Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки

БАКАЛАВРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

" Комп'ютерна мережа для Березівського ліцею Чернівецької селищної ради "

08-54.БКР.001.00.000.ПЗ

Виконав: студент 2 курсу, групи 1КІ-23мс
спеціальності 123 — "Комп'ютерна інженерія"
освітня програма — "Комп'ютерна інженерія"
Абрамчук В.О.
(прізвище та ініціали)

Керівник к.т.н. доц. каф. ОТ
Колесник І.С.
(прізвище та ініціали)

Рецензент к.т.н доц. каф МБІС
Карпінець В.В.
(прізвище та ініціали)

Допущено до захисту
Завідувач кафедри ОТ
д.т.н., проф. Азаров О. Д.
«13» 06 2025 р.

Вінниця ВНТУ — 2025 рік

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки
Освітньо—кваліфікаційний рівень бакалавр
Галузь знань — 12 Інформаційні технології
Спеціальність— 123 Комп'ютерна інженерія
Освітня програма— Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедри ОТ проф., д.т.н.
_____Азаров О. Д.
"___"_____ 2025 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
Абрамчуку Володимиру Олександровичу

1 Тема роботи: Комп'ютерна мережа для Березівського ліцею Чернівецької селищної ради, керівник роботи Колесник Ірина Сергіївна, к.т.н., доцент кафедри ОТ, затверджено наказом №97 вищого навчального закладу від «_20_» _березня_ 2025 року.

2 Строк подання студентом роботи 13.05.2025р.

3 Вихідні дані до роботи: опис архітектури існуючих комп'ютерних мереж, програмне забезпечення Microsoft Visio, протокол VTP.

4 Зміст розрахунково-пояснювальної записки: вступ, загальні поняття та визначення, вибір компонентів для проектування мережі, вибір компонентів для проектування мережі, планування схеми комп'ютерної мережі ліцею, проектування комп'ютерної мережі засобами Cisco Pacet Tracer, висновки.

5 Перелік ілюстративного матеріалу: спроектована схема мережі школи, план приміщення другого поверху школи.

6 Консультанти розділів роботи приведені в таблиці 1.

Таблиця 1 — Консультанти роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1-3	к.т.н., доц. каф. ОТ Колесник І.С.	21.03.2025р.	13.06.2025р.
	відповідальний за н.к. Швець С.І.	14.05.2025р.	30.05.2025р.

7 Дата видачі завдання 07.03.2025 р.

8 Календарний план приведений в таблиці2.

Таблиця 2— Календарний план

з/п	Назва етапів виконання бакалаврського проекту	Строк виконання етапів роботи	Примітка
1	Постановка задачі для створення комп'ютерної мережі	21.03.25	
2	Огляд інформаційних джерел	21.03.25— 29.03.25	
3	Аналіз загальних понять та визначень	21.03.25— 29.03.25	
4	Вибір компонентів для проектування мережі	30.03.25— 11.04.25	
5	Розробка ПЗ комп'ютерної мережі ліцею	12.04.25— 26.04.25	
6	Оформлення пояснювальної записки та ілюстративного матеріалу	27.04.25— 07.05.25	
7	Аналіз виконання роботи. Висновки. Додатки	08.05.25	
8	Перевірка якості виконання бакалаврського проекту та усунення недоліків	14.05.25	

Студент Володимир Абрамчук

Керівник роботи к.т.н., доц. Ірина КОЛЕСНИК

АНОТАЦІЯ

УДК 004.9

Абрамчук В.О. Комп'ютерна мережа для Березівського ліцею Чернівецької селищної ради. Бакалаврська кваліфікаційна робота зі спеціальності 123 — комп’ютерна інженерія, освітня програма — системне програмування. Вінниця: ВНТУ, 2025, 85 с.

На укр.мові. Бібліогр.: 17 назв, рис. 26, табл. 9.

У бакалаврській кваліфікаційній роботі розроблено програмне забезпечення для проектування комп’ютерної мережі Березівського ліцею Чернівецької селищної ради. Комп’ютерна мережа ліцею розроблена з використанням топології «зірка». Комп'ютери, що входять до мережі, виконують широкий спектр функцій, основні з яких — це організація доступу до мережі, управління передачею інформації та її спільна обробка.

Рівень виконання завдання досягнуто за рахунок використання сучасного обладнання, зокрема, мережного адаптера, комутатора та завдяки виборові відповідного мережного програмного забезпечення та мережевого протоколу.

Ключові слова: комп’ютерна мережа, мережевий протокол, комутатор, маршрутизатор, топологія.

ABSTRACT

Abramchuk V.O. Computer network for Berezivsky Lyceum of Chernivtsi Village Council. Bachelor's thesis in specialty 123 - computer engineering, educational program - system programming. Vinnytsia: VNTU, 2025, 85 p.

In Ukrainian. Bibliography: 17 titles, fig. 26, table. 9.

Bachelor's qualification work is devoted to the development of software for designing a computer network for Berezivsky Lyceum of Chernivtsi Village Council.

Computers included in the network perform a wide range of functions, the main ones of which are the organization of access to the network, management of information transfer and its joint processing.

A high level of performance of the task was achieved due to the use of modern equipment, in particular, a network adapter, a switch, and due to the selection of the appropriate network software and network protocol.

Keywords: computer network, network protocol, switch, router, topology.

ЗМІСТ

ВСТУП

На сьогоднішній день у світі існує безліч комп'ютерів і більшість з них об'єднані в різні інформаційно-обчислювальні мережі, від малих локальних мереж в офісах, до глобальних мереж типу Internet.

Всесвітня тенденція до об'єднання комп'ютерів у мережі обумовлена безліччю важливих причин, таких як прискорення передачі інформаційних повідомлень, можливість швидкого обміну інформацією між користувачами, одержання і передача повідомлень не відходячи від робочого місця, можливість миттєвого одержання будь-якої інформації з будь-якої точки земної кулі, обмін інформацією між комп'ютерами різних фірм виробників працюючих під різним програмним забезпеченням.

Тому необхідно розробити принципове рішення питання з організації інформаційно-обчислювальної мережі на базі вже існуючого комп'ютерного парку та програмного комплексу, що відповідає сучасним науково-технічним вимогам, з урахуванням зростаючих потреб і можливістю подальшого поступового розвитку мережі у зв'язку з появою нових технічних і програмних рішень.

З появою локальних обчислювальних мереж (ЛОМ) з’явилася можливість об’єднувати персональні комп’ютери, які розташовані в різних робочих місцях, використовують спільні програмні засоби, устаткування та інформацію.

Робота, що пов’язана з викладанням, завжди вважалася дуже складною, але в той же час поважною діяльністю. З появою персональних комп'ютерів вони стали використовуваною технікою для дому, школи та офісу. Комп’ютерами можна користуватися як для виконання певної роботи, навчання, так і для проведення вільного часу з користю.

За допомогою ЛОМ учителю надається можливість дистанційного розповсюдження потрібної інформації, програмного забезпечення, вільний обмін файлами між персональними комп’ютерами та можливість нагляду за діями учнів.

Впровадження ЛОМ допоможе учителю як фізично так і морально, тому що процес розповсюдження матеріалу буде здійснюватися дистанційно, що зе-

кономить вільний час та зусилля, буде можливість проводити різного типу тестування для перевірки знань учнів за допомогою різного роду програмного забезпечення.

Всі виконані завдання учнів будуть зберігатися на ПК учителя або в базі ліцею, що допоможе мати вільний доступ до матеріалів для навчання.

Для реалізації поставленої мети комп'ютерна мережа повинна виконувати такі задачі:

— управління передачею інформації.

— спільну обробку інформації.

— забезпечення обчислювальними ресурсами.

— централізоване копіювання певних даних.

Обєкт дослідження — засоби та методи створення локальних мереж.

Предмет дослідження — процеси, які відбуваються при розробці локальних мереж.

Методи дослідження — аналіз інформаційних потоків, синтез отриманої інформації.

Практичне значення одержаних результатів: створено інформаційну систему для загальноосвітньої школи.

1 ЗАГАЛЬНІ ПОНЯТТЯ ТА ВИЗНАЧЕННЯ

1.1 Огляд існуючих методів та рішень

Комп'ютерна мережа — це сукупність різних комп'ютерів та пристроїв, що забезпечують обмін інформацією між комп'ютерами без використання будь-якої проміжної інфраструктури.

Комп'ютерна мережа — це географічно розподілена сукупність комп'ютерів, які можуть взаємодіяти один з одним через середовище передачі даних.

Комп'ютерні мережі забезпечують спільний шлях для даних. У мережі комп'ютери, на яких розміщені великі блоки даних, розподілені, і користувачі інших комп'ютерів у мережі отримують до них доступ. Інформація передається між комп'ютерами за допомогою електричних сигналів, які можуть бути як паралельними, так і паралельними. Взаємодія в мережі передбачає віддалений доступ до мережевих ресурсів і відбувається за допомогою технологій. Згідно з владою, комп'ютери в мережі поділяються на сервери та клієнти. [1]

Під час сортування мереж за країною вони визначають:

— персональні (Personal Area Network, PAN) — мережі, що забезпечують

— бездротові — функціонують за допомогою технологій Bluetooth або гарнітури на коротких відстанях (до 10 м);

— локальні (Network of Local Area, NAL) — представляють собою геометричну (іноді дуже велику) кількість комп’ютерів на відносно невеликій області;

— глобальні (Wide Area Network, WAN) – комп’ютерні мережі, що охоплюють великі території (тобто будь-яка мережа, комунікації якої з’єднують великі міста, регіони або навіть цілі країни та складається з десятків, сотень або навіть мільйонів комп’ютерів);

— муніципальні (MAN) – мережі муніципалітетів. [2]

1.2 Види архітектури мережі

Архітектура мережі визначає основні компоненти мережі, її загальну логічну організацію, апаратне забезпечення, програмне забезпечення та методи зв'язку. Архітектура також визначає принципи роботи та структуру програми. Існує три типи мережевих архітектур:

— інфраструктура терміналу — мейнфрейм;

— унікальна архітектура;

— клієнт-серверна архітектура.

Архітектура «термінал-хост» — це інформаційна мережа, в якій вся обробка даних виконується одним або групою віртуальних комп'ютерів. Розглянута архітектура складається з двох апаратних рівнів: апаратне забезпечення – це основний пристрій, який керує мережею, зберігає та зберігає дані; термінали, призначені для надсилання файлів на головний комп'ютер для організації сеансів та управління завданнями, введення даних для управління завданнями та відстеження результатів. Головний процесор зв'язується з вузлами за допомогою бездротових кабелів. Класичним прикладом архітектури нейронної мережі є алгоритм навігації перемиканням (SNA). Однорангова мережа — це мережа, в якій усі комп'ютери мають рівні привілеї. Таким чином, кожен комп'ютер може бути як сервером (надаючи свої ресурси для використання іншому комп'ютеру), так і клієнтом (використовуючи виділені йому ресурси).

Кожен користувач керує власними ресурсами комп'ютера. Однорангова мережа — це мережа «однорангових» комп’ютерів, кожен з яких має унікальне ім’я (ім’я користувача) та зазвичай пароль для доступу до мережі під час запуску комп’ютера. Ім'я користувача та пароль, встановлені власником комп'ютера через операційну систему (ОС). Мережеві комп'ютери можуть бути як клієнтами, так і серверами, оскільки всі мережеві комп'ютери сумісні. Однорангові мережі не мають централізованого контролю над розподілом ресурсів. Кожен комп'ютер може використовувати свої ресурси спільно з будь-яким комп'ютером у мережі. Кожен користувач віртуальної мережі також є адміністратором

мережі. Це означає, що кожен користувач мережі контролює доступ до ресурсів на своєму комп'ютері, а також вирішує, чи надавати іншим користувачам доступ до своїх ресурсів за допомогою простого запиту, чи захищати ці ресурси паролем. Однорангові мережі рідко з'єднують більше 10 комп'ютерів.

Однорангові мережі мають такі переваги:

— легкі в установці та обслуговуванні;

— окремі ПК не працюють на налаштованому сервері;

— користувачі мають можливість контролювати свої ресурси;

— вартість землі та зручність експлуатації;

— низька вартість;

— не вимагають присутності адміністратора;

— призначені для обмеженого кола користувачів.

Проблеми з одноранговим з'єднанням виникають, коли комп'ютери відключені від мережі. У цих випадках частина послуг, які вони надають, видаляється з мережі. Мережеву автентифікацію можна налаштувати лише для одного ресурсу одночасно, і користувач повинен запам'ятати стільки паролів, скільки є мережевих ресурсів. Ви помітите падіння продуктивності браузера під час доступу до спільного ресурсу. Одним з найбільших недоліків однорангових мереж є відсутність централізованого управління.

Архітектура сервер-сервер — це концепція мережі передачі даних, в якій більшість її ресурсів розміщені на серверах, що обслуговують своїх клієнтів. Загальна архітектура визначає два компоненти: сервери та клієнти.

Сервер — це компонент, який надає послуги іншим мережевим компонентам, використовуючи їхні ресурси. Сервіс — це процес обслуговування клієнтів. Сервер відповідає на запити клієнтів та контролює виконання їхніх завдань. Після завершення кожного завдання сервер надсилає результати клієнту, який відправив запит. Домен застосування в клієнт-серверній архітектурі визначається набором прикладних програм, за допомогою яких виконуються різні

прикладні процеси. Процес, який запитує клас програми за допомогою певних функцій, називається клієнтом. Це може бути програма або користувач.

Клієнти — це робочі процеси, які використовують ресурси сервера та надають правильні інтерфейси користувача. Профілі користувачів – це спосіб взаємодії користувача із системою або мережею. Клієнт є хостом і використовує електронну пошту або інші серверні служби. У цьому процесі клієнт запитує тип послуги, налаштовує сеанс, отримує потрібні йому результати та повідомляє про виконання завдання.

У мережах з виділеним файловим сервером, на виділеному автономному ПК встановлюється серверна, мережна операційна система. Цей ПК стає сервером. Програмне забезпечення (ПЗ), встановлене на робочій станції, дозволяє їй обмінюватися даними із сервером.

Мережі на базі серверів мають кращі характеристики й підвищену надійність. Сервер володіє головними ресурсами мережі, до яких звертаються інші робочі станції.

У сучасній клієнт-серверній архітектурі виділяється чотири групи об'єктів: клієнти, сервери, дані й мережні служби. Клієнти розташовуються в системах на робочих місцях користувачів. Дані в основному зберігаються на серверах. Мережні служби є спільно використовуваними серверами й даними. Крім того, служби управляють процедурами обробки даних [3].

Мережі клієнт-серверної архітектури мають наступні переваги:

— дозволяє створювати мережі з великою кількістю робочих місць, які можна виміряти сотнями;

— забезпечення централізованого управління обліковими записами користувачів, безпеки та доступу, що спрощує адміністрування мережі;

— швидкий та ефективний доступ до мережевих ресурсів;

— для доступу в мережу та отримання доступу до всіх ресурсів, до яких належать права користувача, користувачеві потрібен пароль.

Поряд з перевагами архітектури мережі клієнт-сервер існує ряд недоліків:

— збій сервера може зробити мережу непридатною, принаймні, призвести до втратит мережевих ресурсів;

— потрібні висококваліфіковані працівники для адміністрування;

— вищу вартість мереж та мережевого обладнання.

На основі вищесказаного структуру КМ можна представити у вигляді, поданому на рисунку 1.3.

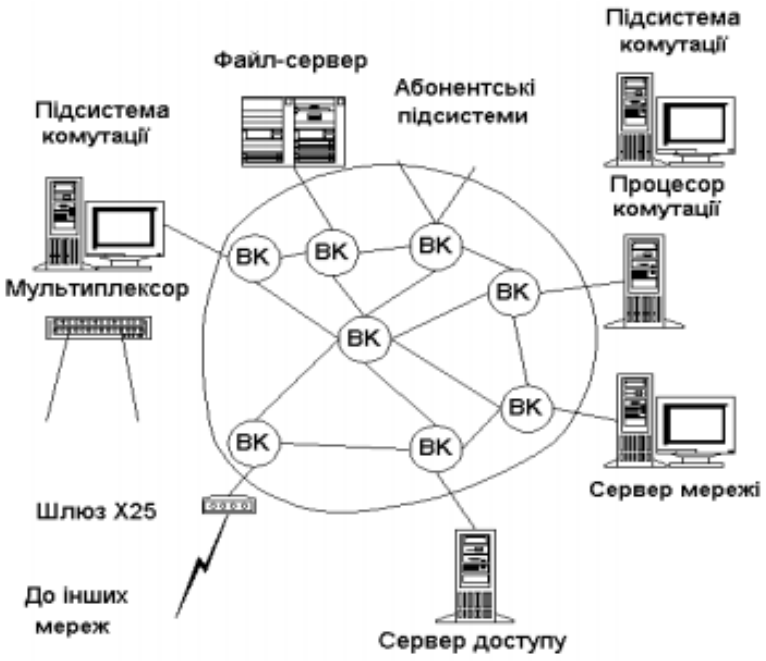

Рисунок 1.3 – Узагальнена структура КМ

1.3 Топологія обчислювальних мереж

Топологія — це структурний опис мережі, який включає розміщення пристроїв разом і їх з'єднання. Топологія мережі стосується фізичного розташування комп'ютерів, мережевих комутаторів та інших мережевих компонентів. Щоб спільно використовувати ресурси або виконувати інші мережеві функції, комп'ютери повинні з'єднуватися один з одним. Крім того, опис містить кілька стандартів, пов'язаних з прокладанням кабелів, взаємодією пристроїв керування та підключенням пристроїв.

Але просто підключити комп'ютер до кабелю, який з'єднує інші комп'ютери, недостатньо. Різні типи компонентів у поєднанні з різними мережевими

картами, мережевими системами та іншими компонентами вимагають різних конфігурацій комп'ютерів. Кожна мережева топологія вимагає кількох функцій.

Наразі існують такі типи топології: (рис. 1.4):

— Кільце;

— Шина;

— Зірка;

— Деревоподібна [4].

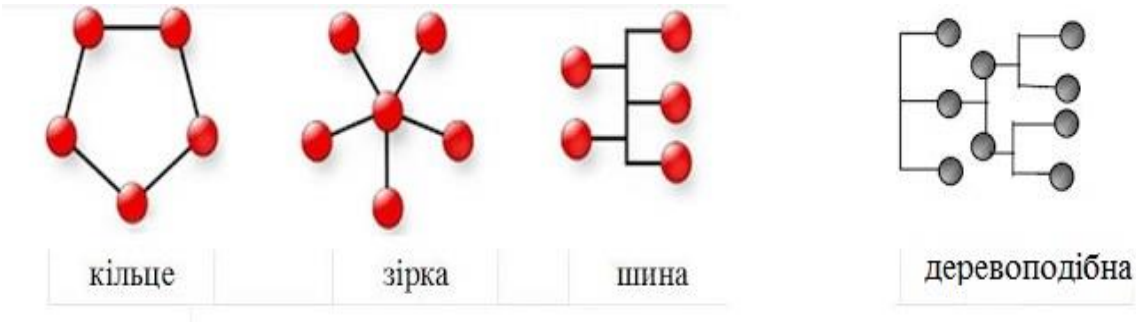

Рисунок 1.4 — Основні топології

Топологія «Шина» (або, як її ще називають, «загальна шина» або «магістраль») – всі ПК підключені до центральної мережі. Дані в такій мережі надсилаються на всі комп'ютери одночасно, тому кожен комп'ютер відповідає за те, чиє повідомлення він отримує. Тільки комп'ютер, на який надсилається повідомлення, може його обробити. [5]

Топологія «шина», самою своєю побудовою, визначає ідентичність мережевих ресурсів комп'ютерів, а також рівний статус усіх клієнтів щодо доступу до мережі. Комп'ютери на шині можуть передавати дані лише по одному, оскільки в цьому випадку існує одна лінія зв'язку. Якщо кілька комп'ютерів передають дані одночасно, це сповільниться через конфлікти, колізії. Шина завжди працює в режимі так званого напівхвильового обміну (в обох напрямках, але паралельно, а не одночасно).

