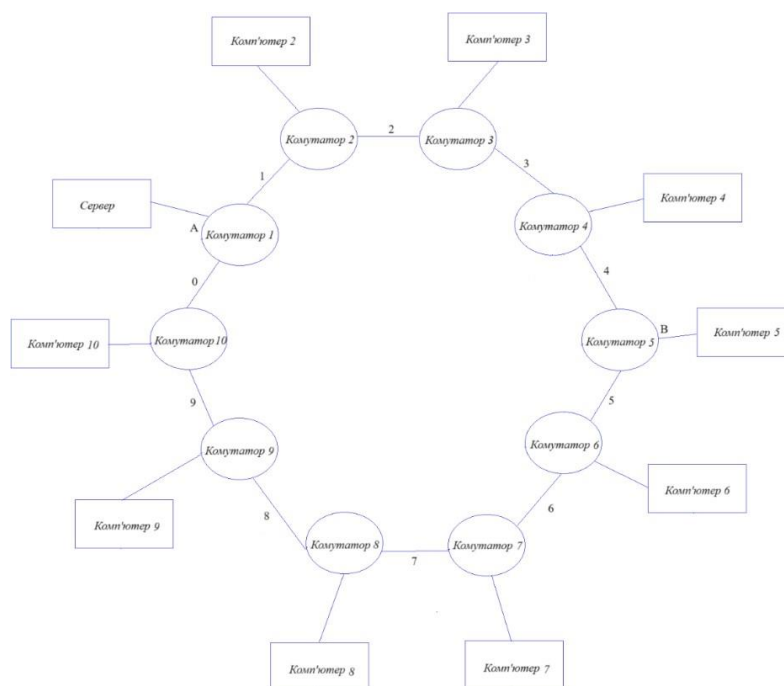


Рисунок 3.8 - Граф надійності мережі кільце

По графу надійності визначимо:

— мінімальні перетини – 1-5, 1-6, 1-7, 1-8, 1-9, 1-10, 2-5, 2-6, 2-7, 2-8, 2-9, 2-10, 3-5, 3-6, 3-7, 3-8, 3-9, 3-10, 4-5, 4-6, 4-7, 4-8, 4-9, 4-10;

— та мінімальні шляхи – 1-2-3-4, 5-6-7-8-9-10.

Еквівалентні графи надійності мережі кільце на рисунку 3.9:

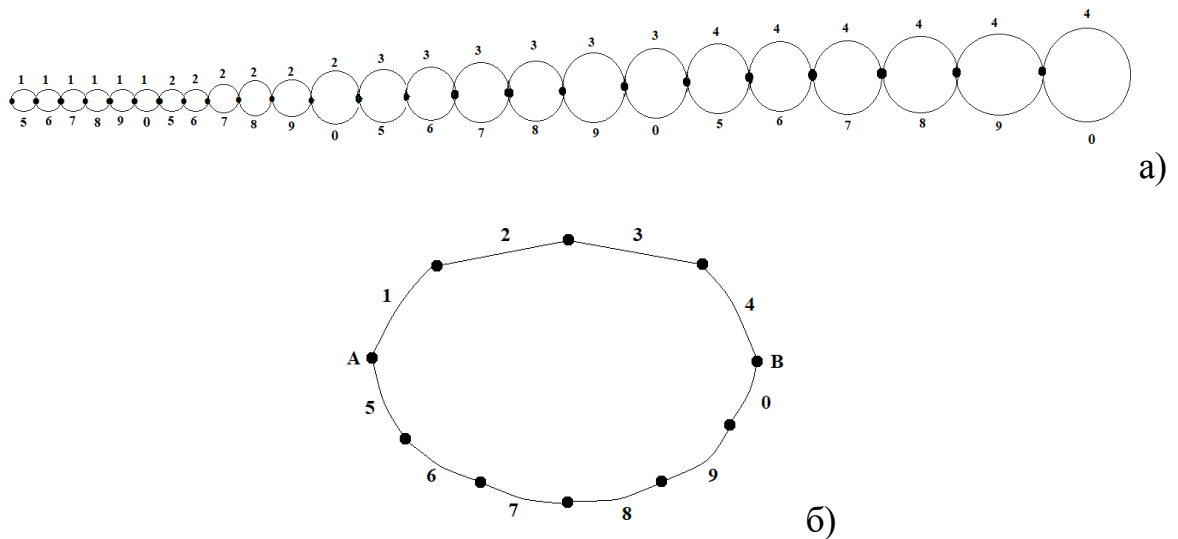


Рисунок 3.9 - Еквівалентні графи надійності для оцінки нижнього P_H (а) та верхнього P_B (б) рівнів імовірності безвідмовної роботи системи

$$q_{zy} = q_c = q_n = 0,2$$

Імовірність безвідмовної роботи знаходимо формулами 3.1 та 3.3, як:

$$P_H = p_{15} * p_{16} * p_{17} * p_{18} * p_{19} * p_{1-10} * p_{25} * p_{26} * p_{27} * p_{28} * p_{29} * p_{20} * p_{35} * p_{36} * p_{37} * p_{38} * p_{39} * p_{30} * p_{45} * p_{46} * p_{47} * p_{48} * p_{49} * p_{40}$$

$$p_{15} = 1 - q^2 = p_{16} = p_{17} = p_{18} = p_{19} = p_{1-10} = p_{25} = p_{26} = p_{27} = p_{28} = p_{29} = p_{20} = p_{35} = p_{36} = p_{37} = p_{38} = p_{39} = p_{30} = p_{45} = p_{46} = p_{47} = p_{48} = p_{49} = p_{40} = 1 - 0,04 = 0,96$$

Якщо підставити значення, одержимо:

$$P_H = 0,96^{24} = 0,375$$

Згідно графу Мінімальних Шляхів для послідовно включених шляхів одержимо:

$$P_{1234} = (1 - q)^4 = (1 - 0,2)^4 = 0,409$$

$$P_{567890} = (1 - q)^6 = (1 - 0,2)^6 = 0,262$$

Визначимо загальну верхню імовірність відмови Q_V при паралельній структурі:

$$Q_V = Q_{12} Q_{345678} = (1 - 0,409) * (1 - 0,262) = 0,436$$

Отже, знайдемо верхній рівень імовірності безвідмовної роботи системи:

$$P_V = 1 - Q_V = 1 - 0,436 = 0,564$$

Загальна імовірність безвідмовної роботи системи знаходиться в межах:

$$0,375 < P_c < 0,564$$

Розбіг значень P_c дозволяє оцінити точність розрахунків надійності мережі кільце [25].

3.3 Оцінка надійності мережі дерево

Граф надійності мережі дерево зображено на рисунку 3.11. Логічну схему зібрано у Cisco Packet Tracer та зображено на рисунку 3.10:

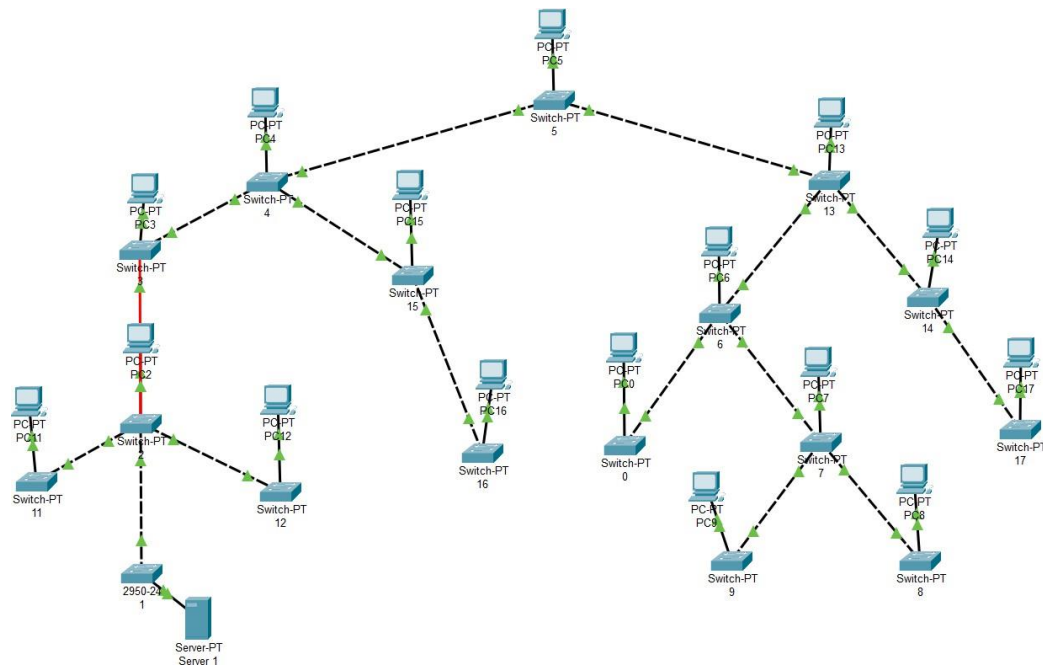


Рисунок 3.10 - Схема мережі дерево у Packet Tracer

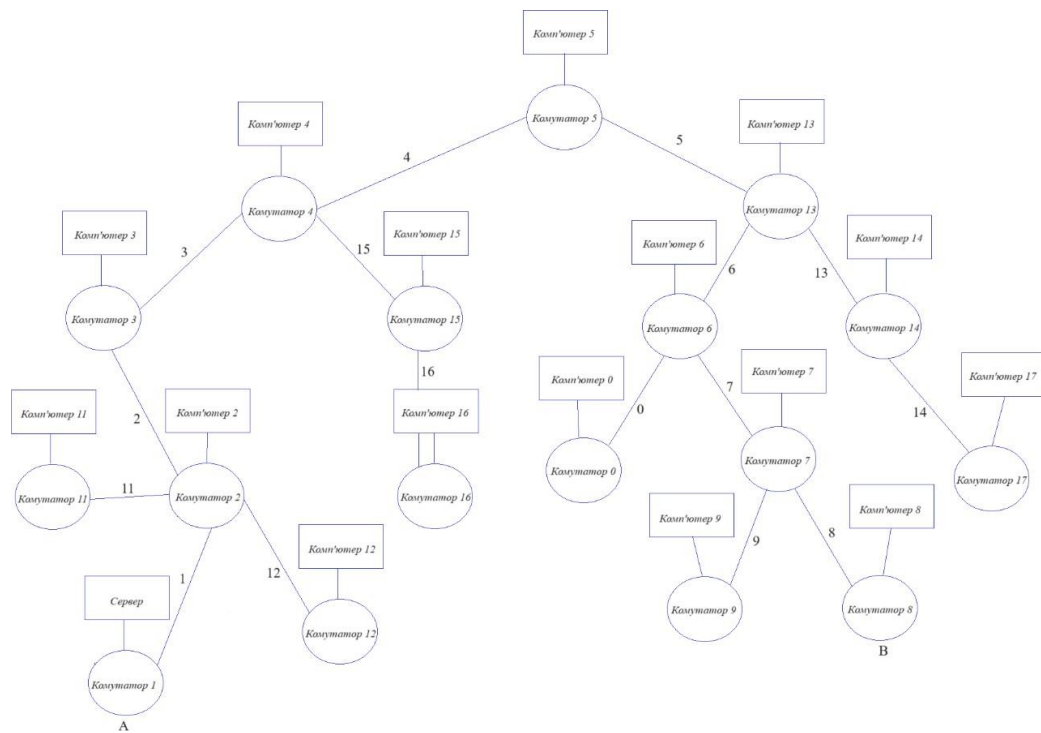


Рисунок 3.11 - Граф надійності мережі дерево

По графу визначимо:

