Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Кіберфізична система для моніторингу пасивних оптичних телекомунікаційних мереж (програмна частина)
Назва теми

КвРКІ 200119.20.01.18 ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія та програмування»*
Назва

Виконав: студент IV курсу, група КІ2-20-1 _____ Д. Д. Ткаченко
Підпис, Ініціали, прізвище

Керівник _____ О. В. Іванов
Підпис, дата, Ініціали, прізвище

Нормоконтролер _____ С.М. Лисенко
Підпис, дата, Ініціали, прізвище

До захисту допускаю:
Зав. кафедри комп'ютерної інженерії та інформаційних систем _____ Т.О. Говорущенко
Підпис, Ініціали, прізвище

«21» червня 2024 р.

Хмельницький 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ

Зав. кафедри Т.О.Говорущенко

"10" 01 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Ткаченку Денису Дмитровичу
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Кіберфізична система для моніторингу пасивних оптичних телекомунікаційних мереж (програмна частина)
Керівник проекту (роботи) Іванов О.В., к.т.н., доцент.
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 15.02.2024 р. № 8

2. Строк подання студентом проекту (роботи) на кафедру 01.06.2024 р.

3. Вихідні дані до проекту (роботи) Завдання на кваліфікаційну роботу

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Кіберфізична система для моніторингу пасивних оптичних телекомунікаційних мереж та постановка задачі щодо розробки такої системи

Проєктування програмно-технічного засобу системи для моніторингу пасивних оптичних телекомунікаційних мереж

Програмно-апаратна реалізація кіберфізичної системи для моніторингу пасивних оптичних телекомунікаційних мереж

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

Логічна топологія схеми мережі

Фізична топологія схеми мережі

Алгоритм системи підтримки прийняття рішень

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Лисенко С.М., професор кафедри КІІС		
Антиплагіат	Нічепорук А.О., доцент кафедри КІІС		

7. Дата видачі завдання «_10_»_____01_____2024 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	01.02.2024	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	05.02.2024	виконано
3	Робота над розділом 1 – дослідження предметної області та визначення задач	23.02.2024	виконано
4	Робота над розділом 2 – проєктування програмно-технічного засобу	29.03.2024	виконано
5	Робота над розділом 3 – програмно-апаратна реалізація та тестування програмно-технічного засобу	06.05.2024	виконано
6	Оформлення пояснювальної записки згідно вимог	25.05.2024	виконано
7	Попередній захист ВКР	30.05.2024	виконано
8	Захист ВКР на засіданні ЕК	Червень 2024 року	

Студент _____ Д. Д. Ткаченко
Підпис Ініціали, прізвище

Керівник роботи _____ О. В. Іванов
Підпис Ініціали, прізвище

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ 200119.20.01.18 ПЗ	Пояснювальна записка	59		
			Графічні матеріали			
2		КвРКІ 200119.20.01.18 Е8	Логічна топологія схеми	1		
			мережі			
3		КвРКІ 200119.20.01.18 Е8	Фізична топологія схеми	1		
			мережі			
4		КвРКІ 200119.20.01.18 Е8	Блок-схема алгоритму	1		
			роботи системи підтримки			
			прийняття рішень			

Зм	Арк	№ докум	Підпис	Дата	КвРКІ 200119.20.01.18 ВП		
Розробив		Ткаченко		17.06	Відомість проекту	Літера	Аркуш 1 / Аркушів 1
Перевір.		Іванов		20.06		У	
Н. контр.		Лисенко		20.06		ХНУ, КІ2-20-1	
Затв.		Говорушенко		21.06			

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Кіберфізична система для моніторингу пасивних оптичних телекомунікаційних мереж (програмна частина)».

Автор роботи: Ткаченко Денис Дмитрович.

Керівник роботи: Іванов Олексій Валентинович.

Пояснювальна записка: 59 с., 43 рис., 2 табл., 3 дод., 44 джерела.

Графічна частина: 3 креслення.

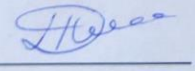
КІБЕРФІЗИЧНА СИСТЕМА, CISCO PACKET TRACER, JAVA, МОНІТОРИНГ, ПАСИВНА ОПТИЧНА МЕРЕЖА.

Метою дипломної роботи є систематизація, закріплення та поширення теоретичних знань з дисципліни, ознайомлення з технічними аспектами пасивних оптичних мереж, стандартами та типами, а також засобами та методами їх моніторингу.

Об'єктом дослідження є функціонування моніторингових елементів пасивних оптичних мереж.

Предметом дослідження є оцінка сценаріїв застосування моніторингу пасивних оптичних мереж.

Під час проведення даного дослідження був використаний метод систематичного огляду літератури для вивчення і аналізу предметної області даного дослідження з текстових джерел інформації.



Підпис студента

20.06.24

Дата

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧЕННЯ

PON (англ. Passive Optical Network) – пасивна оптична мережа

TDM (англ. Time Division Multiplexing) – тимчасовий розподіл каналів

OLT (англ. Optical Line Terminal) – оптичний лінійний термінал

ONU/ONT (англ. - Optical Network Terminal Unit) – оптичний мережевий блок

WDM (англ. Wavelength-Division Multiplexing) – оптичний мультиплексор

FTTB (англ. Fiber to the Building) – оптика до квартири

FTTH (англ. Fiber to the Home) – оптика до дому

FTTC (англ. Fiber to the Carb) – оптика до групи будинків

FTTCab (англ. Fiber to the Cabinet) – оптика до розподільчої шафи

FTTx (англ. Fiber to the x…) – оптика до …

APON (англ. Asynchronous Passive Optical Network) – асинхронна пасивна оптична мережа

GPON (англ. Gigabit Passive Optical Network) – гігабітна пасивна оптична мережа

EPON (англ. Ethernet Passive Optical Network) – езернетна пасивна оптична мережа

XG-PON (англ. 10-Gigabit Passive Optical Network) – десяти гігібітна пасивна оптична мережа

NG-PON2 (англ. Next-Generation Passive Optical Network) – сорока гігабітна пасивна оптична мережа

OLTS (англ. Optical Loss Test Set) – тестер оптичного загасання

VFL (англ. Visual Fault Locator) - візуальний визначник місця пошкодження та дефекту

OTDR (англ. Optical Time Domain Reflectometer) - оптичний рефлектометр

ONMS (англ. Optical Network Management System) - системи управління оптичною мережею

СППР - система підтримки прийняття рішень

ICMP (англ. Internet Control Message Protocol) - міжмережевий протокол керуючих повідомлень

TCP/IP (англ. Transmission Control Protocol / Internet Protocol) – набір протоколів мережі Інтернет

SNR (англ. Signal-to-noise ratio) - співвідношення сигнал/шум

SNMP (англ. Simple Network Management Protocol) - простий протокол керування мережею

NETCONF (англ. Network Configuration) – мережевий протокол для конфігурації

REST (англ. Representational State Transfer) - передача репрезентативного стану

CPT – Cisco Packet Tracer

IDE (англ. Integrated Development Environment) - інтегроване середовище розробки

GUI (англ. Graphical user interface) – графічний інтерфейс користувача

JDK - Java Development Kit

CPDU (англ. Complex Protocol Data Unit) – комплексні налаштування для проведення різних тестувань

ВСТУП

Зі швидким розвитком технологій та зростаючими вимогами до якості й надійності телекомунікацій, пасивні оптичні мережі (PON) стають критично важливими компонентами сучасної інфраструктури зв'язку. Вони забезпечують високошвидкісну передачу даних, стабільність і надійність зв'язку, що робить їх незамінними для задоволення потреб сучасного інформаційного суспільства. Проте ефективне управління та моніторинг таких мереж потребує новітніх підходів та інструментів, які здатні забезпечити своєчасну діагностику, усунення несправностей та оптимізацію використання мережевих ресурсів.

Метою дипломної роботи на тему «Кіберфізична система для моніторингу пасивних оптичних телекомунікаційних мереж (програмна частина)» є розробка та впровадження системи підтримки прийняття рішень (СППР), яка дозволить ефективно моніторити, діагностувати та управляти пасивними оптичними мережами.

Для досягнення поставленої мети було визначено наступні завдання:

– дослідити основні аспекти кіберфізичних систем для моніторингу пасивних оптичних телекомунікаційних мереж;

– вивчити пасивні оптичні мережі, стандарти та типи PON (Passive Optical Network), а також засоби та методи їх моніторингу;

– провести аналіз переваг, які система підтримки прийняття рішень (СППР) приносить у плані ефективного моніторингу та управління оптичними мережами;

– виконати детальний аналіз функціональних та нефункціональних вимог до СППР;

– розробити проект програмно-технічного засобу, інтегруючи принцип пінгування для точного визначення стану мережі та ефективного управління нею;

– використати Cisco Packet Tracer для створення та тестування мереж, візуалізації архітектури, аналізу та оптимізації управління мережевими ресурсами;

– інтегрувати сервіс Complex PDU для централізованого збору даних, управління, діагностики мережі, відстеження подій, аналізу тенденцій та планування вдосконалень;

– розробити систему виявлення несправностей на основі алгоритмів кореляції в Java, створюючи надійний інструмент для аналізу та прогнозування стану мережі;

– провести моделювання та аналіз роботи мережі за допомогою Complex PDU в Cisco Packet Tracer, підтвердивши ефективність впровадження СППР через програмно-апаратну реалізацію та тестування розробленого програмно-технічного засобу.

Загалом, дипломна робота демонструє важливість інтеграції передових кіберфізичних систем у сферу управління пасивними оптичними мережами. Розроблена система підтримки прийняття рішень відкриває нові можливості для оптимізації роботи мереж та підвищення їх надійності. Результати дослідження та розробки підкреслюють значення комплексного підходу до аналізу мережевих систем, враховуючи сучасні технологічні виклики та потреби індустрії.

1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ВИЗНАЧЕННЯ ЗАДАЧ

1.1. Пасивні оптичні мережі

Пасивна оптична мережа (PON) - це технологія передачі даних, яка використовує оптичне волокно для безпосередньої передачі сигналів від центрального вузла до абонентських пристроїв. На відміну від активних оптичних мереж, де сигнали підсилюються та обробляються на кожному вузлі, у пасивних оптичних мережах сигнали розділяються та перенаправляються через пасивні роздільні елементи.

Застосування такої технології несе за собою немало зручних та корисних переваг, як для користувача так і для постачальника (провайдера):

– ефективне використання оптичного волокна: PON дозволяють раціонально використовувати оптичне волокно, розділяючи його між численними абонентами та зменшуючи необхідність у прокладанні нових кабелів;

– економія витрат: у порівнянні з традиційними активними мережами, PON забезпечують значні економічні переваги, оскільки вони потребують менше активного обладнання та споживають менше енергії;

– широкий спектр послуг, PON надають різноманіття послуг, включаючи доступ до Інтернету, голосові та відео послуги, інтерактивне відео, IP-телефонію та інші;

– висока пропускна здатність: PON забезпечують велику пропускну здатність, що дозволяє передавати значні обсяги даних з високою швидкістю;

– зниження витрат на обслуговування, де понад 90% компонентів PON є пасивними, що призводить до зменшення витрат на обслуговування мережі;

– простота розгортання: PON мають просту структуру, що спрощує їх впровадження та розширення мережі;

– масштабованість: PON можуть легко розширюватися для включення нових абонентів або збільшення пропускної здатності в майбутньому без суттєвих змін в існуючій інфраструктурі;

– висока якість обслуговування: забезпечення високої якості обслуговування для кінцевих користувачів завдяки стабільному і надійному з'єднанню;

– екологічна придатність: зменшення споживання електроенергії та викидів CO2 завдяки меншому використанню активного обладнання;

– підтримка новітніх технологій: PON можуть легко адаптуватися до новітніх технологій, таких як високошвидкісні мережі, мультикастові телекомунікаційні послуги, обробка відео в реальному часі тощо.

Дані для всіх користувачів передається одночасно за допомогою тимчасового розподілу каналів TDM від головної станції - оптичного лінійного терміналу OLT до кінцевих оптичних мережевих блоків (ONU/ONT). На рис. 1.1 зображено основні елементи архітектури PON. Передача та прийом у обох напрямах здійснюються по одному оптичному волокну, але на різних хвильових довжинах.

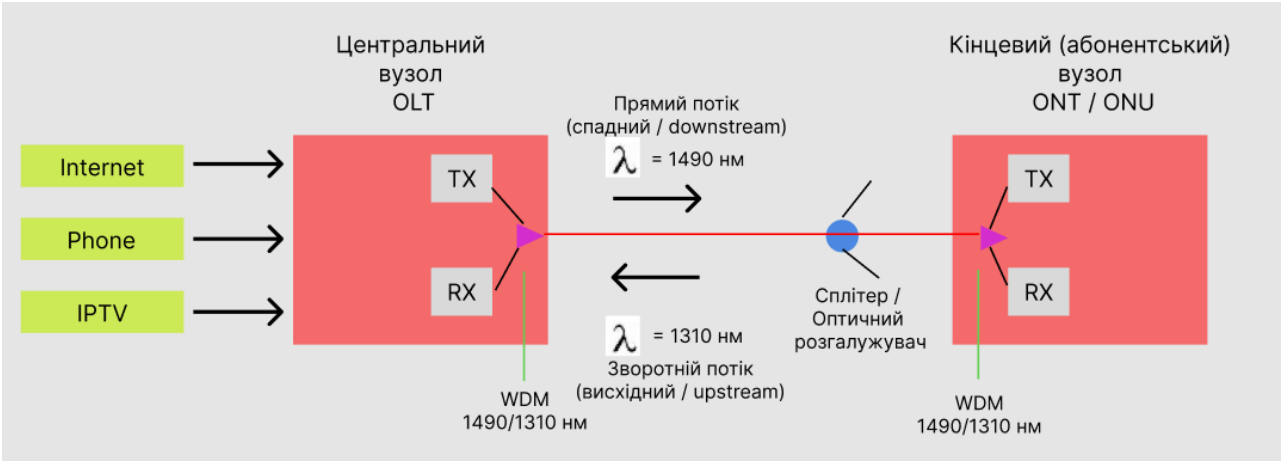


Рисунок 1.1 - Основні елементи архітектури PON

Для передачі потоку інформації від OLT до ONT - прямого (спадного) потоку, зазвичай використовується довжина хвилі 1490 нм. Натомість, дані від різних абонентських вузлів, що надходять до центрального вузла, утворюють зворотний

(висхідний) потік і передаються на довжині хвилі 1310 нм. У вбудованих у OLT та ONT мультиплексорах WDM розділяються вихідні і вхідні потоки.

На рис. 1.2 зображено принцип дії PON який має спадний та висхідний потоки. Спадний, який також називають прямим, має інформацію, яка призначена для всіх ONT, ле кожен кінцевий пристрій виділяє інформацію лише для свого терміналу.

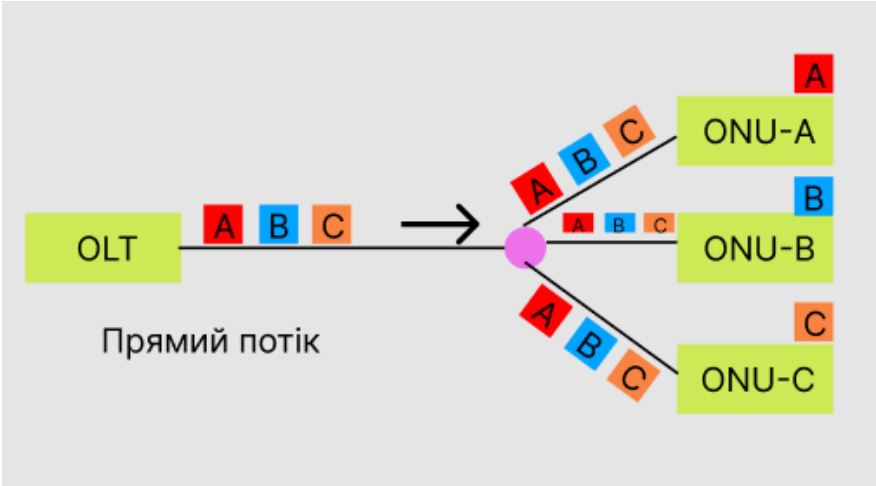


Рисунок 1.2 – Прямий (спадний) потік

В протилежному випадку існує висхідний (зворотній) потік. У зворотному (висхідному) напрямі, після об'єднання загальний потік містить сигнали від усіх користувачів, а від абонентів кожне ONU передає інформацію у свій момент часу. Таку схему представлено на рис. 1.3.

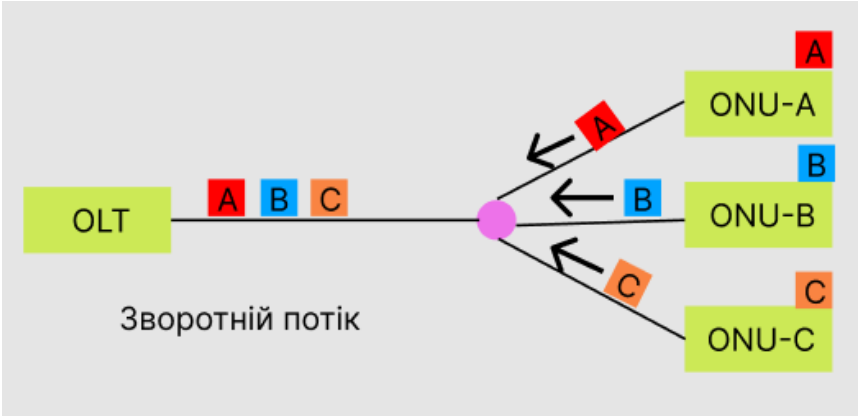


Рисунок 1.3 – Зворотній (висхідний) потік

Деякими з передумов виникнення PON на той момент були і є: підвищений попит на швидкісний Інтернет та передачу даних, що створювало потребу в розвитку ефективних та економічних технологій передачі даних, що відбувались в контексті зростання використання Інтернету та збільшення вимог до швидкості мереж; технологічний прогрес у галузі оптичних волокон відзначався зростанням їх доступності та ефективності, що виражалось в великій пропускній здатності та низьких втратах сигналу; необхідність зменшення витрат на обслуговування мережі стала важливим фактором у оптимізації витрат та покращення ефективності мережевих систем.

Також в наш час в містах, маленьких та великих найспоживанішим місцем для проживання є міська багатоквартирна забудова, у якій найпоширенішим став метод FTTB ("Волокно до під'їзду") для створення мережі, при новому будівництві, за умови наявності якісної кабельної інфраструктури. Використання пасивних оптичних мереж у поєднанні з технологіями FTTx ("Волокно до…") показує, що гнучке поєднання цих підходів дозволяє ефективно організувати мережі доступу для різних категорій абонентів та надавати широкий спектр сучасних телекомунікаційних сервісів. На рис. 1.4 зображена схема такого поєднання.

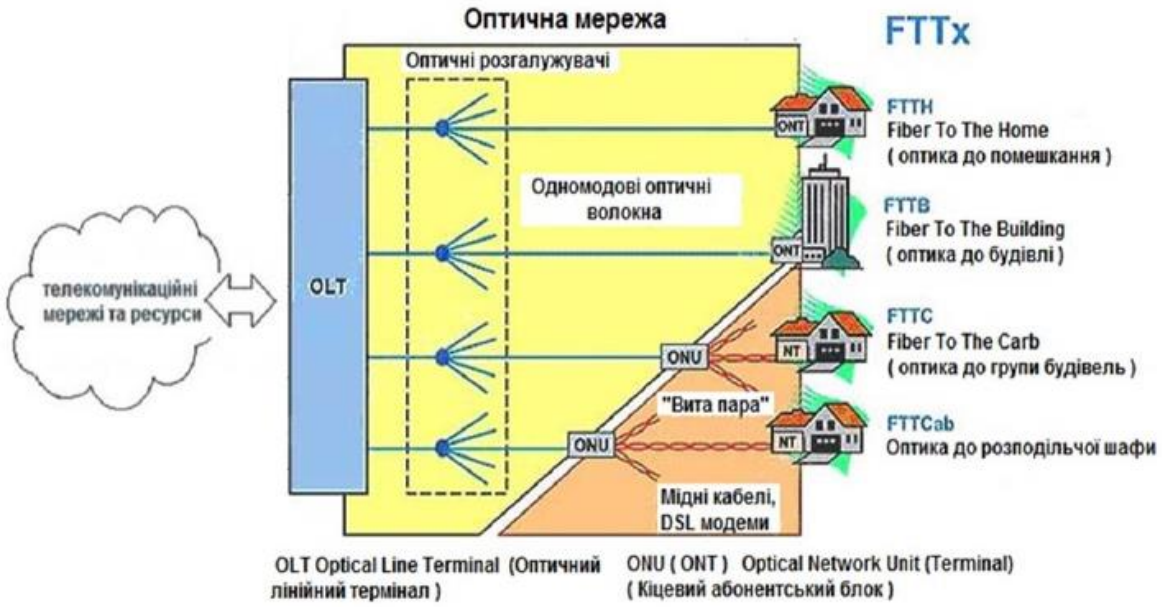


Рисунок 1.4 – Схема оптичної мережі з поєднанням PON та FTTx

1.2. Стандарти та типи PON

Стандарти та типи пасивних оптичних мереж (PON) визначаються різними протоколами та технологіями, які використовуються для передачі даних через оптичне волокно без використання активних елементів підсилення сигналу на шляху передачі. Ось деякі з найпоширеніших стандартів та типів PON:

APON - це тип пасивної оптичної мережі, який використовує асинхронну передачу даних між центральним вузлом і абонентськими пристроями. Ця технологія дозволяє передавати дані на високих швидкостях і забезпечує більшу ефективність мережі, зокрема при великій кількості абонентів. APON була попередницею EPON (Ethernet PON) і GPON (Gigabit PON).

GPON є одним з найпоширеніших стандартів PON, який забезпечує високу швидкість передачі даних до 2,5 Gbps вниз та до 1,25 Gbps вгору. Використовує протоколи, які оптимізовані для послуг Triple Play (голос, відео, дані).

EPON використовує технологію Ethernet для передачі даних і зазвичай пропонує швидкості до 1 Gbps в обох напрямках. Цей стандарт особливо популярний у домашніх та SOHO (малих офісних/домашніх) мережах.

Розгладаючи EPON і GPON, як дві з найпоширеніших типів технологій, можна виконати їх чітке порівняння:

– пропускна здатність: GPON надає більшу пропускну здатність порівняно з EPON. GPON зазвичай підтримує швидкості від 622 Мбіт/с до 2,488 Гбіт/с в напрямку до абонента (зворотний канал) та від 1,244 Гбіт/с до 2,488 Гбіт/с в напрямку від абонента (прямий канал), тоді як EPON зазвичай пропонує швидкості до 1,25 Гбіт/с.;

– протоколи та стандарти: GPON використовує спеціальні протоколи і стандарти, такі як ITU-T G.984, тоді як EPON базується на стандартах IEEE 802.3ah і IEEE 802.3av;

– методи мультиплексування: GPON використовує Time Division Multiplexing (TDM) та Wavelength Division Multiplexing (WDM) для передачі даних, тоді як EPON використовує TDM;

– ресурси каналу зворотного зв'язку: GPON має більше ресурсів каналу зворотного зв'язку, що дозволяє підтримувати більшу кількість абонентів на один центральний вузол порівняно з EPON;

– підтримка послуг: GPON має більше можливостей для підтримки різноманітних послуг, таких як телефонія, інтернет і телевізійне віщання, завдяки більш високій пропускній здатності та підтримці додаткових протоколів;

– вартість обладнання: EPON зазвичай вважається менш дорогим у встановленні та експлуатації порівняно з GPON, особливо для менших мереж. Однак GPON може бути більш вигідним для великих мереж через більшу пропускну здатність та кількість підтримуваних абонентів.

На сьогоднішній день, вже існують більш новітні та сучасні види технологій пасивних оптичних мереж: XG-PON є наступним рівнем розвитку PON, який забезпечує ще більшу швидкість передачі даних до 10 Gbps на вихід і до 2,5 Gbps на вхід, що робить його ідеальним для високопропускних додатків та послуг.

NG-PON2 є ще більш розширеним стандартом, який дозволяє досягнути швидкостей передачі даних від 40 Gbps і більше. Він також підтримує різні хвилі передачі даних, що дозволяє розділити різні види послуг на різних хвилях.

Усі ці стандарти та типи PON надають різні можливості для впровадження та оптимізації оптичних мереж, що відповідають різним потребам і вимогам користувачів.

1.3. Засоби та методи моніторингу PON

Конфігурація оптичної мережі має бути основним фактором у виборі моніторингового методу. Основна структура мережі EPON або GPON визначається кількістю активних абонентських терміналів ONT (ONU), що підключені до

центрального комутатора - оптичного лінійного терміналу (OLT) через оптичні волокна та розгалужувальні спліттери. Нормативні документи про обслуговування оптичного волокна та кабельних споруд обговорюються в рекомендаціях ITU-T SG6 і SG7 L.25, L.40, тощо. Для профілактичних заходів та післяаварійного відновлення, рекомендації L.53 і L.25 визначають потребу у функціях обслуговування оптичного волокна. Варто відзначити, що на сьогоднішній день, незважаючи на наявність зазначених рекомендацій, стандартизовані методи і засоби моніторингу PON мереж відсутні. Моніторинг волокон і локалізація дефектів - це основні функції забезпечення PON мереж, які дозволяють зменшити час пошуку несправностей і знизити витрати людських ресурсів при відновленні кабелю, що є пошкодженим.