Серед переваг мереж з шинною топологією можна назвати наступне:

— ефективне управління трафіком між підключеними пристроями;

— легше додати елемент «автобус», ніж зірку та стрілку, які мають бути розірвані;

— висока надійність, оскільки на роботу заготовок можуть вплинути несправні кабелі або канали, що з'єднують їх з верстатом.

Топологія шини також має деякі недоліки, а саме:

— існування мережі, що з'єднує всі елементи. Якщо мережа між двома вузлами виходить з ладу, то й уся мережа виходить з ладу. Щоб усунути цю ситуацію, нам потрібно захистити мережу або використовувати комутатори з двох причин;

— проблема точного призначення матеріалів компоненту, прикріпленому до машини. Це пов'язано з відсутністю діапазонів концентрацій, що ускладнює вирішення проблеми порівняння розмірів частинок.

У машинній топології немає чітко визначеного центрального елемента, через якого передається вся інформація, що підвищує його надійність (зрештою, якщо центр вийде з ладу, то вся система, що його керує, перестане функціонувати). Додавання нових клієнтів до шини дуже просте і зазвичай це можна зробити навіть під час роботи мережі. У більшості випадків використання шини вимагає мінімальної кількості бездротового з'єднання порівняно з іншими топологіями.

Топологія «кільце». Комп'ютери з'єднані послідовно та утворюють своєрідну паралельну систему. Отже, схема просто не може мати вільного кінця, на якому необхідно розмістити термінатор. Паралельна система використовується для передачі даних по мережі, а точніше, лише один комп'ютер може передавати дані одночасно, і дані передаються наступному комп'ютеру в ланцюжку. Після завершення передачі даних з'єднання роз'єднується, і передача даних продовжується по лінії до основного процесора. Важливою особливістю цього механізму є те, що кожен пристрій пропускає (приймає, підсилює) сигнал, тобто діє як передавач. Зниження сигналу у всьому кільці незначне; значущим є лише трафік між сусідніми комп'ютерами в ланцюзі. Сигнал у петлі послідовно проходить через усі комп'ютери мережі, тому, якщо навіть один з них (або його мережевий комутатор) вийде з ладу, це порушить загальну продуктивність мережі. Це великий недолік ліги. Підсилювач (MSAU – Multi-Station Access Unit)

дозволяє координувати завдання з технічного обслуговування, відключати несправних клієнтів, контролювати продуктивність мережі тощо. Він не виконує жодної обробки даних. Для кожного члена магістралі використовується блок з'єднання магістралі (TCU – Trunk Coupling Unit), який забезпечує автоматичне включення магістралі до магістралі, якщо вона підключена до магістралі та активована. Якщо клієнт відключається від послуги або має несправність, TCU автоматично відновить живлення без втручання цього клієнта. TCU живиться від джерела постійного струму (так званий «фантомний» струм) від абонента, який бажає підключитися до мережі. Хост також може відключитися від пристрою та виконати процедуру самотестування. Значення "фантом" жодним чином не впливає на потік інформації, оскільки потік у черзі не має параметра безпеки.

Топологія «зірка» — це топологія з фіксованим центром, до якого підключені всі інші клієнти. Вузли мережі можуть бути з'єднані один з одним одним із доступних способів, наприклад, через центральний або центральний вузол, утворюючи складнішу мережу або стаючи частиною інтегрованої мережі.

Як центральний вузол використовується будь-який мережевий пристрій з достатньою кількістю вузлів. У найпростішому випадку центральний вузол – це буфер, який завдяки своєму розміру дозволяє надсилати дані лише одному комп'ютеру одночасно. Водночас дані, отримані пристроєм, надсилаються безпосередньо на підключені до нього пристрої. Якщо дані від двох різних посилань надходять через одного й того ж одержувача одночасно, обидва пакети ігноруються.

Якщо говорити про швидкість «зірки» порівняно зі швидкістю комп'ютера, то низька швидкість центрального комп'ютера не впливає на продуктивність решти частини мережі, але будь-яке зниження швидкості краю робить мережу повністю неефективною. Тому слід вжити спеціальних заходів для підвищення ефективності центрального вузла та його мережевих ресурсів. Збій будь-якої мережі або коротке замикання в топології «зірка» впливає на перемикання

лише на один процесор, тоді як усі інші процесори можуть продовжувати функціонувати нормально. Хоча зірка є найдорожчою у використанні порівняно з іншими топологіями, завдяки своїй надійності та відносно низькій швидкості передачі даних, вона швидко стала стандартом.

Ієрархічна топологія — це топологія, в якій вузли організовані в групи (кластери) зі спільним контролером, а правила взаємодії між вузлами всередині кластера та між вузлами різних вузлів є ідентичними. Мережі з ієрархічною топологією мають швидшу маршрутизацію. У більшості випадків мережа керується високопріоритетним маршрутизатором, який ініціює розподіл трафіку в мережі. Такий підхід забезпечує своєрідну точку відліку для управління процесом помилок. Часто в КМ з ієрархічною топологією використовується метод побудови низькорівневої сітки. У низьковольтних конфігураціях пристрій на передній панелі гарнітури забезпечує безпосереднє керування пристроями під гарнітурою. Це зменшує навантаження на центральний вузол, такий як вузол А. У мережах з ієрархічною топологією існує потенціал для швидкої модернізації (зростання) вузлів мережі за допомогою більш ефективного вузла КМ.

Важливими характеристиками мережі з ієрархічною топологією є наступні:

— відносно швидка можливість пошуку проблем;

— гнучкі та адаптивні рішення, якщо потрібна модернізація мережі;

Ця топологія також має деякі недоліки:

— виникнення «вузьких місць» під час керування потоком пристроєм, який розташований найвище;

— мала надійність при відсутності технічного резервування;

— створення конфліктних ситуацій, пов'язаних зі втратою інформаціїї за напрямами «зверху вниз» та «знизу вгору».

На практиці іноді використовуються складні технології. До них належать, наприклад, топологія комірки, топологія сніжинки тощо. Топологія комірки була введена лише в останні роки і тому ще недостатньо застосовується на практиці; її привабливість полягає у відносній стійкості до перевантажень та

відмов. Завдяки надмірності шляхів, створених вузлами мережі, мережу можна маршрутизувати в обхід недійсних або активних вузлів. Хоча цей підхід характеризується складністю та комплексністю (протоколи є відносно складними з точки зору стандартів експлуатації), багато користувачів віддають перевагу стільниковим мережам, оскільки вони безпечніші за інші типи мереж.

1.4 Класифікація відповідно до використовуваних протоколів

На цьому етапі рівень розгортання протоколу поділяється на два підрівні:

— керування логічним каналом (Logical Link Control(LLC));

— контроль доступу до середовища (MAC).

Перший забезпечує контроль над логічною мережею та не втручається у фізичне середовище, тоді як другий забезпечує доступ до фізичного обладнання та діє на нього.

Таблиця 1.1 – Порівняльні характеристики топології обчислювальних мереж

Характеристики	Топологія		
	Зірка	Кільце	Шина
Вартість розширення	Незначна	Середня	Середня
Необхідність виключення при розширенні	Ні	Так	Ні
Під'єднання абонентів	Пасивне	Активне	Пасивне
Захист при відмовах	Незначний	Незначний	Висока
Розміри системи	Будь-які	Будь-які	Обмежені
Контроль помилок	Простий	Простий	Ускладнений
Захищеність від прослуховування	Добра	Добра	Незначна
Вартість під'єднання	Незначна	Незначна	Висока
Поведінка системи при високих навантаженнях	Хороша	Задовільна	Погана
Можливість роботи в реальному	Дуже хороша	Хороша	Погана
режимі часу			
Розводка кабелю	Добра	Задовільна	Добра
Планові витрати	Незначні	Середні	Незначні
Обслуговування	Дуже хороше	Середнє	Середнє
Характер відмови	Повна	Повна	Часткова

На ранніх етапах розвитку локальних мереж кожна окрема мережа могла передавати лише кадри однакового формату.

З часом, коли комп'ютерні мережі стали набагато складнішими та поєднали кілька локальних мереж з різними бездротовими мережами, виникла потреба реалізувати можливість одночасної передачі даних кількох бездротових маршрутизаторів через мережу. Для цього в кожному комп'ютері до коду додається спеціальна керуюча програма — програмне забезпечення, яке динамічно завантажується в пам'ять.

1.4.1 Функціональна реалізація багатопротокольних мереж на рівні з'єднання

На ранніх етапах розвитку локальних мереж кожна окрема мережа могла передавати лише кадри однакового розміру. З часом, коли комп'ютерні мережі стали набагато складнішими та поєднали кілька локальних мереж з різними бездротовими мережами, виникла потреба реалізувати можливість одночасної передачі даних кількох бездротових маршрутизаторів через мережу. Для цього в кожному комп'ютері до коду додається спеціальна керуюча програма — програмне забезпечення, яке динамічно завантажується в пам'ять. Наразі існує три підходи до організації взаємодії програмних драйверів на основі структур протоколів.

У 1989 році Microsoft та 3COM розробили специфікацію NDIS (Network Infrastructure Infrastructure), яка визначала, як мережева служба працюватиме з кількома компонентами. Він використовується в таких системах, як LAN manager, Windows for Workgroups, Windows 9x, Windows NT, Lantas-tic, служби маршрутизації. Існують схеми NDIS як для систем на 16 одиниць (NDIS 2.0), так і для систем на 32 одиниці (NDIS 3.0).

Новелл розробила та керує ODI (відкритою інфраструктурою каналів передачі даних), яка організована подібно до NDIS, але з іншим механізмом доставки.

Для мереж TCP/IP існують драйвери інтерфейсу, розроблені FTP Software відповідно до специфікації PDS (Packet Driver Design).

1.4.2 Протоколи керування доступом

Розглянемо структуру верхнього рівня запису протоколу — таблицю контролю доступу до фізичних даних. Основна функція цього рівня полягає в призначенні зв'язку окремим станціям, щоб пропускна здатність мережі зв'язку могла бути використана ефективно. Процедура організації доступу вузлів мережі до ресурсів називається процедурою доступу. Існує кілька способів доступу. Вони відрізняються: характером фізичного середовища — точками доступу до мережі та мережами через інтерфейс; характер управління — з централізованою та централізованою адміністрацією; тип доступу — особистий або делегований. Давайте розглянемо деякі методи доступу.

1.4.3 Тактові системи

Фундаментальний принцип проектування тактових систем полягає в розкладанні частоти всього часу передачі на фіксовану часову частоту — такти. Кожній станції присвоюється певний слот. Тактові системи мають такі недоліки:

— неефективне використання каналу: через нерівномірності навантаження з'являється багато порожніх слотів, швидкість передачі низька;

— чим більша кількість станцій, тим менша ефективність мережі, тому тактові системи не використовуються у великих мережах.

1.4.4 Метод опитування

Центральне керування передбачає метод вимірювання, який використовується в шинних або ефірних мережах (polled networks). У цьому випадку один із пристроїв, підключених до мережі, вважається контролером. Це захищає передавання. Найпростіший варіант централізованого керування реалізується на основі циклічного опитування. Контролер перехоплює (надсилає кадри) на па-

ралельно підключені пристрої. Вони займаються надсиланням інформації або через мережу, або через приватний фрейм, якщо інформації немає. Після отримання кадру контролер переходить до наступного пристрою тощо. Така шина поєднує два потоки: інформаційний та керуючий. Тестові мережі зазвичай невеликі. Вони використовуються в лабораторіях, інженерії, побуті та військовій справі. Недоліки цих систем полягають у наступному:

— наявність високого рівня контролю, навіть якщо клієнт не має інформації для передачі, але водночас працездатність пристроїв постійно контролюється;

— розмір мережі визначається розміром елемента керування; якщо він вийде з ладу, вся мережа вийде з ладу;

— мережа обмежена за кількістю абонентів; чим більше абонентів, тим довше триває опитування, а отже, тим вища пропускна здатність.

Прикладом мережі з опитуванням є мережа стандарту MIL 1553B. Різні протоколи пропонують різні вимоги до передачі. Складніші забезпечують захист від помилок підключення, автентифікацію підключення та автентифікацію за паролем. Далі ми розглянемо протоколи транспортного рівня.

Прикладами транспортних протоколів є:

— TCP / IP;

— NetBEUI;

— IPX / SPX;

— AppleTalk.

Наразі TCP/IP є найпоширенішим транспортним протоколом. Це базовий код Інтернету.

Набір протоколів TCP/IP (Модель відкритих систем Міністерства оборони США) поділяється на 4 категорії: доступ, транспорт, інтернет та доступ через контент. рівень доступу до мережі, рівень обслуговування, рівень обслуговування). Терміни, що використовуються для позначення фрагмента даних, що передаються, відрізняються, коли використовуються різні транспортні протоколи: TCP та UDP. На рівні застосунку це мережевий (TCP) та обмін повідом-

леннями (UDP); у транспорті – сегмент та компанія. Як і в моделі OSI, високорівневі дані складаються з низькорівневих пакетів даних, таких як домен (TCP) або пакет (UDP), з даними та потоковими заголовками, визначеними в полі даних дейтаграми. [4]

Реалізований рівень: протоколи програмного рівня TCP/IP визначають спосіб організації взаємодії між процесами (програмами) різних мережевих комп'ютерів та форми обміну інформацією для цієї взаємодії. Існує два типи розгортання застосунків: клієнтський та серверний. Протоколи програмного рівня зосереджені на певних функціях програмного забезпечення. Серед традиційних сервісів, що пропонують протоколи прикладного рівня з родини TCP/IP, найпопулярнішими сьогодні є електронна пошта – SMTP та POP3, передача файлів через FTP та TFTP, віддалена мережа – TELNET та інші. З середини 1990-х років активно розвиваються інтернет-сервіси на основі технології WWW, що базуються на протоколі передачі відкритого тексту HTTP. Сьогодні популярні послуги IP-телефонії базуються на специфікаціях IETF, які включають певні стандарти для конфігурації, передачі та мережевих специфікацій, такі як маркування SIP, сигналізація RTP та RTCP у реальному часі, ресурси RSVP, рекомендації ITU H.323 та багато інших.

Протоколи транспортного рівня TCP/IP забезпечують транспортні послуги для операцій маршрутизації. Основними компонентами транспортного рівня TCP/IP є протокол керування передачею (TCP) та протокол користувацьких дейтаграм (UDP). Механізми доставки цих протоколів дуже різні. UDP забезпечує безз'єднувальні застосунки. Однак це не гарантує їх доставку. Протокол TCP забезпечує передачу байтових пакетів шляхом встановлення первинного дуплексного з'єднання передачі (каналу приймача) між TCP-портами мережевого маршрутизатора. Для вирішення проблеми передачі створені протоколи TCP та UDP, які налаштовують свої 20-байтові та 8-байтові заголовки під час передачі даних відповідно. Кожен прикладний процес взаємодіє з модулем транспортного рівня TCP або UDP через інший порт, що дозволяє системам легко ідентифікувати прикладний процес. Ці параметри встановлюються від нуля. Коли

ви надсилаєте запит клієнта до серверної програми, параметр маршрутизації на основі тому або домену вимагає номера порту сервера програм та програмних модулів протоколу сервера. Для цього в заголовку пакета протоколу потоку передачі передбачено два поля – «порт отримання» та «порт відправлення», кожне з яких має розмір 2 байти. Номери портів TCP та UDP для модулів серверних застосунків стандартизовані IETF. Для цього використовуються числа в діапазоні від 1 до 1023, наприклад, вузол TCP-сервера зазвичай зв'язується з HTTP-вузлом з номером порту 80. Клієнтський вузол TCP або UDP зв'язується з будь-яким вузлом розширення з портом, який призначає незалежний номер, більший за 1023.

Міжмережевий рівень: протоколи мережевого рівня TCP/IP є сполучною ланкою між різними архітектурними мережами тощо. Основними компонентами технологічного рівня TCP/IP є мережевий рівень IP та його залежності: рівень адрес ARP; Протокол зворотної адресації RARP (Reverse ARP); Протокол керуючих повідомлень Інтернету (ICMP) надсилає повідомлення мережевому вузлу про помилки маршрутизації під час відправлення пакета.

NetBEUI — це протокол, що використовується в однорангових мережах. Це давня стандартна реалізація NetBIOS, яка була представлена корпорацією Microsoft та впроваджена в сімействі операційних систем Windows. Ще однією варіацією рівня NetBIOS є протокол NetBIOS поверх TCP/IP, який є складнішим за NetBEUI, але ефективнішим у випадку TCP/IP.

NetBEUI забезпечує високу пропускну здатність, але через кілька проблем, таких як перевантаження трафіку та високий рівень шуму у великій мережі, NetBEUI не може бути легко використаний у невеликих локальних мережах (IBM розробила NetBEUI для локальних мереж з кількістю співробітників близько 20 200). Мережі, засновані на фреймворку NetBEUI, легко впроваджувати, але складно підтримувати.

IPX/SPX був дуже популярним протоколом передачі в середині 1990-х років, головним чином завдяки операційній системі Novell NetWare. За застосуванням IPX/SPX наближається до TCP/IP, включаючи зв'язок у цифрових ме-

режах. Сьогодні IPX/SPX поступово замінюється TCP/IP. Навіть найновіші версії операційної системи NetWare вже використовують TCP/IP як основний протокол.

AppleTalk багато в чому схожий на IPX/SPX. Розроблений для зв'язку між програмами Apple для Macintosh, цей протокол використовується в мережах робочих груп і поступово поступається місцем TCP/IP.

Версія AppleTalk, що відповідає сеансовому рівню моделі OSI, включає п'ять модулів, що забезпечують швидку передачу даних, логічне перетворення імені в адресу, доступ до шини, реконфігурацію пакетів тощо. Основний протокол сеансового рівня називається протоколом передачі даних AppleTalk (ADSP). Протокол ADSP забезпечує безпечні двосторонні з'єднання. Ця гнучкість досягається шляхом встановлення логічного з'єднання (сеансу) між двома конкуруючими процесами на хост-машині. Протокол ADSP дозволяє встановити це з'єднання шляхом моніторингу доступу до даних, зміни пакетів та надсилання пакетів автентифікації. Номери вузлів використовуються для визначення зв'язку між вузлами. Після встановлення з’єднання дві системи можуть розпочати обмін даними. Наступним класом протоколів сеансу AppleTalk є протокол сеансу AppleTalk (ASP). ASP забезпечує надійну передачу даних через безпечну автентифікацію сеансу та надає доступ через службу транспортного рівня AppleTalk Transport Protocol (ATP). Протокол маршрутизації AppleTalk (AURP) використовується у великих мережах AppleTalk і в основному використовується для маршрутизації та підтримки обміну даними між пристроями маршрутизації, включаючи зовнішні шлюзові пристрої. Крім того, сеансова клавіатура AppleTalk має протокол переносного доступу (PAP). Хоча протокол PAP спочатку був створений для контролю доступу до мережевих портів, його можна використовувати для обміну даними між різними пристроями. Між пристроями встановлюється двосторонній зв'язок з одночасним моніторингом контролю даних та контролю пріоритетних пакетів. Нарешті, останнім протоколом сеансового рівня є протокол області даних AppleTalk (ZIP). Поштовий індекс надає спосіб систематичного групування окремих мережевих пристроїв за допомогою

«зручних» імен. Такі логічні групи називаються регіонами. У віртуальній мережі комп'ютери можуть використовувати кілька мереж, але зазвичай вони згруповані в одній області. Однак у невеликих, випадково розподілених мережах ми можемо ізолювати окрему область. П'ять стандартних протоколів AppleTalk дозволяють клієнтам налаштовувати логічні з'єднання та обмін даними між комп'ютерами незалежно від відстані між ними.