- мінімальні перетини – 1, 2, 3, 4, 5, 6, 7, 8;
- мінімальні шляхи – 1-2-3-4-5-6-7-8.

Розглянемо побудову еквівалентних графів надійності для проведення надійності системи. Для нижньої оцінки R_n послідовно включено групи мінімальних перетинів, тоді як для верхньої оцінки R_v включено паралельно групи мінімальних шляхів (див. рис. 3.12).

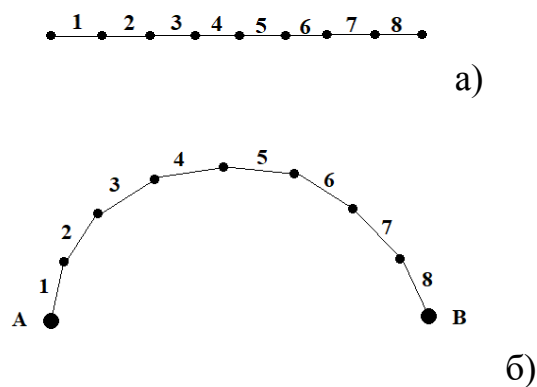


Рисунок 3.12 - Еквівалентні графи надійності для оцінки нижнього R_n (а) та верхнього R_v (б) рівнів імовірності безвідмовної роботи системи

$$q_{zy} = q_c = q_{\pi} = 0,2$$

Імовірність безвідмовної роботи отримаємо за формулами 3.1, 3.2:

$$p_H = p_1 * p_2 * p_3 * p_4 * p_5 * p_6 * p_7 * p_8$$

$$p_1 = 1 - q = p_2 = p_3 = p_4 = p_5 = p_6 = p_7 = p_8 = 1 - 0,2 = 0,8$$

Підставляючи значення, отримаємо:

$$p_H = 0,8^8 = 0,168$$

Імовірність безвідмовної роботи приладу пам'яті позначено, як $P_{zy} = 1 - q_{zy}$, приладу сполучення - через $p_c = 1 - q_c$, процесорів - через $p_{\pi} = 1 - q_{\pi}$. Отже, згідно з графом МШ, для послідовно включених шляхів отримаємо:

$$P_{12345678} = (1 - q)^8 = (1 - 0,2)^8 = 0,168$$

Визначимо загальну верхню імовірність відмови Q_v при паралельній структурі за формулою 3.3:

$$Q_v = Q_{12345678} = 1 - 0,168 = 0,832$$

Визначимо верхній рівень імовірності безвідмовної роботи системи:

$$P_v = 1 - Q_v = 1 - 0,832 = 0,168$$

Загальна імовірність безвідмовної роботи системи знаходиться в межах:

$$0,168 < P_c < 0,168$$

Розбіг значень P_c дає уяву про точність розрахунків надійності мережі дерево [25].

3.4 Оцінка надійності мережі зірка

Граф-схему надійності мережі зірка зображено на рисунку 3.14. Логічну схему у Packet Tracer зібрано на рисунку 3.13:

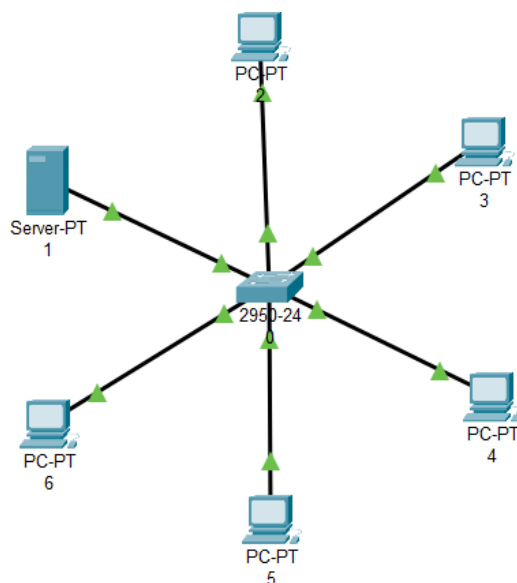


Рисунок 3.13 - Схема мережі зірка у Packet Tracer

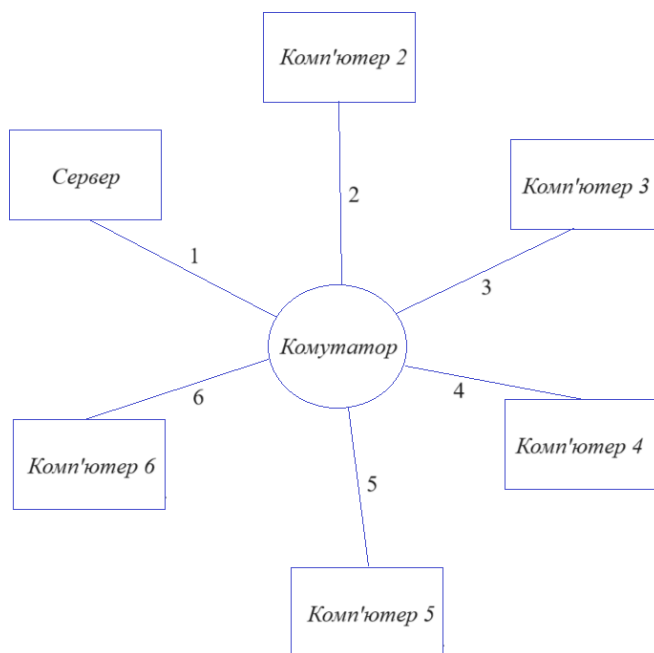


Рисунок 3.14 - Граф надійності мережі зірка

По графу отримаємо:

- мінімальні перетини – 1-2, 1-3, 1-5, 1-6, 2-4, 3-4, 4-5, 4-6;
- мінімальний шлях – 1-4.

Побудуємо графи надійності мережі зірка наступним чином(рис. 3.15):

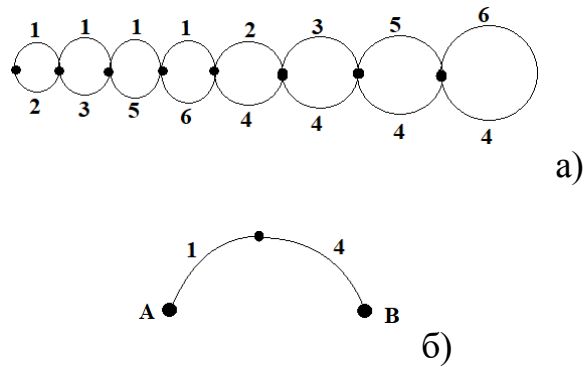


Рисунок 3.15 - Еквівалентні графи надійності для оцінки нижнього P_H (а) та верхнього P_B (б) рівнів імовірності безвідмовної роботи системи

$$q_{zy} = q_c = q_{\Pi} = 0,2$$

Імовірність безвідмовної роботи знаходимо через формули 3.1, 3.2:

$$p_H = p_{12} * p_{13} * p_{15} * p_{16} * p_{24} * p_{34} * p_{45} * p_{46}$$

$$p_{12} = 1 - q^2 = p_{13} = p_{15} = p_{16} = p_{24} = p_{34} = p_{45} = p_{46} = 1 - 0,04 = 0,96$$

Підставляючи значення, отримаємо:

$$p_H = 0,96^8 = 0,721$$

Обчислимо імовірності для послідовно включених шляхів наступним чином:

$$P_{14} = (1 - q)^2 = (1 - 0,2)^2 = 0,64$$

Визначимо їх загальну верхню імовірність відмови Q_B при паралельній структурі:

$$Q_B = Q_{14} = 1 - 0,64 = 0,36$$

Тепер можна визначити верхній рівень імовірності безвідмовної роботи системи:

$$P_B = 1 - Q_B = 1 - 0,36 = 0,64$$

Загальна імовірність безвідмовної роботи системи знаходиться в межах:

$$0,721 < P_c < 0,64$$

Розбіг значень P_c дозволяє оцінити точність розрахунків надійності мережі зірка за методом МШ & МП [25].