Тестування волоконно-оптичних ліній зв'язку та оптичних мереж можна умовно поділити на три категорії:

– моніторинг втрат сигналу (тестування загасань);

– візуальна оцінка механічних з'єднань (конекторів) та стану волоконного провідника;

– комплексне тестування оптичної інфраструктури.

Методика визначення загасань у оптичних системах полягає в вимірюванні втрат сигналу під час його проходження через оптичний тракт. Загасання виражається у децибелах (дБ) і вказує на зменшення сили сигналу. Цей процес є важливим для оцінки ефективності та надійності оптичної мережі, оскільки дозволяє виявити місця, де можуть виникати втрати сигналу через зігнутість, дефекти або інші причини. Вимір загасань зазвичай проводиться за допомогою спеціальних пристроїв, таких як оптичні тестери (OLTS- Optical Loss Test Set). На рис. 1.5 зображений саме такий тестер оптичного загасання, зі значеннями в дБ. Після проведення вимірювань отримані результати аналізуються для визначення ділянок з найбільшими втратами сигналу. Це дозволяє вжити заходів для їх усунення, наприклад, заміни пошкоджених кабелів або корекції зігнутості волокон. Крім того, регулярне вимірювання загасань дозволяє здійснювати моніторинг

стану мережі та своєчасно виявляти потенційні проблеми, що сприяє підтримці високої якості передачі даних.

Рисунок 1.5 - Тестер оптичного загасання (OLTS)

Спеціально для візуальної перевірки, що проводиться за допомогою пристроїв, які випромінюють світло у видимому діапазоні, використовуються спеціальний прилад, такий як VFL - візуальний визначник дефектів, який зазвичай випромінює червоне світло з довжиною хвилі 650 нм з потужністю від одиниць до десятків міліватт або ж від нуля до 16 дБ і може працювати як у імпульсному, так і у постійному режимі з частотою від 1 до 2 Гц. За допомогою нього можна виявити пошкодження, заломлення або обрив оптичного випромінювання, що виходить за межі оптичного провідника у оптичну оболонку. Зазвичай таким чином можна перевірити довжину провідника приблизно до 10-15 км. А у місці обриву або пошкодження оптичного волокна, червоне світіння буде видимим, не прикладаючи особливих зусиль. Приклад такого пристрою зображений на рис 1.6. Такий метод дозволяє швидко і ефективно виявляти дефекти у оптичних волокнах, що особливо корисно під час монтажу та обслуговування мережі. Зокрема, VFL може бути корисним для локалізації мікрозгинів, механічних ушкоджень, а також для перевірки з'єднань на правильність монтажу. Виявлення таких дефектів на ранніх

стадіях дозволяє запобігти серйозним проблемам у роботі мережі та зменшити час простою.

Рисунок 1.6 – Візуальний визначник місця пошкодження (VFL)

Також, одним із ключових інструментів для проведення вимірювань є оптичний рефлектометр OTDR, який використовується саме для виявлення дефектів у волоконних мережах та визначення відстані до неоднорідностей показника заломлення оптичного волокна. Джерелами зворотного відбиття можуть бути механічні роз'єми, тріщини, нерівності в волокні, а також вільні кінці волокон та інші перешкоди. Зображення оптичного рефлетометру з показчиком проходження тестового сигналу по волокну, показано на рис. 1.7.

Рисунок 1.7 – Оптичний рефлектометр (OTDR)

Його принцип роботи полягає у тому, що під час проведення діагностики оптичного волокна, оптичний рефлектометр надсилає в нього зондувальний імпульс - це світловий сигнал певної тривалості та амплітуди, основні параметри якого визначають максимальну довжину вимірюваної лінії та роздільну здатність.

Рефлектометр розпочинає облік часу, одночасно з відправленням зондувального імпульсу. Імпульс, що пройшов оптичне волокно, взаємодіє з різними перешкодами, такими як пошкодження або нерівності, і частина сигналу відбивається від них. Відбитий сигнал повертається у бік рефлектометра, де час його прибуття фіксується. На екрані рефлектометра формується рефлектограма - графічне зображення, яке показує зміни інтенсивності відбитого сигналу вздовж довжини волокна. Аналіз рефлектограми дозволяє ідентифікувати проблемні ділянки та оцінити їхній характер, що є критично важливим для технічного обслуговування та ремонту оптичних мереж.

Усі виявлені нерівності показника заломлення реєструються як "події" рефлектометром. Ці події поділяються на відбиваючі (викликані Френелевським відображенням) та невідбиваючі (викликані Релеєвським розсіюванням). Усе це сприяє підтримці стабільної та ефективної роботи телекомунікаційної інфраструктури.

На рис. 1.8 та 1.9 структурну схему оптичного рефлектометру та приклад такої типової рефлектограми відповідно.

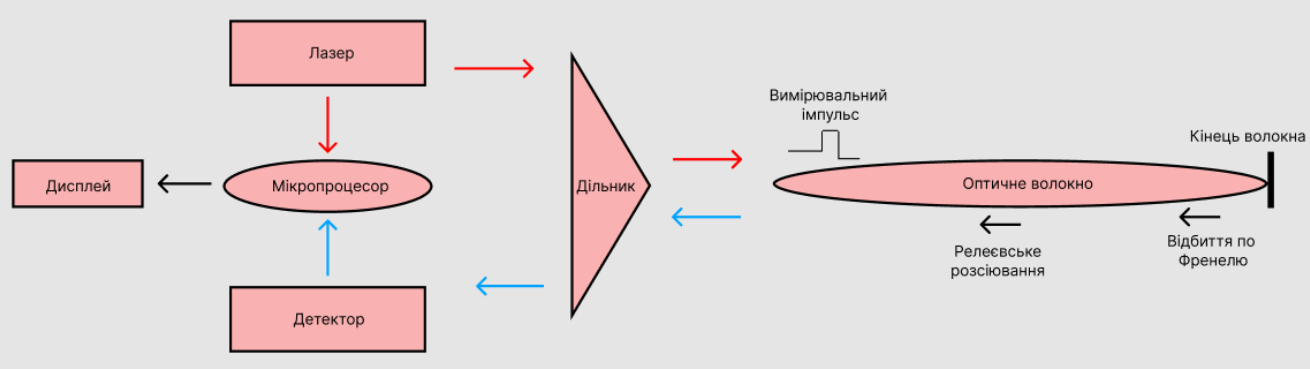


Рисунок 1.8 - Структурну схема оптичного рефлектометру

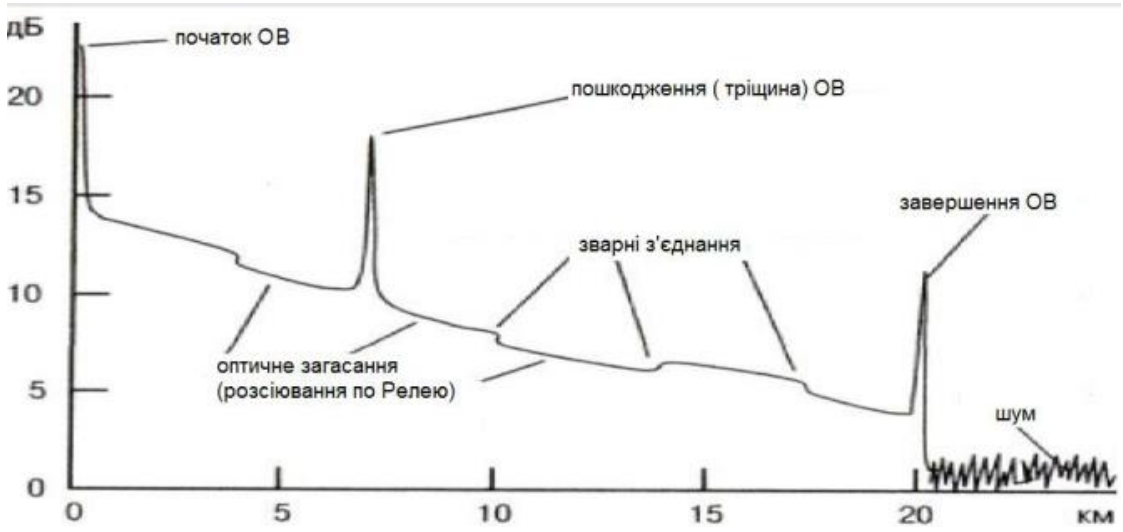


Рисунок 1.9 – Приклад типової рефлектограми

Одним з методів моніторингу, який є широко поширеним (хоча й не найбільш економічно-вигідним) методом такого моніторингу є використання системи ONMS – системи управління оптичною мережею. Ця система є універсальною і може використовуватись не лише для оптичних пасивних мереж доступу FTTx/PON, але й для магістральних, регіональних та міських оптичних мереж. Комплексне тестування пасивних мереж спрямоване на забезпечення безперервного моніторингу мережі під час її роботи, не втручаючись в її режим, тому і використовують ONMS.

Система OMNS, спеціально адаптована для пасивних мереж, що наведена на рис. 1.10, де показана проста схема моніторингу. Її особливість полягає у розміщенні перед кожним кінцевим абонентом спеціальних рефлекторів, які пропускають робочі довжини хвиль, у цьому випадку 1310 нм та 1490 нм та відбивають тестову хвилю 1650 нм, що вводиться в оптоволокно для зняття рефлектограми. Після кожного підключення ONU та встановлення перед ним рефлектора, відбувається запит в ЦУ на подачу тестового сигналу та зняття рефлектограми. Усі ці рефлектори є стандартизованими та пасивними, що значно спрощує процес моніторингу.

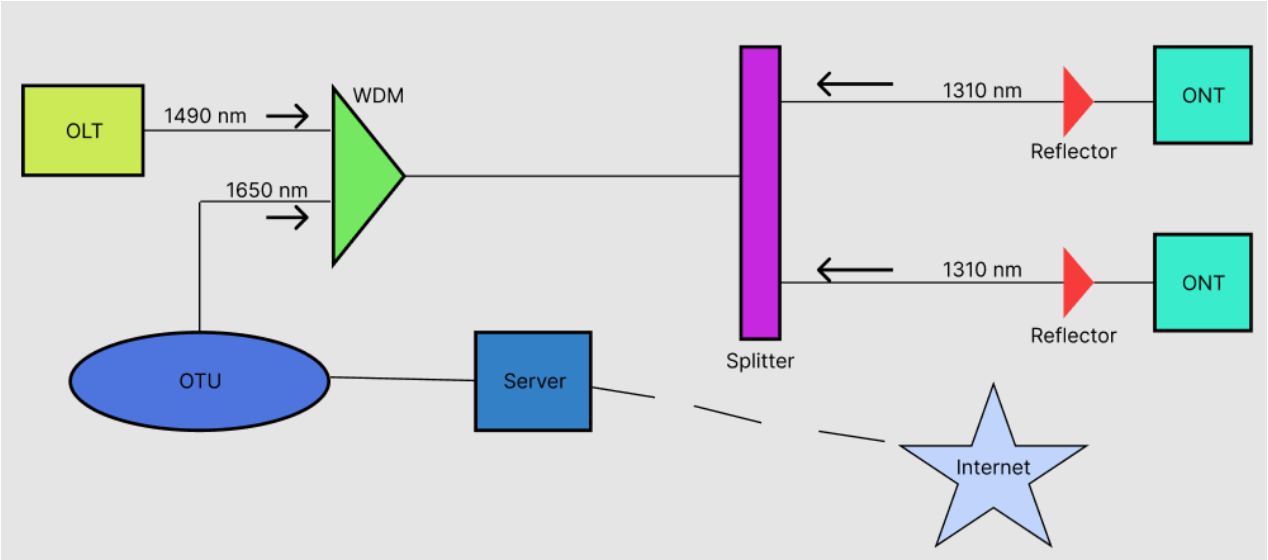


Рисунок 1.10 – Схема OMNS, видозмінена під пасивні мережі

Рефлектограма, яка формується, зберігається в базі даних та використовується як основа для подальших порівнянь. Щоб уникнути перекриття рефлектограм, для кожного рефлектора налаштовуються "піки", тобто проводиться зсув рефлектограми відносно одна одної, та зберігається загальне зображення в базі даних. В підсумку, виходить діаграма зображена на рис 1.11, де по положенню та потужності «піків» ми ідентифікуємо кожного споживача і можемо його моніторити, завдяки встановлених перед кожним ОНУ рефлекторів. Таке налаштування дозволяє створити комплексну картину стану мережі та забезпечити точний моніторинг кожного окремого абонента. У разі виникнення проблеми або збою в роботі конкретного ОНУ, аналіз рефлектограми допомагає швидко визначити місце і причину збою, що дозволяє оперативно усунути неполадку.

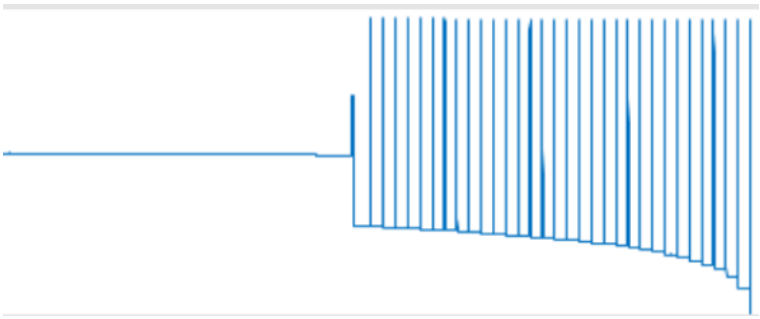


Рисунок 1.11 – Діаграма потужності “піків”

1.4. Система підтримки прийняття рішень (СППР)

Якщо мережа споруджена відкритим способом, де кабельний шлях встановлено на опорах і пошкодження можна візуально побачити, технологія описана вище виявляється складнішою та не обов'язковою. Зазвичай використовуються простіші методи, які можуть бути менш точними, але значно більш доступними з фінансової точки зору. Існує один з таких методів, що може бути використаним - система підтримки прийняття рішень (СППР), яка оперує ймовірнісними категоріями та використовує принцип "пінгування", Воно стало відомим у комп'ютерних мережах за допомогою утиліти Ping, команда якої надсилає повідомлення по протоколу ICMP для перевірки з'єднань в мережах на основі TCP/IP. Такий метод передбачає генерацію та відправлення спеціальних службових команд, у випадку з ICMP - ехо-запиту Echo-Request, та аналіз отриманого сигналу (ICMP Echo-Reply). На рис. 1.12 можна побачити детальну схему системи підтримки прийняття рішень, яка має проблему у вузлі 1-138.

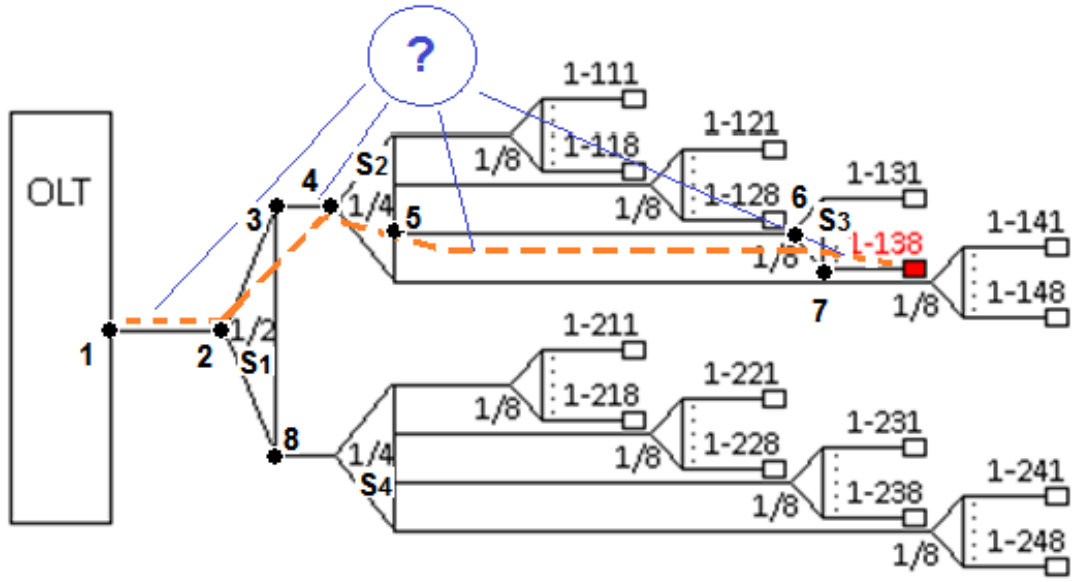


Рисунок 1.12 – Приклад схеми системи підтримки прийняття рішень

Важливо зауважити, що вузол, який перевіряється, повинен бути активним. Отже, у пасивних оптичних мережах, де такі повідомлення пройдуть через оптичні

розгалужувачі (сплітери), такий тип тестування має свої обмеження. Наприклад, при тестуванні в такий спосіб вузла в PON мережі та неприйнятті відповіді, може виникнути складність у визначенні місця пошкодження, але аналіз результатів тестування інших вузлів дерева фрагменту мережі, де знаходиться пошкоджений вузол, може нам прояснити ситуацію. Саме такий приклад дерева фрагменту мережі, з пошкодженням вузла, зображений на рис. 1.13.

Вище згаданий алгоритм є лише системою підтримки прийняття рішень (СППР), яка із значною ймовірністю вказує на можливі місця пошкоджень, а не повноцінною системою моніторингу.

До прикладу, хоча й ймовірність цього досить незначна, якщо відомо про несправність усіх вказаних вузлів від 1-111 до 1-248, існує можливість одночасного виходу з ладу спліттерів S4 і S2, або ділянок 3-4 та 8-9.

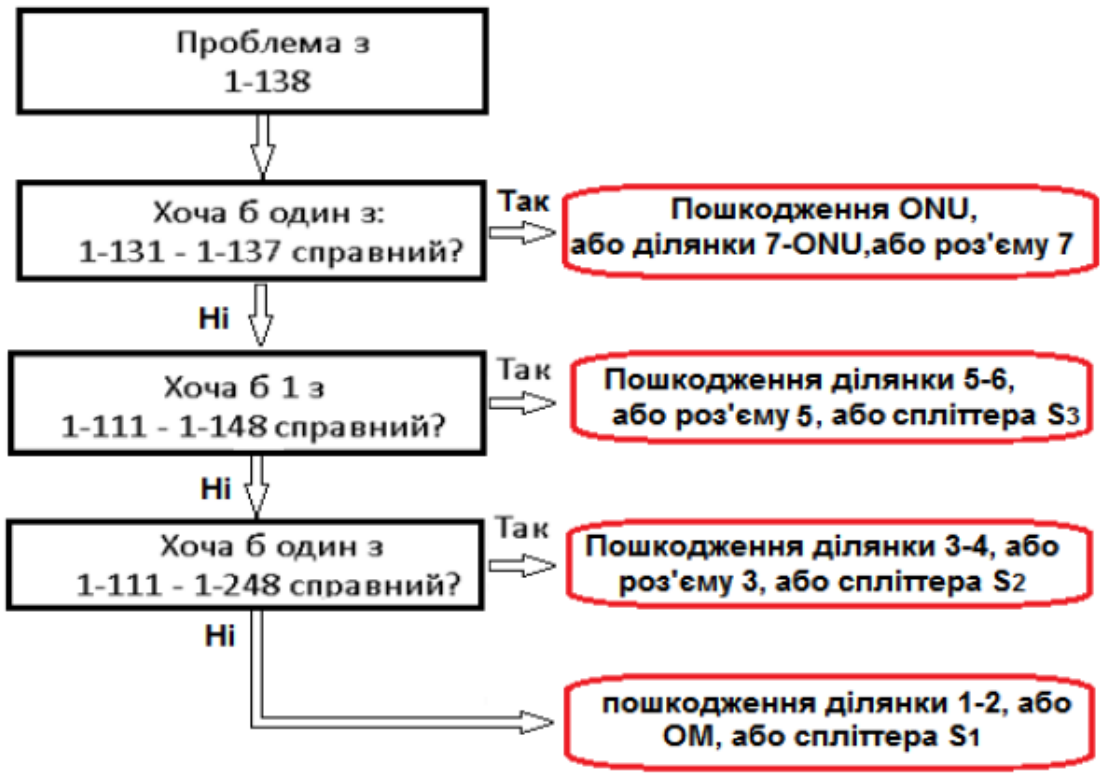


Рисунок 1.13 – Приклад алгоритму для дерева фрагменту мережі, з пошкодженням вузла

Таким чином, застосувавши зазначений алгоритм, ми можемо звузити зону пошуку до міжспліттерних ділянок та самих сплітерів та визначити місце

пошкодження. В кожному конкретному випадку потрібно оцінювати співвідношення ціни та отриманих результатів. У поєднанні з можливістю візуального контролю цілісності кабелів, що розташовані на опорах, ця СППР може бути досить простою та ефективною.

1.5. Висновки

Під час роботи над завданням було вивчено ключові аспекти кіберфізичних систем для моніторингу пасивних оптичних телекомунікаційних мереж. Ознайомлення з пасивними оптичними мережами, стандартами та типами PON (Passive Optical Network), а також засобами та методами моніторингу PON дозволило глибше розуміти принципи функціонування оптичних інфраструктур та їхню важливість для сучасних телекомунікаційних систем.

Було проведено аналіз про те, які переваги принесла система підтримки прийняття рішень (СППР) у плані ефективного моніторингу та управління оптичними мережами. Її універсальність та можливість застосування як на різних рівнях мережі, так і на різних типах оптичних інфраструктур, що робить її важливим інструментом для забезпечення надійності та ефективності роботи телекомунікаційних систем.

Вищезгадані можливості допоможуть розробляти та впроваджувати нові рішення для покращення якості моніторингу оптичних мереж і надалі.

2 ПРОЄКТУВАННЯ ПРОГРАМНО-ТЕХНІЧНОГО ЗАСОБУ

2.1. Аналіз вимог до системи моніторингу

Аналіз вимог є ключовим етапом у розробці кіберфізичної системи для моніторингу пасивних оптичних телекомунікаційних мереж. Він дозволяє визначити основні функціональні та нефункціональні вимоги, які формують основу для подальшого проектування та реалізації системи.

2.1.1. Функціональні вимоги

Функціональні вимоги визначають конкретні задачі та функції, які система має виконувати:

– виявлення та локалізація несправностей, система повинна точно виявляти та локалізувати несправності у мережі, такі як перерви волокон, затухання сигналу або пошкодження інфраструктури;

– моніторинг параметрів мережі, вимірювання фізичних параметрів мережі, включаючи оптичну потужність, довжину хвилі сигналу, та інші критичні індикатори, які впливають на якість з'єднання;

– прогнозування майбутніх несправностей, аналіз даних мережі для виявлення тенденцій і потенційних проблемних зон, дозволяючи запобігати виникненню несправностей перед їх фактичним виникненням;

– звітність та алерти, автоматизація процесу створення звітів про стан мережі та налаштування системи сповіщень для випадків, коли параметри мережі виходять за нормальні межі;

– інтеграція з іншими системами, забезпечення можливості інтеграції з іншими системами управління мережею, IT-інфраструктурою або зовнішніми сервісами для обміну даними та управління.

2.1.2. Нефункціональні вимоги

Нефункціональні вимоги відіграють критичну роль у проектуванні та розвитку кіберфізичної системи моніторингу, оскільки вони визначають параметри якості та оперативні характеристики системи. Ці вимоги можна класифікувати на вимоги до продукту, організаційні вимоги та вимоги до взаємодії з зовнішнім середовищем.

Вимоги до продукту стосуються якості та характеристик самої системи. Продуктивність - система повинна бути здатною обробляти великий обсяг даних в реальному часі з мінімальними затримками. Це включає швидку обробку сигналів з датчиків, аналіз даних і генерацію відповідних попереджень та звітів. Надійність - система має бути стійкою до помилок і збоїв, забезпечувати точність вимірювань та аналізу, і мати механізми для автоматичного відновлення після збоїв. Масштабованість - здатність системи адаптуватися до зростання та розширення мережі, забезпечуючи стабільну роботу незалежно від обсягу моніторингових даних. Безпека - забезпечення захисту даних та систем від несанкціонованого доступу, включаючи шифрування, аутентифікацію та контроль доступу.

Організаційні вимоги визначають стандарти, нормативні вимоги та політики, яким має відповідати система. Стандарти та нормативні акти, де система має бути у відповідності з національними та міжнародними стандартами в галузі телекомунікацій та кібербезпеки. Сумісність з іншими системами, де присутня необхідність інтеграції з іншими системами управління мережею, забезпечення сумісності на рівні програмного забезпечення та апаратних рішень. Політика управління та експлуатації, де є розробка чітких правил та процедур для управління системою, включаючи обслуговування, оновлення та підтримку.