Версія AppleTalk, що відповідає сеансовому рівню моделі OSI, включає п'ять модулів, що забезпечують високошвидкісну передачу даних, логічне перетворення імені в адресу, доступ до шини, пересилання пакетів тощо. Протокол ADSP забезпечує безпечні двосторонні з'єднання. Ця гнучкість досягається шляхом встановлення логічного з'єднання (сеансу) між двома конкуруючими процесами на хост-машині. ADSP дозволяє встановити це з'єднання шляхом моніторингу доступу до даних, комутації пакетів та передачі пакетів. Номери вузлів використовуються для визначення зв'язку між вузлами. Після встановлення з’єднання дві системи можуть розпочати обмін даними. Ще одним рівнем протоколу сеансу AppleTalk є протокол сеансу AppleTalk (ASP). ASP забезпечує надійну передачу даних за допомогою пріоритетної автентифікації сеансу та надає доступ до служби транспортного рівня AppleTalk Transport Protocol (ATP). Протокол автентифікації AppleTalk Authentication Protocol (AURP) використовується в основних мережах AppleTalk і в основному використовується для автентифікації та підтримки обміну даними між хост-пристроями, включаючи зовнішні шлюзові пристрої. Крім того, сеансова клавіатура AppleTalk має протокол переносного доступу (PAP). Хоча PAP спочатку був створений для контролю доступу до мережевих машин, його можна використовувати для обміну даними між різними пристроями. Двосторонній зв'язок між пристроями встановлюється під час керування потоком даних та керування пріоритетними пакетами. Нарешті, останній код рівня сеансу — це код зони даних AppleTalk.

Модель OSI

Протокол ZIP забезпечує механізм логічного групування окремих мережевих пристроїв за допомогою «зручних» імен. Такі логічні групи називаються регіонами. У віртуальній мережі комп'ютери можуть використовувати кілька мереж, але зазвичай вони згруповані в одній області. Однак у менших нішових тунелях ґрунт можна ущільнити. П'ятисторонні протоколи AppleTalk дозволяють клієнтам встановлювати логічні з'єднання та обмін даними між комп'ютерами незалежно від відстані між ними.

Модель OSI (EMI) (Елементарна інформаційна модель для інтеграції відкритих систем, 1978) — це абстрактна мережева модель для моделювання зв'язку та мережевого протоколу. Він представляє шлях мережевого рівня. Кожен рівень є невід'ємною частиною процесу співпраці. Завдяки цій платформі підтримка мережі та програмного забезпечення стає набагато простішою, швидшою та зрозумілішою. Наразі основним стандартом протоколу, що використовується, є TCP/IP, розробка якого не пов'язана з моделлю OSI та також була здійснена до її прийняття. Він не був реалізований за часів існування моделі OSI, і зрозуміло, що ніколи не буде реалізований. Сьогодні використовується

лише кілька версій моделі OSI. Вважається, що модель занадто складна, і її впровадження займе багато часу. Деякі експерти також стверджують, що історія моделі OSI є прикладом невдалого та непослідовного підходу до проектування.

1.5 Стандарт локальної мережі Ethernet

Ethernet — це сімейство технологій передачі пакетних даних для комп'ютерних мереж. Стандарти Ethernet визначають дротові та електричні з'єднання на фізичному рівні, форму кадру та стандарти контролю доступу до даних на програмному рівні моделі OSI (Open Systems Interconnection). Ethernet загалом описується групою стандартів IEEE 802.3. Ethernet став найпоширенішою технологією локальних мереж у середині 1990-х років, замінивши старі технології, такі як Arpanet та Token Ring.

Стандартний протокол Manchester-P використовується для надсилання даних через мережу Ethernet. У цьому випадку один коефіцієнт дорівнює нулю, а інший дорівнює нулю, тобто коефіцієнт варіації ніколи не дорівнює нулю. За відсутності передачі енергія в мережі дорівнює нулю. Гальванічний ланцюг складається з серії адаптерів, резисторів та обмежувачів. У цьому випадку мережеве обладнання гальванічно ізольоване від решти обладнання за допомогою трансформаторів та ізольованого джерела живлення, яке безпосередньо підключене до мережевого обладнання.

Доступ до мережі Ethernet здійснюється за допомогою механізму CSMA/CD (Continuous Compression Controlled Multiple Access), що гарантує можливість повної співпраці між абонентами. Мережа використовує пакети змінної довжини. Довжина кадру Ethernet (тобто пакета без префікса) повинна бути щонайменше 512 бітових циклів або 51,2 мкс. Пропонуються індивідуальні, групові та консультаційні сесії.

На комутаторі Ethernet відображаються такі поля.

Префікс складається з 8 байтів, перші сім з яких – це кадр 10101010, а останній восьмий – кадр 10101011. У стандарті IEEE 802.3 цей останній біт називається роздільником початку кадру (SFD) і представляє сегмент кадру.

Адреса клієнта (хоста) та адреса призначення (одержувача) мають довжину по 6 байтів кожна. Ці групи адрес налаштовуються клієнтом.

Поле керування (L/T - Довжина/Тип) містить інформацію про довжину поля даних. Він також може визначити тип використовуваного протоколу. Загальновизнано, що якщо значення цієї таблиці не перевищує 1500, то вона визначає довжину рядка даних. Якщо значення більше за 1500, то воно визначає тип кадру. Поле керування керується програмно.

Він повинен мати діапазон даних від 46 до 1500 байтів даних. Якщо пакет повинен містити менше 46 байтів даних, поле даних розпаковується на вхідні байти. Згідно зі стандартом IEEE 802.3, у буфері пакетів виділяється поле доповнення (padding data – недійсні дані), яке може мати довжину нуль, коли даних достатньо (більше 46 байт).

Розділ кешу керування (FCS - Frame Control Series) містить 32-бітний контролер схеми (CRC - Circuit Controller) і використовується для контролю цілісності передачі сигналу.

Таким чином, мінімальна довжина кадру (непрефіксований пакет) становить 64 байти (512 бітів). Саме це значення пояснює подвійну затримку реплікації по мережі з 512-бітними інтервалами (51,2 мкс для Ethernet, 5,12 мкс для Fast Ethernet). Правило припускає, що пріоритет може знижуватися під час проходження пакета через різні мережеві пристрої, тому він не враховується. Максимальна довжина кадру становить 1518 байт (12144 біти, тобто 1214,4 мкс для Ethernet, 121,44 мкс для Ethernet відповідно). Це важливо для вибору відповідного балансувальника мережевого навантаження та оцінки загальної продуктивності мережі. Ethernet, мережева технологія зі спільним середовищем передачі, коаксіальним кабелем, розвивалася разом зі зміною потреб користувачів. Відповідаючи найновішим вимогам до кабельних систем, стандарт Ethernet тепер поширений на мережі передачі даних, такі як оптичне волокно та неекранована оптоволоконна мережа. Рушійними силами переходу до цих середовищ є щільна та густа мережа місцевих спільнот у комерційних, урядових та інших органі-

заціях, а також необхідність ефективного та економічно ефективного управління та експлуатації цих мереж.

На основі аналізу ми обрали архітектуру клієнт-сервер, оскільки вона забезпечує централізоване управління, дозволяє підключатися великій кількості користувачів, а також забезпечує швидкий та ефективний доступ до ресурсів. У нашому випадку краще було б використовувати плату "Зірка", яка як середовище передачі даних використовує кабель "вита пара", що повністю відповідає вимогам швидкості передачі та надійності розроблюваних мережевих додатків.

2 ВИБІР КОМПОНЕНТІВ ДЛЯ ПРОЕКТУВАННЯ МЕРЕЖІ

2.1 Принципи ієрархічного проектуваня мерж

Проектування будь-якої мережі має починатися з найнижчого рівня – фізичних засобів передачі інформації. Загалом, проектування фізичного годинника стосується бітів і байтів, вибору найкращої пропускної здатності для ліній зв'язку, мережі передачі даних та методу передачі даних, а також отримання даних з мережі. Усі вищезазначені питання мають велике значення, оскільки блокування каналів зв'язку значною мірою відповідає за порушення передачі та зв'язку через мережу.

Часто проблеми фізичного рівня призводять до змін у мережі, що вимагає оновлення рівня маршрутизації. Однак топологія (структура) мережі має непропорційно більший вплив на її безпеку, ніж вибір між технологіями ATM або Frame Relay для розміщення з'єднань на периферії мережі. Правильно обрана топологія є основою всіх високопродуктивних мереж. Щоб зрозуміти це твердження, спробуємо відповісти на питання: чому труби замерзають? Проста відповідь така: мережі зависають через невідповідність протоколів маршрутизації. Оскільки всі маршрути маршрутизації вводять трафік під час налаштування (жоден вузол маршрутизації не може надати точну інформацію про маршрутизацію під час налаштування карти маршруту), дуже важливо продовжити процес налаштування якомога швидше після виникнення неочікуваних змін у мережі. Час, який протокол маршрутизації потребує для завершення процесу моделювання, залежить від двох факторів:

— кількість шляхів, що беруть участь у процесі розподілу;

— обсяг інформації, згенерованої аналітиками.

Кількість вузлів, що беруть участь у процесі оновлення, залежить від розміру області мережі, на яку впливає зміна топології. Додати ("умова", комбінація) дозволяє приховати певну інформацію про маршрутизацію від браузерів. В

результаті ми маємо зменшення обсягу інформації, що генерується маршрутизаторами, оскільки маршрутизатори без інформації про пункт призначення не повинні вносити зміни до таблиці маршрутів 46, коли маршрут до пункту призначення змінюється або коли мережа пошкоджена, що призводить до недоступності. Обсяг інформації, яку пілоти обробляють під час визначення найкращого маршруту до пункту призначення, залежить від загальної кількості цих маршрутів. У зв'язку з цим агрегація також дозволяє зменшити обсяг інформації, що генерується маршрутизаторами при зміні топології мережі. Таким чином, паралелізм є ключовою концепцією, яка дозволяє зменшити кількість людей, залучених до розробки програмного забезпечення, та обсяг інформації, яку вони генерують. Крім того, інтеграція залежить від правильного вибору проектів розвитку, що з самого початку накладає обмеження на їхню реалізацію. Успішний проект мережі завжди базується на ретельно спланованій топології, яка формує основу мережі. Поганий дизайн мережі майже не залишає можливості вибрати найкращі "спеціально розроблені" програми маршрутизації. Хоча багато людей намагаються вирішити мережеві проблеми, спричинені невдалим вибором топології та комутаційних рівнів, за допомогою ефективніших маршрутизаторів, різноманітної оптимізації комутаційних рівнів або оптимізації комутаційних шляхів, практика показує, що ніщо не замінить погано спроектований мережевий рівень.

Таким чином, існує потреба в інформаційно-обчислювальній мережі для університету, щоб сприяти навчанню, підвищувати його якість та зменшувати витрати. Також мережа, що розробляється, захистить інформацію від несанкціонованого доступу та забезпечить справедливе використання ресурсів.

Проект мережі складається з наступних частин:

— розробка плану будівництва;

— вибір технології мережі;

— розрахунок необхідної кількості мережевих пристроїв та мережеві ресурси.

2.2 Вибір кабельної системи

Одним з найважливіших завдань у проектуванні мережі є вибір мережевих пристроїв для забезпечення її надійності та уникнення перевантаження.

Вибираючи кабель, слід враховувати необхідну довжину, а також захист від зовнішнього впливу та рівень самоізоляції.

Найпоширенішими типами підключених середовищ даних у локальній мережі є три основні схеми підключення: за допомогою волоконно-оптичного кабелю, кабелю «вита пара», чи коаксіального кабелю.

Коаксіальний кабель — це електричний кабель, основним призначенням якого є передача сигналу в різних галузях техніки.

Оптоволоконний кабель – конструкція, що складається з одного або кількох оптичних кабелів (оптичних волокон), ізольованих один від одного та укладених в оболонку. Окрім перемикачів та вимикачів, він може включати дисплей, кабелі живлення та іншу периферію. Це також фізичний пристрій, що складається з кількох оптичних волокон, оточених загальним захисною оболонкою і використовуваних для передачі світла.

Вита пара — це тип мережевого кабелю з однією або кількома парами струмопровідних проводів, скручених разом (з мінімальною кількістю проводів на довжину пари) для зменшення взаємних наведень під час передачі струму та покритих пластиковою ізоляцією. Він використовується як мережевий пристрій у багатьох технологіях, таких як Ethernet, ARCNet та Token Ring. Наразі, завдяки своїм невеликим розмірам та легкій вазі, він є найбільш широко використовуваним для побудови локальних мереж. Комп'ютер підключається до мережевих пристроїв за допомогою порту 8P8C. Він підтримує передачу даних на відстань до 100 метрів [6].

Вибір кабельної системи для мережі майбутнього залежить від:

— швидкості передачі інформації по локальній мережі;

— вартості кабелю;

— інтенсивності трафіку;

— методу управління обміном в мережі;

— захищеності від зовнішньої корозії;

— відстані між робочими місцями.

Під час створення мережі найкращим варіантом було б використання бездротової схеми п’ятої категорії, представленої на рисунку 2.1. Кабель надійний, простий у підключенні та дешевий, можливість передачі даних через кабель важлива для нормальної роботи мережі.

Рисунок 2.1 - Кабель типу вита пара

2.3 Вибір мережного адаптераера

Мережевий адаптер — це апаратний пристрій, який дозволяє комп’ютеру взаємодіяти з іншими мережевими пристроями. У наш час, особливо в персональних комп'ютерах, мережеві карти часто інтегруються в материнські плати для зручності та зниження загальної вартості всього комп'ютера. [7]

Щоб побудувати цю мережу, потрібно використовувати мережеву карту, яка дозволяє комп'ютеру взаємодіяти з іншими мережевими пристроями. У нашому випадку для підключення до мережі буде використовуватися внутрішня мережева карта TP-LINK TG-3468 – недорога та проста у використанні.

Ключові характеристики:

— інтерфейс: PCI Express.

— швидкість передачі даних: 10/100/1000 Мбіт/с.

— стандарт: гігабітний інтернет.

— деталі безпеки: фільтрація портів Ethernet, визначених VLAN.

— додаткові функції: автоматичне узгодження NWay ANSI / IEEE 802.3, керування трафіком IEEE 802.3x (у разі повної пропускної здатності), бездротове підключення IEEE 802.1p, бездротова маршрутизація, підтримка SNMP v1[8].

2.4 Вибір Вибір комутатора

Мережевий комутатор (від англійського слова «Switch») — це пристрій, основним призначенням якого є підключення кількох мережевих пристроїв комп'ютера в межах одного блоку. Зазвичай, маршрутизатор використовується для з'єднання кількох комп'ютерів у мережі [9].

Для побудови мережі вибираємо роз'єм TP-LINK TL-SF1016D (рисунок 2.3). Він має 16 портів Fast Ethernet 10/100, а також є надійним, дешевим та підтримує широкий спектр застосувань. У школі 28 ПК, тому залежно від цього та розподілу мережі, потрібно 3 комутатори. Вибраний клас "Зірка" буде замінено класом "Дерево", тобто він матиме три "Зірки".

Ключові характеристики:

— Кабель RJ45 10/100 Мбіт/с з автоматичним інтерфейсом MDI/MDIX;

— Здатність реагувати у стані напівроізгріву;

— підтримка самонавчання MAC-адрес;

— Технологія Green Ethernet (енергоефективність до 70%);

— керування стандартом IEEE 802.3x;

— Функція введення за замовчуванням.

— Маршрутизатор – це мережевий пристрій, який з’єднує різні комп’ютерні мережі та контролює обмін даними між ними, а також приймає рішення щодо пересилання пакетів мережевого рівня (3-й рівень моделі OSI) між різними вузлами мережі [11].

— Для підключення до Інтернету було обрано пристрій TP-LINK Archer A64 (рисунок 2.4). Його характеристики ідеально підходять для роботи з технологією Wi-Fi.

— Ключові характеристики:

— швидкість Wi-Fi 1167 Мбіт/с.;

— частота роботи Wi-Fi – 2,4 ГГц, 5 ГГц.;

— WAN-порт Ethernet;

— швидкість LAN портів 1 Гбіт/с.;

— інтерфейси: 4 порти LAN 10/100/1000 Мбіт/сек, 1 порт WAN 10/100/1000 Мбіт/сек;

— бездротові можливості: 802.11b, 802.11g, 802.11n, 802.11a, 802.11ac.;

— підтримка протоколів: PPPoE, IPsec, L2TP, PPTP, DHCP, DDNS, UPnP;

— кількість антен: 4;

— функції VPN: PSec / PPTP / L2TP / PPPoE pass-through, IPSec-тунелі;

— функції безпеки: WPA / WPA2 (Personal / Enterprise), WPA3, MAC-фільтр WPS;

— підтримка стандарту IEEE 802.1X для підключення до мережі Інтернет. [12]

2.5 Вибір мережного програмного забезпечення

Операційна система (ОС) — це комплекс програм, який забезпечує керування комп'ютером як єдиним цілим (тоді як насправді комп'ютер складається з багатьох частин), його взаємодія з навколишнім середовищем (людиною, прикладними програмами, іншими системами). ОС — головна частина системного програмного забезпечення. Операційна система управляється командами.

Основні функції операційних систем: керування виконанням програм; ведення файлової системи; розподіл ресурсів, у т.ч. оперативної пам'яті; динамічне компонування виконуваних програм; обробка переривань і забезпечення багатозадачної роботи. [9]

Для робочих станцій обрана операційна система Microsoft Windows 10, тому що вона має: високий рівень безпеки, включаючи можливість шифрування

файлів і папок з метою захисту корпоративної інформації; підтримку мобільних пристроїв для забезпечення можливості працювати автономно або підключатися до комп'ютера у віддаленому режимі; вбудовану підтримку високопродуктивних багатопроцесорних систем; можливість роботи з серверами Microsoft Windows Server і системами управління підприємствами; ефективну взаємодію з іншими користувачами по всьому світу завдяки можливостям багатомовної підтримки [10].

2.6 Вибір мережного протоколу

Мережевий протокол в комп'ютерних мережах – набір правил і угод для обміну інформацією між комп’ютерами. Протокол описує: формат повідомлення, спосіб обміну повідомленнями між комп'ютерами в контексті визначеної дії, як, наприклад, пересилка повідомлення по мережі. Різні протоколи найчастіше описують лише різні сторони одного типу зв'язку та взяті разом утворюють стек протоколів. Назви «протокол» і «стек протоколів» також вказують на програмне забезпечення, яке реалізує протоколи.

Розглянемо найпоширеніші протоколи:

— HTTP (Hyper Text Transfer Protocol) — це протокол передавання гіпертексту, його використовують під час пересилання веб-сторінок між комп’ютерами, під’єднаними до однієї мережі;

— HTTPS (Hypertext Transport Protocol Secure) — це протокол, який забезпечує конфіденційність обміну даними між сайтом і комп’ютером користувача. Захист інформації забезпечується за рахунок використання спеціальних криптографічних протоколів;

— FTP (File Transfer Protocol) — це протокол передавання файлів зі спеціального файлового сервера на комп’ютер користувача. Він надає можливість обмінюватися бінарними і текстовими файлами з будь-яким комп’ютером мережі.

— POP3 (Post Office Protocol) — це стандартний протокол поштового

з’єднання. Сервери POP опрацьовують вхідну пошту, а протокол POP призначений для опрацювання запитів на отримання пошти від клієнтських поштових програм. При цьому всі електронні листи завантажуються користувачеві на комп’ютер;

— SMTP (Simple Mail Transfer Protocol) — це протокол, який задає набір правил для передавання пошти. Сервер SMTP повертає або підтвердження про прийом, або повідомлення про помилку, або вимогу додаткової інформації;

— IMAP (англ. Internet Message Access Protocol) — це протокол прикладного рівня для доступу до електронної пошти. Він надає користувачеві великі можливості для роботи.