3.5 Оцінка надійності mesh-мережі

Граф-схему надійності mesh-мережі зображено на рисунку 3.17. Логічну схему у Packet Tracer зібрано на рисунку 3.16:

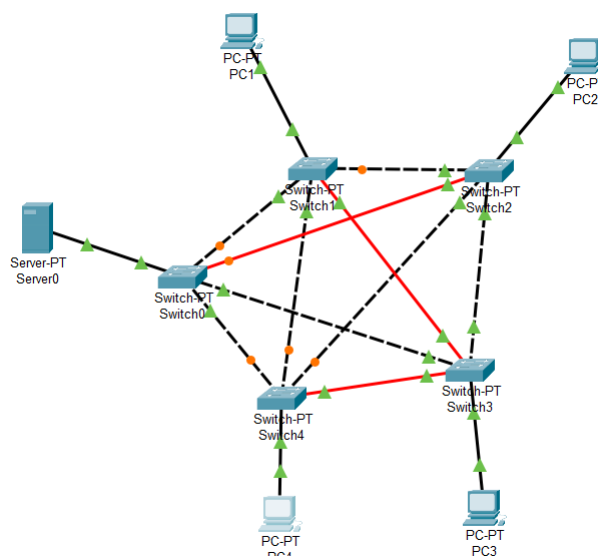


Рисунок 3.16 - Схема mesh-мережі у Packet Tracer

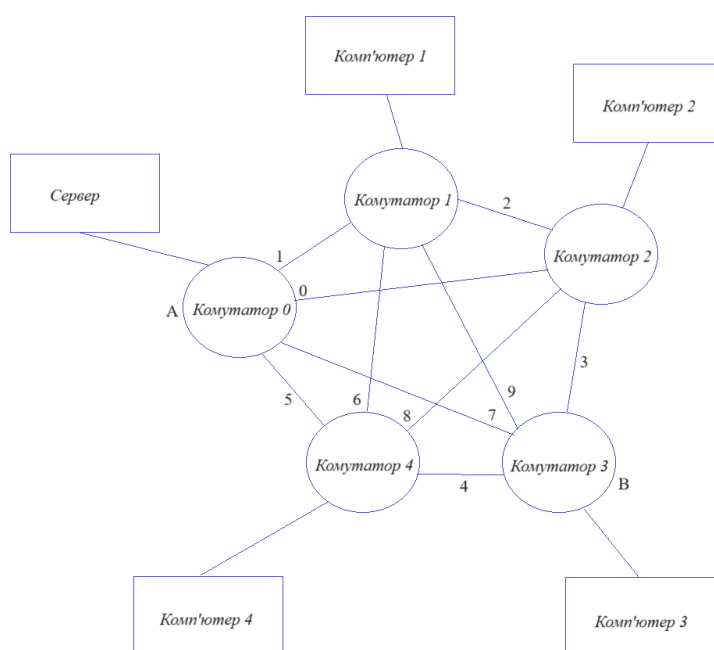


Рисунок 3.17 - Граф надійності mesh-мережі

По графу надійності визначимо:

- мінімальні перетини – 0-1-5-7, 3-4-7-9;
- мінімальні шляхи – 7, 4-5, 1-9, 0-3, 0-4-8, 1-4-6, 1-2-3, 0-2-9, 5-6-9, 3-5-8, 0-2-4-6, 2-5-8-9, 2-3-5-6, 0-8-6-9.

Еквівалентні графи надійності mesh-мережі на рисунку 3.18:

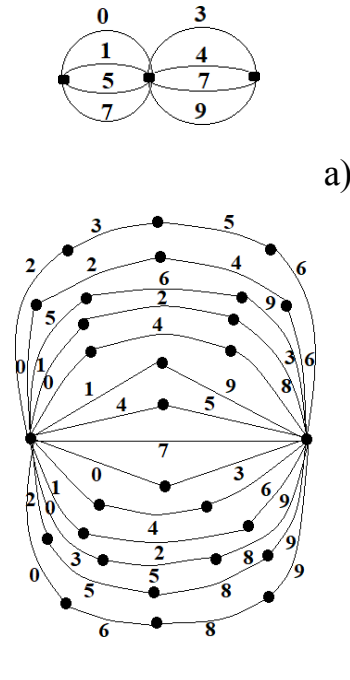


Рисунок 3.18 - Еквівалентні графи надійності для оцінки нижнього P_H (а) та верхнього P_B (б) рівнів імовірності безвідмовної роботи системи

$$q_{zy} = q_c = q_{\Pi} = 0,2$$

Імовірність безвідмовної роботи розраховано таким чином:

$$p_H = p_{0157} * p_{3479}$$

$$p_{0157} = 1 - q^4 = p_{3479} = 1 - 0,0016 = 0,99$$

Підставляючи значення, одержимо:

$$p_H = 0,99 * 0,99 = 0,98$$

Тоді, по графу МШ, для послідовно включених шляхів одержимо:

$$P_7 = 1 - q = 1 - 0,2 = 0,8$$

$$P_{45} = P_{19} = P_{03} = (1 - q)^2 = (1 - 0,2)^2 = 0,64$$

$$P_{048} = P_{146} = P_{123} = P_{029} = P_{569} = P_{358} = (1 - q)^3 = (1 - 0,2)^3 = 0,512$$

$$P_{0246} = P_{2589} = P_{2356} = P_{0689} = (1 - q)^4 = (1 - 0,2)^4 = 0,4096$$

Визначимо їх загальну верхню імовірність відмови Q_v при паралельній структурі:

$$Q_v = Q_{12} Q_{345678} = 0,8 * (1 - 0,64)^3 * (1 - 0,512)^6 * (1 - 0,4096)^4 = 0,00006124939$$

Отже, знайдемо верхній рівень імовірності безвідмовної роботи системи:

$$P_v = 1 - Q_v = 1 - 0,00006124939 = 0,9999$$

Загальна імовірність безвідмовної роботи системи знаходиться в межах:

$$0,98 < P_c < 0,999$$

Розбіг значень P_c дозволяє оцінити точність розрахунків надійності mesh-мережі [25].

3.6 Порівняльна характеристика різних топологій мереж

Mesh-мережа - це мережа, в якій кожен вузол мережі підключений до кількох інших вузлів, утворюючи мережеву структуру, яка може бути більш надійною, ніж інші типи мереж. У mesh-мережі, якщо один з пристроїв вийде з ладу, то мережа все ще може працювати, використовуючи альтернативні шляхи для передачі даних. У mesh-мережі важлива загальна кількість як усіх пристроїв, так і пристроїв між точками А і В.

Мережа кільце - це мережа, в якій вузли мережі підключені в лінійну топологію, утворюючи кільцеву структуру. На рисунку 3.19 зображено графік порівняння мереж кільце з різною кількістю вузлів. У мережі кільце, якщо один з вузлів вийде з ладу, то мережа може перестати працювати повністю, оскільки вузли мережі залежать один від одного в кільці. Існує всього два шляхи від точки А до точки В, у випадку, якщо один з пристроїв обірветься, залишається лише один альтернативний шлях, та усі зв'язки є критичними. Тобто мережа не є дуже

надійною. Загальна кількість пристроїв грає важливу роль, так як підрахунки імовірності безвідмовної роботи трьох систем з різною кількістю пристроїв показали, чим вища кількість пристроїв – тим нижче стають показники імовірності безвідмовної роботи.

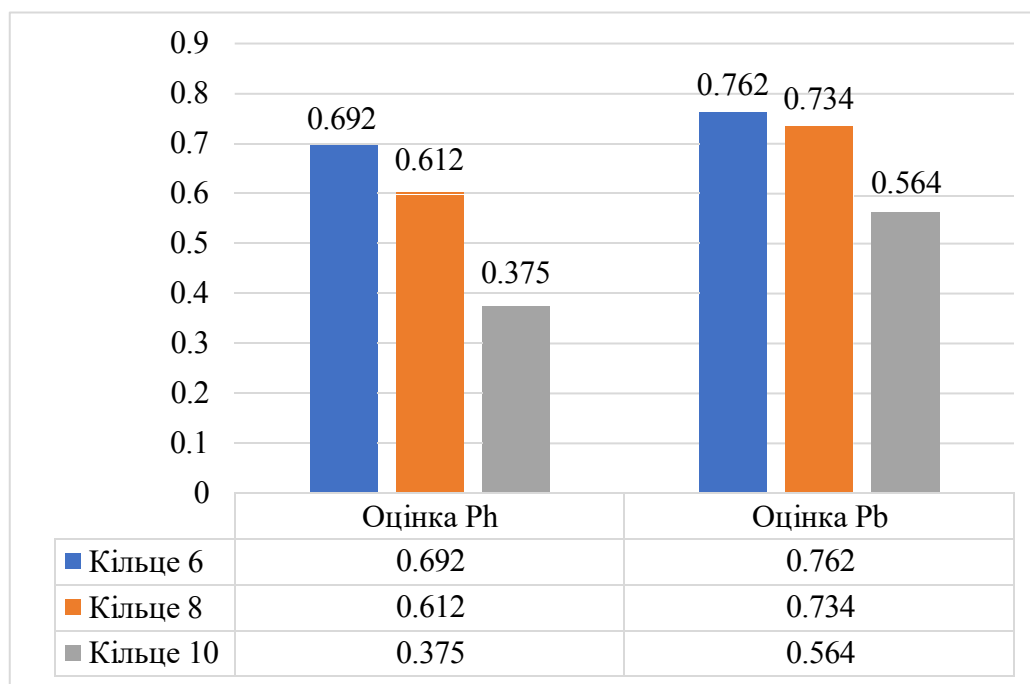


Рисунок 3.19 - Порівняння мереж кільце з різною кількістю вузлів

Мережа дерево - це мережа, в якій кожен вузол мережі має один або більше дочірніх вузлів, утворюючи ієрархічну структуру. Якщо один з вузлів вийде з ладу, то це може призвести до проблем з доступністю дочірніх вузлів, що може знизити надійність мережі. Важливу роль грають пристрої між точками А і В, так як лише вони є критичними, і якщо обірвати, не буде альтернативних шляхів.

У мережі дерево є лише один єдиний шлях, тому пристрої між точками А і В – критичні, а інші – ні, з чого можна зробити висновок, що загальна кількість пристроїв не грає важливу роль, лише кількість між точками А і В. Альтернативних шляхів не має у випадку розпаду шляху, мережа не надійна.

Мережа зірка - це мережа, в якій всі вузли мережі підключені до одного центрального вузла, який називається комутатором. Якщо центральний комутатор вийде з ладу, то всі вузли в мережі можуть втратити зв'язок, що може значно

погіршити надійність мережі. Мережа зірка, так як і дерево, має всього один шлях, але, на відміну від неї, кількість пристроїв завжди однакова – їх два, а загальна кількість пристроїв у мережі не грає важливої ролі. Якщо шлях розпадеться, альтернативних шляхів не має.