Вимоги до взаємодії з зовнішнім середовищем стосуються того, як система взаємодіє з зовнішнім середовищем та користувачами: Екологічні вимоги, де система має бути спроектована з урахуванням впливу на навколишнє середовище, мінімізуючи споживання енергії та викиди відстоїв. Користувацький інтерфейс,

який має бути інтуїтивно зрозумілим, зручним для користувачів різного рівня кваліфікації, забезпечувати легкий доступ до необхідної інформації та управлінських функцій. Система також має відповідати законодавчим вимогам країни експлуатації, включаючи правила зберігання та обробки даних, приватність користувачів і вимоги щодо звітності.

Розробка кіберфізичної системи моніторингу, яка відповідає цим нефункціональним вимогам, забезпечить створення надійної, ефективної та безпечної системи, здатної адекватно реагувати на виклики сучасного телекомунікаційного середовища.

2.1.3. Аналітичні вимоги

Ці вимоги зосереджені на обробці та аналізі даних, які є життєво важливими для функціонування системи моніторингу:

– збір даних і ефективний механізм збору даних з різних частин мережі, що гарантує повноту та точність інформації;

– обробка даних та використання сучасних методів для обробки зібраних даних, включаючи фільтрацію, нормалізацію та агрегацію;

– аналіз даних, що є застосуванням алгоритмів машинного навчання та статистичних методів для аналізу даних, ідентифікації аномалій, та формування прогнозів;

– інтеграція даних показує здатність інтегрувати та корелювати дані з різних джерел для формування повної картини стану мережі.

2.1.4. Аналіз вимог до предметної галузі

Вимоги предметної галузі в контексті кіберфізичної системи моніторингу пасивних оптичних телекомунікаційних мереж стосуються специфікацій та стандартів, які регулюють оптичні телекомунікаційні мережі, а також функціональні та технічні вимоги, специфічні для даної області.

Технічні характеристики мережі: стандарти зв'язку: Кіберфізична система має відповідати міжнародним та національним стандартам у сфері оптичного зв'язку, таким як ITU-T G.652 для одномодового волокна або ITU-T G.657 для волокон із покращеними характеристиками гнучкості. Параметри якості сигналу, де система має вміти вимірювати і моніторити ключові показники якості сигналу, включаючи рівень оптичної потужності, втрати сигналу, SNR (відношення сигнал/шум), та дисперсію. Розуміння топології мережі, в якій система буде використовуватися, є критичним для ефективного моніторингу. Це включає знання про розподілні центри, кінцеві точки, маршрути волокон та місця з'єднань.

Функціональні вимоги предметної галузі:

– виявлення та локалізація несправностей: Система має забезпечувати виявлення та точну локалізацію місця несправностей у волоконно-оптичній мережі, таких як обриви волокна або точки затухання;

– моніторинг змін у мережі: Здатність слідкувати за динамічними змінами у параметрах мережі, як-от коливання в оптичній потужності, що можуть вказувати на потенційні проблеми або нестабільність у мережі;

– адаптація до різних типів мережевих архітектур: Система повинна бути гнучкою, щоб підтримувати різні архітектури оптичних мереж, включаючи точка-до-точки, зіркоподібні, кільцеві та інші топології.

Організаційні та регулятивні вимоги: дотримання норм та регуляцій, де система має відповідати всім відповідним національним та міжнародним нормативним актам, що стосуються оптичних телекомунікаційних мереж. Сумісність з індустріальними стандартами та відповідність стандартам якості та безпеки, таким як ISO/IEC стандарти для телекомунікаційних систем, є необхідною для забезпечення високого рівня якості та надійності.

Вимоги до взаємодії:

– інтерфейсування з існуючим обладнанням: система повинна мати можливість інтеграції з існуючим обладнанням мережі, включаючи оптичні комутатори, роутери та інше мережеве обладнання;

– підтримка стандартних протоколів зв'язку: Необхідність підтримки протоколів, таких як SNMP, NETCONF, або REST API для забезпечення сумісності з системами управління мережею.

Вимоги предметної галузі для кіберфізичної системи моніторингу пасивних оптичних телекомунікаційних мереж формують основу для глибокого розуміння потреб і викликів, з якими може зіткнутися система у реальних умовах експлуатації. Ці вимоги забезпечують цілісний підхід до проектування та розробки, враховуючи технічні, функціональні, організаційні та взаємодійні аспекти, необхідні для створення ефективної та надійної системи.

2.2. Принципи пінгування в кіберфізичних системах

Принцип пінгування в кіберфізичних системах, особливо у контексті моніторингу пасивних оптичних телекомунікаційних мереж, відіграє життєво важливу роль у визначенні стану мережі та виявленні можливих несправностей. Пінгування, у цьому випадку, не обмежується стандартним визначенням відправки пакетів ICMP для перевірки доступності хостів, але розширюється до комплексних методів діагностики стану оптичних мереж.

Концепція пінгування в оптичних мережах полягає у контексті оптичних мереж, пінгування може означати використання спеціалізованих тестових сигналів або квантів світла для оцінки інтегритету волоконних з'єднань та якості сигналу. Це включає вимірювання часу проходження, втрат сигналу, відбиття та інших параметрів, які можуть допомогти ідентифікувати зони зі зниженою продуктивністю або потенційними пошкодженнями.

Методологія пінгування складається з:

– відправки тестових сигналів - ініціювання процесу пінгування вимагає відправки контрольних сигналів або пакетів через оптичні волокна. Використання оптичних рефлектометрів, як-от OTDR (Optical Time-Domain Reflectometer), дозволяє визначити точки втрат, згинів або інших аномалій у волоконному каналі;

– аналізу відгуків, коли тестові сигнали досягають кінцевих точок або локацій з відбиттям, вони повертаються назад до джерела. Аналізуючи ці "відгуки", система може визначити час проходження сигналу та ідентифікувати потенційні несправності;

– ймовірнісного аналізу, що включає застосування ймовірнісних методів дозволяє оцінити ризик несправностей в певних ділянках мережі, засновуючись на історичних даних та статистичному аналізі отриманих метрик.

Технічні аспекти включають інструментарій пінгування - використання спеціалізованого обладнання для пінгування, такого як OTDR, дозволяє отримувати детальну інформацію про стан волоконних з'єднань. OTDR використовує принцип відбиття світла для визначення властивостей волокна на різних ділянках. Та автоматизація процесу, коли відбувається інтеграція пінгування як частини кіберфізичної системи вимагає автоматизації процесів для регулярного моніторингу та аналізу, з мінімальною потребою в ручному втручанні.

Інтеграція з СППР:

– підтримка прийняття рішень, звідки інформація, отримана від пінгування, служить основою для СППР, дозволяючи системі ефективно оцінювати стан мережі та рекомендувати дії для оптимізації або виправлення виявлених проблем;

– адаптивність та масштабованість, де система пінгування має бути адаптивною та масштабованою, щоб відповідати змінам у мережевій інфраструктурі, забезпечуючи точність та надійність моніторингу навіть у розширених або динамічно змінюваних мережах.

Інтеграція пінгування з СППР дозволяє автоматизувати процеси діагностики та управління, мінімізуючи людський фактор та скорочуючи час реагування на неполадки. Це значно підвищує ефективність роботи мережі, знижує ризик тривалих простоїв та покращує якість обслуговування кінцевих користувачів.

Дані від пінгування можуть використовуватися для створення прогнозів та моделей, що дозволяють передбачати можливі проблеми та вживати превентивних

заходів. Це включає виявлення тенденцій у зміні параметрів мережі, які можуть вказувати на потенційні загрози або необхідність оновлення обладнання.

Крім того, адаптивність системи означає, що вона може автоматично підлаштовуватися під нові конфігурації мережі, такі як додавання нових вузлів або зміни у топології. Це забезпечує постійну актуальність даних моніторингу та дозволяє СППР працювати з максимальною ефективністю.

На рис. 2.1 зображене успішне пінгування комп'ютера до серверу, який знаходиться за IP адресом – 192.168.1.100 в Cisco Packet Tracer.

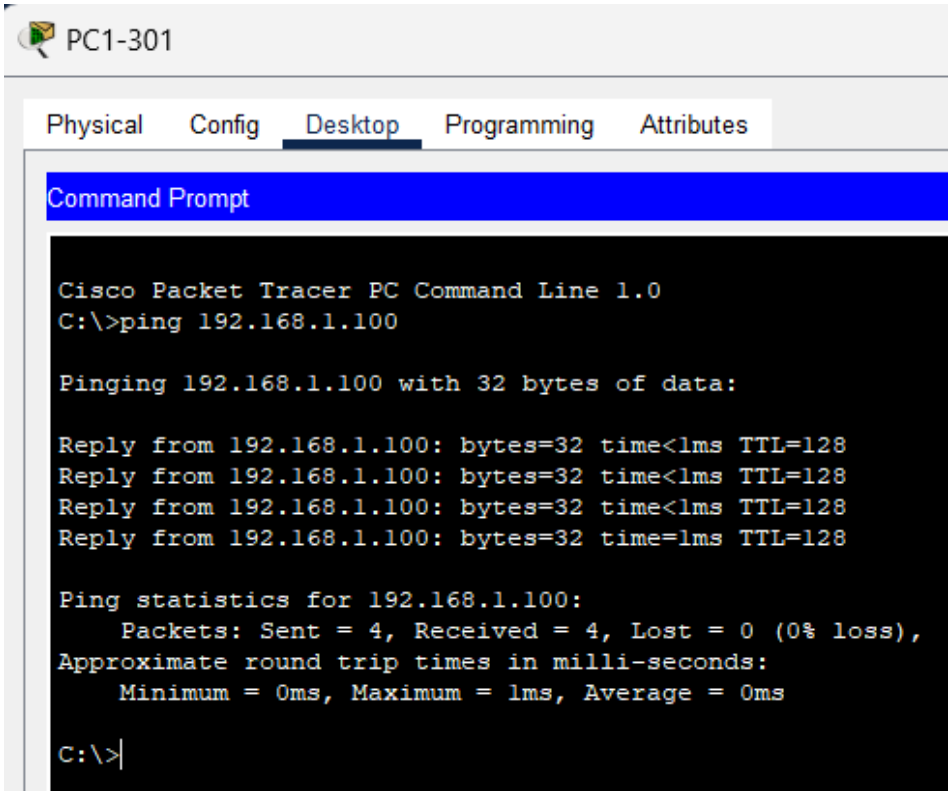


Рисунок 2.1 – Пінгування серверу з комп'ютера в Cisco Packet Tracer

2.3. Компоненти для організації СППР пошуку несправностей.

Cisco Packet Tracer – це інтерактивна потужна програма для моделювання мережі, яка дозволяє експериментувати з мережевими поведінками. В контексті створення системи підтримки прийняття рішень (СППР) для діагностики в пасивних оптичних мережах, Cisco Packet Tracer використовується для візуалізації

та тестування компонентів мережі, що дозволяє ідентифікувати і аналізувати потенційні несправності. На рис.2.2 зображено головне меню Cisco Packet Tracer.

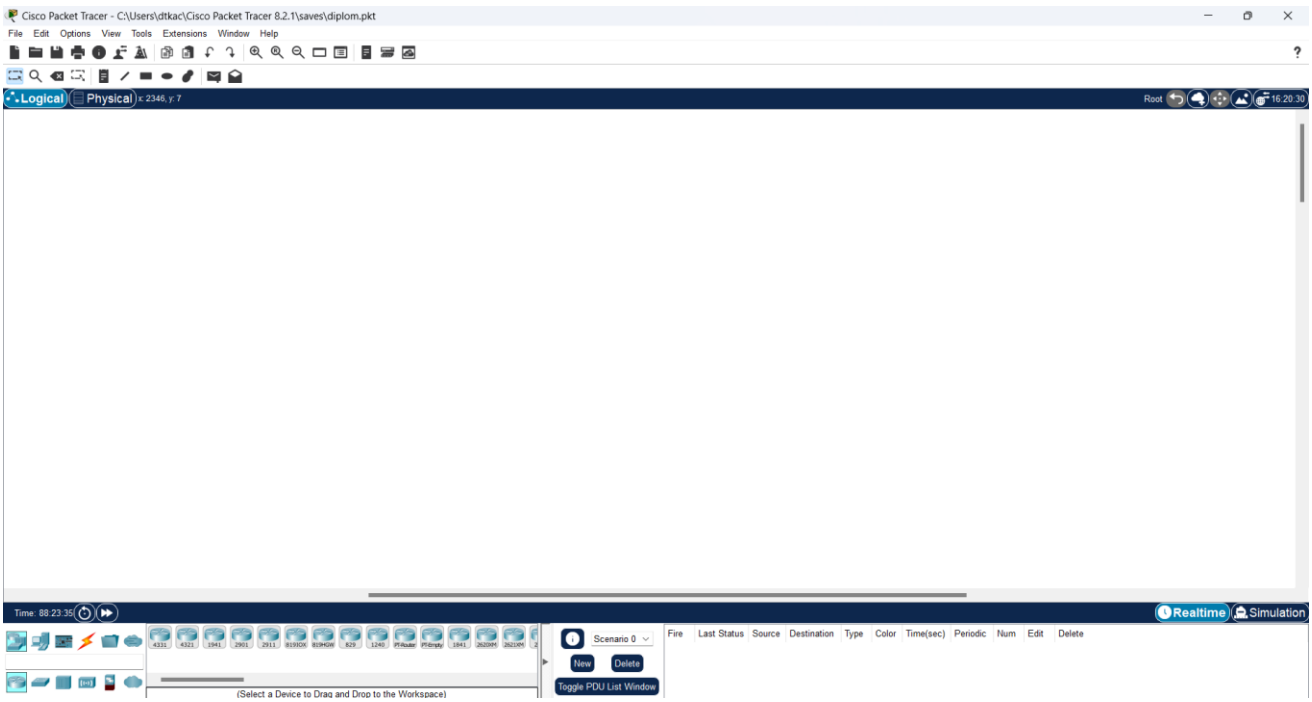


Рисунок 2.2 – Головне меню Cisco Packet Tracer

Cisco Packet Tracer пропонує широкий асортимент компонентів, що можуть бути використані для моделювання різних аспектів мережі. Нижче описані усі необхідні компоненти для роботи у CPR.

Хаби, які були використані, як звичайні спліттери. Всього їх на проекті використано у кількості 6 одиниць. Для використання сплітера у проекті було обрано PT-Hub. Меню з обиранням хабів зображено на рис. 2.3.

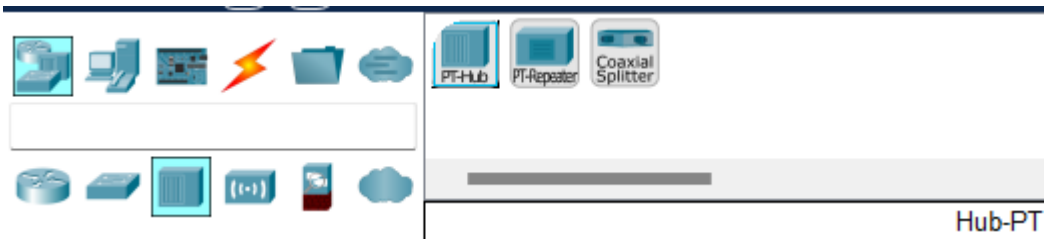


Рисунок 2.3 – Меню з обиранням хабів у Cisco Packet Tracer

Також обов’язково потрібно налаштувати ці хаби. Відкривіємо меню кожного з хабів та на рис. 2.4 та 2.5, відповідно, можна побачити зображення хабу з 6 входами LINK, які потрібно розширити до 10 входів, та на іншому рисунку, представлений готовий варіант. Для цього потрібно спочатку відключити хаб від живлення, а потім додати входи PT-REPEATER-NM-1CFE і заново підключити до мережі.

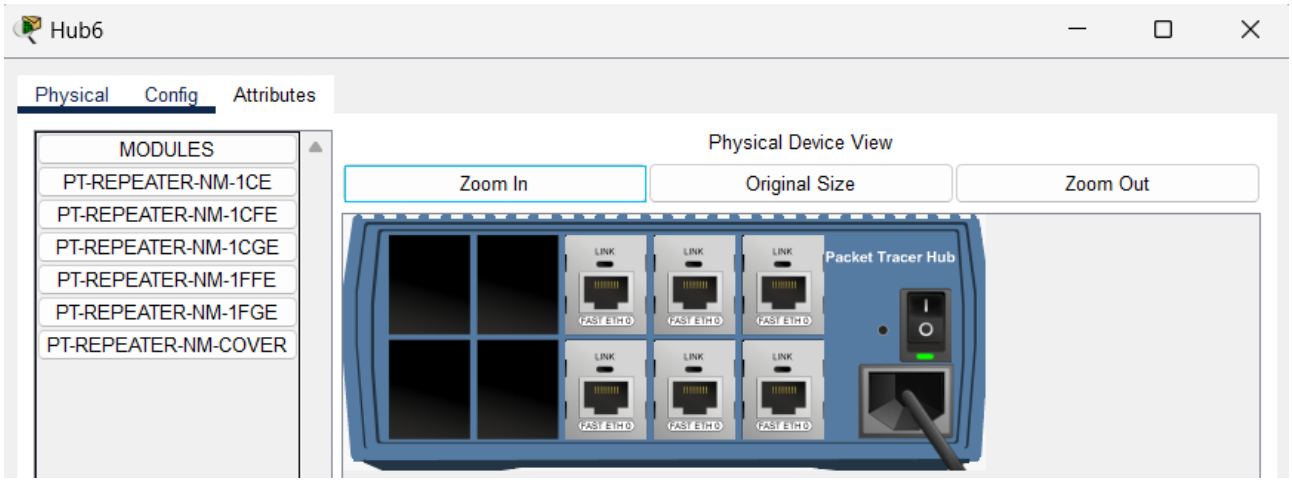


Рисунок 2.4 – Налаштування хабу до змін

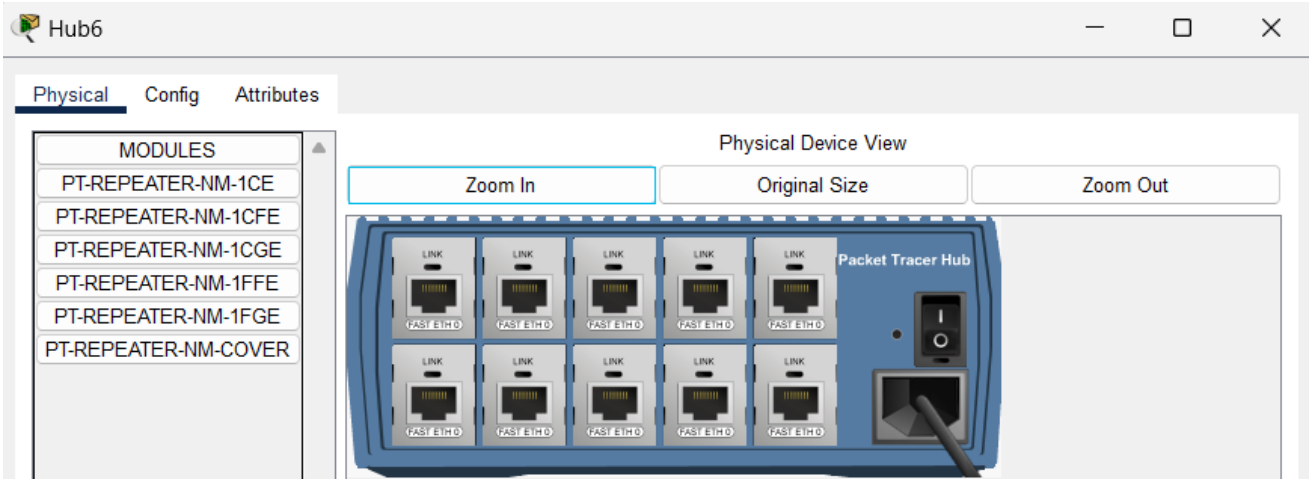


Рисунок 2.5 – Налаштування хабу після змін

Кінцеві пристрої (ендпоінти): комп'ютери, сервери та інші пристрої, що використовуються для генерації та прийому мережевого трафіку.

У даному проекті будуть присутні 32 кінцеві пристрої – комп’ютери, так як була обрана локація сільської місцевості. Передається уся інформація на сервер, який і обробляє дані пінгування цих комп’ютерів. На рис. 2.6 присутнє зображення меню кінцевих пристроїв у Cisco Packet Tracer.

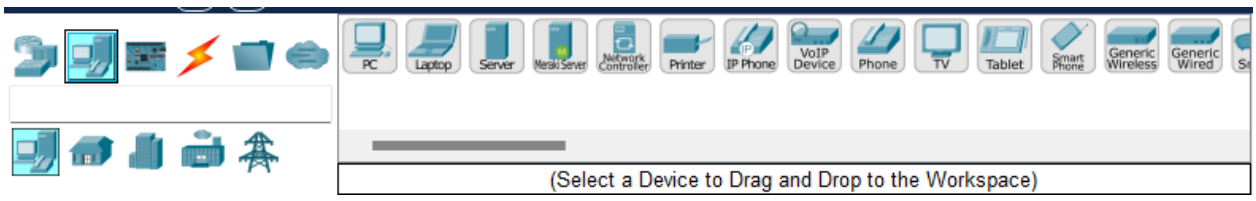


Рисунок 2.6 – Меню кінцевих пристроїв у Cisco Packet Tracer

З’єднання: різні типи з'єднань, включаючи мідні кабелі, волоконно-оптичні лінії та бездротові з'єднання, які використовуються для створення мережевої інфраструктури.

Для здійснення цієї задачі обираємо звичайний Cooper Straight-Through з’єднання та Cooper Cross-Over. На рис. 2.7 намальовано зображення меню можливих з’єднань у Cisco Packet Tracer.

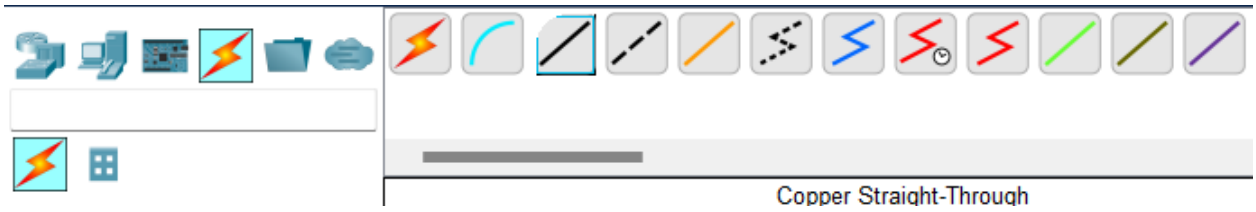


Рисунок 2.7 – Меню з’єднань у Cisco Packet Tracer

Процес створення мережі у Cisco Packet Tracer включає наступні етапи. Планування мережі: визначення структури мережі, включаючи кількість і типи вузлів, схему адресації та маршрутизації. Розміщення компонентів: додавання хабів (сплітерів), серверу та інших пристроїв на робочу область Packet Tracer. Налаштування пристроїв: конфігурація пристроїв з урахуванням необхідних налаштувань IP-адрес, маршрутизаційних протоколів та інтерфейсів.

Тестування з'єднань: використання інструментів Packet Tracer для перевірки з'єднань і виявлення помилок у конфігурації. У таблиці 2.1 якраз представлено адреси кінцевих девайсів у Cisco Packet Tracer. Відповідно у таблиці 2.2 проставлені адреси з’єднань сплітерів між собою.

Таблиця 2.1 – Таблиця адрес кінцевих девайсів у Cisco Packet Tracer

Кінцевий девайс	Підключений до спліттера	IP адреса	Інтерфейс підключення
PC1-301	Splitter3	192.168.1.1	Fa0/0
PC1-302	Splitter3	192.168.1.2	Fa0/1
PC1-303	Splitter3	192.168.1.3	Fa0/2
PC1-304	Splitter3	192.168.1.4	Fa0/3
PC1-305	Splitter3	192.168.1.5	Fa0/4
PC1-306	Splitter3	192.168.1.6	Fa0/5
PC1-307	Splitter3	192.168.1.7	Fa0/6
PC1-308	Splitter3	192.168.1.8	Fa0/7
PC1-311	Splitter4	192.168.2.1	Fa0/0
PC1-312	Splitter4	192.168.2.2	Fa0/1
PC1-313	Splitter4	192.168.2.3	Fa0/2
PC1-314	Splitter4	192.168.2.4	Fa0/3
PC1-315	Splitter4	192.168.2.5	Fa0/4
PC1-316	Splitter4	192.168.2.6	Fa0/5
PC1-317	Splitter4	192.168.2.7	Fa0/6
PC1-318	Splitter4	192.168.2.8	Fa0/7
PC1-321	Splitter5	192.168.3.1	Fa0/0
PC1-322	Splitter5	192.168.3.2	Fa0/1
PC1-323	Splitter5	192.168.3.3	Fa0/2

Кінець таблиці 2.1 – Таблиця адрес кінцевих девайсів у Cisco Packet Tracer

PC1-324	Splitter5	192.168.3.4	Fa0/3
PC1-325	Splitter5	192.168.3.5	Fa0/4
PC1-326	Splitter5	192.168.3.6	Fa0/5
PC1-327	Splitter5	192.168.3.7	Fa0/6
PC1-328	Splitter5	192.168.3.8	Fa0/7
PC1-331	Splitter6	192.168.4.1	Fa0/0
PC1-332	Splitter6	192.168.4.2	Fa0/1
PC1-333	Splitter6	192.168.4.3	Fa0/2
PC1-334	Splitter6	192.168.4.4	Fa0/3
PC1-335	Splitter6	192.168.4.5	Fa0/4
PC1-336	Splitter6	192.168.4.6	Fa0/5
PC1-337	Splitter6	192.168.4.7	Fa0/6
PC1-338	Splitter6	192.168.4.8	Fa0/7
Server0	Splitter1	192.168.1.100	Fa0/1

Таблиця 2.2 – Таблиця адрес з’єднань сплітерів у Cisco Packet Tracer

Початковий сплітер	Кінцевий сплітер	Інтерфейс підключення
Splitter1	Splitter2	Fa0/0
Splitter2	Splitter3	Fa0/0
Splitter2	Splitter4	Fa0/1
Splitter2	Splitter5	Fa0/2
Splitter2	Splitter6	Fa0/3

На рис. 2.8 представлена повна логічна топологія схеми мережі в ідеальному стані, усі 32 кінцевих девайси, під’єднані до мережі.