У переважній більшості комп'ютерних мереж обмін даними здійснюється на основі сімейства (стеку) протоколів TCP/IP (англ. Transmition Control Protocol — протокол керування передаванням; IP — Internet Protocol — міжмережевий протокол).

Протокол TCP забезпечує зв’язок між комп’ютерами та керує передаванням даних, визначає правила розбиття даних на пакети, доставку адресату та об’єднання пакетів в єдине ціле.

У термінології обчислювальних мереж протокол — це заздалегідь узгоджений стандарт, який дозволяє двом комп'ютерам обмінюватися даними. Фактично TCP/IP не один протокол, а декілька. Саме тому його називають набором, а також комплектом протоколів, серед яких TCP і IP - два основних. [15]

На основі виконаного огляду було обрано протокол TCP/IP, так як цей протокол забезпечує всі необхідні функції та доступ до мережі Internet.

2.7 Функціонування мережі

Для того, щоб забезпечити взаємодію в мережі між робочими станціями, кожен мережний вузол повинен бути однозначно ідентифікований. Тобто, кожен вузол повинен мати унікальне ім'я, по якому він розпізнається в мережі. Також, враховуючи те, що в мережі використовується протокол TCP/IP, необхідно призначити кожному вузлу унікальну IP-адресу.

Мережеві імена робочих станцій вибираються на основі назв кабінетів, в яких вони розташовані. Всі встановлені мережеві імена показані на кресленні ДП. 05010201.140.576 ГЧ3.

IP-адреса (скорочення від англ. Internet Protocol Address) - унікальна мережева адреса вузла в комп'ютерній мережі, побудована за протоколом IP. В мережі Інтернет потрібна глобальна унікальність адреси. У разі роботи в локальній мережі потрібна унікальність адреси в межах мережі. У версії протоколу IPv4 IP-адреса має довжину 4 байта.

В 4-й версії IP-адреса являє собою 32-бітове число. Зручною формою запису IP-адреси (IPv4) є запис у вигляді чотирьох десяткових чисел значенням від 0 до 255, розділених крапками, наприклад: 192.168.0.1.

У 6-й версії IP-адреса (IPv6) має 128-бітове представлення. Адреси розділяються двокрапкою (напр. Fe80: 0: 0: 0: 200: f8ff: fe21: 67cf або 2001: 0db8: 85a3: 0000: 0000: 8a2e: 0370: 7334). Велика кількість нульових груп може бути пропущена за допомогою подвійної двокрапки (fe80 :: 200: f8ff: fe21: 67cf).

IP-адресу називають статичною (постійною, незмінною), якщо вона призначається користувачем в налаштуваннях пристрою, або якщо призначається автоматично при підключенні пристрою до мережі і не може бути присвоєна іншому пристрою.

IP-адресу називають динамічною (непостійною, змінною), якщо вона призначається автоматично при підключенні пристрою до мережі і використовується протягом обмеженого проміжку часу, зазначеного в сервісі призначеної IP-адреси [7].

Мережі діляться на класи:

— клас A — «Великі мережі»:

—адреси цих мереж лежать у проміжку: 1 – 126;

— маска мережі: 255.0.0.0;

— містить до 16387064 адрес (256 * 256 * 256);

— адреси хостів в цих мережах виду: 125.*.*.*.

— клас B - «Середні мережі»:

— адреси цих мереж лежать у проміжку: 128.0 - 191.255;

— маска мережі: 255.255.0.0;

— містить до 64516 адрес (256 * 256);

—адреси хостів в цих мережах виду: 136.12.*.*.

— клас C - «Маленькі мережі»:

— адреси мереж лежать в інтервалі: 192.0.0 - 255.254.255;

— маска мережі: 255.255.255.0;

— містить 254 адреси;

— адреси хостів в цих мережах виду: 195.136.12.*.

— клас D - «Multicast-мережі» (групова адресація):

— адреси мереж лежать в інтервалі: 224-239.

В мережі, що розробляється 28 комп'ютерів, тому обираємо IP-адреси класу C, маска підмережі 255.255.255.0.

Для ідентифікатора підмережі перший октет встановимо 192. Інші два октети можуть бути обрані довільно, нехай вони приймуть значення 168 та 57. Отже, ідентифікатор підмережі прийме значення 192.168.57.0.

2.8 Розміщення робочих станцій

Робоча станція (*workstation*) — комплекс апаратних і програмних засобів, призначених для вирішення певного кола завдань.

Робоча станція як місце роботи фахівця являє собою повноцінний комп'ютер або комп'ютерний термінал (пристрої введення-виведення, відокремлені і часто віддалені від керуючого комп'ютера), набір необхідного програмного забезпечення, за необхідністю доповнюються допоміжним обладнанням: друкувальним пристроєм, зовнішнім пристроєм зберігання даних на магнітних та/або оптичних носіях, сканер штрихкоду тощо.

Також, терміном «робоча станція» позначають стаціонарний комп'ютер у складі локальної обчислювальної мережі (ЛОМ) по відношенню до сервера. У локальних мережах комп'ютери поділяються на робочі станції і сервери. На ро-

бочих станціях користувачі вирішують прикладні завдання (працюють в базах даних, створюють документи, роблять розрахунки, грають у комп'ютерні ігри). Сервер обслуговує мережу і надає власні ресурси всім вузлам мережі, в тому числі і робочим станціям.

Існують досить стійкі ознаки конфігурацій робочих станцій, призначених для вирішення певного кола завдань, що дозволяє підрозділити їх на окремі професійні підкласи:

— мультимедіа і, зокрема, комп'ютерна графіка і обробка зображень, відео,

звуку, розробка комп'ютерних ігор;

— різні інженерні, архітектурні (в тому числі містобудівні) та інші САПР ,

ГІС, нші САПР, ГІС, польові дослідження і геодезія тощо;

— наукові та інженерно-технічні обчислення;

— професійний біржевий інтернет-трейдинг.

4 ПЛАНУВАННЯ СХЕМИ КОМП'ЮТЕРНОЇ МЕРЕЖІ ЛІЦЕЮ

4.1 Планування приміщення та розташування обладнання

Для розробки комп'ютерної мережі ліцею використовується програмне забезпечення Microsoft Visio.

Програмне забезпечення Microsoft Visio має низку функціональних особливостей, які роблять його ефективним інструментом для створення схем, діаграм та технічної документації.

Основними перевагами ПЗ є:

— велика кількість вбудованих шаблонів і стилів, що дає змогу оперативно формувати професійно оформлені документи різного типу;

— Visio працює з векторною графікою, що забезпечує високу точність, масштабованість та якість зображень, що особливо важливо при створенні креслень;

— програма підтримує імпорт і експорт даних з різних джерел, зокрема Excel, Access, SQL Server та інших, а також дозволяє зберігати документи в різних форматах для подальшого використання або обміну;

— функція спільної роботи дає змогу кільком користувачам одночасно працювати над одним документом, що значно підвищує ефективність командної взаємодії;

— Visio має інтеграцію з іншими продуктами Microsoft, зокрема Office та SharePoint, що забезпечує зручну роботу з документами в єдиному інформаційному середовищі;

— програма підтримує міжнародні стандарти, такі як ISO та ANSI, що дозволяє використовувати її для створення технічної документації відповідно до вимог стандартів;

— інтерфейс Visio є гнучким до налаштування, що дозволяє адаптувати його під індивідуальні потреби користувача та підвищити зручність у роботі.

Потрібно здійснити проектування комп'ютерної мережі ліцею, охоплюючи вісім приміщень: кабінет інформатики на другому поверсі, бібліотеку, кабі-

нет директора, кабінет заступника директора, кабінет інформатики на третьому поверсі, учительську, актову залу та серверну.

Відповідно до наявного плану приміщень ліцею, здійснюється розробка схеми розміщення комп'ютерного обладнання, яка включає визначення розташування комп'ютерів, робочих станцій, принтерів, мережевих пристроїв, а також організацію кабельного менеджменту.

Загальна кількість робочих станцій становить 37 одиниць. У кабінеті інформатики на другому поверсі передбачено встановлення 14 учнівських комп'ютерів та 1 викладацького. Аналогічна конфігурація передбачена і для кабінету інформатики на третьому поверсі. У серверному приміщенні буде розміщено сервер. По одному комп'ютеру планується встановити в бібліотеці, актовій залі, кабінеті директора та кабінеті заступника директора. В учительській кімнаті передбачено встановлення двох комп'ютерів.

На рисунках 3.1 і 3.2 наведено план приміщення другого та третього поверхів відповідно.

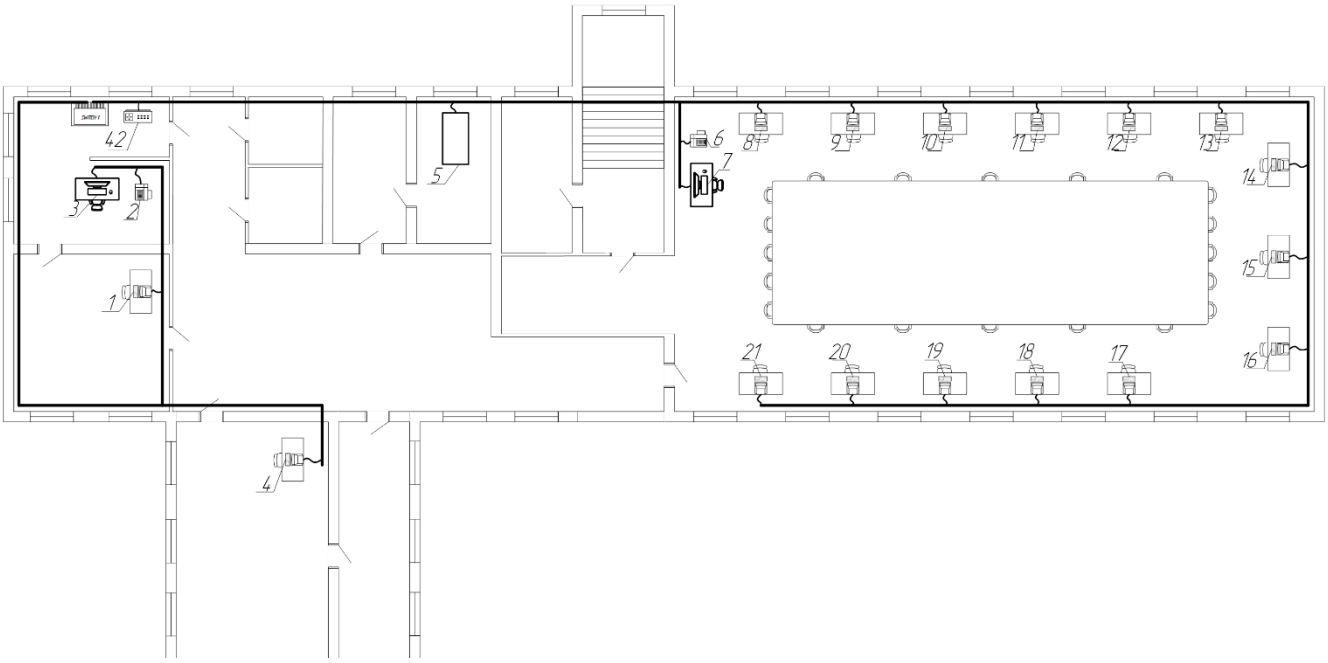

Рисунок 3.1 — План приміщення другого поверху

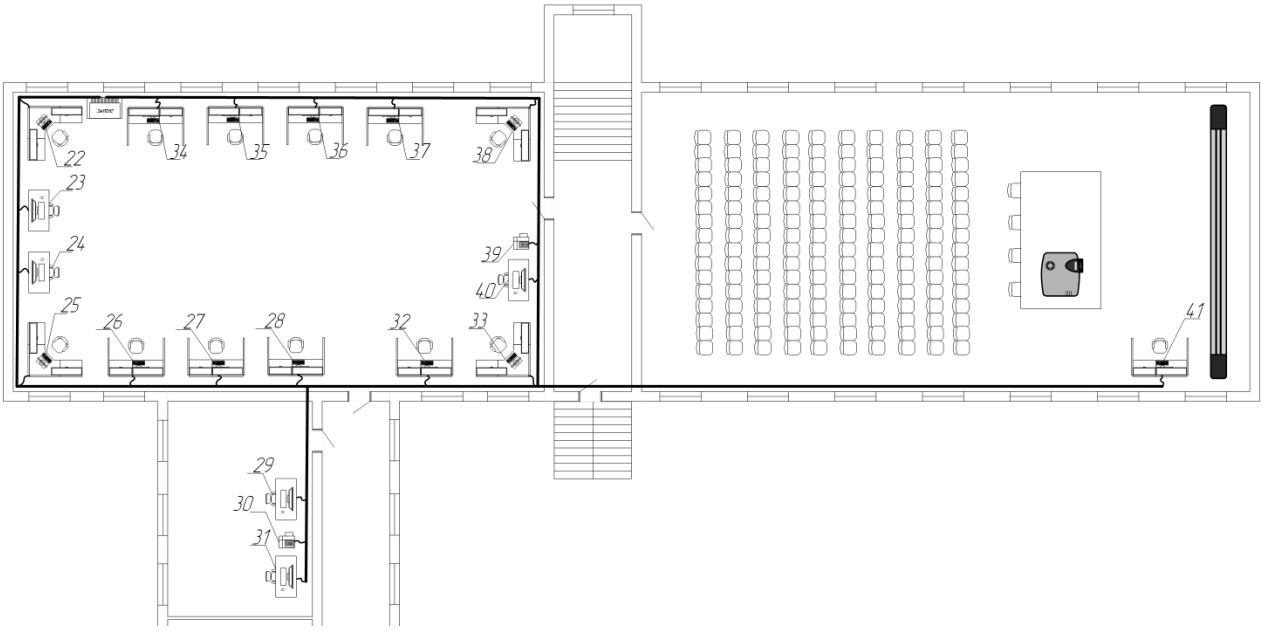

Рисунок 3.2 — План приміщення третього поверху

4.2 Загальні характеристики та розрахунки мережі

Для комп’ютерної мережі ліцею потрібно таке обладнання:

— 36 персональних комп’ютерів;

— 4 принтери;

— 2 комутатори;

— 1 маршрутизатор;

— 1 сервер.

Опис технічних характеристик мережевих вузлів наведено у таблиці 3.1.

Таблиця 3.1 — таблиця технічних характеристик вузлів

№ з/п	Мережне ім’я	Мережна ОС	Місце розташування	Технічні характеристики		
				Тип процесора	Об’єм ОЗП	Тип та ємність пам’яті
1	Zavuch	Windows 10	Кабінет завуча	Intel i5-4570	8Гб	SSD 1Тб
2	DirectorPR		Кабінет директора	Canon PIXMA TS704		
3	Director	Windows 10	Кабінет директора	Intel i5-4570	8Гб	SSD 1Тб
4	Biblioteka	Windows 10	Бібліотека	Intel i3-4170	4Гб	SSD 500Гб
5	Server	Windows 10	Сервер	Ryzen 7 5700G	16 Гб	SSD 2Тб

Продовження таблиці 3.1

6	Kabinf2Pr		Кабінет 2 поверх	HP Laser Jet M211dw		
7	Kabinf21	Windows 10	Кабінет 2 поверх	Intel i3-4170	4Гб	SSD 500Гб
8	Kabinf22	Windows 10	Кабінет 2 поверх	Intel i3-4170	4Гб	SSD 500Гб
9	Kabinf23	Windows 10	Кабінет 2 поверх	Intel i3-4170	4Гб	SSD 500Гб
10	Kabinf24	Windows 10	Кабінет 2 поверх	Intel i3-4170	4Гб	SSD 500Гб
11	Kabinf25	Windows 10	Кабінет 2 поверх	Intel i3-4170	4Гб	SSD 500Гб
12	Kabinf26	Windows 10	Кабінет 2 поверх	Intel i3-4170	4Гб	SSD 500Гб
13	Kabinf27	Windows 10	Кабінет 2 поверх	Intel i3-4170	4Гб	SSD 500Гб
14	Kabinf28	Windows 10	Кабінет 2 поверх	Intel i3-4170	4Гб	SSD 500Гб
15	Kabinf29	Windows 10	Кабінет 2 поверх	Intel i3-4170	4Гб	SSD 500Гб
16	Kabinf210	Windows 10	Кабінет 2 поверх	Intel i3-4170	4Гб	SSD 500Гб
17	Kabinf211	Windows 10	Кабінет 2 поверх	Intel i3-4170	4Гб	SSD 500Гб
18	Kabinf212	Windows 10	Кабінет 2 поверх	Intel i3-4170	4Гб	SSD 500Гб
19	Kabinf213	Windows 10	Кабінет 2 поверх	Intel i3-4170	4Гб	SSD 500Гб
20	Kabinf214	Windows 10	Кабінет 2 поверх	Intel i3-4170	4Гб	SSD 500Гб
21	Kabinf215	Windows 10	Кабінет 2 поверх	Intel i3-4170	4Гб	SSD 500Гб
22	Kabinf31	Windows 10	Кабінет 3 поверх	Intel i3-4170	4Гб	SSD 500Гб
23	Kabinf32	Windows 10	Кабінет 3 поверх	Intel i3-4170	4Гб	SSD 500Гб
24	Kabinf33	Windows 10	Кабінет 3 поверх	Intel i3-4170	4Гб	SSD 500Гб
25	Kabinf34	Windows 10	Кабінет 3 поверх	Intel i3-4170	4Гб	SSD 500Гб
26	Kabinf35	Windows 10	Кабінет 3 поверх	Intel i3-4170	4Гб	SSD 500Гб
27	Kabinf36	Windows 10	Кабінет 3 поверх	Intel i3-4170	4Гб	SSD 500Гб
28	Kabinf37	Windows 10	Кабінет 3 поверх	Intel i3-4170	4Гб	SSD 500Гб
29	Uchitelska	Windows 10	Учительська	Intel i5-4570	8Гб	SSD 1Тб
30	UchitelskaPr		Учительська	HP Laser Jet M211dw		
31	Uchitelska1	Windows 10	Учительська	Intel i3-4170	4Гб	SSD 500Гб
32	Kabinf38	Windows 10	Кабінет 3 поверх	Intel i3-4170	4Гб	SSD 500Гб
33	Kabinf39	Windows 10	Кабінет 3 поверх	Intel i3-4170	4Гб	SSD 500Гб
34	Kabinf310	Windows 10	Кабінет 3 поверх	Intel i3-4170	4Гб	SSD 500Гб
35	Kabinf311	Windows 10	Кабінет 3 поверх	Intel i3-4170	4Гб	SSD 500Гб
36	Kabinf312	Windows 10	Кабінет 3 поверх	Intel i3-4170	4Гб	SSD 500Гб
37	Kabinf313	Windows 10	Кабінет 3 поверх	Intel i3-4170	4Гб	SSD 500Гб
38	Kabinf314	Windows 10	Кабінет 3 поверх	Intel i3-4170	4Гб	SSD 500Гб
39	Kabinf3Pr		Кабінет 3 поверх	Canon PIXMA TS704		

Продовження таблиці 3.1

40	Kabinf315	Windows 10	Кабінет 3 поверх	Intel i3-4170	4Гб	SSD 500Гб
41	ActZala	Windows 10	Актова зала	Intel i3-4170	4Гб	SSD 500Гб
42	Router1		Кабінет директора	MikroTik hAP		

Проект комп'ютерної мережі для ліцею реалізовано з використанням топології типу «зірка». Такий підхід передбачає наявність центрального вузла (мережевого комутатора або маршрутизатора), до якого підключаються всі інші мережеві пристрої. Серед основних переваг цієї топології є простота налаштування та обслуговування кінцевих пристроїв, а також висока надійність функціонування мережі. У випадку виходу з ладу одного з периферійних пристроїв, робота решти елементів мережі не припиняється, що забезпечує її стійкість до відмов.