Порівняльну характеристику мереж зображено у таблиці 3.1:

Таблиця 3.1 – Порівняльна характеристика різних типів мереж

Тип мережі:	Mesh	Кільце	Дерево	Зірка
Загальна імовірність безвідмовної роботи системи знаходиться в межах:	$0,98 < P_c < 0,999$	$0,692 < P_c < 0,762$ $0,612 < P_c < 0,734$ $0,375 < P_c < 0,564$	$0,168 < P_c < 0,168$	$0,721 < P_c < 0,64$
Висновок:	Показники надійності mesh-мережі максимально високі. Обрив одного з вузлів не зупиняє роботу мережі, та вона може далі функціонувати, використовуючи альтернативні шляхи, а таких шляхів є багато. Мінімальних перетинів мало. Це говорить про те, що mesh-мережа є дуже надійною.	Показники надійності мережі зірка середні, і при збільшенні кількості вузлів, показники стають нижче. Обрив одного з ліній не припиняє роботу мережі, та вона може далі працювати, обираючи альтернативні шляхи, а такий шлях є один. Мінімальних перетинів багато, а шляхів всього два, незалежно від кількості вузлів. Отже, мережа кільце не є дуже надійно.	Показники надійності мережі дерево дуже низькі по причині того, що мережа дерево має один єдиний шлях. Кожен вузол цього шляху є критичним окремо, а інші вузли не є критичними, тому показники знаходяться в однакових межах. Якщо обірвати некритичні вузли, мережа працює, але якщо критичні вузли - мережа не буде мати шляху і розпадеться.	Показники надійності мережі зірка середні. Мережа, також як і дерево, має один шлях, але який не залежно від загальної кількості пристроїв в мережі, завжди має всього два вузли, що говорить про те, що загальна кількість пристроїв не важлива, а кількість вузлів між точками А і В завжди однакова.

На рисунку 3.20 добре зображено, яка мережа є найбільш надійною:

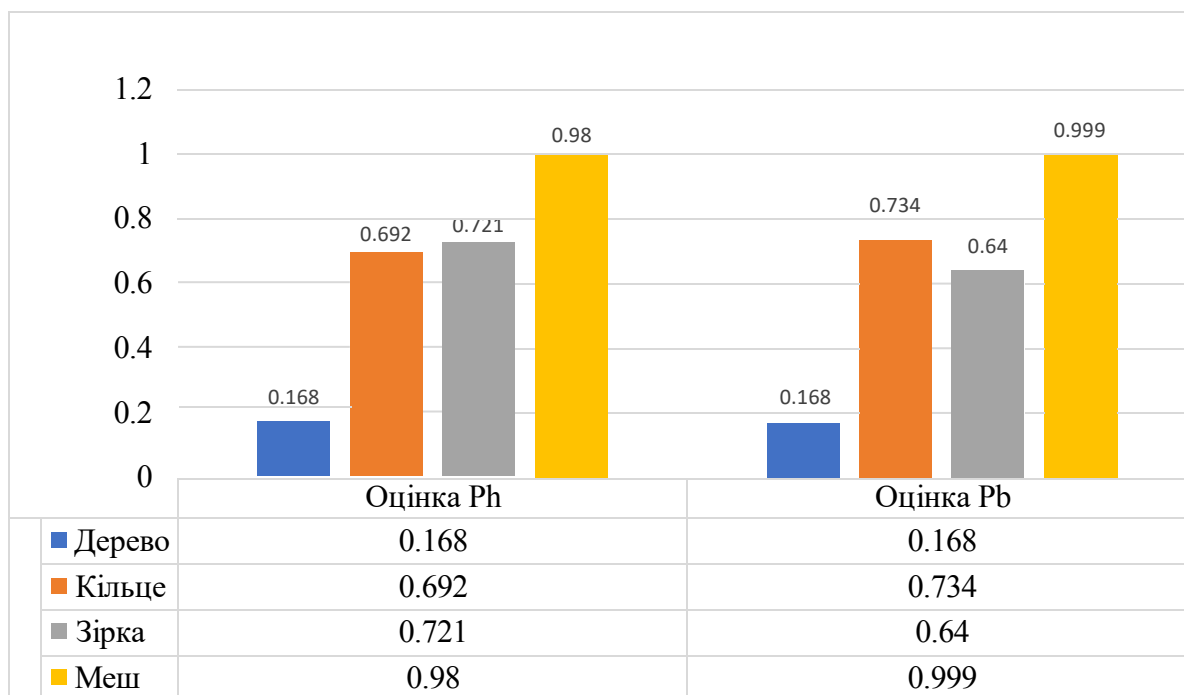


Рисунок 3.20 - Порівняння різних типів мереж

Висновки. Надійність різних типів мереж може відрізнятися в залежності від їхньої структури. Mesh-мережа є найбільш надійною серед різних типів мереж саме завдяки своїй складній структурі.

Надійність mesh-мережі залежить від кількох факторів:

- кількість шляхів: чим більше шляхів між вузлами, тим менше ймовірність, що випадкова відмова вузла призведе до перерви в роботі мережі;
- резервність: деякі mesh-мережі можуть мати резервні вузли, які можуть прийняти на себе трафік, якщо основний вузол відмовить. Це забезпечує вищу доступність та надійність мережі;
- алгоритми маршрутизації: mesh-мережі можуть використовувати різні алгоритми маршрутизації, які визначають шляхи, якими будуть передаватися дані між вузлами. Ефективні алгоритми маршрутизації зменшують час, необхідний для передачі даних, та забезпечують більшу надійність мережі;
- схема керування: mesh-мережі можуть мати різні схеми керування, що визначає, які вузли відповідальні за керування мережею та як вони взаємодіють.

Ефективна схема керування забезпечує більшу надійність мережі та зменшує час, необхідний для розробки та підтримки мережі.

Отже, mesh-мережа є однією з технологій комп'ютерної мережі, в якій кожен вузол (комп'ютер або пристрій) підключений до кількох інших вузлів, утворюючи мережу без центрального керування. Така топологія мережі забезпечує високу надійність і доступність, оскільки випадок відмови одного вузла не призводить до зупинки всієї мережі [26].

4 РОЗРОБКА МЕРЕЖІ З ПОЛІПШЕНОЮ НАДІЙНІСТЮ

4.1 Аналіз структури підприємства

Завданням дипломного проекту є розвиток комп'ютерної мережі для товариства "ТехКом". Перед нами стоїть завдання по об'єднанню головного офісу та його філій в єдину інтегровану мережу. В рамках цього завдання необхідно розглянути вибір топології магістралі, визначити логічну структуру мережі та розбити її на підрівні, а також налаштувати списки контролю доступу.

АТ "ТехКом" є світовим лідером у сфері розробки, виробництва, обслуговування та ремонту авіаційних газотурбінних двигунів для літаків та вертольотів, а також промислових газотурбінних установок. Компанія є частиною Співки виробників нафтогазового обладнання та позиціонується як один з ключових гравців у цій галузі.

На момент 2010 року АТ "ТехКом" розробляло та обслуговувало 61 різновидів та модифікацій газотурбінних двигунів для 70 типів літаків і вертольотів. Це свідчить про вражаючий рівень продукції та широкий вплив компанії на глобальному ринку авіаційних технологій.

Важливим етапом в історії АТ "ТехКом" був запуск відкритого Чемпіонату України з вертольотного спорту 11 листопада 2013 року. Ця подія була відзначена з приводу 67-річчя з дня першого польоту літака Ан-2 та 110-річчя існування

підприємства АТ "ТехКом". У той же день був представлений перший український гвінтокрил, що став результатом десятирічних зусиль та досліджень.

Історія підприємства сягає своїм корінням 1907 року, коли завод спеціалізувався на виробництві сільськогосподарської техніки та механічних інструментів. Поступово виробництво сконцентрувалося на поршневих двигунах різних модифікацій, зокрема на АШ-82ФН, АШ-62ІР, М-6, М-11 та інших. Ці двигуни не лише відзначалися високою якістю, але також регулярно випереджали світові аналоги за їх технічними характеристиками.

У 1947 році завод запустив виробництво газотурбінних двигунів РД-45 і РД-500, що позначило початок нової ери в розвитку газотурбінних технологій. Турбогвинтові двигуни АІ-20 (1957 рік) та АІ-24 (1962 рік), розроблені О. Г. Марченком, стали піонерами цього покоління. Їх численні модифікації досі знаходять застосування у сучасних технологіях.

Вертольот МБ-2 відзначається високим використанням композитних матеріалів, що позначило початок нової ери в розвитку цивільної авіації в Україні. Протягом наступного року планується провести його сертифікацію, що підкреслює серйозний науково-технічний рівень компанії.

Додатково, підприємство планує розпочати постачання авіаційних двигунів для встановлення на літаки DA-50. З 2022 року передбачається масштабне виробництво серійних авіаційних двигунів АІ-450С для постачання на міжнародний ринок. У вересні 2021 року була укладена рамкова угода з австрійською компанією Diamond Aircraft Industries щодо поставки 400 двигунів АІ-450С для використання на європейських бізнес-джетах DA-50.

Світ комп'ютерних мереж вимагає від кожного підключеного комп'ютера унікальної адреси, щоб забезпечити обмін інформацією між ними. Комп'ютерні мережі дозволяють передавати різні типи даних, такі як текстові повідомлення, аркуші, програми, книги тощо. Для цього дані передаються через комутатори та маршрутизатори, кожен з яких визначає наступний крок на шляху до отримувача. Таким чином, інформація подається по мережі до місця призначення.

У процесі розробки розподіленої комп'ютерної мережі для АТ "ТехКом" передбачаються наступні ключові завдання:

а) вибір технології LAN і WAN підключень для відділів. Це включає визначення найбільш оптимальних технологій для підключень у локальних та глобальних мережах між відділами:

- 1) вибір мережевого обладнання: аналіз технічних характеристик та вибір необхідного мережевого обладнання;
- 2) вибір апаратного забезпечення: розгляд можливостей та вибір необхідного апаратного забезпечення для реалізації проекту.