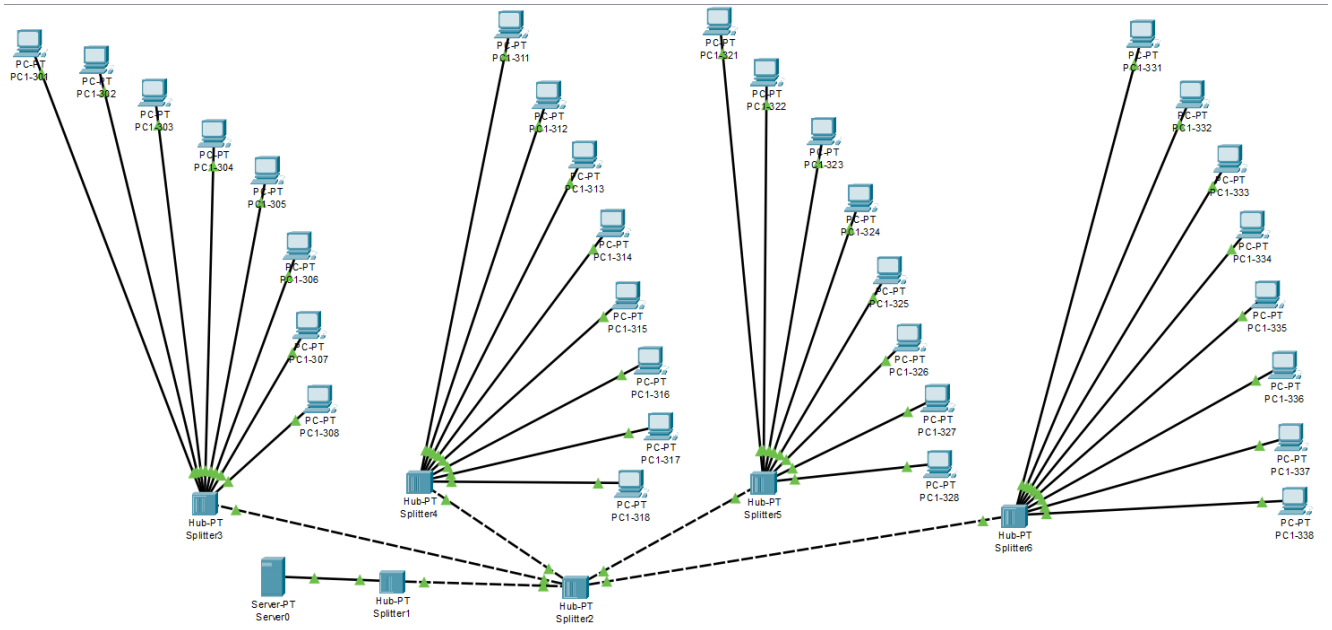


Рисунок 2.8 – Логічна топологія схеми мережі в ідеальному стані

Ефективність компонентів мережі і стратегій виявлення несправностей можна оцінити за допомогою інтегрованих засобів Cisco Packet Tracer - симуляція трафіку: генерація мережевого трафіку для визначення продуктивності мережевих пристроїв і зв'язків. Логування подій: запис подій у мережі, що дозволяє виявляти аномалії і потенційні точки збоїв. Статистичний аналіз: використання статистичних звітів для оцінки відсотка втрат пакетів, затримок та інших критичних параметрів мережі.

Також на рис. 2.9 показано фізичну топологію схеми мережі, на якій знаходяться 32 приватних будинки у сільській місцевості, по вісім у чотири ряди, з розділенням сплітерами.

Для кожного з будинків можна провести індивідуальний аналіз продуктивності мережі та визначити потенційні місця збоїв або втрат сигналу. Використання Cisco Packet Tracer дозволяє симулювати реальні умови експлуатації мережі, що допомагає ідентифікувати та усунути проблеми на етапі проектування.

Інтеграція цих методів у процес управління мережею забезпечує високу надійність і ефективність телекомунікаційної інфраструктури, дозволяючи швидко

реагувати на будь-які неполадки та підтримувати стабільний рівень обслуговування користувачів.

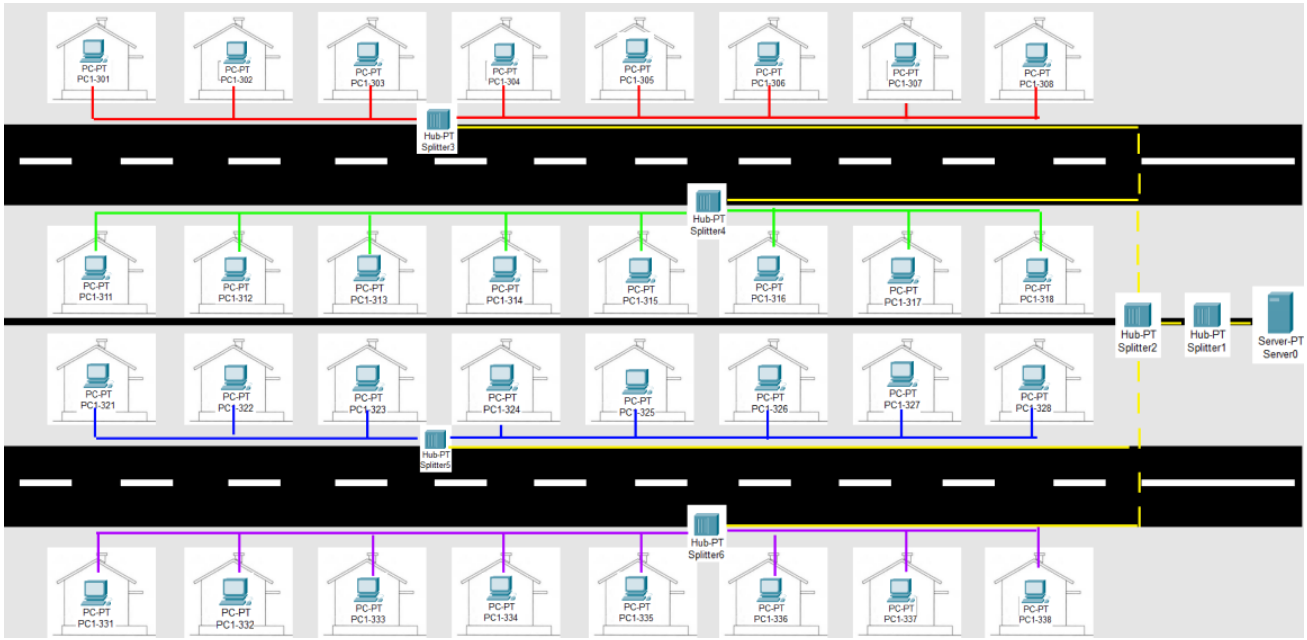


Рисунок 2.9 – Фізична топологія схеми мережі

2.4. Complex PDU як сервіс для системи підтримки прийняття рішень

Complex PDU (Protocol Data Unit) у Cisco Packet Tracer є потужним інструментом для тестування та демонстрації, як мережеві пристрої реагують на різні умови мережі та як вони логують події.

Створення Complex PDU:

– сценарій може бути створений для симуляції мережевих подій, таких як високий трафік, зміни в топології мережі або відмови пристроїв;

– Complex PDU дозволяє імітувати мережевий трафік і спостерігати за реакцією мережевих пристроїв, включаючи генерацію повідомлень від пінгувань.

В цілому, процес створення нічим не відрізняється від Simple PDU, але дозволяє виконувати більш гнучкі налаштування. Через відповідне меню, яке з'являється коли вибирається відправник, можна вказати адресу, визначити порт, порядок виконання, налаштувати періодичність повторного відправлення, а також

обрати через який протокол буде виконуватись перевірка. Відповідне меню налаштувань виглядає наступним чином, його можна побачити на рис. 2.10.

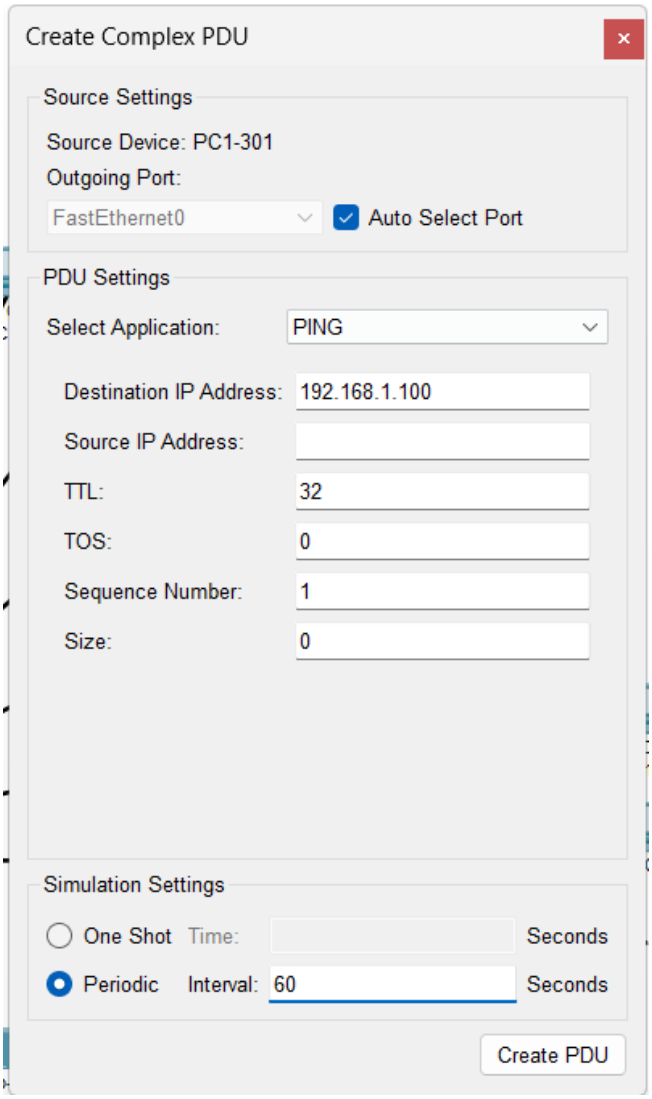


Рис. 2.10 – Налаштування для Complex PDU

У налаштуваннях Complex PDU обирається Destination IP Address, що значить кінцеву IP адресу для відправки даних на сервер. Вказується IP адреса серверу, в даному випадку 192.168.1.100.

Далі вказується Sequence Number – номер черги, ставляться числа від 1 до 32 для всіх кінцевих пристроїв. І в кінці обирається налаштування симуляції. Вибирається періодична система, яка дозволить відправляти повідомлення про пінгування на сервер, один раз на 60 секунд.

2.5. Застосування засобів виявлення несправностей і їх реалізація на Java

Сучасні системи моніторингу мереж вимагають ефективних інструментів для виявлення та аналізу несправностей. Використання алгоритмів кореляції дозволяє значно покращити точність та швидкість реакції на інциденти в мережі. Цей розділ описує розробку та імплементацію таких алгоритмів на Java, а також методи їх тестування та оптимізації.

Алгоритми кореляції аналізують зібрані дані для виявлення залежностей та зразків поведінки, які можуть вказувати на потенційні проблеми в мережі. Основні кроки розробки включають:

– визначення даних для аналізу, які будуть зібрані з мережевих пристроїв (логи, метрики процесора, пам'яті, використання мережі);

– вибір методів кореляції, для аналізу даних, таких як часові ряди, кластерний аналіз або машинне навчання;

– розробка та створення математичної моделі, що дозволяє ідентифікувати зв'язки між різними подіями в мережі.

Apache NetBeans - це відкрите середовище розробки (IDE), яке підтримує розробку додатків на багатьох мовах програмування, включаючи Java. NetBeans особливо відомий своєю підтримкою розробки Java EE, Java ME, і стандартних додатків Java, а також за можливості розробки додатків з графічним інтерфейсом користувача через Swing і JavaFX.

Основні можливості NetBeans:

– інтегроване робоче середовище, що надає всі необхідні інструменти для розробки, від редактора коду з підсвічуванням синтаксису і автодоповненням до дебагера і профайлера;

– підтримка Maven і Ant, підтримує стандартні інструменти управління проектами і залежностями в Java, що дозволяє легко імпортувати проекти, створені з використанням цих інструментів;

– вбудована підтримка Git, присутня можливість керування версіями відбувається прямо з IDE, що дозволяє виконувати коміти, пуші, пули і перегляд історії змін без використання зовнішніх програм;

– плагіни: широкий спектр доступних плагінів для розширення функціональності IDE, зокрема для підтримки нових мов, фреймворків або інструментів розробки;

– розробка графічного інтерфейсу: графічні редактори для Swing і JavaFX, які дозволяють "перетягувати" компоненти інтерфейсу, спрощуючи процес створення GUI.

Необхідні елементи для розробки СППР: Java Development Kit (JDK) - остання версія JDK повинна бути встановлена та налаштована у NetBeans для компіляції і запуску Java-додатків. У базі даних, якщо СППР потребує збереження або аналізу даних, потрібно налаштувати з'єднання з базою даних, такою як MySQL, PostgreSQL чи вбудована база даних H2. Веб-сервер, потрібен для розробки веб-орієнтованих СППР, такий як Apache Tomcat або GlassFish, обидва з яких легко інтегруються з NetBeans. Бібліотеки і фреймворки, треба залежно від вимог проекту, можуть бути необхідні додаткові бібліотеки, такі як JUnit для тестування, Log4j для логування, Spring Framework для розширеного управління компонентами і транзакціями.

Також існують деякі додаткові компоненти, які складаються з інструментами для аналізу та моніторингу, щоб задля ефективної роботи СППР, можуть бути потрібні інструменти для аналізу та моніторингу продуктивності, такі як JVisualVM або Apache JMeter. Вони допоможуть оцінити ефективність додатка та виявити можливі проблеми. Також існує система контролю версій. Для управління кодом проекту необхідно використовувати систему контролю версій, таку як Git. Це дозволить ефективно координувати роботу команди розробників та зберігати історію змін у коді.

Інтеграція всіх цих елементів дозволить створити потужну та надійну систему підтримки прийняття рішень, яка зможе ефективно вирішувати завдання

моніторингу та управління телекомунікаційними мережами. Всі компоненти повинні бути налаштовані та протестовані для забезпечення безперебійної роботи СППР та досягнення високої якості обслуговування кінцевих користувачів.

Згідно опису, представленим вище, на рис. 2.11 зображено головний екран Apache NetBeans.

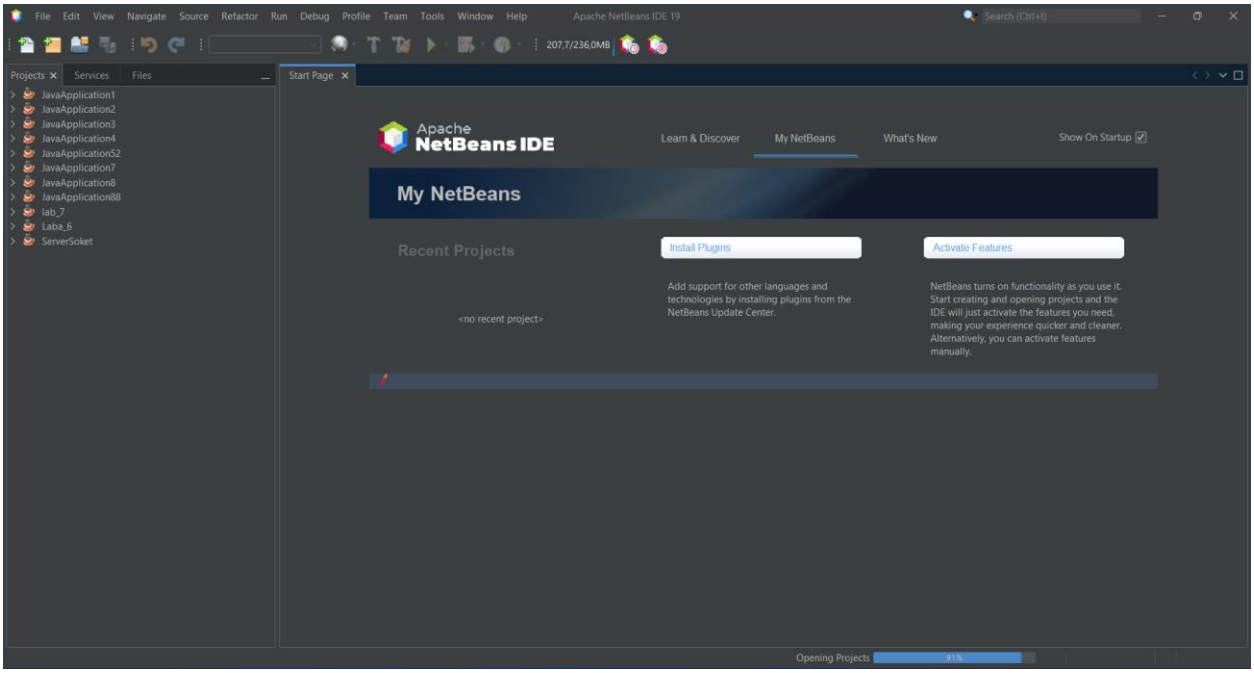


Рисунок 2.11 - Головний екран Apache NetBeans

Процес налаштування проекту - створення проекту: відкривання NetBeans і створення нового проекту, вибравши "Java" або "Java Web" в залежності від типу проекту. Конфігурація проекту, налаштування шляхів до використовуваних бібліотек, вказування версії JDK та налаштування параметрів збірки. Розробка додатку: використовування редактору NetBeans для написання та налагодження коду. Використовування вбудованих інструментів для проектування інтерфейсу користувача, якщо це необхідно. Тестування та розгортання: виконування тестування за допомогою інструментів, інтегрованих у NetBeans, та налаштовування і розгортання додатку на вибраному сервері або платформі.

Для реалізації даної системи підтримки прийняття рішень (СППР) на Java, потрібно додати різні потрібні компоненти. В загальному потрібні такі компоненти як:

– назва комп'ютера (наприклад 1-331);

– IP адреса для кожного кінцевого пристрою;

– дата та час останньої перевірки пінгування;

– Checkbox для перевірки пінгування обраних після натиснення відповідної кнопки перевірки з'єдняння та видачі MessageBox, про один з результатів або наслідків;

– CheckBox для відключення від мережі (неможливості пінгування), після натиснення відповідної кнопки;

– CheckBox для підключення до мережі (відновлення можливості пінгування) після натиснення відповідної кнопки.

На рис. 2.12 зображено повний вигляд застосунку системи підтримки прийняття рішень, одразу після запуску.

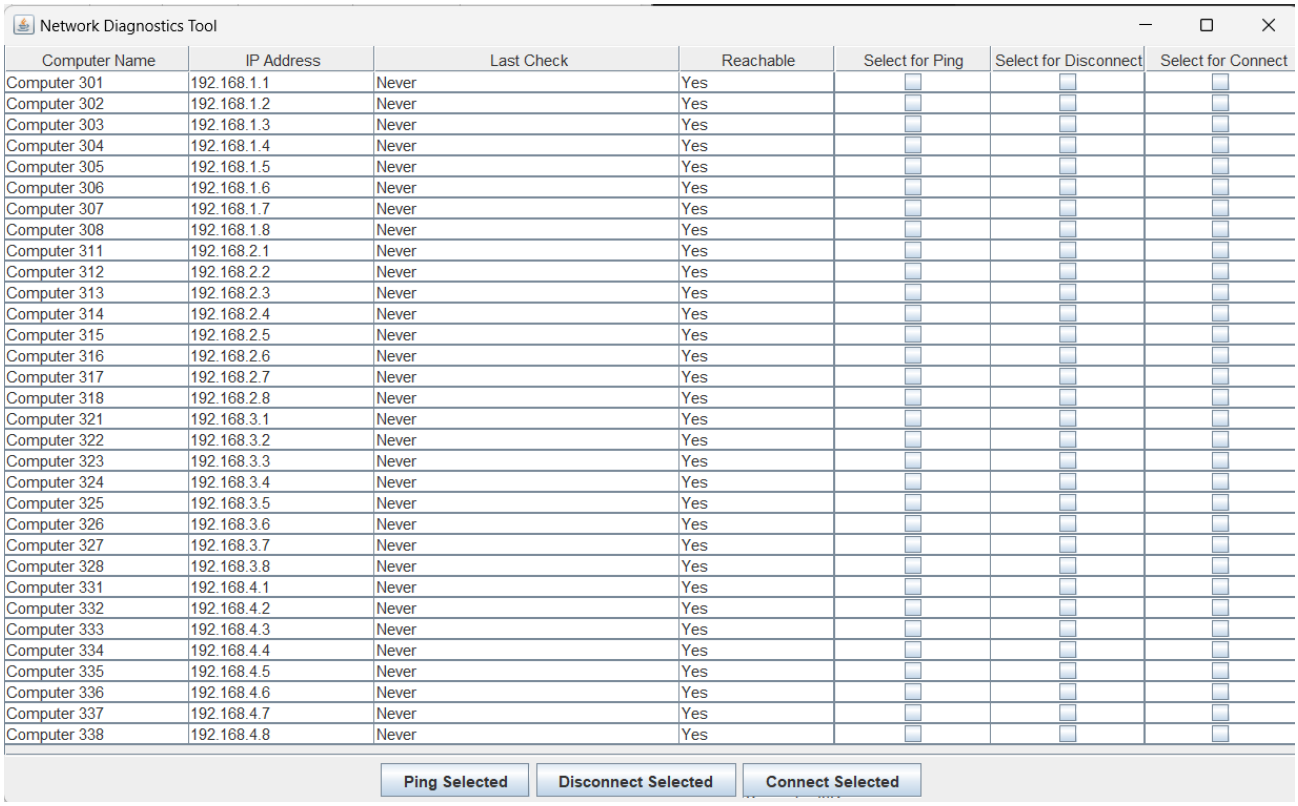


Рисунок 2.12 – Застосунок для системи підтримки прийняття рішень

Загалом програмно-апартний засіб спеціально виконує функції відключення чи під’єднання до мережі з можливістю провести пінгування для того, щоб використовувати різні сценарії роботи пошуку несправностей для системи підтримки прийняття рішень.

2.6. Висновки

Для успішного проектування та реалізації кіберфізичної системи моніторингу пасивних оптичних телекомунікаційних мереж необхідно глибоке розуміння функціональних та нефункціональних вимог. Це включає в себе забезпечення надійності, продуктивності, безпеки та здатності системи до масштабування. Аналітичні вимоги повинні адресувати способи збору, обробки та аналізу даних для забезпечення ефективного моніторингу та управління мережею. Ретельне визначення та аналіз цих вимог є фундаментальним для створення системи, здатної задовольняти потреби сучасних оптичних телекомунікаційних мереж.

Принцип пінгування в кіберфізичних системах для моніторингу пасивних оптичних мереж є фундаментальним для точного визначення стану мережі та ефективного управління нею. Інтеграція пінгування з системою підтримки прийняття рішень дозволяє створити комплексну платформу для аналізу, моніторингу та оптимізації оптичних телекомунікаційних мереж.

Cisco Packet Tracer є ефективним інструментом для створення і тестування мережі, який може використовуватися для розробки СППР пошуку несправностей. Використання цього інструменту дозволяє не тільки візуалізувати архітектуру мережі, але і ефективно аналізувати і оптимізувати рішення, пов'язані з управлінням мережевими ресурсами.

Інтеграція сервісу Complex PDU як частини системи моніторингу та підтримки прийняття рішень у Cisco Packet Tracer надає важливі інструменти для централізованого збору даних, які критично важливі для ефективного управління

та діагностики мережі. Ця система дозволяє не тільки відслідковувати поточні події в мережі, але й аналізувати тенденції та планувати вдосконалення для підвищення загальної ефективності та надійності мережевої інфраструктури.