При цьому, недоліком топології «зірка» є підвищене навантаження на центральний пристрій, що вимагає використання продуктивнішого та надійнішого обладнання. Це, у свою чергу, збільшує загальну вартість побудови мережі. У схемі мережі центральним пристроєм є маршрутизатор.

Наступні чинники є причиною вибору даної топології:

— простота технічного обслуговування та оперативне виявлення можливих несправностей у мережевій інфраструктурі;

— підвищений рівень надійності та безпеки — вихід з ладу одного з кінцевих пристроїв не впливає на роботу інших елементів мережі;

— зручність масштабування — можливість швидкого підключення нових пристроїв до існуючих вузлів без суттєвих змін у структурі мережі.

Водночас, при проектуванні мережі на основі топології «зірка» необхідно враховувати і її недоліки, зокрема:

— централізований характер мережі — вихід з ладу центрального вузла призводить до зупинки роботи всієї мережі;

— обслуговування мережі є спрощеним, але воно може потребувати більше часу через необхідність роботи з центральним вузлом і численними підключеннями;

— збільшені обсяги кабельної розводки, що ускладнює монтаж та підвищує витрати на інфраструктурне забезпечення.

На рисунку 3.3 зображене креслення загальної структури мережі з усіма пристроями мережі. На рисунку позначені мережеві імена пристроїв, їх розподіл по кабінетах та під’єднання пристроїв між собою.

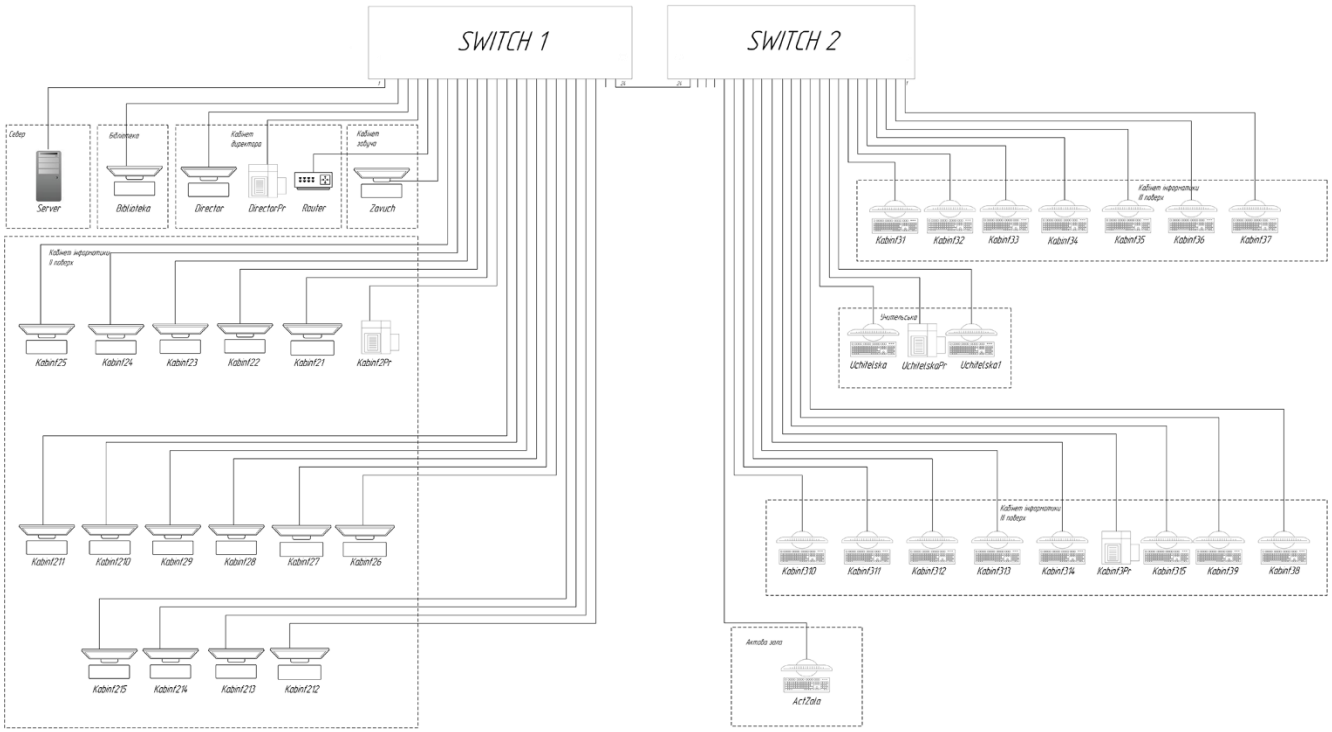

Рисунок 3.3 — Загальна структура мережі

З метою оптимізації витрат на мережеве обладнання, в рамках розробки мережі було прийнято рішення використовувати технологію VLAN (Virtual Local Area Network) замість встановлення окремих маршрутизаторів для кожної підмережі. Такий підхід дає змогу зберегти функціональність мережі при суттєвому зниженні вартості її реалізації.

VLAN — це логічно сформована мережа, яка функціонує в межах фізичної локальної комп’ютерної мережі. Застосування VLAN дає змогу сегментува-

ти мережеве середовище на віртуальні підмережі, незалежно від фізичного розташування пристроїв.

Сегментування за допомогою VLAN дозволяє не лише підвищити загальну продуктивність мережі шляхом оптимізації розподілу трафіку, а й забезпечити більш високий рівень безпеки завдяки ізоляції трафіку між окремими логічними сегментами.

Всього створено 8 віртуальних підмереж:

— VLAN 10 — для сервреної;
— VLAN 20 — для пристроїв у кабінеті інформатики на 2 поверсі;
— VLAN 30 — для пристроїв у кабінеті інформатики на 3 поверсі;
— VLAN 2 — для кабінету завуча;
— VLAN 3 — для кабінету директора;
— VLAN 4 — для бібліотеки;
— VLAN 5 — для учительської;
— VLAN 6 — для актової зали.

У таблиці 3.2 представлено перелік налаштованих VLAN із детальною інформацією щодо призначених IP-адрес та їх розподілу в межах віртуальних сегментів мережі.

Таблиця 3.2 — Опис VLAN-сегментів і призначених IP-адрес

Назви пристроїв	Пул IP-адрес	Шлюз	VLAN
Kabinf21-Kabinf215, Kabinf2Pr	192.168.100.1-16 255.255.255.224	192.168.100.30	20 (Кабінет1)
Kabinf31-Kabinf315, Kabinf2Pr	192.168.100.33-48 255.255.255.224	192.168.100.62	30 (Кабінет 2)
Director, DirectorPr	192.168.100.65-66 /29	192.168.100.70	3 (Директор)
Uchitelska, Uchitelska1, UchitelskaPR	192.168.100.73-75 /29	192.168.100.78	5 (Учительська)
Zavuch	192.168.100.81/30	192.168.100.82	2 (Завуч)
Biblioteka	192.168.100.85/30	192.168.100.86	4 (Бібліотека)

ActZala	192.168.100.89/30	192.168.100.90	6 (Актова зала)
Server	192.168.100.93/30	192.168.100.94	10 (Серверна)

У таблиці 3.3 представлено налаштування мережевих портів, передбачених для реалізації схеми підключення кінцевих пристроїв до мережі.

Таблиці 3.3 — Підключені порти комутаторів

Назва пристрою	Порт	VLAN
Switch1	FastEthernet0/1-16	20
	FastEthernet0/17-18	3
	FastEthernet0/19	2
	FastEthernet0/20	4
	FastEthernet0/21	10
	FastEthernet0/23	Trunk
	FastEthernet0/24	Trunk
Switch2	FastEthernet0/1-16	30
	FastEthernet0/17-19	5
	FastEthernet0/20	6
	FastEthernet0/24	Trunk

Для кожної віртуальної підмережі було обрано оптимальну маску підмережі, виходячи з кількості підключених хостів у відповідному сегменті. Це дозволяє забезпечити раціональне використання IP-адрес та підтримувати стабільну роботу мережі на пристроях кінцевих користувачів.

4.3 Оцінка надійності мережі

Для забезпечення стабільного функціонування мережі, побудованої на основі декількох фізичних сегментів, необхідне дотримання наступних технічних параметрів:

— максимально допустима кількість станцій у мережі — 1024;

— подвоєна затримка поширення сигналу (PDV) між двома найбільш віддаленими мережевими вузлами не повинна перевищувати 575 бітових інтервалів (bit times);

— сумарне скорочення міжкадрового інтервалу (Interpacket Gap Shrinkage) під час проходження потоку кадрів крізь усі каскадовані повторювачі не повинне перевищувати 49 бітових інтервалів.

Для подальших обчислень виконується розрахунок PDV із використанням табличних значень затримок сигналу в окремих мережевих сегментах, які наведені у таблиці 3.4.

Таблиця 3.4 — Затримка сигналів в мережі

Тип сегмента	Затримка середовища на 1 м	Максимальна затримка
1000BASE-TX	0,112	0,112
Комутатор		30

Розрахунок затримки здійснюється з урахуванням максимально допустимих довжин сегментів, що реалізовані в топології мережі.

З метою визначення подвоєної затримки розповсюдження сигналу (Path Delay Value), виконуються обчислення з урахуванням максимальних довжин сегментів мережі:

— сегмент між комутаторами (SWITCH1–SWITCH2): 4 м;

— правий сегмент (ActZala–SWITCH2): 52,9 м;

— лівий сегмент (SWITCH1–Kabinf215): 69,74 м.

Згідно з табличними даними, затримка в мідному кабелі типу UTP становить 0,112 бітових інтервалів/м.

Виконуємо обчислення індивідуальних затримок:

Затримка між комутаторами:

4*0,112=0,48 бітових інтервалів

Затримка правого сегмента:

52,9*0,112=5,92 бітових інтервалів

Затримка лівого сегмента:

69,74*0,112=7,81 бітових інтервалів

Знаходимо PDV, як суму всіх затримок в мережі.

PDV=0,48+5,92+7,81+5,92+30+30=74,21 < 512.

Сумарне значення затримки розповсюдження сигналу (PDV), отримане в результаті розрахунку, є меншим за максимально допустиме значення 512 бітових інтервалів, що встановлено стандартом. Отже, проектована мережа відповідає вимогам щодо затримки сигналу та може функціонувати в заданих умовах без порушення протоколу доступу до середовища.

3.4 Порівняння засобів моделювання

Існують різні підходи до моделювання комп'ютерних мереж, серед яких вирізняють фізичне, аналітичне, імітаційне та комбіноване моделювання. Фізичне моделювання передбачає проведення експериментів у реальному часі з використанням справжнього обладнання для оцінки характеристик досліджуваної мережі. Такий підхід забезпечує високу точність результатів, що наближені до параметрів реальної системи. Однак основним його недоліком є значні фінансові витрати, пов'язані з необхідністю закупівлі та налаштування обладнання.

Аналітичне моделювання ґрунтується на використанні математичних виразів, які описують взаємозв'язки між параметрами системи під час її функціонування. Такий підхід доцільний у випадках, коли система є достатньо простою, а також за умови, що висока точність результатів не є критичною. Імітаційне моделювання, у свою чергу, реалізується у вигляді програмного забезпечення, яке моделює події та процеси, що відбуваються в реальній комп'ютерній мережі.

Імітаційні моделі комп'ютерних мереж забезпечують деталізоване відтворення процесів передавання даних, зокрема розподіл повідомлень на пакети й кадри відповідно до обраних мережевих протоколів. Вони дозволяють фіксувати втрати пакетів і кадрів, а також аналізувати, яким чином комп'ютер отримує доступ до спільного мережевого середовища. У результаті роботи таких моделей формується статистична інформація, що характеризує ключові властивості функціонування мережі.

3.3.1 Аналіз GNS3

Graphical Network Simulator (GNS) — це графічний симулятор мереж, який дозволяє створювати різноманітні мережеві топології на комп’ютері. Найчастіше GNS використовується як лабораторний стенд, де можна перевіряти різні технології та схеми мереж. Цей емулятор дає можливість створити модель комп’ютера або іншого мережевого пристрою та запускати на ньому оригінальне програмне забезпечення.

Емулюються всі основні компоненти пристрою, зокрема процесор, пам'ять та пристрої введення/виведення. У випадку з обладнанням Cisco, емулятор моделює маршрутизатор і запускає реальну операційну систему Cisco IOS, що дозволяє отримати повнофункціональний маршрутизатор.

Симулятор відтворює поведінку системи та її інтерфейсу. Одним із яскравих прикладів є Cisco Packet Tracer, де розробники створили моделі пристроїв із інтерфейсами та командами, схожими на реальні. Переваги GNS3:

— повний функціонал емульованого пристрою — запустивши маршрутизатор Cisco, користувач отримує доступ до майже всіх функцій, доступних на реальному маршрутизаторі, що дозволяє моделювати реальні сценарії;

— можливість створення гетерогенних мереж — у GNS3 можна побудувати мережу, яка включає не лише пристрої Cisco, але й обладнання від інших виробників, таких як Juniper, Mikrotik, CheckPoint та інших;

— додавання повноцінних робочих станцій та серверів — GNS3 дозволяє інтегрувати в мережу реальні робочі станції з операційними системами Windows 10 або Ubuntu, а також сервери з Windows Server або RedHat, що розширює можливості для тестування і налаштування мережі.

Основні недоліки GNS3:

— відсутність можливості емулювати комутатори — в реальних комутаторах використовуються ASIC мікросхеми, які забезпечують високу швидкість обробки пакетів. Однак ці мікросхеми поки що неможливо емулювати на звичайному комп'ютері. Водночас маршрутизатори працюють на процесорах,

схожих або ідентичних до процесорів звичайних комп'ютерів, тому їх емулювати не становить проблеми. Однак варто зазначити, що процесори значно повільніші за ASIC мікросхеми;

— високі вимоги до системних ресурсів — хоча це більше стосується самих пристроїв, що запускаються в GNS3, а не самого симулятора, варто зазначити, що емуляція реальних прошивок пристроїв потребує значної кількості ресурсів. Це є однією з причин, чому GNS3 має більш високі вимоги до апаратного забезпечення порівняно з іншими симуляторами, такими як Cisco Packet Tracer.

3.3.2 Аналіз Cisco Packet Tracer

Cisco Packet Tracer — це програмний продукт, розроблений компанією Cisco, який рекомендовано для використання у процесі навчання телекомунікаційним мережам і мережевому обладнанню, зокрема під час виконання лабораторних робіт у закладах вищої освіти. Cisco Packet Tracer вирізняється широким спектром функціональних можливостей, які роблять його ефективним інструментом для навчання та моделювання мережевих рішень.

Серед основних переваг цієї програми варто виділити:

— зручний графічний інтерфейс користувача (GUI), що полегшує розуміння принципів побудови мереж і роботи окремих пристроїв;

— підтримка створення будь-якої логічної топології завдяки гнучкому робочому простору, що дозволяє змоделювати мережу практично будь-якого масштабу;

— можливість роботи в режимі реального часу (realtime), що забезпечує моделювання подій у такій послідовності, як вони відбуваються насправді;

— наявність режиму «Simulatiom», який дає змогу зупиняти та аналізувати процеси на різних етапах передачі даних;

— деталізоване візуальне представлення мережевого обладнання з можливістю редагування його конфігурації — додавання або вилучення компонентів;

— інструмент Activity Wizard, який дозволяє створювати власні навчальні сценарії, що можуть бути використані як студентами, так і викладачами;

— підтримка проектування фізичної топології мереж із використанням абстракцій таких об'єктів, як місто, будівля чи стійка, що дозволяє наблизити віртуальну модель до реальних умов.

Завдяки широкому функціоналу Cisco Packet Tracer мережеві інженери має можливість не лише проектувати, але й здійснювати налаштування та відлагодження обчислювальних мереж різного рівня складності. Програма є ефективним інструментом у навчальному процесі, оскільки забезпечує візуалізацію роботи мережі, що сприяє кращому засвоєнню теоретичного матеріалу.

Емулятор дозволяє моделювати мережі підвищеної складності, створювати й аналізувати передавання пакетів даних, а також зберігати проекти й додавати до них пояснення. У ПЗ є змога працювати з різними типами мережевого обладнання, зокрема з комутаторами другого та третього рівнів, визначати типи з’єднань між пристроями та здійснювати їхню інтеграцію в топологію.

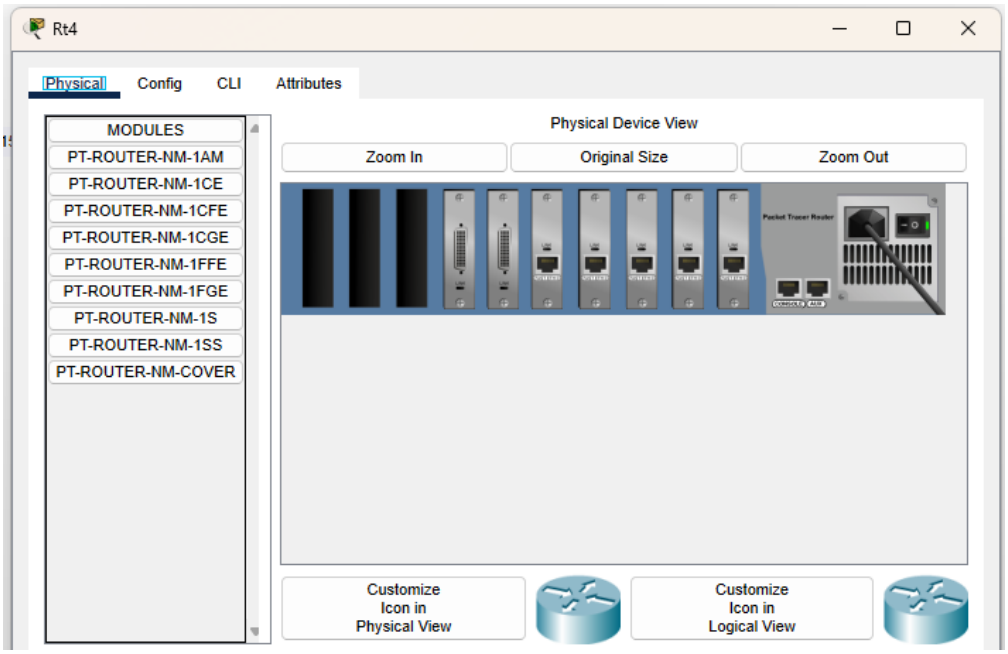

Рисунок 3.4 — Фізичний вигляд маршрутизатора

Кожен пристрій у Cisco Packet Tracer можна налаштувати через вікно властивостей, яке відкривається на обраному пристрої. Перша вкладка Physical

відповідає за налаштування фізичних параметрів пристрою. При налаштуванні маршрутизаторів і комутаторів є можливість додавати нові модулі, а для робочих станцій та серверів — вставляти мережеві адаптери. Її зображення наведено на рисунку 3.4.

На рисунку 3.5 показано вкладку Config. У ній можна налаштувати основні параметри мережевих інтерфейсів, такі як IP-адреси, маски підмережі, налаштування бездротових мереж та інші параметри. Крім того, у мережевих пристроях є можливість конфігурувати маршрутизацію — як статичну, так і динамічну, а для серверів — налаштовувати відповідні служби.