б) розміщення та налаштування мережевого обладнання: ця задача передбачає планування фізичного розміщення та налаштування всього мережевого обладнання:

- 1) монтажна схема мережі: розробка схеми, яка відображає розташування різних компонентів мережі;
- 2) вибір принципу маршрутизації та адресації: визначення методів маршрутизації трафіку та системи адресації в мережі;
- 3) забезпечення мережевої безпеки: розробка та впровадження заходів для забезпечення безпеки мережі та конфіденційності даних;
- 4) підключення мережі до Інтернету: організація підключення мережі до глобального Інтернету для забезпечення зовнішнього доступу;
- 5) налаштування мережі: конфігурація всіх компонентів мережі для оптимальної функціональності та продуктивності;
- 6) тестування мережі: проведення тестів і перевірок для підтвердження стабільності та ефективності роботи мережі.

Цей проект має на меті не лише розширення функціональності мережі АТ "ТехКом", але і забезпечення її надійності та забезпечення високого рівня безпеки і керованості.

4.2 Монтаж та налаштування мережі

Структура АТ «ТехКом». До складу АТ «ТехКом» належать такі структурні одиниці:

— завод №1. Основна структурна одиниця підприємства спеціалізується на виробництві авіадвигунів, їх ремонті та обслуговуванні, виготовленні приводів для газо- та нафтоперекачувальних агрегатів, пересувних автоматизованих електростанцій, а також на виробництві різноманітних товарів народного споживання;

— завод №2. В зв'язку з розробкою та виробництвом великогабаритних двигунів Д-18 на правобережному майданчику в місті було побудовано нову випробувальну станцію, сучасний ливарний цех для точного кріплення деталей із жаростійких сплавів та низку інших цехів. Основним напрямком діяльності заводу є ливарне виробництво та випробування двигунів Д-18Т. Крім цього, на заводі виготовляють газотурбінні електростанції потужністю 100 та 600 кВт;

— завод №3. Завод став першим спеціалізованим заводом у галузі виробництва лопаток для газотурбінних двигунів. Завод виготовляє деталі для авіаційних двигунів, такі як диски компресорів, лопатки компресорів і турбін, а також вироби для гірничо-шахтного обладнання і товари народного споживання;

— завод №4. Основною місією створеного підприємства було забезпечення збирання авіадвигунів за допомогою виготовлення різноманітних деталей та технічних засобів, а також виробництво технологічного обладнання. На заводі був організований цех для виробництва портативних автоматизованих електростанцій ПАЕС-2500, а також здійснюється ремонт двигунів АІ-20 і його модифікацій, таких як АІ-20КЕ, АІ-20КН, АІ-20МЕ, АІ-20МН. Крім того, завод займається виробництвом автозапчастин та виготовляє сільськогосподарські товари;

— авіакомпанія "ТехКом". Ця авіакомпанія була створена у 1998 році і є однією з підпорядкованих структур у складі АТ "ТехКом". "ТехКом"

спеціалізується на пасажирських і вантажних авіаперевезеннях і має різноманітний парк літаків і вертольотів.

Повітряний флот авіакомпанії "ТехКом" включає такі літальні апарати: Як-40, Як-42, Ан-12, Ан-24, Ан-26, Ан-74ТК-200, Ан-140.

Комп'ютерна мережа АТ «ТехКом» складається з п'яти сегментів. Мережа АТ складається з таких об'єктів:

- завод №1 та авіакомпанія «ТехКом» (два офіси);
- завод №2 (один офіс);
- завод №3 (один офіс);
- завод №4 (один офіс).

Мережа складається всього з 68 ПК та двох серверів, які розподілені у п'яти підмережах. Два сервери розташовані в першій та п'ятій підмережах (у даному випадку одна підмережа відповідає одному офісу або сегменту). Перша, друга, третя і четверта підмережі містять по 14 ПК, а п'ята підмережа - 12 ПК. Кожна підмережа обладнана власним комутатором, на якому налаштований DHCP і VLAN.

Кожен офіс використовує свій VLAN: для першого офісу - VLAN 10 (див. лістинг 4.1), для другого - VLAN 20, для третього - VLAN 30, для четвертого - VLAN 40, і для п'ятого - VLAN 50 [27].

Лістинг 4.1 - Налаштування VLAN на комутаторах Cisco:

```
s1(config)#interface range fa0/14
s1(config-if-range)#switchport mode access
s1(config-if-range)#switchport access vlan 10
```

Також налаштовані TRUNK-порти для забезпечення комунікації між комутаторами і підмережами. Отже, одержано поліпшену безпеку, зручність управління та безліч можливостей щодо масштабування мережі.

Граф-схему мережі зображено на рисунку 4.1:

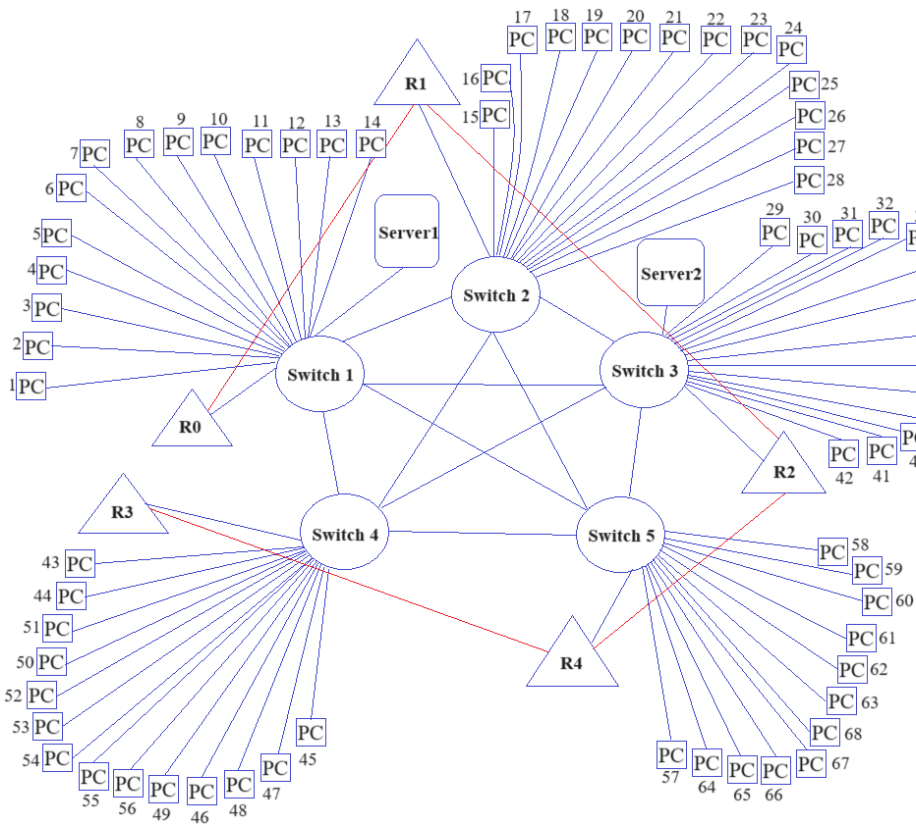


Рисунок 4.1 – Граф-схема мережі підприємства

Логічну схему мережі зображено на рисунку 4.2:

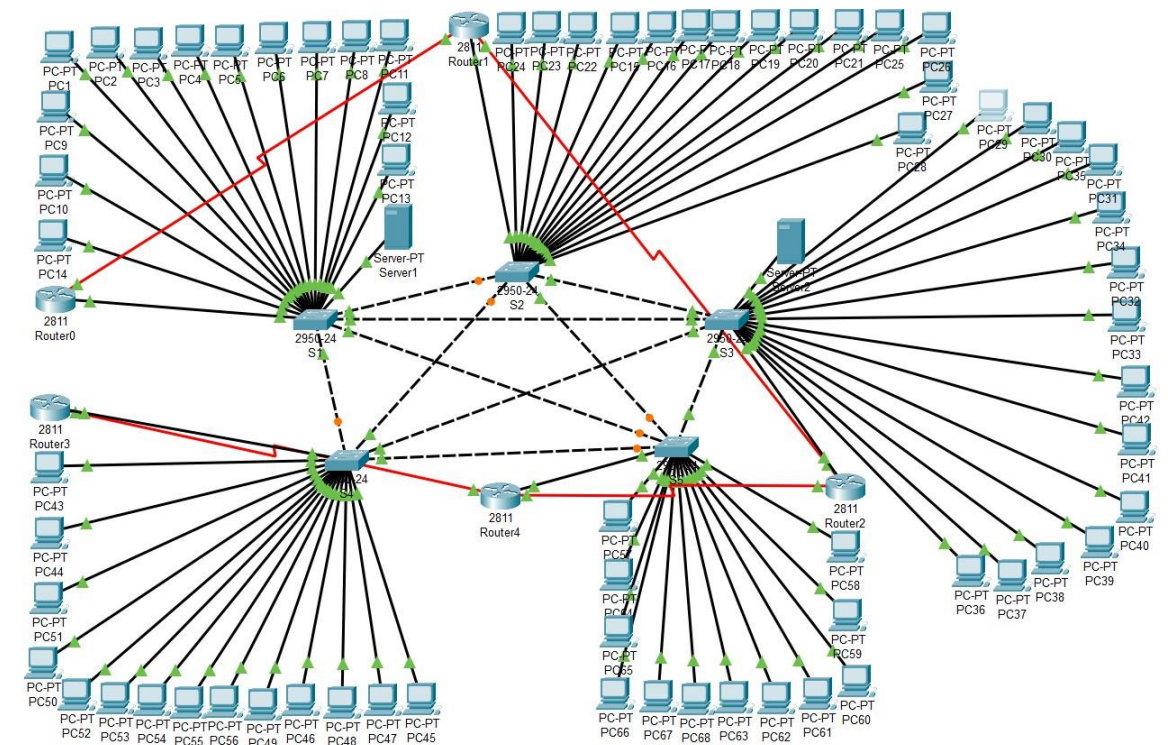


Рисунок 4.2 – Логічна схема мережі

Для забезпечення маршрутизації використовується динамічна OSPF технологія на всіх маршрутизаторах. Крім того, створені тунелі (VPN GRE) з однієї підмережі до двох і з чотирьох до п'яти різних підмереж. Це може бути корисно для встановлення зв'язку між мережею та віддаленими пристроями або іншою віддаленою мережею. Також вся передана по VPN тунелю інформація шифрується алгоритмами шифрування, що захищає підключення.