Розробка та імплементація системи виявлення несправностей на основі алгоритмів кореляції в Java дозволяє створити міцний інструмент для аналізу та прогнозування стану мережі. Така система стає невід'ємною частиною мережевої інфраструктури, сприяючи оптимізації роботи та підвищенню її надійності.

Розширення функціональності та інтеграція з іншими системами створює комплексне рішення для управління та оптимізації мережевої інфраструктури. Навчання персоналу та постійне вдосконалення системи гарантує її ефективне використання та адаптацію до нових викликів.

3 ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ПРОГРАМНО-ТЕХНІЧНОГО ЗАСОБУ

3.1. Алгоритм виконання СППР на основі отриманих результатів

Система підтримки прийняття рішень (СППР) у контексті моніторингу пасивних оптичних телекомунікаційних мереж є комплексним рішенням, що дозволяє ефективно аналізувати стан мережі на основі даних, отриманих від різних вузлів та компонентів системи. Розробка алгоритму виконання СППР у Java вимагає глибокого розуміння мережевої архітектури, мережевих протоколів та методів аналізу даних. Використання сучасних технологій аналізу даних та автоматизації процесів дозволяє значно підвищити якість обслуговування користувачів і знизити ризики простоїв та збоїв у роботі мережі. Інтеграція з іншими системами та постійне вдосконалення функціональних можливостей СППР забезпечують її адаптивність до змін та нових викликів у сфері телекомунікацій. Алгоритм СППР базується на аналізі зібраних даних, кореляції цих даних між собою та визначенні оптимальних рішень для вирішення можливих проблем. Ключовими етапами алгоритму є:

– збір даних і використання мережевих команд та інструментів для збору статистики та стану вузлів;

– обробка та аналіз даних з метою виявлення аномалій та потенційних несправностей;

– кореляція даних та зв'язування даних з різних джерел для створення повної картини стану мережі;

– генерація рішень і визначення кроків, які необхідно вжити для виправлення виявлених проблем.

На рис. 3.1 можна побачити детальну схему системи підтримки прийняття рішень, яка має проблему у вузлі 1-331. Відповідно на рис. 3.2 показано алгоритм роботи СППР у даному проекті.

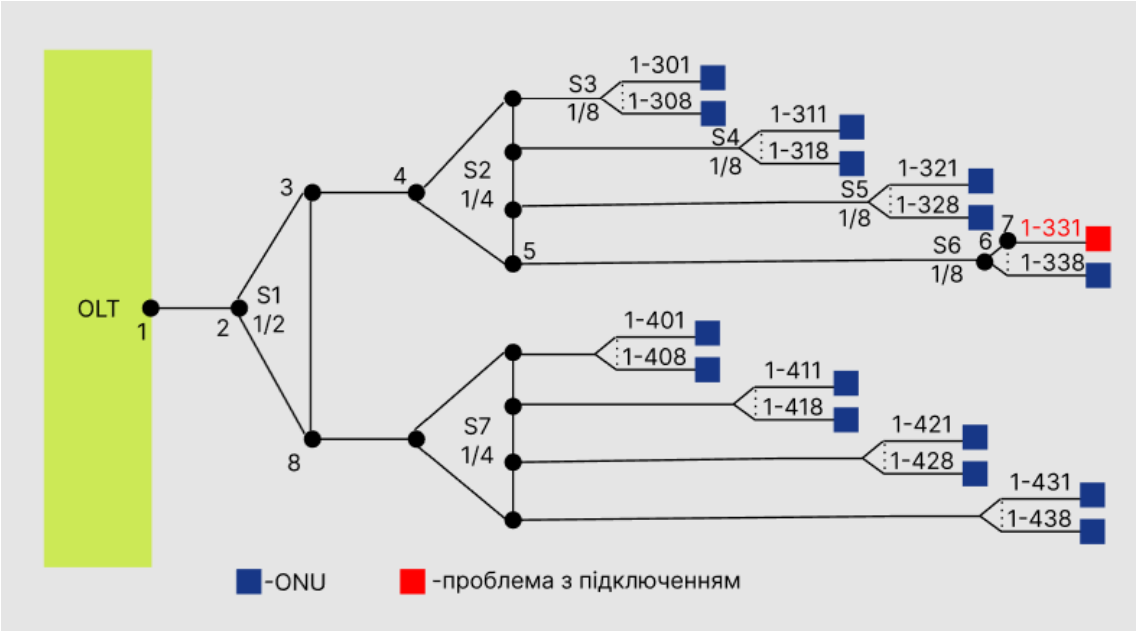


Рисунок 3.1 - Схема системи підтримки прийняття рішень, яка має проблему у вузлі 1-331

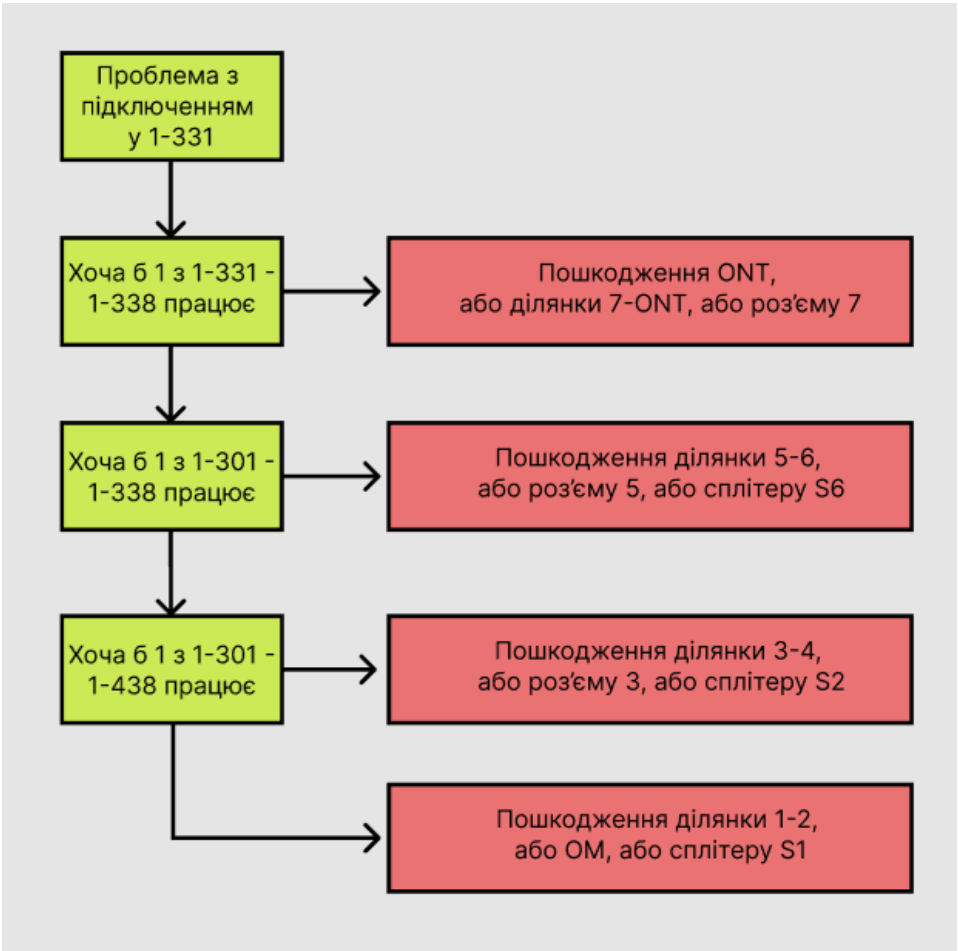


Рисунок 3.2 – Алгоритм роботи СППР

Алгоритм роботи СППР передбачає дерево усього фрагменту мережі, у даному випадку від 1-301 до 1-438, де виникла проблема з кінцевим пристроєм 1-331. Повний алгоритм дій при такій проблемі, підключення вузла 1-331:

а) чи працює хоча б один із вузлів від 1-331 до 1-338?

1) якщо ТАК, то можливе виникнення пошкодження ONT, або ділянки 7-ONT, або роз'єму 7;

2) якщо НІ, то переходимо до наступної дії алгоритму;

б) Чи працює хоча б один із вузлів від 1-301 до 1-338?

1) якщо ТАК, то можливе виникнення пошкодження ділянки 5-6, або сплітеру S6;

2) якщо НІ, то переходимо до наступної дії алгоритму;

в) Чи працює хоча б один із вузлів від 1-301 до 1-438?

1) якщо ТАК, то можливе виникнення пошкодження ділянки 3-4, або сплітеру S2;

2) якщо НІ, то можливе пошкодження ділянки 1-2, або ОМ, або сплітеру S1.

Ймовірність останнього варіанту, є, але зовсім мала.

3.2. Можливі сценарії виконання СППР у графічному представленні

При ідеальних умовах, за допомогою Complex PDU від Cisco Packet Tracer, видає 32 позитивних результати – Successful. На рис. 3.3 показані результати при всіх працюючих з'єднаннях. Однак, у реальних умовах можуть виникати різноманітні проблеми, які впливають на стабільність мережі. Для аналізу таких сценаріїв важливо провести тестування при різних умовах, включаючи симуляцію несправностей та перешкод. Проведення таких тестів дозволяє виявити слабкі місця в мережі та оцінити ефективність існуючих механізмів діагностики та управління. Зібрані дані допомагають оптимізувати мережу, впровадити необхідні покращення та запобігти майбутнім проблемам.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Perioc	Num	Edit
	Successful	PC1-301	192.168.1.100	ICMP		60.000	Y	0	(edit)
	Successful	PC1-302	192.168.1.100	ICMP		60.000	Y	1	(edit)
	Successful	PC1-303	192.168.1.100	ICMP		60.000	Y	2	(edit)
	Successful	PC1-304	192.168.1.100	ICMP		60.000	Y	3	(edit)
	Successful	PC1-305	192.168.1.100	ICMP		60.000	Y	4	(edit)
	Successful	PC1-306	192.168.1.100	ICMP		60.000	Y	5	(edit)
	Successful	PC1-307	192.168.1.100	ICMP		60.000	Y	6	(edit)
	Successful	PC1-308	192.168.1.100	ICMP		60.000	Y	7	(edit)
	Successful	PC1-311	192.168.1.100	ICMP		60.000	Y	8	(edit)
	Successful	PC1-312	192.168.1.100	ICMP		60.000	Y	9	(edit)
	Successful	PC1-313	192.168.1.100	ICMP		60.000	Y	10	(edit)
	Successful	PC1-314	192.168.1.100	ICMP		60.000	Y	11	(edit)
	Successful	PC1-315	192.168.1.100	ICMP		60.000	Y	12	(edit)
	Successful	PC1-316	192.168.1.100	ICMP		60.000	Y	13	(edit)
	Successful	PC1-317	192.168.1.100	ICMP		60.000	Y	14	(edit)
	Successful	PC1-318	192.168.1.100	ICMP		60.000	Y	15	(edit)
	Successful	PC1-321	192.168.1.100	ICMP		60.000	Y	16	(edit)
	Successful	PC1-322	192.168.1.100	ICMP		60.000	Y	17	(edit)
	Successful	PC1-323	192.168.1.100	ICMP		60.000	Y	18	(edit)
	Successful	PC1-324	192.168.1.100	ICMP		60.000	Y	19	(edit)
	Successful	PC1-325	192.168.1.100	ICMP		60.000	Y	20	(edit)
	Successful	PC1-326	192.168.1.100	ICMP		60.000	Y	21	(edit)
	Successful	PC1-327	192.168.1.100	ICMP		60.000	Y	22	(edit)
	Successful	PC1-328	192.168.1.100	ICMP		60.000	Y	23	(edit)
	Successful	PC1-331	192.168.1.100	ICMP		60.000	Y	24	(edit)
	Successful	PC1-332	192.168.1.100	ICMP		60.000	Y	25	(edit)
	Successful	PC1-333	192.168.1.100	ICMP		60.000	Y	26	(edit)
	Successful	PC1-334	192.168.1.100	ICMP		60.000	Y	27	(edit)
	Successful	PC1-335	192.168.1.100	ICMP		60.000	Y	28	(edit)
	Successful	PC1-336	192.168.1.100	ICMP		60.000	Y	29	(edit)
	Successful	PC1-337	192.168.1.100	ICMP		60.000	Y	30	(edit)
	Successful	PC1-338	192.168.1.100	ICMP		60.000	Y	31	(edit)

Рисунок 3.3 – Результати тестування пінгування при ідеальних умовах

Тепер розбираємо декілька інших сценаріїв при яких в результатах Complex PDU буде показаний негативний результат – Failed. Припустимо, що з’єднання з комп’ютером 1-331 відсутнє, що зображено на рис. 3.4. Тоді по алгоритму дій, питаємо - чи працює хоча б один із вузлів від 1-331 до 1-338. Результат зображений на рис. 3.5.

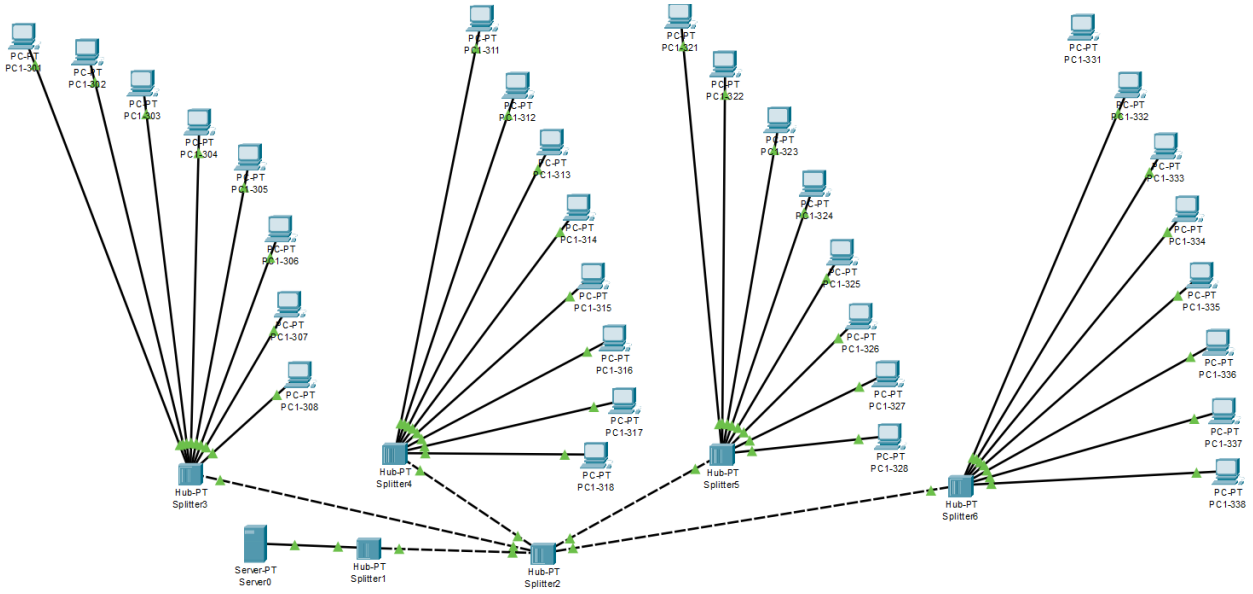


Рисунок 3.4 – Відсутній зв’язок з кінцевим пристроєм 1-331

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Perioc	Num	Edit
	Successful	PC1-301	192.168.1.100	ICMP		60.000	Y	0	(edit)
	Successful	PC1-302	192.168.1.100	ICMP		60.000	Y	1	(edit)
	Successful	PC1-303	192.168.1.100	ICMP		60.000	Y	2	(edit)
	Successful	PC1-304	192.168.1.100	ICMP		60.000	Y	3	(edit)
	Successful	PC1-305	192.168.1.100	ICMP		60.000	Y	4	(edit)
	Successful	PC1-306	192.168.1.100	ICMP		60.000	Y	5	(edit)
	Successful	PC1-307	192.168.1.100	ICMP		60.000	Y	6	(edit)
	Successful	PC1-308	192.168.1.100	ICMP		60.000	Y	7	(edit)
	Successful	PC1-311	192.168.1.100	ICMP		60.000	Y	8	(edit)
	Successful	PC1-312	192.168.1.100	ICMP		60.000	Y	9	(edit)
	Successful	PC1-313	192.168.1.100	ICMP		60.000	Y	10	(edit)
	Successful	PC1-314	192.168.1.100	ICMP		60.000	Y	11	(edit)
	Successful	PC1-315	192.168.1.100	ICMP		60.000	Y	12	(edit)
	Successful	PC1-316	192.168.1.100	ICMP		60.000	Y	13	(edit)
	Successful	PC1-317	192.168.1.100	ICMP		60.000	Y	14	(edit)
	Successful	PC1-318	192.168.1.100	ICMP		60.000	Y	15	(edit)
	Successful	PC1-321	192.168.1.100	ICMP		60.000	Y	16	(edit)
	Successful	PC1-322	192.168.1.100	ICMP		60.000	Y	17	(edit)
	Successful	PC1-323	192.168.1.100	ICMP		60.000	Y	18	(edit)
	Successful	PC1-324	192.168.1.100	ICMP		60.000	Y	19	(edit)
	Successful	PC1-325	192.168.1.100	ICMP		60.000	Y	20	(edit)
	Successful	PC1-326	192.168.1.100	ICMP		60.000	Y	21	(edit)
	Successful	PC1-327	192.168.1.100	ICMP		60.000	Y	22	(edit)
	Successful	PC1-328	192.168.1.100	ICMP		60.000	Y	23	(edit)
	Failed	PC1-331	192.168.1.100	ICMP		60.000	Y	24	(edit)
	Successful	PC1-332	192.168.1.100	ICMP		60.000	Y	25	(edit)
	Successful	PC1-333	192.168.1.100	ICMP		60.000	Y	26	(edit)
	Successful	PC1-334	192.168.1.100	ICMP		60.000	Y	27	(edit)
	Successful	PC1-335	192.168.1.100	ICMP		60.000	Y	28	(edit)
	Successful	PC1-336	192.168.1.100	ICMP		60.000	Y	29	(edit)
	Successful	PC1-337	192.168.1.100	ICMP		60.000	Y	30	(edit)
	Successful	PC1-338	192.168.1.100	ICMP		60.000	Y	31	(edit)

Рисунок 3.5 – Працюють усі вузли окрім 1-331

Після даних результатів можна пройтись по алгоритму дій дерева системи підтримки прийняття рішень. За ним - можливе виникнення пошкодження ONT, або ділянки 7-ONT, або роз'єму 7.

Далі беремо сценарій роботи, за яким вузли 1-331 - 1-338 не працюють, як це накреслено у логічній топологій на рис. 3.6. Тоді ставиться питання – «Чи працює хоча б один із вузлів від 1-301 до 1-338?» Відповіддю на це питання буде – так, працює, як показано на рис. 3.7. Тоді, за алгоритмом, підсумком проблеми є можливе виникнення пошкодження ділянки 5-6, або сплітеру S6.

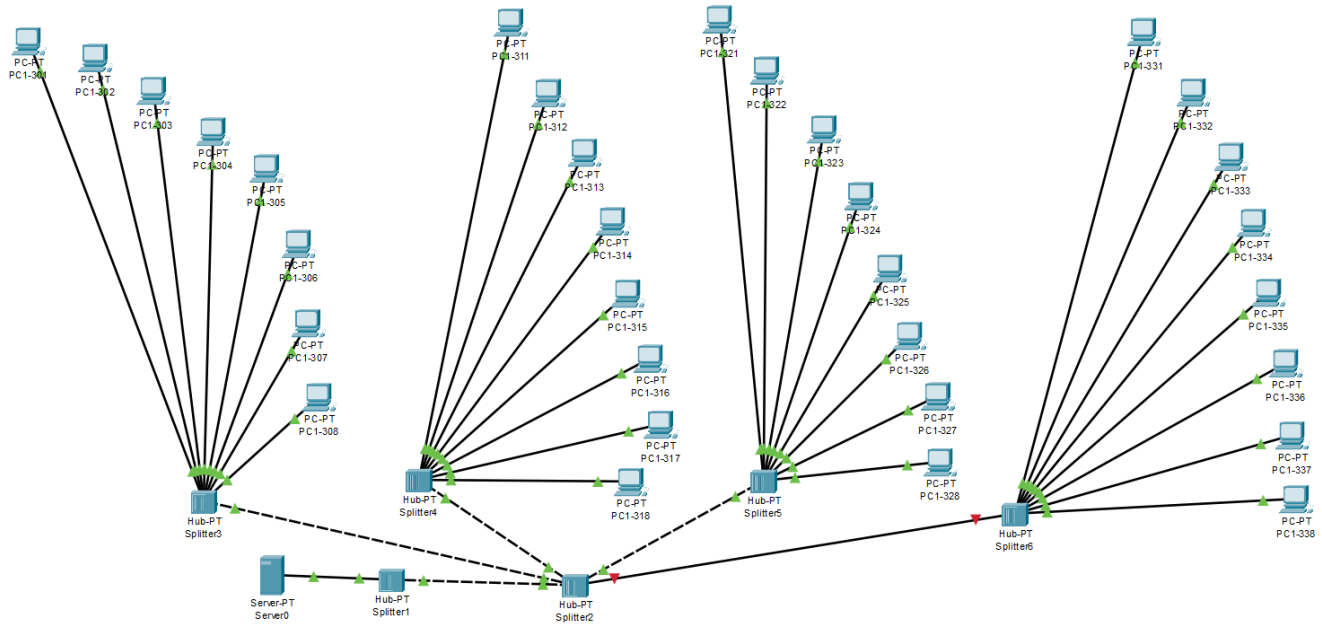


Рисунок 3.6 – Логічна топологія за якою, вузли 1-331 - 1-338 не працюють

Залишається останній сценарій розвитку подій. Проблема стала більш глобальною – потрібно шукати, чи працює хоча б один із вузлів від 1-301 до 1-438. Якщо так, то можливе виникнення пошкодження ділянки 3-4, або сплітеру S2. Якщо ні, то можливе пошкодження ділянки 1-2, або ОМ, або сплітеру.