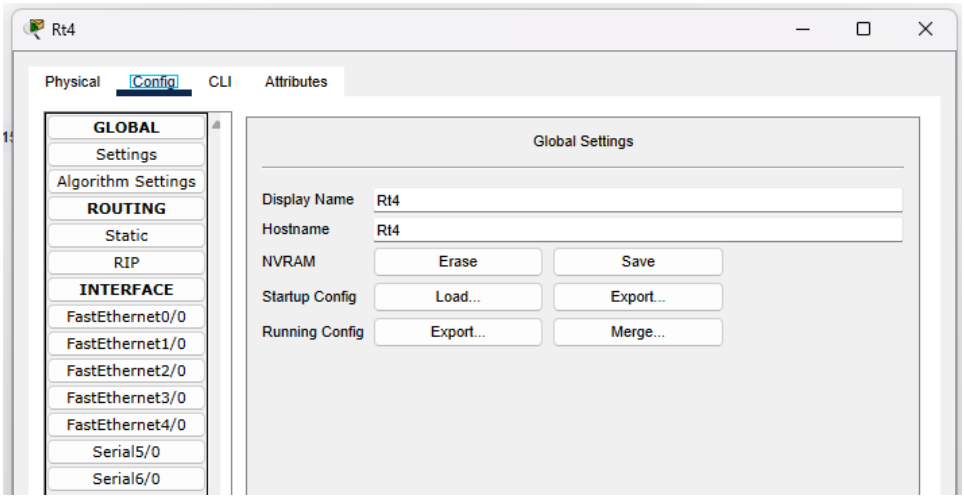

Рисунок 3.5 — Вікно візуального конфігурування пристрою

Вкладка CLI (Command Line Interface) в Cisco Packet Tracer дозволяє користувачам взаємодіяти з мережевими пристроями через командний рядок, що є одним із найбільш популярних способів налаштування та керування обладнанням в реальних мережах. Вона дає змогу здійснювати точне налаштування пристроїв за допомогою команд, які користувач вводить вручну.

У вкладці CLI можна, наприклад, налаштувати маршрутизатор за допомогою команд. Це зображено на рисунку 3.6.

Ці команди дозволяють увімкнути інтерфейс, призначити IP-адресу та підключити його до мережі. Використання вкладки CLI є важливим для тих, хто

хоче поглибити свої знання про налаштування та адміністрування мереж через командний рядок, що є стандартом у професійних середовищах Cisco.

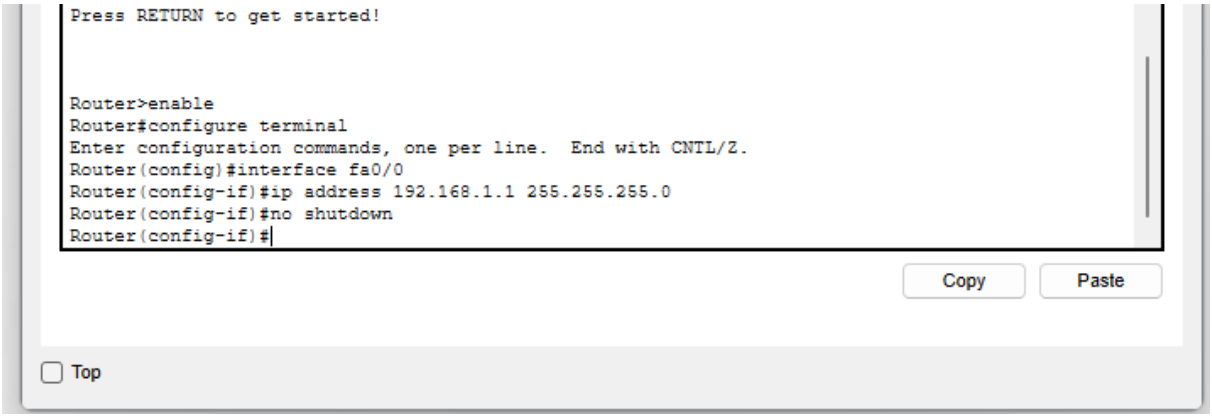

Рисунок 3.6 — налаштування маршрутизатора через командний рядок

Ці команди дозволяють увімкнути інтерфейс, призначити IP-адресу та підключити його до мережі. Використання вкладки CLI є важливим для тих, хто хоче поглибити свої знання про налаштування та адміністрування мереж через командний рядок, що є стандартом у професійних середовищах Cisco.

На завершальному етапі розробки мережі інженер переходить до її налаштування, використовуючи інструменти термінального доступу або інтерфейс командного рядка, приклад робочої області наведено на рисунку 3.7.

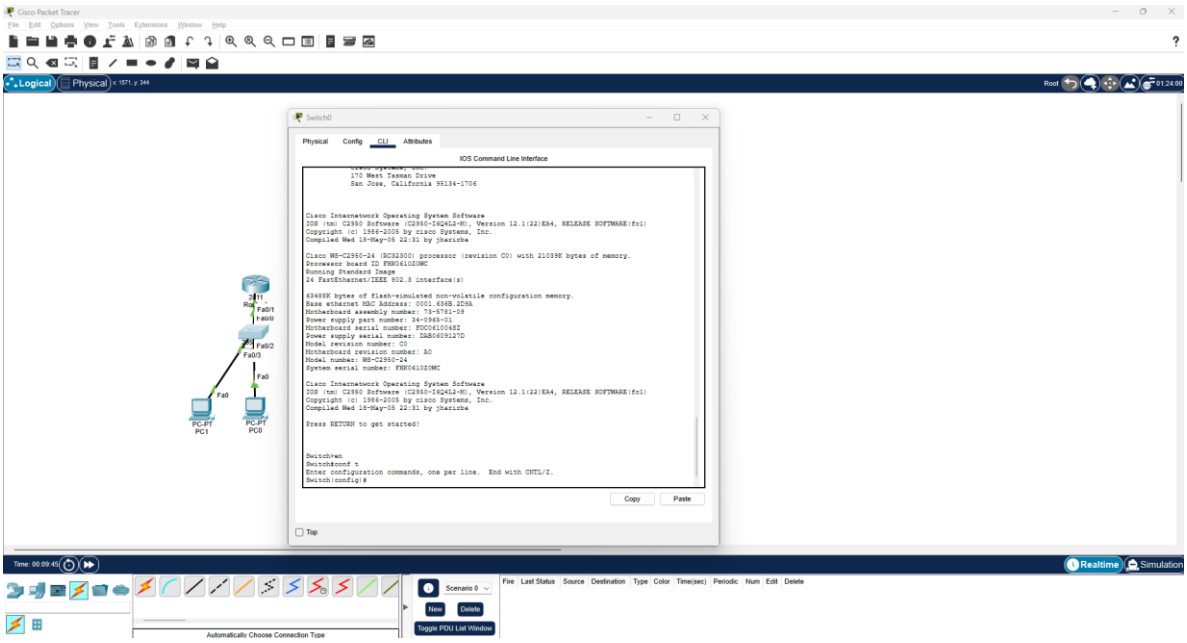

Рисунок 3.7 — Інтерфейс Cisco Packet Tracer

Однією з ключових функцій симулятора Cisco Packet Tracer є режим симуляції. У цьому режимі весь процес передавання пакетів усередині мережі візуалізується у графічному форматі. Така функціональність дає змогу мережевим спеціалістам у наочній формі відслідковувати, яким саме інтерфейсом у конкретний момент проходить пакет, які мережеві протоколи при цьому задіяні тощо. Вікно режиму симуляції наведено на рисунку 3.8.

Проте переваги Cisco Packet Tracer на цьому не обмежуються: у режимі симуляції користувачі мають можливість не лише відстежувати використані протоколи, а й визначати, на якому саме з семи рівнів моделі OSI функціонує кожен з них, що зображено на рисунку 3.9.

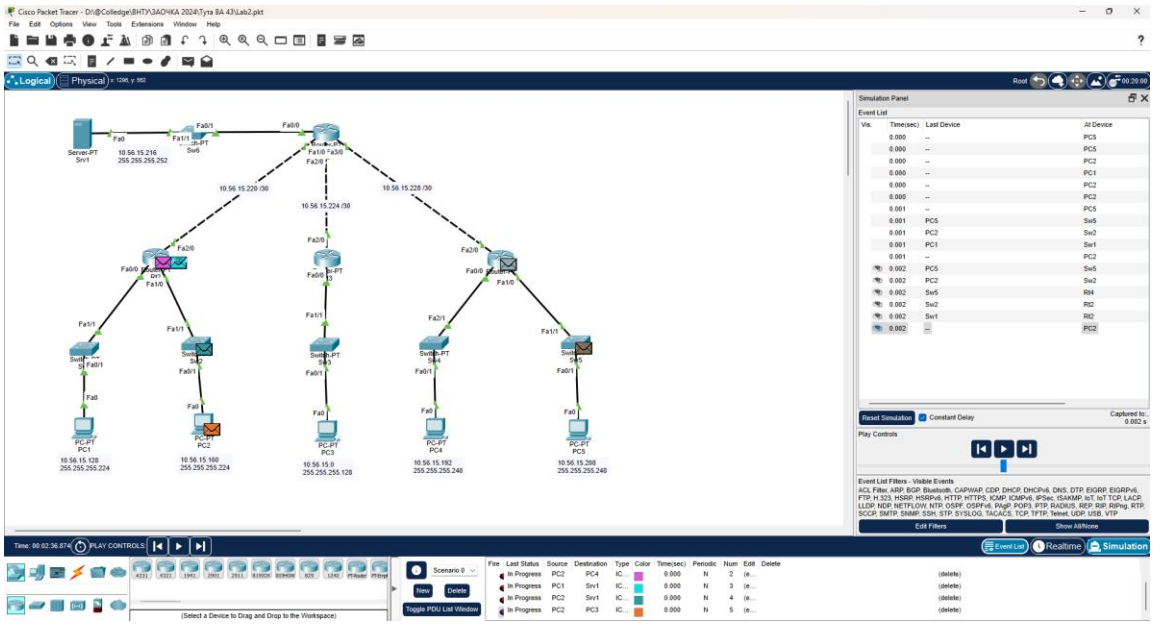

Рисунок 3.8 — Вікно режиму симуляції

Отже, програмні засоби для моделювання комп’ютерних мереж відіграють ключову роль як у навчанні, так і в практичній підготовці майбутніх фахівців. Вони слугують ефективними тренажерами для опанування принципів роботи мереж та дозволяють апробовувати різноманітні варіанти конфігурацій у віртуальному середовищі, максимально наближеному до реального.

При виборі таких інструментів важливо враховувати мету використання: для початкового рівня важливішими є інтуїтивно зрозумілий інтерфейс і досту-

пність базових функцій, тоді як для професійного застосування — підтримка широкого спектра мережевого обладнання.

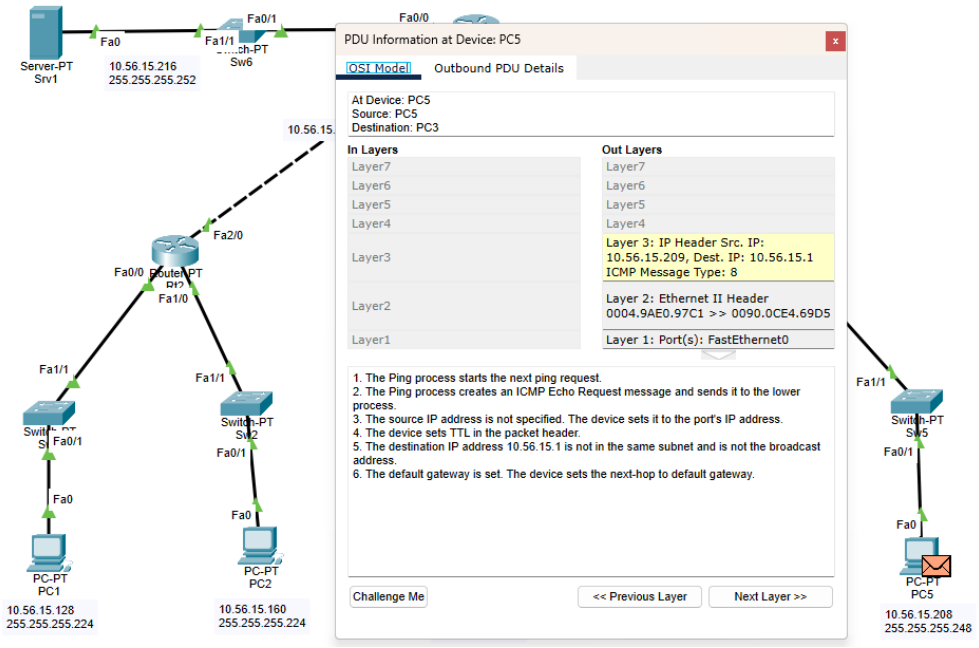

Рисунок 3.9 — Вікно режиму симуляції

Cisco Packet Tracer поєднує в собі простоту, наочність і функціональність, що робить його особливо ефективним у навчальному процесі. Його можливості дозволяють створювати моделі мереж будь-якого рівня складності, закріплюючи теоретичні знання практичними навичками. Саме тому для моделювання мережі використовуватиметься програмне забезпечення Cisco Packet Tracer.

3.4 Налаштування Virtual LAN

Для проектування комп’ютерної мережі використовується програмне забезпечення Cisco Packet Tracer, яке забезпечує широкі можливості для моделювання мережевої інфраструктури. Інструмент дозволяє детально відтворити топологію мережі, здійснити конфігурацію всіх мережевих пристроїв, а також виконати перевірку коректності налаштувань та функціонування мережі в цілому.

Процес проектування починається зі створення топології мережі шляхом підбору необхідних пристроїв, які з’єднуються між собою згідно з планом розподілу підмереж та відповідними портами, що були визначені на етапі проектування.

Для спрощення процесу налаштування комутаторів використовується протокол VTP (VLAN Trunking Protocol), який призначений для обміну інформацією щодо VLAN між мережевими пристроями. Цей протокол дозволяє значно полегшити адміністрування мережі, оскільки загальні налаштування VLAN автоматично передаються від «серверного» комутатора до всіх інших комутаторів у мережі. Це зменшує ймовірність виникнення помилок і скорочує час, необхідний для редагування налаштувань. Налаштування VTP на комутаторі Switch1 наведено в лістингу 4.1.

Лістинг 3.1 — Налаштування VTP на комутаторі Switch1

```
Switch1>enable
Switch1#conf t
Switch1(config)#vtp mode server
Switch1(config)#vtp domain Network_shkola
Switch1(config)#vtp password password_shkola
```

У лістингу 3.2 наведено процес створення VLAN та їх перейменування з метою спрощення адміністрування мережі.

Лістинг 3.2 — Створення VLAN на комутаторі Switch1

```
Switch1(config-vlan)#vlan 10
Switch1(config-vlan)#name Server
Switch1(config-vlan)#vlan 20
Switch1(config-vlan)#name Kabinf2
Switch1(config-vlan)#vlan 30
Switch1(config-vlan)#name Kabinf3
Switch1(config-vlan)#vlan 2
Switch1(config-vlan)#name Zavuch
Switch1(config-vlan)#vlan 3
Switch1(config-vlan)#name Director
Switch1(config-vlan)#vlan 4
Switch1(config-vlan)#name Biblioteka
Switch1(config-vlan)#vlan 5
Switch1(config-vlan)#name Uchitelska
Switch1(config-vlan)#vlan 6
Switch1(config-vlan)#name ActZala
```

Наступним етапом є налаштування комутаторів, що підключені до кінцевих пристроїв. На цих комутаторах необхідно налаштувати відповідні VLAN та перевести порти в режим trunk або в конкретний VLAN відповідно до таблиці 3.3.

Інтерфейс комутатора Fa0/1 переводиться в режим access та призначається до VLAN 20. Для цього використовуються команди: switchport mode access та switchport access vlan 20. Аналогічні налаштування виконуються для інших портів.

На комутаторі Switch1 порти Fa0/23 та Fa0/24 повинні бути переведені в режим trunk, для чого застосовується команда: switchport mode trunk. Незадіяні порти додаються до вимкненого VLAN, який не використовується в мережі, з метою забезпечення безпеки. Це дозволяє уникнути підключення до системи

через незахищені порти комутатора. Налаштування для Switch1 наведене у лістингу 3.3.

Лістинг 4.3 — налаштування комутатора Switch1

```
Switch1(config)#interface range fa0/1-16
Switch1(config-if)#switchport access vlan 20
Switch1(config-if)#interface range fa0/17-18
Switch1(config-if)#switchport access vlan 3
Switch1(config-if)#interface fa0/19
Switch1(config-if)#switchport access vlan 2
Switch1(config-if)#interface fa0/20
Switch1(config-if)#switchport access vlan 4
Switch1(config-if)#interface fa0/21
Switch1(config-if)#switchport access vlan 10
Switch1(config-if)#interface range fa0/1-21
Switch1(config-if)#switchport mode access
Switch1(config-if)#interface range fa0/23-24
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#interface fa0/22
Switch1(config-if)#switchport access vlan 99
Switch1(config-if)#no vlan 99
```

Для отримання короткої інформації про конфігурацію VLAN на комутаторі, використовується команда show vlan brief. Вона виводить список усіх VLAN, що налаштовані на пристрої, разом із їх ідентифікаційними номерами, іменами, а також переліком портів, які належать кожному VLAN. Це зручний спосіб для швидкого перегляду стану VLAN та для перевірки коректності налаштувань. Результат виконання даної команди на комутаторі Switch1 зображено у рисунку 3.10.

Наступним етапом є налаштування маршрутизатора. На схемі між комутатором та маршрутизатором присутнє лише одне фізичне з’єднання, при цьому необхідно реалізувати 8 віртуальних мереж (VLAN).

```
Switch1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
2    Zavuch                           active    Fa0/19
3    Director                         active    Fa0/17, Fa0/18
4    Biblioteka                       active    Fa0/20
5    Uchitelska                       active
6    ActZala                          active
10   Server                           active    Fa0/21
20   Kabinf2                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
30   Kabinf3                          active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch1#
```

Рисунок 3.10 — Опис стану VLAN портів

Для того щоб забезпечити комунікацію між різними VLAN, необхідно створити кілька віртуальних інтерфейсів на одному фізичному інтерфейсі маршрутизатора. Для реалізації між-VLAN маршрутизації використовується підхід Router-on-a-stick. Router-on-a-stick — це метод маршрутизації між VLAN, який використовується для забезпечення комунікації між різними віртуальними мережами (VLAN) через один фізичний інтерфейс маршрутизатора. Цей метод дозволяє зекономити ресурси та зменшити кількість фізичних з’єднань між маршрутизатором і комутаторами, використовуючи один фізичний інтерфейс на маршрутизаторі для роботи з кількома VLAN.

Для налаштування одного інтерфейсу маршрутизатора, який буде використовувати trunk-з’єднання, потрібно створити кілька підінтерфейсів. Після створення підінтерфейсів на маршрутизаторі, кожному з них необхідно призначити відповідний номер VLAN за допомогою команди encapsulation dot1q. Налаштування маршрутизатора Router1 наведено в лістингу 3.4.

Лістинг 3.4 — Налаштування маршрутизатора Router1

```
Router1(config-if)#interface f0/0.10
Router1(config-subif)#encapsulation dot1q 10
Router1(config-subif)#ip address 192.168.100.94 255.255.255.252
```

Продовження лістингу 3.4

```
Router1(config-subif)#interface f0/0.20
Router1(config-subif)#encapsulation dot1q 20
Router1(config-subif)#ip address 192.168.100.30 255.255.255.224
Router1(config-subif)#interface f0/0.30
Router1(config-subif)#encapsulation dot1q 30
Router1(config-subif)#ip address 192.168.100.62 255.255.255.224
Router1(config-subif)#interface f0/0.2
Router1(config-subif)#encapsulation dot1q 2
Router1(config-subif)#ip address 192.168.100.82 255.255.255.252
Router1(config-subif)#interface f0/0.3
Router1(config-subif)#encapsulation dot1q 3
Router1(config-subif)#ip address 192.168.100.70 255.255.255.248
Router1(config-subif)#interface f0/0.4
Router1(config-subif)#encapsulation dot1q 4
Router1(config-subif)#ip address 192.168.100.86 255.255.255.252
Router1(config-subif)#interface f0/0.5
Router1(config-subif)#encapsulation dot1q 5
Router1(config-subif)#ip address 192.168.100.78 255.255.255.248
Router1(config-subif)#interface f0/0.6
Router1(config-subif)#encapsulation dot1q 6
Router1(config-subif)#ip address 192.168.100.90 255.255.255.252
Router1(config-subif)#interface f0/0
Router1(config-if)#no shutdown
```

Налаштування IP-адресації

Після виконання базового налаштування маршрутизатора та комутаторів, наступним етапом є налаштування кінцевих пристроїв. Для цього необхідно відкрити вкладку IP Configuration на комп'ютері та ввести IP-адресу, маску підмережі та адресу шлюзу, які вказані в таблиці 3.2 для відповідного пристрою. Налаштування комп'ютера Kabinf21 продемонстровано на рисунку 3.11.