Після успішного підключення всіх мережевих пристроїв до мережі АТ «ТехКом», необхідно провести їх налаштування. Першочерговою задачею є налаштування кожного індивідуального пристрою в мережі та надання йому унікального ідентифікатора (IP). Для даної мережі використовуються динамічні IP (Internet Protocol) адреси. Починаючи з встановлення Gateway і закінчуючи IP адресою самого пристрою та маскою підмережі.

Таблиця 4.1 – Параметри інтерфейсів

Пристрій	Інтерфейс	Assignment	Network
S1	Fa0/15	Vlan10	10.1.10.1
	Fa0/1-Fa0/14	Vlan10	10.1.10.1
	Fa0/24	Trunk	***
S2	Fa0/1-Fa0/14	Vlan20	10.1.20.1
	Fa0/24	Trunk	***
S3	Fa0/1-Fa0/14	Vlan30	10.1.30.1
	Fa0/16	Vlan30	10.1.30.1
	Fa0/24	Trunk	***
S4	Fa0/1-Fa0/14	Vlan40	10.1.40.1
	Fa0/24	Trunk	***
S5	Fa0/1-Fa0/12	Vlan50	10.1.50.1
	Fa0/24	Trunk	***

Таблиця 4.2 – Адресація

Пристрій	Інтерфейс	ІР-адреса	Маска	Default Gateway
R0	Fa0/0.10	10.56.8.1	255.255.255.0	***
	Serial0/2/0	199.56.8.1	255.255.255.224	***
	Tunnel0	10.10.10.1	255.255.255.0	***
R1	Fa0/0.20	10.56.7.1	255.255.255.0	***
	Serial0/2/0	199.56.8.2	255.255.255.224	***
	Serial0/2/1	199.56.7.1	255.255.255.224	***
R2	Fa0/0.50	10.56.4.1	255.255.255.0	***
	Serial0/2/1	199.56.7.2	255.255.255.224	***
	Serial0/2/0	199.56.6.1	255.255.255.224	***
R3	Fa0/0.30	10.56.6.1	255.255.255.0	***
	Serial0/2/1	199.56.5.2	255.255.255.224	***
R4	Fa0/0.40	10.56.5.1	255.255.255.0	***
	Serial0/2/0	199.56.6.2	255.255.255.224	***
	Serial0/2/1	199.56.5.1	255.255.255.224	***
Server 1	Fa0	10.56.8.7	255.255.255.0	10.56.8.1
Server 2	Fa0	10.56.4.11	255.255.255.0	10.56.4.1
PC1-PC14	***	DHCP	255.255.255.0	10.56.8.1
PC15-PC28	***	DHCP	255.255.255.0	10.56.7.1
PC29-PC-42	***	DHCP	255.255.255.0	10.56.6.1
PC43-PC-56	***	DHCP	255.255.255.0	10.56.5.1
PC57-PC68	***	DHCP	255.255.255.0	10.56.4.1

Моделювання трафіку - це процес створення випадкових моделей потоків даних у мережі, які можуть бути використані для дослідження різних аспектів мережевого трафіку. Цей процес може застосовуватися як у випадку стільникових, так і комп'ютерних мереж.

Існують два основних підходи до моделювання мережевого трафіку: аналітичний та імітаційний. Аналітичний підхід передбачає математичний опис модельованих об'єктів та процесів у вигляді системи математичних рівнянь і виразів. Цей метод дозволяє проводити теоретичні дослідження та аналіз, але може бути складним для використання в реальних мережах через обмежену можливість побудови аналітичних моделей для складних сценаріїв трафіку.

У випадках, коли потрібно провести обчислення робочих характеристик системи, найбільш зручним є використання імітаційних моделей. Ці моделі базуються на алгоритмах, які крок за кроком відтворюють події, які відбуваються

в реальній системі. Один із методів імітаційного моделювання трафіку полягає в створенні алгоритму, який може генерувати послідовності подій, подібні до тих, що спостерігаються в мережі передачі даних.

На сьогоднішній день існують чотири основних класи моделей, які використовуються для моделювання трафіку в мережі:

- класичні моделі потоків, які ґрунтуються на теорії масового обслуговування;
- моделі, що базуються на випадкових процесах з модульованими випадковими величинами;
- фрактальні моделі, які враховують статистичну самоподібність деяких видів трафіку;
- моделі, які генерують імітаційні послідовності, подібні до реального трафіку.

Проведено моделювання потоків трафіку від ПК номер 14 до ПК 36 з використанням імітаційного підходу. PDU з робочої станції до проходу через маршрутизатор один представлено малюнку 4.3:

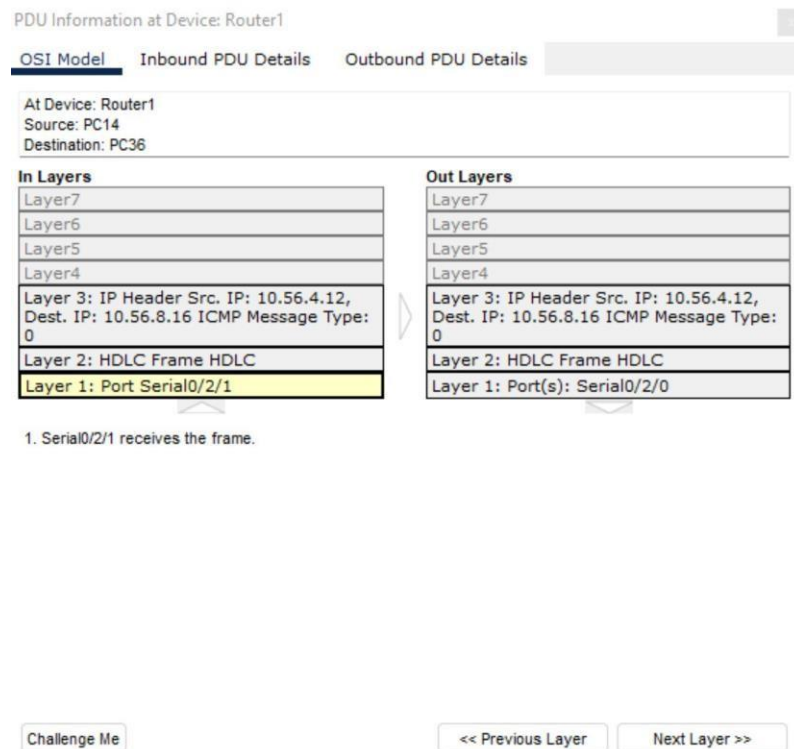


Рисунок 4.3 – Моделювання потоків трафіку

Проведено моделювання потоків трафіку від ПК номер 14 до ПК 36. PDU з робочої станції до проходу через комутатор три представлено рисунку 4.4:

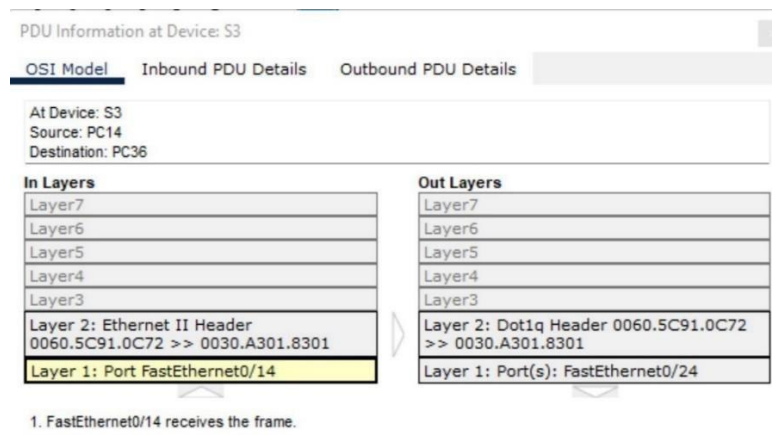


Рисунок 4.4 – Моделювання потоків трафіку

Забезпечення надійності критичних вузлів мережі є важливим завданням. Основні принципи резервування таких важливих вузлів, як комутатори ядра, центри обробки даних (ЦОД) або вузли розподілу, можуть бути описані через розгляд двох загальних методів - стекування та кластеризації.

Кожен із цих методів має свої переваги та недоліки, які будуть розглянуті детальніше.

Нижче наведено загальний рисунок 4.5, яка порівнює обидва методи резервування:

Екстремальні кампусні технології - стекування проти кластеризації

Особливості	Стекування	Кластеризація
Управління	Єдиний керуючий IP	Дві адреси управління
Відстань	Залежить від портів стекування	Залежить від типу SFP
Оновлення програмного забезпечення	Оновлення всього стеку	Оновлення окремих одиниць
Конфігурація	Єдиний загальний конфігураційний файл	Файл конфігурації для кожного вузла
Перехід після відмови	Підсекундне перемикання після відмови L2 Протоколи вищого рівня повинні повторно сходитися	Підсекундна відмова
Складність	Те саме, що один вузол	Вимагає додаткових протоколів (приклад VRRP)
Заміна блоку	Деякі зміни конфігурації стеків EXOS Автоматично на стеках ERS	Повне ручне перенаштування
Стійкість	Високий	Найвищий

Рисунок 4.5 – Порівняння двох методів резервування

а) управління:

- 1) перевага у стекуванні полягає в простоті управління. Кілька комутаторів у стеці представляються як один комутатор з багатьма портами;
- 2) у кластеризації потрібно керувати кількома незалежними комутаторами;

б) відстань:

- 1) у кластеризації може бути перевага у випадку, коли використовуються спеціальні технології стекування через порти або подвійного призначення портів. Тут можливі великі відстані між комутаторами;
- 2) однак, у стекуванні також існують варіанти зі звичайними портами стекування, які мають обмежену довжину кабелю;

в) оновлення ПЗ:

- 1) під час оновлення програмного забезпечення (ПЗ) при стекуванні ви оновлюєте ПЗ на майстер-комутаторі, який потім розповсюджує нове ПЗ на інші члени стеку;
- 2) оновлення ПЗ може вимагати апаратного перезавантаження, що призводить до перерви в роботі всього стеку;
- 3) проте при кластеризації у вас є два незалежних пристрої, на яких ви можете оновлювати ПЗ послідовно один за одним, уникнувши при цьому перерви в роботі. Отже, вибір між стекуванням та кластеризацією залежить від конкретних потреб і обставин мережі, а також від важливості кожного з розглянутих критеріїв;

г) конфігурація налаштувань:

- 1) у стекуванні перевага полягає в зручності конфігурації, оскільки потрібно налаштовувати лише один пристрій та конфігураційний файл.
- 2) у кластеризації кількість файлів конфігурації дорівнює кількості вузлів кластера, що може бути менш зручним у великих мережах.