На рис. 3.8 та 3.9, відповідно, зображені відповідно, логічні топології, де немає зв'язку між сплітерами 1 і 2 та де не проходить сигнал між сервером та сплітером. В іншому випадку у Cisco Packet Tracer представлено тільки комп'ютери

1-301 – 1-338, тому при обох варіантах, усі кінцеві пристрої будуть відключені, та не матимуть можливість для пінгування.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Perioc	Num	Edit
	Successful	PC1-301	192.168.1.100	ICMP		60.000	Y	0	(edit)
	Successful	PC1-302	192.168.1.100	ICMP		60.000	Y	1	(edit)
	Successful	PC1-303	192.168.1.100	ICMP		60.000	Y	2	(edit)
	Successful	PC1-304	192.168.1.100	ICMP		60.000	Y	3	(edit)
	Successful	PC1-305	192.168.1.100	ICMP		60.000	Y	4	(edit)
	Successful	PC1-306	192.168.1.100	ICMP		60.000	Y	5	(edit)
	Successful	PC1-307	192.168.1.100	ICMP		60.000	Y	6	(edit)
	Successful	PC1-308	192.168.1.100	ICMP		60.000	Y	7	(edit)
	Successful	PC1-311	192.168.1.100	ICMP		60.000	Y	8	(edit)
	Successful	PC1-312	192.168.1.100	ICMP		60.000	Y	9	(edit)
	Successful	PC1-313	192.168.1.100	ICMP		60.000	Y	10	(edit)
	Successful	PC1-314	192.168.1.100	ICMP		60.000	Y	11	(edit)
	Successful	PC1-315	192.168.1.100	ICMP		60.000	Y	12	(edit)
	Successful	PC1-316	192.168.1.100	ICMP		60.000	Y	13	(edit)
	Successful	PC1-317	192.168.1.100	ICMP		60.000	Y	14	(edit)
	Successful	PC1-318	192.168.1.100	ICMP		60.000	Y	15	(edit)
	Successful	PC1-321	192.168.1.100	ICMP		60.000	Y	16	(edit)
	Successful	PC1-322	192.168.1.100	ICMP		60.000	Y	17	(edit)
	Successful	PC1-323	192.168.1.100	ICMP		60.000	Y	18	(edit)
	Successful	PC1-324	192.168.1.100	ICMP		60.000	Y	19	(edit)
	Successful	PC1-325	192.168.1.100	ICMP		60.000	Y	20	(edit)
	Successful	PC1-326	192.168.1.100	ICMP		60.000	Y	21	(edit)
	Successful	PC1-327	192.168.1.100	ICMP		60.000	Y	22	(edit)
	Successful	PC1-328	192.168.1.100	ICMP		60.000	Y	23	(edit)
	Failed	PC1-331	192.168.1.100	ICMP		60.000	Y	24	(edit)
	Failed	PC1-332	192.168.1.100	ICMP		60.000	Y	25	(edit)
	Failed	PC1-333	192.168.1.100	ICMP		60.000	Y	26	(edit)
	Failed	PC1-334	192.168.1.100	ICMP		60.000	Y	27	(edit)
	Failed	PC1-335	192.168.1.100	ICMP		60.000	Y	28	(edit)
	Failed	PC1-336	192.168.1.100	ICMP		60.000	Y	29	(edit)
	Failed	PC1-337	192.168.1.100	ICMP		60.000	Y	30	(edit)
	Failed	PC1-338	192.168.1.100	ICMP		60.000	Y	31	(edit)

Рисунок 3.7 - Працюють усі вузли окрім 1-331 – 1-338

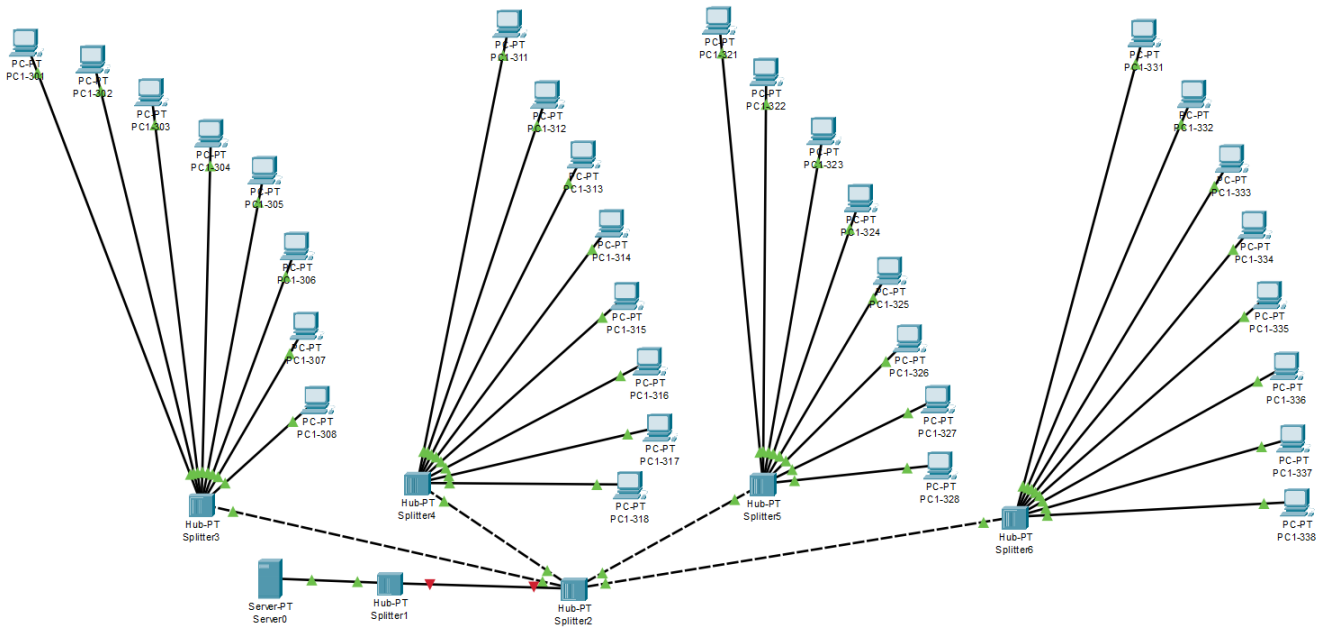


Рисунок 3.8 – Між першим та другим сплітером, відсутній зв’язок

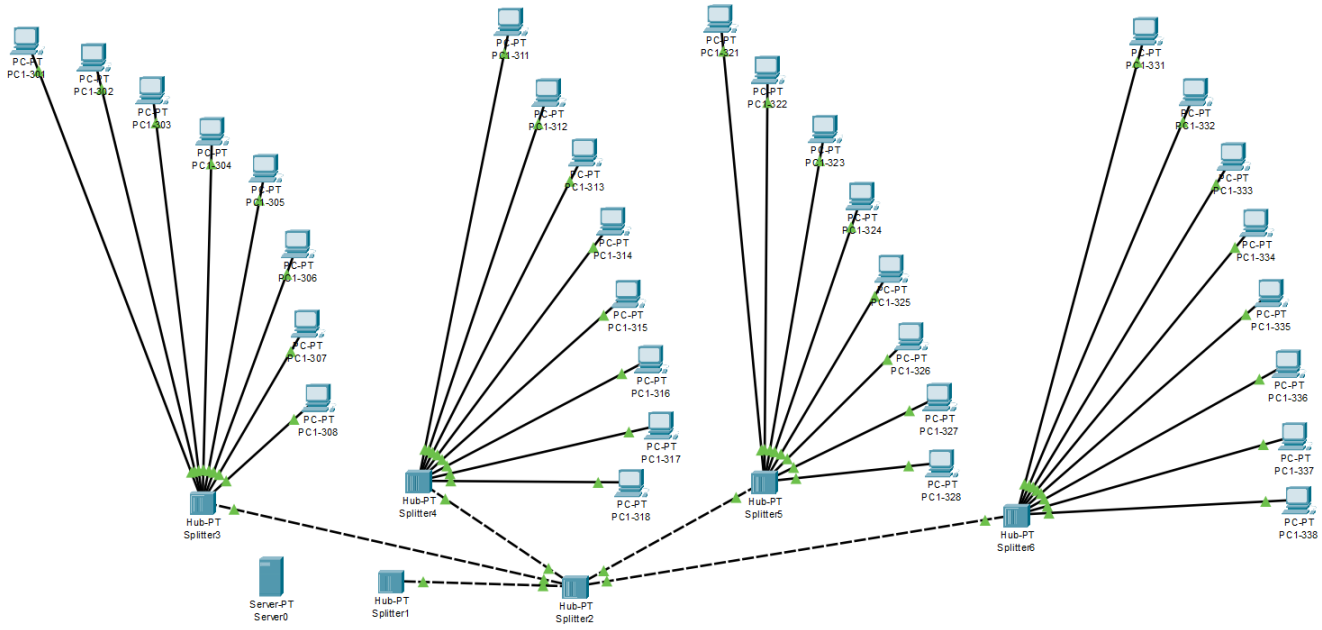


Рисунок 3.9 – Вузол між сервером та першим сплітером, пошкоджено

На рис. 3.10 показано невдалі спроби пінгування, при випадку коли усі кінцеві пристрої відключені від мережі.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Perioc	Num	Edit
	Failed	PC1-301	192.168.1.100	ICMP		60.000	Y	0	(edit)
	Failed	PC1-302	192.168.1.100	ICMP		60.000	Y	1	(edit)
	Failed	PC1-303	192.168.1.100	ICMP		60.000	Y	2	(edit)
	Failed	PC1-304	192.168.1.100	ICMP		60.000	Y	3	(edit)
	Failed	PC1-305	192.168.1.100	ICMP		60.000	Y	4	(edit)
	Failed	PC1-306	192.168.1.100	ICMP		60.000	Y	5	(edit)
	Failed	PC1-307	192.168.1.100	ICMP		60.000	Y	6	(edit)
	Failed	PC1-308	192.168.1.100	ICMP		60.000	Y	7	(edit)
	Failed	PC1-311	192.168.1.100	ICMP		60.000	Y	8	(edit
	Failed	PC1-312	192.168.1.100	ICMP		60.000	Y	9	(edit
	Failed	PC1-313	192.168.1.100	ICMP		60.000	Y	10	(edit
	Failed	PC1-314	192.168.1.100	ICMP		60.000	Y	11	(edit
	Failed	PC1-315	192.168.1.100	ICMP		60.000	Y	12	(edit)
	Failed	PC1-316	192.168.1.100	ICMP		60.000	Y	13	(edit)
	Failed	PC1-317	192.168.1.100	ICMP		60.000	Y	14	(edit)
	Failed	PC1-318	192.168.1.100	ICMP		60.000	Y	15	(edit)
	Failed	PC1-321	192.168.1.100	ICMP		60.000	Y	16	(edit
	Failed	PC1-322	192.168.1.100	ICMP		60.000	Y	17	(edit
	Failed	PC1-323	192.168.1.100	ICMP		60.000	Y	18	(edit
	Failed	PC1-324	192.168.1.100	ICMP		60.000	Y	19	(edit
	Failed	PC1-325	192.168.1.100	ICMP		60.000	Y	20	(edit)
	Failed	PC1-326	192.168.1.100	ICMP		60.000	Y	21	(edit)
	Failed	PC1-327	192.168.1.100	ICMP		60.000	Y	22	(edit)
	Failed	PC1-328	192.168.1.100	ICMP		60.000	Y	23	(edit)
	Failed	PC1-331	192.168.1.100	ICMP		60.000	Y	24	(edit)
	Failed	PC1-332	192.168.1.100	ICMP		60.000	Y	25	(edit)
	Failed	PC1-333	192.168.1.100	ICMP		60.000	Y	26	(edit)
	Failed	PC1-334	192.168.1.100	ICMP		60.000	Y	27	(edit)
	Failed	PC1-335	192.168.1.100	ICMP		60.000	Y	28	(edit)
	Failed	PC1-336	192.168.1.100	ICMP		60.000	Y	29	(edit)
	Failed	PC1-337	192.168.1.100	ICMP		60.000	Y	30	(edit)
	Failed	PC1-338	192.168.1.100	ICMP		60.000	Y	31	(edit)

Рисунок 3.10 – Усі кінцеві пристрої відключені

3.3. Результати тестування сценаріїв ПЗ на Java

При запуску програми всі комп'ютери - підключені і під час перевірки пінгування будь-якого комп'ютера, видається MessageBox – «підключення стабільне». На рис. 3.11 зображено саме такий сценарій, де перевіряється пінг кінцевого девайсу № 1-301.

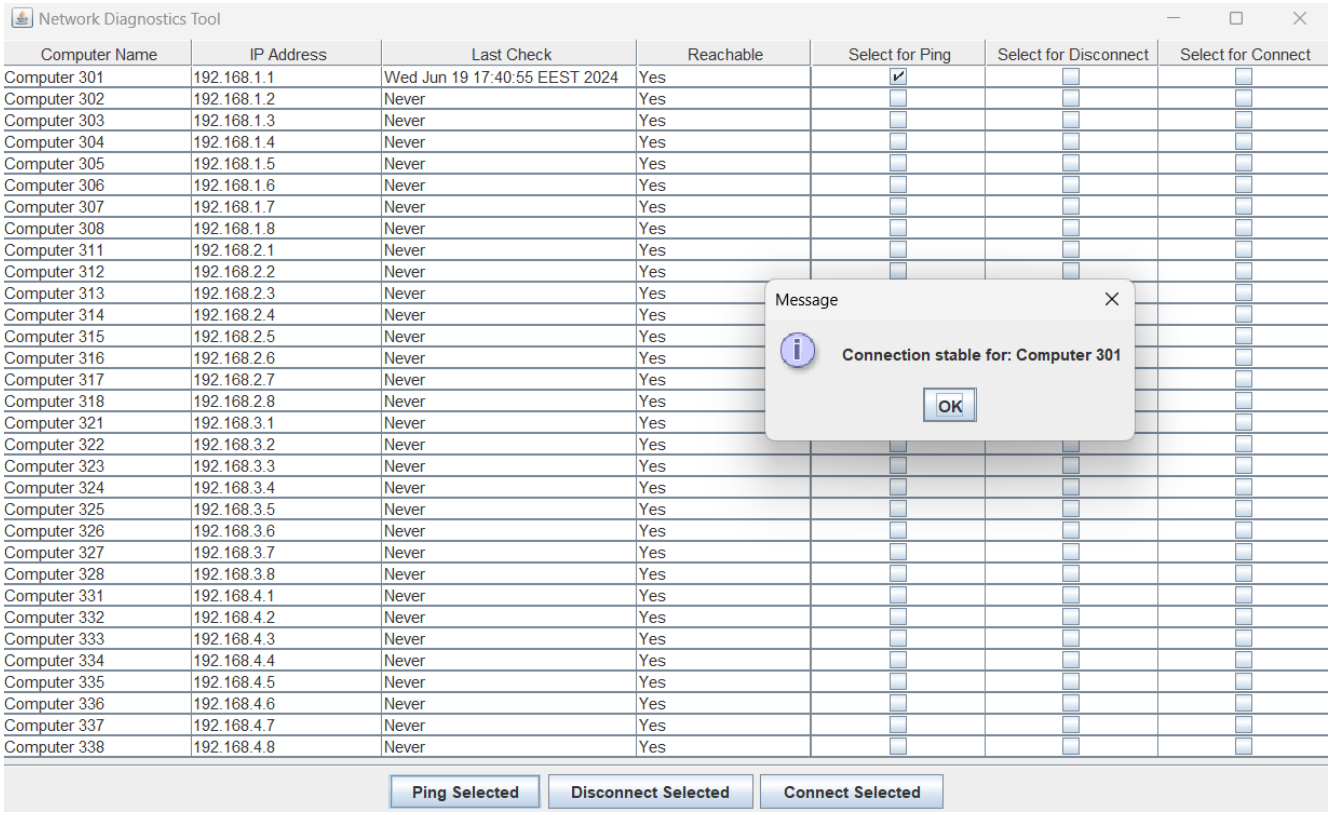


Рисунок 3.11 – Перевірка пінгування користувача 1-301

Більш повна схема системи підтримки прийняття рішень використано на рис. 3.12.

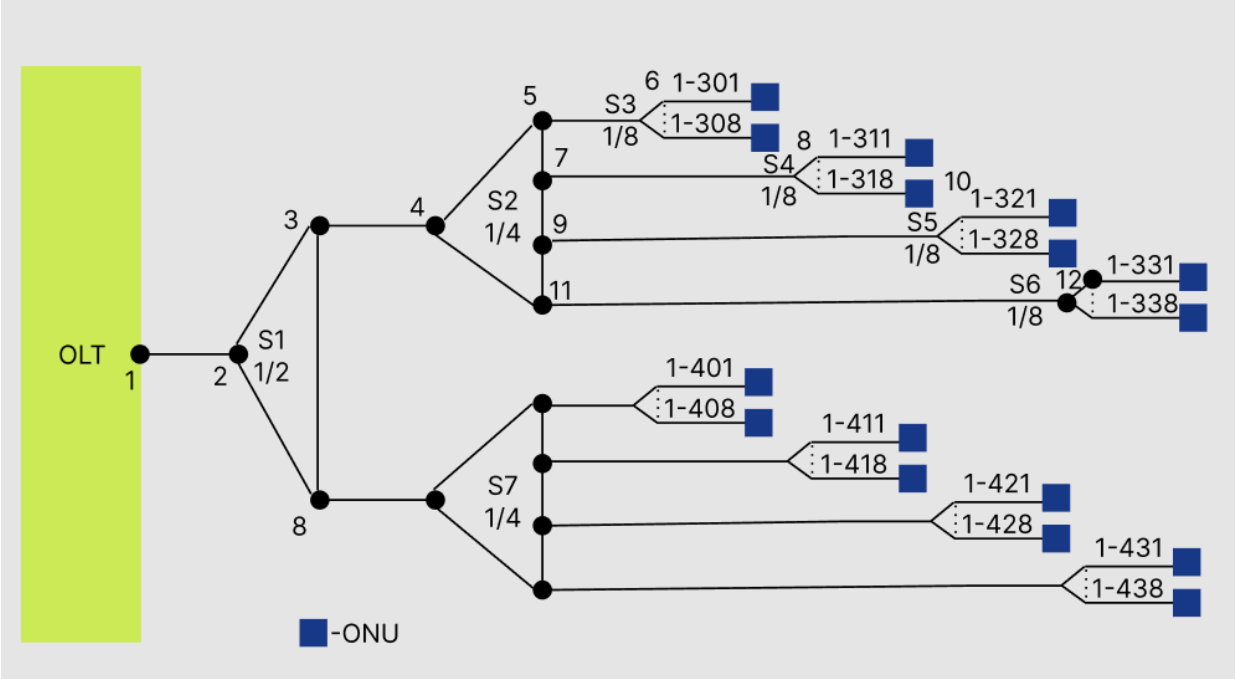


Рисунок 3.12 - Повна схема системи підтримки прийняття рішень

Якщо підключення відсутнє (самостійно відключене), тоді в силу вступають різні послідовності. При відсутності з'єднання з одним з кінцевих пристроїв (1-301 – 1-308), алгоритм дій відбувається відповіддями на запитання, згідно поставленій послідовності.

Задається питання - чи можливе пінгування хоча б одного із комп'ютерів від № 1-301 до 1-308?

– якщо ТАК, то у MessageBox виводиться таке повідомлення - можливе виникнення пошкодження ONT, або ділянки найближчого роз'єму-ONT, або відповідного роз'єму;

– якщо НІ, то переходимо до наступної дії алгоритму.

На рис. 3.13 показано як було відключено кінцевий девайс № 1-301, та його пінгування є неможливим, тому виконується умова ТАК.

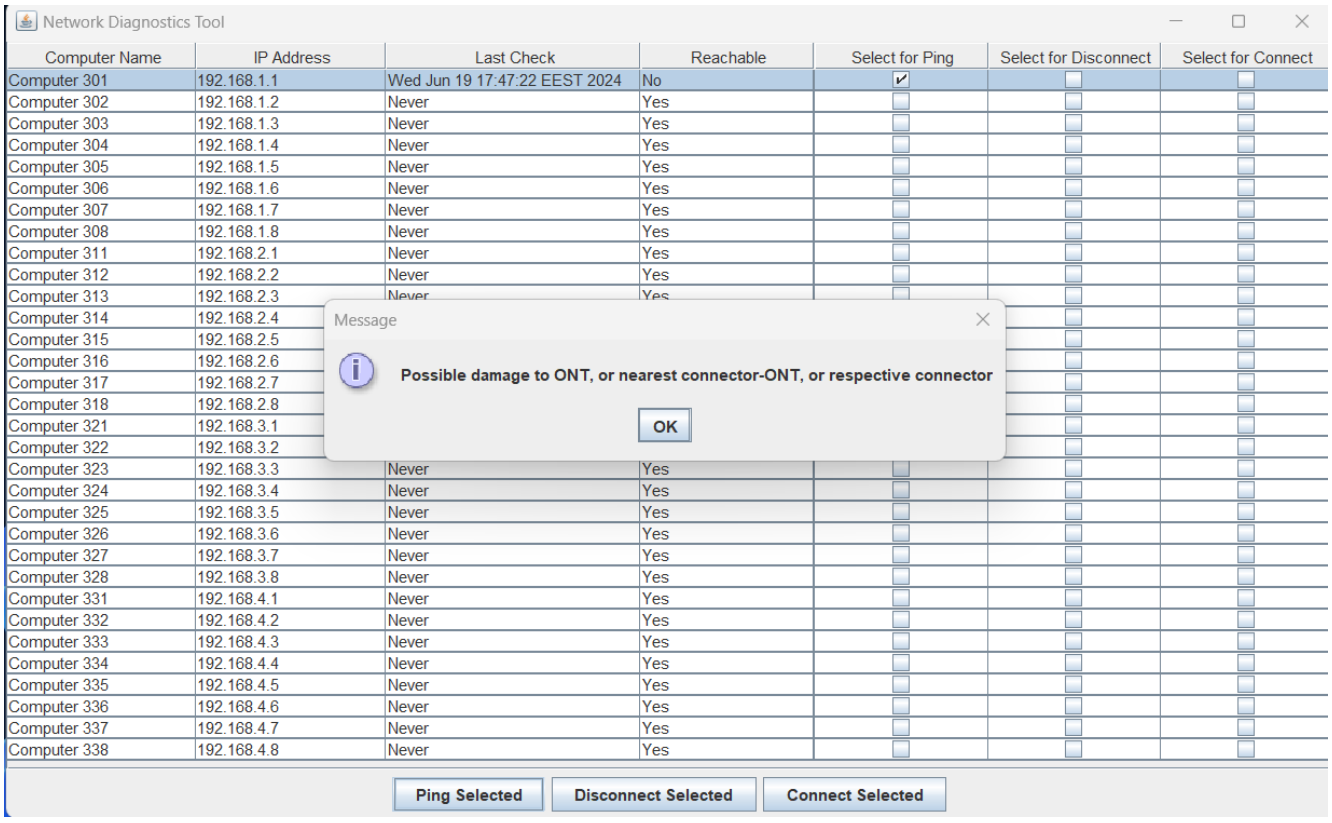


Рисунок 3.13 - Перевірка пінгування користувача 1-301, при його відключенні, з виконанням умови ТАК

Наступним відбувається продовження відповіді на запитання - чи можливе пінгування хоча б одного із комп'ютерів від № 1-301 до 1-338?

– якщо ТАК, то у MessageBox виводиться таке повідомлення - можливе виникнення пошкодження ділянки D5/6, або сплітеру S3;

– якщо НІ, то написати повідомлення-попередження.

Задля виконання даного сценарію дії на рис. 3.14 дано результати в той час коли було відключено такі комп’ютери під номерами: № 1-301 - 1-308.

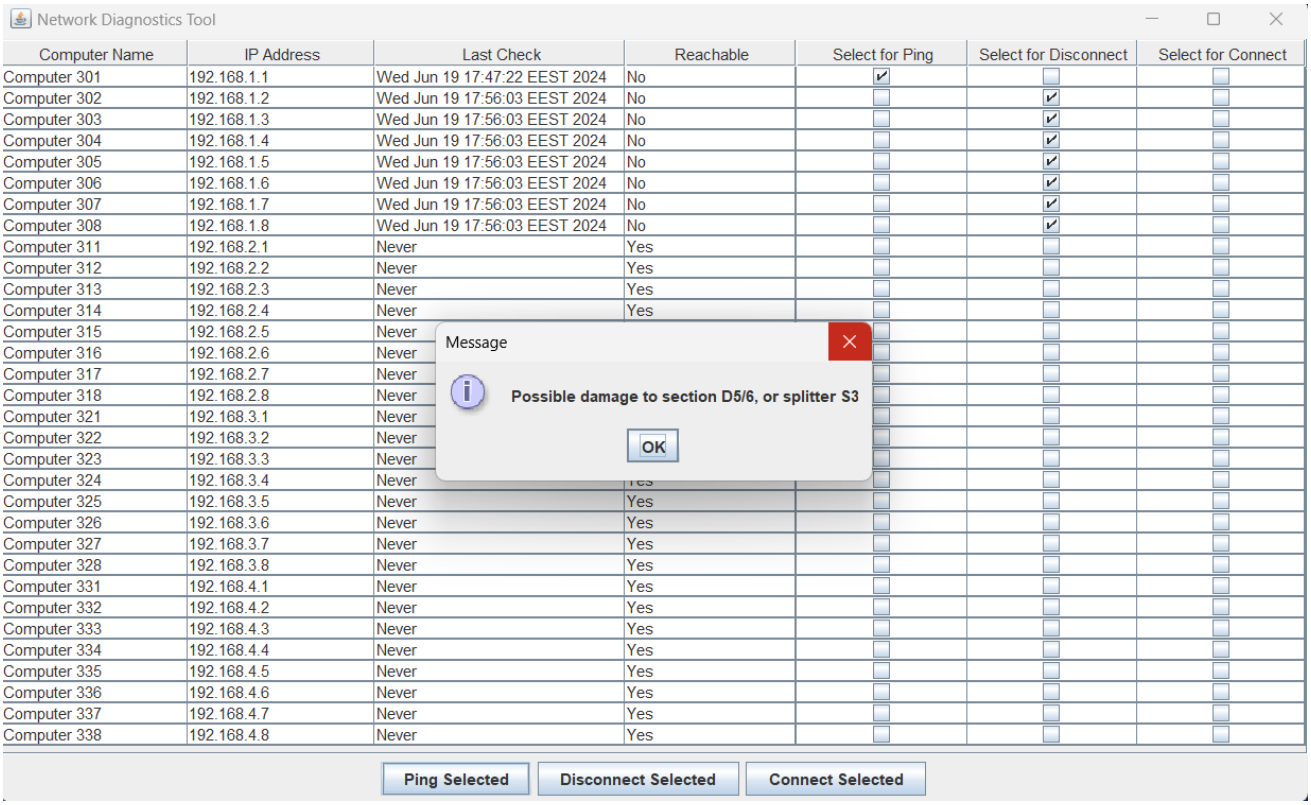


Рисунок 3.14 - Перевірка пінгування користувача 1-301, при відключенні 1-301 – 1-308, з виконанням умови ТАК

При відсутності з'єднання з одним з кінцевих пристроїв (№ 1-311 – 1-318), послідовність дій в данному ланцюгу, змінюється. Далі потрібно дати відповідь на запитання – чи можливе пінгування хоча б одного із комп'ютерів від № 1-311 до 1-318?

– якщо ТАК, то показується MessageBox з надписом: «можливе виникнення пошкодження ONT, або ділянки найближчого роз'єму-ONT, або відповідного роз’єму»;

– якщо НІ, то переходимо до наступної дії алгоритму.

Після цього ставиться запитання - чи можливе пінгування хоча б одного із комп'ютерів від № 1-301 до 1-338?

– якщо ТАК, то відкривається текстом MessageBox - можливе виникнення пошкодження ділянки D7/8, або сплітеру S4;

– якщо НІ, то написати повідомлення-попередження.