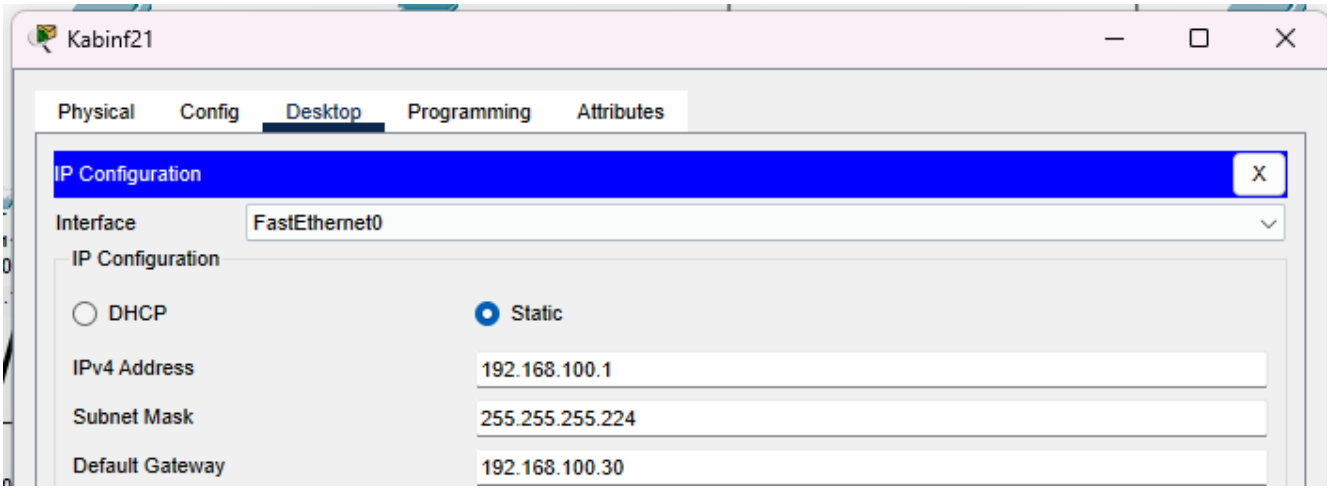

Рисунок 3.11 — Конфігурування основних параметрів комп'ютера

Після завершення налаштування всіх кінцевих пристроїв необхідно перевірити працездатність мережі, надіславши ICMP пакети між різними користувачами. На рисунку 3.3 представлено виконання команди ping з комп'ютера Uchitelska на комп'ютери Kabinf21 та Zavuch.

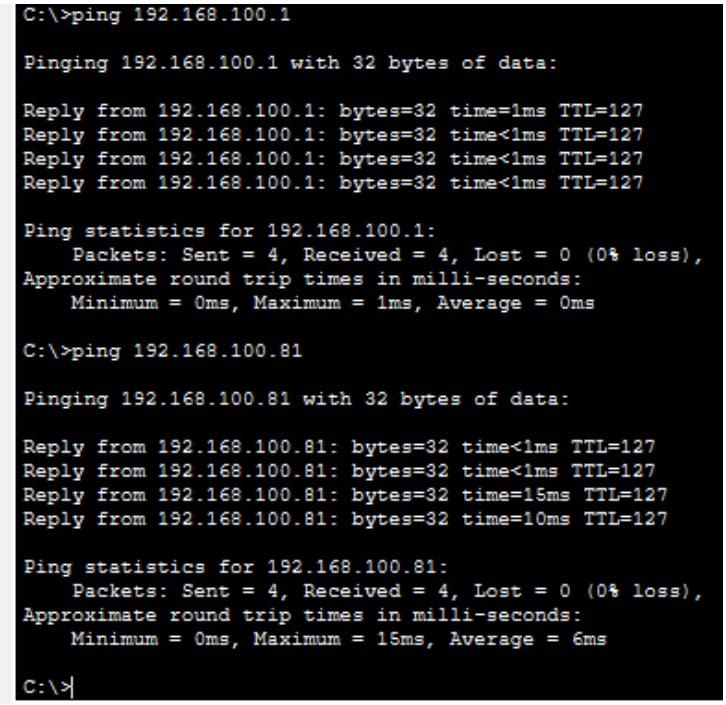

Рисунок 3.12 — Виконання команди ping з Uchitelska

3.5 Захист та підвищення надійності мережі

З метою захисту мережевих пристроїв від несанкціонованого доступу необхідно реалізувати базові заходи безпеки, а саме — встановити паролі на консольне з’єднання, доступ до привілейованого режиму, а також налаштувати автентифікацію для підключення через SSH.

Для обмеження доступу до привілейованого режиму використовується одна з двох команд: enable password або enable secret. Команда enable secret забезпечує автоматичне шифрування пароля в конфігураційному файлі, тоді як enable password зберігає пароль у відкритому вигляді. У разі налаштування обох команд, система надає пріоритет паролю, встановленому за допомогою enable secret.

Захист консольного з’єднання реалізується через налаштування відповідного пароля, що запобігає несанкціонованому фізичному доступу до пристрою. Для цього необхідно перейти в режим конфігурації лінії командою line con 0, задати пароль за допомогою команди password, після чого активувати запит на введення пароля командою login.

З метою попередження користувача про доступ до приватної мережі, до якої він може не мати дозволу, доцільно реалізувати банер-попередження за допомогою команди banner motd. Такий банер слугує повідомленням про політику доступу до системи та може бути використаний як елемент юридичного захисту.

На рисунку 3.13 продемонстровано появу банера привітання та запит пароля при консольному з’єднанні. Крім того, під час переходу до привілейованого режиму користувачу необхідно повторно ввести пароль.

```
UNAUTHORIZED ACCESS IS PROHIBITED! Access is allowed only to authorized users.

User Access Verification

Password:

Switch1>
```

Рисунок 3.15 — Відображення банера-привітання та запит паролю при вході

Слід враховувати, що в середовищі Cisco Packet Tracer під час введення паролів символи не відображаються на екрані (ані текстом, ані замінниками, такими як крапки чи зірочки), що є нормальною поведінкою системи безпеки.

Для забезпечення можливості дистанційного адміністрування мережевих пристроїв доцільно налаштувати один із протоколів віддаленого доступу — Telnet або SSH. У межах даного проекту було обрано SSH (Secure Shell) завдяки його здатності забезпечувати захищене з’єднання через використання механізмів шифрування.

SSH — це мережевий протокол, розроблений для безпечного віддаленого керування пристроями, а також для тунелювання TCP-з’єднань. Під час використання SSH застосовуються різноманітні алгоритми шифрування, що забезпечують конфіденційність, цілісність та автентичність переданих даних. Таким чином, протокол дає змогу здійснювати керування мережевими пристроями без ризику перехоплення критичних даних.

На рисунку 3.5 продемонстровано приклад встановлення SSH-з’єднання з комп’ютера Director до маршрутизатора Router1.

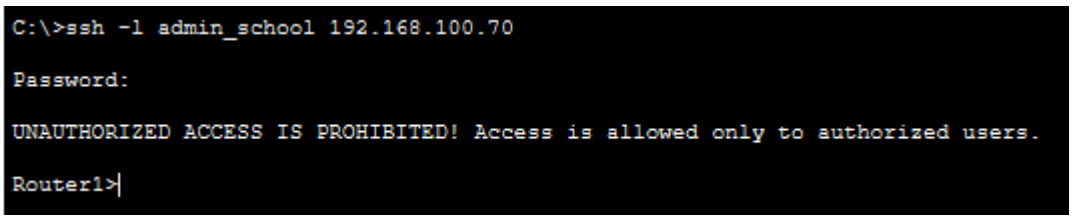

Рисунок 3.5 — Віддалений вхід на Router1за допомогою протоколу SSH

Для забезпечення додаткового рівня безпеки та захисту паролів, що зберігаються у конфігураційному файлі у відкритому вигляді, застосовується команда service password-encryption. Ця команда активує базове шифрування текстових паролів, що зменшує ризик їх компрометації при перегляді конфігурації пристрою. Повний перелік налаштувань підключення та параметрів безпеки мережевих пристроїв представлено у лістингу 3.5.

Лістинг 3.5 — Налаштування підключення та безпеки віддаленого доступу

Switch1>en

Switch1#conf t

Switch1(config)#enable password password

Switch1(config)#enable secret ScHool@123

Switch1(config)# banner motd #UNAUTHORIZED ACCESS IS PROHIBITED! Access is allowed only to authorized users.#

Switch1(config)#ip domain-name google.com

Switch1(config)#crypto key generate rsa

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Switch1(config)#username admin_school secret ScHool@123

*Mar 1 0:38:6.132: %SSH-5-ENABLED: SSH 1.99 has been enabled

Switch1(config)#line vty 0 4

Switch1(config-line)#transport input ssh

Switch1(config-line)#login local

Switch1(config-line)#cdp run

```
Switch1(config)#service password-encryption
Switch1(config)#line con 0
Switch1(config-line)#password ScHool@123
Switch1(config-line)#login
```

Для забезпечення контролю за подіями, що відбуваються в мережевій інфраструктурі, адміністратор може використовувати протокол Syslog. Це стандарт обміну повідомленнями, що дозволяє відправляти та отримувати інформацію про події, які виникають у мережі. Повідомлення Syslog надсилаються на спеціалізований сервер, де вони зберігаються для подальшого аналізу. Такі повідомлення, як правило, містять відомості про час події, ім’я пристрою, на якому вона сталася, а також опис самої події.

Для забезпечення коректної роботи системи журналювання надзвичайно важливо синхронізувати час на всіх мережевих пристроях. З цією метою застосовується NTP (Network Time Protocol) — протокол, призначений для точного та узгодженого налаштування часу в комп’ютерних мережах. Своєчасна синхронізація є критичною для систем, де точне відображення часу має суттєве значення, зокрема — для ведення логів, здійснення фінансових операцій або роботи розподілених інформаційних систем. Налаштування протоколів Syslog та NTP наведено у лістингу 3.6.

Лістинг 3.6 — Налаштування протоколів NTP та Syslog

```
Router1(config)#ntp server 192.168.100.93
Router1(config)#ntp authenticate
Router1(config)#ntp authentication-key 1 md5 cisco
Router1(config)#ntp trusted-key 1
Router1(config)#ntp server 192.168.100.93 key 1
Router1(config)#logging 192.168.100.93
Router1(config)#logging on
Router1(config)#service timestamps log datetime msec
```

У комп’ютерній мережі навчального закладу застосовуються приватні IP-адреси, які не є маршрутизованими в глобальній мережі Інтернет. Для забезпечення виходу локальних пристроїв у зовнішню мережу необхідне використання публічних IP-адрес. Перетворення приватних адрес у публічні здійснюється за допомогою технології NAT (Network Address Translation) — трансляції мережевих адрес.

NAT — це механізм, що дозволяє одному або декільком пристроям з приватними IP-адресами здійснювати комунікацію з публічною мережею шляхом заміни приватної адреси на публічну (і навпаки) під час передавання пакетів. Окрім трансляції адрес, NAT також може змінювати інформацію про порти, що підвищує рівень безпеки завдяки маскуванню внутрішньої структури мережі.

Одним із різновидів NAT є PAT (Port Address Translation) — трансляція портових адрес. Ця технологія дозволяє транслювати велику кількість приватних IP-адрес у одну публічну адресу, використовуючи різні номери портів транспортного рівня, що особливо ефективно в умовах обмеженого пулу публічних адрес.

Налаштування PAT для реалізації доступу до мережі Інтернет з локальної шкільної мережі наведено у лістингу 3.7.

Лістинг 3.7 — Налаштування PAT

```
Router1>enable
Router1#conf t
Router1(config)#acc 1 permit 192.168.100.0 0.0.0.255
Router1(config)#ip nat inside source list 1 int fa0/1 overload
Router1(config)#int fa0/0
Router1(config-if)#ip nat ins
Router1(config-if)#int fa0/1
Router1(config-if)#ip nat out
```

Для моделювання зовнішньої мережі до схеми було додано додатковий маршрутизатор та комп’ютер, які імітують роботу Інтернет-провайдера. Цей сегмент виконує функцію мережі Інтернет, до якої має бути забезпечено доступ з внутрішньої локальної мережі навчального закладу.

На рисунку 3.13 наведено приклад реалізації трансляції мережевих адрес (NAT). Зокрема, на прикладі показано, як під час передачі пакета з внутрішнього маршрутизатора Router1 змінюється IP-адреса відправника. Це підтверджує коректну роботу механізму NAT/PAT, що забезпечує доступ до зовнішньої мережі з приватної адресної області.

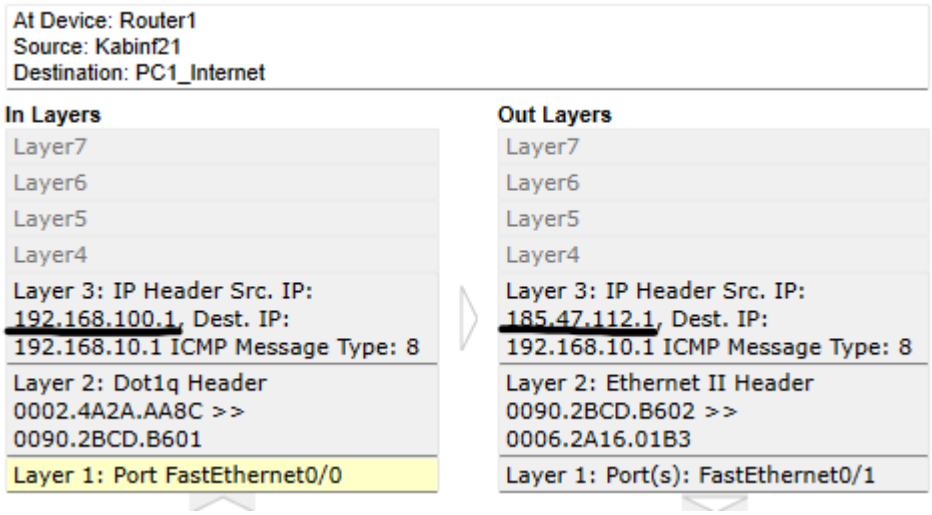

Рисунок 3.12 — Зміна IP-адреси при виході в мережу Інтернет

3.7 Симуляція відправки пакетів у ПЗ

Для візуалізації відправки пакетів у програмному забезпеченні Cisco Packet Tracer, можна використати режим Simulation. У даному режимі є можливість побачити послідовність проходження пакета через мережеві пристрої, перевіряти його стан та вміст на кожному пункті у вигляді моделі OSI або деталях заголовків пакетів.

Процес відсилання пакета в Cisco Packet Tracer у режимі Simulation починається з того, що користувач ініціює передачу даних на пристрої, наприклад, робочій станції. Коли пакет готовий до відправки, на пристрої створюється його структура, що включає не лише дані, але й заголовки різних протоколів, та-

ких як Ethernet, IP, TCP/UDP, в залежності від налаштувань мережі. Після цього, пакет передається через фізичні інтерфейси на наступний пристрій.

Якщо пакет проходить через комутатор, той направляє його до порту, який відповідає за MAC-адресу пристрою призначення. Комутатор не перевіряє IP-адреси, а лише здійснює передачу на основі фізичних адрес. У випадку маршрутизатора, пакет перевіряється на основі IP-адрес, і маршрутизатор використовує свою таблицю маршрутизації для визначення найкращого шляху для пакета, після чого передає його далі. Кожен пристрій у мережі виконує певну роль в обробці і передачі пакета, поки він не досягне кінцевого пристрою, наприклад, робочої станції чи сервера.

На кінцевому пристрої пакет розпаковується, і його вміст передається до відповідного додатка або процесу для подальшої обробки. Весь цей процес у Cisco Packet Tracer у режимі Simulation проходить без затримок, що дає можливість спостерігати передачу даних майже в реальному часі. Це дозволяє користувачам тестувати конфігурації та спостерігати, як пакети переміщуються через мережу, забезпечуючи ефективне навчання і налаштування мережевих сценаріїв. Приклад передачі пакета з кінцевого пристрою Zavuch на кінцевий пристрій Kabinf214 наведено у рисунку 3.13.

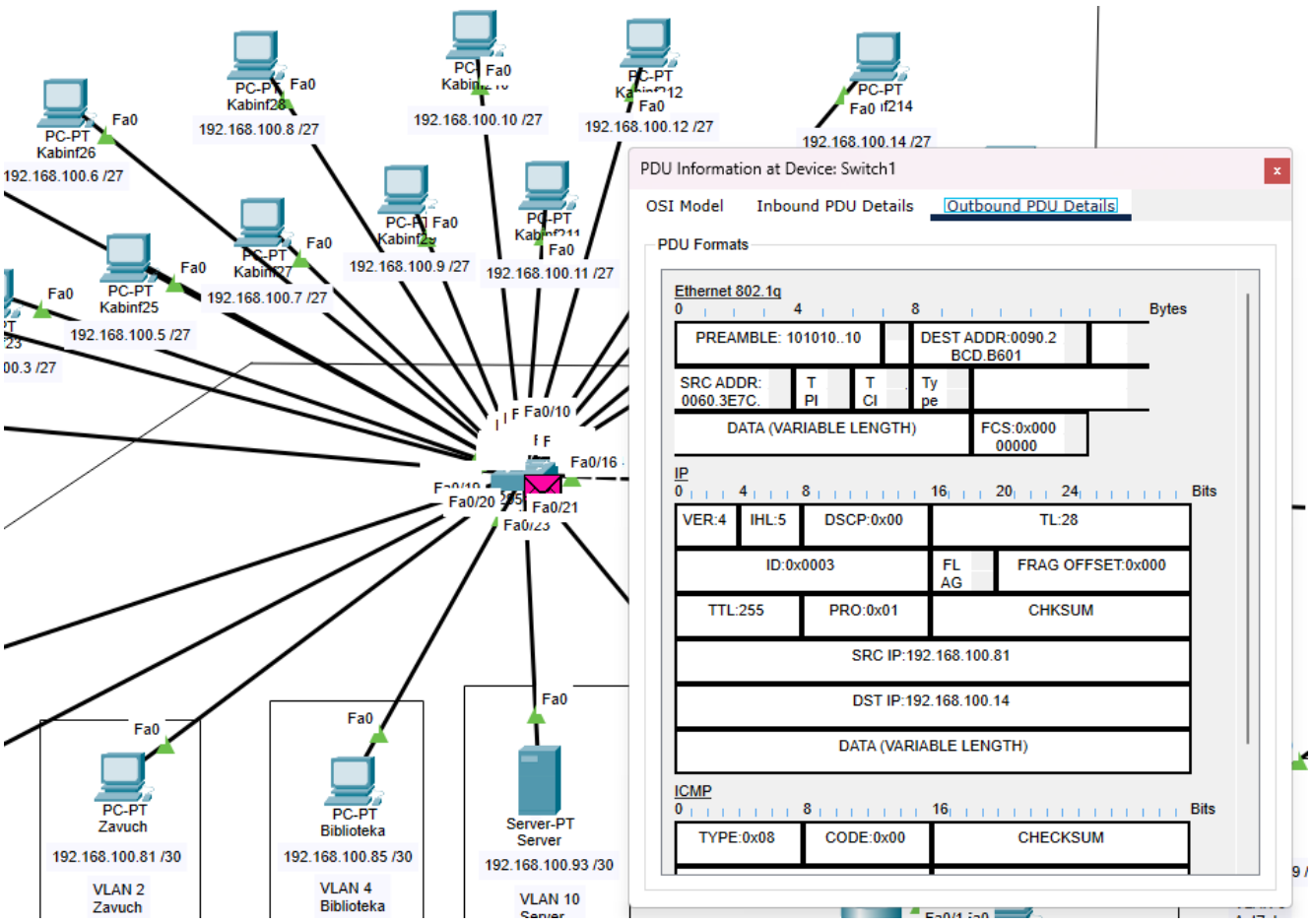

Рисунок 3.13 — Передача пакета в режимі Simulation

У даному розділі було реалізовано повний цикл моделювання комп’ютерної мережі загальноосвітнього навчального закладу. Зокрема, було розроблено план приміщення, обґрунтовано та обрано оптимальну топологію мережі, здійснено розміщення обладнання у відповідних кабінетах, створено модель комп’ютерної мережі в середовищі Cisco Packet Tracer, а також виконано налаштування мережевих пристроїв з урахуванням технічних потреб, фінансових обмежень та вимог інформаційної безпеки. На основі виконаних етапів проектування можна зробити висновок, що поставлена мета щодо створення ефективної, безпечної та економічно обґрунтованої комп’ютерної мережі для школи — досягнута, а всі поставлені задачі успішно реалізовані.