г) відмовостійкість:

- 1) обидві технології в цьому плані приблизно рівні, але кластеризація має невелику перевагу;
- 2) причина полягає в тому, що в кластеризації кожен вузол є самостійним пристроєм зі своїми ресурсами та оброблює певну частину навантаження. Тому, якщо один вузол вийде з ладу, інші можуть продовжувати працювати. У стекуванні також є відмовостійкість, але всі пристрої в стеці спільно обробляють навантаження, тому в разі відмови одного пристрою може виникнути більша перерва в роботі мережі:

- присутній головний комутатор (master-switch), на якому функціонують всі основні процеси та протоколи, такі як протокол динамічної маршрутизації OSPF;

- також існують інші комутатори-підчинені (slave-switch), на яких запущені основні процеси, необхідні для роботи в стеку та обробки трафіку, що проходить через них;

- у випадку виходу з ладу головного комутатора (master-switch), наступний за пріоритетом комутатор-підчинений (slave-switch) виявляє відмову майстра;

- він автоматично ініціює себе як нового майстра та запускає всі процеси, які раніше працювали на головному комутаторі (включаючи протокол OSPF, який є об'єктом нашого спостереження);

- після короткого часу після запуску процесів (зазвичай це відбувається дуже швидко), протокол OSPF починає нормальну роботу;

- отже, при відмові одного з вузлів в системі кластеризації, OSPF відновлює роботу трохи швидше, ніж при стекуванні (на час, необхідний для запуску та ініціалізації процесів та протоколів на комутаторі-підчиненому стеку). Важливо відзначити, що сучасні технології стекування та комутатори зазвичай працюють дуже швидко, і переривання трафіку при перемиканні стеку зазвичай триває менше однієї секунди. Однак за цим параметром кластеризація все одно виграє;

д) складність - на основі представленої таблиці можна зазначити, що стекування виграє за показником складності. Це обумовлено в першу чергу пунктами "керування" та "конфігурації налаштувань". Налаштування та управління окремим вузлом стеку вимагає менше часу та ресурсів. Також при кластеризації часто доводиться налаштовувати додаткові протоколи маршрутизації або протоколи резервування шлюзів, такі як VRRP або HSRP;

е) заміна вузлів - в цьому плані стекування виявляється більш вигідним. Для заміни комутатора в стеці часто потрібно провести мінімальні налаштування обладнання, наприклад:

- 1) оновити програмне забезпечення нового комутатора до версії програмного забезпечення стеку (а це можна робити відразу при підключенні нового комутатора до ЗІП);
- 2) налаштувати кілька базових команд для стекування (а для деяких видів комутаторів це навіть не потрібно);
- 3) вийняти комутатор стеку, що вийшов із ладу, і підключити новий;
- 4) забезпечити електропостачання та підключити патч-кабелі;

є) пружність - як один із основних параметрів. В цілому, пружність - це комплексна характеристика, що вказує на здатність чогось змінюватися під дією навантаження і повертатися до первісного стану після припинення цього навантаження. Дивно, але навіть з урахуванням 4:3 на користь стекування за іншими характеристиками, кластеризація все ж таки виграє в аспекті пружності. Основна причина полягає в людському факторі. Так, ви не помиляєтесь - саме завдяки аспектам, як єдине управління, конфігурація налаштувань і спрощена складність, стекування може бути менш пружним через людський фактор.

Обидві технології мають свої переваги та недоліки, і кожна із них підходить для різних сценаріїв. Проте, для ядра мережі та високонавантажених ЦОД найчастіше вибирають кластеризацію.

Окрім технологій стекування та резервування вузлів мережі, існують загальні принципи резервування окремих компонентів вузла мережі та зв'язків між вузлами:

- резервування живлення блоків - встановлення двох дублюючих блоків живлення (найкраще з підключенням до джерела живлення першої категорії) може значно спростити управління вашою системою;

- резервування модульних плат керування - зазвичай використовується в модульних комутаторах, які мають можливість підключення кількох плат керування для забезпечення надійності;

- резервування інтерфейсних карт - також є актуальним для більшості модульних комутаторів і полягає в можливості дублювання інтерфейсних карт для забезпечення надійності зв'язку.

Під резервуванням зв'язку/лінків розуміється наявність дублюючих кабельних трас (або радіолінків, у випадку відкритих просторів), які можуть бути використані для:

- розподілу по різних кабельних шахтах і каналах всередині будівлі;
- географічного розподілу по території на рівні двох і більше будівель, міст, областей або країн (наприклад, створення об'ємних кілець).

При цьому побудові резервних лінків зв'язку важливо дотримуватися наступних рекомендацій для обладнання:

- у випадку дублювання інтерфейсних карток модульного комутатора або за наявності стеку, лінки повинні розподілятися між юнітами - інтерфейсними картками (для модульних комутаторів) або комутаторами (для стеку);

- бажано використовувати протоколи агрегування зв'язку, такі як LACP, MLT, PAgP і т. д., для об'єднання лінків у групи та балансування навантаження між ними;

- використовувати маршрутизатори, які підтримують протоколи ESMR (Equal-Cost-Multi-Path), які дозволяють розподіляти пакети за декількома найкращими маршрутами з рівними метриками протоколу маршрутизації [28].

4.3 Тестування працездатності мережі

Програмна емуляція та тестування працездатності роботи мережі буде проводитись в програмі Cisco Packet Tracer. Емуляція роботи представлена нижче на рисунку 4.6:

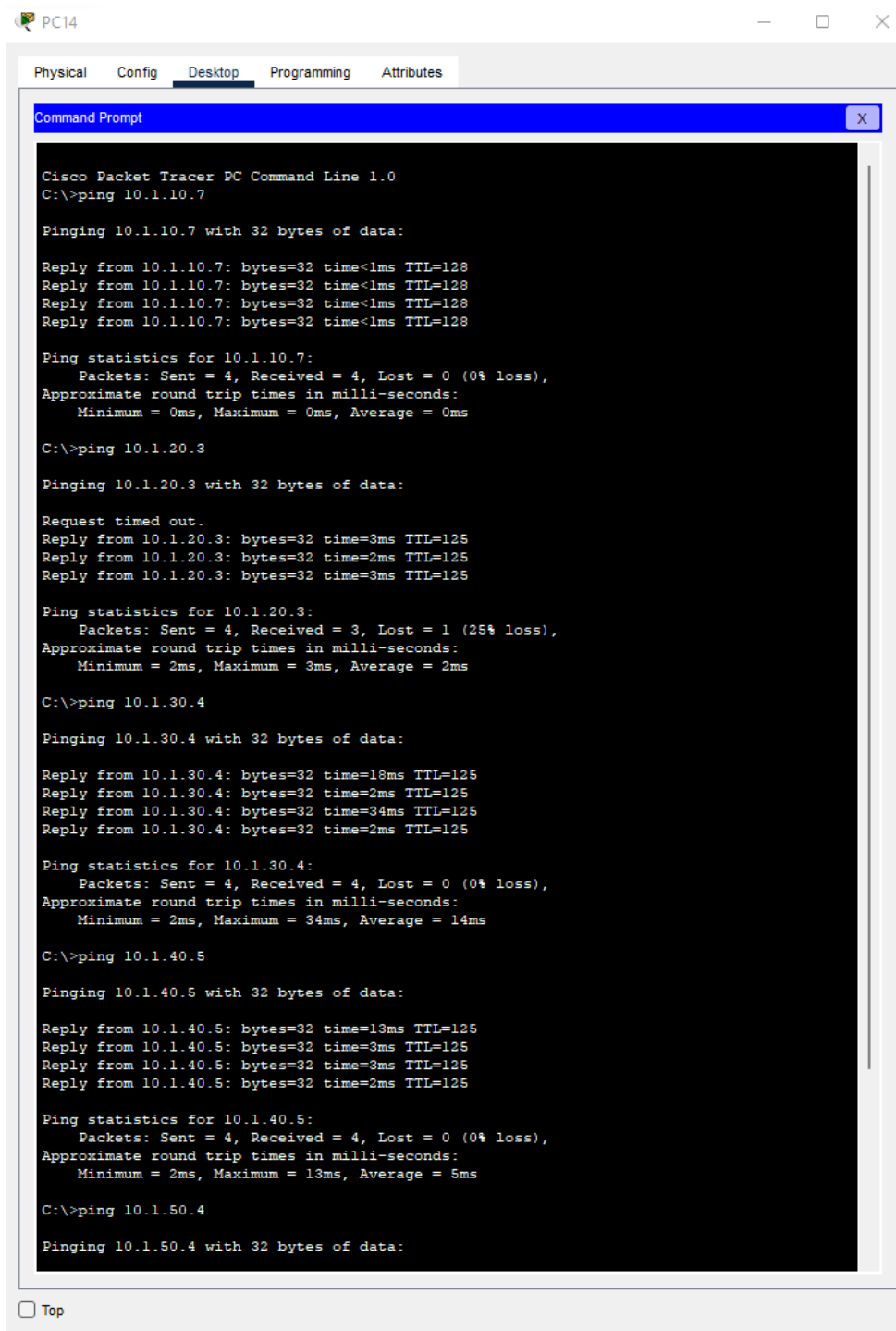


Рисунок 4.6 – Тестування роботи мережі АТ «ТехКом»

Як видно на рисунку 4.6, мережа функціонує надійно: персональні комп'ютери спілкуються між собою без втрати пакетів.

4.4 Забезпечення мережевої безпеки та підключення до Інтернет

Для підключення маршрутизатора до Інтернету необхідно вставити кабель провайдера у порт WAN (Internet). Для доступу до веб-інтерфейсу маршрутизатора, необхідно відкрити веб-браузер та у рядку адреси ввести 192.168.0.1.