На рис. 3.15 показаний результат після пінгування девайса користувача № 1-311.

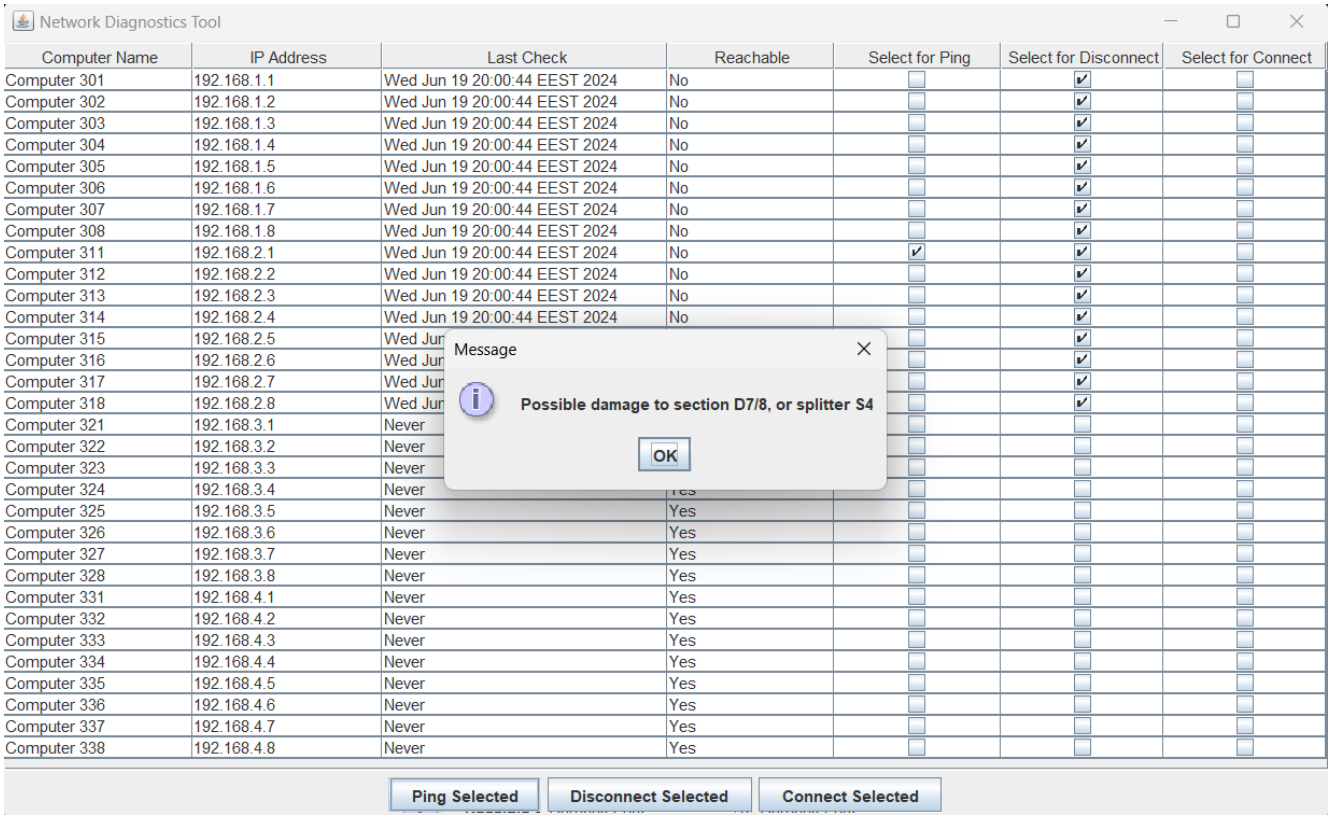


Рисунок 3.15 - Результат після пінгування кінцевого пристрою № 1-311

При відсутності з'єднання з одним з кінцевих пристроїв (№ 1-321 – 1-328), алгоритм продовжується - чи можливе пінгування хоча б одного із комп'ютерів від № 1-321 до 1-328?

– якщо ТАК, то MessageBox - можливе: виникнення пошкодження ONT, або ділянки найближчого роз'єму-ONT, або відповідного роз’єму;

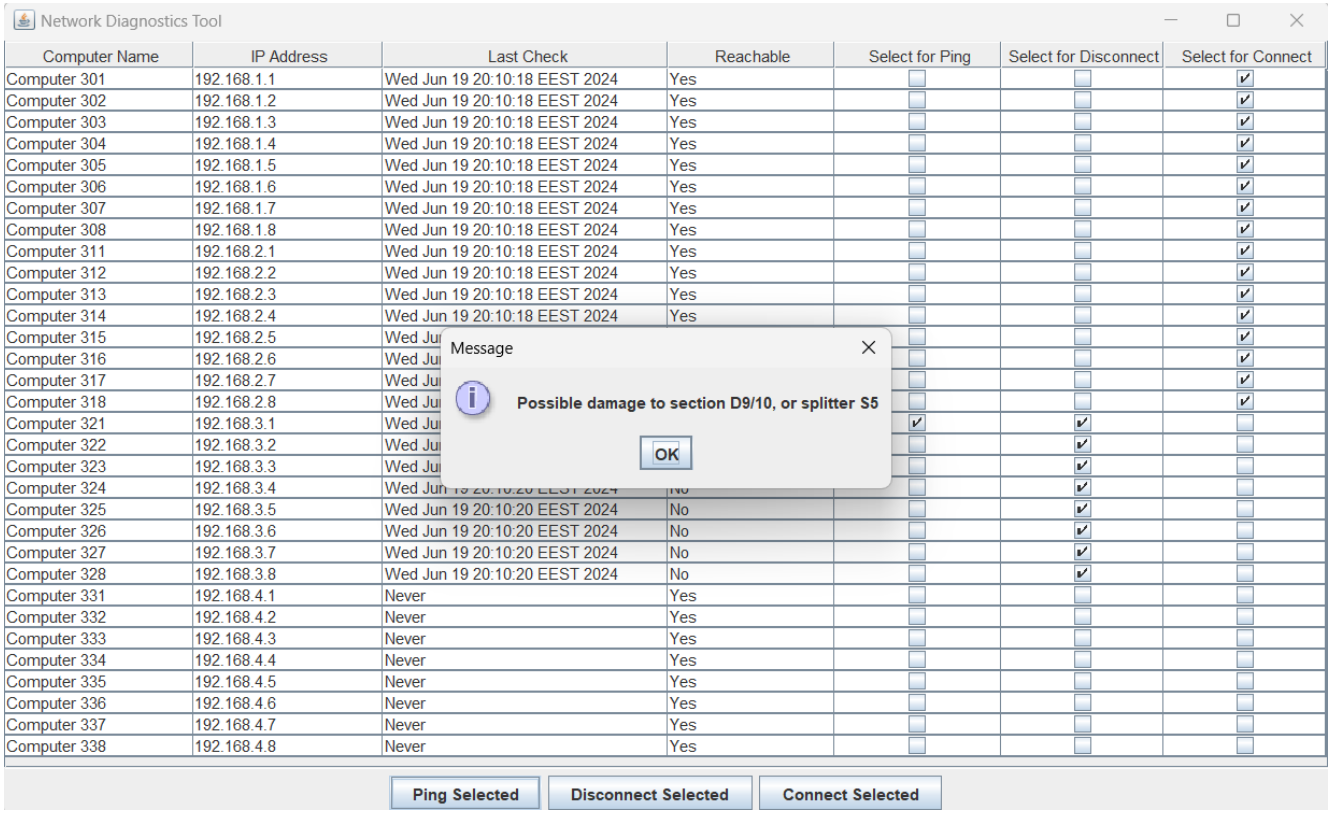
– якщо НІ, то переходимо до наступної дії алгоритму.

Далі йде продоження постановки питань - чи можливе пінгування хоча б одного із комп'ютерів від № 1-301 до 1-338?

– якщо ТАК, то MessageBox - можливе виникнення пошкодження ділянки D9/10, або сплітеру S5;

– якщо НІ, то написати повідомлення-попередження.

На рис. 3.16 зображений результат після пінгування девайса користувача № 1-321.



Computer Name	IP Address	Last Check	Reachable	Select for Ping	Select for Disconnect	Select for Connect
Computer 301	192.168.1.1	Wed Jun 19 20:10:18 EEST 2024	Yes	☐	☐	☑
Computer 302	192.168.1.2	Wed Jun 19 20:10:18 EEST 2024	Yes	☐	☐	☑
Computer 303	192.168.1.3	Wed Jun 19 20:10:18 EEST 2024	Yes	☐	☐	☑
Computer 304	192.168.1.4	Wed Jun 19 20:10:18 EEST 2024	Yes	☐	☐	☑
Computer 305	192.168.1.5	Wed Jun 19 20:10:18 EEST 2024	Yes	☐	☐	☑
Computer 306	192.168.1.6	Wed Jun 19 20:10:18 EEST 2024	Yes	☐	☐	☑
Computer 307	192.168.1.7	Wed Jun 19 20:10:18 EEST 2024	Yes	☐	☐	☑
Computer 308	192.168.1.8	Wed Jun 19 20:10:18 EEST 2024	Yes	☐	☐	☑
Computer 311	192.168.2.1	Wed Jun 19 20:10:18 EEST 2024	Yes	☐	☐	☑
Computer 312	192.168.2.2	Wed Jun 19 20:10:18 EEST 2024	Yes	☐	☐	☑
Computer 313	192.168.2.3	Wed Jun 19 20:10:18 EEST 2024	Yes	☐	☐	☑
Computer 314	192.168.2.4	Wed Jun 19 20:10:18 EEST 2024	Yes	☐	☐	☑
Computer 315	192.168.2.5	Wed Ju		☐	☐	☑
Computer 316	192.168.2.6	Wed Ju		☐	☐	☑
Computer 317	192.168.2.7	Wed Ju		☐	☐	☑
Computer 318	192.168.2.8	Wed Ju		☐	☐	☑
Computer 321	192.168.3.1	Wed Ju		☑	☑	☐
Computer 322	192.168.3.2	Wed Ju		☐	☑	☐
Computer 323	192.168.3.3	Wed Ju		☐	☑	☐
Computer 324	192.168.3.4	Wed Jun 19 20:10:20 EEST 2024	No	☐	☑	☐
Computer 325	192.168.3.5	Wed Jun 19 20:10:20 EEST 2024	No	☐	☑	☐
Computer 326	192.168.3.6	Wed Jun 19 20:10:20 EEST 2024	No	☐	☑	☐
Computer 327	192.168.3.7	Wed Jun 19 20:10:20 EEST 2024	No	☐	☑	☐
Computer 328	192.168.3.8	Wed Jun 19 20:10:20 EEST 2024	No	☐	☑	☐
Computer 331	192.168.4.1	Never	Yes	☐	☐	☐
Computer 332	192.168.4.2	Never	Yes	☐	☐	☐
Computer 333	192.168.4.3	Never	Yes	☐	☐	☐
Computer 334	192.168.4.4	Never	Yes	☐	☐	☐
Computer 335	192.168.4.5	Never	Yes	☐	☐	☐
Computer 336	192.168.4.6	Never	Yes	☐	☐	☐
Computer 337	192.168.4.7	Never	Yes	☐	☐	☐
Computer 338	192.168.4.8	Never	Yes	☐	☐	☐

Рисунок 3.16 - Результат після пінгування кінцевого пристрою № 1-321.

При відсутності з'єднання з одним з кінцевих пристроїв (№ 1-331 – 1-338), то алгоритм продовжується - чи можливе пінгування хоча б одного із комп'ютерів від № 1-331 до 1-338?

– якщо ТАК, то MessageBox - можливе виникнення пошкодження ONT, або ділянки найближчого роз'єму-ONT, або відповідного роз’єму;

– якщо НІ, то переходимо до наступної дії алгоритму.

Зрештою постається одне з останніх запитань - чи можливе пінгування хоча б одного із комп'ютерів від № 1-301 до 1-338?

– якщо ТАК, то MessageBox - можливе виникнення пошкодження ділянки D11/12, або сплітеру S6;

– якщо НІ, то написати повідомлення-попередження.

На рис. 3.17 представлений результат після пінгування девайса користувача № 1-331.

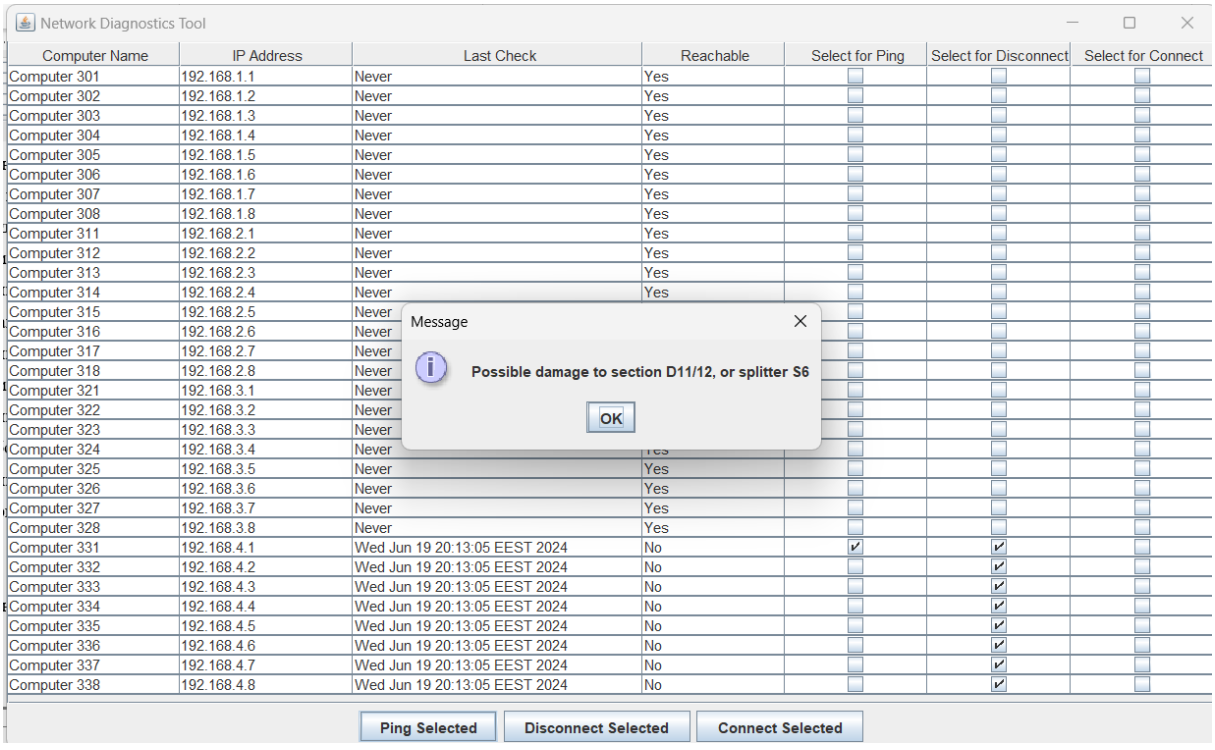


Рисунок 3.17 - Результат після пінгування кінцевого пристрою № 1-331.

Повідомлення-попередження MessageBox з наступним текстом: «можливе виникнення пошкодження ділянки 3-4, або сплітеру S2, можливе пошкодження

ділянки 1-2, або ОМ, або сплітеру S1, потрібна перевірка вузлів від 1-301 до 1-438». На рис. 3.18 зображено сценарій роботи системи підтримки прийняття рішень, при усіх відповіддях - НІ.

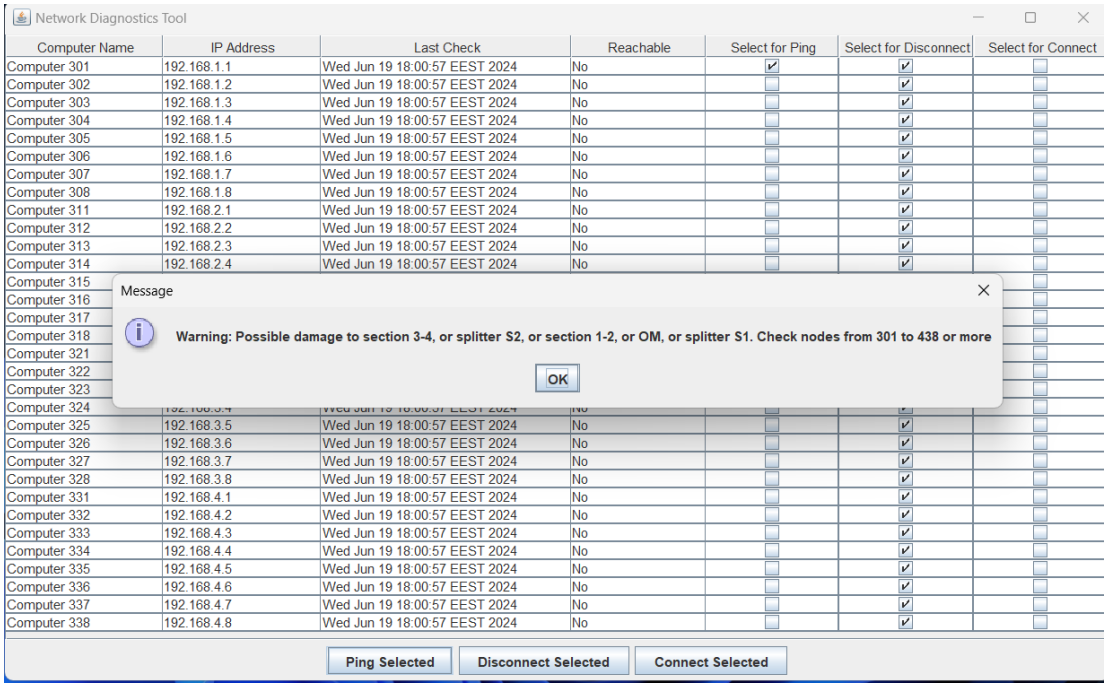


Рисунок 3.18 – Відключення усіх кінцевих девайсів, від 1-301 до 1-338

3.4. Висновки

В даному розділі було проведено моделювання та аналіз різних сценаріїв роботи мережі за допомогою Complex PDU в Cisco Packet Tracer. При ідеальних умовах, всі 32 вузли успішно проходять перевірку з’єднання, що свідчить про стабільну роботу мережі. Однак, у випадку виникнення неполадок, алгоритм системи підтримки прийняття рішень допомагає визначити можливі місця пошкодження. Наприклад, при відсутності з'єднання з окремими комп'ютерами або групами комп'ютерів, алгоритм послідовно аналізує працездатність інших вузлів, що дозволяє локалізувати потенційні проблеми в конкретних ділянках мережі або сплітерах. Такий підхід забезпечує ефективну діагностику та швидке реагування на мережеві неполадки, підвищуючи надійність та стабільність роботи телекомунікаційної інфраструктури.

Також було розроблено програму на мові Java, яка реалізує створення застосунку для системи підтримки прийняття рішень, що використовує принцип пінгування. Програма дозволяє моніторити стан підключення комп'ютерів у мережі, розділеній на чотири сплітери, шляхом пінгування їх IP-адрес. Основні функціональні можливості включають відображення таблиці з назвою комп'ютера, його IP-адресою, датою та часом останньої перевірки пінгування, а також інтерактивними CheckBox для перевірки пінгування, відключення та підключення комп'ютерів до мережі. При відсутності підключення програма автоматично аналізує можливі причини неполадки та виводить відповідні повідомлення для користувача. Завдяки цій програмі можна ефективно діагностувати та реагувати на можливі проблеми у мережі, забезпечуючи стабільну роботу комп'ютерної інфраструктури.

ВИСНОВКИ

У ході виконання дипломної роботи на тему "Кіберфізична система для моніторингу пасивних оптичних телекомунікаційних мереж (програмна частина)" було розглянуто ключові аспекти та виклики, що стосуються розробки та впровадження системи підтримки прийняття рішень (СППР) в сучасних телекомунікаційних мережах.

Перший розділ роботи було досліджено основні аспекти кіберфізичних систем для моніторингу пасивних оптичних телекомунікаційних мереж. Вивчення пасивних оптичних мереж, стандартів і типів PON (Passive Optical Network), а також засобів та методів моніторингу PON дозволило глибше зрозуміти принципи функціонування оптичних інфраструктур та їх важливість для сучасних телекомунікаційних систем. Було проведено аналіз переваг, які система підтримки прийняття рішень (СППР) приносить у плані ефективного моніторингу та управління оптичними мережами. Універсальність СППР та її здатність застосовуватися на різних рівнях мережі й типах оптичних інфраструктур роблять її важливим інструментом для забезпечення надійності та ефективності роботи телекомунікаційних систем.

Другий розділ зосереджувався на проектуванні програмно-технічного засобу. Було виконано детальний аналіз функціональних та нефункціональних вимог до СППР. Принцип пінгування був ключовим для точного визначення стану мережі та ефективного управління нею. Інтеграція пінгування з системою підтримки прийняття рішень створює комплексну платформу для аналізу, моніторингу та оптимізації мереж. Cisco Packet Tracer є ефективним інструментом для створення та тестування мереж, що дозволяє візуалізувати архітектуру мережі, аналізувати та оптимізувати управління мережевими ресурсами. Інтеграція сервісу Complex PDU надає важливі інструменти для централізованого збору даних, управління та діагностики мережі, відслідковування подій, аналізу тенденцій та планування вдосконалень. Розробка системи виявлення несправностей на основі алгоритмів кореляції в Java створює надійний інструмент для аналізу та

прогнозування стану мережі, сприяючи оптимізації її роботи та підвищенню надійності.

Третій розділ підтвердив ефективність впровадження СППР через програмно-апаратну реалізацію та тестування розробленого програмно-технічного засобу. У цьому розділі було проведено моделювання та аналіз роботи мережі за допомогою Complex PDU в Cisco Packet Tracer. У стабільних умовах всі 32 вузли успішно проходять перевірку з'єднання, що свідчить про стабільну роботу мережі. У випадку неполадок, алгоритм системи підтримки прийняття рішень допомагає визначити місця пошкодження, аналізуючи працездатність інших вузлів для локалізації проблем у конкретних ділянках мережі або сплітерах. Це забезпечує ефективну діагностику та швидке реагування на мережеві неполадки, підвищуючи надійність і стабільність телекомунікаційної інфраструктури.

Загалом, дипломна робота демонструє важливість інтеграції передових кіберфізичних систем у сферу управління пасивними оптичними мережами. Розроблена система підтримки прийняття рішень відкриває нові можливості для оптимізації роботи мереж та підвищення їх надійності. Результати дослідження та розробки підкреслюють значення комплексного підходу до аналізу мережевих систем, враховуючи сучасні технологічні виклики та потреби індустрії.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Cisco Networks: Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA 1st ed. Edition by Chris Carthern, William Wilson, Noel Rivera, Richard Bedwell. Springer; 1st ed. edition 2015. 870 p.
2. Andrew Tanenbaum. Computer Networks, Global Edition 6th Edition / Andrew Tanenbaum. – Pearson; 6th edition. 2021. 891p.
3. Wendell Odom. CCNA Routing and Switching Icnd2 200-105 Official Cert Guide / Wendell Odom. – Cisco Press; Har/Cdr edition 2016. 992p.
4. Ben Piper. Learn Cisco Network Administration in a Month of Lunches / Ben Piper. – Manning; 1st edition. 2017. 312p.
5. Michel Thomatis. Network Design Cookbook: 2nd Edition / Michel Thomatis – Lulu Press. 2019. 406p.
6. Cisco IoT Fundamentals: Connecting Things https://static-course-assets.s3.amazonaws.com/IoTFCT201/uk/index.html (дата звернення: 19.04.2024).
7. Networking All-in-One For Dummies Paperback. Doug Lowe. For Dummies; 7th edition 2018. 992 p.
8. Charles J. Brooks. Cybersecurity Essentials / Charles J. Brooks, Christopher Grow, Philip A. Craig Jr., Donald Short – Sybex; 1st edition. 2018. 782 p.
9. Java Platform, Standard Edition Documentation. Oracle. URL: https://docs.oracle.com/javase/8/docs/ (дата звернення: 5.04.2024).
10. Бондаренко С. В. Основи об'єктно-орієнтованого програмування на Java. Київ: Вид-во НАУ, 2021. 288 с.
11. Кузнецов В. В. Програмування на Java для початківців. Львів: Видавництво ЛНУ ім. І. Франка, 2019. 304 с.
12. Сердюк О. Г. Розробка інформаційних систем на Java. Вісник Дніпровського національного університету. Серія: Інформаційні технології, 2020. 123 с.
13. Кравченко І. М. Введення в програмування на Java: підручник. Київ: Вид-во КНТЕУ, 2017. 264 с.

14. Ермоленко О. В. Розробка додатків на Java. Вісник Київського національного університету. Серія: Комп’ютерні науки, 2018. 142 с.

15. Java SE Development Kit 8 Documentation. Oracle. URL: https://www.oracle.com/java/technologies/javase-jdk8-doc-downloads.html (дата звернення: 7.04.2024).