ВИСНОВКИ

В даній кваліфікаційній роботі розглянуті питання розробки локальної мережі для Березівського ліцею Чернівецької селищної ради.

В ході виконання роботи було проведено аналіз завдання, розраховано мережне обладнання та працездатність самої мережі, підібрано оптимальне мережне обладнання, розміщено згідно санітарних вимог всі робочі станції, підібрано мережні імена та IP-адреси.

Необхідним атрибутом практично кожного сучасного комп'ютерного класу є ЛОМ.

Саме ЛОМ надає можливості для повного керування внутрішньою інформацією навчального закладу, здійснювати оперативний доступ до даних з допомогою мережі значно швидше. Керування, передача, обмін та обробка інформації може здійснюватися як між всіма робочими станціями, так і між окремими кабінетами. Керування всією інформацією може здійснюватися безпосередньо з головного ПК, який знаходиться в кабінеті директора. Також, в головному комп'ютері можна встановити рівень доступу до файлів для кожної станції окремо. Це надає велику перевагу в тих випадках, коли деяка інформація повинна бути доступна не для всіх.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1) Комп'ютерна мережа [Електронний ресурс]. URL: https://kppk.com.ua/ELLIB/ebook/Gorbenko/IKT/13/13.htm.
2) Типи мереж [Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/Типи мереж.
3) Топологія мережі [Електронний ресурс]. URL: https://tnpu.edu.ua/index.php.
4) Олесюк. В. Організація комп’ютерної локальної мережі. / Олесюк. В. Тернопіль, 2016. 235с.
5) Локальні мережі [Електронний ресурс]. URL: https://step.org.ua/konspekt/lanwan/tema2.
6) Деревоподібна мережа [Електронний ресурс]. URL: https://uk.warbletoncouncil.org/topologia-de-arbol-15985.
7) Ethernet кабель [Електронний ресурс]. URL: https://www.volta.com.ua/catalog/kabel-provod/telekommunikatsionnyy-kabel/.
8) Коаксіальний кабель [Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/коаксіальний кабель.
9) Мережева карта [Електронний ресурс]. URL: https://lanet.help/blog/shcho-take-merezheva-karta/.
10) Мережева карта TP-LINK TG-3468 [Електронний ресурс]. URL: https://rozetka.com.ua/ua/tp_limnk_tg_3468/p202916/.
11) Комутатор D-Link DGS-1100-24V2/E [Електронний ресурс]. URL: https://www.itbox.ua/ua/product/Komutator_D-Link_DGS-1100-24V2_E-p919232/.
12) Операційна система Windows 10 Professional [Електронний ресурс]. URL: http://vidpoviday.com/windows-10-bezpeka-i-zaxist-vid-zlomu.
13) Технологія DomainJoin [Електронний ресурс]. URL: http://mg-procomp.net.ua/index.php?option=com_content&view.
14) Протоколи TCP/IP [Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/TCP/IP.

15) Антивірус Windows Defender [Електронний ресурс]. URL: https://www.microsoft.com/uk-ua/windows/comprehensive-security.
16) Шестєпалов Є.А. Internet, World Wide Web, Комп'ютерні мережі / Шестєпалов Є.А. Шепетівка, 2018. 134 с.
17) Таблиця місткості короба [Електронний ресурс]. URL: http://www.odicom.com.ua/prod/korob/calc.html.

ДОДАТОК А

Технічне завдання

Міністерство освіти та науки України

Вінницький національний технічний університет

Факультет інформаційних технологій та комп’ютерної інженерії

ЗАТВЕРДЖУЮ

Завідувач кафедри ОТ ВНТУ

д.т.н., проф.

_____О. Д. Азаров

“__” _____ 2025 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання бакалаврської кваліфікаційної роботи
«Комп'ютерна мережа для Березівського ліцею Чернівецької селищної ради»
08-54.БКР.001.00.000 ТЗ

Науковий керівник к.т.н., доц. каф. ОТ

_____ Колесник І.С.

Студент групи 1КІ-23мс

_____ Абрамчук В.О.

Вінниця 2025

1 Найменування та область застосування

Комп'ютерна мережа для Березівського ліцею Чернівецької селищної ради.

2 Основи для розробки

Необхідність реалізації комп'ютерної мережа для Березівського ліцею Чернівецької селищної ради

3 Мета та призначення розробки

Мета дослідження — створення комп'ютерної мережа для Березівського ліцею Чернівецької селищної ради

.

4 Етапи БКР та очікувані результати

Робота виконується у вісім етапів, що наведені в таблиці 4.1.

Таблиця 4.1 — Етапи виконання роботи

з/п	Назва етапів виконання бакалаврського проекту	Строк виконання етапів роботи	Примітка
1	Постановка задачі для створення комп’ютерної мережі	07.03.25	
2	Огляд інформаційних джерел	10.03.25	
3	Аналіз загальних понять та визначень	29.03.25	
4	Вибір компонентів для проектування мережі	22.04.25	
5	Розробка ПЗ комп’ютерної мережі ліцею	11.05.25	
6	Оформлення пояснювальної записки та ілюстративного матеріалу	17.05.25	
7	Аналіз виконання роботи. Висновки. Додатки	01.06.25	
8	Перевірка якості виконання бакалаврського проекту та усунення недоліків	07.03.25	

5 Матеріали, що подаються до захисту БКР

Пояснювальна записка БКР, графічні і ілюстративні матеріали, протокол попереднього захисту БКР на кафедрі, відзив наукового керівника, рецензія опонента, протоколи складання державних екзаменів, анотації до БКР українською та іноземною мовами, довідка про відповідність оформлення БКР діючим вимогам.

6 Порядок контролю виконання та захисту БКР

Виконання етапів графічної та розрахункової документації БКР контролюється науковим керівником згідно зі встановленими термінами. Захист БКР відбувається на засіданні Державної екзаменаційної комісії, затвердженою наказом ректора.

7 Вимоги до оформлювання та порядок виконання БКР.

7.1 При оформлювання БДР використовуються:

— ДСТУ 3008: 2015 «Звіти в сфері науки і техніки. Структура та правила оформлювання»;

— ДСТУ 8302: 2015 «Бібліографічні посилання. Загальні положення та правила складання»;

— міждержавний ГОСТ 2.104-2006 «Єдина система конструкторської документації. Основні написи»;

— Методичні вказівки до виконання бакалаврських кваліфікаційних робіт зі спеціальності 123 «Комп'ютерна інженерія» (освітня програма «Комп'ютерна інженерія»). Кафедра обчислювальної техніки ВНТУ 2022;

— документами на які посилаються у вище вказаних.

7.2 Порядок виконання БКР викладено в «Положення про кваліфікаційні роботи на першому (бакалаврському) рівні вищої освіти СУЯ ВНТУ-03.02.02-П.001.01:21»

ДОДАТОК Б
ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи:

Комп'ютерна мережа для Березівського ліцею Чернівецької селищної ради

Тип роботи: Бакалаврська кваліфікаційна робота
(БДР, МКР)

Підрозділ: кафедра обчислювальної техніки
(кафедра, факультет)

Показники звіту подібності StrikePlagiarism

Оригінальність 91,5 Схожість 9%

Аналіз звіту подібності (відмітити потрібне):

✓ Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

☐ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її автора. Роботу направити на доопрацювання.

☐ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Захарченко С.М.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою StrikePlagiarism щодо роботи.

Автор роботи _____ Абрамчук В.О.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Колесник І.С.
(підпис) (прізвище, ініціали)

ДОДАТОК В

Ілюстративна частина

КОМП’ЮТЕРНА МЕРЕЖА ДЛЯ БЕРЕЗІВСЬКОГО ЛІЦЕЮ ЧЕРНІВЕЦЬКОЇ СЕЛИЩНОЇ РАДИ

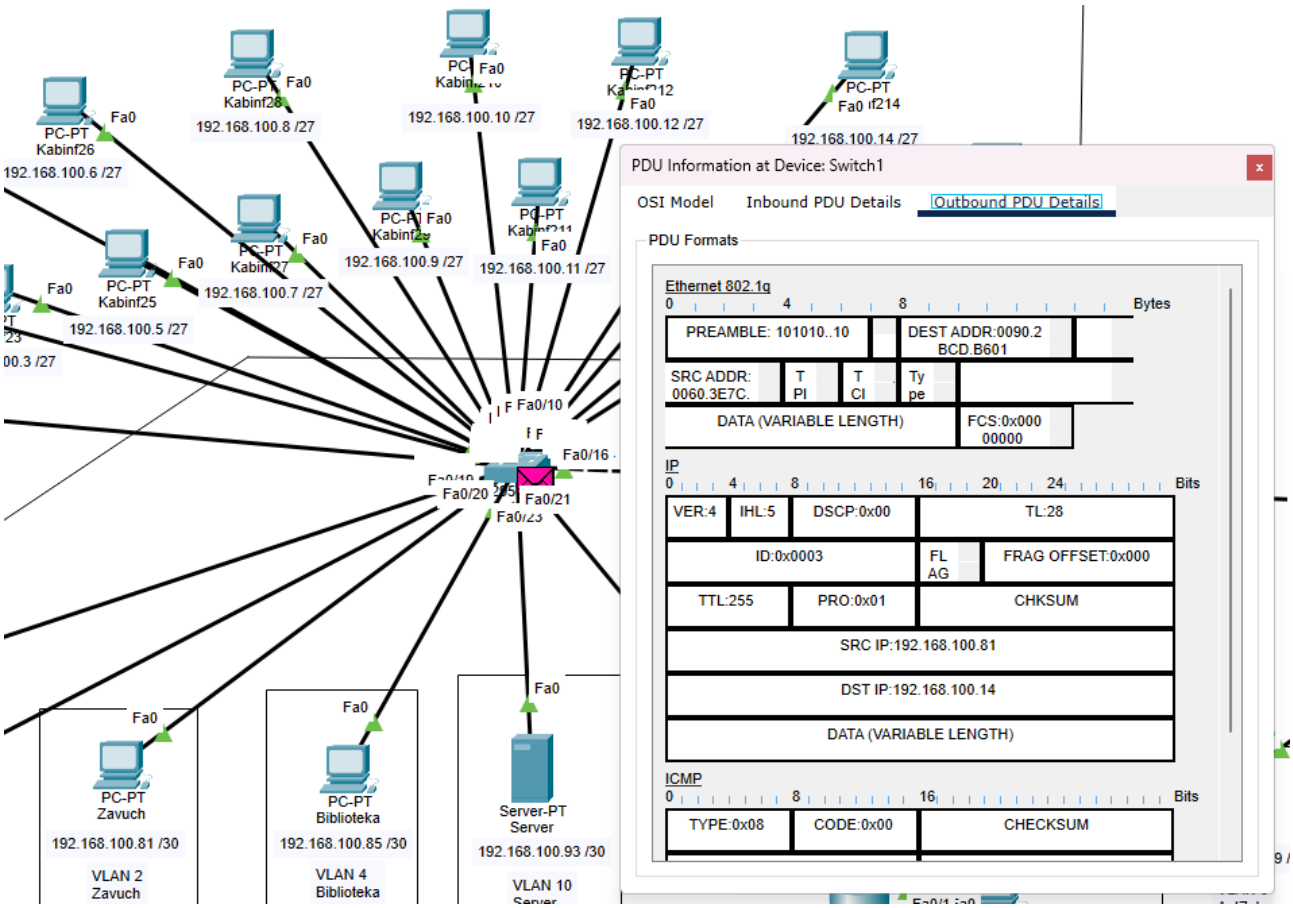

Рисунок В.1 — Схема мережі, спроектована в Cisco Packet Tracer

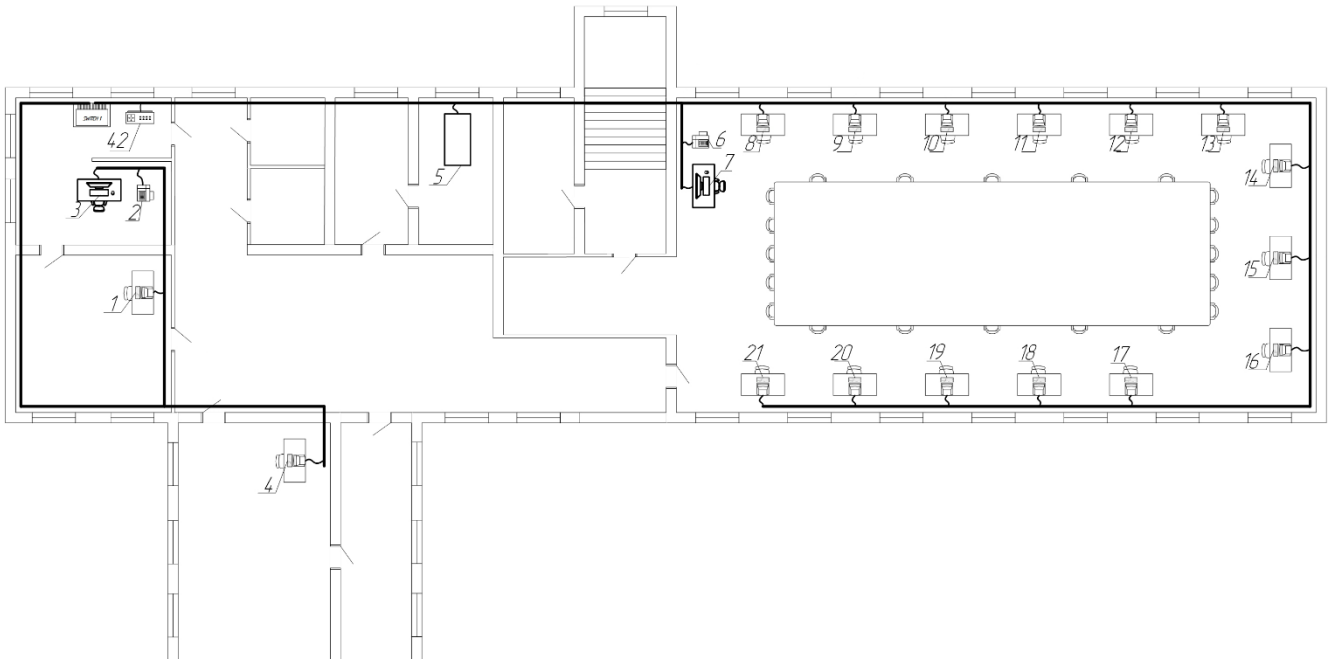

Рисунок В.2 — План приміщення другого поверху школи

ДОДАТОК Г

Лістинг програмного забезпечення

Лістинг .1 — Повний лістинг маршрутизатора Router1

```
Current configuration : 2160 bytes
!
version 15.1
service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router1
!
enable secret 5 $1$mERr$Iq8qfiHzb3PFYNan5gz62/
enable password 7 08314D5D1A0E0A0516
!
ip cef
no ipv6 cef
!
username admin_school secret 5 $1$mERr$Iq8qfiHzb3PFYNan5gz62/
!
license udi pid CISCO2811/K9 sn FTX10179JES-
!
ip domain-name google.com
!
spanning-tree mode pvst
!
interface FastEthernet0/0
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip address 192.168.100.82 255.255.255.252
 ip nat inside
!
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip address 192.168.100.70 255.255.255.248
 ip nat inside
!
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.168.100.86 255.255.255.252
 ip nat inside
!
```

```
interface FastEthernet0/0.5
 encapsulation dot1Q 5
 ip address 192.168.100.78 255.255.255.248
 ip nat inside
!
interface FastEthernet0/0.6
 encapsulation dot1Q 6
 ip address 192.168.100.90 255.255.255.252
 ip nat inside
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.100.94 255.255.255.252
 ip nat inside
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.100.30 255.255.255.224
 ip nat inside
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.100.62 255.255.255.224
 ip nat inside
!
interface FastEthernet0/1
 ip address 185.47.112.1 255.255.255.0
 ip nat outside
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
router rip
!
ip nat inside source list 1 interface FastEthernet0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 185.47.112.254
!
ip flow-export version 9
!
access-list 1 permit 192.168.100.0 0.0.0.255
!
banner motd ^CUNAUTHORIZED ACCESS IS PROHIBITED! Access is allowed only to
authorized users.^C
!
logging 192.168.100.93
line con 0
 password 7 08124F660616093743595F
 login
```

```
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
!
ntp authentication-key 1 md5 0822455D0A16 7
ntp authenticate
ntp trusted-key 1
ntp server 192.168.100.93 key 1
!
end
```

ДОДАТОК Д

Лістинг комутатора

Лістинг Д.1 — Повний лістинг комутатора Switch1

```
Current configuration : 2643 bytes
!
version 12.1
service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Switch1
!
enable secret 5 $1$mERr$Iq8qfiHzb3PFYNan5gz62/
enable password 7 08314D5D1A0E0A0516
!
ip domain-name google.com
!
username admin_school secret 5 $1$mERr$Iq8qfiHzb3PFYNan5gz62/
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/7
```

```
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/20
```

```
 switchport access vlan 4
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 99
!
interface FastEthernet0/23
 switchport mode trunk
!
interface FastEthernet0/24
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan20
 ip address 192.168.100.29 255.255.255.224
!
banner motd ^CUNAUTHORIZED ACCESS IS PROHIBITED! Access is allowed only to
authorized users.^C
logging 192.168.100.93
!
line con 0
 password 7 08124F660616093743595F
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login
!
ntp authenticate
ntp trusted-key 1
ntp server 192.168.100.93 key 1
!
end
```

ДОДАТОК Е

Лістинг комутатора

Лістинг Е.1 — Повний лістинг комутатора Switch2

```
Current configuration : 2623 bytes
!
version 12.1
service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Switch2
!
enable secret 5 $1$mERr$Iq8qfiHzb3PFYNan5gz62/
enable password 7 08314D5D1A0E0A0516
!
ip domain-name google.com
!
username admin_school secret 5 $1$mERr$Iq8qfiHzb3PFYNan5gz62/
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/7
```

```
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 5
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 5
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 5
 switchport mode access
!
interface FastEthernet0/20
```

```
 switchport access vlan 6
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 99
!
interface FastEthernet0/22
 switchport access vlan 99
!
interface FastEthernet0/23
 switchport access vlan 99
!
interface FastEthernet0/24
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan30
 ip address 192.168.100.61 255.255.255.224
!
banner motd ^CUNAUTHORIZED ACCESS IS PROHIBITED! Access is allowed only to
authorized users.^C
logging 192.168.100.93
!
line con 0
 password 7 08124F660616093743595F
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login
!
ntp authenticate
ntp trusted-key 1
ntp server 192.168.100.93 key 1
!
end
```