Щоб налаштувати підключення до Інтернету:

- обрати «Network» та «WAN»,
- вибрати тип підключення WAN: Dynamic IP,
- зберегти налаштування, натиснувши кнопку "Save".

Деталі щодо налаштування підключення до Інтернету наведено на рисунку 4.7:

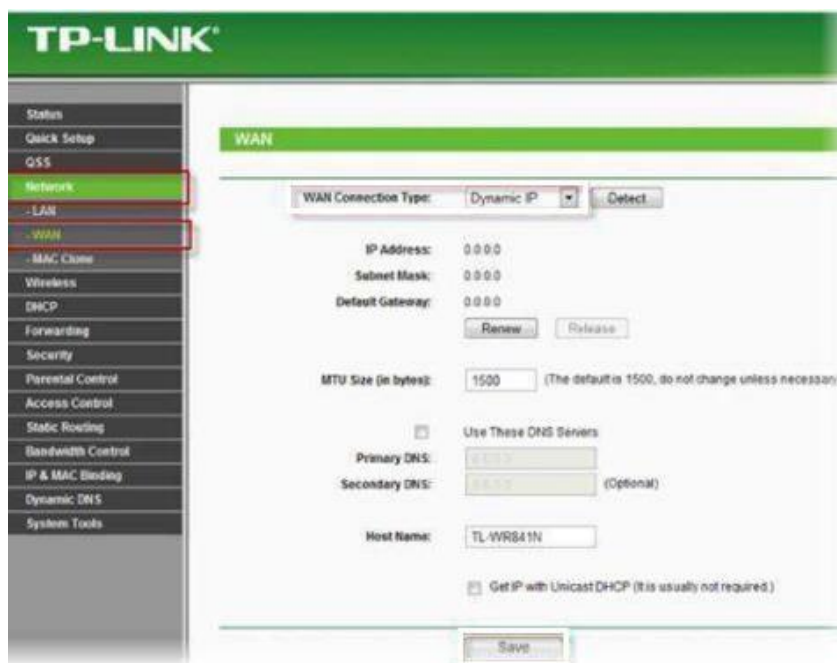


Рисунок 4.7 – Налаштування підключення до Інтернету

Після збереження налаштувань, для їх введення в дію, потрібно виконати перезавантаження маршрутизатора. Це можна здійснити, перейшовши до розділу

"Reboot" та натиснувши кнопку "Reboot," щоб перезавантажити пристрій, як показано на рисунку 4.8:



Рисунок 4.8 – Налаштування підключення до Інтернету

Тепер налаштовано підключення до Інтернету, та мережева безпека забезпечена.

Висновки: було проведено аналіз структури підприємства та налаштовано логічну схему та граф-схему мережі, тестування якої було проведено та встановлено, що функціонує надійно. Отже, цю мережу можна успішно впровадити та використовувати на підприємстві.

ВИСНОВКИ

У ході дослідження, предметом якого була мережа підприємства «ТехКом» з використанням mesh-технології, а метою – підвищення надійності мережі, було проведено аналіз та розглянуто важливі аспекти надійності в інформаційних системах та бізнесі. Досліджено методи підвищення готовності мереж, визначення надійності складових елементів мережі та їх ризику. В рамках роботи було проведено порівняльний аналіз різних типів мереж, таких як кільцеві, зіркові, деревоподібні та mesh-мережі, для визначення їхньої надійності та проблем, які можуть виникнути в процесі експлуатації.

На прикладі підприємства «ТехКом», яке спеціалізується на зборі та обробці великої кількості даних, було розроблено модель об'єднаної мережі та проведено аналіз її структури та обсягу трафіку. Результати дослідження дозволили виявити проблеми, пов'язані з низькою надійністю деяких типів мереж та виділити mesh-мережу як найбільш надійний варіант для задач даного підприємства.

Загальний контекст сучасного світу підкреслює важливість комп'ютерних мереж, які стають все більш актуальними та необхідними завдяки зростаючій кількості підключених пристроїв, вимогам до надійності та безпеки мереж, а також розподіленості та глобальності мережових інфраструктур. Використання mesh-мереж може значно покращити доступність та надійність мережових послуг, що стає надзвичайно важливим аспектом в інформаційній технології сьогодення.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Network reliability – The invisible driver of business productivity. *New Charter Technologies*. URL: <https://www.newchartertech.com/network-reliability-the-invisible-driver-of-business-productivity/> (date of access: 14.09.2023).
2. Поняття надійності стосовно комп'ютерних мереж. *Студопедия*. URL: https://studopedia.su/4_51013_ponyattya-nadiynosti-stosovno-kompyuternih-merezh.html (дата звернення: 14.10.2023).
3. Основи надійності комп'ютерних мереж. *StudFiles*. URL: <https://studfile.net/preview/5609065/> (дата звернення: 15.09.2023).
4. Надійність, відмовостійкість і безпека корпоративних комп'ютерних мереж. *StudFiles*. URL: <https://studfile.net/preview/5011354/page:3/> (дата звернення: 15.09.2023).
5. Показники надійності та відмовостійкості URL: http://ni.biz.ua/4/4_13/4_137832_pokazateli-nadezhnosti-i-otkazoustoychivosti.html (дата звернення: 14.10.2023).
6. Принципи мережевого аналізу та оптимізації. *Studizba*. URL: <https://studizba.com/files/show/doc/129087-2-62762.html> (дата звернення: 14.10.2023).
7. Martin L. Shooman. Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design: a Wiley-Interscience Publication John Wiley & Sons, inc. New York: Polytechnic University and Martin L. Shooman & Associates, 2002. 546 с. URL: <http://pws.npru.ac.th/sarththong/data/files/Wiley%20-%20Reliability%20Of%20Computer%20Systems%20And%20Networks%20-%20Fault%20Tolerance,%20Analysis%20And%20Design.pdf> (date of access: 14.09.2023).
8. Використання Cisco Packet Tracer. URL: <https://ua5.org/lan/1469-vykorystannya-cisco-packet-tracer.html> (дата звернення: 03.10.2023).

9. Знайомство з cisco packet tracer. URL:<http://nickshevtsov.blogspot.com/2017/10/cisco-packet-tracer.html> (дата звернення: 03.10.2023).
10. Advantages and disadvantages of cisco packet tracer. URL: <https://brainly.in/question/1782890> (date of access: 03.10.2023).
11. Що таке Lan і Wan, в чому їхня відмінність і яке застосування. *SmartAndYoung технологічний журнал*. URL: <http://smartandyoung.com.ua/shho-take-lan-i-wan-v-chomu-ihnja-vidminnist-i> (дата звернення: 14.10.2023).
12. Апаратура 100BASE-TX. URL: http://ni.biz.ua/9/9_2/9_27370_apparatura-BASE-TX.html (дата звернення: 14.10.2023).
13. Опис технології Fast Ethernet. URL: <https://www.ixbt.com/comm/tech-fast-ethernet.shtml> (дата звернення: 14.03.2022).
14. Маршрутизатор Cisco 2901. URL: <http://surl.li/dxgff> (дата звернення: 14.03.2022).
15. Комутатор Cisco Catalyst 2950-24. URL: <http://surl.li/dxgfr> (дата звернення: 14.03.2022).
16. Все, що потрібно знати про виту пару. URL: <https://deps.ua/ua/knowegable-base/reference-information/9634.html> (дата звернення: 14.03.2022).
17. Топологія комп'ютерних мереж. URL:https://stud.com.ua/53329/informatika/topologiya_kompyuternih_merezh (дата звернення: 19.10.2023).
18. Топологія комп'ютерних мереж. *Комп'ютерні мережі*. URL: https://comp-net.at.ua/index/topologija_komp_39_juternikh_merezh/0-6 (дата звернення: 19.10.2023).
19. Mesh-мережі (сітчаста мережа) URL: <https://ips.ligazakon.net/document/TM071839> (дата звернення: 19.10.2023).
20. Григорян М.С., Зеленцова І.Я., Тягунова М.Ю. Використання MESH-мереж у кіберфізичних системах: наук.-техн. конф., тези доп., 24-28 квітня 2023 р. / редкол.: ШАЛОМЄЄВ В. (відпов. ред.) Запоріжжя : НУ «Запорізька політехніка», 2023. С. 28-29 – 1 електрон. -опт. диск (DVD-ROM).

21. Mesh-мережі: переваги та недоліки, впровадження та сфери застосування. URL: <http://www.incore.me/internet-texnologii/preimushhestva-i-nedostatki-mesh-setej-vnedrenie-i-oblasti-primeneniya-mesh-setej/> (дата звернення: 19.10.2023).
22. Метод мінімальних шляхів і мінімальних перетинів. URL: https://stud.com.ua/164255/informatika/metod_minimalnih_shlyahiv_minimalnih_peretiviv (дата звернення: 15.09.2023).
23. Methods for analysis of complex reliability networks. *Science Direct*. URL: <https://www.sciencedirect.com/science/article/abs/pii/B9780080447285500032> (date of access: 15.09.2023).
24. New and efficient method to find all minimal paths. URL: <https://goo.su/YExE4> (date of access: 15.09.2023).
25. Щербаков А. М. Надійність, контроль, діагностика, комп'ютерної техніки. Методичні вказівки до лабораторних робіт з дисципліни “Надійність, контроль, діагностика та експлуатація комп'ютерної техніки” для студентів спеціальності 8.09150І-“Комп'ютерні системи та мережі“, 7.091503-“Спеціалізовані комп'ютерні системи” усіх форм навчання. Запоріжжя: ЗНТУ, 2003.-59 с.
26. Григорян М. С., Зеленцова І.Я. Дослідження впливу конфігурації мережі на показники її надійності. Інформаційні технології в освіті та науці: міжнар. наук.-практ. конф., тези доп., 25-26 травня 2023 р. МДПУ ім. Богдана Хмельницького. – Запоріжжя. - 2023. С. 106-112.
27. Основи комп'ютерних мереж. Тема №6. Поняття VLAN, Trunk та протоколи VTP та DTP. *Habr*. URL: <https://goo.su/oOWSbKS> (дата звернення: 15.11.2023).
28. Дизайн мережі підприємства на комутаторах Extreme. *Habr*. URL: <http://surl.li/dxgbi> (дата звернення 14.03.2022).