16. Нікітенко С. В. Використання мови Java для розробки мережевих застосунків. Вісник Національного технічного університету України «КПІ». Серія: Інформатика та обчислювальна техніка, 2021. 152 с.

17. Петренко О. Ю. Програмування на Java: теорія і практика. Харків: Вид-во НТУ «ХПІ», 2019. 352 с.

18. Смирнов Д. В. Розробка програмного забезпечення на мові Java для мобільних пристроїв. Вісник Одеської національної академії зв'язку, 2020. 220 с.

19. Шаповал І. М. Основи програмування на Java для студентів технічних спеціальностей. Львів: Вид-во НУЛП, 2018. 336 с.

20. Тимошенко В. Г. Практичний курс з програмування на Java. Київ: Вид-во КНУБА, 2017. 420 с.

21. Власюк М. С. Програмування на Java для початківців. Вінниця: Видавництво ВНТУ, 2019. 290 с.

22. Лук'яненко О. В. Основи програмування на мові Java: підручник. Дніпро: Вид-во ДНУ ім. О. Гончара, 2018. 402 с.

23. Середа І. В. Основи програмування на Java: підручник. Київ: Вид-во КНУБА, 2020. 456 с.

24. Кравченко С. В. Об’єктно-орієнтоване програмування на Java. Київ: Либідь, 2019. 384 с.

25. Зубков О. А. Розробка корпоративних застосунків на Java. Одеса: Видавництво ОНПУ, 2018. 330 с.

26. Java SE Development Kit 14 Documentation. Oracle. URL: https://www.oracle.com/java/technologies/javase-jdk14-doc-downloads.html (дата звернення: 9.04.2024).

27. O'Reilly Media. Java in a Nutshell, 7th Edition. URL: https://www.oreilly.com/library/view/java-in-a/9781492037255/ (дата звернення: 19.04.2024).

28. Baeldung. Guide to Java 8 Optional. URL: https://www.baeldung.com/java-8-optionals (дата звернення: 1.05.2024).

29. DigitalOcean. How To Install Java with Apt on Ubuntu 20.04. URL: https://www.digitalocean.com/community/tutorials/how-to-install-java-with-apt-on-ubuntu-20-04 (дата звернення: 26.04.2024).

30. Java SE Development Kit 11 Documentation. Oracle. URL: https://www.oracle.com/java/technologies/javase-jdk11-doc-downloads.html (дата звернення: 24.04.2024).

31. Packet Tracer. Cisco Packet Tracer Mobile 3.0. URL: https://www.packettracer.com/download/packet-tracer-mobile-3-0 (дата звернення: 30.04.2024).

32. Pearson IT Certification. Cisco Packet Tracer 101. URL: https://www.pearsonitcertification.com/articles/article.aspx?p=2167437 (дата звернення: 18.04.2024).

33. Network Academy. Introduction to Cisco Packet Tracer. URL: https://www.netacad.com/courses/packet-tracer/introduction (дата звернення: 26.04.2024).

34. The Engineering Projects. Cisco Packet Tracer: A Beginner’s Guide. URL: https://www.theengineeringprojects.com/2020/08/cisco-packet-tracer.html (дата звернення: 15.05.2024).

35. Computer Networking Notes. Cisco Packet Tracer: Installation and Setup. URL: https://www.computernetworkingnotes.com/cisco/packet-tracer.html (дата звернення: 20.04.2024).

36. University of Kentucky. Passive Optical Networks. URL: https://www.uky.edu/PassiveOpticalNetworks (дата звернення: 22.02.2024).

37. ResearchGate. Performance Analysis of Passive Optical Networks. URL: https://www.researchgate.net/publication/324563451_Performance_Analysis_of_Passive_Optical_Networks (дата звернення: 25.02.2024).

38. Lightwave. Advances in Passive Optical Networks. URL: https://www.lightwaveonline.com/fttx/pon-systems/article/14180894/advances-in-passive-optical-networks (дата звернення: 16.02.2024).

39. IEEE Xplore. Passive Optical Network (PON) Technologies. URL: https://ieeexplore.ieee.org/document/8303803 (дата звернення: 2.03.2024).

40. Baeldung. Guide to Networking in Java. URL: https://www.baeldung.com/java-networking (дата звернення: 11.05.2024).

41. Oracle. Java SE Specifications. URL: https://docs.oracle.com/javase/specs/ (дата звернення: 19.04.2024).

42. Stack Overflow. Java Ping Implementation. URL: https://stackoverflow.com/questions/11506380/how-to-ping-an-ip-address-using-java (дата звернення: 26.04.2024).

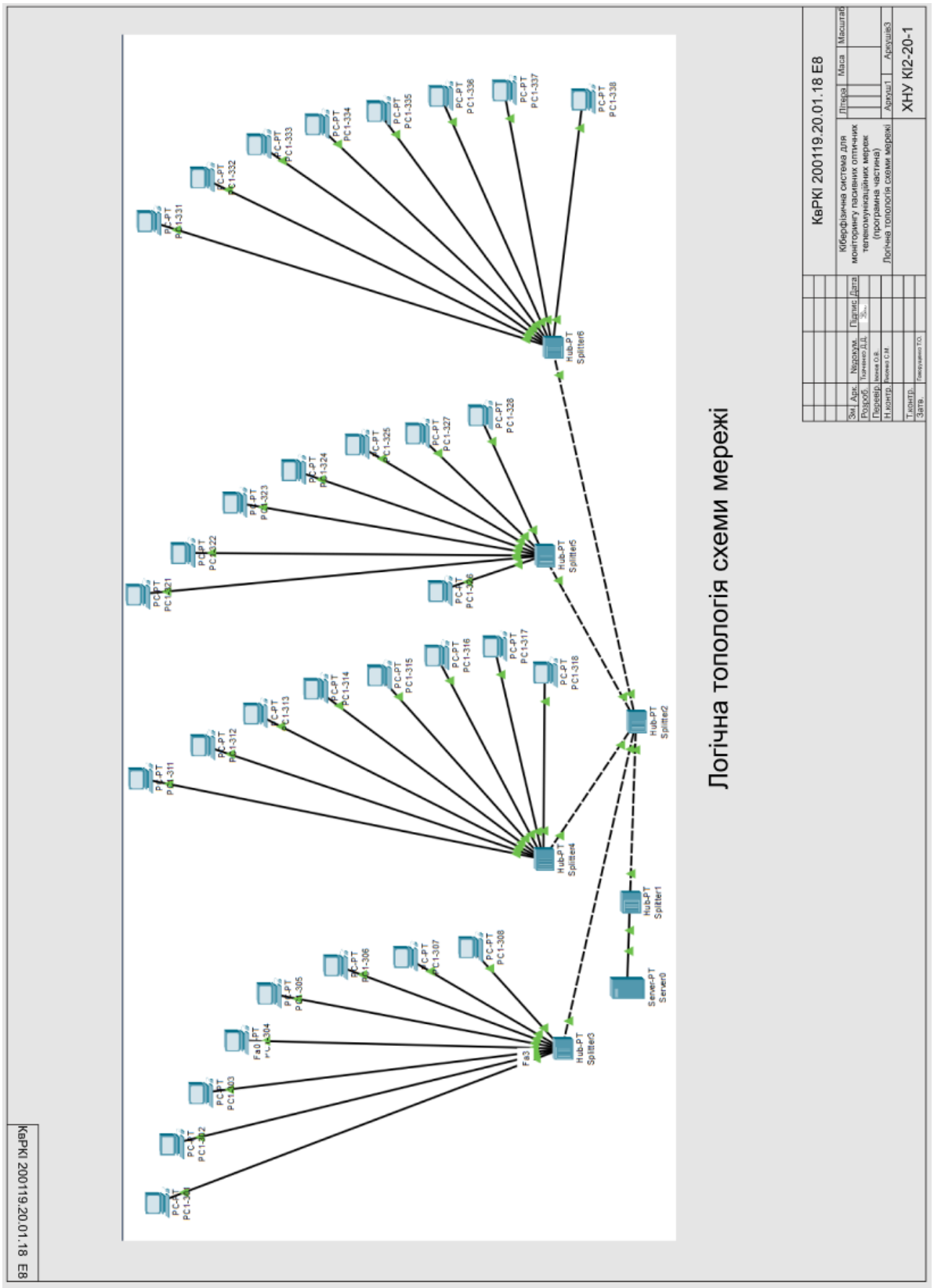
43. JavaWorld. Understanding Java Network Programming. URL: https://www.javaworld.com/article/2077322/understanding-java-network-programming.html (дата звернення: 19.05.2024).

44. GitHub. Ping in Java. URL: https://github.com/username/ping-in-java (дата звернення: 30.04.2024).

Додаток А

(обов’язковий)

Копія-креслення «Логічна топологія схеми мережі»



Додаток Б

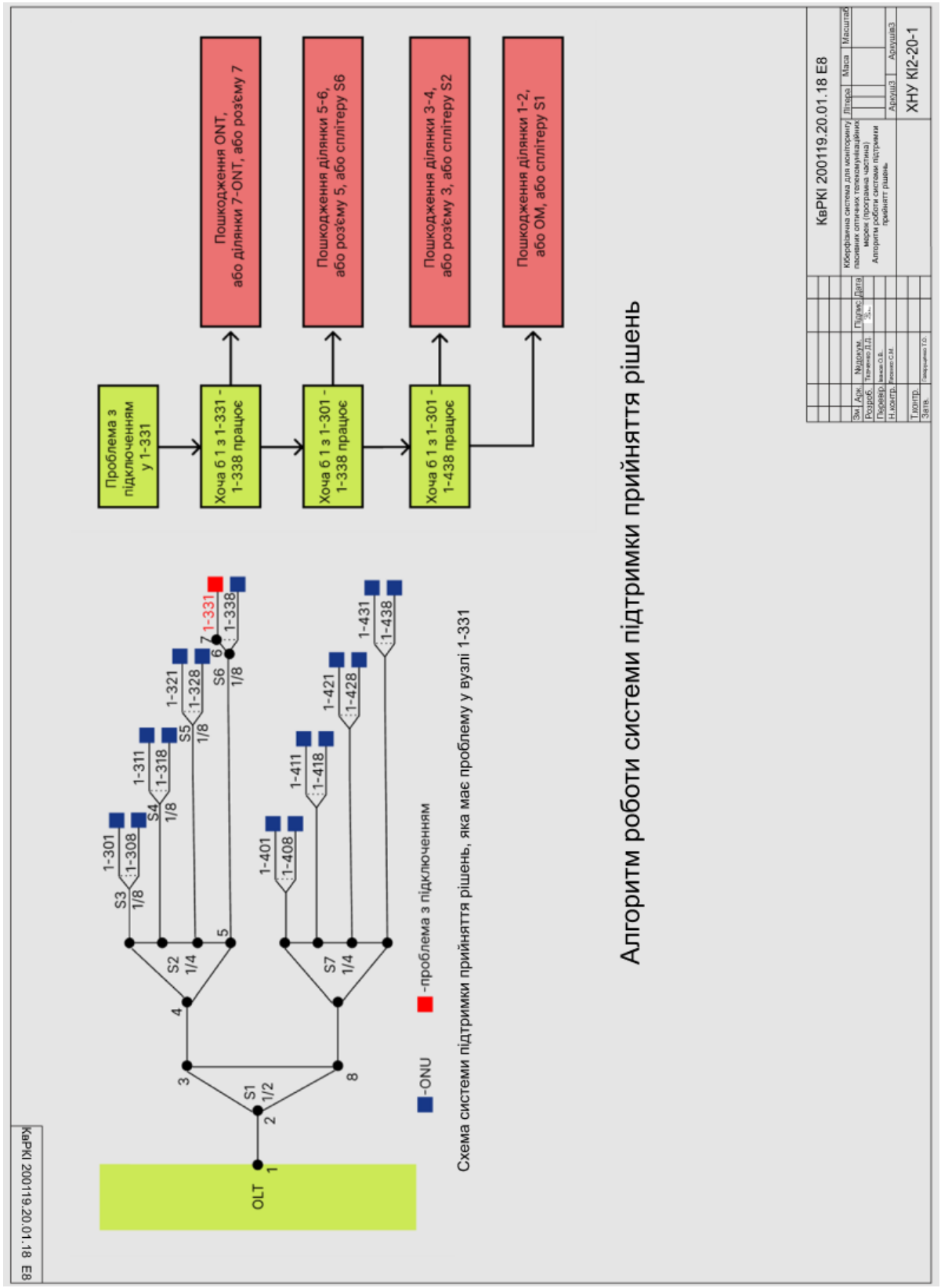
(обов’язковий)

Копія-креслення «Фізична топологія схеми мережі»

Додаток В

(обов'язковий)

Копія-креслення «Алгоритм роботи системи підтримки прийняття рішень»



Додаток Г

Лістинг коду системи підтримки прийняття рішень

```
package diplom;

/**
 *
 * @author dtkac
 */
import javax.swing.*;
import javax.swing.table.AbstractTableModel;
import java.awt.*;
import java.awt.event.ActionEvent;
import java.io.IOException;
import java.net.InetAddress;
import java.util.ArrayList;
import java.util.Date;
import java.util.List;

public class NetworkDiagnosticsTool extends JFrame {
    private JTable table;
    private List<Node> nodes;
    private NodeTableModel model;
    private JButton pingButton;
    private JButton disconnectButton;
    private JButton connectButton;

    public NetworkDiagnosticsTool() {
        super("Network Diagnostics Tool");
        setDefaultCloseOperation(JFrame.EXIT_ON_CLOSE);
        setSize(1000, 500);
        setLocationRelativeTo(null);

        nodes = createNodes();
        model = new NodeTableModel(nodes);
        table = new JTable(model);

        pingButton = new JButton("Ping Selected");
        pingButton.addActionListener(this::pingSelected);

        disconnectButton = new JButton("Disconnect Selected");
        disconnectButton.addActionListener(this::disconnectSelected);

        connectButton = new JButton("Connect Selected");
        connectButton.addActionListener(this::connectSelected);

        JPanel buttonPanel = new JPanel();
        buttonPanel.add(pingButton);
        buttonPanel.add(disconnectButton);
```

```
        buttonPanel.add(connectButton);

        getContentPane().add(new JScrollPane(table), BorderLayout.CENTER);
        getContentPane().add(buttonPanel, BorderLayout.SOUTH);
    }

    private List<Node> createNodes() {
        List<Node> nodeList = new ArrayList<>();
        int[][] splitters = {{301, 308}, {311, 318}, {321, 328}, {331, 338}};
        for (int[] range : splitters) {
            int segment = (range[0] - 301) / 10 + 1;
            for (int i = 1; i <= 8; i++) {
                String name = "Computer " + (range[0] + i - 1);
                String ip = "192.168." + segment + "." + i;
                nodeList.add(new Node(name, ip));
            }
        }
        return nodeList;
    }

    private void pingSelected(ActionEvent e) {
        for (Node node : nodes) {
            if (node.isSelected()) {
                if (node.isReachable()) {
                    node.setLastCheck(new Date());
                    JOptionPane.showMessageDialog(this, "Connection stable
for: " + node.getName());
                } else {
                    diagnoseProblem(node);
                }
            }
        }
        model.fireTableDataChanged();
    }

    private void disconnectSelected(ActionEvent e) {
        for (Node node : nodes) {
            if (node.isDisconnectSelected()) {
                node.setReachable(false);
                node.setLastCheck(new Date());
            }
        }
        model.fireTableDataChanged();
        JOptionPane.showMessageDialog(this, "Nodes disconnected. You can now
proceed with pinging to verify the status.");
    }

    private void connectSelected(ActionEvent e) {
        for (Node node : nodes) {
            if (node.isConnectSelected()) {
```

```
                node.setReachable(true);
                node.setLastCheck(new Date());
            }
        }
        model.fireTableDataChanged();
        JOptionPane.showMessageDialog(this, "Nodes connected. You can now
proceed with pinging to verify the status.");
    }

    private void diagnoseProblem(Node node) {
        int number = Integer.parseInt(node.getName().split(" ")[1]);
        int start, end;
        String splitter;
        String damageRange;
        String nextDamageRange;

        if (number >= 301 && number <= 308) {
            start = 301;
            end = 308;
            splitter = "S3";
            damageRange = "D5/6";
            nextDamageRange = "3-4";
        } else if (number >= 311 && number <= 318) {
            start = 311;
            end = 318;
            splitter = "S4";
            damageRange = "D7/8";
            nextDamageRange = "3-4";
        } else if (number >= 321 && number <= 328) {
            start = 321;
            end = 328;
            splitter = "S5";
            damageRange = "D9/10";
            nextDamageRange = "3-4";
        } else if (number >= 331 && number <= 338) {
            start = 331;
            end = 338;
            splitter = "S6";
            damageRange = "D11/12";
            nextDamageRange = "3-4";
        } else {
            return;
        }

        boolean segmentActive = false;
        boolean overallActive = false;

        for (Node n : nodes) {
            int nNumber = Integer.parseInt(n.getName().split(" ")[1]);
            if (nNumber >= start && nNumber <= end && n.isReachable()) {
```

```
                segmentActive = true;
            }
            if (n.isReachable()) {
                overallActive = true;
            }
        }

        if (segmentActive) {
            JOptionPane.showMessageDialog(this, "Possible damage to ONT, or
nearest connector-ONT, or respective connector");
        } else if (overallActive) {
            JOptionPane.showMessageDialog(this, "Possible damage to section
" + damageRange + ", or splitter " + splitter);
        } else {
            JOptionPane.showMessageDialog(this, "Warning: Possible damage to
section " + nextDamageRange + ", or splitter S2, or section 1-2, or OM, or
splitter S1. Check nodes from 301 to 438 or more");
        }
    }

    public static void main(String[] args) {
        SwingUtilities.invokeLater(()                ->                new
NetworkDiagnosticsTool().setVisible(true));
    }
}

class Node {
    private String name;
    private String ipAddress;
    private boolean selected;
    private boolean disconnectSelected;
    private boolean connectSelected;
    private Date lastCheck;
    private boolean reachable;

    Node(String name, String ipAddress) {
        this.name = name;
        this.ipAddress = ipAddress;
        this.selected = false;
        this.disconnectSelected = false;
        this.connectSelected = false;
        this.lastCheck = null;
        this.reachable = true; // By default, the node is reachable.
    }

    public String getName() {
        return name;
    }

    public String getIpAddress() {
```

```
        return ipAddress;
    }

    public boolean isSelected() {
        return selected;
    }

    public void setSelected(boolean selected) {
        this.selected = selected;
    }

    public boolean isDisconnectSelected() {
        return disconnectSelected;
    }

    public void setDisconnectSelected(boolean disconnectSelected) {
        this.disconnectSelected = disconnectSelected;
    }

    public boolean isConnectSelected() {
        return connectSelected;
    }

    public void setConnectSelected(boolean connectSelected) {
        this.connectSelected = connectSelected;
    }

    public Date getLastCheck() {
        return lastCheck;
    }

    public void setLastCheck(Date lastCheck) {
        this.lastCheck = lastCheck;
    }

    public boolean isReachable() {
        return reachable;
    }

    public void setReachable(boolean reachable) {
        this.reachable = reachable;
    }
}

class NodeTableModel extends AbstractTableModel {
    private final String[] columnNames = {"Computer Name", "IP Address",
"Last Check", "Reachable", "Select for Ping", "Select for Disconnect",
"Select for Connect"};
    private List<Node> nodes;
```

```
    NodeTableModel(List<Node> nodes) {
        this.nodes = nodes;
    }

    @Override
    public int getRowCount() {
        return nodes.size();
    }

    @Override
    public int getColumnCount() {
        return columnNames.length;
    }

    @Override
    public Object getValueAt(int rowIndex, int columnIndex) {
        Node node = nodes.get(rowIndex);
        switch (columnIndex) {
            case 0: return node.getName();
            case 1: return node.getIpAddress();
            case    2:    return    node.getLastCheck()    !=    null    ?
node.getLastCheck().toString() : "Never";
            case 3: return node.isReachable() ? "Yes" : "No";
            case 4: return node.isSelected();
            case 5: return node.isDisconnectSelected();
            case 6: return node.isConnectSelected();
            default: return null;
        }
    }

    @Override
    public void setValueAt(Object aValue, int rowIndex, int columnIndex) {
        Node node = nodes.get(rowIndex);
        if (columnIndex == 4) {
            node.setSelected((Boolean) aValue);
        } else if (columnIndex == 5) {
            node.setDisconnectSelected((Boolean) aValue);
        } else if (columnIndex == 6) {
            node.setConnectSelected((Boolean) aValue);
        }
    }

    @Override
    public Class<?> getColumnClass(int columnIndex) {
        return columnIndex == 4 || columnIndex == 5 || columnIndex == 6 ?
Boolean.class : String.class;
    }

    @Override
    public boolean isCellEditable(int rowIndex, int columnIndex) {
```

```
        return columnIndex == 4 || columnIndex == 5 || columnIndex == 6;
    }

    @Override
    public String getColumnName(int column) {
        return columnNames[column];
    }
}
```

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра КІ

ID перевірки:
1016377375

Дата перевірки:
20.06.2024 09:58:40 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
20.06.2024 10:00:25 EEST

ID користувача:
100005591

Назва документа: Ткаченко_Кіберфізична система для моніторингу пасивних оптичних телекомунікаційних ...

Кількість сторінок: 60 Кількість слів: 8903 Кількість символів: 69020 Розмір файлу: 4.42 MB ID файлу: 1016185813

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

2.99%
Схожість

Найбільша схожість: 1.14% з джерелом з Бібліотеки (ID файлу: 1011387865)

2.29% Джерела з Інтернету | 195 ..... Сторінка 62

1.88% Джерела з Бібліотеки | 155 ..... Сторінка 63

1.01% Цитат

Цитати | 3 ..... Сторінка 64

Посилання | 1 ..... Сторінка 64

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи | 2

Підозріле форматування | 20 сторінок

Thu Jun 20 08:58:36 EEST 2024, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 11%**

	Документ		Сумарний збіг по Базі Даних	
ID: 131676 Назва: БКР Кіберфізична система для моніторингу пасивних оптичних телекомунікаційних мереж (програмна частина) Додано в БД: 2024-06-20 Автора: Д. Д. Ткаченко Керівники: О. В. Іванов Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	56643	467	1130 (2%)	19 (4%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Ткаченко Денис Дмитрович

Тема: Кіберфізична система для моніторингу пасивних оптичних телекомунікаційних мереж (програмна частина)

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень ___3____ Кількість сторінок записки ___59___

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є створення системи підтримки прийняття рішень, для моніторингу пасивних оптичних телекомунікаційних мереж

2. Висновок про відповідність роботи дипломному завданню: Робота повністю відповідає поставленому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: В першому розділі кваліфікаційної роботи проведено дослідження предметної області (проаналізовано застосування цієї технології, основні елементи, типи й стандарти, а також розроблення і опис системи підтримки прийняття рішень) та виконано постановку задачі дослідження. В другому розділі кваліфікаційної роботи проведено аналіз вимог до системи моніторингу, а саме іхні функціональні, нефункціональні та аналітичні, було проведено дослідження принципів пінгування в кіберфізичних системах, було описано компоненти для організації системи підтримки прийняття рішень в Cisco Packet Tracer, в графічному вигляді та зроблено програмно-технічний засіб на мові програмування Java. В третьому розділі кваліфікаційної роботи виконано програмно-апаратну реалізацію системи підтримки прийняття рішень, а саме: реалізовано алгоритм та схему виконання СППР, при виникненні проблеми, а також проведено реалізацію різних сценаріїв дії СППР, для пошуку несправностей та моніторингу пасивних оптичних телекомунікаційних мереж.

4. Позитивні сторони роботи: виконана робота має високу практичну цінність.

5. Негативні сторони роботи: недостатня увага реалізації спроєктованої системи.

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації.

7. Відгук про роботу в цілому: Робота виконана на належному науково-технічному рівні.

8. Інші зауваження: _____

9. Оцінка дипломної роботи: добре (4.0/C)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) _____

Федуна Микола Васильович, к.т.н., доцент каф. АКІТмаР

_____

"20" 06 2024 р. _____(підпис)

Завідувачу кафедри КІІС
д-р.техн.наук, проф. Говорущенко Т. О.

Ткаченка Дениса Дмитровича
ПІБ здобувача вищої освіти

ФІТ, 4 курсу, групи КІ2-20-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

14 червня 2024 року

(підпис)

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Кіберфізична система для моніторингу пасивних оптичних телекомунікаційних мереж (програмна частина)

Автор: Ткаченко Денис Дмитрович

Спеціальність: 123– Комп'ютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Іванов Олексій Валентинович к.т.н., доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з 10-40 джерелами на один фрагмент речення;
4) в якості запозичень в окремих місцях системою зафіксовано послідовності чотирьохрозряних двійкових кодів, які є вхідними даними до великої кількості задач і не можуть розглядатися як об'єкт авторських прав і, відповідно, їх порушення;
5) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.(Тут текст можна і треба модифікувати)

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 2.99% і адресується до 350 першоджерел, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ О. В. Іванов

Гарант ОП _____ С.М. Лисенко

Завідувач кафедри КІІС _____ Т. О. Говорущенко